Franz Lemmermeyer

Binary Quadratic Forms

An Elementary Approach to the Arithmetic of Elliptic and Hyperelliptic Curves

November 8, 2010

Franz Lemmermeyer
email hb3@ix.rzuser.uni-heidelberg.de
WWW http://www.rzuser.uni-heidelberg.de/~hb3/

Preface

Quadratic forms are everywhere. Even in elementary number theory, many of the most beautiful theorems deal with quadratic forms. The following gives a small list of well known and less well known results involving quadratic forms.

Binary Quadratic Forms

- The most famous result in elementary number theory involving binary quadratic forms is Fermat's Two-Squares Theorem: every positive prime $p \equiv 1 \bmod 4$ can be written in the form $p = x^2 + y^2$. Lurking in the background is the first supplementary law of quadratic reciprocity: -1 is a square modulo an odd prime p if and only if $p \equiv 1 \bmod 4$.
- Solving the Pell equation $x^2 - my^2 = 1$ requires finding representations of 1 by binary quadratic forms such as $x^2 - my^2$.
- The first conceptual proof of the quadratic reciprocity law provided by Gauss used his theory of binary quadratic forms.
- One of Euler's first conjectures in the theory of higher power residues was the following result first proved by Gauss: 2 is a fourth power modulo a prime $p \equiv 1 \bmod 4$ if and only if $p = a^2 + 64b^2$.

Ternary Quadratic Forms

- One of Fermat's first conjectures claimed that every positive integer is the sum of three triangular numbers; these are numbers of the form $n(n+1)/2$. Fermat observed that this would follow from the fact that numbers $N \equiv 3 \bmod 8$ are sums of three squares. Euler and Legendre stated more precisely that every positive integer not of the form $4^m(8n+7)$ can be written as a sum of three squares, a result which was finally proved by Gauss.
- The first partial proof of the quadratic reciprocity law was obtained by Legendre with the help of ternary quadratic forms.
- A natural number $n \geq 1$ is called congruent if it is the area of a right angled triangle with rational sides; equivalently n is congruent if there is a rational number x such that $x^2 - n$ and $x^2 + n$ both are squares of rational numbers.
  Assuming the truth of the conjecture of Birch and Swinnerton-Dyer on elliptic curves, Tunnell showed that an odd integer n is congruent if and only if $A_p = 2B_p$, where
  $$A_p = \#\{(a,b,c) : 2a^2 + b^2 + 8c^2 = n\},$$
  $$B_p = \#\{(a,b,c) : 2a^2 + b^2 + 32c^2 = n\}.$$
  It is easily checked that $A_1 = B_1 = 2$ (the only solutions of $2a^2 + b^2 + 8c^2 = 1$ are $(a,b,c) = (0, \pm 1, 0)$) and $A_3 = B_3 = 4$, hence $n = 1$ and $n = 3$ are not congruent; on the other hand it is even more obvious that $A_5 = B_5 = 0$ and $A_7 = B_7 = 0$, which shows that $n = 5$ and $n = 7$ are congruent (modulo the BSD-conjecture).
  Tunnell also gave a similar criterion for $2n$ to be congruent.

Quaternary Quadratic Forms

- The 4-squares theorem by Fermat, Euler and Lagrange: every positive integer n is the sum of four squares, that is, $n = x^2 + y^2 + z^2 + w^2$.
- Langlands gave a concrete example of his very general conjecture about nonabelian reciprocity laws involving the quaternary quadratic forms

$$P(x, y, u, v) = x^2 + xy + 3y^2 + u^2 + uv + 3v^2 \tag{0.1}$$
$$Q(x, y, u, v) = 2(x^2 + y^2 + u^2 + v^2) + 2xu + xv + yu - 2yv \tag{0.2}$$

and the elliptic curve $E : y^2 + y = x^3 - x^2 - 10x - 20$. For each integer $k \geq 0$ define

$$n(P, k) = \#\{(a, b, c, d) \in \mathbb{Z}^4 : P(a, b, c, d) = k\},$$
$$n(Q, k) = \#\{(a, b, c, d) \in \mathbb{Z}^4 : Q(a, b, c, d) = k\}.$$

For any prime $p \neq 11$ put

$$a_p = \#E(\mathbb{F}_p) - p,$$

where $\#E(\mathbb{F}_p)$ denotes the number of solutions of the congruence $y^2 + y \equiv x^3 - x^2 - 10x - 20 \bmod p$.

Then Langlands claims that for any prime $p \neq 11$, we have

$$4a_p = n(P, p) - n(Q, p).$$

The special role of the prime 11 is explained partially by the observation that $4P(x, y, u, v) = (2x + y)^2 + 11y^2 + (2u + v)^2 + 11v^2$.

The major part of Gauss's Disquisitiones Arithmeticae is devoted to quadratic forms, and the most technical section is the explanation of composition of forms. In the proofs of the results above, composition play no role at all. Moreover, just about everyone regards the theory of binary quadratic forms as an antiquated version of ideal theory in quadratic fields. If the theory of composition of forms is not necessary for understanding or proving theorems such as those quoted above, then why should anyone bother learning the classical theory? Here are a few reasons:

- Modern algorithms for computing the structure of the class group of quadratic number fields or for finding the size of the smallest solution of the Pell equations as well as for solving a host of related problems all involve reduction and composition of forms.
  Of course the relevant algorithms can (and most of the time are) described in ideal theoretic terms, but the point is that they were *discovered* using forms.
- Similarly, many fundamental concepts were invented by people working with quadratic forms: let me just mention Shanks' discovery of the infrastructure or the Stark conjectures (half of Stark's first paper on this topic deals with the arithmetic of binary quadratic forms "because it is very difficult to find this material today").
- Cryptographers need to compute with elements of the Jacobians of elliptic and hyperelliptic curves. The group law on elliptic curves is easily explained geometrically, but algorithms for hyperelliptic curves cannot hide their origin in the theory of composition of quadratic forms.

These examples show that there are plenty of reasons for learning more about the classical theory of binary quadratic forms. I have to admit, however, that what made me eventually sit down and study composition of forms was none of the reasons listed above. It is quite exciting to learn beautiful theories, but it is hard work to go through technical details, and composition of forms is filled with all kinds of technicalities. I certainly was in good company with my attitudes on composition; Gordon Pall starts his article [Pal1973] on Gauss composition with the following words:

> At least two recent writers[1] have described Gauss's theory of composition of binary quadratic forms as a tour de force, and not a few mathematicians have told me it was much too complicated.

Dan Shanks [Sh1989a] has made similar experiences: he remarks that

> It was frequently said that composition is "difficult", sometimes even "very difficult"

and observes that

> many number-theorists seem to have a real fear of composition; we might call it *compophobia*. They are uncomfortable until they can translate it into ideals, continued fractions, or some other formalism that they feel they understand better.

What eventually converted me into a dedicated follower of the language of quadratic forms was the simple fact that binary quadratic forms were necessary for understanding what I have called the arithmetic of Pell conics: the role that principal homogeneous spaces play in the arithmetic of elliptic curves is played by conics $Q(x, y) = 1$ in the theory of Pell conics, where $Q(x, y)$ is a binary quadratic form having the same discriminant as the Pell conic.

Then I got hold of unpublished lecture notes [Hel1986] by Hellegouarche, where the group law on elliptic curves is discussed via quadratic forms (and modules) over polynomial rings $\mathbb{F}_p[T]$. Bhargava's charming exposition [Bha2001] of Gauss composition appeared just at the right time, and the present book contains an introduction to the classical theory using Bhargava's cubes. My aim was showing that the theory of quadratic forms is anything but oldfashioned; the theory can be developed using modern techniques in such a way that the simplicity and inherent beauty of the theory of binary quadratic forms becomes obvious.

This book consists of two parts. In the first, we introduce binary quadratic forms with integral coefficients, and discuss the basic notions such as reduction and composition. Then we continue with binary quadratic forms over polynomial rings and derive the group laws on Jacobians of elliptic and hyperelliptic curves[2]. For getting to these group laws as fast as possible it is sufficient to work through Sections 1.1 – 1.4, 2.1 – 2.4, 3.1 – 3.2, and 4.4.

The second part deals with various applications to algorithmic number theory and cryptography.

There are several classical introductions to the theory of binary quadratic forms and the Pell equation; here is a list of those I like best:

- Mathews [Mat1892] is perhaps *the* classical textbook on binary quadratic forms after Dedekind's edition of Dirichlet's lectures.
- Flath [Fla1989] presents the main content of the Disquisitiones Arithmeticae in modern language; a treatment a lot closer to the original can be found in Venkov's book [Ven1970].
- Cox [Co1989] is mainly interested in positive definite forms because his goal is to study complex multiplication, right up to the solution of Gauss's class number 1 problem (modulo some results from class field theory, which are explained but not proved).
- Buchmann & Vollmer [BV2007] emphasize the algorithmic aspect of quadratic forms.
- Jacobson & H. Williams [JW2009] give a modern account of methods for solving the Pell equation.

[1] Apparently, H. Cohn [Coh1962] was one of them.

[2] I intend continuing this part in a second volume, where the descent on Pell conics will be described up to the proof of the analog of the Birch and Swinnerton-Dyer conjecture for elliptic curves.

In this book I have mainly used original articles, all of which are mentioned and discussed in the historical part. For certain topics, I have used some sources more extensively:

- The reduction of indefinite forms is based on Zagier's excellent book [Zag1981].
- The composition of forms is based on Bhargava's articles on Gauss composition, in particular [Bha2002, Bha2004a]; the actual algorithm for composition of forms is a modified version of Speiser's account in [Spe1912].
- The discussion of forms with nonfundamental discriminants owes a lot to the presentation given by Jung [Ju1936].
- The theory of quadratic forms with coefficients in $\mathbb{F}_p[T]$ and the group law on the Jacobians of elliptic and hyperelliptic curves is close to the treatment in Hellegouarche [Hel1986].

Most of the material in this book was used in various undergraduate courses in elementary number theory (reduction and composition of positive definite quadratic forms, the basic arithmetic of the domain $\mathbb{F}_p[T]$), cryptography (group laws on conics and elliptic curves), algebraic geometry (Mason's Theorem), or algebraic number theory (quadratic forms over $\mathbb{F}_p[T]$, Jacobians of elliptic and hyperelliptic curves).

Prerequisites are elementary number theory up to quadratic reciprocity, some linear algebra, and a little bit of abstract algebra (groups, rings, unique factorization domains etc.).

Acknowledgements

Jeff Lagarias

I thank Samuel Hambleton for various contributions, most notably the group structure on Pell surfaces. Brian Conrad, Keith Conrad and Torsten Ekedahl showed me how to look at forms over fields with characteristic 2.

Contents

1. Reduction of Binary Quadratic Forms

A *form* of degree n in r variables over some ring R is a homogeneous polynomial in $R[x_1, \ldots, x_r]$, that is, an R-linear combination of monomials $x_1^{a_1} \cdots x_r^{a_r}$ with constant degree $n = a_1 + \ldots + a_r$. Thus a *quadratic form* q in r variables $x_1, \ldots, x_r$ is an expression of the form $q = \sum_{i,j} a_{ij} x_i x_j$, where the coefficients a_{ij} $(1 \le i, j \le r)$ are from some fixed domain R.

A *binary quadratic form* is a quadratic form in two variables; we will usually write

$$Q(x, y) = Ax^2 + Bxy + Cy^2,$$

and abbreviate this by $Q = (A, B, C)$. Forms in three or four variables are called *ternary* and (*quaternary*, ...) quadratic forms, respectively.

Our principal object of study are binary quadratic forms whose coefficients A, B, C are taken from the ring of integers $\mathbb{Z}$; for understanding elliptic and hyperelliptic curves, however, we will later also have to study quadratic forms whose coefficients are taken from polynomial rings $k[T]$ over fields k.

The integer $\Delta = B^2 - 4AC$ is called the *discriminant* of the form Q. For example, $(1, 0, 1)$ denotes the form $x^2 + y^2$ with discriminant $\Delta = -4$. We say that an integer n is *represented* by Q if there exist integers x, y such that $Q(x, y) = n$, and that n is *represented primitively*[1] by Q if we can find coprime integers x, y with $Q(x, y) = n$. For example, 4 is represented primitively by $Q = (1, 0, 3)$ since $Q(1, 1) = 4$; the representation $Q(2, 0) = 4$ is not primitive.

We get the integers represented by a form (dA, dB, dC) by multiplying the integers represented by (A, B, C) by d. We will therefore usually only consider forms (A, B, C) with $\gcd(A, B, C) = 1$; such forms are called *primitive*.

The central question we will study in this chapter is the following: which integers (and, more specifically, which primes) are represented (primitively) by a given (primitive) binary quadratic form Q?

Answering this seemingly innocent question quickly leads us into areas that were (and still are) important for the development of algebraic number theory: reciprocity laws and class fields. We know from elementary number theory that the following conditions on odd primes p are equivalent:

1. $p \equiv 1 \bmod 4$;
2. $i^2 \equiv -1 \bmod p$ is solvable for some $i \in \mathbb{Z}$, i.e., $(\frac{-1}{p}) = +1$;
3. $p = x^2 + y^2$ is a sum of two integral squares.

The directions 3. $\Longrightarrow$ 2. $\Longrightarrow$ 1. are easy to prove; the claim 1. $\Longrightarrow$ 2. is the difficult part of the first supplementary law of quadratic reciprocity. For showing that 2. implies 3. one has to prove the following claim: if p divides a sum o two coprime squares, then p itself is a sum of two squares. Fermat and Euler used infinite descent to prove such statements;

[1] The classical terminology is “represented properly”; using the word “primitive” seems, however, more natural.

Lagrange developed a reduction theory of quadratic forms which allowed to prove similar results almost instantaneously.

Studying the prime divisors of more general forms $x^2 + ay^2$ led Euler, Lagrange, and Legendre to the discovery of the quadratic reciprocity law. Here are a few of their main results generalizing the equivalence of conditions 1. – 3. above:

congruence	condition	form
$p \equiv 1 \bmod 4$	$x^2 \equiv -1 \bmod p$	$p = x^2 + y^2$
$p \equiv 1 \bmod 3$	$x^2 \equiv -3 \bmod p$	$p = x^2 + 3y^2$
$p \equiv \pm 1 \bmod 8$	$x^2 \equiv +2 \bmod p$	$p = x^2 - 2y^2$
$p \equiv 1, 3 \bmod 8$	$x^2 \equiv -2 \bmod p$	$p = x^2 + 2y^2$

As in the case of two squares above, the equivalence of the first and the second column (for primes not dividing the discriminant) is a consequence of the quadratic reciprocity law, which Euler discovered but could not prove; the special cases needed for the table above were, however, already known to Euler. The equivalence of the second and the third column requires different techniques: while the direction 3. $\Longrightarrow$ 2. is easy to prove (if e.g. $p = x^2 - 2y^2$ is an odd prime, then $x^2 \equiv 2y^2 \bmod p$, hence $2 \equiv (\frac{x}{y})^2 \bmod p$), the other direction lies deeper: if $x^2 \equiv 2 \bmod p$, then $p \mid x^2 - 2 \cdot 1^2$, so it suffices to solve the following

Problem. *Every odd prime divisor of a number of the form $x^2 - ay^2$ $(a = -1, \pm 2, \pm 3)$ with coprime integers x, y again has this form.*

Lagrange attacked this problem by observing that certain forms can be transformed into each other; transforming forms with large coefficients into forms with small coefficients is the essence of Lagrange's theory of reduction.

1.1. The Action of the Modular Group

Where the group of 2×2-matrices with integral coefficients and determinant 1 enters the stage as an actor on quadratic forms with given discriminant.

Consider the quadratic form $Q = (2, 2, 1)$ with discriminant $\Delta = -4$. The identity $Q(x, y) = 2x^2+2xy+y^2 = (x+y)^2+y^2$ implies that $Q = (2, 2, 1)$ and $Q' = (1, 0, 1)$ represent exactly the same integers. In fact, we have $Q(x, y) = Q'(x+y, y)$ and $Q'(x, y) = Q(x, y-x)$. Forms that can be transformed into each other by transformations similar to the one above will be called equivalent; the proper definition uses the *special linear group* (also called the *modular group*; it is connected with modular forms)

$$\mathrm{SL}_2(\mathbb{Z}) = \Big\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \;\Big|\; r, s, t, u \in \mathbb{Z}, ru - st = +1 \Big\}.$$

For any matrix $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and a quadratic form $Q = (A, B, C)$ we define a new quadratic form $Q' = (A', B', C')$ by putting

$$Q'(x, y) = Q\big((x, y)S'\big) = Q(rx + sy, tx + uy), \tag{1.1}$$

(where S' is the transpose of S) and write $Q' = Q|_S$. A quick calculation shows that A', B', C' are integers defined by

$$\left.\begin{aligned} A' &= Ar^2 + Brt + Ct^2, \\ B' &= 2(Ars + Ctu) + B(ru + st), \\ C' &= As^2 + Bsu + Cu^2. \end{aligned}\right\} \tag{1.2}$$

These equations can also be written in matrix[2] form

$$\begin{pmatrix} A' \\ B' \\ C' \end{pmatrix} = \begin{pmatrix} r^2 & rt & t^2 \\ 2rs & ru+st & 2tu \\ s^2 & su & u^2 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix}. \tag{1.3}$$

Definition. Two binary quadratic forms Q and Q' are called *equivalent*[3] (we write $Q' \sim Q$) if there exists a matrix $S \in \mathrm{SL}_2(\mathbb{Z})$ such that $Q' = Q|_S$. This is an equivalence relation (see Ex. 1Reduction of Binary Quadratic Formschapter.1.1ExercisesItem.79 – 1Reduction of Binary Quadratic Formschapter.1.2ExercisesItem.80), and the equivalence class containing Q will be denoted by $[Q]$. The number of equivalence classes of primitive forms with discriminant Δ will be shown to be finite; it is called the *class number* of Δ in the strict sense and will be denoted by $h^+(\Delta)$. We will later also introduce a class number $h(\Delta)$ in the wide (or usual) sense, and show that $h(\Delta) = h^+(\Delta)$ for negative discriminants. For this reason, we will denote the class number in the strict sense also by $h(\Delta)$ if $\Delta < 0$.

The most important transformation operations are the following:

- The shift operation using the matrix $T = T_n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$; for $Q = (A, B, C)$ we find $Q' = Q|_T = (A, B + 2An, C')$ for $C' = An^2 + Bn + C = Q(n, 1)$. The shift operation is used to reduce the middle coefficient B modulo $2A$.
- The flip $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ transforms $Q = (A, B, C)$ into $Q' = Q|_S = (C, -B, A)$.

In particular we have the relations $(A, -A, C) \sim (A, A, C)$ (shift by $n = -1$) and $(A, -B, A) \sim (A, B, A)$ (flip). In general, however, it is not true that $(A, -B, C) \sim (A, B, C)$, although both forms represent the same integers.

For studying the representation of integers by forms it seems more natural to call two forms equivalent if they can be transformed into each other by matrices in

$$\mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \;\middle|\; r, s, t, u \in \mathbb{Z}, ru - st = \pm 1 \right\}.$$

Such a notion of equivalence was used by Lagrange and Legendre; Gauss almost apologized for replacing it by $\mathrm{SL}_2(\mathbb{Z})$-equivalence, but promised that the reason for doing so would become clear eventually.

Remark. Clearly, the identity matrix $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ acts trivially on quadratic forms; but so does its negative, $-I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. For this reason, we often consider the *projective special linear group* $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$. Its elements are represented by matrices $M \in \mathrm{SL}_2(\mathbb{Z})$, but we identify the matrices M and $-M$. Observe that $S^2 = -I$ for $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, hence S has order 4 in $\mathrm{SL}_2(\mathbb{Z})$, but order 2 in $\mathrm{PSL}_2(\mathbb{Z})$.

Having defined the notion of equivalence of forms, there are a couple of questions that immediately suggest themselves:

1. What can we say about the number of equivalence classes?
2. Given two forms Q and Q', how can we decide in finitely many steps whether they are equivalent or not?
3. Given two equivalent forms Q and Q', how can we determine a matrix $S \in \mathrm{SL}_2(\mathbb{Z})$ with $Q' = Q|_S$?

The key to answering these questions is the theory of reduction, which will be discussed in the next section. First, however, we will add some more Linear Algebra to our toolbox.

[2] The 3×3-matrix occurring in (1.3The Action of the Modular Groupequation.1.1.3) has interesting properties; see e.g. Exer. 1Reduction of Binary Quadratic Formschapter.1.13ExercisesItem.93. We also remark that the matrix occurs as an automorph of a certain ternary quadratic form.

[3] This version of equivalence is called equivalence in the strict sense; Gauss called two such forms properly equivalent. Later we will also introduce equivalence in the wide sense.

Some more Linear Algebra.

Linear algebra is an important tool that helps us understand certain aspects of quadratic forms. To every form $Q = (A, B, C)$ we can attach symmetric matrices

$$M(Q) = \begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} \qquad \text{and} \qquad m(Q) = \frac{1}{2} M(Q) = \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}.$$

The advantage of using $M(Q)$ is mainly typographical, because there are no fractions involved if Q has integral coefficients. On the other hand, $m(Q)$ is often more natural; for example, we have

- $4Q(x, y) = (x, y)M(Q)\binom{x}{y}$, but $Q(x, y) = (x, y)m(Q)\binom{x}{y}$.

The following facts can be checked in a straightforward manner:

- $\operatorname{disc} Q = -\det M(Q) = -4 \operatorname{disc} m(Q)$.
- The matrix $M(Q|_S)$ attached to the quadratic form $Q' = Q|_S$ is given by

  $$M(Q|_S) = S'M(Q)S$$

  (here S' denotes the transpose of the matrix S):

  $$\begin{aligned} S'M(Q)S = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} &= \begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} 2Ar + Bt & 2As + Bu \\ Br + 2Ct & Bs + 2Cu \end{pmatrix} \\ &= \begin{pmatrix} 2Ar^2 + 2Brt + 2Ct^2 & 2Ars + 2Ctu + B(ru + st) \\ 2Ars + 2Ctu + B(ru + st) & 2As^2 + 2Bsu + 2Cu^2 \end{pmatrix} \end{aligned}$$

- This implies that

  $$\operatorname{disc} Q' = -\det M(Q|_S) = -(\det S)^2 \det M(Q) = (\det S)^2 \operatorname{disc} Q,$$

  and since $S \in \mathrm{SL}_2(\mathbb{Z})$ has determinant 1, we conclude that $\operatorname{disc} Q' = \operatorname{disc} Q$: the discriminant of a form is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$.
- We also have $M(Q|_{ST}) = (ST)'M(Q)(ST) = T'S'M(Q)ST$, hence $Q|_{ST} = (Q|_S)|_T$: this is usually expressed by saying that $\mathrm{SL}_2(\mathbb{Z})$ acts on quadratic forms from the right.

We can now give a simple proof for

Proposition 1.1. *Let $Q = (A, B, C)$ be a quadratic form, $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ an element of the modular group $\mathrm{SL}_2(\mathbb{Z})$, and $Q' = (A', B', C') = Q|_S$. Then*

1. $\operatorname{disc} Q = \operatorname{disc} Q'$.
2. $\gcd(A, B, C) = \gcd(A', B', C')$.
3. *If $\Delta < 0$, then A and A' have the same sign.*
4. *$Q(x, y) = Q'(u, v)$, where $\binom{u}{v} = S^{-1}\binom{x}{y}$.*
5. *Q and Q' represent exactly the same integers.*
6. *Q and Q' represent exactly the same integers primitively.*

Proof. 1. We already proved this.

2. From (1.1The Action of the Modular Groupequation.1.1.1) it is clear that $\gcd(A, B, C) \mid \gcd(A', B', C')$. Since $Q = Q'|_{S^{-1}}$, we also have $\gcd(A', B', C') \mid \gcd(A, B, C)$, and this implies the claim.
3. Assume that $\Delta = B^2 - 4AC < 0$. Then $4AA' = 4A^2r^2 + 4ABrt + 4ACt^2 = (2Ar + Bt)^2 - \Delta t^2 \geq 0$, with equality if and only if $r = t = 0$. But this would imply $\det S = 0$, hence $AA' > 0$.

4. Write $M = M(Q)$; then $4n = (x,y)M\binom{x}{y}$. Since $M(Q|_S) = S'MS$, we find that $4n = 4Q|_S(u,v) = (u,v)S'MS\binom{u}{v}$ for the vector $\binom{u}{v} = S^{-1}\binom{x}{y}$.
5. Assume that $n = Q(x,y)$ for integers x, y. Since $S \in \mathrm{SL}_2(\mathbb{Z})$, we have $S^{-1} \in \mathrm{SL}_2(\mathbb{Z})$ as well, and this means that u and v are integers.
6. From $\binom{u}{v} = S^{-1}\binom{x}{y}$ we get $\gcd(x,y) \mid \gcd(u,v)$, and the relation $\gcd(u,v) \mid \gcd(x,y)$ follows from symmetry.

This completes the proof. $\square$

Example 1. $Q(x,y) = x^2 + y^2$ represents $5 = 2^2 + 1^2$. With $S = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ we have found $Q|_S(x,y) = 5x^2 + 6xy + 2y^2$. Now $S^{-1} = \left(\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right)$, hence $S^{-1}\binom{2}{1} = \binom{1}{0}$, and indeed we have $Q|_S(1,0) = 5$.

Example 2. The forms $Q = (1,0,5)$ and $Q' = (2,2,3)$ both have discriminant $\Delta = -20$; they are not equivalent, since the first form represents 1, whereas the second does not: $1 = 2x^2 + 2xy + 3y^2$ leads to $2 = (2x+y)^2 + 5y^2$, which is impossible in integers.

Even more Linear Algebra

There is a second and perhaps less intuitive way of associating a matrix to a quadratic form (which, however, will turn out to be completely natural within the context of quadratic number fields): for each quadratic form $Q = (A,B,C)$ we set

$$\beta = \begin{cases} \frac{B}{2} & \text{if } \Delta = 4m, \\ \frac{1+B}{2} & \text{if } \Delta = 4m+1, \end{cases}$$

and define β' by $\beta + \beta' = \sigma$, where $\sigma \in \{0,1\}$ is determined by $\Delta = 4m + \sigma$. Then we set

$$\mu(Q) = \begin{pmatrix} \beta' & -C \\ A & \beta \end{pmatrix}. \tag{1.4}$$

It is easily checked that $\operatorname{Tr}\mu(Q) = \sigma$ and $\det\mu(Q) = -m$, so $\mu(Q)$ satisfies (by Cayley-Hamilton) the equation $\mu(Q)^2 = \sigma\mu(Q) + mI$, where $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is the 2×2-identity matrix. Thus $\mu(Q)$ is a root of the quadratic polynomial $X^2 - \sigma X - m = Q_0(X,-1)$, where Q_0 is the principal form with discriminant $\Delta = 4m + \sigma$.

The connection between the matrices $m(Q)$ and $\mu(Q)$ attached to a binary quadratic form Q with discriminant Δ can be expressed by the simple formulas

$$m(Q) = J\big(\mu(Q) - \tfrac{\sigma}{2}I\big), \quad \text{and} \quad \mu(Q) = J'm(Q) + \tfrac{\sigma}{2}I, \tag{1.5}$$

where $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $J' = J^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. The action of $\mathrm{SL}_2(\mathbb{Z})$ on the form Q induces actions on the associated matrices; we already know that $m(Q|_S) = S'm(Q)S$, and this implies

$$J\big(\mu(Q|_S) - \tfrac{\sigma}{2}I\big) = m(Q|_S) = S'm(Q)S = S'J\big(\mu(Q) - \tfrac{\sigma}{2}I\big)S.$$

Applying $S'J = JS^{-1}$, we find

$$\mu(Q|_S) = S^{-1}\mu(Q)S. \tag{1.6}$$

Two integral 2×2-matrices M and M_1 are called *similar* if $M_1 = S^{-1}MS$ for some $S \in \mathrm{SL}_2(\mathbb{Z})$. The set $\{M\}$ of all matrices $S^{-1}MS$ with $S \in \mathrm{SL}_2(\mathbb{Z})$ is called the *similarity class* of M.

The characteristic polynomial of a matrix M is the polynomial $f_M(X) = \det(XI - M)$. A simple calculation shows that the characteristic polynomial of $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is given by the monic quadratic polynomial $f_M(X) = X^2 - (a+d)X + ad - bc = X^2 - \mathrm{Tr}\,(M)X + \det M$. Since the trace and the determinant of a matrix only depend on the similarity class $\{M\}$ of M, the characteristic polynomial of M is an invariant of $\{M\}$.

Let us now consider the similarity classes of matrices $\mu = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with characteristic polynomial $f(X) = Q_0(X,-1)$. Then $a + d = \sigma$ and $ad - bc = -m$. Setting $\Lambda(\mu) = J\big(\mu - \frac{\sigma}{2}I\big)$ we find that the symmetric matrix $\Lambda(\mu)$ corresponds to the quadratic form $Q = (c, d-a, -b)$ with discriminant $(d-a)^2 + 4bc = (d+a)^2 - 4(ad-bc) = 4m + \sigma = \Delta$ (observe that Q is positive definite if and only if $\Delta < 0$ and $c > 0$). Since $\Lambda(S^{-1}\mu S) = S'\Lambda(\mu)S$, similar matrices get mapped to equivalent matrices, which in turn are attached to equivalent forms.

Thus Λ maps similarity classes to equivalence classes and has an inverse, and we have proved the following

Theorem 1.2. *There is a bijection between the set* $\mathrm{Cl}(\Delta)$ *of equivalence classes of primitive quadratic forms with discriminant* Δ *and the set of similarity classes of matrices* $\mu = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *with characteristic polynomial* $f(X) = Q_0(X,-1)$*; if* $\Delta < 0$*, we also have to assume* $c > 0$*.*

Example. The similarity classes of integral 2×2-matrices with characteristic polynomial $f(X) = X^2 - X + 6$ (observe that $\Delta = -23$ and $m = -6$) are given by

$$\begin{pmatrix} 0 & -6 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & -3 \\ 2 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & -3 \\ 2 & 1 \end{pmatrix}.$$

These correspond to the equivalence classes of the forms $(1,1,6)$, $(2,-1,3)$ and $(2,1,3)$.

Summary

Using the notion of equivalence, we can state the results proved above as follows:

- Equivalent forms represent the same integers (primitively).
- Equivalent forms have the same discriminant.
- If Q is primitive and equivalent to Q', then Q' is primitive.
- The leading coefficients of equivalent forms with negative discriminant have the same sign.

1.2. Lagrange Reduction

Where we will study the action of $\mathrm{SL}_2(\mathbb{Z})$ *on quadratic forms with discriminant* Δ*, and show that the number of equivalence classes is finite.*

The main question behind the idea of reduction is simple: is there a more or less “canonical” representative of each equivalence class? Lagrange found that the answer is yes for positive definite quadratic forms, and he did so by finding a form Q' equivalent to a given form Q with the property that its coefficients are as small as possible. It turns out that the minimal possible value of A for all forms (A,B,C) in a given equivalence class is connected with the smallest integer represented by the forms in this class:

Lemma 1.3. *If the integer* n *is represented primitively by a form* Q*, then* $Q \sim Q' = (A', B', C')$ *for a form* Q' *with first coefficient* $A' = n$*.*

Proof. We need to find a matrix $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $n = A' = Ar^2 + Brt + Ct^2$. We know that Q primitively represents n, i.e., that there exist coprime integers r, t with $n = Ar^2 + Brt + Ct^2$. By Bezout, there exist integers s, u with $ru - st = 1$. But now $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ has the desired properties. $\square$

Among the forms in a given equivalence class, pick a form $Q = (A, B, C)$ with minimal $|A|$. Applying the matrix $S = \left(\begin{smallmatrix} 1 & s \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ we get $Q|_S = (A, B + 2sA, C')$ for $C' = Q(s, 1)$; this allows us to change $B \bmod 2A$, and by picking a suitable integer s we find a form $Q' = (A, B', C') = Q|_S$ with $|B'| \le |A|$. By the choice of A we also have $|A| \le |Q'(0, 1)| = |C'|$. We have proved

Proposition 1.4. *Every equivalence class of binary quadratic forms contains a form (A, B, C) with $|B| \le |A| \le |C|$.*

A form $Q = (A, B, C)$ is called *Lagrange-reduced* if $|B| \le |A| \le |C|$. We have just shown that every form is equivalent to a Lagrange-reduced form.

The proof given above is an existence proof, which can easily be transformed into a constructive proof. Given a quadratic form $Q = (A, B, C)$ with discriminant $\Delta = B^2 - 4AC$, we use a suitable matrix $S = \left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right)$ to reduce B modulo $2A$, then flip the resulting form using $T = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and reduce the middle coefficient of this new form using another matrix of the form $S = \left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right)$. Since reduction is always followed by a flip (except near the end of the reduction process), we may as well apply $R_n = ST = \left(\begin{smallmatrix} n & 1 \\ -1 & 0 \end{smallmatrix}\right)$ repeatedly.

For reducing the quadratic form $Q = (A, B, C)$, we put $Q' = (A', B', C') = Q|_R$ and find $Q' = (An^2 - Bn + C, 2An - B, A)$. We choose n in such a way that $|B'|$ becomes as small as possible, i.e., with $|2An - B| \le |A|$. With this choice of s, we will always have $|B'| \le |C'|$. Now we claim that $|B'| < |B|$ except when $|B| \le |A|$: In fact, if $|B| > |A|$ then Euclidean division provides us with an integer n such that $|B'| = |B - 2An| < |B|$. Since the natural number $|B|$ cannot decrease indefinitely, after finitely many steps we must reach a form $Q = (A, B, C)$ with $|B| \le |C|$ and $|B| \le |A|$. Then Q is Lagrange-reduced except when $|C| < |A|$, in which case $Q|_T = (C, -B, A)$ is Lagrange-reduced.

Our next result shows that there are only finitely many equivalence classes of forms with discriminant Δ:

Proposition 1.5. *The coefficients of a Lagrange-reduced form $Q = (A, B, C)$ satisfy the inequalities*[4]

$$
\begin{array}{llll}
|B| \le \sqrt{\dfrac{-\Delta}{3}}, & |A| \le \sqrt{\dfrac{-\Delta}{3}}, & |C| \le \dfrac{1 - \Delta}{4} & \textit{if } \Delta < 0, \textit{ and} \\[2ex]
|B| \le \sqrt{\dfrac{\Delta}{5}}, & |A| \le \dfrac{\sqrt{\Delta}}{2}, & |C| \le \dfrac{\Delta}{4} & \textit{if } \Delta > 0.
\end{array}
$$

Proof. If $\Delta < 0$, we have $B^2 - 4AC = \Delta < 0$, hence $AC > 0$. Now $-\Delta = 4AC - B^2 \ge 4A^2 - A^2 = 3A^2$ gives $|A| \le \sqrt{-\Delta/3}$; the inequality $|B| \le |A|$ follows from the fact that (A, B, C) is Lagrange-reduced. Finally we find

$$|C| = \frac{B^2}{4|A|} - \frac{\Delta}{4|A|} \le \frac{A^2}{4|A|} - \frac{\Delta}{4|A|} = \frac{|A|}{4} - \frac{\Delta}{4|A|}.$$

As a function of $|A|$ (assuming Δ to be constant), the expression on the right hand side is decreasing in the interval $[1, \sqrt{-\Delta}\,]$, hence attains its maximum at the boundary $|A| = 1$. This implies the claim.

Now assume that $\Delta > 0$. Then $|AC| \ge B^2 > 4AC$ implies $AC < 0$. Thus $\Delta = B^2 - 4AC = B^2 + 4|AC| \ge 5B^2$, which gives $|B| \le \sqrt{\Delta/5}$. The inequalities $B^2 \ge 0$ and $|C| \ge |A|$ then show $\Delta = B^2 + 4|AC| \ge 4A^2$, hence $|A| \le \frac{1}{2}\sqrt{\Delta}$. Finally we find $4|C| \le 4|AC| = \Delta - B^2 \le \Delta$, which gives the last inequality. $\square$

[4] For storing quadratic forms $Q = (A, B, C)$ with fixed discriminant $\Delta = B^2 - 4AC$ it is sufficient to keep track of A and B, since C can easily be computed via $C = \frac{B^2 - \Delta}{4A}$ whenever it is needed. Note that, for reduced forms (A, B, C), the coefficient C can have up to twice as many digits as A and B.

These bounds can be improved somewhat in the indefinite case:

Proposition 1.6. *Every indefinite primitive form is equivalent to a form $Q = (A, B, C)$ with $0 \le B \le |A| \le |C|$, and $AC < 0$, where either $Q \sim (1, 1, -1)$ or $|A| \le \sqrt{\Delta/8}$.*

Proof. We already have shown the first part of the claim. Assume now that A is an integer represented by Q with minimal $|A|$. Assume moreover that $A > 0$ (the case $A < 0$ is similar). Then $C < 0$, and since $Q(1, 1) = A + B + C$ and $Q(1, -1) = A - B + C$, the minimality of $|A|$ shows that $A + B + C \ge A$ or $A + B + C \le -A$.

In the first case, $B + C \ge 0$ and $B \le -C$ imply $B = -C$, and $B \le A \le -C$ shows that $A = B$. Since the form is primitive, we must have $Q \sim (1, 1, -1)$.

In the second case, $2A + B \le -C$, hence $\Delta = B^2 + 4A(-C) \ge B^2 + 4A(2A + B) \ge 8A^2$ as claimed. □

Using the bounds in Prop. 1.5lemmacount.1.5 it is easy to list all Lagrange-reduced quadratic forms with small discriminant. For finding all reduced forms with discriminant $\Delta = -4 \cdot 65$, we first observe that $|B| \le \sqrt{-\Delta/3} < 10$ and $B \equiv \Delta \equiv 0 \bmod 2$. Now for each B with $-8 \le B \le 8$ we compute $AC = \frac{B^2 - \Delta}{4}$ and determine all possible factorizations with $|B| \le A \le C$. This way we find

- $B = 0$, $AC = 65$, so $Q = (1, 0, 65), (5, 0, 13)$;
- $B = \pm 2$, $AC = 66$, so $Q = (2, \pm 2, 33)$, $(3, \pm 2, 22)$, $(6, \pm 2, 11)$;
- $B = \pm 4$, $AC = 69$: here we find no forms, since e.g. $(3, 4, 23)$ is not reduced;
- $B = \pm 6$, $AC = 74$: no reduced forms here;
- $B = \pm 8$, $AC = 81$, hence $Q = (9, \pm 8, 9)$.

Thus the Lagrange-reduced primitive forms with discriminant $\Delta = -4 \cdot 65$ are $(1, 0, 65)$, $(5, 0, 13)$, $(2, \pm 2, 33)$, $(3, \pm 2, 22)$, $(6, \pm 2, 11)$, and $(9, \pm 8, 9)$.

Table 1.1Lagrange-reduced Forms with Small Discriminanttable.1.1 contains the results (for negative discriminants we only have considered positive definite forms) for discriminants $-16 \le \Delta \le 21$.

Δ	Lagrange-reduced forms	Δ	Lagrange-reduced forms
-3	$(1, \pm 1, 1)$	5	$(1, \pm 1, -1), (-1, \pm 1, 1)$
-4	$(1, 0, 1)$	8	$(1, 0, -2), (-1, 0, 2)$
-7	$(1, \pm 1, 2)$	12	$(1, 0, -3), (-1, 0, 3)$
-8	$(1, 0, 2)$	13	$(1, \pm 1, -3), (-1, \pm 1, 3)$
-11	$(1, \pm 1, 3)$	17	$(1, \pm 1, -4), (-1, \pm 1, 4)$,
-12	$(1, 0, 3), (2, \pm 2, 2)$		$(\pm 2, 1, \mp 2), (\pm 2, -1, \mp 2)$
-15	$(1, \pm 1, 4), (2, \pm 1, 2)$	20	$(1, 0, -5), (-1, 0, 5), (2, \pm 2, -2)$
-16	$(1, 0, 4), (2, 0, 2)$	21	$(1, \pm 1, -5), (-1, \pm 1, 5)$

Table 1.1. Lagrange-reduced Forms with Small Discriminant

Remark 1. The bound for $|A|$ in Prop. 1.5lemmacount.1.5 is best possible for $\Delta < 0$ since we find $|A| \le 1$ for the "minimal" discriminant $\Delta = -3$. The corresponding bound for $\Delta > 0$ would be $|A| \le \sqrt{\Delta/5}$, which would give $|A| \le 1$ for the minimal positive discriminant $\Delta = 5$. This inequality fails for the form $(2, 1, -2)$ with discriminant $\Delta = 17$, however. On the other hand it is possible to prove that each equivalence class contains a Lagrange reduced form (A, B, C) with $|A| \le \sqrt{\Delta/5}$.

Remark 2. It is easy to verify that some of the reduced forms in Table 1.1Lagrange-reduced Forms with Small Discriminanttable.1.1 are equivalent; for example, shifting by

$s = 1$ shows that $(1, -1, c) \sim (1, 1, c)$. We will deal with the problem of finding all equivalence classes of forms of a given negative discriminant in Section 1.4.Reduction of Positive Definite Formssection.1.4, and discuss the related problem for positive discriminants in Section 1.5.Indefinite Forms: Zagier Reductionsection.1.5 below; in the next section we would like to show that the concept of reduction already allows us to prove several classical results on quadratic forms in a very simple way.

1.3. Representations by Quadratic Forms

Where we deduce a few classical results on the representation of primes by certain quadratic forms.

Let us now investigate the primes represented by a given quadratic form. Since discriminants satisfy $\Delta = B^2 - 4AC \equiv B^2 \equiv 0, 1 \bmod 4$, every discriminant has the form $\Delta = -4m$ or $\Delta = 1 - 4m$ for some integer $m \in \mathbb{Z}$. The form

$$Q_0 = \begin{cases} (1, 0, m) & \text{if } \Delta = -4m, \\ (1, 1, m) & \text{if } \Delta = 1 - 4m \end{cases} \tag{1.7}$$

has discriminant Δ and is Lagrange reduced; it is called the *principal form* with discriminant Δ.

Lemma 1.7. *For a discriminant Δ, the following statements are equivalent:*

1. *$p \mid Q_0(a, b)$ for a pair of coprime integers a, b.*
2. *$(\frac{\Delta}{p}) \neq -1$.*
3. *There is a quadratic form $Q = (p, B, C)$ with discriminant Δ.*
4. *There is a quadratic form Q with discriminant Δ that primitively represents p.*

Proof. Observe that 3. $\Longrightarrow$ 4. is trivial since $Q(1, 0) = p$ for the form $Q = (p, B, C)$. For the other claims, we first give the proof for odd primes, and then for $p = 2$.

1. p is odd.
   - 1. $\Longrightarrow$ 2. Assume that $p \mid Q_0(a, b)$ for a pair of coprime integers a, b. If $m \equiv 1 \bmod 4$, $4Q_0(a, b) = (2a + b)^2 - mb^2$. Thus $a^2 \equiv mb^2 \bmod p$ or $(2a + b)^2 \equiv mb^2 \bmod p$ according as $\Delta = 4m$ or $\Delta = 4m + 1$. We must have $p \nmid b$ since otherwise $p \mid a$ and $p \mid \gcd(a, b)$; this implies $(\frac{m}{p}) = (\frac{\Delta}{p}) = 1$ if $p \nmid m$, and $(\frac{\Delta}{p}) = 0$ otherwise.
   - 2. $\Longrightarrow$ 3. Let us first consider the case $p \mid \Delta$ and write $\Delta = pb$; then $\Delta \equiv 1 \bmod 4$ implies $p \equiv b \bmod 4$, hence $p - b = 4C$. Now $Q = (p, p, C)$ is a form with discriminant $p^2 - 4pC = p(p - 4C) = pb = \Delta$.
     Now assume that $(\frac{\Delta}{p}) = +1$. Since Δ is a square mod p and mod 4, there is an integer B such that $\Delta \equiv B^2 \bmod 4p$. With $C = \frac{B^2 - \delta}{4p}$, the form $Q = (p, B, C)$ has discriminant $B^2 - 4pC = \Delta$.
   - 4. $\Longrightarrow$ 1. Assume that Q represents p, that is, $p = Ax^2 + Bxy + Cy^2$ for (necessarily coprime) integers x, y. If $p \mid A$, then $\Delta \equiv B^2 \bmod p$, and the claim follows. If $p \nmid A$, then $4Ap = 4A^2x^2 + 4ABxy + 4ACy^2 = (2Ax + By)^2 - \Delta y^2$. Reduction modulo p gives $\Delta y^2 \equiv (2Ax + By)^2 \bmod p$. Next $p \nmid y$: otherwise we would also have $p \mid 2Ax$; since $\gcd(x, y) = 1$, this implies $p \mid 2A$, which we have excluded here. Thus $\Delta \equiv ((2Ax + By)/y)^2 \bmod p$.
2. $p = 2$.

- 1. $\Longrightarrow$ 2. The claim $(\frac{\Delta}{2}) \neq -1$ is trivial if $\Delta = 4m$. If $\Delta = 4m+1$ and $Q_0(a,b) = a^2 + ab - mb^2$ is even for coprime integers a, b, then b must be odd, and we find $4Q_0(a,b) = (2a+b)^2 - \Delta b^2 \equiv 0 \bmod 8$. Since b is odd, we have $b^2 \equiv 1 \bmod 8$, and this implies $\Delta \equiv (2a+b)^2 \equiv 1 \bmod 8$, that is, $(\frac{\Delta}{2}) = +1$.
- 2. $\Longrightarrow$ 3. If $2 \mid \Delta$, then $\Delta = 4m$. If m is odd, write $m = 1 - 2C$ and take $(2, 2, C)$. If $m = 2C$ is even, take $(2, 0, C)$.
  If $\Delta \equiv 1 \bmod 8$, then $C = \frac{1-\Delta}{8}$ is an integer. But then $Q = (2, 1, C)$ has discriminant $1 - 8C = \Delta$.
- 4. $\Longrightarrow$ 1. If $p \mid A$, then B must be odd, hence $\Delta \equiv B^2 \equiv 1 \bmod 8$ and thus $(\frac{\Delta}{2}) = +1$. If $p \nmid A$, then $8A = (2Ax+By)^2 - \Delta y^2$. Now $2 \mid y$ would imply $4 \mid 2Ax$, that is, $2 \mid Ax$; but this contradicts our assumptions. Thus $y^2 \equiv 1 \bmod 8$, and we find $\Delta \equiv (2Ax + By)^2 \equiv 1 \bmod 8$ as desired.

The proof is now complete. □

It is not necessarily true that the form representing p (in Lemma 1.7lemmacount.1.7.3 and 1.7lemmacount.1.7.4) is primitive; for example, 2 is represented by the non-primitive form $2x^2 + 2y^2$ with discriminant $\Delta = -16$, but it is not represented by the unique primitive reduced form with $\Delta = -16$, namely $Q = (1, 0, 4)$.

This cannot happen for squarefree discriminants: in fact, if $Q = (p, B, C)$ is not primitive, then $B = pB'$ and $C = pC'$; this implies $\Delta = B^2 - 4pC = p^2\Delta'$ for the discriminant $\Delta' = (B')^2 - 4C'$.

The discriminants Δ with the property that every form with discriminant Δ is primitive are called *fundamental*. It is easy to see that a discriminant is fundamental if and only if it cannot be written in the form $\Delta = n^2\Delta'$ for some integer $n > 1$ and a discriminant Δ'. In fact, if (A, B, C) is not primitive and $\gcd(A, B, C) = n > 1$, then writing $A = na$, $B = nb$, $C = nc$ shows that $\Delta = B^2 - 4AC = n^2(b^2 - 4ac) = n^2\Delta'$, where Δ' is the discriminant of (a, b, c).

Lemma 1.8. *A discriminant Δ is fundamental if and only if*

$$\Delta = \begin{cases} 4m & \text{for } m \equiv 2, 3 \bmod 4, \\ m & \text{for } m \equiv 1 \bmod 4 \end{cases}$$

with m squarefree.

Proof. Clearly $\Delta = 4m$ is fundamental in the first case since $\Delta' = m$ is not a discriminant (discriminants are $\equiv 0, 1 \bmod 4$); in the second case this is completely obvious.

Assume therefore that Δ is fundamental. If p is a prime with $p^2 \mid \Delta$, then $p = 2$ since otherwise $\Delta = p^2\Delta'$ for some discriminant Δ'. If $\Delta = 4m$, then $4 \nmid m$ since otherwise m is a discriminant; moreover $m \not\equiv 1 \bmod 4$ for the same reason. □

We now have the following powerful

Proposition 1.9. *If $(\frac{\Delta}{p}) \neq -1$ for some prime p, then p is represented by some Lagrange-reduced form with discriminant Δ.*

Proof. By Lemma 1.7lemmacount.1.7, there is a form $Q = (p, B, C)$ that represents p. Since Q and $Q|_S$ represent the same numbers, p is also represented by $Q|_S$ for any $S \in \mathrm{SL}_2(\mathbb{Z})$. In particular, p is represented by some reduced form with discriminant Δ. □

As a direct corollary we obtain a classical result:

Corollary 1.10. *If m divides a sum of two coprime squares, then m itself can be written as a sum of two squares.*

Proof. From $m \mid x^2 + y^2$ we find $(\frac{x}{y})^2 \equiv -1 \bmod m$; thus -1 is a square modulo every prime p dividing m. By Prop. 1.9lemmacount.1.9, p is represented by some reduced form with discriminant -4. Since $Q = (1, 0, 1)$ is the only such form, p is a sum of two squares. The product formula $(x^2 + y^2)(z^2 + w^2) = (xz - yw)^2 + (xw + yz)^2$ now shows that m is a sum of two squares. $\square$

Here are some more examples that show the power of this result.

- $\Delta = -4$: there is only one reduced form $Q = (1, 0, 1)$, and we conclude that primes $p \equiv 1 \bmod 4$ have the form $p = x^2 + y^2$.
- $\Delta = -3$: the only reduced form is $Q = (1, 1, 1)$, hence every prime $p \equiv 1 \bmod 3$ has the form $p = x^2 + xy + y^2$.
- $\Delta = -20$: there are two reduced forms, namely $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. Every prime $p \equiv 1, 3, 7, 9 \bmod 20$ (these are exactly the odd primes $p \nmid 20$ with $(\frac{-5}{p}) = +1$) is represented by one of these forms. We can even say exactly which primes are represented by each of these forms: if $p = x^2 + 5y^2$, then $p \equiv x^2 + y^2 \equiv 1 \bmod 4$, and if $p = 2x^2 + 2xy + 3y^2$, then y is odd, hence $p = 2x(x + y) + 3y^2 \equiv 3 \bmod 4$ because $x(x + y)$ is even and $y^2 \equiv 1 \bmod 4$. Thus the primes $p \equiv 1, 9 \bmod 20$ are represented by the principal form $x^2 + 5y^2$, whereas the primes $p \equiv 3, 7 \bmod 20$ are represented by $2x^2 + 2xy + 3y^2$.
- $\Delta = 5$: There is only one equivalence class (all four reduced forms are obviously equivalent), hence every prime $p \equiv \pm 1 \bmod 5$ is represented by the form $x^2 + xy - y^2$.
- $\Delta = 8$: since $(1, 0, -2) \sim (-1, 0, 2)$ by Exercise 1Reduction of Binary Quadratic Formschapter.1.8ExercisesItem.88, every prime $p \equiv \pm 1 \bmod 8$ is represented by the form $x^2 - 2y^2$.
- $\Delta = 12$: by Exercise 1Reduction of Binary Quadratic Formschapter.1.8ExercisesItem.88, the classes of the forms $(1, 0, -3)$ and $(-1, 0, 3)$ are distinct. This implies that $p = x^2 - 3y^2$ for primes $p \equiv 1 \bmod 12$, and $p = -x^2 + 3y^2$ (or $-p = x^2 - 3y^2$) for $p \equiv -1 \bmod 12$.
- $\Delta = 20$: from Exercise 1Reduction of Binary Quadratic Formschapter.1.8ExercisesItem.88 we find that $(-1, 0, 5) = (1, 0, -5)|_S$ for $S = \left(\begin{smallmatrix} 2 & -5 \\ 1 & -2 \end{smallmatrix}\right)$. Thus every prime $p \equiv \pm 1 \bmod 5$ is represented by the form $x^2 - 5y^2$.

Let us briefly recall how we proved these results: if p is a prime with $(\frac{\Delta}{p}) \neq -1$, then p is represented by some quadratic form with discriminant Δ. Since equivalent forms represent the same integers and have the same discriminant, p is also represented by some reduced form with discriminant Δ.

1.4. Reduction of Positive Definite Forms

Where we show that each class of equivalent positive definite primitive forms contains a unique reduced form, and explain how to compute class numbers.

The reduction theory of binary quadratic forms with negative discriminant differs considerably from that of positive discriminant. In this section we will deal with the simpler case of positive definite forms.

Thus we will assume that $Q = (A, B, C)$ has $A > 0$ and $\Delta = B^2 - 4AC < 0$. Such forms are positive definite since $4AQ(x, y) = (2Ax + By)^2 - \Delta y^2$. Moreover, we will only consider primitive forms, that is, forms with $\gcd(A, B, C) = 1$.

We have already seen that every equivalence class of primitive quadratic forms contains a Lagrange-reduced form, and that some classes contain more than one. It turns out that for positive definite forms it is possible to define the notion of reduced forms in such a way that every class contains exactly one reduced form.

Definition. A positive definite primitive form $Q = (A, B, C)$ is called *reduced* if A, B, C satisfy the following conditions: Q is Lagrange-reduced ($|B| \le A \le C$; note that $A > 0$ since Q is positive definite), and $B > 0$ if one of the inequalitites is not strict.

The main result is then

Theorem 1.11. *Every class of primitive positive definite quadratic forms contains a unique reduced form.*

Theorem 1.11lemmacount.1.11 states that the class number coincides with the number of reduced primitive forms. The number of reduced forms with discriminant Δ (including the non-primitive forms) is called the Kronecker class number and will be denoted by $H(\Delta)$.

Δ	$H(\Delta)$	Reduced forms
-3	1	$(1,1,1)$
-4	1	$(1,0,1)$
-7	1	$(1,1,2)$
-8	1	$(1,0,2)$
-11	1	$(1,1,3)$
-12	2	$(1,0,3), (2,2,2)$
-15	2	$(1,1,4), (2,1,2)$
-16	2	$(1,0,4), (2,0,2)$

Table 1.2. Reduced Forms of Small Discriminant

Clearly $H(\Delta) = h(\Delta)$ if Δ is a fundamental discriminant. Moreover, we have $h(\Delta) = 1$ if and only if Q_0 is the only reduced primitive form with discriminant Δ.

If we delete all non-reduced forms (those of type $(a, -a, c)$ or $(a, -b, a)$ for $b > 0$) and all non-primitive forms (such as the form $(2, 0, 2)$ with discriminant -16) from Table 1.1Lagrange-reduced Forms with Small Discriminanttable.1.1, we get lists of all reduced forms of small discriminant; Tables 1.3Reduced primitive forms with discriminant $0 \ge \Delta \ge -100$table.1.3 and 1.4Reduced primitive forms with discriminant $-100 > \Delta \ge -200$table.1.4 give such lists of primitive reduced forms for negative discriminants ≥ -200.

For proving the uniqueness part of Theorem 1.11lemmacount.1.11 we use

Lemma 1.12 (Legendre's Lemma). *If $Q = (A, B, C)$ is reduced and if $B > 0$, then the three smallest integers primitively represented by Q are A, C, and $A - B + C$. More precisely, we have $A = Q(\pm 1, 0)$, $C = Q(0, \pm 1)$, $A - B + C = Q(\pm 1, \mp 1)$, as well as*

$$\begin{aligned}
Q(x, y) &\ge A && \textit{for } (x, y) \ne (0, 0), (\pm 1, 0);\\
Q(x, y) &\ge C && \textit{for } (x, y) \ne (0, 0), (\pm 1, 0), (0, \pm 1);\\
Q(x, y) &\ge A - B + C && \textit{for } (x, y) \ne (0, 0), (\pm 1, 0), (0, \pm 1), (\pm 1, \mp 1).
\end{aligned}$$

The assumption $B > 0$ was only made to simplify the statements; if B is negative, the three smallest integers represented primitively by Q are A, C, and $A + B + C$: this follows at once from the fact that $Q = (A, B, C)$ and $Q' = (A, -B, C)$ represent exactly the same numbers since $Q(x, y) = Q'(x, -y)$.

Proof. In order to show that these are the smallest integers represented primitively by Q we have to show that $Q(x, y) \ge A - |B| + C$ for integers x, y with $xy > 1$. We now distinguish three cases:

Δ	$h(\Delta)$	reduced forms
-3	1	$(1,1,1)$
-4	1	$(1,0,1)$
-7	1	$(1,1,2)$
-8	1	$(1,0,2)$
-11	1	$(1,1,3)$
-12	1	$(1,0,3)$
-15	2	$(1,1,4),(2,1,2)$
-16	1	$(1,0,4)$
-19	1	$(1,1,5)$
-20	2	$(1,0,5),(2,2,3)$
-23	3	$(1,1,6),(2,\pm1,3)$
-24	2	$(1,0,6),(2,0,3)$
-27	1	$(1,1,7)$
-28	1	$(1,0,7)$
-31	3	$(1,1,8),(2,\pm1,4)$
-32	2	$(1,0,8),(3,2,3)$
-35	2	$(1,1,9),(3,1,3)$
-36	2	$(1,0,9),(2,2,5)$
-39	4	$(1,1,10),(2,\pm1,5),(3,3,4)$
-40	2	$(1,0,10),(2,0,5)$
-43	1	$(1,1,11)$
-44	3	$(1,0,11),(3,\pm2,4)$
-47	5	$(1,1,12),(2,\pm1,6),(3,\pm1,4)$
-48	2	$(1,0,12),(3,0,4)$
-51	2	$(1,1,13),(3,3,5)$
-52	2	$(1,0,13),(2,2,7)$
-55	4	$(1,1,14),(2,\pm1,7),(4,3,4)$
-56	4	$(1,0,14),(2,0,7),(3,\pm2,5)$
-59	3	$(1,1,15),(3,\pm1,5)$
-60	2	$(1,0,15),(3,0,5)$
-63	4	$(1,1,16),(2,\pm1,8),(4,1,4)$
-64	2	$(1,0,16),(4,4,5)$
-67	1	$(1,1,17)$
-68	4	$(1,0,17),(2,2,9),(3,\pm2,6)$
-71	7	$(1,1,18),(2,\pm1,9),(3,\pm1,6),(4,\pm3,5)$
-72	2	$(1,0,18),(2,0,9)$
-75	2	$(1,1,19),(3,3,7)$
-76	3	$(1,0,19),(4,\pm2,5)$
-79	5	$(1,1,20),(2,\pm1,10),(4,\pm1,5)$
-80	4	$(1,0,20),(3,\pm2,7),(4,0,5)$
-83	3	$(1,1,21),(3,\pm1,7)$
-84	4	$(1,0,21),(2,2,11),(3,0,7),(5,4,5)$
-87	6	$(1,1,22),(2,\pm1,11),(3,3,8),(4,\pm3,6),$
-88	2	$(1,0,22),(2,0,11)$
-91	2	$(1,1,23),(5,3,5)$
-92	3	$(1,0,23),(3,\pm2,8)$
-95	8	$(1,1,24),(2,\pm1,12),(3,\pm1,8),(4,\pm1,6),(5,5,6)$
-96	4	$(1,0,24),(3,0,8),(4,4,7),(5,2,5)$
-99	2	$(1,1,25),(5,1,5)$
-100	2	$(1,0,25),(2,2,13)$

Table 1.3. Reduced primitive forms with discriminant $0 \geq \Delta \geq -100$.

Δ	$h(\Delta)$	reduced forms
-103	5	$(1,1,26),(2,\pm1,13),(4,\pm3,7)$
-104	6	$(1,0,26),(2,0,13),(3,\pm2,9),(5,\pm4,6)$
-107	3	$(1,1,27),(3,\pm1,9)$
-108	3	$(1,0,27),(4,\pm2,7)$
-111	8	$(1,1,28),(2,\pm1,14),(3,3,10),(4,\pm1,7),(5,\pm3,6)$
-112	2	$(1,0,28),(4,0,7)$
-115	2	$(1,1,29),(5,5,7)$
-116	6	$(1,0,29),(2,2,15),(3,\pm2,10),(5,\pm2,6)$
-119	10	$(1,1,30),(2,\pm1,15),(3,\pm1,10),(4,\pm3,8),(5,\pm1,6),(6,5,6)$
-120	4	$(1,0,30),(2,0,15),(3,0,10),(5,0,6)$
-123	2	$(1,1,31),(3,3,11)$
-124	3	$(1,0,31),(5,\pm4,7)$
-127	5	$(1,1,32),(2,\pm1,16),(4,\pm1,8)$
-128	4	$(1,0,32),(3,\pm2,11),(4,4,9)$
-131	5	$(1,1,33),(3,\pm1,11),(5,\pm3,7)$
-132	4	$(1,0,33),(2,2,17),(3,0,11),(6,6,7)$
-135	6	$(1,1,34),(2,\pm1,17),(4,\pm3,9),(5,5,8)$
-136	4	$(1,0,34),(2,0,17),(5,\pm2,7)$
-139	3	$(1,1,35),(5,\pm1,7)$
-140	6	$(1,0,35),(3,\pm2,12),(4,\pm2,9),(5,0,7)$
-143	10	$(1,1,36),(2,\pm1,18),(3,\pm1,12),(4,\pm1,9),(6,\pm5,7),(6,1,6)$
-144	4	$(1,0,36),(4,0,9),(5,\pm4,8)$
-147	2	$(1,1,37),(3,3,13)$
-148	2	$(1,0,37),(2,2,19)$
-151	7	$(1,1,38),(2,\pm1,19),(4,\pm3,10),(5,\pm3,8)$
-152	6	$(1,0,38),(2,0,19),(3,\pm2,13),(6,\pm4,7)$
-155	4	$(1,1,39),(3,\pm1,13),(5,5,9)$
-156	4	$(1,0,39),(3,0,13),(5,\pm2,8)$
-159	10	$(1,1,40),(2,\pm1,20),(3,3,14),(4,\pm1,10),(5,\pm1,8),(6,\pm3,7)$
-160	4	$(1,0,40),(4,4,11),(5,0,8),(7,6,7)$
-163	1	$(1,1,41)$
-164	8	$(1,0,41),(2,2,21),(3,\pm2,14),(5,\pm4,9),(6,\pm2,7)$
-167	11	$(1,1,42),(2,\pm1,21),(3,\pm1,14),(4,\pm3,11),(6,\pm5,8),(6,\pm1,7)$
-168	4	$(1,0,42),(2,0,21),(3,0,14),(6,0,7)$
-171	4	$(1,1,43),(5,\pm3,9),(7,5,7)$
-172	3	$(1,0,43),(4,\pm2,11)$
-175	6	$(1,1,44),(2,\pm1,22),(4,\pm1,11),(7,7,8)$
-176	6	$(1,0,44),(3,\pm2,15),(4,0,11),(5,\pm2,9)$
-179	5	$(1,1,45),(3,\pm1,15),(5,\pm1,9)$
-180	4	$(1,0,45),(2,2,23),(5,0,9),(7,4,7)$
-183	8	$(1,1,46),(2,\pm1,23),(3,3,16),(4,\pm3,12),(6,\pm3,8)$
-184	4	$(1,0,46),(2,0,23),(5,\pm4,10)$
-187	3	$(1,1,47),(7,\pm3,7)$
-188	5	$(1,0,47),(3,\pm2,16),(7,\pm6,8)$
-191	13	$(1,1,48),(2,\pm1,24),(3,\pm1,16),(4,\pm1,12),$
		$(5,\pm3,10),(6,\pm1,8),(6,\pm5,9)$
-192	4	$(1,0,48),(3,0,16),(4,4,13),(7,2,7)$
-195	4	$(1,1,49),(3,3,17),(5,5,11),(7,1,7)$
-196	4	$(1,0,49),(2,2,25),(5,\pm2,10)$
-199	9	$(1,1,50),(2,\pm1,25),(4,\pm3,13),(5,\pm1,10),(7,\pm5,8)$
-200	6	$(1,0,50),(2,0,25),(3,\pm2,17),(6,\pm4,9)$

Table 1.4. Reduced primitive forms with discriminant $-100 > \Delta \geq -200$.

- $|x| = |y|$. Then $Q(x,y) = x^2(A \pm B + C) \geq (A - |B| + C)x^2 > A - |B| + C$.
- $|x| > |y|$. Then

$$\begin{aligned} Q(x,y) &\geq Ax^2 - |B||xy| + Cy^2 > (A - |B|)|xy| + Cy^2 \\ &\geq (A - |B| + C)y^2 > A - |B| + C. \end{aligned}$$

- $|x| < |y|$. Then $Q(x,y) \geq (A - |B| + C)x^2 > A - |B| + C$.

□

Note that these three integers A, C, and $A - |B| + C$ need not be distinct: if $Q = (1,1,1)$, then actually $A = C = A - |B| + C = 1$.

Legendre's Lemma is not very deep, but can it can be applied in a lot of situations; in particular we will use it for proving that any two equivalent reduced forms are equal, as well as for proving the following observation:

Corollary 1.13. *A (positive definite) quadratic form representing* 1 *is equivalent to the principal form.*

Proof. Let Q be such a quadratic form. Then Q is equivalent to some reduced form Q', which also represents 1. Since 1 is the smallest natural number represented by Q', Lemma 1.12Legendre's Lemmalemmacount.1.12 implies that $Q' = (A,B,C)$ with $A = 1$ (applying Lemma 1.3lemmacount.1.3 would give the same result). Since Q' is reduced, we must have $|B| \leq |A| = 1$, hence $Q' = (1,0,C)$ or $Q' = (1,1,C)$. But these are exactly the principal forms with discriminant $\Delta = -4C$ and $\Delta = 1 - 4C$, respectively. □

We have already seen that every equivalence class $[Q]$ of a quadratic form (positive definite and primitive, with discriminant Δ) contains a reduced form (because Q is equivalent to some reduced form). Now we will prove that every equivalence class contains *exactly one* reduced form. This will have the important consequence that there are exactly as many equivalence classes of forms as there are reduced forms, or in other words, that the number of reduced forms is just the class number $h(\Delta)$.

Proof of Thm. 1.11lemmacount.1.11. We have to show that if $Q = (A,B,C)$ and $Q' = (A',B',C')$ are reduced forms with $Q \sim Q'$, then $Q = Q'$.

First we observe that the smallest natural number represented by Q and Q' is A and A', respectively. Since $Q \sim Q'$, they represent the same integers, hence we must have $A = A'$. Note that $C \geq A$ since Q is reduced; we now distinguish some cases.

1. $C > A$. Since $A = Q(\pm 1, 0)$ is represented exactly twice by Q, it is also represented exactly twice by Q', hence $C' = Q'(0, \pm 1) > A' = A$. Now C is the second smallest integer represented by Q, and therefore also by Q'. Since Q and Q' represent the same integers, we must have $C = C'$. Since $\operatorname{disc} Q = \operatorname{disc} Q'$, we see that $|B| = |B'|$. If we had $B' = -B$, then $(A,B,C) = Q \sim Q' = (A,-B,C)$. Assume that $Q' = Q|_S$ for $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then $A = A' = Ar^2 + Brt + Ct^2$, and since $C > A$, the only solutions of this equation are $r = \pm 1$, $t = 0$. Thus $S = \left(\begin{smallmatrix} 1 & s \\ 0 & 1 \end{smallmatrix}\right)$ or $S = \left(\begin{smallmatrix} -1 & s \\ 0 & -1 \end{smallmatrix}\right)$, hence $-B = B' = 2As + B$, or $As = -B$. Since $|B| \leq A$, we must have $s = 0$ (and then $B = 0 = -B = B'$) or $s = 1$ (and then $B = -A$, which contradicts the assumption that Q is reduced). Thus we have $Q = Q'$ in all cases considered here.
2. $C = A$. Then $A = Q(\pm 1, 0) = Q(0, \pm 1)$ shows that A is represented at least four times by Q, hence also by Q'. But this implies $C' = A$ and therefore $C = C'$. As above this gives $B' = \pm B$. But since $(A,B,A) \sim (A,B',A)$ are reduced, B and B' must be positive, and we get $Q = Q'$.

The proof is now complete. □

Remark. Theorem 1.11lemmacount.1.11 solves the problem of deciding whether two given positive definite forms Q and Q' are equivalent: let Q_1 and Q_1' be the unique reduced forms equivalent to Q and Q', respectively; then $Q \sim Q'$ if and only if $Q_1 = Q_1'$. Thus for checking whether two forms are equivalent it is sufficient to reduce them and check for equality of the reduced forms. Of course a necessary condition for equivalence is that the forms have the same discriminant.

Studying the tables of reduced primitive forms given on pp. 15Reduced primitive forms with discriminant $0 \ge \Delta \ge -100$table.1.3 – 16Reduced primitive forms with discriminant $-100 > \Delta \ge -200$table.1.4 it is quite easy to come up with a few observations; some of them more or less prove themselves:

- The tables reveal a family of reduced forms $Q_m = (2, 1, m)$ for every $m \ge 2$. Since $\operatorname{disc} Q_m = 1 - 8m$, this shows that $h(\Delta) > 1$ for all $\Delta = 1 - 8m < -7$.
- The family of reduced forms $Q_m = (2, 2, m)$ for odd integers $m \ge 3$ shows that $h(\Delta) > 1$ for discriminants $\Delta = 4 - 8m$.

Some observations, such as the following, are not immediately clear:

- The class number $h(\Delta)$ is odd if $\Delta = q$ or $\Delta = -4q$, where $q \equiv 3 \bmod 4$ is a prime number.
- If Δ is a power of an odd prime, then $h(\Delta)$ is odd.
- If $\Delta = f^2\Delta'$ for discriminants Δ and Δ', then $h(\Delta') \mid h(\Delta)$.

The proofs of these results are already nontrivial. Other observations are only valid for small discriminants:

- Within the range of computations, we have $h(\Delta) \le \sqrt{\Delta}$.

This observation turns out to be false for larger values of Δ; for example, $h(-311) = 19$, $h(-479) = 25$, $h(-551) = 26$ etc. Even the weaker conjecture $h(\Delta) < 2\sqrt{\Delta}$ is not true, as e.g. $h(-2954591) = 3464$ shows. This leads us to the following question:

- Is the function $h(\Delta)/\sqrt{-\Delta}$ bounded as $\Delta \longrightarrow -\infty$?

It turns out that the answer is no, but this result is already quite deep. I do not know whether it can be proved that, say, $h(\Delta) > \sqrt{-\Delta} \cdot \log\log\log(-\Delta)$ infinitely often.

Other observations, such as the next two, seem to remain true even after extending the table considerably:

- There are only finitely many discriminants Δ with class number 1, or, more generally, with any given class number.
- For any number $n \in \mathbb{N}$ there exist infinitely many discriminants $\Delta < 0$ with $n \mid h(\Delta)$.

Some of these questions lead to extremely deep and difficult problems.

Remark. It is known that the quotient $\frac{h(\Delta)}{\sqrt{-\Delta}}$ for negative discriminants Δ is not bounded as $\Delta \longrightarrow -\infty$. On the other hand, a special case of the Brauer-Siegel theorem predicts that

$$\lim_{\Delta \to -\infty} \frac{\log h(\Delta)}{\log(-\Delta)} = 1,$$

and in fact it can be shown, using analytic techniques, that $h(\Delta) \le \sqrt{|\Delta|}\log(|\Delta|)$ for negative discriminants Δ. Scholz has conjectured that $h(\Delta) > \sqrt{-\Delta} \cdot \log\log\log|\Delta|$ for infinitely many discriminants.

Reduction Algorithms ... and what to do with them

The standard reduction algorithm proceeds as follows: given a form (A, B, C) with discriminant Δ, find a small $B' \equiv B \bmod 2A$, determine C' such that (A, B', C') has discriminant Δ, and then flip; the form $(C', -B', A)$ is then reduced as above by minimizing $-B' \bmod C'$, and this procedure is repeated until we reach a reduced form.

We can avoid the flipping by alternately reducing modulo $2A$ and modulo $2C$: reduction modulo $2A$ means applying a matrix $T_n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, whereas reduction modulo $2C$ is described by $T'_n = \left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$. Two subsequent reduction steps then correspond to some product $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} mn+1 & n \\ m & 1 \end{smallmatrix}\right)$ in the version avoiding flipping, and $\left(\begin{smallmatrix} -n & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} m & 1 \\ -1 & 0 \end{smallmatrix}\right) = -\left(\begin{smallmatrix} mn+1 & n \\ m & 1 \end{smallmatrix}\right)$ in the other case (the reason for the entry m in the second matrix comes from the fact that the middle coefficients has switched signs).

Here are the two methods for $Q = (15, 66, 73)$:

form	matrix
$(15, 66, 73)$	$\left(\begin{smallmatrix} 1 & -2 \\ 0 & 1 \end{smallmatrix}\right)$
$(15, 6, 1)$	$\left(\begin{smallmatrix} 1 & 0 \\ -3 & 1 \end{smallmatrix}\right)$
$(6, 0, 1)$	

form	matrix
$(15, 66, 73)$	$\left(\begin{smallmatrix} 2 & 1 \\ -1 & 0 \end{smallmatrix}\right)$
$(1, -6, 15)$	$\left(\begin{smallmatrix} -3 & 1 \\ -1 & 0 \end{smallmatrix}\right)$
$(6, 0, 1)$	

Let us now describe how to reduce positive definite forms by hand[5] Assume we have a form $Q = (A, B, C)$, and assume for now that $B = 2b$ is even. Consider the corresponding matrix $M = \left(\begin{smallmatrix} A & b \\ b & C \end{smallmatrix}\right)$, and assume that $C < A$. We then reduce B modulo $2C$, that is, find an integer m such that $|b + mC|$ is minimal. We then set $b' = b + mC$ and compute $A' = A + Bm + Cm^2$. This integer can more easily be found as follows: if we set $A + nb = \alpha$, then we get $\alpha + mb' = A + mb + m(b + mC) = A + mB + m^2C = A'$. Here is what we write down:

$$\begin{array}{ccc} & m & \\ A & b & \alpha \\ b & C & b' \\ \alpha & b' & A' \end{array}$$

From this table we then can read off that $(A, B, C) \sim (A', B', C)$ with $B' = 2b'$. The next step is finding an integer n such that $|b' + nA'|$ is minimal, and repeating the procedure above; computing $\beta = C + nb'$, $b'' = b' + nA'$ and $C' = \beta + nb''$ gives the table

$$\begin{array}{cccc} & m & n & \\ A & b & \alpha & \\ b & C & b' & \beta \\ \alpha & b' & A' & b'' \\ & \beta & b'' & C' \end{array}$$

Here is a simple example. Consider the matrix $M = \left(\begin{smallmatrix} 1009 & 469 \\ 469 & 218 \end{smallmatrix}\right)$ with determinant 1 and the corresponding quadratic form $Q = (1009, 938, 218)$ with discriminant -4. This matrix was computed from a solution $x = b$ of the congruence $x^2 \equiv -1 \bmod 1009$; with $b = 469$ we find $A = p = 1009$ and $C = (b^2 + 1)/p = 218$.

The reduction process yields

[5] Doing calculations by hand may look like a waste of time in times when cheap calculators are available that can produce results in fractions of a second. On the other hand I am certain that there is a lot of insight to be gained by occasionally performing an algorithm by hand (with computer assistance for the boring parts).

$$\begin{array}{rrrrr}
 & -2 & -7 & 2 & \\
1009 & 469 & 71 & & \\
469 & 218 & 33 & -13 & \\
71 & 33 & 5 & -2 & 1 \\
 & -13 & -2 & 1 & 0 \\
 & & 1 & 0 & 1
\end{array}.$$

Here is the traditional version of reduction:

$$\begin{array}{ccc}
(1009, 938, 218) & n = 0 & \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \\
(218, -938, 1009) & n = 2 & \left(\begin{smallmatrix} 2 & 1 \\ -1 & 0 \end{smallmatrix}\right) \\
(5, 66, 218) & n = -7 & \left(\begin{smallmatrix} -7 & 1 \\ -1 & 0 \end{smallmatrix}\right) \\
(1, 4, 5) & n = -2 & \left(\begin{smallmatrix} -2 & 1 \\ -1 & 0 \end{smallmatrix}\right) \\
(1, 0, 1) & &
\end{array}$$

Observe that the integers n in the traditional method agree with those found above up to sign.

These methods can be used to compute the representation of a prime $p \equiv 1 \bmod 4$ as a sum of two squares when a square root of $-1 \bmod p$ is given: since $Q = (A, 2b, C)$ represents $A = p$, so does $(1, 0, 1)$, and we can write p as a sum of two squares by computing the reduction matrices.

In the example above, the product of the reduction matrices is $S = S_0 S_2 S_{-7} S_{-2} = \left(\begin{smallmatrix} -13 & 7 \\ -28 & 15 \end{smallmatrix}\right)$; since $\det S = 1$, we have $S^{-1} = \left(\begin{smallmatrix} 15 & -7 \\ 28 & -13 \end{smallmatrix}\right)$, and from $Q(1, 0) = 1009$ and $\binom{x}{y} = S^{-1}\binom{1}{0}$ we read off $x = 15$ and $y = 28$, that is, $1009 = 15^2 + 28^2$.

1.5. Indefinite Forms: Zagier Reduction

Where we learn how to reduce indefinite forms.

The reduction theory of indefinite forms is a lot more complicated (and, in a sense, also more interesting) than that for definite forms. Here are the main differences:

- The conditions for a form to be reduced are more complicated than in the definite case, at least for the most common notions of reduction.
- There are in general many reduced forms in each equivalence class.
- There exist nontrivial elements $S \in \mathrm{SL}_2(\mathbb{Z})$ with $Q = Q|_S$, which are connected with the solvability of the *Pell equation* $Q_0(T, U) = 1$.
- Simple questions like whether $(A, B, C) \sim (-A, B, -C)$ turn out to be highly nontrivial, and are related to the solvability of the "Anti-Pellian" equation $Q_0(T, U) = -1$.
- More generally, the question whether two reduced forms are equivalent or not is very difficult to answer if the discriminant is large.
- The set of reduced forms in the principal class carries an additional structure (Shanks' infrastructure), which is useful for calculations and adds a lot to our understanding of indefinite forms.
- There are two natural definitions of equivalence, giving rise to two different structures, the class groups in the strict and in the wide sense.

In addition, there are different reduction theories. In this chapter we will present the one due to Zagier, which allows us to prove the main results rather painlessly; the classical theory due to Gauss, which is most suitable for calculations since the coefficients involved are much smaller than in Zagier's theory, will be sketched in the Notes below.

It would be nice if we could define the notion of a reduced form for indefinite forms in such a way that every equivalence class contains exactly one reduced form; this is certainly possible: we can pick, in each equivalence class, a form with minimal $A > 0$ (if there are more than one, pick the one with minimal $B > 0$) and then reduce B modulo $2A$. The disadvantage of such a definition is that there is no “reduction theory”, that is, no simple and effective algorithm for reducing a given form.

If we can’t get exactly one reduced form per class, maybe we should try to define reduced forms in such a way that each class contains as few reduced forms as possible. History has followed a different path: the best definitions work with quite large sets of reduced forms; as a trade-off, the set of reduced forms carries some kind of structure, and in mathematics, structure is in general more important than cardinality.

The classical theory of reduction of indefinite forms by Gauss is vastly superior to that given by Lagrange, although there are more forms reduced in the sense of Gauss than there are Lagrange-reduced forms. In his excellent book [Zag1981], Zagier suggested a reduction theory differing from Gauss’s. Zagier’s theory has much cleaner proofs[6] than the classical one; other hand, Gauss’s theory is the one used for doing calculations because the coefficients of Gauss-reduced forms have only about half as many digits as those of Zagier-reduced forms.

For explaining the motivation behind the definition of reduced forms, recall how we came up with the notion of Lagrange reduced forms: we picked a form (A, B, C) in a given equivalence class with minimal $|A|$ and then changed B modulo $2A$ to find a minimal B. We do something similar here: given an equivalence class of forms, we choose a form with minimal first coefficient $A > 0$. Since we are allowed to change B modulo $2|A|$, we can demand that B lie in some interval of length $2A$, and we pick $B \in [\sqrt{\Delta}, \sqrt{\Delta} + 2A]$. With this choice, we have $AC > 0$, and since Q represents C, the minimality of A implies $A \le C$: thus we also have $B \in [\sqrt{\Delta}, \sqrt{\Delta} + 2C]$.

We now call a form (A, B, C) with positive nonsquare discriminant Δ a Zagier reduced (or simply Z-reduced) form if the coefficients A, B, C satisfy the following inequalities:

$$\begin{cases} \sqrt{\Delta} < B < \sqrt{\Delta} + 2A, \\ \sqrt{\Delta} < B < \sqrt{\Delta} + 2C. \end{cases} \tag{1.8}$$

Table 1.5Zagier-reduced Forms with discriminants $0 < \Delta \le 44$table.1.5 displays the primitive Zagier reduced forms with non-square discriminants $0 < \Delta \le 44$.

The number $\kappa_Z(\Delta)$ of Zagier-reduced forms with discriminant Δ is called the *caliber* of the discriminant; the caliber grows rather quickly (experimentally, there seem to be up to $\frac{1}{4}\Delta$ (and even more) reduced forms with fundamental discriminants). The following table gives the values of $\kappa_Z(\Delta)$ for small discriminants.

Δ	κ_Z	Δ	κ_Z	Δ	κ_Z	Δ	κ_Z	Δ	κ_Z
5	1	41	11	77	8	8	2	12	3
13	3	53	7	85	14	24	6	28	7
17	5	57	16	89	21	40	10	44	9
21	4	61	11	93	12	56	10	60	12
29	5	65	16	97	27	88	18	76	17
33	10	69	10	101	11	104	16	92	13
37	7	73	21	105	26	120	20	124	25

The number $h^+(\Delta)$ of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive forms with discriminant Δ is usually a lot smaller than the number of Z-reduced forms. The five Z-reduced forms with discriminant $\Delta = 17$, for example, are all equivalent, hence $h^+(17) = 1$.

[6] These proofs essentially consist in verifying inequalities involving the coefficients of the forms; in Zagier’s theory, these coefficients are all positive.

Δ	κ_Z	Primitive Zagier-reduced forms
5	1	$(1,3,1)$
8	2	$(1,4,2), (2,4,1)$
12	3	$(1,4,1), (2,6,3), (3,6,2)$
13	3	$(1,5,3), (3,5,1), (3,7,3)$
17	5	$(1,5,2), (2,5,1), (2,7,4), (4,7,2), (4,9,4)$
20	4	$(1,6,4), (4,6,1), (4,10,5), (5,10,4)$
21	4	$(1,5,1), (3,9,5), (5,9,3), (5,11,5)$
24	6	$(1,6,3), (2,8,5), (3,6,1), (5,8,2), (5,12,6), (6,12,5)$
28	7	$(1,6,2), (2,6,1), (3,8,3), (3,10,6), (6,10,3), (6,14,7), (7,14,6)$
29	5	$(1,7,5), (5,7,1), (5,13,7), (7,13,5), (7,15,7)$
32	5	$(1,6,1), (4,12,7), (7,12,4), (7,16,8), (8,16,7)$
33	10	$(1,7,4), (2,7,2), (2,9,6), (3,9,4), (4,7,1),$ $(4,9,3), (6,9,2), (6,15,8), (8,15,6), (8,17,8)$
37	7	$(1,7,3), (3,7,1), (3,11,7), (7,11,3), (7,17,9), (9,17,7), (9,19,9)$
40	10	$(1,8,6), (2,8,3), (3,8,2), (3,10,5), (5,10,3)$ $(6,8,1), (6,16,9), (9,16,6), (9,20,10), (10,20,9)$
41	11	$(1,7,2), (2,7,1), (2,9,5), (4,11,5), (4,13,8), (5,9,2),$ $(5,11,4), (8,13,4), (8,19,10), (10,19,8), (10,21,10)$
44	9	$(1,8,5), (2,10,7), (5,8,1), (5,12,5), (7,10,2)$ $(7,18,10), (10,18,7), (10,22,11), (11,22,10)$

Table 1.5. Zagier-reduced Forms with discriminants $0 < \Delta \le 44$.

We will now present various sets of conditions on the coefficients of a quadratic form (A,B,C) which are equivalent to (1.8Indefinite Forms: Zagier Reductionequation.1.5.8):

Theorem 1.14. *Let $Q = (A,B,C)$ be a primitive indefinite form with discriminant $\Delta = B^2 - 4AC$, and let $\xi_1 = \frac{B+\sqrt{\Delta}}{2A}$ and $\xi_2 = \xi_1'$ denote the two roots of the quadratic equation $Q(x,-1) = Ax^2 - Bx + C = 0$. Then the following statements are equivalent:*

$$(A,B,C) \text{ is Z-reduced.} \tag{1.9}$$
$$(C,B,A) \text{ is Z-reduced.} \tag{1.10}$$
$$0 < B - \sqrt{\Delta} < 2A < B + \sqrt{\Delta}. \tag{1.11}$$
$$0 < B - \sqrt{\Delta} < 2C < B + \sqrt{\Delta}. \tag{1.12}$$
$$0 < \xi_2 < 1 < \xi_1. \tag{1.13}$$
$$A > 0,\ C > 0,\ B > A + C. \tag{1.14}$$

Proof. The symmetry between A and C in (1.8Indefinite Forms: Zagier Reductionequation.1.5.8) implies that (1.9equation.1.5.9) and (1.10equation.1.5.10) are equivalent.

(1.9equation.1.5.9) $\Longrightarrow$ (1.11equation.1.5.11): It follows immediately from (1.8Indefinite Forms: Zagier Reductionequation.1.5.8) that $A > 0$ and $C > 0$; this implies $B^2 = \Delta + 4AC > \Delta$, hence $B > \sqrt{\Delta}$, or $0 < B - \sqrt{\Delta}$. Next, $B < \sqrt{\Delta} + 2A$ is equivalent to $B - \sqrt{\Delta} < 2A$, and we find $2A = \frac{B^2-\Delta}{2C} < \frac{B^2-\Delta}{B-\sqrt{\Delta}} = B + \sqrt{\Delta}$.

(1.9equation.1.5.9) $\Longrightarrow$ (1.12equation.1.5.12) follows by replacing (A,B,C) by (C,B,A) in the proof above; moreover, (1.11equation.1.5.11) and (1.12equation.1.5.12) imply (1.9equation.1.5.9). This shows that properties (1.9equation.1.5.9)– (1.12equation.1.5.12) are equivalent.

Dividing the inequalities in (1.11equation.1.5.11) through by $2A > 0$ we see that (1.11equation.1.5.11) and (1.13equation.1.5.13) are equivalent.

We finally show that (1.13equation.1.5.13) and (1.14equation.1.5.14) are equivalent. Let us first show (1.13equation.1.5.13) $\Longrightarrow$ (1.14equation.1.5.14). From $\xi_1 - \xi_2 > 0$ we deduce that $A > 0$. Then $\xi_1 = \frac{B+\sqrt{\Delta}}{2A} > 1$ and $\xi_2 = \frac{B-\sqrt{\Delta}}{2A} < 1$ imply $|B - 2A| < \sqrt{\Delta}$, hence the identity

$$\Delta - (B-2A)^2 = 4A(B - A - C) \tag{1.15}$$

shows that $B > A + C$. Finally, $C = \xi_1 \xi_2 > 0$.

Now assume that (1.14equation.1.5.14) holds. Then (1.15Indefinite Forms: Zagier Reductionequation.1.5.15) implies that $|B - 2A| < \sqrt{\Delta}$, which is equivalent to $\xi_1 > 1$ and $\xi_2 < 1$. Since $0 < C = \xi_1 \xi_2$, we must have $\xi_2 > 0$, which proves (1.13equation.1.5.13). □

The basic questions we will have to address are the following:

1. Is every form equivalent to a reduced form?
2. Are there only finitely many equivalence classes of forms with given discriminants?
3. Are there only finitely many Z-reduced forms?
4. Is there an algorithm for reducing a given form?
5. Is there an algorithm for deciding when two reduced forms are equivalent?

Some of these questions are easily answered:

1. We have already seen during the considerations that led to our definition (1.8Indefinite Forms: Zagier Reductionequation.1.5.8) that the answer is yes: every form is equivalent to some Z-reduced form.
2. We already know from the reduction theory of Lagrange that there are only finitely many equivalence classes of forms with given discriminant.
3. This question also has a positive answer (and shows again that there are only finitely many equivalence classes of forms), as we will see in the proposition below.
4. Below we shall give an algorithm that produces a Z-reduced form after finitely many steps.
5. For deciding whether two forms are equivalent, all we have to do is reduce both and then check whether the reduced forms are equivalent. Below we will see that this boils down to computing the cycle of, say, the first form and then checking whether the Z-reduced form equivalent to the second form occurs in this cycle. This can be performed in finitely many steps, but if the cycle is very long, this can take forever. The difficulty of deciding whether two forms are equivalent can be used for cryptographic purposes.

Now we show

Proposition 1.15. *There are only finitely many Z-reduced forms with discriminant Δ. In fact, the coefficients of Z-reduced forms (A, B, C) satisfy the inequalities $0 < A, C \le \frac{\Delta}{4}$ and $\sqrt{\Delta} < B \le \frac{\Delta+1}{2}$.*

Proof. It is sufficient to prove the inequalities: we have

$$A = \frac{\Delta - (B - 2A)^2}{4(B - A - C)} \le \frac{\Delta}{4},$$

and the corresponding inequality for C follows by symmetry. Finally, $B^2 = \Delta + 4AC \le \Delta + \frac{1}{4}(\Delta - 1)^2 = \frac{1}{4}(\Delta + 1)^2$ implies the last claim. □

Given some notion of reduced forms on the set $\mathcal{F}_\Delta$ of primitive forms with discriminant Δ, we can consider the subset $\mathcal{R}_\Delta$ of reduced form. In such a situation we call a map $\rho : \mathcal{F}_\Delta \longrightarrow \mathcal{F}_\Delta$ a *reduction map* if it has the following properties:

R1 Given any form $Q \in \mathcal{F}_\Delta$, there is an integer $\nu \ge 0$ such that

$$\rho^\nu(Q) = \underbrace{\rho \circ \rho \circ \ldots \circ \rho}_{\nu \text{ times}}(Q)$$

is reduced. In other words: if ν is large enough, then $\rho^\nu(Q) \in \mathcal{R}_\Delta$.

R2 If Q is reduced, then so is $\rho(Q)$. In other words: ρ maps $\mathcal{R}_\Delta$ into $\mathcal{R}_\Delta$.

In such a case, the form $\rho(Q)$ is called the *right neighbor* of Q, and the forms in the image of ρ are called semi-reduced.

If $\mathcal{R}_\Delta = \mathcal{R}_{\rm Zag}$ is the set of Zagier reduced forms with discriminant Δ, then such a reduction map exists: given a form $Q = (A, B, C)$, the right neighbor $\rho(Q)$ is the form $Q' = (A', B', C')$ with $Q' = Q|_S$, where $S = S_n = \left(\begin{smallmatrix} n & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ is defined by $n > \frac{B+\sqrt{\Delta}}{2A} > n-1$. Note that $S_n = \left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, so S represents a shift followed by a flip.

There is a method for computing $\rho(Q)$ that does not explicitly involve the number n:

Lemma 1.16. *The right neighbor of the form $Q = (A, B, C)$ can be computed as follows:*

1. *$C' = A$;*
2. *$B + B' \equiv 0 \bmod 2A$ and* $\begin{cases} \sqrt{\Delta} < B' < \sqrt{\Delta} + 2A & \textit{if } A > 0, \\ \sqrt{\Delta} + 2A < B' < \sqrt{\Delta} & \textit{if } A < 0. \end{cases}$
3. *${B'}^2 - 4A'C' = \Delta$.*

These conditions determine respectively C', B', and A'.

Proof. Write $B + B' = 2An$ for some integer n, and put $S = \left(\begin{smallmatrix} n & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then $Q|_S = (A', B', C')$ with

$$A' = An^2 - Bn + C, \quad B' = 2An - B, \quad C' = A.$$

Clearly $(A', B', C') = \rho(Q)$ if we can show that $2An > B + \sqrt{\Delta} > 2A(n-1)$ (if $A > 0$) or $2An < B + \sqrt{\Delta} < 2A(n-1)$ (if $A < 0$). In the following, we only deal with the first case and leave the second case to the reader.

The first inequality is equivalent to $2An - B > \sqrt{\Delta}$, which holds by our choice of $\sqrt{\Delta} < B' = 2An - B$. The second inequality is equivalent to $2An - B < \sqrt{\Delta} + 2A$, which again holds because $2An - B = B' < \sqrt{\Delta} + 2A$. □

Example. For $Q = (1, 4, 2)$ we have $\rho(Q) = Q' = (2, 4, 1)$ and $\rho(Q') = Q$; in particular, $h^+(8) = 1$. In fact, let $(A, B, C) = (1, 4, 2)$; then $C' = A = 1$, and $B' \equiv -B \equiv -4 \equiv 0 \bmod 2A$ and $\sqrt{8} < B' < \sqrt{8} + 2$ implies $B' = 4$. Finally, $A' = \frac{(B')^2 - \Delta}{4C'} = \frac{4^2-8}{4} = 2$.

The next lemma will be used for showing that ρ is a reduction map for $\mathcal{R}_{\rm Zag}$:

Lemma 1.17. *Let $Q = (A, B, C)$ be a quadratic form with positive discriminant Δ, and let $Q' = (A', B', C') = \rho(Q)$ be its right neighbor.*

1. *If $A < 0$, then $A' > A$.*
2. *If $A > 0$, then $A' > 0$.*
3. *If $A' \ge A > 0$, then Q' is Z-reduced.*
4. *If Q is Zagier reduced, then $\rho(Q) = Q|_S$ for some $S = S_n = \left(\begin{smallmatrix} n & 1 \\ -1 & 0 \end{smallmatrix}\right)$ with $n \ge 2$.*

Proof. Write $\frac{B+\sqrt{\Delta}}{2A} = n - \theta$ for some real number θ with $0 < \theta < 1$. Plugging $n = \frac{B+\sqrt{\Delta}}{2A} + \theta$ into the formula $A' = An^2 - Bn + C$ we easily find that

$$A' = A\theta^2 + \sqrt{\Delta}\theta.$$

This immediately implies property 2.

Property 1. is also clear: if $A < 0$, then $A' - A = A(\theta^2 - 1) + \sqrt{\Delta}\theta > 0$ since both A and $\theta^2 - 1$ are negative.

For proving 3, assume that $A' \ge A > 0$. Then

$$\begin{aligned}0 \le A' - A &= \theta\sqrt{\Delta} - A(1-\theta^2)\\ &< (1+\theta)\sqrt{\Delta} - A(1-\theta^2) = (1+\theta)(\sqrt{\Delta} - A(1-\theta))\\ &= \frac{1+\theta}{1-\theta}\big(\sqrt{\Delta}(1-\theta) - A(1-\theta)^2\big) = \frac{1+\theta}{1-\theta}(B' - A' - C').\end{aligned}$$

Thus $A' \ge A > 0$, $C' = A > 0$, and $B' > A' + C'$, hence Q' is Zagier reduced.

Finally assume that Q is Zagier reduced. Then $\xi_2 = \frac{B+\sqrt{\Delta}}{2A} > 1$, and this implies $n \ge 2$. □

Now we can prove

Proposition 1.18. *The map ρ is a reduction map. In fact, let $Q = (A, B, C)$ be a quadratic form with positive discriminant Δ.*

1. *There is an integer $\nu > 0$ such that $\rho^\nu(Q)$ is Z-reduced.*
2. *If Q is Zagier reduced, then so is $\rho(Q)$.*

Proof. If A is negative, then $A' > A$ by Lemma 1.17lemmacount.1.17.1; thus repeatedly applying ρ will give us a form with positive first coefficient. By Lemma 1.17lemmacount.1.17.2, the first coefficient will then stay positive, and since $C' = A$, another application of ρ produces a form in which the first and the last coefficient are positive. Since the first coefficient stays positive, there must be a point at which $A' \ge A$. But then Lemma 1.17lemmacount.1.17.1 tells us that one more application of ρ produces a Zagier reduced form.

If Q is Zagier reduced, then $A', C' > 0$, and

$$B' - A' - C' = (1-\theta)(\sqrt{\Delta} - A(1-\theta)) > 0$$

because $\frac{\sqrt{\Delta}}{A} = n - \theta - \frac{B-\sqrt{\Delta}}{2A} > 1 - \theta$. Thus $Q' = \rho(Q)$ is also Zagier reduced. □

For each form Q there is a right neighbor $\rho(Q)$. In general, many different forms might have the same right neighbor. This does not hold for forms (A, B, C) satisfying

$$\begin{cases}\sqrt{\Delta} < B' < \sqrt{\Delta} + 2A & \text{if } A > 0,\\ \sqrt{\Delta} + 2A < B' < \sqrt{\Delta} & \text{if } A < 0.\end{cases} \tag{1.16}$$

Such forms are called semi-reduced (in Zagier's sense).

Proposition 1.19. *The reduction map ρ is injective on semi-reduced forms.*

Proof. □

Thus we can define a *left neighbor* $\lambda(Q)$ by inverting the reduction map ρ: assume that $\rho(Q) = Q'$ for $Q = (A, B, C)$ and $Q' = (A', B', C')$. Then we would like to have $\lambda(Q') = Q$ if possible. To this end we set

1. $A = C'$;
2. $B + B' \equiv 0 \bmod 2C'$ and $\begin{cases}\sqrt{\Delta} < B < \sqrt{\Delta} + 2C' & \text{if } C' > 0,\\ \sqrt{\Delta} + 2C' < B < \sqrt{\Delta} & \text{if } C' < 0.\end{cases}$
3. $B^2 - 4AC = \Delta$.

This allows us to compute A, B and C successively from A', B' and C'.

Here is an alternative characterization of $\lambda(Q)$:

Lemma 1.20. *Let $Q' = (A', B', C')$ be a primitive quadratic form. Then $\lambda(Q') = Q'|_S$ for $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & n \end{smallmatrix}\right)$, where n is an integer defined by $n > \frac{B'+\sqrt{\Delta}}{2C'} > n - 1$.*

Proof. Define an integer n by $B = -B' + 2An$. Then

$$C = \frac{B^2 - \Delta}{4A} = A' - B'n + C'n^2,$$

hence $Q = \lambda(Q') = Q'|_S$ for $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & n \end{smallmatrix}\right)$.

Note that $n = \frac{B'+B}{2A} = \frac{B'+B}{2C'}$. If $C' > 0$, then $B > \sqrt{\Delta}$ and $n > \frac{B'+\sqrt{\Delta}}{2C'} > n - 1$. If $C' < 0$, then $B < \sqrt{\Delta}$ and again $n > \frac{B'+\sqrt{\Delta}}{2C'} > n - 1$. $\square$

It follows from the construction of λ that taking left and right neighbors are operations inverse to each other on the set of reduced forms:

Lemma 1.21. *If Q is semi-reduced, then $\lambda \circ \rho(Q) = Q$ and $\rho \circ \lambda(Q) = Q$.*

This immediately implies the following

Corollary 1.22. *The reduction map ρ permutes the set of reduced forms.*

Of course the same result holds for the reduction map λ.

Proof. We already know that ρ maps reduced forms to reduced forms. Assume that Q and Q' are reduced forms with $\rho(Q) = \rho(Q')$. Applying λ immediately shows that $Q = Q'$. $\square$

Since ρ induces a permutation of the reduced forms, the orbits under this action are disjoint; these orbits are called cycles. Cycles of reduced forms do in general not have the same cardinality, as Table 1.6Cycles and Class numberstable.1.6 shows. The main result of reduction theory proved below will show that the number $h^+(\Delta)$ of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes is equal to the number of cycles.

Consider e.g. the principal form $Q_0 = (1, 1, -8)$ with discriminant $\Delta = 33$:

Fig. 1.1. Zagier Reduction of $(1, 1, -8)$

[illegible]

The form $\rho(Q) = (4, 7, 1)$ is already Zagier reduced (actually, $\rho(Q_0)$ is Zagier reduced for every principal form Q_0: see Exercise 1Reduction of Binary Quadratic Formschapter.1.37ExercisesItem.124). The cycle of reduced forms has length 4; the product of the transformation matrices inside a cycle is equal to $S = S_2 S_3 S_2 S_7 = \left(\begin{smallmatrix} 51 & 8 \\ -32 & -5 \end{smallmatrix}\right)$. This matrix S transforms Q into itself; such transformations are called automorphs. In the next section we will see that the automorph S we have just found gives rise to the solution $(T, U) = (27, -8)$ of the Pell equation $T^2 + TU - 8U^2 = 1$.

It is also possible to apply λ for reducing the form $Q = (1, 1, -8)$; we find $Q' = \lambda(Q) = (-8, 1, 1)$ and $\lambda(Q') = (1, 7, 4)$; from then on, λ traverses the cycle above in the opposite direction.

Δ	#	cycles	$h^+(\Delta)$
5	1	$(1,3,1)$	1
8	1	$(1,4,2),(2,4,1)$	1
12	1	$(1,4,1)$	2
	2	$(2,6,3),(3,6,2)$	
13	1	$(1,5,3),(3,5,1),(3,7,3)$	1
17	1	$(1,5,2),(2,5,1),(2,7,4),(4,7,2),(4,9,4)$	1
20	1	$(1,6,4),(4,6,1),(5,10,4),(4,10,5)$	1
21	1	$(1,5,1)$	2
	2	$(3,9,5),(5,9,3),(5,11,5)$	
24	1	$(1,6,3),(3,6,1)$	2
	2	$(2,8,5),(5,8,2),(6,12,5),(5,12,6)$	
28	1	$(1,6,2),(2,6,1)$	2
	2	$(3,8,3),(6,10,3),(7,14,6),(6,14,7),(3,10,6)$	
29	1	$(1,7,5),(5,7,1),(7,13,5),(7,15,7),(5,13,7)$	
33	1	$(1,7,4),(4,7,1),(3,9,4),(4,9,3)$	2
	2	$(2,7,2),(6,9,2),(8,15,6),(8,17,8),(6,15,8),(2,9,6)$	
37	1	$(1,7,3),(3,7,1),(7,11,3),(9,17,7),(9,19,9),(7,17,9),(3,11,7)$	
40	1	$(1,8,6),(6,8,1),(9,16,6),(10,20,9),(6,16,9)$	2
	2	$(2,8,3),(3,8,2),(5,10,3),(3,10,5)$	
41	1	$(1,7,2),(2,7,1),(5,9,2),(4,11,5),(8,13,4),(10,19,8)$ $(10,21,10),(8,19,10),(4,13,8),(5,11,4),(2,9,5)$	1
44	1	$(1,8,5),(5,8,1),(5,12,5)$	2
	2	$(2,10,7),(7,10,2),(10,18,7),(11,22,10),(10,22,11),(7,18,10)$	
52	1	$(1,8,3),(3,8,1),(4,10,3),(9,14,4),(12,22,9),$ $(13,26,12),(12,26,13),(9,22,12),(4,14,9),(3,10,4)$	
	2	$(2,10,6),(6,10,2),(6,14,6)$	
136	1	$(1,12,2),(2,12,1)$	4
	2	$(3,14,5),(10,16,3),(11,24,10),(6,20,11),(5,16,6)$	
	3	$(5,14,3),(6,16,5),(11,20,6),(10,24,11),(3,16,10)$	
	4	$(9,26,15),(18,28,9),(25,44,18),(30,56,25),(33,64,30)$ $(34,68,33),(33,68,34),(30,64,33),(25,56,30),(18,44,25)$ $(9,28,18),(15,26,9),(17,34,15),(15,34,17)$	
221	1	$(1,15,1)$	4
	2	$(5,19,7),(11,21,5),(7,23,11)$	
	3	$(7,19,5),(11,23,7),(5,21,11)$	
	4	$(13,39,25),(25,39,13),(35,61,25),(43,79,35),(49,93,43)$ $(53,103,49),(55,109,53),(55,111,55),(53,109,55)$ $(49,103,53),(43,93,49),(35,79,43),(25,61,35)$	
229	1	$(1,17,15),(15,17,1),(27,43,15),(37,65,27),(45,83,37),(51,97,45)$ $(55,107,51),(57,113,55),(57,115,57),(55,113,57),(51,107,55)$ $(45,97,51),(37,83,45),(27,65,37),(15,43,27)$	3
	2	$(3,17,5),(11,19,3),(9,25,11),(17,29,9),(19,39,17),(15,37,19),(5,23,15)$	
	3	$(5,17,3),(15,23,5),(19,37,15),(17,39,19),(9,29,17),(11,25,9),(3,19,11)$	
316	1	$(1,18,2),(2,18,1)$	6
	2	$(3,20,7),(14,22,3),(15,34,14),(6,26,15),(7,22,6)$	
	3	$(3,22,14),(7,20,3),(6,22,7),(15,26,6),(14,34,15)$	
	4	$(5,24,13),(18,26,5),(25,46,18),(26,54,25),$ $(21,50,26),(10,34,21),(9,26,10),(13,28,9)$	
	5	$(5,26,18),(13,24,5),(9,28,13),(10,26,9),$ $(21,34,10),(26,50,21),(25,54,26),(18,46,25)$	
	6	$(15,44,27),(30,46,15),(43,74,30),(54,98,43),(63,118,54),$ $(70,134,63),(75,146,70),(78,154,75),(79,158,78),$ $(78,158,79),(75,154,78),(70,146,75),(63,134,70),$ $(54,118,63),(43,98,54),(30,74,43),(15,46,30),(27,44,15)$	

Table 1.6. Cycles and Class numbers

Remark. Looking at the cycles of Zagier reduced forms with discriminant $\Delta = 4{\cdot}79 = 316$, it is difficult to overlook the role of the middle coefficient B: I have started the cycle at a form with minimal B, and then subsequent applications of ρ give rise to forms whose middle coefficient increases up to a maximum, and then returns to the minimal value. Perhaps these observations deserve to be studied more carefully.

The Main Theorem of Zagier Reduction

Forms contained in the same cycle are, by definition, equivalent. The converse result is a fundamental result in any serious reduction theory for binary quadratic forms.

Theorem 1.23. *Two primitive Z-reduced forms Q, Q' with discriminant Δ are equivalent if and only if they belong to the same cycle.*

While the idea behind the proof is rather simple, the actual argument is partially clouded by technical details, which we have packed into the fundamental

Lemma 1.24 (Fundamental Lemma). *Assume that there are Zagier reduced forms Q, Q' with $Q' = Q|_S$ for some matrix $S = (\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}) \in \mathrm{SL}_2(\mathbb{Z})$. Then $S = S_a S_b \ldots S_h$ is the product of reduction matrices, and the forms $Q_1 = Q|_{S_a}$, $Q_2 = Q_1|_{S_b}$, … are all Zagier reduced.*

Proof. Then

$$A' = Q(r,t) > 0, \tag{1.17}$$
$$C' = Q(s,u) > 0, \tag{1.18}$$
$$A' + C' - B = Q(r-s, t-u) < 0. \tag{1.19}$$

If we had $t = u$, then $Q(r-s, t-u) = Q(r-s, 0) > 0$; this contradiction shows that $t \neq u$. Replacing S by $-S$ if necessary we may assume that

$$u > t. \tag{1.20}$$

- $t = 0$: Then $ru = 1$, and $u > t = 0$ shows that $r = u = 1$. Now observe that

$$Q(s,1) = Q(s,u) > 0 > Q(r-s, t-u) = Q(s-1, 1),$$
$$C' = Q(0,1) > 0 > Q(-1,1) = A' + C' - B',$$

  and since for a quadratic polynomial $Q(x,1)$ there is at most one integer n such that $Q(n,1) > 0 > Q(n-1,1)$ we conclude that $s = 0$. Thus $S = (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})$ and $Q' = Q$. In particular, Q and Q' belong to the same cycle.
- $t < 0$: we claim that $Q' = \rho^\nu(Q)$ for some $\nu \geq 1$, in other words: $Q' = Q|_S$, where $S \in \mathrm{SL}_2(\mathbb{Z})$ is the product of the corresponding matrices S_n. Assume that $Q^* = \rho(Q)$, and that S_n is the corresponding matrix; then $Q^* = Q|_{S_n}$. Let

$$S^* = \begin{pmatrix} r^* & s^* \\ t^* & u^* \end{pmatrix} = S_n^{-1} S = \begin{pmatrix} -t & -u \\ r+tn & s+un \end{pmatrix}$$

  be the matrix mapping Q^* to Q':

  We claim that S^* also satisfies the condition (1.20The Main Theorem of Zagier Reductionequation.1.5.20), i.e., that $u^* > t^*$. In fact, we have $r^* - s^* = u - t > 0$, and $Q(r^* - s^*, t^* - u^*) < 0$ implies that $r^* - s^*$ and $t^* - u^*$ have opposite signs.

Next we claim that $t < t^* \le 0$. These inequalities are equivalent to $t < r + nt \le 0$, that is, to

$$n - 1 < -\frac{r}{t} \le n. \tag{1.21}$$

Since $A' = Q(r,t) > 0 > Q(r-s, t-u) = A' + C' - B'$ by (1.17The Main Theorem of Zagier Reductionequation.1.5.17) and (1.19The Main Theorem of Zagier Reductionequation.1.5.17), the polynomial $Q(x,-1) = Ax^2 - Bx + C$ is positive for $x = -\frac{r}{t}$ and negative for $x = -\frac{r-s}{t-u}$; moreover, $-\frac{r}{t} > -\frac{r-s}{t-u}$ because $ru - st = 1 > 0$. Thus the larger root $\xi_1 = \frac{B+\sqrt{\Delta}}{2A}$ of $Q(x,-1)$ satisfies

$$-\frac{r-s}{t-u} < \xi_1 < -\frac{r}{t}.$$

The observation $n-1 < \xi_1$ now implies the first inequality in (1.21The Main Theorem of Zagier Reductionequation.1.5.21).

For proving the second inequality, observe that $-\frac{r}{t} > n$ and $n > \xi_1$ would imply $-\frac{r-s}{t-u} < n < -\frac{r}{t}$, hence $-rt + su < nt(t-u) < -rt + su = 1$, which gives the contradiction $n \le 1$.

Now our claim that S is a product of matrices S_n follows by induction: In the sequence $t < t^* < t^{**} < \ldots \le 0$, some element $t^{*\cdots*}$ must be 0; by what we have proved in the case $t = 0$, we have $Q^{*\cdots*} = Q$, and the corresponding transition matrix $S^{*\cdots*}$ is the identity matrix.

- $t > 0$: here we claim that $Q = \rho^\nu(Q')$; from $Q' = Q|_S$ we get $Q = Q'|_{S^{-1}}$ for $S^{-1} = \left(\begin{smallmatrix} u & -s \\ -t & r \end{smallmatrix}\right)$. Since $-t < 0$, the claim will follow from the second case above if we can show that S^{-1} satisfies the condition (1.20The Main Theorem of Zagier Reductionequation.1.5.20), i.e., that $r > -t$.

  To this end, observe that $\frac{r}{-t} < \frac{r-s}{-t+u}$ since $ru - st = 1 > 0$, hence the inequalities $Q(\frac{r}{-t}, -1) > 0 > Q(\frac{r-s}{-t+u}, -1)$ coming from (1.17The Main Theorem of Zagier Reductionequation.1.5.17) and (1.19The Main Theorem of Zagier Reductionequation.1.5.17) imply that $\frac{r}{-t}$ is smaller than the smallest root of $Q(-x,1) = 0$. This shows that $\frac{r}{-t} < \frac{B-\sqrt{\Delta}}{2A} < 1$.

This finishes the proof of the Fundamental Lemma. □

The Fundamental Lemma allows us to give a clean

Proof of Thm. 1.23lemmacount.1.23. If two forms belong to the same cycle, then they are clearly equivalent. Assume therefore that $(A', B', C') = (A, B, C)|_S$ for some $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. By the fundamental Lemma 1.24Fundamental Lemmalemmacount.1.24, $S = S_a S_b \ldots S_h$ is a product of reduction matrices. But then Q' is in the same cycle as S since applying S_a, S_b, ..., S_h transforms Q into Q' via reduced forms. □

This result allows us to compute the class number for positive discriminants Δ: list all Zagier reduced forms, and determine the cycles to which they belong.

1.6. Automorphs and the Pell Equation

Where the Pell Conic makes its first appearance.

Given a quadratic form Q, the set of all $S \in \mathrm{SL}_2(\mathbb{Z})$ transforming Q into itself forms a group with respect to composition of maps called the group of automorphs of Q. It is also called the special orthogonalroup for Q and is denoted by

$$\mathrm{SO}(Q) = \mathrm{Aut}^+(Q) = \{S \in \mathrm{SL}_2(\mathbb{Z}) : Q|_S = Q\}.$$

Let $Q = (A, B, C)$ be a primitive quadratic form with discriminant Δ, and assume that $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ is an automorph. Recall that using $M(Q) = \left(\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right)$ we can write the equation $Q = Q|_S$ in the form $M(Q) = M(Q|_S) = S'M(Q)S$ or, equivalently, as

$$\begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} u & -t \\ -s & r \end{pmatrix} \begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix}.$$

This gives us the three equations

$$Bt = A(u - r), \qquad As = -Ct, \qquad Bs = C(r - u).$$

The first two equations imply $A \mid Bt$ and $A \mid Ct$; since Q is primitive, we have $\gcd(A, \gcd(B, C)) = 1$, and we deduce that we must have $A \mid t$. Setting $U = \frac{t}{A} \in \mathbb{Z}$ we get $s = -CU$ and $t = AU$, as well as $BU = u - r$. Now we distinguish two cases:

1. $\Delta = 4m$: from $B \equiv \Delta \bmod 2$ we see that B is even. This implies that $A(r - u) \equiv C(r - u) \equiv 0 \bmod 2$, and since (A, B, C) is primitive, at least one of A or C is odd, so we must have $r \equiv u \bmod 2$. Setting $u + r = 2T$ for $T \in \mathbb{Z}$ we can express r, s, t, u in terms of T, U, and the coefficients A, B, C of Q. These equations can be expressed in matrix form
$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} T - \frac{B}{2}U & -CU \\ AU & T + \frac{B}{2}U \end{pmatrix}. \tag{1.22}$$
Next $1 = ru - st = T^2 - mU^2$, whence
$$T^2 - mU^2 = 1. \tag{1.23}$$
Thus every automorph comes from an integral solution of the Pell equation (1.23Automorphs and the Pell Equationequation.1.6.23), and conversely, every integral solution of (1.23Automorphs and the Pell Equationequation.1.6.23) gives rise to an automorph of Q.
2. $\Delta = 4m + 1$: then $B \equiv \Delta \bmod 2$ is odd, hence $u + r \equiv u - r = BU \equiv U \bmod 2$. Thus we can write $r + u = 2T + U$ for some $T \in \mathbb{Z}$, and then we get $r = T + \frac{1-B}{2}U$, $u = T + \frac{1+B}{2}U$, and
$$1 = ru - st = T^2 + TU + U^2\frac{1 - B^2}{4} + ACU^2 = T^2 + TU - mU^2.$$
Collecting everything we get
$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} T + \frac{1-B}{2}U & -CU \\ AU & T + \frac{1+B}{2}U \end{pmatrix}, \tag{1.24}$$
as well as
$$T^2 + TU - mU^2 = 1. \tag{1.25}$$

The plane algebraic curve
$$\mathcal{P}_\Delta : Q_0(X, Y) = 1, \tag{1.26}$$
where Q_0 is the principal form with discriminant Δ defined in (1.7Representations by Quadratic Formsequation.1.3.7), is called the *Pell conic* with discriminant Δ. The number of integral points on a Pell conic (that is, the number of integral solutions of the corresponding Pell equation) depends on the sign of the discriminant: for $\Delta < 0$, there are only finitely many integral points, whereas for nonsquare discriminants $\Delta > 0$ there are infinitely many.

We have shown:

Theorem 1.25. *Let $Q = (A, B, C)$ be a primitive binary quadratic form with discriminant Δ. Then the maps defined by (1.22Automorphs and the Pell Equationequation.1.6.22) and (1.24Automorphs and the Pell Equationequation.1.6.24) induce a bijection between automorphs $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ of Q and integral points (T, U) on the Pell conic $Q_0(X, Y) = 1$.*

Multiplying through by 4 and completing the square shows that the Pell equations (1.23Automorphs and the Pell Equationequation.1.6.23) and (1.25Automorphs and the Pell Equationequation.1.6.25) both can be written in the form $T^2 - \Delta U^2 = 4$. For working with Pell conics over fields of characteristic 2, using Equation (1.25Automorphs and the Pell Equationequation.1.6.25) is absolutely necessary.

Constructing automorphs of a quadratic form Q is equivalent to solving the associated Pell equation $Q_0(X, Y) = 1$, which is very easy for negative discriminants: if $\Delta < -4$, then the Pell equations $Q_0(X, Y) = 1$ only have the trivial solutions $(\pm 1, 0)$: this follows from the fact that, for $\Delta < -4$, the equation $X^2 - \Delta Y^2 = 4$ only has the trivial integral solutions $(X, Y) = (\pm 2, 0)$. For $\Delta = -3$ and $\Delta = -4$, there are solutions $\neq (\pm 1, 0)$:

Δ	$Q_0(X,Y) = 1$	solutions (T,U)
-3	$X^2 + XY + Y^2 = 1$	$(\pm 1, 0); (0, \pm 1); (\pm 1, \mp 1)$
-4	$X^2 + Y^2 = 1$	$(\pm 1, 0); (0, \pm 1)$

For positive nonsquare values of Δ, there always seem to exist nontrivial solutions:

Δ	T	U	Δ	T	U	Δ	T	U	Δ	T	U	Δ	T	U	Δ	T	U
5	1	1	41	1729	640	73	2014249	534000	8	3	2	44	10	3	76	170	39
13	4	3	45	3	1	77	4	1	12	2	1	48	7	2	80	9	2
17	25	16	53	22	7	85	37	9	20	9	4	52	649	180	84	55	12
21	2	1	57	131	40	89	447001	106000	24	5	2	56	15	4	88	197	42
29	11	5	61	664	195	93	13	3	28	8	3	60	4	1	92	24	5
33	19	8	65	113	32	97	56432281	12754704	32	3	1	68	33	8	96	5	1
37	61	24	69	11	3	101	181	40	40	19	6	72	17	4	104	51	10

Fig. 1.2. Minimal Solutions of Pell Equations

There are several different proofs of the fact that the Pell equation always has nontrivial integral solutions for all positive nonsquare discriminants Δ. Here we will give a proof based on reduction theory of indefinite forms.

Solving the Pell Equation

Let $\Delta > 0$ be a nonsquare discriminant, and let Q be any reduced form with discriminant Δ. Then $\rho(Q) = Q|_S$ for some transformation matrix S_n, and there is an integer $m \geq 1$ such that $\rho^m(Q) = Q$. Let $S = \prod S_n$ be the product of the transformation matrices inside the cycle generated by Q. Since the only automorph coming from the trivial solution of the Pell equation is the identity matrix (up to sign), we will have proved the next theorem if we can show that $S \neq \pm I$:

Theorem 1.26. *Let $\Delta > 0$ be a nonsquare discriminant. Then the Pell equation $Q_0(T, U) = 1$ always has a solution with $U \neq 0$.*

Proof. Let Q be a reduced form with discriminant Δ. Then there exists an $m > 0$ such that $\rho^m(Q) = Q$; the product of the corresponding transition matrices $S = \prod_{j=1}^m S_n = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ is an automorph of Q, and the existence of a nontrivial solution of the Pell equation $Q_0(T,U) = 1$ will follow from the fact that $t \neq 0$. We will prove by induction that we always have $t < u \le 0$: if $m = 1$, then $S = S_n$ and $t = -1 < 0 = u$. Now assume that the result holds for some m, i.e., that $S = \prod_{j=1}^m S_n = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ with $t < u \le 0$. Setting $S' = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \cdot S_m$, we have $t' = nt - u$ and $u' = t$. Thus $u' < 0$, and $t' < u'$ is equivalent to $nt - u < t$, that is, to $(n-1)t < u$. This follows from $n \ge 2$ (see Lemma 1.17lemmacount.1.17.4): we have $(n-1)t \le t < u$ by induction assumption. □

Example. It is easy to compute a solution of the Pell equation $T^2 - 79U^2 = 1$, where $\Delta = 4 \cdot 79$, from the principal cycle $Q = (1,18,2) \xrightarrow{\rho} (2,18,1) \xrightarrow{\rho} (1,18,2)$: the corresponding reduction matrices are S_{18} and S_9, giving the automorph $S = S_{18}S_9 = \left(\begin{smallmatrix} 161 & 18 \\ -9 & -1 \end{smallmatrix}\right)$ of Q and the solution $(T,U) = (80,-9)$.

Similarly, the cycle starting with $Q = (3,20,7)$ gives the automorph $S = S_7S_2S_2S_4S_3 = \left(\begin{smallmatrix} 170 & 63 \\ -27 & -10 \end{smallmatrix}\right)$ of Q and the solution $(T,U) = (80,-9)$ of the Pell equation.

The solution of the Pell equation given by running through the principal cycle is always the smallest nontrivial solution:

Proposition 1.27. *Let (T,U) be the smallest solution of the Pell equation $Q_0(T,U) = 1$ with $T,U > 0$. Then the algorithm used in the proof of Thm. 1.26lemmacount.1.26 produces (T,U) or $(T,-U)$.*

Proof. Let S be the automorph of a form Q with discriminant Δ. Now apply the Fundamental Lemma to $Q = Q|_S$. □

The proof also shows that running through different cycles always gives the same solution (T,U), at least up to sign.

Group Structure

Next we observe that the set of automorphs is a group with respect to composition of maps: given two automorphs $S_Q^{(T,U)}$ and $S_Q^{(T',U')}$, the compositions $S_Q^{(T,U)} \circ S_Q^{(T',U')}$ and $S_Q^{(T',U')} \circ S_Q^{(T,U)}$ must also be automorphs, hence they correspond to certain points on the Pell conic $Q_0(X,Y) = 1$.

This can be proved almost without calculation by observing that

$$S_Q^{(T,U)} = TI + U\mu(Q),$$

where $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We find

$$\begin{aligned} (T'', U'') &= (TI + U\mu(Q))(T'I + U'\mu(Q)) \\ &= (TT' + mUU')I + (TU' + T'U + \sigma UU')\mu(Q), \end{aligned}$$

where, as usual, $\sigma \in \{0,1\}$ is defined by $\Delta = 4m + \sigma$.

Since switching (T,U) and (T',U') does not change (T'',U''), the matrices $S_Q^{(T,U)}$ and $S_Q^{(T',U')}$ commute, that is, we have $S_Q^{(T,U)} \circ S_Q^{(T',U')} = S_Q^{(T',U')} \circ S_Q^{(T,U)}$. We have proved

Proposition 1.28. *The automorphs $S_Q^{(T,U)}$ of a quadratic form Q with discriminant Δ form an abelian group $\mathrm{Aut}^+(Q)$ with respect to composition. By "transport of structure", the set of integral points (T,U) on the Pell conic $\mathcal{P} : Q_0(X,Y) = 1$ becomes a group with respect to the addition law*

$$(T,U)\oplus(T',U')=\begin{cases}(TT'+mUU',TU'+T'U) & \textit{if } \Delta=4m,\\ (TT'+mUU',TU'+T'U+UU') & \textit{if } \Delta=4m+1.\end{cases}$$

With this group law, the bijection $\mathcal{P}(\mathbb{Z})\longrightarrow \mathrm{Aut}^+(Q)$ becomes an isomorphism of groups. Its neutral element is $(1,0)$, and the inverse of (T,U) is $(T+\sigma U,-U)$, where $\sigma\in\{0,1\}$ is defined by $\Delta=4m+\sigma$.

It is easy to describe the structure of all solutions of the Pell equation. For doing so, we need the "minimal solution" of the Pell equation $Q_0(T,U)=1$: this is the unique solution (T,U) with $T,U\ge 1$ such that any solution (T',U') of the Pell equation with $T'\ge 1$ satisfies $T\le T'$.

Theorem 1.29. *Let (T,U) be the minimal solution of $Q_0(X,Y)=1$ with $T,U>0$. Then every solution of the Pell equation has the form (X,Y), where X and Y are given by $X+Y\omega=(-1)^a(T+U\omega)^n$; here $a\in\{0,1\}$ and $n\in\mathbb{Z}$. Moreover, the map $(T+U\omega)^n\longmapsto S_Q^{(T,U)}$ induces an isomorphism between the group of units $\varepsilon>0$ in $\mathcal{O}_\Delta$ and the group of automorphs of a form Q with discriminant Δ.*

Proof. We give the proof only for discriminants $\Delta=4m$; the other case is left to the reader. For any integer $n\in\mathbb{Z}$, set $(T_n,U_n)=n(T,U)$; then $(T_0,U_0)=(1,0)$ and $(T_1,U_1)=(T,U)$. Let (T',U') with $T',U'>0$ be a solution and write $T_k\le T'<T_{k+1}$. Then $U_k\le U'<U_{k+1}$; in fact, we have $mU'^2=T'^2-1<T_{k+1}^2-1=mU_{k+1}^2$, and the other claim follows similarly.

Define $(T'',U'')=(T',U')-k(T,U)$; we claim that (T'',U'') is a solution of the Pell equation with $1\le T''<T$, By the minimality of T, we must have $T''=1$, hence $T'=T_k$.

This is proved by induction: setting $(T'',U'')=(T',U')+(T,U)$ we find, if $\Delta=4m$, that $T''=T'T+mU'U$, hence $T''\ge T_kT+mU_kU=T_{k+1}$ and $T''<T_{k+1}T+mU_{k+1}U=T_{k+2}$, hence $T_{k+1}\le T''<T_{k+2}$.

□

1.7. Notes

Reduction: Goldbach-Euler, Lagrange, Gauss, Hurwitz, Hermite, Klein,

Although the condition (1.34equation.1.8.34) for reduced forms is extremely simple, it is hardly ever mentioned in the relevant literature. A notable exception is the article [CB2006] by Castaño-Bernard.

Cornacchia et al

Hermite [Her1848] showed how to solve the equation $p=x^2+y^2$ for primes $p\equiv 1 \bmod 4$ by solving the congruence $a^2+1\equiv 0 \bmod p$ and developing $\frac{a}{p}$ into a continued fraction. He generalized this to a procedure of solving $p^h=x^2+my^2$ in [Her1849].

Theorem 1.2lemmacount.1.2 is a special case of a result due to Latimer & MacDuffee [LMD1933]. It was popularized by Olga Taussky in various articles, starting with [Tau1949].

Legendre (see [Leg1798, p. 69–76]; [Leg1808, p. 61–76]; [Leg1830, I, p. 72–80]) proved that the minimal number represented by the reduced positive definite form (A,B,C) is A.

The next two minimal numbers represented by (A, B, C) were given by Hermite [Her1851, p. 168], and two more by Humbert [Hu1915] and Julia [Ju1916]; see Exer. 1Reduction of Binary Quadratic Formschapter.1.33ExercisesItem.120 for the exact statements.

Mertens [Mer1880] gave a simplified proof of Gauss's Theorem that two forms are equivalent if and only if they belong to the same cycle. His proof was further streamlined by Scholz [Sch1939] and Rehm [Reh2006].

The connection between the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane and the reduction theory of positive definite binary quadratic forms was already noticed by Gauss [Gau1900b, p. 105]. As a matter of fact, Gauss let

$$\Gamma(2) = \{\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) : ru - st = 1, r \equiv u \equiv 1, s \equiv t \equiv 0 \bmod 2\}$$

act on the right half plane via $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) z = \frac{rz - si}{tiz + u}$ (see Houzel [Hou2007]).

Continued Fractions

The first investigation of "negative continued fractions" is due to Möbius [Moe1830] and, independently, to Stern [Ste1866]; see also Perron [Per1913] and Zurl [Zur1936]. For a modern treatment of these continued fractions, see Katok [Kat2001, Chap. 1].

Minnigerode [Min1873b] introduced a notion of reduced forms that lies somewhat between Gauss's and Zagier's.

Negative continued fractions resurfaced in the work of Hirzebruch [Hir1973] on singularities of Hilbert modular surfaces; as a corollary, he obtained an "amusing" class number formula which was proved more directly by Zagier [Zag1975b] in connection with Kronecker's limit formula. Connections between negative continued fractions and quadratic forms (and Dedekind sums) had earlier been observed by Rademacher [Rad1956]. The reduction theory of quadratic forms correcponding to these negative continued fractions was worked out by Zagier in his book [Zag1981]; although Zagier's book became well known, Zagier reduction did not become popular; it was used, however, by Choie & Parson [CP1989, CP1991].

The caliber of a quadratic number field was introduced by Lachaud [Lac1984, Lac1988]. Zagier [Zag1975b] had called the cycle length with respect to Zagier reduction the *length* of the form class.

The Pell Equation.

The Pell equation has a long history. In his measurement of the circle, where Archimedes gave bounds for π (the ratio of the circumference and the diameter of a circle), the estimates

$$\frac{265}{153} < \sqrt{3} < \frac{1351}{780}$$

for the square root of 3 were used (without comments). Since $265^2 - 3 \cdot 153^2 = -2$ and $1351^2 - 3 \cdot 780^2 = 1$, these estimates must have come from some procedure generating solutions of the equations $x^2 - 3y^2 = -2$ and $x^2 - 3y^2 = 1$.

The Pell equation also appears in another contribution by Archimedes, the famous cattle problem (the smallest solution of the equation in this problem has more than 200 000 digits). For more, see [JW2009, Chap. 2.1].

Indian mathematicians such as Brahmagupta (598–670) and Bhaskara II (1114–1185) gave recipes for solving the Pell equation. The contributions of the Indian mathematicians to number theory became known in the west through Colebrooke's translation [Col1817] of the algebra of Brahmagupta and Bhascara. A little later, Chasles [Cha1837] discussed their work on quadratic diophantine equations. For a detailed exposition of the "cyclic method", see Selenius [Sel1963, Sel1975]. The first proof that the cyclic method always produces a solution of the Pell equation was provided by Ayyangar [Ayy1929, Ayy1940].

Fermat posed the problem of solving the Pell equation as a challenge for the English mathematicians, and Brouncker gave a method for doing so, but failed to prove that his method always provides a solution. Fermat claimed to have such a proof; for reconstructions of what he might have had in mind, see Hofmann [Hof1944] or Weil [Wei1977, Wei1984].

Euler described Brouncker's method using continued fractions, and Lagrange finally proved that this method for solving the Pell equation $X^2 - DY^2 = 1$ always produces a solution whenever D is a nonsquare positive integer.

1.8. Projects

We now describe several projects in which readers are asked to provide the proofs themselves.

1.8.1 The Complex Upper Half Plane

In this project we give a geometric description of the reduction of positive definite quadratic forms. This point of view becomes indispensible for studying complex multiplication, an area closely related to the more advanced arithmetic of elliptic curves, but also tied to certain questions related to binary quadratic forms such as Gauss's class number 1 problem, or the theory of *Heegner points*.

Consider a positive definite form $Q = (A, B, C)$ with discriminant $\Delta = B^2 - 4AC < 0$; the quadratic polynomial $f_Q(X) = Q(X, 1) = AX^2 + BX + C$ has two roots, namely $x_{1,2} = \frac{-B \pm \sqrt{\Delta}}{2A}$. To each such form Q, we associate the root $z(Q)$ with positive imaginary part by setting

$$z(Q) = \frac{-B + i\sqrt{-\Delta}}{2A}.$$

This complex number is a point in the *upper half plane* $\mathcal{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. Note that from every such point we can get back the form Q: the coefficients A and B can be read off directly, and then C can be determined from $\Delta = B^2 - 4AC$. Let us record the following observation:

Lemma 1.30. *For every positive definite form $Q = (A, B, C)$ and the associated point $z = z(Q)$, we have*

$$AX^2 + BXY + CY^2 = A(X - zY)(X - \overline{z}Y).$$

It is clear that the modular group $\mathrm{SL}_2(\mathbb{Z})$ acts on these roots; by studying this action, we can give a geometric description of Lagrange's theory of reduction.

Remark. Dirichlet studied the action of the modular group $\mathrm{SL}_2(\mathbb{Z})$ on the roots of the polynomial $f_Q(X) = AX^2 + BX + C$ attached to a positive definite form $Q = (A, B, C)$, and called the root with positive imaginary part the first root. Dedekind then viewed these roots as elements of the upper half plane and introduced the fundamental domain. A sketch of this fundamental domain was also found in the posthumous papers of Gauss.

We start by making $\mathrm{SL}_2(\mathbb{Z})$ act on the upper half plane $\mathcal{H}$ via

$$S(z) = \frac{rz + s}{tz + u} \tag{1.27}$$

for $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$. Observe that this resembles the action of $\mathrm{SL}_2(\mathbb{Z})$ on the projective line (see (A.1The Projective Lineequation.A.4.1)); in fact, the upper half plane is just a piece of the complex projective line $\mathbb{P}^1\mathbb{C}$. This suggests defining analogs of the upper half plane for $\mathbb{P}^1\mathbb{F}_p$ and $\mathbb{P}^1\mathbb{F}_p[T]$ as well. Can you work out the details?

Proposition 1.31. *Equation (1.27The Complex Upper Half Planeequation.1.8.27) defines an action of* $\mathrm{SL}_2(\mathbb{Z})$ *on the upper half plane:*

1. *For $z \in \mathcal{H}$ we have $S(z) \in \mathcal{H}$.*
2. *We have $Iz = -Iz = z$ for the identity matrix I and its additive inverse $-I$.*
3. *We have $(ST)z = S(Tz)$ for $z \in \mathcal{H}$ and $S, T \in \mathrm{SL}_2(\mathbb{Z})$.*

The action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half is compatible with the action of $\mathrm{SL}_2(\mathbb{Z})$ on quadratic forms:

Lemma 1.32. *Let Q be a positive definite quadratic form. Then $z(Q|_S) = S^{-1}z(Q)$ for all $S \in \mathrm{SL}_2(\mathbb{Z})$.*

In the following, the matrices $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ will play a prominent role. T represents a shift by 1 to the right since $T(z) = z + 1$, and S is the composition of reflection at the unit circle and a reflection at the imaginary axis ($S(z) = -\frac{1}{z}$). It is easily checked that $S^2 = (ST)^3 = -I$. Note that although S and ST have finite order, the product $S \cdot ST = T$ has infinite order.

Definition. We define an equivalence relation on $\mathcal{H}$ by setting $z' \sim z$ for $z, z' \in \mathcal{H}$ if $z' = M(z)$ for some $M \in \mathrm{SL}_2(\mathbb{Z})$. We also define the fundamental domain F with respect to this action by

$$F = \{z \in \mathcal{H} : |z| \ge 1,\ -\tfrac{1}{2} \le \mathrm{Re}(z) < \tfrac{1}{2}, \text{ and } \mathrm{Re}(z) \le 0 \text{ if } |z| = 1\}.$$

With this definition, we have

Lemma 1.33. *A binary quadratic form $Q = (A, B, C)$ with negative discriminant is reduced if and only if $z(Q) \in F$.*

It follows from Lagrange's reduction theory that every point $z(Q)$, where Q is a positive definite binary quadratic form, is equivalent to a unique point inside F. The next result, which is fundamental in the theory of modular forms, shows that this holds for all points in the upper half plane, not just those of the form $z(Q)$:

Theorem 1.34. *The fundamental domain F is a complete set of representatives for $\mathcal{H}/\sim$, i.e., for every $z \in \mathcal{H}$ there is a unique $z' \in F$ with $z' \sim z$.*

Moreover, if $gz = z$ for some $z \in D$ and $g \in \Gamma = \mathrm{PSL}_2(\mathbb{Z})$, then

$$\begin{cases} z = i & \text{and } g = S; \\ z = \rho & \text{and } g = ST \text{ or } g = (ST)^2. \end{cases}$$

Theorem 1.35. *The group $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ is generated by S and T.*

If you know some group theory, then this result can be stated in the form $\Gamma = \langle S, T | S^2 = (ST)^3 = 1\rangle$; in more fancy language, this means that Γ is the free product of $\langle S\rangle \simeq \mathbb{Z}/2\mathbb{Z}$ and $\langle ST\rangle \simeq \mathbb{Z}/3\mathbb{Z}$.

The Real Analog For finding a real analog of the upper half plane, one should replace the complex numbers $a + bi$ with $i^2 = -1$ by numbers of the form $a + bj$, where $j^2 = +1$. These numbers are added and multiplied in the obvious way; for example, we have $(a + bj)(c + dj) = ac + bd + (ad + bc)j$. The dual numbers form a two-dimensional algebra over the reals; since $(1 + j)(1 - j) = 1 - j^2 = 0$, this algebra contains zero divisors, and is not a division algebra (an algebra is called a division algebra if we can divide by nonzero elements; in the dual numbers, division by $1 + j$ is not possible).

ρ $\qquad$ $1+\rho$

Fig. 1.3. Fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

1.8.2 Gauss Reduction

Let $Q = (A, B, C)$ be an indefinite quadratic form of discriminant $\Delta > 0$ (in the following, we will always assume that Δ is not a square). Let A be an integer such that $|A|$ is minimal among all numbers represented by Q. By changing B modulo $2A$ we can demand that B lies in some fixed interval of length $2A$. We could choose $\sqrt{\Delta}-|A| < B < \sqrt{\Delta}+|A|$ (this choice minimizes $|B^2-\Delta|$), but almost everyone follows Gauss's condition $\sqrt{\Delta}-2|A| < B < \sqrt{\Delta}$ (forms satisfying this condition are called semi-reduced); thus, in particular, $B < \sqrt{\Delta}$). Since $|A|$ is minimal, we must have $|A| \le |C|$, hence our forms satisfy

$$\begin{cases} \sqrt{\Delta} - 2|A| < B < \sqrt{\Delta}, \\ \sqrt{\Delta} - 2|C| < B < \sqrt{\Delta}. \end{cases} \tag{1.28}$$

Forms with these properties are called *Gauss reduced* (or, in this section, simply *reduced*). Every reduced form is semi-reduced, and for every indefinite form (A, B, C) there is exactly one semi-reduced form (A, B', C'). The symmetry of the conditions for a form to be reduced implies that (A, B, C) is reduced if and only if (C, B, A) is.

The analog of Thm. 1.14lemmacount.1.14 is:

Theorem 1.36. *Let $Q = (A, B, C)$ be a primitive indefinite form with discriminant $\Delta = B^2 - 4AC$, and let ξ_1 and $\xi_2 = \xi_1'$ denote the two roots of the quadratic equation $Q(x, 1) = Ax^2 + Bx + C = 0$. Then the following statements are equivalent:*

$$(A, B, C) \text{ is reduced.} \tag{1.29}$$

$$(C, B, A) \text{ is reduced.} \tag{1.30}$$

$$0 < \sqrt{\Delta} - B < 2|A| < \sqrt{\Delta} + B. \tag{1.31}$$

$$0 < \sqrt{\Delta} - B < 2|C| < \sqrt{\Delta} + B. \tag{1.32}$$

$$\xi_1\xi_2 < 0, \quad |\xi_1| < 1 < |\xi_2|. \tag{1.33}$$

$$AC < 0, \ B > |A + C|. \tag{1.34}$$

It is clear from the following lemma that there are only finitely many reduced forms of a given discriminant:

Lemma 1.37. *If the indefinite form $Q = (A, B, C)$ is reduced, then*

$$B > 0, \quad AC < 0, \quad \text{and} \quad 0 < |A|, B, |C| < \sqrt{\Delta}.$$

For discriminants $\Delta > 5$, the principal form Q_0 is not reduced.

Lemma 1.38. *For every positive discriminant Δ, the principal form Q_0 is equivalent to a unique reduced form $(1, B, C)$, where B is the largest integer with $B < \sqrt{\Delta}$ and $B \equiv \Delta \bmod 2$.*

For a form $Q = (A, B, C)$ with discriminant Δ, the form $\rho(Q) = Q' = (A', B', C')$ is called the right neighbor of Q if it satisfies the following conditions:

1. $A' = C$;
2. $B + B' \equiv 0 \bmod 2A'$ and $\sqrt{\Delta} - |2A'| < B' < \sqrt{\Delta}$;
3. $B'^2 - 4A'C' = \Delta$.

Observe that these conditions determine respectively A', B' and C'. Observe also that $\rho(Q) = Q|_S$ for $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -t \\ 0 & 1 \end{smallmatrix}\right)$, where t is determined by $B + B' = 2Ct$.

Lemma 1.39. *1. If Q is a primitive indefinite form, then $\rho(Q)$ is semi-reduced.*
2. If Q is reduced, then so is $\rho(Q)$.

Lemma 1.40. *Let $Q = (A, B, -A)$ be a quadratic form with discriminant $\Delta = B^2 + 4A^2$, let c denote the class of Q in $\mathrm{Cl}^+(\Delta)$, and k the class of $-Q_0$, where $-Q_0 = (-1, 0, m)$ or $(-1, -1, m)$ according as $\Delta = 4m$ or $\Delta = 4m + 1$. Then $c^2 = k$.*

Prove that these cycles have the following properties:

1. Every reduced form belongs to some cycle. What we have to prove here is that every reduced form is part of the cycle it generates, that is, we have to prove that if Q is reduced and $\rho^m(Q) = \rho(Q)$, then $\rho^{m-1}(Q) = Q$.
2. Forms in the same cycle are equivalent.
3. Forms in different cycles are not equivalent.

1.8.3 Zagier's One-Line Proof of the Two-Squares Theorem

In this project, we analyse Heath-Brown's short proof of the fact that primes $p \equiv 1 \bmod 4$ are sums of two squares, which was popularized by Zagier [Zag1990]. Zagier's proof is a modification of a proof given by Heath-Brown [HB1984], which in turn is apparently connected to results obtained by Liouville. For more on this proof, see Elsholtz [Els1994, Els2003] and Jackson [Jac2000a, Jac2000b].

Zagier's Version. Zagier's proof works with a set

$$S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}.$$

The map

$$g : (x, y, z) \longmapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z, \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y, \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

defines an involution on S with exactly one fixed point $(1, 1, \frac{p-1}{4})$. Thus S has odd cardinality, hence the involution

$$(x, y, z) \longmapsto (x, z, y)$$

also has exactly one fixed point. Thus there is a point $(x, y, z) \in S$ with $y = z$, and we have $p = x^2 + 4y^2$.

As short and elegant this proof is, many people have complained that they do not understand what makes it work. In this section we will uncover the underlying structure.

Δ	h^+	cycles
5	1	$(1,1,-1), (-1,1,1)$
8	1	$(1,2,-1), (-1,2,1)$
12	2	$(1,2,-2), (-2,2,1)$
		$(-1,2,2), (2,2,-1)$
13	1	$(1,3,-1), (-1,3,1)$
17	1	$(1,3,2), (-2,1,2), (2,3,-1), (-1,3,2), (2,1,-2), (-2,3,1)$
20	1	$(1,4,-1), (-1,4,1)$
21	2	$(1,3,-3), (-3,3,1)$
		$(-1,3,3), (3,3,-1)$
24	2	$(1,4,-2), (-2,4,1)$
		$(-1,4,2), (2,4,-1)$
28	2	$(1,4,-3), (-3,2,2), (2,2,-3), (-3,4,1)$
		$(-1,4,3), (3,2,-2), (-2,2,3), (3,4,-1)$
29	1	$(1,5,-1), (-1,5,1)$
32	2	$(1,4,-4), (-4,4,1)$
		$(-1,4,4), (4,4,-1)$
33	2	$(1,5,-2), (-2,3,3), (3,3,-2), (-2,5,1)$
		$(-1,5,2), (2,3,-3), (-3,3,2), (2,5,-1)$
37	1	$(1,5,-3), (-3,1,3), (3,5,-1), (-1,5,3), (3,1,-3), (-3,5,1)$
40	2	$(1,6,-1), (-1,6,1)$
		$(2,4,-3), (-3,2,3), (3,4,-2), (-2,4,3), (3,2,-3), (-3,4,2)$
41	1	$(1,5,-4), (-4,3,2), (2,5,-2), (-2,3,4), (4,5,-1),$ $(-1,5,4), (4,3,-2), (-2,5,2), (2,3,-4), (-4,5,1)$
44	2	$(1,6,-2), (-2,6,1)$
		$(-1,6,2), (2,6,-1)$
45	2	$(1,5,-5), (-5,5,1)$
		$(-1,5,5), (5,5,-1)$
48	2	$(1,6,-3), (-3,6,1)$
		$(-1,6,3), (3,6,-1)$
52	1	$(1,6,-4), (-4,2,3), (3,4,-3), (-3,2,4), (4,6,-1),$ $(-1,6,4), (4,2,-3), (-3,4,3), (3,2,-4), (-4,6,1)$
53	1	$(1,7,-1), (-1,7,1)$
56	2	$(1,6,-5), (-5,4,2), (2,4,-5), (-5,6,1)$
		$(-1,6,5), (5,4,-2), (-2,4,5), (5,6,-1)$
76	2	$(1,8,-3), (-3,4,5), (5,6,-2), (-2,6,5), (5,4,-3), (-3,8,1)$
		$(-1,8,3), (3,4,-5), (-5,6,2), (2,6,-5), (-5,4,3), (3,8,-1)$
134	4	$(1,10,-9), (-9,8,2), (2,8,-9), (-9,10,1)$
		$(-1,10,9), (9,8,-2), (-2,8,9), (9,10,-1)$
		$(3,8,-6), (-6,4,5), (5,6,-5), (-5,4,6), (6,8,-3), (-3,10,3)$
		$(-3,8,6), (6,4,-5), (-5,6,5), (5,4,-6), (-6,8,3), (3,10,-3)$
229	3	$(1,15,-1), (-1,15,1)$
		$(3,11,-9), (-9,7,5), (5,13,-3), (-3,11,9), (9,7,-5), (-5,13,3)$
		$(3,13,-5), (-5,7,9), (9,11,-3), (-3,13,5), (5,7,-9), (-9,11,3)$

Table 1.7. Cycles of Gauss-Reduced Forms with Discriminants $0 < \Delta \leq 56$.

Heath-Brown's Version. Heath-Brown works with three involutions. He starts by considering the finite set

$$S = \{(x,y,z) \in \mathbb{Z}^3 : 4xy + z^2 = p, x > 0, y > 0\},$$

on which he defines the involution

$$f : (x,y,z) \longmapsto (y, x - z).$$

This map f sends solutions in

$$T = \{(x,y,z) \in S : x > 0\}$$

to solutions in $S \setminus T$ and has no fixed points. Similarly, f maps the solutions in

$$U = \{(x,y,z) \in S : x - y + z > 0\}$$

to solutions in $S \setminus U$.

Thus f sets up bijections between T and $S \setminus T$, as well as between U and $S \setminus U$. This implies that these sets all have the same cardinality.

The second involution is defined on U by

$$g : (x,y,z) \longmapsto (x - y + z, y, 2y - z).$$

It has exactly one fixed point $(\frac{p-1}{4}, 1, 1)$, hence U must have odd cardinality.

Finally, the involution on T defined by

$$h : (x,y,z) \longmapsto (y,x,z)$$

must have a fixed point since T and U have odd cardinality. Thus there is a solution $(x,y,z) \in S$ with $x = y$, and this implies the claim.

Interpretation using Quadratic Forms. The first observation is that the points $(x,y,z) \in S$ correspond to binary quadratic forms $(A,B,C) = (-y,x,z)$ with discriminant p and $A < 0$, $B, C > 0$. The fixed point of the second involution is the form $(-y,x,y)$.

Frick [Fri1918] has shown that if $\Delta = a^2 + 4b^2$ is odd and a sum of two squares, then the form $Q = (b,a,-b)$ is Gauss reduced and is contained in the principal cycle, which always has even length since the signs of the first coefficient change in each reduction step. Zagier's proof is based on a slightly modified reduction map ζ with the property that the principle cycle has odd length.

Consider binary quadratic forms (A,B,C) with prime discriminant $\Delta = B^2 - 4AC = p$, where $p \equiv 1 \bmod 4$ is prime. Call such a form pre-reduced if $A < 0$, $B > 0$ and $C > 0$. Clearly there are only finitely many pre-reduced forms, and they satisfy $0 < B < \sqrt{p}$, $0 > A \ge -\frac{p-1}{4}$, and $0 < C < \frac{p-1}{4}$.

The following observation is trivial:

Lemma 1.41. *If (A,B,C) is pre-reduced, then so is $(-C,B,-A)$.*

Define a map ζ sending a pre-reduced form (A,B,C) to

$$\zeta(A,B,C) = \begin{cases} (A+B+C, B+2C, C) & \text{if } A+B+C < 0, \\ (-A-B-C, -B-2A, -A) & \text{if } A+B+C > 0,\ B+2A < 0, \\ (A, B+2A, A+B+C) & \text{if } A+B+C > 0,\ B+2A > 0. \end{cases}$$

Observe that $A+B+C = 0$ implies $\Delta = B^2 - 4AC = (A-C)^2$ is a square. Similarly, $B + 2A = 0$ implies $\Delta = 4A(A-C)$, which is impossible for discriminants $\Delta = 4m + 1$.

Lemma 1.42. *If Q is pre-reduced, then so is $\zeta(Q)$.*

Proof. Set $\zeta(A,B,C) = (A',B',C')$. There are three cases to consider.

1. $A+B+C<0$. Here $A' = A+B+C < 0$, $C' = C > 0$ and $B+2C > B > 0$.
2. $A+B+C>0$, $B+2A<0$. Then $A' = -A-B-C < 0$, $B' = -B-2A > 0$ and $C' = -A > 0$.
3. $A+B+C>0$, $B+2A>0$. Then $A' = A < 0$, $B' = B+2A > 0$ and $C' = A+B+C > 0$.

This completes the proof. □

Now we claim

Lemma 1.43. *We have $Q \sim \zeta(Q)$, where $\sim$ denotes equivalence with respect to the action of* $\mathrm{GL}_2(\mathbb{Z})$ *defined by (3.18Class Groups in the Strict and Wide Senseequation.3.6.18).*

Proof. Again we distinguish three cases:

- $A+B+C<0$: here $\zeta(Q) = Q|_S$ for $S = \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$.
- $A+B+C>0$, $B+2A<0$: here $S = \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$.
- $A+B+C>0$, $B+2A>0$: here $S = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$.

Note that $\det\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right) = -1$. □

Proposition 1.44. *Every primitive form with discriminant $\Delta \equiv 1 \bmod 4$ is* $\mathrm{GL}_2(\mathbb{Z})$*-equivalent to a pre-reduced form.*

Proof. Every primitive form is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to a Gauss-reduced form (A,B,C), which satisfies $B>0$ and $AC<0$. If (A,B,C) is not pre-reduced, then $(-C,B,-A)$ is; but ?? □

Lemma 1.45. *The map ζ is injective on the set of pre-reduced forms.*

Proof. □

The injectivity of ζ is an immediate consequence of the fact that ζ can be written as a composition of two involutions.

The cycle of pre-reduced forms with discriminant $\Delta = 41$ produced by ζ is given by

$$(-10,1,1),(-8,3,1),(-4,5,1),(-2,3,4),(-5,1,2),(-2,5,2),$$

$$(-2,1,5),(-4,3,2),(-1,5,4),(-1,3,8),(-1,1,10),(-10,1,1).$$

In the center of the anti-symmetric cycle there is the form $(-2,5,2)$. Forms $(A,B,-A)$ give a representation of p as a sum of two squares: $p = B^2 + 4A^2$.

Lemma 1.46. *If $\zeta(A,B,C) = (A',B',C')$, then $\zeta(-C',B',-A') = (-C,B,-A)$.*

Proof. We distinguish three cases.

- $A+B+C<0$: here $(A',B',C') = (A+B+C, B+2C, C)$, hence $(-C',B',-A') = (-C, B+2C, -A-B-C)$. Thus $-C'+B'-A' = -A > 0$ and $B'-2C' = B+4C > 0$, hence $\zeta(-C',B',-A') = (-C,B,-A)$ as claimed.
- $A+B+C>0$, $B+2A<0$:
- $A+B+C>0$, $B+2A>0$:

□

1.8.4 Gauss's Class Number Problem.

In this project we discuss Gauss's conjecture that there are no discriminants $\Delta < -163$ with class number 1. Here is a list of the fundamental discriminants with class number 1 and 2:

h	Δ
1	$-3, -4, -7, -8, -11, -19, -43, -67, -163$
2	$-15, -20, -24, -35, -40, -51, -52, -88, -91, -115,$
	$-123, -148, -187, -232, -235, -267, -403, -427$

In addition, the following non-fundamental discriminants have class number 1 or 2:

h	Δ
1	$-12, -16, -27$
2	$-28, -32, -36, -48, -64, -72, -75, -99, -100, -147$

The following claims are easy to prove:

1. Assume that $m \equiv 2, 3 \bmod 4$ is squarefree and $m < -2$, and let $\Delta = 4m$. Then $h(\Delta) > 1$.
   If $m \equiv 3 \bmod 4$, then $(1, 0, -m)$ and $(2, 2, \frac{1-m}{2})$ are distinct reduced forms with discriminant $4m$. If $m \equiv 2 \bmod 4$, consider $(1, 0, -m)$ and $(2, 0, -m/2)$.
2. If $\Delta = 1 - 4m$ and $h(\Delta) = 1$, then Δ is prime.
   If $p \mid \Delta$, then p is represented by some form, and since $h = 1$, by the principal form: $p = x^2 + xy + my^2$. Thus $4p = (2x + 1)^2 - \Delta y^2$, and $p \mid (2x + 1)$. Show that $2x + 1 = 0$ and deduce that $p = \Delta$.
3. If $\Delta = 1 - 4m < -3$ and $h(\Delta) = 1$, then m is prime.
   Again, p is represented by the principal form. Now use Legendre's Lemma.
4. If $\Delta = 1 - 8m < -7$, then $h(\Delta) > 1$.
   This is because the form $(2, 1, m)$ is reduced and not equivalent to the principal form.
5. If $\Delta = 1 - 4m$ and $h(\Delta) = 1$, then $(\frac{\Delta}{p}) = -1$ for all $p < m$.
   This is proved exactly as the preceding claim.
6. If $\Delta = 1 - 4m$ and $(\frac{\Delta}{p}) = -1$ for all $p < \sqrt{-\Delta/3}$, then $h(\Delta) = 1$.
   Let $Q = (A, B, C)$ be a reduced form with discriminant Δ. If $A > 1$, then there is a prime $p \mid A$. Show that $(\Delta/p) \neq -1$ and deduce that A cannot be reduced.

Collecting these results we find the following

Theorem 1.47. *Let $\Delta = 1-4m$ be squarefree and negative. Then the following statements are equivalent:*

1. $h(\Delta) = 1$;
2. $(\frac{\Delta}{p}) = -1$ *for all* $p < \sqrt{-\Delta/3}$;
3. $(\frac{\Delta}{p}) = -1$ *for all* $p < m$.

This result is connected with prime producing polynomials. Euler discovered in 1772 that the polynomial $f(x) = x^2 + x + 41$ attains only prime values for $x = 0, 1, 2, \ldots, 39$ (note that $f(40) = 40^2 + 40 + 41 = (40 + 1)^2$ is composite).

More generally, the polynomials $f(x) = x^2 + x + m$ for $m = 3, 5, 11, 17, 41$ yield prime values for all $x = 0, 1, \ldots, m - 2$. The discriminant of $x^2 - x + m$ is $1 - 4m$, which equals -11, -19, -43, -67 and -163 for the above values of m. This is of course no accident.

In fact, $f(x) = Q(x, 1)$ for the principal quadratic form $Q = (1, 1, m)$ with discriminant $\Delta = 1 - 4m$. What little we know about quadratic forms already allows us to explain the mathematics behind Euler's prime producing polynomial:

Theorem 1.48. *For fundamental discriminants $\Delta = 1 - 4m \leq -7$, the following statements are equivalent:*

1. $h(\Delta) = 1$;
2. $f(x) = x^2 + x + m$ *attains only prime values for* $x = 0, 1, \dots, m-2$.

Euler could not explain the mystery behind his prime producing polynomial x^2+x+41; this was accomplished by Rabinowitsch [Rab1913b], Remak and Frobenius [Fro1912]. See Sasaki [Sas1986] and Mollin [Mol1996] for more.

Frobenius proved the following results: ??? check ???

Proposition 1.49. *If* $\Delta = 1 - 4m$ *and* $h(\Delta) = 1$, *then every integer* $< m^2$ *represented by the principal form* Q_0 *with discriminant* Δ *is prime.*

If not, then this integer has a prime factor $q < m$, which also must be represented by Q_0; but this is impossible.

Proposition 1.50. *If* $\Delta = -8m$ *and* $h(\Delta) = 2$, *then every integer* $< (m+2)^2$ *represented by some form with discriminant* Δ *is prime.*

In fact, if the class number equals 2 then the only reduced forms with discriminant $-8m$ are $(1, 0, 2m)$ and $(2, 0, m)$, none of which can represent primes $< m + 2$.

Proposition 1.51. *If* $\Delta = m(m+4)$ *and* $h^+(\Delta) = 2$, *then every integer* $< (2m-1)^2$ *that is not divisible by* m *or* $m + 4$, *and is primitively represented by the form* $Q = (1, m, -m)$ *with discriminant* Δ, *is prime.*

This result requires more work since it deals with indefinite forms.

Here is another curious fact, first observed by Hermite [Her1859, p. 61] and Kronecker:

Δ	$\exp(\pi\sqrt{-\Delta})$
-43	$884736743.99977746603490666\dots$
-67	$147197952743.99999866245422450\dots$
-163	$262537412640768743.99999999999925007\dots$

As you can see, the values of $e^{\pi\sqrt{-\Delta}}$ are very close to an integer for these values of Δ. This phenomenon becomes much more visible if we subtract 744 and take the cube root:

Δ	$(\exp(\pi\sqrt{-\Delta}) - 744)^{1/3}$
-11	$31.99809333222744098975227354\dots$
-19	$95.99999195891694508468060476\dots$
-43	$959.99999999991951173137537734\dots$
-67	$5279.99999999999998400738235224\dots$
-163	$640319.99999999999999999999999939\dots$

What is even more amazing is the fact that the integer x approximated by $\sqrt[3]{e^{\pi\sqrt{-\Delta}} - 744}$ satisfies the diophantine equation $x^3 + 1728 = -\Delta y^2$ for some $y \in \mathbb{N}$. Look and see:

$$
\begin{aligned}
11 \cdot 56^2 &= 32^3 + 1728 \\
19 \cdot 216^2 &= 96^3 + 1728 \\
43 \cdot 4536^2 &= 960^3 + 1728 \\
67 \cdot 4\,6872^2 &= 5280^3 + 1728 \\
163 \cdot 401\,33016^2 &= 640320^3 + 1728
\end{aligned}
$$

Explaining these facts requires more advanced techniques (modular forms, elliptic curves, complex multiplication, class field theory, ...); these are in fact exactly the techniques one needs to prove Gauss's conjecture (see Borel et al. [BC1957] and Cox [Co1989]).

Already Gauss conjectured that for every integer $n \ge 1$, there are only finitely many discriminants $\Delta < 0$ with $h(\Delta) = n$. In this form, the conjecture was proved by Heilbronn and Siegel in the 1930s. The enumeration of all discriminants with given class number turned out to be much more difficult and was solved for $h = 1$ independently by Heegner (1952), Baker (1966) and Stark (1967). Using the theory of elliptic curves, Goldfeld(1976) and Gross & Zagier (1986) introduced techniques that, in principle, allowed to enumerate all discriminants with given class number. This has now been done for all class numbers ≤ 100.

1.8.5 Negative Continued Fractions

The reduction theory of indefinite binary quadratic forms is closely related to the theory of continued fractions. Here, we will briefly sketch the continued fractions associated to Zagier reduction.

Let n_0, n_1, n_2, ... be integers with $n_i \ge 2$ for $i \ge 1$. Consider the continued fraction

$$[n_0, n_1, \ldots, n_s] = n_0 - \cfrac{1}{n_1 - \cfrac{1}{n_2 - \cfrac{1}{\ddots - \frac{1}{n_s}}}}.$$

The limit $[n_0, n_1, \ldots] = \lim_{s\to\infty}[n_0, n_1, \ldots, n_s]$ always exists and so denotes some real number. Conversely, given any real number α we set $n_0 = \lfloor \alpha \rfloor + 1$ and $\alpha_1 = \frac{1}{n_0-\alpha}$, and define $n_i = \lfloor \alpha_i \rfloor + 1$ and $\alpha_{i+1} = 1/(n_i - \alpha_i)$.

Lemma 1.52. *The continued fractions introduced above have the following properties:*

1. *Every real number α can be written as a continued fraction: $\alpha = [n_0, n_1, \ldots]$.*
2. *We have $\alpha \in \mathbb{Q}$ if and only if there is an integer N such that $n_i = 2$ for all $i \ge N$.*
3. *The number α is a quadratic irrational if and only if the n_i become periodic (that is, there are integers N and r such that $n_{i+r} = n_i$ for all $i \ge N$) and $n_j > 2$ for some index j.*

We denote such a periodic continued fraction by $[n_0, n_1, \ldots, n_q, \overline{n_{q+1}, \ldots, n_{q+r}}]$.

α	continued fraction
$\sqrt{2}$	$[2, \overline{2, 4}]$
$\sqrt{3}$	$[2, \overline{4}]$
$\sqrt{5}$	$[3, \overline{2, 2, 2, 6}]$
$\sqrt{6}$	$[3, \overline{2, 6}]$
$\sqrt{7}$	$[3, \overline{3, 6}]$
$\sqrt{10}$	$[4, \overline{2, 2, 2, 2, 2, 8}]$

α	continued fraction
$\frac{1+\sqrt{5}}{2}$	$[2, \overline{3}]$
$\frac{1+\sqrt{13}}{2}$	$[3, \overline{2, 2, 5}]$
$\frac{1+\sqrt{17}}{2}$	$[3, \overline{3, 2, 2, 3, 5}]$
$\frac{1+\sqrt{21}}{2}$	$[3, \overline{5}]$
$\frac{1+\sqrt{29}}{2}$	$[4, \overline{2, 2, 2, 2, 7}]$
$\frac{1+\sqrt{33}}{2}$	$[4, \overline{2, 3, 2, 7}]$

Here are a few observations on the continued fraction expansions of $\sqrt{m}$:

- We have $\sqrt{m} = [n_0, \overline{n_1, n_2, \ldots, n_r}]$ with $n_2 = 2n_0$.
- We have $n_1 = n_{r-1}$, $n_2 = n_{r-2}$, ...;
- The continued fraction expansion of $\sqrt{m}$ has period length 1 if and only if $m = n^2 - 1$.
- The continued fraction expansion of $\frac{1}{2}(1 + \sqrt{m})$ has period length 1 if and only if $m = (2n + 1)^2 - 4$.

There are also examples of purely periodic continued fractions such as $2 + \sqrt{2} = [\overline{4, 2}]$, $\frac{3+\sqrt{5}}{2} = [\overline{3}]$, and $\frac{5+\sqrt{13}}{2} = [\overline{5, 2, 2}]$. Periodic continued fractions are connected intimately with reduced quadratic forms:

Proposition 1.53. *Let α be a quadratic irrational. Then the continued fraction expansion of α is purely periodic if and only if α is the larger root of a quadratic polynomial $Ax^2 - Bx + C = 0$ such that the quadratic form (A, B, C) is Zagier reduced.*

More precisely, let $Q_1 = (A_1, B_1, C_1)$ be a Zagier reduced quadratic form and let $Q_j = (A_j, B_j, C_j)$ $(1 \le j \le n)$ denote the reduced forms in the cycle generated by Q_1. If we set $S(n_i) = \left(\begin{smallmatrix} n_i & 1 \\ -1 & 0 \end{smallmatrix}\right)$, then $Q_i|_{S(n_i)} = Q_{i+1}$. Thus Zagier reduction is essentially the computation of some continued fraction expansion.

As an example, consider the form $(1, 1, -8)$. The associated quadratic polynomial is $x^2 - x - 8$, and its larger root is $\frac{1+\sqrt{33}}{2}$. The continued fraction expansion in the table above then corresponds exactly to the reduction presented in Fig. 1.1Zagier Reduction of $(1, 1, -8)$figure.1.1.

By breaking off the periodic continued fraction expansion of a quadratic irrationality α at some point, we get reational approximations P_i/Q_i to α. In fact: we have $r_i := [n_0, n_1, \ldots, n_i] = P_i/Q_i$ for integers P_i, Q_i defined recursively as follows:

$$\begin{aligned} P_{-2} &= 0 & P_{-1} &= 1 & P_i &= n_i P_{i-1} - P_{i-2} \\ Q_{-2} &= -1 & Q_{-1} &= 0 & Q_i &= n_i Q_{i-1} - Q_{i-2} \end{aligned}$$

The recursion can be written in matrix form

$$\begin{pmatrix} P_r & Q_r \\ P_{r-1} & Q_{r-1} \end{pmatrix} = \begin{pmatrix} n_r & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} n_0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

which shows that $P_r Q_{r-1} - P_{r-1} Q_r = -1$. Dividing through by $Q_r Q_{r-1}$ we find

$$\frac{P_{r-1}}{Q_{r-1}} - \frac{P_r}{Q_r} = \frac{1}{Q_r Q_{r-1}},$$

hence the sequence P_n/Q_n is monotonically decreasing.

In the case of $\alpha = \sqrt{m}$, the fact that $\sqrt{m} - P_n/Q_n$ is small means that $P_n + Q_n\sqrt{m}$ has a small norm $P_n^2 - mQ_n^2 = R_n$; for $m = 7$, we find

n	r_n	P_n	Q_n	R_n
0	$[3]$	3	1	2
1	$[3, 3]$	8	3	1
2	$[3, 3, 6]$	45	17	2
3	$[3, 3, 6, 3]$	127	48	1

Note that $[3, 3, 6] = 3 - \frac{1}{3 - \frac{1}{6}} = \frac{45}{17}$.

For $m = 31$, we find the continued fraction expansion $\sqrt{31} = [6, \overline{3, 2, 2, 7, 2, 2, 3, 12}\,]$ and the approximations

	P_n	Q_n	R_n
$[6]$	6	1	5
$[6, 3]$	17	3	10
$[6, 3, 2]$	28	5	9
$[6, 3, 2, 2]$	39	7	2

The cycle generated by the principal form $(1, 0, -31)$ is $(1, 12, 5)$, $(10, 18, 5)$, $(9, 22, 10)$, $(2, 14, 9)$, $(9, 14, 2)$, $(10, 22, 9)$, $(5, 18, 10)$. Compare the first coefficients of these forms with the values of R_n, formulate a conjecture, and prove it.

The following result is the analog of the claim that every positive definite form with discriminant Δ is equivalent to a form with first coefficient $\le \sqrt{-\Delta/3}$:

Proposition 1.54. *Let Q be a primitive form with nonsquare discriminant $\Delta > 0$. Then there is a form (A, B, C) equivalent to Q with $|A| \le \sqrt{\Delta/5}$.*

Exercises

1.1 Show that $\mathrm{SL}_2(\mathbb{Z})$ is a group.

1.2 Let G be a group and X a set. We say that G acts on X (from the left) if there is a map $G \times X \longrightarrow X$ sending (g, x) to $g.x$ with the properties
1. $1.x = x$ for all $x \in X$;
2. $g.(h.x) = (gh).x$ for all $g, h \in G$ and all $x \in X$.

Define a relation on X by setting $x' \sim x$ for $x, x' \in X$ if there is a $g \in G$ such that $x' = gx$. Show that this is an equivalence relation, i.e., that it is
- reflexive: $x \sim x$.
- symmetric: $x \sim x'$ implies $x' \sim x$.
- transitive: $x \sim x'$ and $x' \sim x''$ imply $x \sim x''$.

1.3 Assume that a group G acts from the left on a set X. Show that G also acts from the right via $x.g := g^{-1}.x$, i.e., show that $x.1 = x$ and $(x.g).h = x.(gh)$.

1.4 A matrix $M \in \mathrm{PSL}_2(\mathbb{Z})$ is symmetric if and only if $M^{-1} = J^{-1}MJ$, where $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

1.5 For a binary quadratic form $Q = Ax^2 + Bxy + Cy^2$, its Hessian is defined as $\mathrm{Hess}(Q) = \left(\begin{smallmatrix} Q_{xx} & Q_{xy} \\ Q_{yx} & Q_{yy} \end{smallmatrix}\right)$, whose entries are partial derivatives of Q. Show that $\mathrm{Hess}(Q) = M(Q)$.

1.6 Let $Q = (A, B, C)$ and $Q' = (A', B', C')$ primitive quadratic forms, and assume that $Q' = Q|_S$ for $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Show that $A' = Q(r, t)$, $C' = Q(s, u)$, and $B' = Q(r, t) + Q(s, u) - Q(r - s, t - u)$.

1.7 Show that the table for reducing the form $(103, 64, 10)$ is given by

$$\begin{array}{cccc} & -3 & -2 & \\ 103 & 32 & 7 & \\ 32 & 10 & 2 & \\ 7 & 2 & 1 & 0 \\ & 6 & 0 & 6 \end{array} .$$

1.8 Let $Q = (1, 0, -m)$ and $Q' = (-1, 0, m)$ be forms of discriminant $\Delta = 4m$. Show that $Q' = Q|_S$ for some $S \in \mathrm{SL}_2(\mathbb{Z})$ if and only if the equation $T^2 - mU^2 = -1$ has a solution in natural numbers. Also show that, in this case, $S = \left(\begin{smallmatrix} T & -mU \\ U & -T \end{smallmatrix}\right)$ has the desired properties. (Hint: use (1.2The Action of the Modular Groupequation.1.1.2).)

1.9 Let $Q = (1, 1, -m)$ and $Q' = (-1, 1, m)$ be forms with discriminant $\Delta = 4m + 1$ (note that $(-1, 1, m) \sim (-1, -1, m)$ via a simple shift). Show that $Q' = Q|_S$ for some $S \in \mathrm{SL}_2(\mathbb{Z})$ if and only if the equation $T^2 + TU - mU^2 = -1$ has a solution in natural numbers. Also show that, in this case, $S = \left(\begin{smallmatrix} T & -mU \\ U & -T-U \end{smallmatrix}\right)$ has the desired properties.

1.10 Use the preceding two exercises and Table 1.1Lagrange-reduced Forms with Small Discriminanttable.1.1 to verify the following table of class numbers $h^+(\Delta)$:

Δ	5	8	12	13	17	20	21	24
$h^+(\Delta)$	1	1	2	1	1	1	2	2

1.11 Show that there are at most two reduced forms of given discriminant $\Delta < 0$ that represent a prime p.
Hints: Let Q and Q' be forms with discriminant Δ representing p, and write $Q = (p, B, C)$ and $Q' = (p, B', C')$; choose $-p < B, B' \le p$. From $\operatorname{disc} Q = \operatorname{disc} Q'$ deduce that $B^2 - B'^2 = 4p(C - C')$, and conclude that $B = \pm B'$ and $C = C'$. This implies $Q = Q'$ or $Q' = (p, -B, C)$.

1.12 (Plesken [Ple1982]) Let $\mathrm{Sym}_2(K)$ denote the subspace of symmetric 2×2-matrices with coefficients in a field K; show that the map

$$\phi : \mathrm{Sym}_2(K) \longrightarrow K^3; \qquad \begin{pmatrix} a & b \\ b & c \end{pmatrix} \longmapsto \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

is an isomorphism of K-vector spaces.
The determinant of $S = \left(\begin{smallmatrix} x & y \\ y & z \end{smallmatrix}\right) \in \mathrm{Sym}_2(K)$ is the ternary quadratic form $\det(x, y, z) = xz - y^2$.

The automorphism group $\mathrm{Aut}(Q)$ of an n-ary quadratic form Q is the group of all $g \in GL_2(K)$ with $g' A_Q g = A_Q$, where A_Q is the symmetric $n \times n$-matrix attached to Q.
Show that the map $\overline{\delta} : \mathrm{PSL}_2(K) \longrightarrow \mathrm{Aut}(\det, \mathrm{Sym}_2(K))$ sending $g \in \mathrm{PSL}_2(K)$ to the map $\overline{\delta}(g) : X \longmapsto g' X g$ is a group homomorphism. Let δ denote the map which makes the following diagram commutative:

$$\begin{array}{ccc} \mathrm{Sym}_2(K) & \xrightarrow{\overline{\delta}} & \mathrm{Sym}_2(K) \\ {\scriptstyle \phi}\downarrow & & {\scriptstyle \phi}\downarrow \\ K^3 & \xrightarrow[\delta]{} & K^3 \end{array}$$

Show that δ sends the matrix $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(K)$ to $\begin{pmatrix} r^2 & rt & t^2 \\ 2rs & ru+st & 2tu \\ s^2 & su & u^2 \end{pmatrix}$.

1.13 Show that, for any $M = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in M_2(\mathbb{Z})$, the 3×3-matrix $\mathcal{M}$ in (1.3The Action of the Modular Groupequation.1.1.3) has determinant $(\det M)^3$, and that the map sending M to $\mathcal{M}^{-1}$ induces an injective group homomorphism $\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_3(\mathbb{Z})$.
Hints.
1. Consider the vector space $M_2(K)$ of 2×2-matrices with entries from a field K. For an invertible matrix $M \in \mathrm{GL}_2(K)$, consider the endomorphism L of $M_2(K)$ defined by $L(A) = MA$ for $A \in M_2(K)$. By looking at the transformation of the canonical basis, show that L has determinant $\det(L) = (\det M)^2$. Deduce that the endomorphism L_2 defined by $L_2(A) = M'AM$ has determinant $\det(L) = (\det M)^4$.
2. Let $\mathrm{Sym}_2(K)$ denote the subspace of symmetric matrices in $M_2(K)$. Show that the map λ sending $S \in \mathrm{Sym}_2(K)$ to $M'SM$ for a fixed $M \in \mathrm{GL}_2(K)$ is an endomorphism of $\mathrm{Sym}_2(K)$, and that $M_2(K) = \mathrm{Sym}_2(K) \oplus \mathrm{Sym}_2^-(K)$, where $\mathrm{Sym}_2^-(K)$ is the subspace of antisymmetric matrices (these are matrices satisfying $A' = -A$).
3. If U_1, U_2 are subspaces of a K-vector space V, and if they both are invariant under the action of an endomorphism L of V, then $\det L$ is the product of the determinants of the restrictions of L to U_1 and U_2.
4. Show that the restriction of L_2 to Sym_2^- has determinant $\det M$.
5. Finally show that if $M \longmapsto \mathcal{M}^{-1}$ and $N \longmapsto \mathcal{N}^{-1}$ for two matrices $M, N \in \mathrm{SL}_2(\mathbb{Z})$, then $MN \longmapsto (\mathcal{N}\mathcal{M})^{-1} = \mathcal{M}^{-1}\mathcal{N}^{-1}$.

1.14 Show that the map sending a pair of matrices A and B to the element $\mathrm{Tr}\,(AB)$ induces a pairing $T : M_2(\mathbb{Q}) \times M_2(\mathbb{Q}) \longrightarrow K$, and that $\mathrm{Sym}_2(\mathbb{Z})$ is the dual of $\mathrm{Sym}_2(\mathbb{Z})^*$ with respect to this pairing; here $\mathrm{Sym}_2(\mathbb{Z})^*$ is the set of all matrices of the form $\left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ with $a, b, c \in \mathbb{Z}$.

1.15 Consider the form $Q(x, y) = x^2 + y^2$ with discriminant $\Delta = -4$, and the matrix $S = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Show that $Q|_S(x, y) = 5x^2 + 6xy + 2y^2$.

1.16 Show that the forms $(0, 1, 0)$ and $(1, 1, 0)$ with discriminant 1 are equivalent.

1.17 Let Q be a form that represents 0 primitively. Show that its discriminant is a square.

1.18 Determine all positive definite quadratic forms Q with the property that the smallest integers represented by Q are 2, 3, and 5.

1.19 Determine the class number $h(-103)$.

1.20 Compute $h(-107)$.

1.21 Compute $h(-420)$.

1.22 Reduce the form $(101, 20, 1)$.

1.23 Reduce the form $(3, 4, 3)$.

1.24 Reduce the forms $(5, 16, 21)$ and $(7, 16, 15)$.

1.25 For a matrix $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, the group of all matrices with integer entries and determinant ± 1, define a form $Q' = Q|_S$ by

$$Q'(x, y) = Q(rx + sy, tx + uy). \qquad (1.35)$$

Show that this defines an action of $\mathrm{GL}_2(\mathbb{Z})$ on the set of primitive quadratic forms with discriminant Δ. Show also that if Q is positive definite, then so is $Q|_S$.

1.26 There are a number of very good reasons for defining the action of $\mathrm{GL}_2(\mathbb{Z})$ not as above, but by the formula

$$Q'(x,y) = \frac{1}{\det S}\, Q(rx+sy, tx+uy). \tag{1.36}$$

Since $\det S = \pm 1$, we could actually write $\det S$ instead of $\frac{1}{\det S}$, but in more general situations the formula (1.36Exercisesequation.1.8.36) turns out to be the correct one.
Show that (1.36Exercisesequation.1.8.36) also defines an action of $\mathrm{GL}_2(\mathbb{Z})$ on the set of primitive quadratic forms with discriminant Δ. Also show that the set of positive definite form is not invariant under this action of $\mathrm{GL}_2(\mathbb{Z})$.

1.27 Show that the number of equivalence classes of positive definite primitive forms with discriminant Δ with respect to $\mathrm{SL}_2(\mathbb{Z})$ is equal to the number of equivalence classes of all primitive forms with discriminant Δ with respect to the action of $\mathrm{GL}_2(\mathbb{Z})$ defined by (1.36Exercisesequation.1.8.36).

1.28 Let $\mathrm{Aut}(Q) = \{S \in \mathrm{GL}_2(\mathbb{Z}) : Q|_S = Q\}$, where the action of $\mathrm{GL}_2(\mathbb{Z})$ is defined by (1.36Exercisesequation.1.8.36). Show that $\mathrm{Aut}(Q)$ is a group containing $\mathrm{Aut}^+(Q)$ as a subgroup.
Prove the following analog of Thm. 1.25lemmacount.1.25: There is a bijection between the elements of $\mathrm{Aut}(Q)$ and solutions of the equations $Q_0(T,U) = \pm 1$

1.29 Let F be a field with characteristic $\ne 2$, and V a finite dimensional F-vector space. A pair (V,ϕ), where ϕ is a symmetric bilinear form $V \longrightarrow F$ is called a quadratic space. A quadratic space determines a *quadratic form* $q : V \longrightarrow F$ via $q(x) = \phi(x,x)$.
1. Show that $q(\lambda x) = \lambda^2 q(x)$.
2. Show that q determines ϕ via $\phi(x,y) = \frac14(q(x+y) - q(x-y))$.

1.30 Define a bilinear form $\langle \cdot,\cdot \rangle$ on the space $\mathcal{F}$ of binary quadratic forms with rational coefficients by setting

$$\langle Q, Q' \rangle = BB' - 2(AC' + A'C),$$

where $Q = (A,B,C)$ and $Q' = (A',B',C')$. Show that this gives $\mathcal{F}$ the structure of a quadratic space, and that $\langle Q, Q\rangle = \operatorname{disc} Q$.

1.31 (continued) Let $Q_1, Q_2 \in \mathcal{F}$ be binary quadratic forms. For $S \in \mathrm{SL}_2(\mathbb{Q})$, let $T = S'$ denote the transpose of S. Show that

$$\langle Q_1|_S, Q_2 \rangle = \langle Q_1, Q_2|_T \rangle. \tag{1.37}$$

1.32 (continued) Assume that the form $Q_1 = (1,0,-a)$ represents b, say $r^2 - as^2 = b$. Then $Q_2 = (as, 2r, s)$ is a form with discriminant $4b$.
Now consider the case $b = -1$; then $Q_2 = (as, 2r, s)$ has discriminant 4, hence is equivalent to $(1,0,1)$, say $Q_2 = (1,0,1)|_S$ for some $S \in \mathrm{SL}_2(\mathbb{Z})$. Use (1.37Exercisesequation.1.8.37) to deduce that $Q_2|_T = (A, 2B, -A)$ with $a = A^2 + B^2$.

1.33 Let $Q(x,y) = Ax^2 - Bxy + Cy^2$ denote a positive definite quadratic form with $B > 0$. Pove the identities

$$\begin{aligned} Q(x-1,y) &= Q(x,y) - A(x-y) - y(A-B) - A(x-1), \\ Q(x,y-1) &= Q(x,y) - C(y-x) - x(C-B) - C(y-1). \end{aligned}$$

Use this to prove the following extension of Legendre's Lemma 1.12Legendre's Lemmalemmacount.1.12: The minimal integers represented by Q are $A = Q(1,0)$, $C = Q(0,1)$, $A - B + C = Q(1,1)$, $A + B + C = Q(1,-1)$, $4A - 2B + C = Q(2,1)$, $\min(Q(2,-1), Q(1,2))$ and $\max(Q(2,-1), Q(1,2))$.

1.34 Let $\Delta = 4m+1$. Show that $(m, 2m+1, m)$ is a Zagier-reduced form with discriminant Δ.

1.35 Let $\Delta = 4m$ with $m \equiv 3 \bmod 4$. Show that $Q = (m, 2m, m-1)$ is a Zagier-reduced form with discriminant Δ, and that $[Q]$ has order 2 in $\mathrm{Cl}^+(\Delta)$.

1.36 Assume that $\Delta = (2n+1)^2 - 4$. Show that the cycle of the principal form Q_0 with discriminant Δ consists of a single form. Deduce that $h^+ = 1$ for such Δ if and only if $n = 1$.

1.37 Let $Q_0 = (1,0,m)$ be the principal form with discriminant $\Delta = 4m$ ($m > 0$). Show that $\rho_Z(Q_0) = (A, B, 1)$ with $B \equiv A \equiv 0 \bmod 2$ and $0 \le A \le B - 2$. In particular, $\rho_Z(Q_0)$ is Z-reduced.

1.38 Show that $A' = A\theta^2 + \sqrt{\Delta}\theta$, where $n = \frac{B+\sqrt{\Delta}}{2A} + \theta$ and $A' = An^2 - Bn + C$ (see Lemma 1.17lemmacount.1.17).

1.39 Show that $\sqrt{\Delta}(1-\theta) - A(1-\theta)^2 = B' - A' - C'$ in the proof of Lemma 1.17lemmacount.1.17.

1.40 Assume that (A, B, C) is Zagier reduced. Show that $\frac{B}{A} > \frac{B+\sqrt{\Delta}}{2A} > \frac{B}{A} - 1$. Deduce that $\rho_Z(Q) = Q|_S$ for $S = \left(\begin{smallmatrix} n & 1 \\ -1 & 0 \end{smallmatrix}\right)$, where $n = \lceil \frac{B}{A} \rceil$.

1.41 Show that the right Zagier neighbors of $(-1, -5, -1)$ are $(3, 3, -1)$ and $(5, 9, 3)$.

1.42 Show that if you run through the same cycle, but starting with two different forms, then you get the same unit.

1.43 Show that if a cycle produces the unit ε, then running through the same cycle n times produces the unit ε^n.

1.44 Develop a reduction theory for forms if a reduced form is defined by the following conditions:

$$\begin{cases} \sqrt{\Delta} - |A| < B < \sqrt{\Delta} + |A|, \\ \sqrt{\Delta} - |C| < B < \sqrt{\Delta} + |C|. \end{cases} \tag{1.38}$$

1.45 Show that if (A, B, C) is a Zagier reduced form with discriminant $\Delta \equiv 5 \bmod 8$, then A, B and C are odd.

1.46 A Zagier-reduced form is called palindromic if it has the form (A, B, A). Show that the palindromic Zagier-reduced forms (A, B, A) with odd discriminant Δ correspond to certain factorizations of Δ. In particular, $(m, 2m+1, m)$ is the only palindromic Zagier-reduced form with prime discriminant $\Delta = 4m + 1$.
Deduce that the caliber $\kappa_Z(\Delta)$ with discriminant $\Delta = 4m + 1$ is odd if and only if Δ is prime.
Show similarly that $\kappa_Z(\Delta)$ is even if $\Delta = 4p$ for some prime $p \equiv 3 \bmod 4$.

1.47 Assume that $\Delta = 4m + 1$ is a positive fundamental discriminant. Show that the forms

$$\begin{aligned}
Q_0 &= (m, 2m+1, m), \\
Q_1^+ &= (m, 2m-1, m-2) \\
Q_1^- &= (m-2, 2m-1, m), \\
&\dots \\
Q_k^+ &= (m - 2(k^2 - k), 2m - 2k^2 + 1, m - 2(k^2 + k)), \\
Q_k^- &= (m - 2(k^2 + k), 2m - 2k^2 + 1, m - 2(k^2 - k)), \dots
\end{aligned}$$

have discriminant Δ, and are Zagier reduced for all $0 \le k \le \frac{1}{2}(\sqrt{2m+1} - 1)$.

1.48 (continued) Show more exactly that

$$\kappa_Z(\Delta) \ge \begin{cases} n & \text{if } \Delta = n^2 + 4, \\ n+1 & \text{if } \Delta = n^2 + 1, \end{cases}$$

with equality if Δ is prime.

1.49 Let $p \equiv 1 \bmod 4$ be a prime, and write $p = a^2 + 4b^2$ for integers a, b. Show that $(a, 4b, -a)$ is a form with discriminant $\Delta = 4p$, and that $(b, a, -b)$ has discriminant p. Which forms are equivalent to Q_0?

1.50 (Frick [Fri1918]) Assume that $\Delta = a^2 + 4b^2$ is odd and a sum of two squares. Show that the form $Q = (b, a, -b)$ is Gauss reduced. Show that the principal cycle always contains a form of this type, and devise an algorithm to write primes $p \equiv 1 \bmod 4$ as a sum of two squares.

1.51 Assume that $\Delta = a^2 + 4b^2$ is odd and a sum of two squares. Show that the form $Q = (b, a + 2b, a)$ is Zagier reduced. Show that the principal cycle always contains a form of this type, and devise an algorithm to write primes $p \equiv 1 \bmod 4$ as a sum of two squares.

1.52 Assume that $p = c^2 + 2d^2 \equiv 3 \bmod 8$. Show that the forms $Q = (d, 2c, -2d)$ and $Q' = (d, 2c + 2d, 2c - d)$ are primitive with discriminant $\Delta = 4p$. Show that either Q or Q' is Gauss reduced. Devise an algorithm to represent primes $p \equiv 3 \bmod 8$ by the form $x^2 + 2y^2$.

1.53 (Yamamoto [Yam1971]) Consider the family of discriminants $\Delta_n = (2^n + 3)^2 - 8$. Show that $\varepsilon = (\alpha - 1)\alpha^n/2^n$ is a unit in $\mathbb{Q}(\sqrt{\Delta})$, where $\alpha = 2^{n-1} + 1 + \omega$.

1.54 (Chebyshev [Che1851]) Assume that $\Delta = 4m$, let (T, U) be a fundamental solution of the Pell equation $Q_0(T, U) = 1$, and let $N > 0$ be an integer. If the equation $Q_0(x, y) = x^2 - my^2 = N$ has an integral solution, then there is one satisfying

$$0 < x \le \sqrt{\frac{T+1}{2}N}, \qquad 0 < y \le \sqrt{\frac{T+1}{2m}N}.$$

Hints. Assume that $x^2 - my^2 = N$ for integers $x, y \ge 0$; show that $(xT - yUm)^2 - m(xU - yT)^2 = N$. Show that $0 \le x' < x$ for $x' = xT - yUm$ unless $x \le \sqrt{(T + 1)N/2}$ and $y \le \sqrt{\frac{T+1}{2m}N}$.
Derive similar bounds for negative N, and for discriminants $\Delta = 4m + 1$.

1.55 Show that the equations $x^2 - 79y^2 = \pm 3$ do not have integral solutions.

1.56 Euler discovered connections between higher reciprocity and binary quadratic forms; the following proofs are modeled after ideas due to Dirichlet.
Let $p \equiv 1 \bmod 8$ be prime.
1. Show that $p = a^2 + 4b^2 = c^2 + 8d^2$ for positive integers a, b, c, d.
2.
3.

1.57 Here is the corresponding problem for the congruence $x^4 \equiv -3 \bmod p$. Let $p \equiv 1 \bmod 12$ be prime.
1. Show that $p = a^2 + 4b^2 = c^2 + 3d^2$ for positive integers a, b, c, d.
2. Show that $(-3)^{(p-1)/4} \equiv (-1)^{(c-1)/2}(\frac{2}{p})(\frac{c}{3}) \bmod p$.
3. Show that either a or b is divisible by 3.
4. Write $(c - 2b)(c + 2b) = a^2 - 3d^2$.
If $3 \mid b$, show that $3 \nmid (c + 2b)$ and check that $(\frac{c+2b}{3}) = (-1)^{(c-1)/2}(\frac{2}{p})$; deduce that $(-3/p)_4 = +1$.
If $3 \mid a$, show that $3 \nmid c$ and check that $-(\frac{c}{3}) = (\frac{c\pm 2b}{3}) = (-1)^{(c-1)/2}(\frac{2}{p})$; deduce that $(-3/p)_4 = -1$.
5. Show that $(1, 0, 36)$ represents p if and only if $(-3/p)_4 = +1$, and that $(4, 0, 9)$ represents p if and only if $(-3/p)_4 = -1$.

1.58 Recall that the Dirichlet composition of $Q_1 = (A, B, A'C)$ and $Q_2 = (A', B, AC')$ is $Q_3 = (AA', B, C)$. Identify the neutral element with the class of $Q_0 = (1, B, AC)$ (which is equivalent to the principal form), and send each of these forms Q_j to the corresponding point $z_j = z(Q_j)$ in the upper half plane. Then check the identity

$$z_1 z_2 = z_3 z_0.$$

From this point of view, composition is just multiplication of certain complex numbers. For a closer investigation of how composition relates points on the modular curve, see Penner [Pen1996].

1.59 The equations on p. 43Gauss's Class Number Problemlemmacount.1.51 are divisible by $2^6 \cdot 3^3 = 1728$ for all $|\Delta| \ge 19$; show that this implies

$$1^2 - 27 \cdot 19 \cdot 1^2 = -8^3$$
$$1^2 - 27 \cdot 43 \cdot 21^2 = -80^3$$
$$1^2 - 27 \cdot 67 \cdot 217^2 = -440^3$$
$$1^2 - 27 \cdot 163 \cdot 185801^2 = -53360^3$$

Relations of the form $X^2 - 27\Delta Y^2 = Z^3$ can be used to define forms with discriminant -3Δ.

The fundamental units for discriminants -3Δ seem to grow similarly as the solutions above:

-3Δ	ε
$-3\cdot 11$	$23+4\sqrt{33}$
$-3\cdot 19$	$151+20\sqrt{57}$
$-3\cdot 43$	$16855+1484\sqrt{129}$
$-3\cdot 67$	$515095+35332\sqrt{201}$
$-3\cdot 163$	$7592629975+343350596\sqrt{489}$

For $\Delta\le -19$, write $\varepsilon = T+U\sqrt{-3\Delta}$. Here are the factorizations of $T+1$ and y:

Δ	$T+1$	y
-19	$2^3\cdot 19$	$2^3\cdot 3^3$
-43	$2^3\cdot 7^2\cdot 43$	$2^3\cdot 3^4\cdot 7$
-67	$2^3\cdot 31^2\cdot 67$	$2^3\cdot 3^3\cdot 7\cdot 31$
-163	$2^3\cdot 19^2\cdot 127^2\cdot 163$	$2^3\cdot 3^3\cdot 7\cdot 11\cdot 19\cdot 127$

Let $p\equiv 19 \bmod 24$ be prime, and let $\varepsilon = t+u\sqrt{3p}$ denote the fundamental unit of $\mathbb{Q}(\sqrt{3p}\,)$. Then $t+1=8pa^2$ for some integer a (this is easy to prove), and $a\mid y$ for the solution of $x^3+1728=-\Delta y^2$ provided by the exponential function (this is a mystery).

3. Bhargava's Cubes

Bhargava recently found a clever way of explaining Gauss composition on quadratic forms using certain cubes of integers. In this chapter we will see how to construct quadratic forms from these cubes, and conversely, how to find a suitable integer cube from a given pair of quadratic forms with the same discriminant. We will then use these results to define a group structure on the set of equivalence classes of primitive quadratic forms with given discriminant.

3.1. From Cubes to Forms

Where we will learn how to attach a triple of quadratic forms of the same discriminant to a cube, and watch minors develop a relation.

After having introduced the technique of reduction of binary quadratic forms, our next major goal is the definition of a group structure on the set of equivalence classes of primitive quadratic forms with nonzero discriminants Δ. It was Gauss who first succeeded in giving such a group structure, but his proofs were technical and unmotivated. Later writers gave simpler approaches[1], but actually all of them are more or less equivalent. Gauss and Dedekind used 2×4-matrices, Cayley $2 \times 2 \times 2$-hypermatrices, and Bhargava used cubes. Below, we will follow Bhargava's ideas, and give the connections with the more classical approaches in the historical part.

For each octuple $(a, b, \ldots, h)$ of integers $a, b, \ldots, h$ we define a cube

$$\mathcal{A} = \begin{array}{ccccccc} & & e & & \text{---} & & f \\ & & | & & & & | \\ a & \text{---} & & & b & & | \\ | & & | & & | & & | \\ | & & g & \text{---} & | & \text{---} & h \\ | & & & & | & & \\ c & & \text{---} & & d & & \end{array} \tag{3.1}$$

denoted occasionally by $\mathcal{A} = [a, b, c, d, e, f, g, h]$. Each such cube can be sliced in three different ways, producing three pairs of 2×2-matrices (up-down, left-right, front-back[2]):

$$\begin{array}{lll} UD & M_1 = U = \begin{pmatrix} a & e \\ b & f \end{pmatrix}, & N_1 = D = \begin{pmatrix} c & g \\ d & h \end{pmatrix}, \\[2ex] LR & M_2 = L = \begin{pmatrix} a & c \\ e & g \end{pmatrix}, & N_2 = R = \begin{pmatrix} b & d \\ f & h \end{pmatrix}, \\[2ex] FB & M_3 = F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, & N_3 = B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}. \end{array}$$

[1] Let us mention in alphabetical order Arndt [Arn1857], Cayley [Cay1845, Cay1846], Dedekind [Ded1905], Dirichlet [DD1999], Riss [Ris1978], Shanks [Sha1978, Sh1989a, Sh1989b], Speiser [Spe1912], and Weber [Web1907].

[2] I have resisted the temptation to borrow the notation from physics, where the three pairs of charms have quite similar names.

To each such slicing of the cube $\mathcal{A}$ we can associate a binary quadratic form $Q_i = Q_i^{\mathcal{A}}$ by putting

$$Q_i(x,y) = -\det(M_i x + N_i y).$$

This way we find

$$Q_1(x,y) = (be - af)x^2 + (bg + de - ah - cf)xy + (dg - ch)y^2, \tag{3.2}$$

$$Q_2(x,y) = (ce - ag)x^2 + (cf + de - ah - bg)xy + (df - bh)y^2, \tag{3.3}$$

$$Q_3(x,y) = (bc - ad)x^2 + (bg + cf - ah - de)xy + (fg - eh)y^2. \tag{3.4}$$

If we set $Q_i = (A_i, B_i, C_i)$, then the coefficients of these forms are given by

$$\left.\begin{array}{lll} A_1 = -\det U, & \frac{B_1+B_2}{2} = -\det D_{UL}, & C_3 = -\det D, \\ A_2 = -\det L, & \frac{B_2+B_3}{2} = -\det D_{LF}, & C_2 = -\det R, \\ A_3 = -\det F, & \frac{B_1+B_2}{2} = -\det D_{FU}, & C_1 = -\det B, \end{array}\right\} \tag{3.5}$$

where $D_{UL} = \left(\begin{smallmatrix} a & e \\ d & h \end{smallmatrix}\right)$ is the "diagonal" matrix containing the edge ac common to the faces U and L; similarly, we have $D_{LF} = \left(\begin{smallmatrix} a & c \\ f & h \end{smallmatrix}\right)$ and $D_{FU} = \left(\begin{smallmatrix} a & b \\ g & h \end{smallmatrix}\right)$.

Example. The three forms attached to the cube

$$\mathcal{A} = \begin{array}{cccc} & 3 & & 1 \\ 0 & & 1 & \\ & 0 & & -7 \\ 2 & & 0 & \end{array}$$

are $Q_1 = (3, -2, 14)$, $Q_2 = (6, 2, 7)$, and $Q_3 = (2, 2, 21)$; these forms all have the same discriminant $\Delta = -4 \cdot 41$. In Prop. 3.4lemmacount.3.4 we will see that this is not accidental: forms attached to a single cube always have the same discriminant.

Let γ denote the rotation of the cube by 120° around the diagonal ah; then

$$\gamma\mathcal{A} = \begin{array}{cccc} & b & & d \\ a & & c & \\ & f & & h \\ e & & g & \end{array} \qquad \gamma^2\mathcal{A} = \begin{array}{cccc} & c & & g \\ a & & e & \\ & d & & h \\ b & & f & \end{array} \tag{3.6}$$

and $\gamma^3\mathcal{A} = \mathcal{A}$. The quadratic forms associated to the rotated cube $\gamma\mathcal{A}$ are Q_3, Q_1, Q_2: in fact we have

$$\begin{array}{lll} Q_{UD}^{\gamma\mathcal{A}} = Q_{FB}^{\mathcal{A}}, & Q_{LR}^{\gamma\mathcal{A}} = Q_{UD}^{\mathcal{A}}, & Q_{FB}^{\gamma\mathcal{A}} = Q_{LR}^{\mathcal{A}}, \\ Q_{UD}^{\gamma^2\mathcal{A}} = Q_{LR}^{\mathcal{A}}, & Q_{LR}^{\gamma^2\mathcal{A}} = Q_{FB}^{\mathcal{A}}, & Q_{FB}^{\gamma^2\mathcal{A}} = Q_{UD}^{\mathcal{A}}. \end{array}$$

Other symmetries of a cube will not just permute the forms:

1. By switching the front and the back of a cube, for example, the forms $Q_j = (A_j, B_j, C_j)$ will be transformed into

$$Q_1' = (-A_1, -B_1, -C_1), \quad Q_2' = (-A_2, -B_2, -C_2), \quad \text{and} \quad Q_3' = (C_3, B_3, A_3).$$

Similar remarks apply to switching left and right, or up and down faces.

2. Let β denote the rotation of the cube by 90° around the vertical axis; then

$$\beta\mathcal{A} = \begin{tikzcd}[row sep=small, column sep=small]
 & f \arrow[rr, dash] \arrow[dd, dash] & & b \arrow[dd, dash] \\
e \arrow[rr, dash] \arrow[dd, dash] & & a \arrow[dd, dash] & \\
 & h \arrow[rr, dash] & & d \\
g \arrow[rr, dash] & & c &
\end{tikzcd}$$

and we find

$$Q_1' = (-A_1, -B_1, -C_1), \quad Q_2' = (C_3, B_3, A_3), \quad \text{and} \quad Q_3' = (-A_2, -B_2, -C_2).$$

Applying β twice we find that a rotation of the cube by 180° around the vertical axis gives

$$Q_1' = (A_1, B_1, C_1), \quad Q_2' = (-C_2, -B_2, -A_2), \quad \text{and} \quad Q_3' = (-C_3, -B_3, -A_3).$$

Let us now investigat how the three quadratic forms Q_i attached to a cube $\mathcal{A}$ are related to each other. The following result, which generalizes classical formulas like

$$(x_1^2 + y_1^2)(x_2^2 + y_2^2) = (x_1x_2 \mp y_1y_2)^2 + (x_1y_2 \pm x_2y_1)^2, \tag{3.7}$$

was used by Legendre and Gauss for composing forms:

Theorem 3.1. *Let $\mathcal{A} = [a, b, c, d, e, f, g, h]$ be a cube to which three primitive forms $Q_i = Q_i^{\mathcal{A}}$ are attached. Then*

$$Q_1(x_1, y_1)Q_2(x_2, y_2) = Q_3(x_3, -y_3), \tag{3.8}$$

where x_3 and y_3 are linear forms in x_1, y_1 and x_2, y_2, and are given by

$$\left.\begin{aligned} x_3 &= ex_1x_2 + fx_1y_2 + gx_2y_1 + hy_1y_2, \\ y_3 &= ax_1x_2 + bx_1y_2 + cx_2y_1 + dy_1y_2. \end{aligned}\right\} \tag{3.9}$$

Similarly we have

$$Q_2(x_2, y_2)Q_3(x_3, y_3) = Q_1(x_1, -y_1) \quad \textit{with} \quad \begin{cases} x_1 = bx_2x_3 + dx_2y_3 + fx_3y_2 + hy_2y_3, \\ y_1 = ax_2x_3 + cx_2y_3 + ex_3y_2 + gy_2y_3, \end{cases}$$

$$Q_1(x_1, y_1)Q_3(x_3, y_3) = Q_2(x_2, -y_2) \quad \textit{with} \quad \begin{cases} x_2 = cx_1x_3 + gx_1y_3 + dx_3y_1 + hy_1y_3, \\ y_2 = ax_1x_3 + ex_1y_3 + bx_3y_1 + fy_1y_3. \end{cases}$$

Equation (3.8equation.3.1.8) should be interpreted as an identity in the polynomial ring $\mathbb{Z}[x_1, x_2, y_1, y_2]$. The proof below actually uses this interpretation in that it uses derivatives of polynomials.

Proof. This may be proved by a direct verification, for example by a short pari program. Here is a proof due to Dedekind: for the forms $Q_j(x_j, y_j)$, consider the partial derivatives

$$\frac{\partial Q_j}{\partial x_j} = 2A_jx_j + B_jy_j =: 2u_j, \quad \frac{\partial Q_j}{\partial y_j} = B_jx_j + 2C_jy_j =: 2v_j.$$

A special case of Euler's relation,[3] which can easily be verified directly, states that

[3] See Equation A.7Kapferer's Theoremequation.A.5.7.

$$u_j x_j + v_j y_j = Q_j(x_j, y_j). \tag{3.10}$$

Eliminating the product x_1x_2 from the equations for x_3 and y_3 in Thm. 3.1lemmacount.3.1 we get

$$\begin{aligned} ax_3 - ey_3 &= (af - be)x_1y_2 + (ag - ce)x_2y_1 + (ah - de)y_1y_2 \\ &= -A_1x_1y_2 - A_2x_2y_1 - \frac{B_1 + B_2}{2} y_1y_2 \\ &= -y_2u_1 - y_1u_2, \end{aligned}$$

and similarly we can derive

$$\begin{aligned} bx_3 - fy_3 &= x_2u_1 - y_1v_2, \\ cx_3 - gy_3 &= -y_2v_1 + x_1u_2, \\ dx_3 - hy_3 &= x_2v_1 + x_1v_2 \end{aligned}$$

by eliminating x_1y_2, x_2y_1, and x_2y_2, respectively. These four equations can be written in matrix form:

$$\begin{pmatrix} cx_3 - gy_3 & dx_3 - hy_3 \\ ax_3 - ey_3 & bx_3 - fy_3 \end{pmatrix} = \begin{pmatrix} x_1 & v_1 \\ -y_1 & u_1 \end{pmatrix} \begin{pmatrix} u_2 & v_2 \\ -y_2 & x_2 \end{pmatrix}.$$

Taking determinants and using (3.10From Cubes to Formsequation.3.1.10) then gives (3.8equation.3.1.8); in fact, the determinant on the left hand side is $-\det(Fx_3 - By_3) = Q_3(x_3, -y_3)$.

The other two sets of formulas are proved similarly; they also follow upon replacing $\mathcal{A}$ by $\gamma\mathcal{A}$ and $\gamma^2\mathcal{A}$. □

The following observation will often be useful:

Corollary 3.2. *If $\mathcal{A}$ is a cube to which the quadratic forms Q_i are attached, and if Q_1 and Q_2 represent a_1 and a_2, respectively, then Q_3 represents a_1a_2.*

Proof. This follows immediately from Thm. 3.1lemmacount.3.1: if $Q_1(x_1, y_1) = a_1$ and $Q_2(x_2, y_2) = a_2$, then $Q_3(x_3, -y_3) = a_1a_2$, with x_3, y_3 as in (3.9equation.3.1.9). □

Remark 1. The forms Q_3 satisfying the identity (3.8equation.3.1.8) are not uniquely determined (not even up to equivalence) by the forms Q_1 and Q_2; in other words: given Q_1 and Q_2, there might exist nonequivalent forms Q_3 and Q_3' both satisfying (3.8equation.3.1.8), of course with different bilinear forms x_3 and y_3.

For an explicit example, consider e.g. the form $(5, 6, 10)$ with discriminant $\Delta = -4 \cdot 41$. Then

$$(5x_1^2 + 6x_1y_1 + 10y_1^2)(5x_2^2 + 6x_2y_2 + 10y_2^2) = X^2 + 41Y^2$$

for

$$X = 5x_1x_2 + 3x_1y_2 + 3x_2y_1 + 10y_1y_2, \qquad \text{and} \qquad Y = x_1y_2 - x_2y_1.$$

On the other hand, we also have

$$(5x_1^2 + 6x_1y_1 + 10y_1^2)(5x_2^2 + 6x_2y_2 + 10y_2^2) = 2X^2 + 6XY + 25Y^2$$

for

$$X = 5x_1y_2 + 5x_2y_1 - 6y_1y_2, \qquad Y = x_1x_2 - 2y_1y_2.$$

Since $(2, 6, 25) \sim (2, 2, 21)$, this form is not equivalent to the principal form $(1, 0, 41)$. Thus the form $(5, 6, 10)$ can be composed with itself in two essentially different ways.

Remark 2. It is possible to remove the asymmetry (the minus sign of y_3; see Shanks' comments in [Sh1989b]) from (3.8equation.3.1.8): Dedekind and Weber have shown the existence of trilinear forms x_4 and y_4 such that $Q_1(x_1, y_1)Q_2(x_2, y_2)Q_3(x_3, y_3) = Q_0(x_4, y_4)$, where Q_0 is the principal form with discriminant Δ.

The Plücker Relation

Instead of using a cube such as (3.1From Cubes to Formsequation.3.1.1) for encoding the integers $a, b, \ldots, h$, we can also represent them by a 2×4-matrix

$$M(\mathcal{A}) = \begin{pmatrix} a & b & c & d \\ e & f & g & h \end{pmatrix}. \tag{3.11}$$

Let M_{ij} denote the 2×2-minor of $M(\mathcal{A})$ formed with the columns i and j; then e.g. $M_{12} = \left|\begin{smallmatrix} a & b \\ e & f \end{smallmatrix}\right|$, $M_{13} = \left|\begin{smallmatrix} a & c \\ e & g \end{smallmatrix}\right|$, $\ldots$, and we find

$$\begin{aligned} M_{12} &= -A_1, & M_{13} &= -A_2, & M_{14} &= -\frac{B_2 + B_1}{2}, \\ M_{34} &= -C_1, & M_{24} &= -C_2, & M_{23} &= -\frac{B_2 - B_1}{2}. \end{aligned}$$

These minors are known to satisfy the *Plücker Relation*, which is most easily derived by writing down the Laplace expansion of the determinant

$$N = \begin{vmatrix} a & b & c & d \\ e & f & g & h \\ a & b & c & d \\ e & f & g & h \end{vmatrix}$$

into 2×2-determinants with respect to the first two rows, and oberving that $N = 0$ since the rows are linearly dependent:

Proposition 3.3. *The minors M_{ij} of (3.11The Plücker Relationequation.3.1.11) satisfy the Plücker relation*

$$0 = M_{12}M_{34} - M_{13}M_{24} + M_{14}M_{23}. \tag{3.12}$$

Expressing these minors using the coefficients of the quadratic forms (see (3.5From Cubes to Formsequation.3.1.5)) shows that the Plücker Relation (3.12equation.3.1.12) is equivalent to

$$A_1C_1 - A_2C_2 + \frac{1}{4}(B_1^2 - B_2^2) = 0,$$

or, after a slight rearrangement, to

$$B_1^2 - 4A_1C_1 = B_2^2 - 4A_2C_2. \tag{3.13}$$

Thus the Plücker Relation implies that the two quadratic forms Q_1 and Q_2 have the same discriminant.

If we do the same for the matrices attached to the cubes $\gamma\mathcal{A}$ and $\gamma^2\mathcal{A}$ in (3.6From Cubes to Formsequation.3.1.6):

$$M(\gamma\mathcal{A}) = \begin{pmatrix} a & c & e & g \\ b & d & f & h \end{pmatrix} \quad \text{and} \quad M(\gamma^2\mathcal{A}) = \begin{pmatrix} a & e & b & f \\ c & g & d & h \end{pmatrix},$$

then we get

Proposition 3.4. *Let Q_1, Q_2, Q_3 denote the three forms attached to a cube $\mathcal{A}$. Then* $\operatorname{disc} Q_1 = \operatorname{disc} Q_2 = \operatorname{disc} Q_3$.

We call this common discriminant the *discriminant* of the cube $\mathcal{A}$ and denote it by $\operatorname{disc}\mathcal{A}$. It is easily checked that

$$\begin{aligned}\operatorname{disc}(\mathcal{A}) = a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 \\ - 2(abgh + cdef + acfh + bdeg + aedh + bfcg) \\ + 4(adfg + bceh).\end{aligned} \tag{3.14}$$

In Section 3.4.From Forms to Cubessection.3.4, we will solve the following problem: given six integers M_{ij} $(1 \le i < j \le 4)$, can we find a 2×4-matrix $M = \left(\begin{smallmatrix} a & b & c & d \\ e & f & g & h \end{smallmatrix}\right)$ such that the M_{ij} are its six minors? Clearly a necessary condition for the existence of M is that the M_{ij} satisfy the Plücker relation. We will see in Section 3.4.From Forms to Cubessection.3.4 that this condition is actually sufficient. For a lower-dimensional analogue of this construction see Exercise 3Bhargava's Cubeschapter.3.13ExercisesItem.219.

3.2. Automorphs

Where the Pell conic makes another appearance.

Recall that a matrix $S \in \mathrm{SL}_2(\mathbb{Z})$ is called an automorph of a form Q if $Q|_S = Q$. We have seen that automorphs of forms with discriminant Δ come from solutions of the corresponding Pell equation $Q_0(T,U) = 1$. In this section we will construct automorphs using Gauss composition, namely Equation (3.8equation.3.1.8).

What do we get if we pick $Q_1 = Q_0$, the principal form with discriminant Δ? If we can find a solution of the equation $Q_0(T,U) = 1$, then (3.8equation.3.1.8) shows that the forms Q_2 and Q_3 will represent the same integers.

Let $Q = (A,B,C)$ be a form with discriminant Δ; define an integer b via $B = 2b - \sigma$, where $\sigma \in \{0,1\}$ is determined by $\Delta = 4m+\sigma$, and set $b' = \sigma - b$. Assume that $Q_0(T,U) = 1$. Then the three forms attached to the cube

$$\begin{tikzcd}[row sep=small, column sep=small]
 & 1 \arrow[rr, dash] \arrow[dd, dash] & & 0 \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & 1 \arrow[dd, dash] & \\
 & b \arrow[rr, dash] & & C \\
A \arrow[rr, dash] & & b' &
\end{tikzcd}$$

are $Q_1 = Q_0$, $Q_2 = Q = (A,B,C)$ and $Q_3 = (A,-B,C)$, hence Thm. 3.1lemmacount.3.1 shows that $Q_0(T,U)Q(x,y) = Q(x',y')$ for

$$\begin{aligned} x' &= (T - bU)x - CUy, & \qquad x' &= (T + b'U)x - CUy, \\ y' &= AUx + (T + bU)y. & \qquad y' &= AUx + (T + bU)y \end{aligned}$$

These equations can be written in matrix form $\binom{x'}{y'} = S_Q^{(T,U)}\binom{x}{y}$, where $S_Q^{(T,U)}$ is the 2×2-matrix

$$S_Q^{(T,U)} = \begin{pmatrix} T - \frac{B}{2}U & -CU \\ AU & T + \frac{B}{2}U \end{pmatrix} \qquad S_Q^{(T,U)} = \begin{pmatrix} T + \frac{1-B}{2}U & -CU \\ AU & T + \frac{1+B}{2}U \end{pmatrix}.$$

Example. The solution $(T,U) = (2,1)$ of the Pell equation $T^2 - 3U^2 = 1$ gives rise to the automorph $\left(\begin{smallmatrix} 2 & 3 \\ 1 & 2 \end{smallmatrix}\right)$ of $Q = (1,0,-3)$; in fact we have

$$Q(2x+3y, x+2y) = (2x+3y)^2 - 3(x+2y)^2 = x^2 - 3y^2.$$

Let us now derive a few formal properties of automorphs. Let us start with the following problem: assume that $Q' = Q|_S$ for some $S \in \mathrm{SL}_2(\mathbb{Z})$. Then an integral solution (T,U) gives rise to automorphs $S_Q^{(T,U)}$ and $S_{Q'}^{(T,U)}$, and it is natural to ask how these are related.

Proposition 3.5. *Assume that $Q' = Q|_S$ for some $S \in \mathrm{SL}_2(\mathbb{Z})$, and that (T,U) is an integral solution of the associated Pell equation. Then*

$$S_{Q'}^{(T,U)} = S^{-1} S_Q^{(T,U)} S.$$

Proof. Writing $S_Q(T,U) = TI + U\mu(Q)$ (the matrices $\mu(Q)$ were defined in Chap. 1, Eqn. (1.4Even more Linear Algebraequation.1.1.4)) we find

$$S^{-1} S_Q^{(T,U)} S = S^{-1}(TI + U\mu(Q))S = TI + US^{-1}\mu(Q))S = TI + U\mu(Q|_S) = S_{Q'}^{(T,U)}.$$

□

Our next lemma shows that all the integral solutions of the equation $Q(x,y) = 1$ can be computed from a single integral solution by applying automorphs. As a warning we add the remark that this does not hold in general[4] for equations of the form $Q(x,y) = n$ with $n \neq 1$.

Lemma 3.6. *Let Q be a quadratic form with discriminant Δ, and assume that there are integers x, y, x', y' such that $Q(x,y) = Q(x',y') = 1$. Then there is an automorph $S = S_Q^{(T,U)}$ with $\binom{x'}{y'} = S^{-1}\binom{x}{y}$.*

Proof. Solving the system $\binom{x}{y} = S\binom{x'}{y'}$ for U and T we get

$$x = (T - \tfrac{B}{2}U)x' - CUy' \qquad y = AUx' + (T + \tfrac{B}{2}U)y',$$

which we can write as

$$x = Tx' - (Cy' + \tfrac{B}{2}x')U \qquad y = Ty' + (Ax' + \tfrac{B}{2}y')U.$$

Multiplying these equations through by $-y'$ and x', respectively, and adding the resulting equations gives

$$x'y - xy' = U[Ax'^2 + Bx'y' + Cy'^2] = U.$$

Eliminating U, we similarly find

$$\begin{aligned} x(Ax' + \tfrac{B}{2}y') + y(Cy' + \tfrac{B}{2}x') &= T[x'(Ax' + \tfrac{B}{2}y') + y'(Cy' + \tfrac{B}{2}x')] \\ &= T(Ax'^2 + Bx'y' + Cy'^2) = T. \end{aligned}$$

This proves the claim. □

3.3. The Action of the Modular Group on Cubes

Where the modular group returns to the stage and acts in a triple role.

We now define an action of $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ on the cube by replacing the cube $\mathcal{A}$ with upper face M_1 and bottom face N_1 by the cube $\mathcal{A}'$ with upper face $rM_1 + tN_1$ and bottom face $sM_1 + uN_1$. It turns out that this action induces the usual SL_2-action on Q_1: the form Q_1' attached to the cube $\mathcal{A}'$ is nothing but $Q_1|_S$.

Lemma 3.7. *Let $\mathcal{A}$ be a cube, $S \in \mathrm{SL}_2(\mathbb{Z})$, and let $\mathcal{A}' = \mathcal{A}|_S$ be the cube we get by letting S act on the upper and bottom faces of $\mathcal{A}$; then* $\operatorname{disc} \mathcal{A}' = \operatorname{disc} \mathcal{A}$. *If the associated quadratic forms are denoted by Q_i and Q_i', then $Q_1' = Q_1|_S$, $Q_2' = Q_2$, and $Q_3' = Q_3$.*

[4] Exercise: Where does the proof go wrong in this case?

Proof. We know that $Q_1 = -\det(M_1x + N_1y)$; applying $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ we see that

$$\begin{aligned} Q_1'(x,y) &= -\det\big((rM_1 + tN_1)x + (sM_1 + uN_1)y)\big) \\ &= -\det\big(M_1(rx+sy) + N_1(tx+uy)\big). \end{aligned}$$

Since $Q_1 = (A, B, C) = -\det(M_1x + N_1y)$, we find

$$\begin{aligned} Q_1'(x,y) &= A(rx+sy)^2 + B(rx+sy)(tx+uy) + C(tx+uy)^2 \\ &= (A', B', C'), \end{aligned}$$

where A', B' and C' agree with the values we have computed in (1.2The Action of the Modular Groupequation.1.1.2):

$$\begin{aligned} A' &= Ar^2 + Brt + Ct^2, \\ B' &= 2(Ars + Ctu) + B(ru + st), \\ C' &= As^2 + Bsu + Cu^2. \end{aligned}$$

Thus we see that $Q_1'(x,y) = Q|_S(x,y)$ as claimed.

Observe also that the action of $\mathrm{SL}_2(\mathbb{Z})$ is trivial on the quadratic forms Q_2 and Q_3, since this group acts by row and column operations on M_j and N_j for $j = 2, 3$, hence does not change the determinants $\det(M_jx + N_jy)$. □

The last claim can be made more obvious by using the matrix representation (3.11The Plücker Relationequation.3.1.11): then the cube $\mathcal{A}|_S$ (where $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ as before) is represented by the matrix

$$M(\mathcal{A}|_S) = \begin{pmatrix} ra+te & rb+tf & rc+tg & rd+th \\ sa+ue & sb+uf & sc+ug & sd+uh \end{pmatrix} = S^{\mathrm{tr}} M(\mathcal{A}).$$

Note that

$$M(\mathcal{A}|_{ST}) = (ST)^{\mathrm{tr}} M(\mathcal{A}) = T^{\mathrm{tr}} S^{\mathrm{tr}} M(\mathcal{A}) = T^{\mathrm{tr}} M(\mathcal{A}|_S) = M((\mathcal{A}|_S)|_T),$$

so this is indeed an action.

We have already seen (see (3.5From Cubes to Formsequation.3.1.5)) that the six minors of $M(\mathcal{A})$ essentially are the coefficients of $Q_1^{\mathcal{A}}$ and $Q_2^{\mathcal{A}}$. Since the minors of $M(\mathcal{A}|_S)$ are the minors of $M(\mathcal{A})$ multiplied by S^{tr} from the left, they have equal determinants, and this shows that the forms Q_1 and Q_2 computed from $\mathcal{A}$ and $\mathcal{A}|_S$ are indeed the same.

Now instead of letting $\mathrm{SL}_2(\mathbb{Z})$ act on the pair (M_1, N_1) as above we can also let it act on (M_2, N_2) and (M_3, N_3), respectively. In this way we get an action of the group $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ on the set of cubes; the action $A|_S$ described above now is $A|_{(S,I,I)}$, where I is the identity element in $\mathrm{SL}_2(\mathbb{Z})$. Note that the action of the three factors in Γ commutes: if you let an element (S_1, S_2, S_3) act on a cube then it does not matter whether you first let S_1 act on (M_1, N_1) and then S_2 on (M_2, N_2) or the other way round (check this! This follows from the fact that row and column transformations commute, which in turn may be seen as a consequence of the associativity of matrix multiplication).

Observe also that the action of the subgroup $I \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ of Γ is trivial on the quadratic form Q_1 (as above, this subgroup acts by row and column operations on M_1 and N_1, hence does not change the determinant $\det(M_1x + N_1y)$).

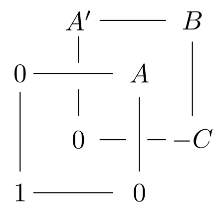
Primitive Cubes

A cube $\mathcal{A}$ is called *primitive*[5] if its three associated quadratic forms $Q_i^{\mathcal{A}}$ are primitive.

Theorem 3.8. *The group* $\mathrm{SL}_2(\mathbb{Z})^3 = \mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_2(\mathbb{Z})$ *acts on the set of primitive cubes with discriminant* Δ.

This follows immediately from the fact that $\mathrm{SL}_2(\mathbb{Z})$ acts on primitive forms with discriminant Δ. For showing that a cube is primitive if two of its quadratic forms are primitive, we need a lemma that will also be helpful later on.

Lemma 3.9. *Let $\mathcal{A}$ be a cube for which $Q_1^{\mathcal{A}}$ is primitive. Then $\mathcal{A}$ is equivalent to a cube of the form*



Proof. We start by observing that if Q_1 is primitive, then $\gcd(a, b, \ldots, h) = 1$. This implies that the element 1 is a $\mathbb{Z}$-linear combination of the coefficients $a, b, \ldots, h$, and we can transform $\mathcal{A} = [a, b, \ldots, h]$ into a cube with $c = 1$ by letting a suitable element of $\mathrm{SL}_2(\mathbb{Z})^3$ act on it. The element $c = 1$ can then be used to make the adjacent corners a, d and g vanish. □

Let us record the following

Corollary 3.10. *Given primitive forms Q and Q' with the same discriminant, we can find integers A, A', B, C with $Q \sim (A, B, A'C)$, $Q' \sim (A', B, AC)$, and* $\gcd(A, A', B) = 1$.

Proof. The fact that $\gcd(A, A', B) = 1$ follows from the primitivity of Q. □

Now we can prove

Lemma 3.11. *If the forms Q_1 and Q_2 attached to the cube $\mathcal{A}$ are primitive, then so is Q_3.*

Proof. The primitivity of forms is an invariant under the action of the modular group; we thus may assume without loss of generality that $\mathcal{A}$ is as in Lemma 3.9lemmacount.3.9. The three quadratic forms associated to $\mathcal{A}$ are

$$\begin{aligned} Q_1 &= Ax^2 + Bxy + A'Cy^2, \\ Q_2 &= A'x^2 + Bxy + ACy^2, \\ Q_3 &= AA'x^2 - Bxy + Cy^2. \end{aligned}$$

For showing that Q_3 is primitive we need to check that $\gcd(AA', B, C) = 1$, or that $\gcd(AA', B)$ and C are coprime. But from elementary number theory we know that $\gcd(AA', B) \mid \gcd(A, B)\gcd(A', B)$, and since Q_1 and Q_2 are primitive, these gcd's are coprime to $A'C$ and AC, respectively; in particular, they are coprime to C. □

The same kind of argument also proves the following lemma:

Lemma 3.12. *If the forms Q_1 and Q_2 attached to the cube $\mathcal{A}$ are positive definite, then so is Q_3.*

Indeed, a form with negative discriminant is positive definite if and only if its leading coefficient is positive; in the notation of Lemma 3.11lemmacount.3.11, this means that $A > 0$ and $A' > 0$. But then $AA' > 0$, and this implies that Q_3 is positive definite.

[5] Bhargava used the term “projective”.

3.4. From Forms to Cubes

Where we show how to compute a cube to which two given primitive forms with the same discriminant are attached: variations on a Gauss composition by Speiser, Arndt, and Dirichlet.

We have seen how to attach three binary quadratic forms with the same discriminant to a cube $\mathcal{A}$. Now we show that, conversely, to each pair of primitive binary quadratic forms of the same discriminant Δ we can construct a cube $\mathcal{A}$ giving rise to these forms. The literature on quadratic forms contains countless ways of constructing these cubes; here we present three of them, due respectively to Speiser, Arndt, and Dirichlet.

Let us call three primitive quadratic forms Q_1, Q_2, Q_3 collinear (we will write $Q_1Q_2Q_3 \sim 1$) if there is a cube $\mathcal{A}$ such that $Q_i = Q_i^{\mathcal{A}}$ for $i = 1, 2, 3$. So far we have proved the following results on collinearity:

- If $Q_1Q_2Q_3 \sim 1$ and Q_1 and Q_2 are primitive, then so is Q_3 (Lemma 3.11lemmacount.3.11).
- If $Q_1Q_2Q_3 \sim 1$ and Q_1 and Q_2 are positive definite, then so is Q_3 (Lemma 3.12lemmacount.3.12).

In this section, we will present several methods for computing a form Q_3 collinear with given forms Q_1, Q_2; in other words:

- Given two primitive forms Q_1 and Q_2 with the same discriminant Δ, there always is a form Q_3 with discriminant Δ such that $Q_1Q_2Q_3 \sim 1$ (Thm. 3.13lemmacount.3.13).

Afterwards we will use collinearity to define a group structure on the set of equivalence classes of primitive forms with discriminant Δ.

Composition of Forms

The main result in this section is

Theorem 3.13. *Let $\Delta \neq 0$ be a discriminant. For any pair $Q_1 = (A_1, B_1, C_1)$ and $Q_2 = (A_2, B_2, C_2)$ of primitive forms with discriminant Δ there is a cube $\mathcal{A}$ such that $Q_1 = Q_1^{\mathcal{A}}$ and $Q_2 = Q_2^{\mathcal{A}}$.*

More precisely: if $A_1A_2 \neq 0$, and if we put $B = \frac{1}{2}(B_1 + B_2)$, $e = \gcd(A_1, A_2, B)$, $a = 0$, $b = A_1/e$, $c = A_2/e$, and $d = B/e$, then there exist integral solutions f, g, h of the diophantine equations

$$bg - cf = \frac{B_1 - B_2}{2}, \qquad h = \frac{fd - C_2}{b}$$

such that

$$\begin{tikzcd}[row sep=small, column sep=small]
 & e \arrow[rr, dash] \arrow[dd, dash] & & f \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & A_1/e \arrow[dd, dash] & \\
 & g \arrow[rr, dash] & & h \\
A_2/e \arrow[rr, dash] & & B/e &
\end{tikzcd} \tag{3.15}$$

is a cube with associated forms Q_1, Q_2 and $Q_3 = (A_3, B_3, C_3)$, where

$$A_3 = \frac{A_1A_2}{e^2} \quad \text{and} \quad B_3 = g\frac{A_1}{e} + f\frac{A_2}{e} - B. \tag{3.16}$$

The matrix $\mathcal{M} = \left(\begin{smallmatrix} 0 & b & c & d \\ e & f & g & h \end{smallmatrix}\right)$ associated to the cube $\mathcal{A}$ will be called a *composition matrix* for Q_1 and Q_2. Observe that the gcd in the definition of e is determined only up to sign; but replacing e by $-e$ changes the composition matrix $\mathcal{M}$ into $-\mathcal{M}$, which produces the same triple of forms Q_1, Q_2, Q_3.

In the proof of Thm. 3.13lemmacount.3.13 we will use the following lemma:

Lemma 3.14. *Let $Q_1 = (A_1, B_1, C_1)$ and $Q_2 = (A_2, B_2, C_2)$ be quadratic forms with discriminant Δ, and set $B = \frac{1}{2}(B_1 + B_2)$, $e = \gcd(A_1, A_2, B)$, and $\alpha = \gcd(A_1/e, A_2/e)$. Then $\alpha \mid \frac{1}{2}(B_1 - B_2)$.*

Proof. From the "Plücker relation"

$$\frac{B_1 - B_2}{2} \cdot \frac{B_1 + B_2}{2} = A_1C_1 - A_2C_2$$

we deduce that $\alpha \mid \frac{1}{2}(B_1 - B_2) \cdot \frac{B}{e}$. The claim follows from the observation that α and $\frac{B}{e}$ are coprime. ☐

Proof of Thm. 3.13lemmacount.3.13. In the proof below we will assume that $A_2 = -M_{13} \neq 0$. It can easily be modified if any of A_1, C_1 or C_2 is $\neq 0$. In the remaining case, the primitivity of the forms implies $B_1 = \pm 1$, hence $\Delta = 1$; in this case we will see that there is only one reduced form, so composition is trivial.

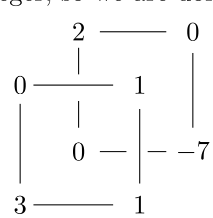
If we set $a = 0$, $e = \gcd(A_1, A_2, B)$, $b = A_1/e$, $c = A_2/e$, and $d = B/e$, then the cube $\mathcal{A}$ in (3.15equation.3.4.15) satisfies $\det U = -A_1$, $\det L = -A_2$, and $\det D_{UL} = B$. Thus the three minors M_{12}, M_{13} and M_{14} of $M(\mathcal{A}) = \left(\begin{smallmatrix} a & b & c & d \\ e & f & g & h \end{smallmatrix}\right)$ already have the desired values. Observe also that $A_3 = bc - ad = A_1A_2/e^2$ as claimed.

Next we determine integers f and g such that $M_{23} = bg - cf = \frac{1}{2}(B_1 - B_2)$. This equation is solvable in integers because $\gcd(b, c) \mid M_{23}$ by Lemma 3.14lemmacount.3.14.

Finally, h is determined by $-C_2 = M_{24} = bh - fd$: we get $h = (M_{24} + df)/b$. The resulting cube $\mathcal{A}$ now gives rise to the correct forms Q_1 and Q_2: all the minors M_{ij} with the possible exception of M_{34} have the desired values, and the fact that $M_{34} = -C_1$ follows from the Plücker relation (observe that $M_{12} = -A_2 \neq 0$).

If h happens to be an integer, we are done. If not, then we observe that bh and ch are integers, hence the denominator of h must divide $\gcd(b, c) = \alpha$. Write $h = H/\alpha$ and determine an integer r such that $r\frac{B}{e} \equiv H \bmod \alpha$ (this is possible since $\frac{B}{e}$ and α are coprime). Then subtract $\frac{r}{\alpha}$ times the front face from the back face of $\mathcal{A}$; since a, b, c are divisible by α, the numbers $e' = e$, f', g' will remain integral. Moreover, we get $h' = h - \frac{r}{\alpha}\frac{B}{e} = \frac{H - r\frac{B}{e}}{\alpha} \in \mathbb{Z}$. ☐

Example 1. Let us take the forms $Q_1 = (2, 2, 21)$ and $Q_2 = (6, 2, 7)$ with discriminant $\Delta = -164$. We set $a = 0$, $B = 2$, $e = \gcd(2, 6, 2) = 2$, $b = 2/2 = 1$, $c = 6/2 = 3$, and $d = 2/2 = 1$. Since $M_{23} = (B_1 - B_2)/2 = 0$, we can take $f = g = 0$. Finally, $h = (M_{24} + df)/b = -7$ is an integer, so we are done. We have found

$\mathcal{A} =$ 

and the associated quadratic forms are $Q_1 = (2, 2, 21)$, $Q_2 = (6, 2, 7)$, and $Q_3 = (3, -2, 14)$.

Example 2. Let us compose the forms $Q_1 = (6, 5, 8)$ and $Q_2 = (6, 1, 7)$ with discriminant $\Delta = -167$. Using $e = \gcd(A_1, A_2, (B_1 + B_2)/2) = 3$ we easily find $\left(\begin{smallmatrix} a & b & c & d \\ e & f & g & h \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 2 & 2 & 1 \\ 3 & 0 & 1 & -7/2 \end{smallmatrix}\right)$.

For getting integral entries we add half the top row to the bottom row and get $\left(\begin{smallmatrix} 0 & 2 & 2 & 1 \\ 3 & 1 & 2 & -3 \end{smallmatrix}\right)$, which in turn gives $Q_3 = (4, 3, 11)$.

Example 3. Let us compose the forms $Q_1 = (5, 26, 18)$ and $(15, 44, 27)$ with discriminant $\Delta = 316$. We set $B = 35$, $a = 0$, $e = \gcd(5, 15, 35) = 5$, $b = A_1/e = 1$, $c = A_2/e = 3$ and $d = B/e = 7$, and then solve the equation $g - 3f = bg - cf = (B_1 - B_2)/2 = -9$ by putting $g = 0$ and $f = 3$, and finally set $h = (fd - C_2)/b = (21 - 27)/1 = -6$. Thus we get $M(\mathcal{A}) = \left(\begin{smallmatrix} 0 & 1 & 3 & 7 \\ 5 & 3 & 0 & -6 \end{smallmatrix}\right)$, which yields the form $Q_3 = (3, -26, 30) \sim (3, 20, 7)$.

Example 4. A composition matrix for the forms $Q_1 = (3, 8, 0)$ and $Q_2 = (0, 8, 5)$ with discriminant $\Delta = 8^2$ is given by $M = \left(\begin{smallmatrix} 0 & 3 & 0 & 8 \\ 1 & 1 & 0 & 1 \end{smallmatrix}\right)$; it yields $Q_3 = (0, -8, -1)$, so $Q_1Q_2 \sim (0, 8, -1)$.

Arndt's Congruences

We have seen above how to construct cubes from given primitive forms Q_1, Q_2 with the same discriminant; these cubes then give us a form Q_3 with $Q_1Q_2Q_3 \sim 1$. Since collinearity will be used for defining a group structure on the set of equivalence classes, it is important to have simple formulas for computing Q_3. In this section we will derive such formulas which will turn out to be useful later when we will discuss the group laws on Jacobians of elliptic and hyperelliptic curves. Assume that we are given primitive quadratic forms $Q_1 = (A_1, B_1, C_1)$ and $Q_2 = (A_2, B_2, C_2)$ with the same discriminant, and set $e = \gcd(A_1, A_2, B)$. We would like to have formulas for computing a form Q_3 such that $Q_1Q_2Q_3 \sim 1$. We have seen in the proof of Thm. 3.13lemmacount.3.13 that we can take $A_3 = A_1A_2/e^2$. Since C_3 can be computed from A_3 and B_3 and the common discriminant, it remains to give a formula for B_3. Actually, since we are only interested in the equivalence class of Q_3, it is sufficient to know the congruence class $B_3 \bmod 2A_3$.

In the proof of Thm. 3.13lemmacount.3.13 we have used the equations

$$\begin{aligned} \frac{A_1}{e}g - \frac{A_2}{e}f &= \frac{B_1 - B_2}{2}, \\ B_3 &= \frac{A_1}{e}g + \frac{A_2}{e}f - \frac{B_1 + B_2}{2}, \end{aligned}$$

from which we deduce

$$B_3 = 2\frac{A_1}{e}g - B_2 \equiv -B_2 \bmod 2\frac{A_1}{e}.$$

Similarly we can prove that $B_3 \equiv -B_1 \bmod 2A_2/e$. Finally we find

$$\begin{aligned} \frac{B}{e}B_3 &= \frac{B}{e}\Big(\frac{A_1}{e}g + \frac{A_2}{e}f - B\Big) = -\frac{B^2}{e} + \frac{A_1B}{e^2}g + \frac{A_2B}{e^2}f \\ &= -\frac{B^2}{e} + \frac{A_1}{e}\Big(C_1 + \frac{A_2}{e}h\Big) + \frac{A_2}{e}\Big(C_2 + \frac{A_1}{e}h\Big) \\ &= -\frac{B^2}{e} + \frac{A_1C_1}{e} + \frac{A_2C_2}{e} + 2\frac{A_1A_2}{e}h \ \equiv \ -\frac{1}{e}(B^2 + A_1C_1 + A_2C_2) \\ &= \frac{1}{e}\Big(- B^2 + 2A_1C_1 + B\frac{B_2 - B_1}{2}\Big) = -\frac{\Delta + B_1B_2}{2} \qquad \bmod 2A_1A_2/e^2. \end{aligned}$$

Thus B_3 satisfies the congruences

$$\left.\begin{aligned} \tfrac{A_2}{e}B_3 &\equiv \ -\tfrac{A_2}{e}B_1 \ \bmod 2\tfrac{A_1A_2}{e^2}, \\ \tfrac{A_1}{e}B_3 &\equiv \ -\tfrac{A_1}{e}B_2 \ \bmod 2\tfrac{A_1A_2}{e^2}, \\ \tfrac{B}{e}B_3 &\equiv -\tfrac{\Delta+B_1B_2}{2} \bmod 2\tfrac{A_1A_2}{e^2}. \end{aligned}\right\} \tag{3.17}$$

Since the coefficients of B_3 on the left hand side, namely A_1/e, A_2/e and B/e, have greatest common divisor 1, these congruences determine B_3 uniquely modulo $2A_1A_2/e^2 = 2A_3$. In fact, if we choose integers λ, μ, ν satisfying the Bezout equation $\lambda A_1 + \mu A_2 + \nu B = e$, then clearly

$$\begin{aligned} B_3 &= \frac{1}{e}(\lambda A_1 + \mu A_2 + \nu B)B_3 \\ &\equiv -\lambda \frac{A_1}{e} B_2 - \mu \frac{A_2}{e} B_1 - \nu \frac{\Delta + B_1 B_2}{2} \qquad \bmod 2A_1A_2. \end{aligned}$$

But now we observe that the residue class $B_3 \bmod 2A_3$ determines the equivalence class of Q_3; in fact we find

Corollary 3.15. *Let $Q_i = (A_i, B_i, C_i)$ $(i = 1, 2)$ be primitive binary quadratic forms with discriminant Δ, and set $B = \frac{B_1+B_2}{2}$ and $\gcd(A_1, A_2, B) = e$. Then $Q_1Q_2Q_3 \sim 1$ for $Q_3 = (A_3, B_3, C_3)$, where $A_3 = A_1A_2/e^2$, B_3 is determined by the congruences (3.17Arndt's Congruencesequation.3.4.17), and $C_3 = \frac{B_3^2-\Delta}{4A_3}$.*

Alternatively, given a solution of the Bezout equation $\lambda A_1 + \mu A_2 + \nu B = e$, we can compute B_3 using the formula

$$eB_3 = -\lambda A_1 B_2 - \mu A_2 B_1 - \nu \frac{\Delta + B_1 B_2}{2}.$$

Example. Using Speiser's method '(Example 2 above) we have found that $Q_1Q_2Q_3 \sim 1$ for the forms $Q_1 = (6, 5, 8)$ and $Q_2 = (6, 1, 7)$, which implies that $Q_1 * Q_2 \sim (4, -3, 11)$.

Composition via Arndt's congruences requires solving the equation $6\lambda + 6\mu + 3\nu = 1$; taking $\lambda = \mu = 0$ and $\nu = 1$, we find $A_3 = A_1A_2/e = 4$ and $B_3 = \frac{1}{6}(167 - 5) = 27$. Thus $Q_3 = (4, 27, 56) \sim (4, 3, 11)$.

Dirichlet's Concordant Forms

Dirichlet's method of concordant forms is yet another technique for computing a form Q_3 collinear with given forms Q_1 and Q_2. The basic idea is the following: since we are only interested in the equivalence class of Q_3, we may use the action of $\mathrm{SL}_2(\mathbb{Z})$ to replace Q_1 and Q_2 by equivalent forms before we compute Q_3. Dirichlet realized that the representatives Q_1 and Q_2 of their equivalence classes can be chosen in such a way that composition is as easy as plain multiplication of integers.

Let us call quadratic forms (A, B, C) and (A', B', C') with nonsquare discriminant Δ *concordant* if the coefficients have the following properties:

1. $B = B'$;
2. $A' \mid C$ and $A \mid C'$.

The composition of concordant forms is almost trivial:

Proposition 3.16. *If Q and Q' are concordant, then $Q = (A, B, A'C)$ and $Q' = (A', B, AC)$ for integers A, A', B, C, and with $Q'' = (AA', B, C)$, we have $QQ'Q''^{-} \sim 1$.*

Proof. Consider the cube $\mathcal{A}$ given by

$$\begin{tikzcd} & A' \arrow[rr, dash] \arrow[dd, dash] & & B \arrow[dd, dash] \\ 0 \arrow[rr, dash] \arrow[dd, dash] & & A \arrow[dd, dash] & \\ & 0 \arrow[rr, dash] & & -C \\ 1 \arrow[rr, dash] & & 0 & \end{tikzcd}$$

Its associated quadratic forms are

$$\begin{aligned} Q &= Ax^2 + Bxy + A'Cy^2, \\ Q' &= A'x^2 + Bxy + ACy^2, \\ Q'' &= AA'x^2 - Bxy + Cy^2. \end{aligned}$$

This implies the claim. □

In order to be able to actually work with Dirichlet composition, we need a method for changing two given forms Q_1, Q_2 into equivalent forms $Q_1' \sim Q_1$ and $Q_2' \sim Q_2$ such that Q_1' and Q_2' are concordant. The main lemma for achieving this is the following:

Lemma 3.17. *Let $Q = (A, B, C)$ be a primitive quadratic form. Then for any $N \in \mathbb{N}$ there are $r, s \in \mathbb{Z}$ such that $Q(r, s)$ is coprime to N.*

Proof. Write $N = rst$, where $(r, C) = 1$, and where the primes $p \mid s$ and $q \mid t$ satisfy $p \mid C$, $p \nmid A$, $q \mid A$ and $q \mid C$. Then we find

$$\begin{aligned} \gcd(Q(r, s), r) &= \gcd(Cs^2, r) = 1, \\ \gcd(Q(r, s), s) &= \gcd(Ar^2, s) = 1, \\ \gcd(Q(r, s), t) &= \gcd(Brs, t) = 1, \end{aligned}$$

where we have used that $\gcd(B, t) = 1$ because Q is primitive. □

For composing two forms it is sufficient to make two forms concordant; for the proof of associativity of composition we need to do the same with three given forms:

Proposition 3.18. *Let Q_1, Q_2, Q_3 be primitive quadratic forms with discriminant Δ. Then there exist integers A_1, A_2, A_3, B, C such that*

$$Q_1 \sim (A_1, B, A_2A_3C), \qquad Q_2 \sim (A_2, B, A_1A_3C), \qquad Q_3 \sim (A_3, B, A_1A_2C).$$

Proof. By Lemma 3.17lemmacount.3.17, we may assume without loss of generality that the A_i are odd and pairwise coprime. Since each B_i may be changed modulo $2A_i$, we need to show that the system of congruences

$$B \equiv B_1 \bmod 2A_1, \qquad B \equiv B_2 \bmod 2A_2, \qquad B \equiv B_3 \bmod 2A_3$$

is solvable. Since the A_i are pairwise coprime, we have $\gcd(2A_1, 2A_2, 2A_3) = 2$, hence the system has a solution if and only if $B_1 \equiv B_2 \equiv B_2 \bmod 2$. But this follows from the fact that the forms have the same discriminant.

Now we have forms (A_i, B, C_i) with $\Delta = B^2 - 4A_iC_i$. Thus $4A_1C_1 = 4A_2C_2$, hence $A_1C_1 = A_2C_2$; since A_1 and A_2 are coprime, we must have $A_2 \mid C_1$ and $A_1 \mid C_2$. Thus we can write $Q_1 = (A_1, B, A_2C')$, $Q_2 = (A_2, B, A_1C')$.

Next $A_3C_3 = A_1C' = A_2C'$ implies $A_1A_2 \mid C_3$ and $A_3 \mid C'$, hence there is an integer C such that $Q_1 = (A_1, B, A_2A_3C)$, $Q_2 = (A_2, B, A_1A_3C)$ and $Q_3 = (A_3, B, A_1A_2C)$. □

Example. For composing the forms $Q_1 = (3, 20, 7)$ and $Q_2 = (3, 22, 14)$, we replace the first form by the equivalent form $(7, -20, 3)$ and then solve the system of congruences $B \equiv -20 \bmod 14$ and $B \equiv 22 \bmod 6$. We find $B = 22$, so $(7, -20, 3) \sim (7, 22, 6)$. Thus $A = 7$, $B = 22$, $A' = 3$, $C = 2$, hence $Q_1Q_2 \sim (21, 22, 2)$.

3.5. Collinearity and the Group Law

Where forms line up and classes form a group.

The notion of collinearity of forms, which we have introduced above, seems to have little to do with collinearity, except that three classes may or may not be collinear, whereas for two given classes there is always a third such that the three are collinear. Only when we will study the group law on elliptic curves we will see that the connection is more than superficial.

In this section we will prove a couple of properties of collinearity, which we will use to endow the set $\mathrm{Cl}^+(\Delta)$ of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive forms of discriminant Δ with a group structure. We start with

Lemma 3.19. *Collinearity only depends on the equivalence classes of the forms: If $Q_1Q_2Q_3 \sim 1$ and $Q_j' \sim Q_j$ for $j = 1, 2, 3$, then $Q_1'Q_2'Q_3' \sim 1$.*

Proof. Since $Q_1Q_2Q_3 \sim 1$, there is a cube $\mathcal{A}$ with $Q_i = Q_i^{\mathcal{A}}$. Next $Q_j' \sim Q_j$ for $j = 1, 2, 3$ implies the existence of elements $S_i \in \mathrm{SL}_2(\mathbb{Z})$ with $Q_i' = Q_i|_{S_i}$. Now put $\mathcal{B} = \mathcal{A}|_{(S_1,S_2,S_3)}$. □

We will have to investigate to which degree Q_3 is determined by Q_1 and Q_2 and the condition that the three forms be collinear.

Let us start by showing that collinearity does not depend on the choice of the cube:

Lemma 3.20. *If $\mathcal{A}$ and $\mathcal{B}$ are cubes with $Q_1^{\mathcal{A}} = Q_1^{\mathcal{B}}$ and $Q_2^{\mathcal{A}} = Q_2^{\mathcal{B}}$, then $Q_3^{\mathcal{A}} \sim Q_3^{\mathcal{B}}$.*

This result[6] will be proved by invoking Gauss's Lemma (there are actually three results known as Gauss's Lemma: one in the theory of quadratic residues, one in the theory of polynomial rings, and the following):

Lemma 3.21 (Gauss's Lemma)**.** *Let*

$$M = \begin{pmatrix} p_1 & p_2 & \dots & p_n \\ q_1 & q_2 & \dots & q_n \end{pmatrix} \quad \text{and} \quad M' = \begin{pmatrix} p_1' & p_2' & \dots & p_n' \\ q_1' & q_2' & \dots & q_n' \end{pmatrix}$$

be two $2 \times n$-matrices ($n \geq 3$) with the following properties:

1. *the 2×2-minors of M are coprime;*
2. *there is an integer m such that each minor of M' is m times the corresponding minor of M.*

Then there is a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with determinant m such that $M' = AM$.

Proof. Since the minors $M_{ik} = \left|\begin{smallmatrix} p_i & p_k \\ q_i & q_k \end{smallmatrix}\right|$ of M are coprime, there exist n^2 integers x_{ik} such that the Bezout relation

$$\sum_{i,k=1}^{n} x_{ik} \begin{vmatrix} p_i & p_k \\ q_i & q_k \end{vmatrix} = 1$$

holds. Then we find

$$\begin{aligned} p_k \begin{vmatrix} p_i' & p_j' \\ q_i & q_j \end{vmatrix} + q_k \begin{vmatrix} p_i & p_j \\ p_i' & p_j' \end{vmatrix} &= p_i' \begin{vmatrix} p_k & p_j \\ q_k & q_j \end{vmatrix} - p_j' \begin{vmatrix} p_k & p_i \\ q_k & q_i \end{vmatrix} \\ &= \frac{1}{m}\left(p_i' \begin{vmatrix} p_k' & p_j' \\ q_k' & q_j' \end{vmatrix} - p_j' \begin{vmatrix} p_k' & p_i' \\ q_k' & q_i' \end{vmatrix} \right) = \frac{1}{m} p_k' \begin{vmatrix} p_i' & p_j' \\ q_i' & q_j' \end{vmatrix} = p_k' \begin{vmatrix} p_i & p_j \\ q_i & q_j \end{vmatrix}. \end{aligned}$$

[6] Lemma 3.19lemmacount.3.19 shows that it is sufficient to assume that $Q_1^{\mathcal{A}} \sim Q_1^{\mathcal{B}}$ and $Q_2^{\mathcal{A}} \sim Q_2^{\mathcal{B}}$.

Now set

$$a = \sum_{ij} x_{ij} \begin{vmatrix} p_i' & p_j' \\ q_i & q_j \end{vmatrix}, \qquad b = \sum_{ij} x_{ij} \begin{vmatrix} p_i & p_j \\ p_i' & p_j' \end{vmatrix}, \qquad c = \sum_{ij} x_{ij} \begin{vmatrix} q_i' & q_j' \\ q_i & q_j \end{vmatrix}, \qquad d = \sum_{ij} x_{ij} \begin{vmatrix} p_i & p_j \\ q_i' & q_j' \end{vmatrix}.$$

Then a, b, c, d are integers satisfying

$$ap_k + bq_k = \sum x_{ij} \left(p_k \begin{vmatrix} p_i' & p_j' \\ q_i & q_j \end{vmatrix} + q_k \begin{vmatrix} p_i & p_j \\ p_i' & p_j' \end{vmatrix} \right) = p_k' \sum x_{ij} \begin{vmatrix} p_i & p_j \\ q_i & q_j \end{vmatrix} \quad = \quad p_k'.$$

Similarly, we find $cp_k + dq_k = q_k'$, and this completes the proof. The fact that $\det A = m$ follows by taking the determinants of any relation $M' = AM$ for a nonsingular M. $\square$

In the applications we have in mind, the matrix will always be a 2×4-matrix, and we always will have $\det A = m = 1$.

Proof of Lemma 3.20lemmacount.3.20. Assume now that $\mathcal{A}$ and $\mathcal{B}$ are cubes with $Q_2^{\mathcal{A}} = Q_2^{\mathcal{B}} = Q_2$ and $Q_3^{\mathcal{A}} = Q_3^{\mathcal{B}} = Q_3$ (we have changed indices); we have to show that $Q_1^{\mathcal{A}} \sim Q_1^{\mathcal{B}}$. Let $M(\mathcal{A})$ and $M(\mathcal{B})$ denote the 2×4-matrices corresponding to $\mathcal{A}$ and $\mathcal{B}$; then the six minors of $M(\mathcal{A})$ and $M(\mathcal{B})$ are determined by the coefficients of $Q_2^{\mathcal{A}}$, $Q_3^{\mathcal{A}}$ and $Q_2^{\mathcal{B}}$, $Q_3^{\mathcal{B}}$, respectively, so they must be equal. Gauss's Lemma then says that there is some $S \in \mathrm{SL}_2(\mathbb{Z})$ such that $M(\mathcal{B}) = S^{\mathrm{tr}} M(\mathcal{A})$. But then $Q_1^{\mathcal{B}} = Q_1^{\mathcal{A}}|_S \sim Q_1^{\mathcal{A}}$ as claimed. $\square$

Of course, collinearity should not depend on how Q_1, Q_2, Q_3 are ordered:

Lemma 3.22. *If Q_1, Q_2 and Q_3 are collinear, then so is any permutation of these forms.*

Proof. Observe that the quadratic forms attached to the cubes

$$\mathcal{A} = \begin{tikzcd}[row sep=small, column sep=small]
& e \arrow[rr, dash] \arrow[dd, dash] & & f \arrow[dd, dash] \\
a \arrow[rr, dash] \arrow[dd, dash] & & b & \\
& g \arrow[rr, dash] & & h \\
c \arrow[rr, dash] & & d \arrow[uu, dash, crossing over] &
\end{tikzcd} \qquad
\mathcal{B} = \begin{tikzcd}[row sep=small, column sep=small]
& e \arrow[rr, dash] \arrow[dd, dash] & & g \arrow[dd, dash] \\
a \arrow[rr, dash] \arrow[dd, dash] & & c & \\
& f \arrow[rr, dash] & & h \\
b \arrow[rr, dash] & & d \arrow[uu, dash, crossing over] &
\end{tikzcd}$$

satisfy $Q_1^{\mathcal{B}} = Q_1^{\mathcal{A}}$, $Q_2^{\mathcal{B}} = Q_3^{\mathcal{A}}$, and $Q_3^{\mathcal{B}} = Q_2^{\mathcal{A}}$. For cyclic permutations of the forms Q_i, consider the cubes attached to the matrices $\gamma\mathcal{A}$ and $\gamma^2\mathcal{A}$. $\square$

Examples of Collinear Classes

Next we produce examples of collinear equivalence classes of forms.

Lemma 3.23. *Let Q_0 be he principal form with discriminant Δ. Then $Q_0Q_0Q_0 \sim 1$; moreover, for any primitive form $Q = (A, B, C)$ and its opposite form $Q^- = (A, -B, C)$, we have $Q_0QQ^- \sim 1$.*

Proof. The proof of the first claim is easy: just take

$$\begin{tikzcd}[row sep=small, column sep=small]
& 1 \arrow[rr, dash] \arrow[dd, dash] & & 0 \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & 1 & \\
& 0 \arrow[rr, dash] & & m \\
1 \arrow[rr, dash] & & 0 \arrow[uu, dash, crossing over] &
\end{tikzcd} \qquad \text{or} \qquad
\begin{tikzcd}[row sep=small, column sep=small]
& 1 \arrow[rr, dash] \arrow[dd, dash] & & 1 \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & 1 & \\
& 1 \arrow[rr, dash] & & \mu \\
1 \arrow[rr, dash] & & 1 \arrow[uu, dash, crossing over] &
\end{tikzcd}$$

according as $\Delta = 4m$ or $\Delta = 4m + 1 = 4\mu - 3$, with $\mu = m + 1$. Note that these cubes are "triply symmetric": rotations by 120° about the long diagonal containing m and μ, respectively, leave the cubes invariant.

Next observe that $B \equiv \Delta \bmod 2$; thus we can put $B = 2b$ if $\Delta = 4m$, and $B = 2b - 1$ if $\Delta = 1 + 4m$. With $b' = 1 - b$ we then find that the two cubes

$$\begin{tikzcd}[column sep=small, row sep=small]
& A \arrow[rr, dash] \arrow[dd, dash] & & -b \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & 1 \arrow[dd, dash] & \\
& b \arrow[rr, dash] & & -C \\
1 \arrow[rr, dash] & & 0 &
\end{tikzcd}
\quad \text{and} \quad
\begin{tikzcd}[column sep=small, row sep=small]
& A \arrow[rr, dash] \arrow[dd, dash] & & b' \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & 1 \arrow[dd, dash] & \\
& b \arrow[rr, dash] & & -C \\
1 \arrow[rr, dash] & & 0 &
\end{tikzcd}$$

give rise to the quadratic forms $Q_1 = Q_0$, $Q_2 = (A, B, C)$, and $Q_3 = (A, -B, C)$. This implies the claim. □

The Group Law

We are now ready to define composition of (equivalence classes of) forms. Let Δ be a nonsquare discriminant, and write $\Delta = \sigma^2 - 4m$ for $\sigma \in \{0, 1\}$. We will make the set $\mathrm{Cl}^+(\Delta)$ of equivalence classes of primitive binary quadratic forms of discriminant Δ into a group whose neutral element is the class $1 = [Q_0]$ of the principal form $Q_0 = (1, \sigma, m)$.

Remark. Gauss wrote composition additively; Poullet-Delisle, who translated the Disquisitiones into French, wrote it multiplicatively, but still talked about duplication (instead of squaring). Writing the group law additively has certain advantages; on the other hand, it is rather unusual to talk about duplicates instead of squares. Moreover it will become clear that composition of forms has a lot more in common with multiplication than with addition. In particular (and this was already known to Gauss), the class group of forms with square discriminant N^2 is isomorphic to the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$.

Theorem 3.24. *There is a unique group law on the the set $\mathrm{Cl}^+(\Delta)$ of equivalence classes of primitive binary quadratic forms of discriminant Δ with the following properties:*

1. *The class $1 = [Q_0]$ of the principal form $Q_0 = (1, \sigma, m)$ is the neutral element;*
2. *For three classes $c_1, c_2, c_3 \in \mathrm{Cl}^+(\Delta)$ we have $c_1c_2c_3 = 1$ if and only if they are collinear.*

Since we have already shown that the classes of Q_0, $Q = (A, B, C)$ and $Q^- = (A, -B, C)$ are collinear, and since the class of Q_0 is the neutral element, we conclude that the class of Q^- is the inverse of $[Q]$.

Now we can define the "product" of two equivalence classes $[Q_1]$ and $[Q_2]$ by setting $[Q_1][Q_2] = [Q_3]$ if the classes of Q_1, Q_2, and Q_3^- are collinear. It remains to show that the group axioms are verified.

Neutral Element. The first axiom to check is that $[Q][Q_0] = [Q]$. But this is just the claim that the classes of Q_0, Q and Q^- are collinear (Lemma 3.23lemmacount.3.23).

Inverse Elements. We have already seen (Lemma 3.23lemmacount.3.23) that the inverse element of $[Q]$, where $Q = (A, B, C)$, is the class of the form $Q^- = (A, -B, C)$.

Commutativity. The fact that composition is abelian follows from the observation that if the classes of Q_1, Q_2, Q_3 are collinear, then so are the permutations of theses classes (Lemma 3.22lemmacount.3.22).

Associativity. This is the axiom that is the most difficult to check given primitive quadratic forms Q_1, Q_2, Q_3 of discriminant Δ, we have to show that $([Q_1][Q_2])[Q_3] = [Q_1]([Q_2][Q_3])$. Setting $[Q_{12}] = [Q_1][Q_2]$ and $[Q_{23}] = [Q_2][Q_3]$, this boils down to showing that if $Q_{12}Q_3Q_4 \sim 1$ and $Q_1Q_{23}Q_5 \sim 1$, then $Q_4 \sim Q_5$.

Our proof of associativity uses Dirichlet composition: for checking that $([Q_1][Q_2])[Q_3] = [Q_1]([Q_2][Q_3])$, we may assume that the representatives Q_i of these classes can be written in the following form (see Prop. 3.18lemmacount.3.18):

$$Q_1 = (A_1, B, A_2A_3C), \qquad Q_2 = (A_2, B, A_1A_3C), \qquad Q_3 = (A_3, B, A_1A_2C).$$

Dirichlet composition then implies that

$$([Q_1][Q_2])[Q_3] = [(A_1A_2A_3, B, C)] = [Q_1]([Q_2][Q_3]).$$

Using the composition algorithms it is now easy to compute group tables for the class groups $\mathrm{Cl}^+(\Delta)$. In fact, class groups with squarefree order are necessarily cyclic; the cyclic group of order n is denoted by (n) in Table 3.1Class groups for negative discriminantstable.3.1 below. For distinguishing between, say, the cyclic group (4) and the bicyclic group $(2, 2)$ it is sufficient to compute the orders of elements.

Δ	$\mathrm{Cl}^+(\Delta)$	Δ	$\mathrm{Cl}^+(\Delta)$	Δ	$\mathrm{Cl}^+(\Delta)$	Δ	$\mathrm{Cl}^+(\Delta)$	Δ	$\mathrm{Cl}^+(\Delta)$
-3	(1)	-43	(1)	-83	(3)	-123	(2)	-163	(1)
-4	(1)	-44	(3)	-84	$(2,2)$	-124	(3)	-164	(8)
-7	(1)	-47	(5)	-87	(6)	-127	(5)	-167	(11)
-8	(1)	-48	(2)	-88	(2)	-128	(4)	-168	$(2,2)$
-11	(1)	-52	(2)	-91	(2)	-131	(5)	-171	(4)
-12	(1)	-51	(2)	-92	(3)	-132	$(2,2)$	-172	(3)
-15	(2)	-55	(4)	-95	(8)	-135	(6)	-175	(6)
-16	(1)	-56	(4)	-96	$(2,2)$	-136	(4)	-176	(6)
-19	(1)	-59	(3)	-99	(2)	-139	(3)	-179	(5)
-20	(2)	-60	(2)	-100	(2)	-140	(6)	-180	$(2,2)$
-23	(3)	-63	(4)	-103	(5)	-143	(10)	-183	(8)
-24	(2)	-64	(2)	-104	(6)	-144	(4)	-184	(4)
-27	(1)	-67	(1)	-107	(3)	-147	(2)	-187	(2)
-28	(1)	-68	(4)	-108	(3)	-148	(2)	-188	(5)
-31	(3)	-71	(7)	-111	(8)	-151	(7)	-191	(13)
-32	(2)	-72	(2)	-112	(2)	-152	(6)	-192	$(2,2)$
-35	(2)	-75	(2)	-115	(2)	-155	(4)	-195	$(2,2)$
-36	(2)	-76	(3)	-116	(6)	-156	(4)	-196	(4)
-39	(4)	-79	(5)	-119	(10)	-159	(10)	-199	(9)
-40	(2)	-80	(4)	-120	$(2,2)$	-160	$(2,2)$	-200	(6)

Table 3.1. Class groups for negative discriminants.

3.6. Class Groups in the Strict and Wide Sense

Where we investigate different definitions of equivalence.

As far as the theory of composition is concerned, there is no difference between forms with positive and forms with negative discriminant. For defining the class group $\mathrm{Cl}^+(\Delta)$, however, we have used the set $\mathcal{F}^+(\Delta)$ of positive definite primitive forms with discriminant Δ if $\Delta < 0$, and the set $\mathcal{F}(\Delta)$ of all primitive forms with discriminant Δ if $\Delta > 0$.

The group $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{F}(\Delta)$ of equivalence classes of primitive forms modulo $\mathrm{SL}_2(\mathbb{Z})$-equivalence contains $\mathrm{Cl}^+(\Delta) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{F}^+(\Delta)$ as a subgroup, but we do not get anything new from this construction since we have $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{F}(\Delta) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{Cl}^+(\Delta)$.

Something more interesting happens if we change the notion of equivalence: call two forms Q and Q' *equivalent* (in the wide sense) if $Q' = Q|_S$ for some matrix $S \in \mathrm{GL}_2(\mathbb{Z})$, where the action of S on Q is defined by the formula

$$Q'(X,Y) = \frac{1}{\det S}\, Q(rX + sY, tX + uY). \tag{3.18}$$

Since $\det S = \pm 1$, we could actually write $\det S$ instead of $\frac{1}{\det S}$, but in more general situations the formula (3.18Class Groups in the Strict and Wide Senseequation.3.6.18) turns out to be the correct one.

Remark. Omitting the factor $\det S$ in (3.18Class Groups in the Strict and Wide Senseequation.3.6.18) leads to a notion of equivalence (see Exercise 1Reduction of Binary Quadratic Formschapter.1.25ExercisesItem.110) used by Lagrange, Legendre, and Gauss; in fact, Gauss called forms which are equivalent with respect to (1.35Exercisesequation.1.8.35) "improperly equivalent". With respect to improper equivalence, the set of equivalence classes does not carry a natural group structure. On the other hand, improperly equivalent forms represent the same integers.

Remark. If two forms Q, Q' are equivalent with respect to $\mathrm{GL}_2(\mathbb{Z})$, it is not necessarily true anymore that Q and Q' represent the same integers. An example is given by the two forms $(1, 0, -3)$ and $(-1, 0, 3)$ with discriminant 12.

The class group in the strict sense, which we have used so far, was defined as

$$\mathrm{Cl}^+(\Delta) = \begin{cases} \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{F}(\Delta) & \text{if } \Delta > 0, \\ \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{F}(\Delta)^+ & \text{if } \Delta < 0. \end{cases}$$

From now on, the strict equivalence class of a form Q will be denoted by $[Q]^+$, and we write $Q \overset{+}{\sim} Q'$ if Q and Q' are $\mathrm{SL}_2(\mathbb{Z})$-equivalent. We now define $\mathrm{Cl}(\Delta)$ as the set of (wide) equivalence classes with respect to the action of $\mathrm{GL}_2(\mathbb{Z})$:

$$\mathrm{Cl}(\Delta) = \mathrm{GL}_2(\mathbb{Z})\backslash\mathcal{F}_\Delta.$$

The wide equivalence class of a form Q will be denoted by $[Q]$.

For a primitive quadratic form $Q = (A, B, C)$, set $-Q = (-A, -B, -C)$ and $Q^{-1} = (A, -B, C)$, as well as $Q^* = -Q^{-1} = (-A, B, -C)$. Observe that

$$Q^* = Q|_R \quad \text{for} \quad R = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{SL}_2(\mathbb{Z}). \tag{3.19}$$

In fact, since $\mathrm{SL}_2(\mathbb{Z})$ has index 2 in $\mathrm{GL}_2(\mathbb{Z})$, the matrix R represents the nontrivial coset of $\mathrm{GL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})$.

Lemma 3.25. *If Q is a positive definite primitive form with negative discriminant $\Delta < 0$, then $[Q]$ is the disjoint union of the $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes $[Q]^+$ and $[Q^*]^+$:*

$$[Q] = [Q]^+ \cup [Q^*]^+.$$

Proof. The equivalence class containing Q contains only positive definite forms, the one containing Q^* only negative definite forms; this shows that the classes are disjoint. Moreover, $Q \sim Q^* = Q|_R$ by (3.19Class Groups in the Strict and Wide Senseequation.3.6.19), so $[Q]$ contains both $[Q]^+$ and $[Q^*]^+$. Since $\mathrm{SL}_2(\mathbb{Z})$ has index 2 in $\mathrm{GL}_2(\mathbb{Z})$, the coset $[Q]$ splits into at most two cosets, and this completes the proof. □

The projection map $\pi : \mathrm{Cl}^+(\Delta) \longrightarrow \mathrm{Cl}(\Delta)$ sending $[Q]^+$ to $[Q]$ is clearly surjective. For negative discriminants, Lemma 3.25lemmacount.3.25 shows that π is bijective. For positive discriminants, we will use π for giving $\mathrm{Cl}(\Delta)$ a group structure: given two classes $[Q_1]$ and $[Q_2]$, set $[Q_1][Q_2] = \pi([Q_1]^+[Q_2]^+)$. We only have to show that this is well defined. In fact, pulling a class $[Q_1]$ back to $\mathrm{Cl}^+(\Delta)$ can be done in two different ways: we have $\pi([Q_1]^+) = [Q_1]$ as well as $\pi([Q_1^*]^+) = [Q_1]$; all other preimages of Q_1 differ from Q_1 and Q_1^* only by $\mathrm{SL}_2(\mathbb{Z})$-equivalence. What we have to show is that, say, $\pi([Q_1]_+[Q_2]_+) = \pi([Q_1^*]_+[Q_2]_+)$, which in turn would follow from the fact that $Q_1Q_2Q_3 \overset{+}{\sim} 1$ implies $Q_1^*Q_2Q_3^* \overset{+}{\sim} 1$. Since $Q_1^* \overset{+}{\sim} -Q_1^{-1}$, this is equivalent to $(-Q_1^{-1})Q_2(-Q_3^{-1}) \overset{+}{\sim} 1$, or, by inverting the relation, to $(-Q_1)Q_2^{-1}(-Q_3) \overset{+}{\sim} 1$. This follows from the following

Proposition 3.26. *If Q_1, Q_2, Q_3 are primitive binary quadratic forms with discriminant $\Delta > 0$, then $Q_1Q_2Q_3 \overset{+}{\sim} 1$ if and only if $(-Q_1)(-Q_2)(Q_3^{-1}) \overset{+}{\sim} 1$.*

Proof. Let $\mathcal{A}$ be a cube with $Q_i = Q_i^{\mathcal{A}}$. Let $\mathcal{B}$ be the cube you get from $\mathcal{A}$ by switching the front and the back faces, then (see p. 72From Cubes to FormsItem.178) $Q_1^{\mathcal{B}} = -Q_1$, $Q_2^{\mathcal{B}} = -Q_2$, and $Q_3^{\mathcal{B}} = Q_3^{-1}$. □

Since we have used π to give $\mathrm{Cl}(\Delta)$ a group structure, the map $\pi : \mathrm{Cl}^+(\Delta) \longrightarrow \mathrm{Cl}(\Delta)$ becomes a surjective group homomorphism. Clearly π is an isomorphism if $\Delta < 0$, and $\ker \pi$ is generated by the class $[Q^*]^+$ if $\Delta > 0$. In other words: $\mathrm{Cl}^+(\Delta) \simeq \mathrm{Cl}(\Delta)$ if and only if $[Q^*]^+ = [Q]^+$. This condition is equivalent to the solvability of the "Anti-Pell" equation $Q_0(T,U) = -1$:

Lemma 3.27. *Let Δ be a positive nonsquare discriminant and Q a form with discriminant Δ. Then $[Q^*]^+ = [Q]^+$ if and only if there exists an integral solution of the equation $Q_0(T,U) = -1$.*

Proof. Write $Q = (A,B,C)$ and $Q^* = (-A,B,-C)$. Then $Q \sim Q^*$ is equivalent to the existence of a matrix $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $Q^* = Q|_S$; using $M(Q) = \left(\begin{smallmatrix} 2A & B \\ B & 2C \end{smallmatrix}\right)$, this relation can be written in the form

$$\begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} u & -t \\ -s & r \end{pmatrix} \begin{pmatrix} -2A & B \\ B & -2C \end{pmatrix}.$$

This matrix equation is equivalent to the three equations

$$A(r+u) = -Bt, \qquad As = Ct, \qquad C(r+u) = -Bs.$$

From $A \mid Bt$ and $A \mid Ct$ we deduce that $A \mid t$: this follows from the fact that Q is primitive, i.e., that $\gcd(A,B,C) = 1$. Thus $t = AU$ for some integer U, and consequently $s = CU$. Now we distinguish two cases:

1. $\Delta = 4m$: from $B \equiv \Delta \bmod 2$ we see that B is even. From $A(r+u) = -Bt = -BAU$ we get $r + u = -BU$, hence $r \equiv u \bmod 2$. Thus we may set $r - u = 2T$ for some integer T. This finally gives us the equations

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} T - \frac{B}{2}U & CU \\ AU & -T - \frac{B}{2}U \end{pmatrix}, \tag{3.20}$$

we well as $1 = ru - st = -T^2 + mU^2$, that is:

$$T^2 - mU^2 = -1. \tag{3.21}$$

Thus every $S \in \mathrm{SL}_2(\mathbb{Z})$ transforming Q into Q^* comes from an integral solution of the Anti-Pell equation (3.21Class Groups in the Strict and Wide Senseequation.3.6.21), and conversely, every integral solution of (3.21Class Groups in the Strict and Wide Senseequation.3.6.21) gives rise to such an S.

2. $\Delta = 4m+1$: then $B \equiv \Delta \bmod 2$ is odd, hence $r - u \equiv U \bmod 2$. Thus we can write $r - u = 2T + U$ for some $T \in \mathbb{Z}$, and then we get $r = T + \frac{1-B}{2}U$, $u = -T - \frac{1+B}{2}U$, and $1 = ru - st = T^2 + TU + U^2\frac{1-B^2}{4} + ACU^2 = -T^2 - TU + mU^2$. Collecting everything we get
$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} T + \frac{1-B}{2}U & CU \\ AU & -T - \frac{1+B}{2}U \end{pmatrix}, \tag{3.22}$$
we well as
$$T^2 + TU - mU^2 = -1. \tag{3.23}$$
$\square$

We have shown:

Theorem 3.28. *The projection map π is bijective if $\Delta < 0$, or if $\Delta > 0$ and the equation $Q_0(T,U) = -1$ is solvable in integers; in all other cases, every class in the wide sense is the union of two classes in the strict sense.*

Proof. If the equations (3.21Class Groups in the Strict and Wide Senseequation.3.6.21) and (3.21Class Groups in the Strict and Wide Senseequation.3.6.21) do not have integral solutions, the two classes $[Q_0]^+$ and $[Q_0^*]^+$ are distinct, but become equal in the wide class group: $[Q_0] = [Q_0^*]$. $\square$

Δ	$\mathrm{Cl}(\Delta)$	$\mathrm{Cl}^+(\Delta)$	Δ	$\mathrm{Cl}(\Delta)$	$\mathrm{Cl}^+(\Delta)$	Δ	$\mathrm{Cl}(\Delta)$	$\mathrm{Cl}^+(\Delta)$
5	(1)	(1)	41	(1)	(1)	85	(1)	(2)
8	(1)	(1)	44	(1)	(2)	88	(1)	(2)
12	(1)	(2)	53	(1)	(1)	89	(1)	(1)
13	(1)	(1)	56	(1)	(2)	93	(1)	(2)
17	(1)	(1)	57	(1)	(2)	92	(1)	(2)
21	(1)	(2)	60	(2)	(2, 2)	97	(1)	(1)
24	(1)	(2)	61	(1)	(1)	101	(1)	(1)
28	(1)	(2)	65	(1)	(2)	104	(2)	(2)
29	(1)	(1)	69	(1)	(2)	105	(2)	(2, 2)
33	(1)	(2)	73	(1)	(1)	109	(1)	(1)
37	(1)	(1)	76	(1)	(2)	120	(2)	(2, 2)
40	(2)	(2)	77	(1)	(2)	136	(2)	(4)

Table 3.2. Class groups in the wide and the strict sense.

Theorem 3.28lemmacount.3.28 gives us an exact sequence
$$1 \longrightarrow K_\Delta \longrightarrow \mathrm{Cl}^+(\Delta) \xrightarrow{\ \pi\ } \mathrm{Cl}(\Delta) \longrightarrow 1,$$
where $\ker \pi = K_\Delta$ is the group generated by the class of Q_0^*. In particular, we have
$$K_\Delta \simeq \begin{cases} 1 & \text{if } Q_0(T,U) = -1 \text{ is solvable,} \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

The structure of $\mathrm{Cl}^+(\Delta)$ does in general not only depend on the structure of $\mathrm{Cl}(\Delta)$ and K_Δ. In fact, if $\mathrm{Cl}(\Delta) \simeq (2,4)$ and $h^+(\Delta) = 16$, then $\mathrm{Cl}^+(\Delta)$ is isomorphic to exactly one of the groups $(2,2,4)$, $(4,4)$ or $(2,8)$. In the first case, $\mathrm{Cl}^+(\Delta)$ is the direct product of $\mathrm{Cl}(\Delta)$ and the group of order 2; in the other two cases, the class in the kernel of π is a square in $\mathrm{Cl}^+(\Delta)$.

Proposition 3.29. *Let $\Delta > 0$ be a discriminant, and assume that $Q_0(T,U) = -1$ is not solvable in integers. Then $\mathrm{Cl}^+(\Delta) \simeq \mathrm{Cl}(\Delta) \times \mathbb{Z}/2\mathbb{Z}$ if and only if Δ is not a sum of two squares.*

Proof. We have $\mathrm{Cl}^+(\Delta) \simeq \mathrm{Cl}(\Delta) \times \mathbb{Z}/2\mathbb{Z}$ if and only if the $[Q_0^*]$ is not a square, that is, if and only if Q_0^* represents a square coprime to Δ. If $\Delta = 4m$ (we leave the case $\Delta = 4m+1$ to the reader), this happens if and only if $-x^2+my^2 = z^2$ for some z coprime to $2m$. Thus $my^2 = x^2 + z^2$, and since x and z can be chosen to be coprime, m divides a sum of two coprime squares and therefore is itself a sum of two squares by Cor. 1.10lemmacount.1.10.

Conversely, assume that $m = a^2+b^2$. Then $-a^2+m\cdot 1^2 = b^2$ shows that Q_0^* represents a square, which in turn implies that the class $[Q_0^*] = c^2$ is a square. Thus c has order 4 in $\mathrm{Cl}^+(\Delta)$, but has order 2 in $\mathrm{Cl}(\Delta)$. This implies the claim. □

3.7. Nonfundamental Discriminants

Where residue class groups make a surprising appearance.

In this section we will study the class group of primitive forms whose discriminant Δ is not fundamental, that is, which can be written in the form $\Delta = \Delta_0 N^2$ for some (fundamental) discriminant Δ_0. In the first part, we treat the special case where $\Delta = N^2$ is a perfect square.

2.6.1. Square Discriminants

Although basically all interesting applications of the theory of binary quadratic forms concern nonsquare discriminants, Gauss also studied forms whose discriminants are squares (he even considered the case where $\Delta = 0$, which we exclude). It will follow from the discussion below that every primitive form with discriminant $\Delta = 64$ is equivalent to one of $(A,8,0)$ with $A = 1,3,5,7$, and that composition means multiplying the leading coefficient modulo 8.

Lemma 3.30. *Every primitive form of discriminant $\Delta = N^2$ primitively represents* 0.

Proof. Multiplying $Q(x,y) = Ax^2+Bxy+Cy^2 = 0$ through by $4A$ and completing the square we get $(2Ax+By)^2 - \Delta y^2 = 0$, that is, $(2Ax+By)^2 = (Ny)^2$. The equation $2Ax+By = Ny$ has the solution $x = N-B$ and $y = 2A$; cancelling common factors of x and y we get a primitive solution of $Q(x,y) = 0$. □

Forms that primitively represent 0 are equivalent to forms $(0,B,C)$ and (apply a flip) $(A,B,0)$. Since $N^2 = \Delta = B^2-4AC = B^2$, we must have $B = \pm N$. The following lemma shows that we can always choose $B = N$:

Lemma 3.31. *For any primitive form $Q = (A,N,0)$ there is an $S \in \mathrm{SL}_2(\mathbb{Z})$ such that $Q|_S = (A',-N,0)$, where $AA' \equiv 1 \bmod N$.*

Proof. Since $\gcd(A,N) = 1$, there is an integer A' with $AA' \equiv 1 \bmod N$; we write $AA'-Nt = 1$, and set $S = \left(\begin{smallmatrix} A' & -N \\ -t & A \end{smallmatrix}\right)$. Then $S \in \mathrm{SL}_2(\mathbb{Z})$, and we have $Q|_S = (A_1,B_1,C_1)$ with

$$\begin{aligned} A_1 &= A'(AA'-Nt) = A', \\ B_1 &= -2AA'N + N(AA'+Nt) = -N, \\ C_1 &= AN^2 - N^2A = 0. \end{aligned}$$

This proves the claim. □

Our next result will tell us how to define reduced forms with square discriminants:

Lemma 3.32. *Every primitive form of discriminant $\Delta = N^2$ is equivalent to a unique form $Q = (A, N, 0)$ with $0 < A < N$.*

Proof. Every primitive form with discriminant N^2 represents zero, hence is equivalent to some form $(A, N, 0)$. We claim that we can choose $0 < A < N$. In fact, applying $S = \left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right)$ we find $(A, N, 0)|_S = (A', B', C')$, where

$$A' = A + Nt, \qquad B' = N, \qquad \text{and} \quad C = 0.$$

By choosing t appropriately we can make sure that $0 < A' < N$ as claimed.

It remains to prove that if $(A, N, 0) \sim (A', N, 0)$ with $0 < A, A' < N$, then $A = A'$. Assume therefore that $(A, N, 0)|_S = (A', N, 0)$. Then

$$\begin{aligned} A' &= Ar^2 + Nrt = r(Ar + Nt), \\ N &= 2Ars + N(ru + st), \\ 0 &= As^2 + Nsu = s(As + Nu). \end{aligned}$$

If $s = 0$, then $1 = ru + st = ru$, hence $r = u = 1$ or $r = u = -1$; from $A' = A \pm Nt$ we get $A' \equiv A \bmod N$, hence $A' = A$ since we have assumed that $0 < A, A' < N$.

If $As + Nu = 0$, then $s = -\lambda N$ and $u = \lambda A$ for some integer λ. From $ru - st = 1$ we then deduce that $\lambda = \pm 1$; replacing S by $-S$ we may in fact assume that $\lambda = 1$. Then $s = -N$, $u = A$, $rA + Nt = 1$, and $N = -2ArN + N(rA - Nt) = -N(Ar + Nt) = -N$, which is only possible if $N = 0$, a case we have excluded. $\square$

We will call a form $Q = (A, B, C)$ with discriminant $\Delta = N^2$ reduced if $B = N > 0$ and $C = 0$.

Since there are exactly $\phi(N)$ coprime residue classes modulo N, we get

Corollary 3.33. *If $\Delta = N^2$, then $h^+(\Delta) = \phi(N)$.*

Now we can determine the structure of $\mathrm{Cl}^+(\Delta)$ for square discriminants $\Delta = N^2$. First observe that the principal form is the one representing 1; from $Ax^2 + Nxy = 1$ we immediately deduce $x = \pm 1$, hence $A \equiv 1 \bmod N$. This shows that the principal class is the one containing the form $(1, N, 0)$. More generally, we have

Theorem 3.34. *Let $\Delta = N^2$ be a square. The map $\gamma : \mathrm{Cl}^+(\Delta) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$ defined by $(A, N, 0) \longmapsto A + N\mathbb{Z}$ is a group isomorphism.*

Proof. Clearly γ is surjective, and since both groups have the same order, γ is bijective. Dirichlet composition immediately shows that $(A, N, 0)$, $(A', N, 0)$ and $(AA', -N, 0)$ are collinear. $\square$

The observation that $\mathrm{Cl}(N^2) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$ shows that class groups for square discriminants are not very interesting. On the other hand, we will see below that this results can be generalized to give a similarly explicit description of the "new class group" $\mathrm{Cl}(\Delta N^2)/\mathrm{Cl}(\Delta)$, and this piece of the class group has several important applications in algorithmic number theory and cryptography.

The primes represented by a form with square discriminant are easy to describe:

Proposition 3.35. *Let $Q = (A, N, 0)$ be a primitive form with discriminant $\Delta = N^2$, where N is a positive integer. Then Q represents the primes $p \equiv A, A^{-1} \bmod N$.*

Proof. If $Q(x, y) = p$, then $x \mid p$. If $x = \pm 1$, then $p = A \pm Ny$, and this is equivalent to $p \equiv A \bmod N$. If $x = \pm p$, then $p = Ap^2 \pm Npy$ gives $1 = Ap \pm Ny$, which has an integral solution if and only if $p \equiv A^{-1} \bmod N$. $\square$

2.6.2. Nonfundamental Discriminants

We have seen above that the class group of forms with square discriminants is isomorphic to a residue class group. Something similar will happen in general for class groups of primitive forms with discriminant $\Delta = \Delta_0 N^2$: the "new part" of the class group is understood very well.

Given a form Q of discriminant Δ and a matrix $S \in \mathrm{SL}_2(\mathbb{Z})$ we know that the form $Q' = Q|_S$ also has discriminant Δ. If $\det S = N$, on the other hand, then $\mathrm{disc}(Q|_S) = \Delta N^2$. It is therefore natural to ask whether every primitive form Q' of discriminant ΔN^2 is the result of transforming a form with discriminant Δ with a matrix of determinant N. It turns out that the answer is yes. The following trivial observation will be used quite often below:

Lemma 3.36. *Every primitive form Q with discriminant ΔN^2 is equivalent to a form (A, BN, CN^2) with* $\gcd(A, N) = 1$.

Proof. Every primitive form with discriminant ΔN^2 represents an integer A coprime to $2N$, hence is equivalent to a form (A, B', C'). Applying a shift we can change this into (A, B'', C'') with $B'' = B' + 2As$; since $\gcd(A, N) = 1$, we can choose s in such a way that $B'' = BN$. From $\Delta N^2 = B^2N^2 - 4AC''$ we deduce that $N^2 \mid 4C''$, hence $N^2 \mid C$ whenever N is odd.

If N is even, there are two cases:

1. $\Delta \equiv 0 \bmod 4$. Here we choose $B'' = 2BN$ and find $\Delta N^2 = 4B^2N^2 - 4AC''$, hence $4N^2 \mid 4AC''$ and finally $N^2 \mid C''$.
2. $\Delta \equiv 1 \bmod 4$. Here we choose $B'' = BN$ for some odd value of B, which is possible since $B' \equiv \Delta \bmod 2$ is odd, too. Then $N^2(\Delta - B^2) = -4AC'N^2$ is divisible by $4N^2$, hence $N^2 \mid C''$.

This proves our claim in all cases. □

The same argument (or the application of a flip) shows

Corollary 3.37. *Every primitive form Q with discriminant ΔN^2 is equivalent to a form (AN^2, BN, C) with* $\gcd(C, N) = 1$.

It seems to be largely irrelevant whether we prefer to work with forms (A, BN, CN^2) or rather with (AN^2, BN, C). Our composition algorithms, however, are not invariant under flipping forms since they all use $e = \gcd(A_1, A_2, B)$. It turns out that for composing derived forms (see Thm. 3.47lemmacount.3.47), the second choice is to be preferred.

Congruence Subgroups. Next we investigate how elements of $\mathrm{SL}_2(\mathbb{Z})$ must look like if they transform quadratic forms of type (A, BN, CN^2) into $(A', B'N, C'N^2)$. This is a straightforward calculation:

Lemma 3.38. *Let $Q = (A, BN, CN^2)$ be a primitive form, and set $Q' = Q|_S$ for some $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then the following assertions are equivalent:*

1. *$Q' = (A', B'N, C'N^2)$ for integers A', B', C'.*
2. *$s \equiv 0 \bmod N$.*

Proof. If Q' has the given form, then $C'N^2 = As^2 + BNsu + CN^2u^2$: since Q is primitive, $\gcd(A, N) = 1$, and then $N \mid As^2$ implies $N \mid s^2$. In fact, we must have $N \mid s$; using induction, we shall prove that $p^a \mid N$ implies $p^a \mid s$. Clearly $p \mid N$ implies $p \mid s$. Assume the claim holds for some $a \geq 1$, and suppose that $p^{a+1} \mid N$; then $p^a \mid s$ by induction assumption, so $p^{2a+1} \mid Ns$ and thus $p^{2a+1} \mid s^2$: but then $p^{a+1} \mid s$.

The converse (2. $\Longrightarrow$ 1.) is equally clear. □

We now consider the map sending the equivalence class of a form (A, BN, CN^2) with discriminant $\varDelta N^2$ to a suitable class of the form (A, B, C) with discriminant $\varDelta$. To this end we first have to study the effect of some $S \in \mathrm{SL}_2(\mathbb{Z})$ on A, B and C:

Lemma 3.39. *Assume that $Q = (A, BN, CN^2)$ and $Q' = (A', B'N, C'N^2)$ are primitive quadratic forms with discriminant $\varDelta N^2$, and that $Q' = Q|_S$ for some $S = \left(\begin{smallmatrix} r & Ns \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then $(A', B', C') = (A, B, C)|_T$ for $T = \left(\begin{smallmatrix} r & s \\ Nt & u \end{smallmatrix}\right)$.*

Proof. We find

$$\begin{aligned} A' &= Ar^2 + BNrt + CN^2t^2, \\ B'N &= 2(ArNs + CN^2tu) + BN(ru + Nst), \\ C'N^2 &= AN^2s^2 + BN^2su + CN^2u^2, \end{aligned}$$

so cancelling the powers of N yields

$$\begin{aligned} A' &= Ar^2 + BrNt + C(Nt)^2, \\ B' &= 2(Ars + CNtu) + B(ru + sNt), \\ C' &= As^2 + Bsu + Cu^2. \end{aligned}$$

This implies the claim. □

Let us now introduce the subgroups

$$\Gamma^0(N) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad N \mid s \right\} \quad \text{and} \quad \Gamma_0(N) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad N \mid t \right\}$$

of $\mathrm{SL}_2(\mathbb{Z})$. Two forms Q, Q' are called $\Gamma_0(N)$-equivalent if there is an $S \in \Gamma_0(N)$ such that $Q' = Q|_S$. The equivalence class of a primitive form $Q = (A, B, C)$ with discriminant $\varDelta$ and last coefficient C coprime to N will be denoted by $[Q]_{[N]}$, and the set of such equivalence classes by $\mathrm{Cl}^+_{[N]}(\varDelta)$; in particular, we have $\mathrm{Cl}^+(\varDelta) = \mathrm{Cl}^+_{[1]}(\varDelta)$.

Sending the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of (A, BN, CN^2) in $\mathrm{Cl}(\varDelta N^2)$ to the $\Gamma_0(N)$-equivalence class of (A, B, C) in $\mathrm{Cl}^+_{[N]}(\varDelta)$ defines a map $\lambda : \mathrm{Cl}^+(\varDelta N^2) \longrightarrow \mathrm{Cl}^+_{[N]}(\varDelta)$.

Observe that λ is well defined: if we have $(A, BN, CN^2) \sim (A', B'N, C'N^2)$ then (A, B, C) and (A', B', C') are equivalent with respect to $\Gamma_0(N)$ by Lemma 3.39lemmacount.3.39.

Theorem 3.40. *The set $\mathrm{Cl}^+_{[N]}(\varDelta)$ can be given a group structure in such a way that the natural map $\lambda : \mathrm{Cl}^+(\varDelta N^2) \longrightarrow \mathrm{Cl}^+_{[N]}(\varDelta)$ becomes an isomorphism of groups.*

Proof. We first show that λ is bijective.

1. λ is onto: given a class in $\mathrm{Cl}^+_{[N]}(\varDelta)$ represented by a form (A, B, C) with $\gcd(A, N) = 1$, the class of (A, B, C) is the image of the class of (A, BN, CN^2).

2. λ is injective: assume that $Q = (A, BN, CN^2)$ and $Q' = (A', B'N, C'N^2)$ have the same image; then (A, B, C) and (A', B', C') are equivalent with respect to some $T = \left(\begin{smallmatrix} r & s \\ Nt & u \end{smallmatrix}\right) \in \Gamma_0(N)$, and this implies that $S' = Q|_S$ for $S = \left(\begin{smallmatrix} r & Ns \\ t & u \end{smallmatrix}\right)$. Thus $Q \sim Q'$ as claimed.

It remains to give $\mathrm{Cl}^+_{[N]}(\varDelta)$ a group structure and verify that λ is a group homomorphism.

To this end, take two quadratic forms $Q_1 = (A_1, B_1, C_1)$ and $Q_2 = (A_2, B_2, C_2)$, and assume that $\gcd(A_1A_2, N) = 1$. For composing Q_1 and Q_2, we set $e = \gcd(A_1, A_2, B)$, where $B = \frac{1}{2}(B_1 + B_2)$, define integers $a = 0$, $b = A_1/e$, $c = A_2/e$ and $d = B/e$, and determine integers f, g, h as solutions of the diophantine equations $bg - cf = \frac{1}{2}(B_1 - B_2)$

and $fd-bh = C_2$. Then $Q_1Q_2Q_3 \sim 1$ for the three forms attached to the cube represented by the composition matrix $\mathcal{M} = \left(\begin{smallmatrix} 0 & b & c & d \\ e & f & g & h \end{smallmatrix}\right)$.

Now let us similarly compose the derived forms $Q_1^* = (A_1, B_1N, C_1N^2)$ and $Q_2^* = (A_2, B_2N, C_2N^2)$. We find $e^* = \gcd(A_1, A_2, \frac12(B_1+B_2)N) = e$ because $\gcd(A_1A_2, N) = 1$, and set $a^* = 0 = a$, $b^* = A_1/e = b$, $c^* = A_2/e = c$ and $d^* = BN/e = dN$. Then we solve the diophantine equations $b^*g^* - c^*f^* = \frac12(B_1-B_2)N$ and $f^*d^* - b^*h^* = C_2N^2$. These can be written in the form $bg^* - cf^* = \frac12(B_1-B_2)N$ and $f^*dN - bh^* = C_2N^2$, hence we can simply choose $f^* = Nf$, $g^* = Ng$ and $h^* = N^2h$. This shows that the composition matrix for the derived forms can be written as $\mathcal{M}^* = \left(\begin{smallmatrix} 0 & b & c & Nd \\ e & Nf & Ng & N^2h \end{smallmatrix}\right)$. The third form attached to this matrix is $Q_3^* = (A_3, NB_3, NC_3^2)$. Thus we have shown that $Q_1Q_2Q_3 \sim 1$ implies $Q_1^*Q_2^*Q_3^* \sim 1$, and the converse is equallly clear.

Associativity of composition in $\mathrm{Cl}^+_{[N]}(\Delta)$ is a consequence of the fact that the formulas for composing forms are essentially the same: we have shown that $(Q_1*Q_2)^* = Q_1^* * Q_2^*$, i.e., that deriving commutes with composition. This implies that $(Q_1^*Q_2^*)Q_3^* = ((Q_1Q_2)Q_3)^* = (Q_1(Q_2Q_3))^* = Q_1^*(Q_2^*Q_3^*)$. □

If we had used forms (AN^2, BN, C) in the proof of Thm. 3.40lemmacount.3.40, we would have had to compute $e^* = \gcd(AN^2, A'N^2, \frac12(B+B')N) = N\cdot\gcd((AN, A'N, \frac12(B+B'))$. In this case, e^* is divisible by N and divides N^2, and composition is complicated by the fact that we cannot give e exactly. For this reason, we have used forms of the type (A, BN, CN^2) here. Below we will use forms of the type (Ap^2, Bp, C); the isomorphism between $\Gamma^0(N)$ and $\Gamma_0(N)$ (see Ex. 3Bhargava's Cubeschapter.3.21ExercisesItem.227) extends to an isomorphism of the class groups of forms with respect to $\Gamma^0(N)$-equivalence and $\Gamma_0(N)$-equivalence. Thus the $\Gamma^0(N)$-equivalence classes of forms (A, B, C) with C coprime to N are in bijection with the usual equivalence classes of forms with discriminant ΔN^2 represented by forms (AN^2, BN, C).

Derived Forms. If Q is a form with discriminant Δ and $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ a 2×2-matrix with integral entries and determinant p, then $Q|_S = Q(rX+sY, tX+uY)$ is a quadratic form with discriminant Δp^2. In the following, we will show that representatives for the equivalence classes of forms with discriminant Δp^2 can be generated by at most $p+1$ carefully chosen matrices $S = P_0, P_1, \ldots, P_{p-1}, P_\infty$. For the indices j of these matrices P_j we will be using the set $\mathbb{P}^1\mathbb{F}_p$.

Lemma 3.41. *Let R be a matrix with integral coefficients and prime determinant p. Then there is some $S \in \mathrm{SL}_2(\mathbb{Z})$ such that $RS^{-1} = P_k$, where*

$$P_k = \begin{pmatrix} p & k \\ 0 & 1 \end{pmatrix}, \quad k = 0, 1, \ldots, p-1; \quad \text{and} \quad P_\infty = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}.$$

Also, $P_k = \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)P_0$.

Proof. Given R, we have to find some $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and an index $k \in \mathbb{P}^1\mathbb{F}_p$ such that $R = P_kS$. Write $R = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. The equation $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} p & k \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ yields the four equations $a = pr + bt$, $b = ps + ku$, $c = t$ and $d = u$.

If $\gcd(c, d) = 1$, set $t = c$, $u = d$, and find integers t and u such that $ru - st = 1$. Then $p(ru - st) = p = ad - bc = au - bt$ implies $u(a - pr) = t(b - ps)$, and since $\gcd(t, u) = 1$ we must have $t \mid (a - pr)$. Thus we can write $a - pr = kt$ for some $k \in \mathbb{Z}$, and plugging this into $u(a - pr) = t(b - ps)$ we get $b = ps + ku$ as desired. It remains to show that we can choose $0 \le k < p$. Write $k = m + pn$ with $0 \le m < p$; then $\left(\begin{smallmatrix} 1 & k \\ 0 & p \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & m \\ 0 & p \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, and our claim follows upon replacing $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$.

If $\gcd(c, d) > 1$, then $ad - bc = p$ implies that we must have $\gcd(c, d) = p$. Set $a = -t$, $b = -u$, $c = pr$ and $d = ps$; then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ for $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. □

Given a primitive form (A, B, C) with discriminant Δ we can write down a form (A, BN, CN^2) with discriminant ΔN^2. We have already seen that every form with discriminant ΔN^2 can be generated in this way; now we have to investigate which of these forms are primitive, and which primitive forms are equivalent. To this end, we restrict our attention to one prime at a time.

Lemma 3.42. *Let $Q = (A, B, C)$ be a primitive quadratic form with discriminant Δ, and let $P = P_k$ run through the matrices with determinant p introduced above. Then among the forms $Q_k = Q|_{P_k}$, there are exactly $p - (\frac{\Delta}{p})$ primitive forms.*

If we assume that $p \nmid A$, then we have more precisely:

1. *If $(\frac{\Delta}{p}) = -1$, then all $p+1$ forms $Q|_P$ are primitive.*
2. *If $(\frac{\Delta}{p}) \neq -1$, then $\Delta \equiv b^2 \bmod p$ for some integer b. For $p \neq 2$, the imprimitive forms are given by $k_1 = [-\frac{B-b}{2}, A]$ and $k_2 = [-\frac{B+b}{2}, A]$. Observe that $k_1 = k_2$ if and only if $b \equiv 0 \bmod p$, that is, if and only if $p \mid \Delta$; moreover, $k_1 = k_2 = [-B : A]$ in this case.*

Proof. We can choose $Q = (A, B, C)$ in such a way that $p \nmid A$. Observe that $p \mid C$ implies $p \mid \Delta$ or $(\Delta/p) = +1$.

- The form $Q|_{P_\infty} = (Ap^2, Bp, C)$ is imprimitive if and only if $p \mid C$.
- The form $Q|_{P_k} = (A + kB + k^2C, p(B + 2Ck), p^2C)$ is imprimitive if and only if $p \mid (A + kB + k^2C)$. If $p \mid C$, this happens if and only if $kB \equiv -A \bmod p$, that is, for $k = [-B : A]$. Assume from now on that $p \nmid C$.
  If p is odd, then $A + kB + k^2C \equiv 0 \bmod p$ is equivalent to $(2A + kB)^2 \equiv k^2\Delta \bmod p$ since $p \nmid A$. This congruence has no solution if $(\Delta/p) = -1$. Assume therefore that $\Delta \equiv b^2 \bmod p$. Then $(2A + kB)^2 \equiv (kb)^2 \bmod p$ implies that $2A + kB \equiv \pm kb \bmod p$, hence $k(B \pm b) \equiv -2A \bmod p$. This gives $k_1 = [-\frac{B-b}{2}, A]$ and $k_2 = [-\frac{B+b}{2}, A]$. Here $B \equiv \pm b \bmod p$ if and only if $B^2 \equiv b^2 \equiv \Delta \bmod p$, which in turn is equivalent to $p \mid C$. In this case, we can choose the sign of b in such a way that $B \equiv b \bmod p$; then $k_1 = [0 : 1]$ and $k_2 = [-B : A]$, which agrees with our results above.
  Now assume that $p = 2$. The forms derived from (A, B, C) are $(4A, 2B, C)$, $(A, 2B, 4C)$, and $(A + B + C, 2(B + 2C), 4C)$. The second form is always primitive.
  1. $\Delta \equiv 1 \bmod 4$. Here B is odd; the first form is primitive if and only if C is odd, and the third form is primitive if and only if $A + B + C$ is odd, which happens if and only if C is odd. Thus there are no imprimitive forms if C is odd (which is equivalent to $\Delta = B^2 - 4AC \equiv 1 - 4 \equiv 5 \bmod 8$), and two imprimitive forms if C is even, that is, if $\Delta \equiv 1 \bmod 8$.
  2. $\Delta \equiv 0 \bmod 4$. Here B is even; the first form is primitive if and only if C is odd, and the third form is primitive if and only if $A+B+C$ is odd, that is, if and only if C is even. Thus there is exactly one imprimitive form.

In all cases, there are exactly $2 - (\frac{\Delta}{2})$ primitive forms. □

Example 1. Let $\Delta = 5$ and $p = 2$. There is only one Zagier reduced form with discriminant 5, namely $Q = (1, 3, 1)$. We find $Q_\infty = (4, 6, 1)$, $Q_0 = (1, 6, 4)$, $Q_1 = (5, 10, 4)$ and $Q_2 = (11, 14, 4)$. All derived forms are equivalent.

Example 2. Let $\Delta = 5$ and $p = 3$. The derived forms are $Q_\infty = (9, 9, 1)$, $Q_0 = (1, 9, 9)$, $Q_1 = (5, 15, 9)$, and $Q_2 = (11, 21, 9)$. Both Q_∞ and Q_0 are equivalent to the principal form $(1, 7, 1)$. The forms Q_1 and Q_2 are both reduced and belong to the same cycle.

The matrix $S = (\begin{smallmatrix} 0 & -1 \\ 1 & 3 \end{smallmatrix})$ is an automorph of Q, and we have $Q_\infty|_S = (1, -3, -9) \sim (1, 7, 1)$ and $Q_1|_S = (9, 39, 41) \sim Q_1$. Thus S acts trivially on the classes of the derived forms.

The permutation on the P_k defined by S is given by the following table:

k	∞	0	1	2
m	0	∞	2	1

Observe that $Q_\infty|_S = Q_0$ for the matrix $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 9 \end{smallmatrix}\right)$. Thus $P_\infty S P_0^{-1} = S'$ must be an automorph of Q. In fact, $S' = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 3 \end{smallmatrix}\right)$.

It remains to investigate how many of the $p - (\frac{\Delta}{p})$ primitive forms are equivalent to each other. Any form with discriminant Δp^2 is equivalent to Q_k for some $k \in \mathbb{P}^1\mathbb{F}_p$. Among these forms there are exactly $p - (\frac{\Delta}{p})$ primitive forms. We now have to check which of these forms are equivalent.

Lemma 3.43. *If Q and Q' are primitive forms with discriminant Δ, and if $Q_k \sim Q'_l$, then $Q \sim Q'$.*

Proof. We have $Q_k \sim Q'_l$ if and only if there is an $S \in \mathrm{SL}_2(\mathbb{Z})$ with $Q_k|_S = Q'_l$. This is equivalent to the claim that $P_k S P_l^{-1}$ transforms Q into Q'. Thus $Q \sim Q'$ if we can show that $S' = P_k S P_l^{-1} \in \mathrm{SL}_2(\mathbb{Z})$. It is clear that $\det S' = 1$, so we only have to verify that S' has integral entries.

Leaving the cases where k or l or both are infinite as an exercise for the readers, let us consider the case where both k and l are finite. In this case, $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ satisfies $s = ps'$ by Lemma 3.38lemmacount.3.38. A simple calculation then shows that $P_k S P_l^{-1}$ indeed has integral coefficients. □

Thus we only have to test whether, for a fixed form Q, any of the forms Q_k for $k \in \mathbb{P}^1\mathbb{F}_p$ are equivalent. If $Q_k \sim Q_l$, say if $Q_k|_S = Q_l$ for some $S \in \mathrm{SL}_2(\mathbb{Z})$, then $P_k S P_l^{-1}$ must transform Q into itself, hence is an automorph of Q. Thus $P_k S P_l^{-1} = S_Q^{(T,U)}$.

We now claim that if S_S is an automorph of Q, then S_Q must permute the derived forms:

Proposition 3.44. *Let $Q = (A, B, C)$ be a quadratic form with nonsquare discriminant Δ, let $Q_0 = Q|_{P_0} = (Ap^2, Bp, C)$ be the derived form, and let $S_Q^{(T,U)}$ be an automorph of Q. Then the following claims are equivalent:*

- *$Q_k \sim Q_l$ for some $k, l \in \mathbb{P}^1\mathbb{F}_p$;*
- *there is an $S \in \mathrm{SL}_2(\mathbb{Z})$ such that $P_l S P_k^{-1} = S_Q^{(T,U)}$.*

More precisely, $S_Q^{(T,U)} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ permutes the equivalence classes of the primitive forms Q_k, and this permutation is given by $Q_k|_{S_Q} \sim Q_l$ for $l = S_Q(k)$, that is:

$$l \equiv \frac{ak + b}{ck + d} \bmod p. \tag{3.24}$$

Using indices from $\mathbb{P}^1\mathbb{F}_p$, we can write $k = [e : f]$ and $l = [g : h]$ with $e, f, g, h \in \mathbb{F}_p$, and then

$$S_Q([e : f]) = [ag + bh : cg + dh]. \tag{3.25}$$

Observe that (3.25equation.3.7.25) describes the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{P}^1\mathbb{F}_p$ introduced in (A.1The Projective Lineequation.A.4.1).

Proof. We have $Q_k \sim Q_l$ if and only if there is an $S \in \mathrm{SL}_2(\mathbb{Z})$ such that $Q_k = Q_l|_S$, i.e., if and only if $S_Q P_k = P_l S$ for some automorph S_Q of Q. Write $S_Q = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$. The special role played by the matrices P_∞ forces us to distinguish cases.

1. $\boldsymbol{k, l \neq \infty}$. The equation $S_Q P_k = P_l S$ gives

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ap & ak+b \\ cp & ck+d \end{pmatrix} = \begin{pmatrix} pr+lt & ps+lu \\ t & u \end{pmatrix} = \begin{pmatrix} p & l \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix},$$

Here a, b, c, d, k are given, and we have to prove the existence of integers r, s, t, u, m. We find $t = cp$ and $u = ck + d$; Next $ak + b = ps + lu$ shows that

$$l(ck+d) \equiv ak + b \bmod p. \tag{3.26}$$

Now we distinguish two cases:

1. $p \nmid (ck+d)$: then $l \equiv \frac{ak+b}{ck+d} \bmod p$. Since $0 \le l < p$, this determines l uniquely, and now $ap = pr + lt = pr + clp$ gives $a = r + cl$.
   Note that with $k \equiv e/f \bmod p$ and $l \equiv g/h \bmod p$, the congruence (3.261. $k, l \neq \infty$equation.3.7.26) can be written in the form $g(ce+df) \equiv h(ae+bf) \bmod p$.
2. $p \mid (ck+d)$: in this case, we try $l = \infty$; from $S_Q P_k = P_\infty S$ we get $ap = -t$, $ak+b = -u$, $cp = pr$ and $ck + d = ps$, which uniquely determines S.
   Observe that $ck + d \equiv 0 \bmod p$ gives $ce + df \equiv 0 \bmod p$; thus (3.25equation.3.7.25) holds because $[g : h] = [1 : 0] = [ae + bf, ce + df] = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})[e : f]$.

2. $\boldsymbol{k = \infty}$. Here, the equation $S_Q P_\infty = P_l S$ gives

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} = \begin{pmatrix} bp & -a \\ dp & -c \end{pmatrix} = \begin{pmatrix} pr+lt & ps+lu \\ t & u \end{pmatrix} = \begin{pmatrix} p & l \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix},$$

We find $t = dp$, $u = -c$, and $lc \equiv a \bmod p$.

1. $p \nmid c$: in this case, we have $l \equiv \frac{a}{c} \bmod p$ and $r = b - dl$.
2. $p \mid c$: in this case, we solve the equation $S_Q P_\infty = P_\infty S$ and find

It is easy to check that (3.25equation.3.7.25) is satisfied in both cases.

It remains to show that the permutation leaves the set of imprimitive forms invariant. *****

The class of Q_k is fixed by S_Q if and only if $[e : f] = (\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})[e : f] = [ae+bf, ce+df]$, that is, if and only if the congruence $e(ce + df) \equiv f(ae + bf) \bmod p$ holds, which is equivalent to $ce^2 + (d-a)ef - bf^2 \equiv 0 \bmod p$. From $(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) = S_Q^{(T,U)}$ we find $b = -CU$, $c = AU$, $a - d = BU$, hence $ce^2 + (d-a)ef - bf^2 = U(Ae^2 - Bef + Cf^2)$. Since $p \nmid U$, this implies $Ae^2 - Bef + Cf^2 \equiv 0 \bmod p$. □

The Class Number Formula

Lemma 3.45. *The smallest power of S inducing the trivial permutation is S^f, where f is the smallest positive integer such that $m(T, U) = (T', U')$ with $p \mid U'$.*

Observe that f is also the smallest positive integer such that $\varepsilon^m \in \mathcal{O}_\Delta$, where $\varepsilon = T + U\omega$ is the positive fundamental unit of $\mathcal{O}$.

Proof. □

Now we state

Theorem 3.46. *For any prime p, we have*

$$h^+(\Delta p^2) = \frac{p - \chi(p)}{f} h^+(\Delta),$$

where $\chi(p) = (\frac{\Delta}{p})$ and where f is defined in Lemma 3.45lemmacount.3.45.

Proof. Each class of $\mathrm{Cl}^+(\Delta p^2)$ is represented by some form Q_k, where $[Q]$ runs through the classes of $\mathrm{Cl}(\Delta)$. If $Q_k \sim Q_l'$, then $Q \sim Q'$, hence $Q = Q'$. If $Q_k|_S = Q_l$, then S must be an automorph of Q. The group of automorphs of Q is cyclic and is generated by $S = S_Q^{(T,U)}$, where (T, U) is the fundamental solution of the Pell equation $Q_0(T, U) = 1$ (here Q_0 denotes the principal form with discriminant Δ). The automorph S permutes the $p - (\Delta/p)$ primitive forms Q_k, and the order of this permuation is f. Thus each orbit of the classes $[Q_k]$ has f elements, and there must be $\frac{1}{f}(p - (\frac{\Delta}{p}))$ distinct classes among each set $[Q_k]$. This proves the claim. $\square$

Here are a few examples.

Δ	p	Δp^2	$h(\Delta)$	f	$h(\Delta p^2)$
5	2	20	1	3	1
5	3	45	1	2	2
5	5	125	1	5	1

Here are the cycles for these discriminants:

Δ	#	cycles	$h^+(\Delta)$
20	1	$(1, 6, 4), (4, 6, 1), (5, 10, 4), (4, 10, 5)$	1
45	1	$(1, 7, 1)$	2
	3	$(5, 15, 9), (9, 15, 5), (11, 21, 9), (11, 23, 11), (9, 21, 11)$	
125	1	$(1, 13, 11), (11, 13, 1), (19, 31, 11), (25, 45, 19), (29, 55, 25), (31, 61, 29),$ $(31, 63, 31), (29, 61, 31), (25, 55, 29), (19, 45, 25), (11, 31, 19)$	1

Using induction it is easy to show that $h(5^n) = 1$. In particular, there are infinitely many positive discriminants with class number 1. The question whether there are infinitely many fundamental discriminants with class number 1 is still open.

It remains to determine the structure of the "new class group". To this end, we consider the map $\pi : \mathrm{Cl}^+(\Delta p^2) \longrightarrow \mathrm{Cl}^+(\Delta)$ sending the class of a form (A, Bp, Cp^2) to the class of (A, B, C).

Theorem 3.47. *The natural projection $\pi : \mathrm{Cl}^+(\Delta p^2) \longrightarrow \mathrm{Cl}^+(\Delta)$ is a surjective group homomorphism. The kernel of π is a cyclic group of order $\frac{1}{f}(p - (\frac{\Delta}{p}))$. Its group law can be described as follows: if $\Delta = 4m$, set $Q_k = (p^2, 2kp, k^2 - m)$ for $0 \le k < p$, and $Q_\infty = (1, 0, -mp^2)$. Then $Q_k Q_l Q_n \sim 1$ for $n \equiv \frac{kl+m}{k+l} \bmod p$.*

Proof. We will give the proof for discriminants $\Delta = 4m$. A derived form is in the kernel of π if it is derived from the principal form $(1, 0, -m)$. Assume therefore that $Q_k = (p^2, 2kp, k^2 - m)$ and $Q_l = (p^2, 2lp, l^2 - m)$ are primitive. For composing these forms, we have to compute $e = \gcd(p^2, p(k + l)) = p \cdot \gcd(p, k + l)$.

Assume first that $p \nmid (k+l)$. Then $e = p$, and we set $a = 0$, $b = p$, $c = p$, and $d = k+l$. Then we solve the diophantine equation $bg-cf = p(g-f) = p(k-l)$, so we can take $g = k$ and $f = l$. Finally, we set $h = (df - C')/b = ((k + l)l - l^2 + m)/p = (kl + m)/p$, which gives us our preliminary composition matrix $\mathcal{M} = \big(\begin{smallmatrix} 0 & p & p & k+l \\ p & l & k & (kl+m)/p \end{smallmatrix}$. For making h integral we have to solve $nd \equiv kl + m \bmod p$, which gives $n \equiv \frac{kl+m}{k+l} \bmod p$. With this value of n (normalized by $0 \le n < p$) we find $\mathcal{M} = \big(\begin{smallmatrix} 0 & p & p & k+l \\ p & l+n & k+n & (kn+ln+kl+m)/p \end{smallmatrix}$. Thus $Q_k Q_l Q' \sim 1$ for $Q' = (p^2, 2np, n^2 - m)$.

Now suppose that $k + l = np$. Then $e = p^2$, and we find $a = 0$, $b = 1$, $c = 1$; this implies $A_3 = 1$, hence $Q_k * Q_l$ is equivalent to the principal form Q_∞. Since we also have $Q_\infty Q_k \sim Q_k Q_\infty \sim Q_k$, we have covered all cases. $\square$

Our definition of the forms Q_k implies that $Q_kQ_l \sim Q_n$ for $n \equiv -\frac{kl+m}{k+l} \bmod p$. If we use the forms

$$Q_k = (p^2, -2kp, k^2 - m) \tag{3.27}$$

instead, we find $Q_kQ_l \sim Q_n$ for $n \equiv \frac{kl+m}{k+l} \bmod p$. Thus we have proved

Corollary 3.48. *The kernel of the map $\pi : \mathrm{Cl}^+(\Delta p^2) \longrightarrow \mathrm{Cl}^+(\Delta)$ consists of the $p - (\frac{\Delta}{p})$ primitive forms Q_k defined by (3.27The Class Number Formulaequation.3.7.27). This group is isomorphic to the group of points on the projective line defined in (2.2The Group Law on Linesequation.2.1.2); in particular, $\ker \pi$ is cyclic.*

Example. Consider the forms $Q = (2, 2, 21)$ and $Q' = (6, 2, 7)$ with discriminant $\Delta = -164$. We have computed their composition matrix $\mathcal{M} = \left(\begin{smallmatrix} 0 & 1 & 3 & 1 \\ 2 & 0 & 0 & -7 \end{smallmatrix}\right)$ in Example 1 on p. 81Composition of Formslemmacount.3.14, and found that $QQ'Q'' \sim 1$ for $Q'' = (3, -2, 14)$.

Now let us compose the derived forms $Q_1 = (18, 18, 25)$ and $Q_2' = (54, 78, 35)$ with discriminant Δp^2 for $p = 3$. We find $e^* = 6$ and set $a^* = 0$, $b^* = 3$, $c^* = 9$ and $d^* = 8$. Now we have to solve the equations $b^*g^* - c^*f^* = -30$ and $h^* = (f^*d^* - 35)/b^*$. Dividing the first equation through by 3 we get $g^* - 3f^* = -10$, and we can take $f^* = 4$ and $g^* = 2$. The second equation then implies $h^* = -1$. Thus we have the composition matrix $\mathcal{M}^* = \left(\begin{smallmatrix} 0 & 3 & 9 & 8 \\ 6 & 4 & 2 & -1 \end{smallmatrix}\right)$, which gives $Q_1Q_2'(27, -6, 14) \sim 1$.

Example. Now take $p = 7$; the derived forms we want to compose are $Q_1 = (98, 42, 25)$ and $Q_1' = (294, 98, 15)$. Here $e^* = \gcd(98, 294, 70) = 14$ and $a^* = 0$, $b^* = 7$, $c^* = 21$, $d^* = 5$. Next we solve $7g^* - 21f^* = -28$, that is, $g^* - 3f^* = -4$ by taking $g^* = f^* = 2$, and then take $h^* = (10 - 15)/7 = -5/7$.

Thus $\mathcal{M}' = \left(\begin{smallmatrix} 0 & 7 & 21 & 5 \\ 14 & 2 & 2 & -5/7 \end{smallmatrix}\right)$, which gives the imprimitive form $Q'' = (147, -14, 14)$. Making h^* integral by adding $\frac{1}{7}$ of the top row to the bottom row gives the composition matrix $\mathcal{M}^* = \left(\begin{smallmatrix} 0 & 7 & 21 & 5 \\ 14 & 3 & 5 & 0 \end{smallmatrix}\right)$ and the form $Q'' = (147, 28, 15)$.

Proposition 3.49. *There is a natural map $\pi_N : \mathrm{Cl}^+(\Delta N^2) \longrightarrow \mathrm{Cl}^+(\Delta)$ defined by sending the class of $Q = (A, BN, CN^2)$ to that of (A, B, C). The maps π_N are surjective group homomorphisms.*

This result allows us in some sense to compose forms with different discriminants: given primitive forms Q, Q' with discriminants Δm^2 and Δn^2, where $\gcd(m, n) = 1$, we can form $\pi_m(Q) + \pi_n(Q')$; the result will be a primitive form with discriminant Δ.

3.8. Notes

Already Diophantus studied the numbers that can be written as sums of two squares. He knew that if p and q can be written as sums of two squares, then the same is true for the product pq. In fact, in Book III of his Arithmetika (Problem 19) he writes (see Weil [Wei1984, p.11]):

> It is in the nature of 65 that it can be written in two different ways as a sum of two squares, viz., as $16 + 49$ and as $64 + 1$; this happens because it is the product of 13 and 5, each of which is a sum of two squares.

Today, we derive Diophantus' observation from the identity

$$(r^2 + s^2)(t^2 + u^2) = (x^2 + y^2), \quad \text{where} \quad x = rt - su,\ y = ru + st. \tag{3.28}$$

This identity occurs explicitly in al-Khazin's discussion of Diophantus' problem around 950 AD. It is also given in Problem 6 of Leonardo Pisano's (Leonardo of Pisa, today better known as Fibonacci) Book of Squares written in 1225.

A much more general identity was known to the Indian mathematicians, who studied integral solutions of the equation $Ny^2 + m = x^2$; Brahmagupta in the 7th century had a rule (bhavana) for the "production" of new solutions which may be expressed using modern formalism as

$$(x^2 - Ny^2)(z^2 - Nw^2) = (xz \pm Nyw)^2 - N(xw \pm yz)^2. \tag{3.29}$$

Using a solution of $x^2 - Ny^2 = m$ and a solution of the "Pell equation" $z^2 - Nw^2 = 1$ he could then derive a second solution of $x^2 - Ny^2 = m$.

The first glimpses of what later would be called composition of classes became visible in a problem going back to Fermat, who had observed that primes dividing $x^2 + y^2$ or $x^2 + 2y^2$ again had this form, but that this fails for primes dividing $x^2 + 5y^2$: in fact, $21 = 1^2 + 5 \cdot 2^2$, but neither 3 nor 5 are represented by this form. Fermat conjectured that any product of two primes of the form $20n + 3, 7$ could be represented by $x^2 + 5y^2$.

Euler claimed that $2p = x^2 + 5y^2$ for primes $p \equiv 3, 7 \bmod 20$; this would imply Fermat's conjecture by multiplying the representations $2p = x^2 + 5y^2$ and $2q = u^2 + 5v^2$ and then cancelling 4:

$$4pq = (x^2 + 5y^2)(u^2 + 5v^2) = (xu - 5yv)^2 + 5(xv + yu)^2$$

(note that x, y, u, v are all odd). In his Algebra, Euler also used identities such as

$$(ax^2 + cy^2)(au^2 + cv^2) = (axu \pm cyv)^2 + ac(xv \mp yu)^2.$$

Lagrange realized that Fermat's and Euler's conjectures would follow from the more precise statement that such primes are represented by the binary quadratic form $Q'(x, y) = 2x^2 + 2xy + 3y^2$, the reason being the identity (see [Lag1773, p. 789])

$$(2r^2 + 2rs + 3s^2)(2t^2 + 2tu + 2u^2) = x^2 + 5y^2, \tag{3.30}$$

where

$$x = 2rt + st + ru + 3su, \quad y = ru - st.$$

More generally, Lagrange showed that [ref??]

$$(Ar^2 + Brs + A'Cs^2)(A't^2 + Btu + ACu^2) = AA'x^2 + Bxy + Cy^2,$$

where

$$x = rt - Csu, \qquad y = Aru + A'st + Bsu.$$

Legendre generalized Lagrange's identities by showing that two arbitrary primitive forms with the same discriminant can be composed: in art. 358 (3rd ed.) he stated the problem

> Étant donnés deux diviseurs quadratiques Δ, Δ' d'une même formule $t^2 + au^2$, trouver le diviseur quadratique qui renferme leur produit.[7]

By a quadratic divisor of a form $t^2 + au^2$ Legendre denoted a quadratic form with the same discriminant; the notation can be explained by the observation that primes dividing $t^2 + au^2$ are represented by such forms.

Legendre then proceeds to develop the formulas needed in the calculation and remarks that, because of an ambiguity of sign in some of the formulas, the problem considered here has two solutions in general. Seen from our point of view, Legendre's construction suffered from the following defects:

[7] Given two quadratic forms Δ, Δ' of the same discriminant $-4a$, find the quadratic divisor that contains their product.

1. Legendre's composition of forms was not unique due to an ambiguity of signs.
2. Legendre does not prove that the equivalence classes of his composed forms $F = f \cdot f'$ only depend on the classes of f and f' (and the choice of signs).
3. Legendre does not distinguish between proper and improper equivalence; the classes with respect to the action of $\mathrm{GL}_2(\mathbb{Z})$ he used do not form a group.

It took Gauss to figure out exactly what was not right here; actually, Gauss claimed that he had not been aware of Legendre's work on composition of forms at the time he was working on his Disquisitiones: he explains the reason for this in his preface:

> Since this book[8] came to my attention after the greater part of my work was already in the hands of the publishers, I was unable to refer to it in analogous sections of my book. I felt obliged, however, to add Additional Notes on a few passages and I trust that this understanding and illustrious man will not be offended.

Many authors seem to think that the problems with composition magically disappear when proper equivalence is used instead of Lagrange-equivalence; this is, however, simply not true. For details on Legendre's composition and how Gauss removed its defects see the projects below.

Gauss worked exclusively with forms $ax^2 + 2bxy + cy^2$, which he denoted by (a, b, c), and with the determinant $b^2 - ac$. The transition to forms with not necessarily even middle coefficients was promoted by Eisenstein and Dedekind.

Gauss proved that, according to his definitions, two forms can be composed if their discriminants differ by a square factor. He had to pay for this generality by rather technical calculations. In the following, we will therefore restrict our attention to the case of primitive forms with the same discriminant.

Gauss's exposition of composition consisted of the following parts:

1. The class of the composed form $F = ff'$ only depends on the classes of f and f' (art. 237–239).
2. The class of the principal form is the neutral element (art. 243.1).
3. The class of $(A, -B, C)$ is the inverse of the class of (A, B, C) (art. 243.2).
4. Associativity of composition is proved in art. 240: Gauss claims that $(Q_1 * Q_2) * Q_3 \sim (Q_1 * Q_3) * Q_2$ and then presents a set of 27 equations in the coefficients of the forms involved, remarking that "it would take too much time to derive all 27 of these equations". He then needs two more pages of calculations to finish the proof.

Gauss also knew the basic idea behind Dirichlet composition (art. 243.1): given two forms (a, b, c) and (a', b', c') with discriminant D and coprime values of a and a', we can form the composed form (A, B, C) by taking $A = aa'$, solving the congruences $B \equiv b \bmod a$ and $B \equiv b' \bmod a'$, and setting $C = (B^2 - D)/A$.

Gauss already worked with the minors M_{ij} of $M(\mathcal{A})$; he used the notation $P = M_{12}$, $Q = M_{13}$, ..., $U = M_{34}$. The Plücker relation then is given by the equation $PU - QT + RS = 0$. Gauss did not state this relation explicitly, but Poullet-Delisle gave it in the notes of his French translation of the Disquisitiones.

Note: Gauss used $\det M = A$ etc.! effect on (3.8equation.3.1.8) etc.!

[8] Legendre's "Essai d'une théorie des nombres".

The general problem of finding necessary and sufficient conditions for the existence of a matrix with given minors was solved by Bazin [Baz1851a]. A modern account of these results can be found in Griffiths & Harris [GH1978].

Composition after Gauss

The first mathematician after Dirichlet who drastically simplified Gauss composition (and whose contribution was either not noticed at all or instantly forgotten) was Arthur Cayley. He had developed a theory of hyperdeterminants, which generalize determinants for matrices by attaching numbers to "higher dimensional matrices" such as a $2 \times 2 \times 2$-matrix $A = (a_{ijk})$ $(i, j, k = 0, 1)$, which has hyperdeterminant (see Cayley [Cay1845])

$$\begin{aligned} \operatorname{Det}(A) = {} & a_{000}^2 a_{111}^2 + a_{001}^2 a_{110}^2 + a_{010}^2 a_{101}^2 + a_{011}^2 a_{100}^2 \\ & - 2(a_{000}a_{001}a_{110}a_{111} + a_{000}a_{010}a_{101}a_{111} + a_{000}a_{011}a_{100}a_{111} \\ & + \quad a_{001}a_{010}a_{101}a_{110} + a_{001}a_{011}a_{110}a_{100} + a_{010}a_{011}a_{101}a_{100}) \\ & + 4(a_{000}a_{011}a_{101}a_{110} + a_{001}a_{010}a_{100}a_{111}). \end{aligned}$$

It can be shown ([GKZ1994, Chap. 14, Prop. 1.4]) that $\operatorname{Det}(A)$ is invariant under the natural action of the group $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$, and in fact it can be shown that $\operatorname{Det}(A)$ is the Γ-invariant of A of minimal degree.

With the identification

$$\begin{array}{llll} a_{000} = a, & a_{100} = b, & a_{010} = c, & a_{110} = d, \\ a_{001} = e, & a_{101} = f, & a_{011} = g, & a_{111} = h, \end{array}$$

$\operatorname{Det}(A)$ becomes (see Cayley [Cay1846, p. 14]) (3.14The Plücker Relationequation.3.1.14). The hyperdeterminant $\operatorname{Det}(A)$ can then be written (see Cayley [Cay1845, p. 89] and [Cay1846, p. 14]) in the form

$$\begin{aligned} \operatorname{Det}(A) &= (ah - bg - cf + de)^2 - 4(bc - ad)(fg - eh) \\ &= (ah - bg - de + cf)^2 - 4(af - be)(ch - dg) \\ &= (ah - cf - de + bg)^2 - 4(ag - ce)(bh - df). \end{aligned}$$

In this situation Cayley defines three quadratic forms

$$F_1 = (A, 2B, C), \quad F_2 = (A', 2B', C') \quad \text{and} \quad F_3 = (A'', 2B'', C'')$$

by putting

$$\begin{array}{rlrlrl} A &= ag - ce, & 2B &= ah - cf - de + bg, & C &= bh - df, \\ A' &= af - be, & 2B' &= ah - bg - de + cf, & C' &= ch - dg, \\ A'' &= fg - eh, & 2B'' &= ah - bg - cf + de, & C'' &= bc - ad. \end{array}$$

It is then clear that $\operatorname{Det}(A)$ is the common discriminant of these three quadratic forms. It is also easy to verify the following equations:

$$\begin{cases} AA' &= A''a^2 + 2B''ae + C''e^2, \\ AB' &= A''ac + B''(ag+ce) + C''eg, \\ AC' &= A''c^2 + 2B''cg + C''g^2; \end{cases} \tag{3.31}$$

$$\begin{cases} BA' &= A''ab + B''(af+be) + C''ef, \\ BB' + \Theta &= A''ad + B''(ah+de) + C''eh, \\ BB' - \Theta &= A''be + B''(bg+cf) + C''fg, \\ BC' &= A''cd + B''(ch+dg) + C''gh; \end{cases} \tag{3.32}$$

$$\begin{cases} CA' &= A''b^2 + 2B''bf + C''f^2, \\ CB' &= A''bd + B''(bh+df) + C''fh, \\ CC' &= A''d^2 + 2B''dh + C''h^2, \end{cases} \tag{3.33}$$

where $\Theta = \frac{1}{4}\Delta$. Adding the two middle equations in (3.32Composition after Gaussequation.3.8.31) gives

$$2BB' = A''(ad+be) + B''(ah+de+bg+cf) + C''(eh+fg),$$

and now (3.31Composition after Gaussequation.3.8.31) – (3.33Composition after Gaussequation.3.8.31) show that we have the identity

$$\begin{aligned} &A''z_1^2 + 2B''z_1z_2 + C''z_2^2 \\ &\quad = (Ax_1^2 + 2Bx_1x_2 + Cx_2^2)(A'y_1^2 + 2B'y_1y_2 + C'y_2^2), \end{aligned} \tag{3.34}$$

where

$$\begin{aligned} z_1 &= ax_1x_2 + by_1y_2 + cx_1y_2 + dy_1y_2, \\ z_2 &= ex_1x_2 + fy_1y_2 + gx_1y_2 + hy_1y_2. \end{aligned}$$

This shows that F_3 is the composition of the forms F_1 and F_2.

Now consider the cube

$$A = \begin{array}{cccc} & e & & f \\ -a & & -b & \\ & g & & h \\ -c & & -d & \end{array}$$

Its associated quadratic forms are

$$\begin{aligned} Q_1(x,y) &= (bc-ad)x^2 + (ah-bg-cf+de)xy + (fg-eh)y^2, \\ Q_2(x,y) &= (ag-ce)x^2 + (ah-cf-de+bg)xy + (bh-df)y^2, \\ Q_3(x,y) &= (af-be)x^2 + (ah-bg-de+cf)xy + (ch-dg)y^2. \end{aligned}$$

Comparing with Cayley's forms we see that

$$\begin{aligned} Q_1 &= (C'', 2B'', A'') \sim (A'', -2B'', C''), \\ Q_2 &= (A, 2B, C), \\ Q_3 &= A', 2B', C'). \end{aligned}$$

Thus Cayley's composition $(A'', 2B'', C'') \sim (A, 2B, C)(A', 2B', C')$ coincides with Gauss's $[Q_1, Q_2, Q_3] \sim 0$ since $(A'', -2B'', C'') \sim -(A'', 2B'', C'')$.

Now $(A, 2B, C)$ represents A and C, and $(A', 2B', C')$ represents A' and C'; thus the form $(A'', 2B'', C'')$ must represent the products AA', AC', CA' and CC', and in fact these representations are given by the formulas (3.31Composition after Gaussequation.3.8.31) and (3.33Composition after Gaussequation.3.8.31). More exactly, we have

$$\begin{aligned} AA' &= Q''(a,e), & CA' &= Q''(b,f), \\ AC' &= Q''(c,g), & CC' &= Q''(d,h). \end{aligned}$$

Dedekind showed that his theory of ideals and Gauss's theory of binary quadratic forms are equivalent, and, in [Ded1905], gave a simplified account of composition. considers two rows of four numbers

$$\begin{matrix} p\ p'\ p''\ p''' \\ q\ q'\ q''\ q''' \end{matrix} \tag{3.35}$$

and form the six determinants

$$\begin{aligned} P &= pq' - qp', & Q &= pq'' - p''q, & R &= pq''' - p'''q, \\ S &= p'q'' - q'p'' & T &= p'q''' - q'p''', & U &= p''q''' - q''p'''. \end{aligned}$$

He then observes the equations

$$Up' - Tp'' + Sp''' = 0, \quad Uq' - Tq'' + Sq''' = 0,$$

and by multiplying them by $-q$ and p, respectively, and adding the results he finds the Plücker relation

$$PU - QT + RS = 0.$$

Next he gives the proof of (3.8equation.3.1.8) and shows that the Plücker equation guarantees that the discriminants of the three quadratic forms attached to (3.35Composition after Gaussequation.3.8.35) have the same discriminant. Equation (3.8equation.3.1.8) does not reflect the symmetry of the cube $\mathcal{A}$ from which it is derived; a symmetric equation would have the product $Q_1Q_2Q_3$ on one side and something else on the other. Dedekind found such a formula:

$$Q_1(x_1,y_1)Q_2(x_2,y_2)Q_3(x_3,y_3) = \frac{H'^2 - \Delta H^2}{4},$$

where H, H' are trilinear forms given by

$$\begin{aligned} H &= ax_1x_2x_3 + \ldots \\ H' &= \end{aligned}$$

A special case of this formula was rediscovered by Goins [Goi2001].

Weber [Web1907] bases his theory of composition, which is inspired by Dedekind's account, on the trilinear form

$$\begin{aligned} H = {} & \alpha_0x_1x_2x_3 + \alpha_1x_1y_2y_3 + \alpha_2y_1x_2y_3 + \alpha_3y_1y_2x_3 \\ & + \beta_0y_1y_2y_3 + \beta_1y_1x_2x_3 + \beta_2x_1y_2x_3 + \beta_3x_1x_2y_3. \end{aligned} \tag{3.36}$$

As in Dedekind, let (r,s,t) be a permutation of $(1,2,3)$. Define the partial derivatives

$$\begin{aligned} X_r &= \frac{\partial H}{\partial y_r} = \beta_rx_sx_t + \alpha_sx_sy_t + \alpha_tx_ty_s + \beta_0y_sy_t, \\ -Y_r &= \frac{\partial H}{\partial x_r} = \alpha_0x_sx_t + \beta_tx_sy_t + \beta_sx_ty_s + \alpha_ry_sy_t, \end{aligned}$$

as well as the three quadratic forms

$$f_t = -\begin{vmatrix} \frac{\partial X_r}{\partial x_s} & \frac{\partial X_r}{\partial y_s} \\ \frac{\partial Y_r}{\partial x_s} & \frac{\partial Y_r}{\partial y_s} \end{vmatrix} = \frac{\partial^2 H}{\partial x_r \partial y_s} \frac{\partial^2 H}{\partial x_s \partial y_r} - \frac{\partial^2 H}{\partial x_r \partial x_s} \frac{\partial^2 H}{\partial y_r \partial y_s}. \tag{3.37}$$

Explicitly he finds $f_t = (a_t, b_t, c_t)$ with

$$\begin{aligned} a_t &= \beta_r \beta_s - \alpha_0 \alpha_t, \\ b_t &= \alpha_r \beta_r + \alpha_s \beta_s - \alpha_t \beta_t - \alpha_0 \beta_0, \\ c_t &= \alpha_r \alpha_s - \beta_0 \beta_t. \end{aligned}$$

Now set

$$\begin{aligned} u_r &= \frac{\partial f_r}{\partial y_r} - x_r \sqrt{\Delta}, & \overline{u}_r &= \frac{\partial f_r}{\partial y_r} + x_r \sqrt{\Delta}, \\ v_r &= -\frac{\partial f_r}{\partial x_r} - y_r \sqrt{\Delta}, & \overline{v}_r &= -\frac{\partial f_r}{\partial x_r} + y_r \sqrt{\Delta}. \end{aligned}$$

Then

$$Q(x_r, y_r) = \frac{1}{4} u_r \overline{u}_r.$$

Weber gives two proofs of associativity; the first one uses Dirichlet composition.

Speiser [Spe1912] starts with a bilinear substitution

$$\begin{aligned} x_1 &= p y_1 z_1 + p' y_1 z_2 + p'' y_2 z_1 + p''' y_2 z_2, \\ x_2 &= q y_1 z_1 + q' y_1 z_2 + p'' q_2 z_1 + p''' q_2 z_2 \end{aligned} \tag{3.38}$$

and tries to find forms f_1, f_2, f_3 satisfying

$$f_1(x_1, x_2) = f_2(y_1, y_2) f_3(z_1, z_2). \tag{3.39}$$

Solving (3.38Composition after Gaussequation.3.8.38) for y_1 and y_2 we get

$$\begin{aligned} y_1 &= \frac{q'' x_1 z_1 + q''' x_1 z_2 - p'' x_2 z_1 - p''' x_2 z_2}{\phi_3(z_1, z_2)} &= \frac{Y_1}{\phi_3}, \\ y_2 &= \frac{-q x_1 z_1 - q' x_1 z_2 + p x_2 z_1 + p' x_2 z_2}{\phi_3(z_1, z_2)} &= \frac{Y_2}{\phi_3}, \end{aligned} \tag{3.40}$$

where

$$\phi_3(z_1, z_2) = \begin{vmatrix} p z_1 + p' z_2 & p'' z_1 + p''' z_2 \\ q z_1 + q' z_2 & q'' z_1 + q''' z_2 \end{vmatrix}.$$

Substituting (3.40Composition after Gaussequation.3.8.40) in (3.39Composition after Gaussequation.3.8.39) and clearing denominators gives

$$\phi_3(z_1, z_2)^2 f_1(x_1, x_2) = f_2(Y_1, Y_2) f_3(z_1, z_2).$$

Since $K[x_1, x_2, y_1, y_2, z_1, z_2]$ is factorial, and since $\gcd(f_3, f_1) = 1$, we conclude that

$$f_3 \mid \phi_3^2.$$

Solving for z_1 and z_2 instead we similarly get

$$\begin{aligned} z_1 &= \frac{q' x_1 y_1 + q''' x_1 y_2 - p' x_2 y_1 - p''' x_2 y_2}{\phi_2(y_1, y_2)} &= \frac{Z_1}{\phi_2}, \\ z_2 &= \frac{-q x_1 y_1 - q'' x_1 y_2 + p x_2 y_1 + p'' x_2 y_2}{\phi_2(y_1, y_2)} &= \frac{Z_2}{\phi_2}, \end{aligned} \tag{3.41}$$

where

$$\phi_2(y_1, y_2) = \begin{vmatrix} p y_1 + p'' y_2 & p' y_1 + p''' y_2 \\ q y_1 + q'' y_2 & q' y_1 + q''' y_2 \end{vmatrix}.$$

We also find that

$$f_2 \mid \phi_2^2.$$

Now let

$$f_1(x_1, x_2) = \phi_2(y_1, y_2)\phi_3(z_1, z_2) \tag{3.42}$$

for x_1, x_2 as in (3.38Composition after Gaussequation.3.8.38). Replacing y_1 and y_2 by the right hand sides of (3.40Composition after Gaussequation.3.8.40) we get

$$\phi_2(Y_1, Y_2) = f_1(x_1, x_2)\phi_3(z_1, z_2).$$

Now we see that

$$f_1 \mid \phi_1,$$

where

$$\phi_1(x_1, x_2) = \begin{vmatrix} q''x_1 - p''x_2 & q'''x_1 - p'''x_2 \\ -qx_1 + px_2 & -q'x_1 + p'x_2 \end{vmatrix}.$$

Since f_1 and ϕ_1 are homogeneous quadratic forms, they only can differ by a constant c:

$$c\phi_1(x_1, x_2) = \phi_2(y_1, y_2)\phi_3(z_1, z_2).$$

Solving (3.40Composition after Gaussequation.3.8.40) for z_1/ϕ_3 and z_2/ϕ_3 we find

$$\frac{z_1}{\phi_3} = \frac{-q'x_1y_1 + p'x_2y_1 - q'''x_1y_2 + p'''x_2y_2}{\phi_1(x_1, x_2)}.$$

Comparing this with the first equation in (3.41Composition after Gaussequation.3.8.41) we get

$$-\phi_1 = \phi_2\phi_3.$$

We have proved:

$$\begin{aligned} -&\begin{vmatrix} q''x_1 - p''x_2 & q'''x_1 - p'''x_2 \\ -qx_1 + px_2 & -q'x_1 + p'x_2 \end{vmatrix} \\ &\qquad = \begin{vmatrix} py_1 + p''y_2 & p'y_1 + p'''y_2 \\ qy_1 + q''y_2 & q'y_1 + q'''y_2 \end{vmatrix} \cdot \begin{vmatrix} pz_1 + p'z_2 & p''z_1 + p'''z_2 \\ qz_1 + q'z_2 & q''z_1 + q'''z_2 \end{vmatrix}. \end{aligned} \tag{3.43}$$

Speiser's algorithm for composing two forms was given in Thm. 3.13lemmacount.3.13. For his proof of Gauss's Lemma, see Lemma 3.21Gauss's Lemmalemmacount.3.21.

Composition of Forms

After preliminary work on the multiplication of forms by Euler and Lagrange, Legendre proved that any two forms with the same discriminant can be composed. The major drawback of Legendre's attempts was the fact that the composite of two forms was not well defined, not even up to equivalence.

Gauss's theory of composition differs in two subtle but important points from that of his predecessors: he introduced "proper equivalence" (equivalence with respect to $\mathrm{SL}_2(\mathbb{Z})$ instead of allowing matrices with determinant ± 1) and, through a judicious choice of signs in Legendre's composition algorithm (which he claims he was not aware of at the time he was writing his Disquisitiones), manages to make composition single-valued, thereby defining a group structure on the set of proper equivalence classes of forms. Gauss's proof of associativity involved solving a system of 27 equations, and was extremely technical.

Dirichlet simplified Gauss composition by introducing united forms in his lectures on number theory. The main idea, namely replacing the forms Q_1 and Q_2 by suitable equivalent forms Q_1' and Q_2' before composing them, was characterized by Arndt [Arn1859a,

p. 65] as avoiding technical calculations but lacking the elegance of Gauss's construction. Edwards [Edw1977, Edw2005, GSS2007, Edw2007a, Edw2008] made a habit out of complaining that Dirichlet's method was a composition of classes and not of forms. But if $Q_3' \sim Q_1'Q_2'$ in Dirichlet's sense, where $Q_1' \sim Q_1$ and $Q_2' \sim Q_2$ are concodrant, then we also have $Q_3' \sim Q_1Q_2$ in the sense of Gauss.

Cayley [Cay1846] developed a theory of hyperdeterminants; these are determinants of higher dimensional matrices. The hyperdeterminant of a $2 \times 2 \times 2$-matrix turned out to be related to Gauss composition of binary quadratic forms; in fact, his $2 \times 2 \times 2$-matrices are obviously incarnations of what we have called Bhargava's cubes. The hyperdeterminant of such a $2 \times 2 \times 2$-matrix coincides with the common discriminant of the forms attached to a cube. It can be shown (see Gelfand, Kapranov, & Zelevinsky [GKZ1994, Chap. 14, Prop. 1.4]) that $\mathrm{Det}(A)$ is invariant under the natural action of the group $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$, and in fact it can be shown that $\mathrm{Det}(A)$ is the Γ-invariant of A of minimal degree.

Bazin [Baz1851b] observed that the composition matrix can also be chosen in such a way that $a = 1$ and $e = 0$. Arndt [Arn1859a] showed that composition can be performed by solving a certain system of congruences. His method has become more or less the standard way of composing forms in the recent literature (see Buell [Bue1989], Lenstra [Len1982], Schoof [Sch1982]), mainly because it follows easily from the approach to composition via modules in quadratic number fields.

Pépin [Pep1880b] gave a detailed account of Gauss's theory of binary quadratic forms; like almost all authors who simplified Gauss's approach, he started with the bilinear substitution and then derived Gauss's six conclusions. He then gave an account of genus theory, and finally studied connections with Cauchy's and Jacobi's work on cyclotomy as well as with Joubert's results obtained with the help of elliptic functions, and gave applications to Euler's idoneal numbers. Smith [Smi1865] also gave a clean exposition of Gauss composition.

Dedekind showed that Gauss composition can be expressed clearly using the language of modules; he gave a full account of this approach in Dirichlet's lectures on number theory [DD1893, DD1999].

In an unpublished diary entry from Oct. 20, 1898 (see Fenster & Schwermer [FS2007]), Hurwitz presented an approach to Gauss composition which closely resembles Pépin's account discussed above. It is very unlikely that Hurwitz (or anyone else in the german number theoretic community) had read Pépin's memoir; the resemblance testifies to the naturality of this approch for anyone who had mastered Gauss's theory of composition. In fact, Dedekind proceeded in a similar way when returned to the problem of giving a satisfying account of composition in [Ded1905], and investigated what we have called the composition matrix $\mathcal{M} = \left(\begin{smallmatrix} a & b & c & d \\ e & f & g & h \end{smallmatrix}\right)$. In his investigations, he was led to the corresponding trilinear form $ax_1x_2x_3 + bx_1x_2y_3 + \ldots + hy_1y_2y_3$, which Weber [Web1907] put at the beginning of his account of composition. Speiser [Spe1912] gave a very simple introduction to composition based on Dedekind's approach, from which we have borrowed a substantial part.

An interesting approach to Gauss composition using matrices was presented by Brandt [Bra1919]. As Emmy Noether remarked in her Jahrbuch review of Brandt's article, some of his techniques were anticipated by Steinitz [Ste1899], who did not apply his results on modules to the composition of quadratic forms (or to anything else, for that matter). Steinitz's work on divisibility in integral matrix rings was based on fundamental results by Frobenius on elementary divisors.

Du Pasquier [dPa1906] and Châtelet [Cha1911, Cha1924] studied the greatest right divisors in the rings of integral matrices: for matrices $A, B \in M_n(\mathbb{Z})$, a matrix $D \in M_n(\mathbb{Z})$ is called a *right divisor* of A if $A = A_1D$ for some $A_1 \in M_n(\mathbb{Z})$. A common right divisor of A and B is a matrix D which is a right divisor of A and B. A right divisor D of A and B is called a greates common right divisor if every right divisor D' of A and B has the form

$D' = D_1 D$. Châtelet proved the existence of greatest common right divisors and provided an algorithm for computing it.

Grace Shover and MacDuffee [SMD1931] showed that Châtelet's theory could be used for doing ideal arithmetic in number fields. Jenkins [Jen1935] then translated their results to give a new method for composing binary quadratic forms. Rice [Ric1971] interpreted composition with the help of quaternion algebras.

Shanks [Sh1989b] rediscovered the "magic matrix" $M(\mathcal{A})$ implicitly contained in Gauss's work, and which occurred in various guises in the contributions by Cayley, Dedekind, Weber and Speiser. Shanks showed that the composed form Q_3 could be at least partially reduced by working with $M(\mathcal{A})$ instead of the coefficients of Q_3. Shanks also complained that the theory of composition had encountered "One Hundred Years of Solitude" between Dedekind's 1871 contribution and those of his own.

Riss [Ris1978] gave another (modern) account of Gauss composition using linear algebra.

The problem of extending Gauss composition of quadratic forms to more general domains was discussed by Lubelski [Lub1961], Kaplansky [Kap1968], Butts & Estes [BE1968], Dulin & Butts [DB1972], and then extensively by Towber [Tow1980]. Taussky's account of composition in [Tau1981] is incoherent and resembles Legendre's version of composition.

A generalization of Gauss composition to general rings was given by Kneser [Kne1982a, Kne1982b] (see also [GSS2007]), who replaced quadratic forms with coefficients from a ring R by quadratic spaces. Independently, Koecher [Koe1987] gave a similar solution.

In his Ph.D. thesis [Bha2001], Manjul Bhargava introduced the cubes $\mathcal{A}$ to represent collinear triples of quadratic forms. The main topic in Bhargava's thesis was not so much giving a new interpretation of Gauss composition, but studying various possible composition laws and applying them to finding the density of number fields of degree ≤ 5. Our definition of the forms Q_i attached to a cube $\mathcal{A}$ differs slightly from Bhargava's. Also, what we have called "primitive cubes" are called projective by Bhargava because of a connection with projective modules.

An approach to composition via wedge products was provided by Chua [Chu2008]; connections between composition and the wedge product already were spotted by Bosma & Stevenhagen [BS1996b].

Derived Forms

Gauß [Gau1801] proved the formula giving $h^+(\Delta N^2)/h^+(\Delta)$ only for negative discriminants Δ; Dirichlet [Dir1839, § 8] derived the general result from his class number formula, and Lipschitz [Lip1857] then gave an algebraic proof for the general result. The approach to nonfundamental discriminants given in the text is based on Jung's book [Ju1936]; see also Pall [Pal1935] and Flath [Fla1989].

3.9. Projects

3.9.1 Legendre and the composition of forms

1. Fermat's Conjecture. Verify that

$$(2x_1^2 + 2x_1y_1 + 3y_1^2)(2x_2^2 + 2x_2y_2 + 2y_2^2) = X^2 + 5Y^2$$

for

$$\begin{aligned} X &= x_3 = 2x_1x_2 + x_1y_2 + x_2y_1 - 2y_1y_2, & Y &= y_3 = x_1y_2 + x_2y_1 + y_1y_2, \qquad \text{or} \\ X &= x_4 = 2x_1x_2 + x_1y_2 + x_2y_1 + 3y_1y_2, & Y &= y_4 = x_1y_2 - x_2y_1, \end{aligned}$$

by computing the products

$$(2x_1 + y_1 + y_1\sqrt{-5}\,)(2x_2 + y_2 \pm y_2\sqrt{-5}\,) = 2(X + Y\sqrt{-5}\,).$$

From these identities, read off the coefficients of the corresponding composition matrix $\mathcal{M}$ (since the three forms attached to $\mathcal{M}$ and $-\mathcal{M}$ are identical, we will not distinguish between these matrices, or between the corresponding cubes) using (3.8equation.3.1.8):

X Y	$[a,b,c,d,e,f,g,h]$	Q_1	Q_2	Q_3
x_3 y_3	$[0,1,1,1,2,1,1,-2]$	$(2,2,3)$	$(2,2,3)$	$(1,0,5)$
x_3 $-y_3$	$[0,-1,-1,-1,2,1,1,-2]$	$(-2,-2,-3)$	$(-2,-2,-3)$	$(1,0,5)$
x_4 y_4	$[0,1,-1,0,2,1,1,3]$	$(2,2,3)$	$(-2,-2,-3)$	$(-1,0,-5)$
x_4 $-y_4$	$[0,1,-1,0,-2,-1,-1,-3]$	$(-2,-2,-3)$	$(2,2,3)$	$(-1,0,-5)$

Observe that among the four possible cubes there is exactly one giving the correct forms Q_1 and Q_2. If we demand that the composite form Q_3 be positive definite, we are left with the first two possibiities, each of which gives $(1,0,5)$ as the composed form. In this way, the composition table of the equivalence classes $\mathcal{A} = [(1,0,5)]$ and $\mathcal{B} = [(2,2,3)]$ becomes

$*$	$\mathcal{A}$	$\mathcal{B}$
$\mathcal{A}$	$\mathcal{A}$	$\mathcal{B}$
$\mathcal{B}$	$\mathcal{B}$	$\mathcal{A}$

2. Brahamgupta's Identity. Verify that

$$(x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) = x_3^2 - Ny_3^2$$

is satisfied for the following choices of x_3 and y_3, and explain them with Bhargava's cubes:

x_3	y_3	$[a,b,c,d,e,f,g,h]$	Q_1	Q_2	Q_3
$x_1x_2 + Ny_1y_2$	$x_1y_2 + x_2y_1$	$[0,1,1,0,1,0,0,N]$	$(1,0,-N)$	$(1,0,-N)$	$(1,0,-N)$
$x_1x_2 + Ny_1y_2$	$-x_1y_2 - x_2y_1$	$[0,-1,-1,0,1,0,0,N]$	$(-1,0,N)$	$(-1,0,N)$	$(1,0,-N)$
$x_1x_2 - Ny_1y_2$	$x_1y_2 - x_2y_1$	$[0,1,-1,0,1,0,0,-N]$	$(-1,0,N)$	$(-1,0,N)$	$(-1,0,N)$
$x_1x_2 - Ny_1y_2$	$-x_1y_2 + x_2y_1$	$[0,-1,1,0,1,0,0,-N]$	$(1,0,-N)$	$(1,0,-N)$	$(-1,0,N)$

Among the four possibilities, only one gives the correct forms Q_1 and Q_2.

Composition of General Forms. Legendre's method for composing two primitive forms $Q = ax^2+2bxy+cy^2$ and $Q' = a'z^2+2b'zw+c'w^2$ with determinant $\delta = b^2-ac = b'^2-a'c'$ was the following: Multiply Q and Q' through by a and a' and then apply Brahmagupta's identity (3.29Notesequation.3.8.29); divide through by aa' and show that you find

$$Q(x,y)Q'(z,w) = Au^2 + 2Buv + Cv^2,$$

where

$$\begin{aligned} A = aa', \qquad C &= (B^2-\delta)/A, \\ v &= (ax+by)w \pm (a'z+b'w)y, \\ Au + Bv &= (ax+by)(a'z+b'w) \pm \delta yw, \end{aligned}$$

and where B has still to be determined. Calculations give $u = xz + myw + m'xw + nyw$ with

$$m = \frac{b \mp B}{a}, \quad m' = \frac{b' - B}{a'}, \quad n = mm' \mp C.$$

Now Legendre assumes that $\gcd(a, a') = 1$ (this can always be achieved by replacing Q' by a suitably chosen equivalent form). Then there is an integer B with $B \equiv \pm b \bmod a$ and $B \equiv b' \bmod a'$, and we get

$$B^2 \equiv b^2 \equiv \delta \bmod a, \qquad B^2 \equiv {b'}^2 \equiv \delta \bmod a',$$

and all the coefficients above are integers.

Summarizing the above procedure, Legendre has found two forms

$$Q_j''(u, v) = A_j u^2 + B_j uv + C_j v^2$$

$(j = 1, 2)$ with determinant $B^2 - AC = \Delta$, and such that

$$Q(x, y)Q'(z, w) = Q_j''(L_j(x, y; z, w), L_j'(x, y; z, w))$$

for two pairs of bilinear forms L_j and L_j' in x, y and z, w.

For giving an explicit example, consider e.g. the form $(5, 6, 10)$ of discriminant $\Delta = -4 \cdot 41$. We find

$$(5x_1^2 + 6x_1y_1 + 10y_1^2)(5x_2^2 + 6x_2y_2 + 10y_2^2) = X^2 + 41Y^2$$

for

$$X = 5x_1x_2 + 3x_1y_2 + 3x_2y_1 + 10y_1y_2, \qquad \text{and} \qquad Y = x_1y_2 - x_2y_1.$$

On the other hand, we also have

$$(5x_1^2 + 6x_1y_1 + 10y_1^2)(5x_2^2 + 6x_2y_2 + 10y_2^2) = 2X^2 + 6XY + 25Y^2$$

for

$$X = 5x_1y_2 + 5x_2y_1 - 6y_1y_2, \qquad Y = x_1x_2 - 2y_1y_2.$$

Since $(2, 6, 25) \sim (2, 2, 21)$, this form is not equivalent to the principal form $(1, 0, 41)$. Thus the form $(5, 6, 10)$ can be composed with itself in two essentially different ways.

Thm. 3.1lemmacount.3.1 allows us to read off the coefficients of a cube $\mathcal{A}$ attached to identities of this form. In our case we find the cubes

$$\mathcal{A} = \begin{tikzcd}[row sep=small, column sep=small]
 & 1 \arrow[rr, dash] \arrow[dd, dash] & & 0 \arrow[dd, dash] \\
0 \arrow[rr, dash] \arrow[dd, dash] & & -1 \arrow[dd, dash] & \\
 & 3 \arrow[rr, dash] & & 10 \\
5 \arrow[rr, dash] & & 3 &
\end{tikzcd}, \qquad
\mathcal{A}' = \begin{tikzcd}[row sep=small, column sep=small]
 & 0 \arrow[rr, dash] \arrow[dd, dash] & & 2 \arrow[dd, dash] \\
-1 \arrow[rr, dash] \arrow[dd, dash] & & 0 \arrow[dd, dash] & \\
 & 5 \arrow[rr, dash] & & -6 \\
0 \arrow[rr, dash] & & 5 &
\end{tikzcd}$$

and the forms $Q_1 = (-5, -6, -10)$, $Q_2 = (5, 6, 10)$, $Q_3 = (-1, 0, -41)$, as well as $Q_1' = (5, 6, 10)$, $Q_2' = (5, 6, 10)$, and $Q_3' = (2, 6, 25)$. Thus we see that the first cube does not give rise to the right forms.

It turns out that there are, in general, two ways in which we can compose two forms, but that only one of them is compatible with Bhargava's cubes.

Example. Consider the following forms of discriminant $-4 \cdot 41$:

$$\begin{aligned}
\mathcal{A} &= x^2 + 41y^2, \\
\mathcal{B} &= 2x^2 + 2xy + 21y^2, \\
\mathcal{C} &= 5x^2 + 6xy + 10y^2, \\
\mathcal{D} &= 3x^2 + 2xy + 14y^2, \\
\mathcal{E} &= 6x^2 + 2xy + 7y^2.
\end{aligned}$$

Note that the form $(5,6,10)$ is not L-reduced; it is L-equivalent, however, to $(5,4,9)$. Composing C with itself we find

$$(5x^2+6xy+10y^2)(5z^2+6zw+10w^2) \\ = (5zx+3xw+3yz+10yw)^2+41(xw-yz)^2.$$

On the other hand, we also have

$$(5x^2+6xy+10y^2)(5z^2+6zw+10w^2) = 2X^2+6XY+25Y^2$$

for

$$X = 5xw+5zy-6yw, \qquad Y = xz-2yw.$$

This form has discriminant $6^2-8\cdot 25 = -4\cdot 41$, but it is not reduced. The transformation $X \longmapsto X-Y$ shows that it is equivalent to

$$2(X-Y)^2+6(X-Y)Y+25Y^2 = 2X^2+2XY+21Y^2.$$

Thus, as Legendre observes, we have $\mathcal{C}*\mathcal{C} \sim \mathcal{A}$ as well as $\mathcal{C}*\mathcal{C} \sim \mathcal{B}$, and in fact, his composition of reduced forms gives in general two different answers.

The complete "multiplication table" for the set of reduced forms of discriminant $-4\cdot 41$ is given by Legendre as

	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{D}$	$\mathcal{E}$
$\mathcal{A}$	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{D}$	$\mathcal{E}$
$\mathcal{B}$	$\mathcal{B}$	$\mathcal{A}$	$\mathcal{C}$	$\mathcal{E}$	$\mathcal{D}$
$\mathcal{C}$	$\mathcal{C}$	$\mathcal{C}$	$\mathcal{A}$ or $\mathcal{B}$	$\mathcal{D}$ or $\mathcal{E}$	$\mathcal{D}$ or $\mathcal{E}$
$\mathcal{D}$	$\mathcal{D}$	$\mathcal{E}$	$\mathcal{D}$ or $\mathcal{E}$	$\mathcal{A}$ or $\mathcal{C}$	$\mathcal{B}$ or $\mathcal{C}$
$\mathcal{E}$	$\mathcal{E}$	$\mathcal{D}$	$\mathcal{D}$ or $\mathcal{E}$	$\mathcal{B}$ or $\mathcal{C}$	$\mathcal{A}$ or $\mathcal{C}$

Anyone knowing about groups immediately sees that Legendre must be doing something wrong: composition is not well defined, and cancellation does not work (we have $\mathcal{A}*\mathcal{C}=\mathcal{C}$ and $\mathcal{B}*\mathcal{C}=\mathcal{C}$).

3.9.2 Gauss Composition

Let us return to Legendre's composition of reduced forms of discriminant $-4\cdot 41$. He found $A*X = X$ for all forms X, so A should be the neutral element of this "group". He also found $B*B \sim A$, which indicates that B should have order 2. But any group with an element of order 2 must have even order, whereas Legendre only had five classes to work with.

It is therefore clear that we will have to modify our definition of equivalence in such a way that we get fewer (say 4) or more (for example 6 or 8) classes. In order to get fewer classes we would have to allow more matrices T for which $Q|_T = Q$; but matrices with determinant $\neq \pm 1$ are not invertible in $\mathrm{GL}_2(\mathbb{Z})$, so we lose integrality or equivalence.

In order to get more classes we will have to restrict our class of matrices $T \in \mathrm{GL}_2(\mathbb{Z})$; the most obvious choice would of course be that of allowing only T with determinant 1. This is what Gauss did: he called two forms Q, Q' *properly* equivalent if $Q' = Q|_T$ for some $T \in \mathrm{SL}_2(\mathbb{Z})$.

Now consider the class $[Q]_L$ of a form $Q=(A,B,C)$ in the sense of Legendre; it contains at most two classes in the sense of Gauss, namely the class of forms properly equivalent to Q and the class $[Q^-]$ of forms properly equivalent to $Q^- = (A,-B,C)$, because $Q^- = Q|_T$ for $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{SL}_2(\mathbb{Z})$. Note that Q and Q^- represent the same integers since $Q(x,y) = Q^-(x,-y)$.

Although Q and Q^- are improperly equivalent (Gauss's expression for equivalence in the sense of Lagrange and Legendre), they might still be properly equivalent; this will definitely happen if $B = 0$, since then $Q = Q^-$. It also happens for forms (A, A, C) since $(A, -A, C) \sim (A, A, C)$ via $S = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Thus $\mathcal{A} \sim \mathcal{A}^-$ and $\mathcal{B} \sim \mathcal{B}^-$ for Legendre's classes $\mathcal{A}$ and $\mathcal{B}$. It can be shown, however, that Legendre's classes $[\mathcal{C}]_L$, $[\mathcal{D}]_L$, and $[\mathcal{E}]_L$ split into two distinct classes in the sense of Gauss.

Thus we end up with 8 classes of forms $[\mathcal{A}]$, $[\mathcal{B}]$, $[\mathcal{C}]$, $[\mathcal{C}^-]$, $[\mathcal{D}]$, $[\mathcal{D}^-]$, $[\mathcal{E}]$, and $[\mathcal{E}^-]$. Gauss also had to fix a choice of signs in the definition of composition; saving the details for later, we now can explain Legendre's $\mathcal{C} * \mathcal{C} \sim \mathcal{A}$ and $\mathcal{C} * \mathcal{C} \sim \mathcal{B}$ using Gauss composition: these relations correspond to Gauss's $[\mathcal{C}]+[\mathcal{C}^-] = [\mathcal{C}^-]+[\mathcal{C}] = [\mathcal{A}]$ and $[\mathcal{C}]+[\mathcal{C}] = [\mathcal{C}^-]+[\mathcal{C}^-] = [\mathcal{A}]$.

The cancellation problem also disappears since Legendre's $\mathcal{A} * \mathcal{C} \sim \mathcal{B} * \mathcal{C} \sim \mathcal{C}$ now become $[\mathcal{A}] + [\mathcal{C}] = [\mathcal{C}]$, $[\mathcal{A}] + [\mathcal{C}^-] = [\mathcal{C}^-]$, $[\mathcal{B}] + [\mathcal{C}] = [\mathcal{C}^-]$, and $[\mathcal{B}] + [\mathcal{C}^-] = [\mathcal{C}]$.

Gauss's definition of composition in art. 235 reads as follows:

> If the form $F = AX^2 + 2BXY + CY^2$ is transformed into the product of two forms
> $$f = ax^2 + 2bxy + cy^2 \quad \text{and} \quad f' = ax'^2 + 2b'x'y' + c'y'^2$$
> by the substitution
> $$\left.\begin{array}{l} X = pxx' + p'xy' + p''yx' + p'''yy', \\ Y = qxx' + q'xy' + q''yx' + q'''yy', \end{array}\right\} \tag{3.44}$$
> [...] we shall simply say that the form F is transformable in ff'. If, further, this transformation is so constructed that the six numbers
> $$\begin{array}{ll} P = pq' - qp', & Q = pq'' - p''q, \\ R = pq''' - p'''q, & S = p'q'' - q'p'', \\ T = p'q''' - q'p''', & U = p''q''' - q''p''' \end{array} \tag{3.45}$$
> do not have a common divisor, we will call the form F a composite of the forms f and f'.

As in Legendre's composition, there are in general two forms F that are composites of f and f'. By a lengthy caluclation, Gauss shows that there are integers $n, n' = \pm 1$ (we are assuming that the forms involved have the same discriminant; in Gauss's exposition, n and n' are just nonzero rational numbers) such that

$$\begin{array}{lll} P = an', & R - S = 2bn', & U = cn', \\ Q = a'n, & R + S = 2b'n, & T = c'n, \end{array}$$

and Gauss says that F is the (direct) composition of f and f' if $n = n' = +1$.

Gauss's theory of quadratic forms is maximally general: he makes no assumption on discriminants at all, and even composes forms of different discriminants. In the case of interest to us, the discriminants of the forms f, f' and F are equal, and the forms are primitive. Under these assumptions, the conditions on the gcd of P, Q, ..., U are always satisfied. Moreover, Gauss shows that (end of art. 235) that

$$(a, 2b, c) = (P, R - S, U) \quad \text{and} \quad (a', 2b', c') = (Q, R + S, T), \tag{3.46}$$

or, using the numbers p, p' etc,

$$\begin{aligned} (a, 2b, c) &= (pq' - qp', pq''' + q'p'' - p'''q - p'q'', p''q''' - q''p'''), \\ (a', 2b', c') &= (pq'' - p''q, pq''' + p'q'' - p'''q - q'p'', p'q''' - q'p'''), \\ (A, 2B, C) &= (q'q'' - qq''', pq''' + qp''' - p'q'' - q'p'', p'p'' - pp'''). \end{aligned}$$

At this point Gauss knows that

$$F(X,Y) = f(x,y)f'(x',y'),$$

where X and Y are defined as in (3.44Gauss Compositionequation.3.9.44).

In the following, we will present the composition algorithm of Gauss in the form presented by Smith [Smi1865] and Mathews [Mat1891].

Lemma 3.50. *Let P, Q, R, S, T, U be real numbers. Show that the matrices*

$$A = \begin{pmatrix} 0 & P & Q & R \\ -P & 0 & S & T \\ -Q & -S & 0 & U \\ -R & -T & -U & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & U & -T & S \\ -U & 0 & R & -Q \\ T & -R & 0 & P \\ -S & Q & -P & 0 \end{pmatrix}$$

satisfy $AB = BA = -(PU - QT + RS)E$, where E is the 4×4-unit matrix.

For $t = (t_0, t_1, t_2, t_3)^{\mathrm{tr}} \in \mathbb{R}^4$ define $x = (x_0, x_1, x_2, x_3)^{\mathrm{tr}} \in \mathbb{R}^4$ by $At = x$. Verify that $x \cdot t = 0$ and $Bx = 0$.

Let P, Q, R, S, T, U be integers satisfying the Plücker relation $PU - QT + RS = 0$. Choose arbitrary integers t_0, t_1, t_2, t_3 with $\gcd(t_0, t_1, t_2, t_3) = 1$ and choose $\lambda \in \mathbb{N}$ in such a way that $q = (q_0, q_1, q_2, q_3)^{\mathrm{tr}}$ satisfies $q = \lambda x$ for $x = At$ and $\gcd(q_0, q_1, q_2, q_3) = 1$. Using the Euclidean algorithm, find $r = (r_0, r_1, r_2, r_3)^{\mathrm{tr}} \in \mathbb{Z}^4$ with $r \cdot q = 1$, and set $p = \mu y$ for $y = Ar$ with $\gcd(p_0, p_1, p_2, p_3) = 1$.

Check that $M = \left(\begin{smallmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{smallmatrix}\right)$ has the minors P, Q, R, S, T, U.

Example.

3.9.3 Brandt Composition

Heinrich Brandt is perhaps best known for his introduction of groupoids in connection with composition of quaternary quadratic forms. In this project, we will present his approach to composition of quadratic forms based on linear algebra published in [Bra1919].

As usual, let $Q_0 = (1, \sigma, m)$ denote the principal form of discriminant $\Delta = \sigma^2 - 4m$, where $\sigma \in \{0, 1\}$. Let $Q = (A, B, C)$ be a quadratic form with discriminant $\Delta = B^2 - 4AC$. We say that a matrix T belongs to Q if $T^{\mathrm{tr}} M(Q_0) T = A \cdot M(Q)$. Verify that e.g. $T = \left(\begin{smallmatrix} A & \frac{B-\sigma}{2} \\ 0 & 1 \end{smallmatrix}\right)$ works.

Lemma 3.51. *If T belongs to Q, then, for any $S \in \mathrm{SL}_2(\mathbb{Z})$, TS belongs to $Q|_S$.*

Assume that $Q_i = (A_i, B_i, C_i)$ $(i = 1, 2, 3)$ are three quadratic forms to which the matrices T_i belong, and assume in addition that $\gcd(A_1, A_2) = 1$. Then $[Q_1] + [Q_2] = [Q_3]$ if and only if there exist matrices $S, S' \in \mathrm{SL}_2(\mathbb{Z})$ such that $T_3 = T_1 S T_2 = T_2 S' T_1$. We shall write $T_3 = T_1 * T_2$.

Brandt calls matrices T, T' equivalent if there exist $S, S' \in \mathrm{SL}_2(\mathbb{Z})$ with $T = T'S = S'T$. This is an equivalence relation.

Lemma 3.52. *Let T_i, T_i' $(i = 1, 2, 3)$ be matrices whose determinants* $\det T_i$ *are pairwise coprime. If $T_i \sim T_i'$, and if $T_3 = T_1 * T_2$ and $T_3' = T_1' * T_2'$, then $T_3' \sim T_3$.*

????

Let us prove associativity. We are given three forms Q_i, and we assume that $\gcd(A_1, A_2) = \gcd(A_1, A_3) = \gcd(A_2, A_3) = 1$. Assume that $[Q_1] + [Q_2] = [Q_{12}]$ and $[Q_2] + [Q_3] = [Q_{23}]$; we have to show that $[Q_{12}] + [Q_3] = [Q_1] + [Q_{23}]$. Let T_i and T_{ij} be matrices belonging to these forms; then $T_{12} = T_1 S_{12} T_2 = T_2 S_{21} T_1$, $T_{23} = T_2 S_{23} T_3 = T_3 S_{32} T_2$, and we have to show $T_{12} S_3 T_3 = T_3 S_4 T_{12}$??

Example.

Exercises

3.1 Assume that the primitive forms $Q_i = (A_i, B_i, C_i)$ are attached to the cube

$$\mathcal{A} = \begin{array}{ccccc} & & e & — & f \\ & & | & & | \\ a & — & b & & | \\ | & & | & & | \\ | & & g & — & h \\ | & & | & & \\ c & — & d & & \end{array}$$

Since A_i, C_i are represented by the forms Q_i for $i = 1, 2$, the products A_1A_2, A_1C_2 etc. must be represented by Q_3. Show that, in fact,

$$A_1A_2 = Q_3(c, -a), \qquad A_1C_2 = Q_3(d, -b),$$
$$C_1A_2 = Q_3(g, -e), \qquad C_1C_2 = Q_3(h, -f).$$

3.2 Compute the three quadratic forms attached to the cube
3.3 Compute the action of the element $\in \mathrm{SL}_2(\mathbb{Z})^3$ on the cube
3.4 Compute a cube attached to the three forms
3.5 Compute a cube attached to the three forms $(2, 2, m)$,(2,2,m), Q_0
3.6 Here's a different proof for Lemma 3.17lemmacount.3.17. Show that $Q(1, 0)$, $Q(0, 1)$ and $Q(1, 1)$ do not have a common divisor. Conclude that for each $p \mid N$ there is a pair $(x_p, y_p) \in \{(1, 0), (0, 1), (1, 1)\}$ such that $p \nmid Q(x_p, y_p)$. Now use the Chinese Remainder Theorem to find x, y such that $Q(x, y)$ is coprime to N.
3.7 Let $(A, 2B, C)$ be a form of discriminant $4B^2 - 4AC = 4n$, and show that

$$(Ax_1^2 + 2Bx_1y_1 + Cy_1^2)(Ax_2^2 + 2Bx_2y_2 + Cy_2^2) = x_3^2 - ny_3^2, \qquad \text{where}$$
$$x_3 = Ax_1y_1 + Bx_1y_2 + By_1x_1 + Cy_1y_2, \qquad y_3 = x_1y_2 - x_2y_1$$

generalizes Lagrange's identity in the special case $n = -5$.
3.8 (Smith, p. 233; Weber) Consider the expressions

$$X = axx' + bxy' + cx'y + dyy',$$
$$-Y = exx' + fxy' + gx'y + hyy'.$$

Show that the matrices

$$J = \begin{pmatrix} \frac{dX}{dx} & \frac{dX}{dy} \\ \frac{dY}{dx} & \frac{dY}{dy} \end{pmatrix}, \qquad J' = \begin{pmatrix} \frac{dX}{dx'} & \frac{dX}{dy'} \\ \frac{dY}{dx'} & \frac{dY}{dy'} \end{pmatrix}$$

have determinants $\det J = Q_2(x', y')$ and $\det J' = Q_3(x, y)$, where Q_2 and Q_3 are the quadratic forms attached to the cube $\mathcal{A}$.
3.9 Assume that $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Show that $Q(r, s)Q^-(t, u) = Q_0(x, y)$, where

$$(x, y) = \begin{cases} (Art - bru + bst - Cuy, 1) & \text{if } \Delta = 4m,\ B = 2b \\ (Art - bru + (1 - b)st - Cuy, 1) & \text{if } \Delta = 4m + 1, B = 2b + 1. \end{cases}$$

Hint: rotate the cubes on p. 86Examples of Collinear Classeslemmacount.3.23 with γ^2 so that the associated forms are $Q = (A, B, C)$, $Q^- = (A, -B, C)$ and Q_0; the corresponding matrices are then $M(\mathcal{A}) = \left(\begin{smallmatrix} 0 & 1 & 1 & 0 \\ A & -b & b & -C \end{smallmatrix}\right)$ and $M(\mathcal{A}) = \left(\begin{smallmatrix} 0 & 1 & 1 & 0 \\ A & b & b' & -C \end{smallmatrix}\right)$, respectively, where $b' = 1 - b$. Deduce that $Q(x_1, y_1)Q^-(x_2, y_2) = Q_0(x_3, y_3)$ with x_3, y_3 as in (3.8equation.3.1.8).

3.10 Show that if $Q_0Q_0Q \sim 1$, then $Q \sim Q_0$.

3.11 Let $m \equiv 1 \bmod 4$ be an integer. Show that $QQQ_0 \sim 1$ for the forms $Q_0 = (1, 0, m)$ and $Q = (2, 2, \frac{m+1}{2})$ with discriminant $\Delta = -4m$.

3.12 The next three exercises deal with connections between the cross product of vectors and composition.
Let $a_1, a_2, a_3, b_1, b_2, b_3$ be integers, and set

$$\begin{pmatrix} A_1 \\ A_2 \\ A_3 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}, \quad \text{that is,} \quad A_1 = \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, \quad A_2 = \begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix}, \quad A_3 = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}.$$

Show that $a_1A_1 + a_2A_2 + a_3A_3 = 0$. (Hint: imitate the proof of the Plücker relation.)

3.13 Let a_1, a_2, a_3 and A_1, A_2, A_3 be integers with $a_1A_1 + a_2A_2 + a_3A_3 = 1$ and $\gcd(a_1, a_2, a_3) = \gcd(A_1, A_2, A_3) = 1$. Show that there exist integers b_1, b_2, b_3 such that

$$\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} = A_1, \quad \begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix} = A_2, \quad \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = A_3.$$

Hints. Use Bezout to find integers c_1, c_2, c_3 satisfying $a_1c_1 + a_2c_2 + a_3c_3 = 1$, then set

$$b_1 = a_1 - c_2A_3 + c_3A_2, \quad b_2 = a_2 - c_3A_1 + c_1A_3, \quad b_3 = a_3 - c_1A_2 + c_2A_1.$$

3.14 (Bosma & Stevenhagen [BS1997, Lemma 2.8.]) Let $Q = (A, B, C)$ be a primitive quadratic form with discriminant Δ, and assume that there are vectors $a = (a_1, a_2, a_3)^{\mathrm{tr}}$ and $b = (b_1, b_2, b_3)^{\mathrm{tr}}$ such that

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_2b_3 - a_3b_2 \\ a_3b_1 - a_1b_3 \\ a_1b_2 - a_2b_1 \end{pmatrix}.$$

Show that $[Q]^2 = [Q']$ for $Q' = (A', B', C')$ and

$$\begin{pmatrix} A' \\ B' \\ C' \end{pmatrix} = \begin{pmatrix} a_2^2 - a_1a_3 \\ a_1b_3 + a_3b_1 - 2a_2b_2 \\ b_2^2 - b_1b_3 \end{pmatrix}.$$

3.15 Show that the forms $Q_1 = (2, 2, 33)$ and $Q_2 = (3, 2, 22)$ are concordant. Deduce that $Q_1Q_2Q_3 \sim 1$ for $Q_3 = (6, -2, 11)$.

3.16 Use Dirichlet's technique to show that $Q^2Q' \sim 1$ for the forms $Q = (2, 1, 2)$ and $Q' = (4, -1, 1)$ with discriminant $\Delta = -15$.

3.17 Show that the primitive forms (A, B, C) and (C, B, A) are concordant, and deduce the relation $(A, B, C)(C, B, A)(AC, -B, 1) \sim 1$.

3.18 Show that the form $Q = (2, 1, 3)$ with discriminant $\Delta = -23$ is not concordant with itself. Verify that $Q' = Q|_M = (2, -3, 4)$ for $M = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, and then compute $[Q]^2$.

3.19 Define an action of $\mathrm{GL}_2(\mathbb{Z})$ on the set of primitive quadratic forms with discriminant Δ by $M(Q|_S) = S^{\mathrm{tr}}M(Q)S$. Show that $(A, B, C) \sim (A, -B, C)$ under this action, hence the equivalence classes modulo $\mathrm{GL}_2(\mathbb{Z})$ are the union of $\mathrm{SL}_2(\mathbb{Z})$-classes and their inverses. In particular, these equivalence classes in general do not form a group with respect to composition.

3.20 Let $p \geq 3$ be an integer and set $\Delta = -(2^p - 1)$. Show that $h^+(\Delta) \equiv 0 \bmod p - 2$ by showing that the class of the form $Q = (2, 1, 2^{p-3})$ has order $p - 2$.

3.21 Show that the set of matrices $\left(\begin{smallmatrix} r & Ns \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ form a subgroup $\Gamma^0(N)$ of $\mathrm{SL}_2(\mathbb{Z})$, and that the map sending $\left(\begin{smallmatrix} r & Ns \\ t & u \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} r & s \\ Nt & u \end{smallmatrix}\right) \in \Gamma_0(N)$ induces an isomorphism of groups.

3.22 Define a map $\Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$ by sending $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \Gamma_0(N)$ to the residue class $r + N\mathbb{Z}$ induces an exact sequence

$$1 \longrightarrow \Gamma_1(N) \longrightarrow \Gamma_0(N) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow 0,$$

where $\Gamma_1(N)$ is the set of matrices $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $r \equiv u \equiv 1 \bmod N$ and $t \equiv 0 \bmod N$.

3.23 (continued) Show that the map $\Gamma_1(N) \longrightarrow \mathbb{Z}/N\mathbb{Z}$ given by $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \to s + N\mathbb{Z}$ induces an exact sequence

$$1 \longrightarrow \Gamma(N) \longrightarrow \Gamma_1(N) \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow 0,$$

where $\Gamma(N)$ is the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ consisting of matrices $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ with $r \equiv u \equiv 1 \bmod N$ and $s \equiv t \equiv 0 \bmod N$.

3.24 Show that two matrices $R = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ and $R' = \left(\begin{smallmatrix} r' & s' \\ t' & u' \end{smallmatrix}\right)$ with determinant p and $\gcd(r,t) = \gcd(r',t') = 1$ are right equivalent if and only if $rt' \equiv r't \bmod p$.

3.25 Prove the special case $n = 3$ (and $m = 1$) of Gauss's Lemma 3.21Gauss's Lemmalemmacount.3.21 as follows: Let $M = \left(\begin{smallmatrix} p_1 & p_2 & p_3 \\ q_1 & q_2 & q_3 \end{smallmatrix}\right)$ and $N = \left(\begin{smallmatrix} r_1 & r_2 & r_3 \\ s_1 & s_2 & s_3 \end{smallmatrix}\right)$ be integral matrices such that the minors of M are coprime. Find integers t_1, t_2, t_3 such that the determinant of the matrices

$$A = \begin{pmatrix} p_1 & p_2 & p_3 \\ q_1 & q_2 & q_3 \\ t_1 & t_2 & t_3 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} r_1 & r_2 & r_3 \\ s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \end{pmatrix}$$

equals 1. Show that

$$A^{-1}B = \begin{pmatrix} r & s & 0 \\ t & u & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and verify that $S = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ has the desired properties.

3.26 Let $\Delta = \Delta_0 f^2$ for some fundamental discriminant Δ_0, and let N be a positive integer satisfying $(\Delta/p) = +1$ for all primes $p \mid N$. Then the congruence $B_0^2 \equiv \Delta_0 \bmod 4N$ is solvable; fix a solution B_0.
A form (A,B,C) is called a Heegner form if

1. $\operatorname{disc} Q = \Delta$;
2. $N \mid A$;
3. $B \equiv B_0 f \bmod 2N$.

Let $\mathcal{F}_N$ denote the set of Heegner forms; show that $\mathcal{F}_N$ is fixed by the action of $\Gamma_0(N)$, and that the natural map $\pi_N : \mathcal{F}_N/\Gamma_0(N) \longrightarrow \mathcal{F}/\mathrm{SL}_2(Z)$ is a bijection.
Also show that $\mathcal{F}_N/\Gamma_0(N)$ carries a natural group structure (consider $\Gamma_0(N)$-equivalence classes of forms (A,B,C) with C coprime to N), and that π_N is an isormorphism of abelian groups.

3.27 (continued) Consider the free abelian group G_Δ generated by Heegner forms belonging to the pair (Δ, N). For each prime p and some Heegner form $Q = (A,B,C)$ introduce the forms $Q_\infty = (A, Bp, Cp^2)$ and $Q_k = (Ap^2, (B+2Ak)p, Ak^2 + Bk + C)$ for $0 \le k < p$. Show that the Q_k are Heegner forms.
Define the Hecke operator T_p via $T_pQ = Q_\infty + Q_0 + Q_1 + \ldots + Q_{p-1}$, with the object on the right hand side interpreted as an element of G_Δ. The Atkin-Lehner involution w_N is defined by $w_N(Q) = (CN, B, A/N)$. Show that $w_N(Q)$ is a Heegner form, and that $w_N \circ w_N$ is the identity map.
Set $F_N = (N, B_0 f, C)$ for $C = (B_0^2 f^2 - \Delta)/4N$. Show that $w_N(Q) = F_N \cdot Q^{-1}$ in $\mathcal{F}_N/\Gamma_0(N)$.

3.28 (Shanks & Weinberger [SW1972]) Let $p = A^6 + 4B^6$ be a prime, and consider the form $Q = (B^3, A^3, -B^3)$ with discriminant $\Delta = p$. Show that $Q \sim Q_0$.
Hints: Show that Q represents B^3 and $-B^3$, and use composition to deduce that Q^2 represents -1, and that Q^4 represents 1. By genus theory, the class number $h^+(\Delta)$ is odd, hence we must have $Q \sim Q_0$.

3.29 (continued) Set $Q_1 = (3(A^2+B^2), 3A^3, A^4 - A^2B^2 + B^4)$. Show that Q_1 is the composition of the forms $Q_2 = (A^2 + B^2, 3A^3, 3(A^4 - A^2B^2 + B^4))$ and $Q_3 = (3, 3, \frac{1}{4}(\Delta + 3))$.
Show that $Q_3^2 \sim Q_0$ and $Q_2^2 \sim Q_1^{-1}$, and deduce that $Q_2^3 \sim Q_0$.
If $\Delta > 5$, show that Q_2 is not equivalent to the principal form.

3.30 Show that if $p \mid C$, then the solutions of the quadratic congruence $A + Bk + Ck^2 \equiv 0 \bmod p$ (see Lemma 3.42lemmacount.3.42) can still be given by the formula $k_{1,2} \equiv \frac{-B \pm \sqrt{\Delta}}{2A} \bmod p$ if it is interpreted correctly.
Show first that you may choose $\sqrt{\Delta} \equiv B \bmod p$; choosing the minus sign in the formula for k then gives $k = \infty$. For the plus sign, use the identity $\frac{-B+\sqrt{\Delta}}{2C} = \frac{2A}{-B-\sqrt{\Delta}}$.

3.31 (Steinitz [Ste1899]) Consider the ring M_n of $n \times n$-matrices with integral entries (much of what follows can be transferred to principal ideal domains). For each $1 \le k \le n$, let $d_k(A) \ge 0$ denote the greatest common divisor of the determinants of all $k \times k$-minors of A (we set $d_k(A) = 0$ if all these determinants vanish); the elements d_k are called determinant divisors.
We say that $B \mid A$ for $A, B \in M_R$ if there exist matrices $C, D \in M_R$ such that $A = CBD$. We call two matrices A, B associate (and write $A \sim B$) if $A \mid B$ and $B \mid A$. Let $[A]$ denote the equivalence class of A.
Prove the first fundamental theorem of Frobenius: we have $[A] = [B]$ if and only if they have the same determinant divisors. In this case, there exist matrices $E_1, E_2 \in \mathrm{GL}_n(\mathbb{Z})$ such that $A = E_1 B E_2$.
A matrix $A \in M_n$ is called principal if it is a diagonal matrix of the form $A = \mathrm{diag}(e_1, e_2, \ldots, e_n)$ with $e_j \ge 0$ for $1 \le j \le n$ and $e_j \mid e_{j+1}$ for $1 \le j < n$. Show that every class contains a unique principal matrix.
We call $e_1, e_2, \ldots, e_n$ the invariants of a class $[A]$. Prove the second fundamental theorem of Frobenius: we have $B \mid A$ if and only if each invariant of B divides the corresponding invariant of A.

References

[Ab1826] N.H. Abel, *Über die Integration der Differential-Formel $\frac{\sqrt{\rho}dx}{R}$, wenn R und ρ ganze Functionen sind*, J. Reine Angew. Math. **1** (1826), 185–221

[AL2008] W. Aitken, F. Lemmermeyer, *Simple counterexamples to the Local-Global Principle*, Amer. Math. Monthly 2008

[ACH1965] N. C. Ankeny, S. Chowla, H. Hasse, *On the class number of the real subfield of a cyclotomic field*, J. Reine Angew. Math. **217** (1965), 217–220

[Ant1989a] A.A. Antropov, *On the history of the concept of genus of binary quadratic form* (Russian), Istor. Metodol. Estestv. Nauk No. **36**, (1989), 17–27

[Ant1989b] A.A. Antropov, *Partitioning of forms by genus and the reciprocity law in L. Euler's work* (Russian), Voprosy Istor. Estestvoznan. i Tekhn. 1989, no. 1, 56–57

[Ant1995] A.A. Antropov, *On Euler's partition of forms into genera*, Historia Math. **22** (1995), 188–193

[Arn1845] F. Arndt, *Disquisitiones nonnullae de fractionibus continuis*, Diss. Sundia 1845, 32pp

[Arn1846] F. Arndt, *Bemerkungen über die Verwandlung der irrationalen Quadratwurzel in einen Kettenbruch*, J. Reine Angew. Math. **31** (1846), 343–358

[Arn1851] F. Arndt, Archiv Math. Phys. **17** (1851), 1–53

[Arn1852] F. Arndt, Archiv Math. Phys. **19** (1852), 408–418

[Arn1857] F. Arndt, *Zur Theorie der binären kubischen Formen*, J. Reine Angew. Math. **53** (1857), 309–321

[Arn1859a] F. Arndt, *Auflösung einer Aufgabe in der Composition der quadratischen Formen*, J. Reine Angew. Math. **56** (1859), 64

[Arn1859b] F. Arndt, *Ueber die Anzahl der Genera der quadratischen Formen*, J. Reine Angew. Math. **56** (1859), 72–78

[Art2002] S.N. Arteha, *Method of hidden parameters and Pell's equation*, JPJ Algebra Number Theory Appl. **2** (2002), 21–46; cf. p.

[Art1924a] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen I. (Arithmetischer Teil)*, Math. Z. **19** (1924), 153–206,

[Art1924b] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen II. (Analytischer Teil)*, Math. Z. **19** (1924), 207–246

[AZ2001] R.M. Avanzi, U.M. Zannier, *Genus one curves defined by separated variable polynomials and a polynomial Pell equation*, Acta Arith. **99** (2001), no. 3, 227–256

[Ayy1929] A.A.K. Ayyangar, *New light on Bhaskara's Chakravala or cyclic method of solving indeterminate equations of the second degree in two variables*, J. Indian Math. Soc. **18** (1929/30), 225–248

[Ayy1940] A.A.K. Ayyangar, *Theory of the nearest square continued fraction*, J. Mysore Univ. **1** (1940), 21–32; ibid. (1941), 97–117

[Azu1984] T. Azuhata, *On the fundamental units and the class numbers of real quadratic fields* Nagoya Math. J. **95** (1984), 125–135

[Azu1987] T. Azuhata, *On the fundamental units and the class numbers of real quadratic fields. II*, Tokyo J. Math. **10** (1987), no. 2, 259–270

[Bal1999] N. Baldisserri, *The group of primitive quasi-Pythagorean triples* (Italian), Rend. Circ. Mat. Palermo (2) **48** (1999), 299–308; cf. p.

[Bap1989] L. Bapoungué, *Sur la résolubilité de l'équation* $ax^2 + 2bxy - kay^2 = \pm 1$, Thèse Univ. Caen, 1989; see also C. R. Acad. Sci. Paris **309** (1989), 235–238; cf. p.

[Bap1998] L. Bapoungué, *Un critère de résolution pour l'équation diophantienne* $ax^2 + 2bxy - kay^2 = \pm 1$, Expos. Math. **16** (1998), 249–262; cf. p.

[Bap2000a] L. Bapoungué, *Sur la résolubilité de l'équation* $ax^2 + 2bxy - 8ay^2 = \pm 1$, IMHOTEP, J. Afr. Math. Pures Appl. **3** (2000), 97–111; cf. p.

[Bap2000b] L. Bapoungué, *Sur les solutions génerales de l'équation diophantienne* $ax^2 + 2bxy - kay^2 = \pm 1$, Expos. Math. **18** (2000), 165–175; cf. p.

[Bap2002] L. Bapoungué, *The diophantine equation* $ax^2 + 2bxy - 4ay^2 = \pm 1$, Intern. J. Math. Math. Sci. **35** (2003), 2241–2253

[Bar2003] E. Barbeau, *Pell's Equation*, Springer Verlag 2003

[Bas1980] I.G. Bashmakova, *Composition of quadratic forms in the mathematics from the 13th to the 16th century* (Russian), Istor.-Mat. Issled. **25** (1980), 303–314

[Bas1972] I.G. Bashmakova, *Diophantus and diophantine equations*, Updated by Joseph Silverman, The Dolciani Mathematical Expositions **20**, MAA (1997); German Transl. *Diophant und diophantische Gleichungen*, Basel, Stuttgart 1974; Russ. original 1972

[Baz1851a] M. Bazin, *Une question relative aux déterminants*, J. Math. Pure Appl. **16** (1851), 145–160

[Baz1851b] M. Bazin, *Sur la théorie de la composition des formes quadratiques*, J. Math. Pure Appl. **16** (1851), 161–170

[BS1996] R.A. Beauregard, E.R. Suryanarayan, *Pythagorean triples: the hyperbolic view*, College Math. J. 1996; cf. p.

[BS1997] R.A. Beauregard, E.R. Suryanarayan, *Arithmetic Triangles*, Math. Mag. **70** (1997), 105–115; cf. p.

[BS1999] R.A. Beauregard, E.R. Suryanarayan, *Integral Triangles*, Math. Mag. **72** (1999), 287–294; cf. p.

[Beg1777] N. Beguelin, *Solution particulière du problème sur les nombres premiers*, Mem. Acad. Royale Sci. et Belles-Lettres Berlin 1775 (1777), 300–322

[Bel2005] K. Belabas, *Paramétrisation de structures algébriques et densité de discriminants (d'après Bhargava)*, Séminaire Bourbaki 2003/2004, Astérisque **299** (2005), Exp. No. 935, ix, 267–299

[BLS1998] E. Benjamin, F. Lemmermeyer, C. Snyder, *Real quadratic number fields with Abelian Gal(k^2/k)*, J. Number Theory **73** (1998), 182–194

[Ber1853] C.A.W. Berkhan, *Die merkwürdigen Eigenschaften der Pythagoreischen Zahlen*, Eisleben 1853; cf. p.

[Ber1976] L. Bernstein, *Fundamental units and cycles in the period of real quadratic number fields. I*, Pacific J. Math. **63** (1976), 37–61

[Ber1976] L. Bernstein, *Fundamental units and cycles in the period of real quadratic number fields. II*, Pacific J. Math. **63** (1976), no. 1, 63–78

[BH1975] L. Bernstein, H. Hasse, *Ein formales Verfahren zur Herstellung parameterabhängiger Scharen quadratischer Grundeinheiten*, J. Reine Angew. Math. **276** (1975), 206–212

[Ber1990] T.G. Berry, *On periodicity of continued fractions in hyperelliptic function fields*, Arch. Math. (Basel) **55** (1990), no. 3, 259–266

[Bha2001] M. Bhargava, *Higher composition laws*, Ph. D. thesis, Princeton 2001

[Bha2002] M. Bhargava, *Gauss composition and generalizations*, Algorithmic number theory (Sydney, 2002), 1–8, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002

[Bha2004a] M. Bhargava, *Higher composition laws. I: A new view on Gauss composition, and quadratic generalizations*, Ann. Math. **159** (2004), 217–250

[Bha2004b] M. Bhargava, *Higher composition laws. II. On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), no. 2, 865–886

[Bha2004c] M. Bhargava, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360

[Bha2005] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. (2) **162** (2005), no. 2, 1031–1063

[Blo1976] J. Bloom, *On the* 4*-rank of the strict class group of a quadratic number field*, Selected topics on ternary forms and norms (Sem. Number Theory, California Inst. Tech., Pasadena, Calif., 1974/75), Paper No. 8, 4 pp. California Inst. Tech., Pasadena, Calif., 1976

[Boe1974] R. Bölling, *Über den* 3*-Rang von quadratischen Zahlkörpern und den Rang gewisser elliptischer Kurven*, Math. Nachr. **73** (1976), 155–170

[Boe1980] R. Bölling, *Über einen Homomorphismus der rationalen Punkte elliptischer Kurven*, Math. Nachr. **96** (1980), 207–244

[BC1957] Borel, Chowla et al. (eds.), *Seminar on complex multiplication*, Lecture Notes Math 21, Springer-Verlag 1957

[Bo1895] E. Bortolotti, *Sulle frazioni continue algebriche periodiche*, Palermo Rend. **9** (1895), 136–149

[BS1996a] W. Bosma, P. Stevenhagen, *Density Computations for real quadratic units*, Math. Comp. **65** (1996), 1327–1337

[BS1996b] W. Bosma, P. Stevenhagen, *On the computation of quadratic* 2*-class groups*, J. Théor. Nombres **8** (1996), 283–313

[Bou1902] A. Boutin, *Résolution complète de l'équation* $x^2 - (Am^2 + Bm + C)y^2 = 1$ *où* A, B, C *sont des entiers, par une infinité des polynômes en* m, L'Interméd. Math. **9** (1902), 60

[Bou1971a] L. Bouvier, *Sur le 2-groupe des classes de certains corps biquadratiques*, Thèse 3^e cycle, Grenoble

[Bou1971b] L. Bouvier, *Sur le 2-groupe des classes au sens restreint de certaines extensions biquadratiques de* $\mathbb{Q}$, C. R. Acad. Sci. Paris **272** (1971), 193–196

[Bra1919] H. Brandt, *Komposition er binären quadratischen Formen relativ einer Grundform*, J. Reine Angew. Math. **150** (1919), 1–46

[Bra1952] H. Brandt, *Zur Zahlentheorie der ternären quadratischen Formen*, Math. Ann. **124** (1952), 334–342

[Bri1954] W. Briggs, *An elementary proof of a theorem about the representation of primes by quadratic forms*, Can. J. Math. **6** (1954), 353–363

[Bro1983] E. Brown, *The class number and fundamental unit of* $Q(\sqrt{2p})$ *for* $p \equiv 1 \bmod 16$ *a prime*, J. Number Theory **16** (1983), no. 1, 95–99

[BV2007] J. Buchmann, Vollmer, *Binary Quadratic Forms. An Algorithmic Approach*, Springer-Verlag 2007

[Bue1976] D. Buell, *Class groups of quadratic fields*, Math. Comp. **30** (1976),

[Bue1977] D. Buell, *Elliptic curves and class groups of quadratic fields*, J. London Math. Soc. (2) **15** (1977), 19–25

[Bue1989] D. Buell, *Binary Quadratic Forms. Classical theory and modern computations*, Springer Verlag 1989

[BE1995] D.A. Buell, V. Ennola, *On a parametrized family of quadratic and cubic fields*, J. Number Theory **54** (1995), 134–148

[Bue2002] T. Bülow, *Power residue criteria for quadratic units and the negative Pell equation*, Canad. Math. Bull. **24** (2002), no. 2, 55–60

[Bul2008] M. Bullynck, *Mathematical Tables and other ways to Gauss and computation*, Arch. Hist. Exact Sci.

[BE1968] H.S. Butts, D. Estes, *Modules and binary quadratic forms over integral domains*, Linear Algebra Appl. **1** (1968), 153–180

[BP1968] H.S. Butts, G. Pall, *Modules and binary quadratic forms*, Acta Arith. **15** (1968), 23–44

[Bye1954] G.C. Byers, *Class number relations for quadratic forms over* $GF[q,x]$, Duke Math. J. **21** (1954), 445–461

[CON1998] R.M. Campello de Souza, H. M. de Oliveira, A.N. Kauffman, *Trigonometry in finite fields and a new Hartley transform*, Proc. 1998 Int. Symp. Information Theory, Cambridge MA 1998, p. 293

[CON2002] R.M. Campello de Souza, H. M. de Oliveira, A.N. Kauffman, *The Z transform over finite fields*, Int. Telecommunications Symp. Natal, Brazil, 2002

[CON2004] R.M. Campello de Souza, H. M. de Oliveira, A.N. Kauffman, *The discrete cosine transform over prime finite fields*, LNCS **3124** (2004), 482–487

[Can1987] D. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), 95–101

[CGE2000] J.M. Carnicer, M. García-Esnaola, *Lagrange interpolation on conics and cubics*, Computer Aided Geometric Design **19** (2002), 313–326

[Car1915] R.D. Carmichael, *Diophantine Analysis*, 1915; reprint Dover, 1959

[Car1976] J. Carroll, *The Redei-Reichardt theorem*, Selected topics on ternary forms and norms (Sem. Number Theory, California Inst. Tech., Pasadena, Calif., 1974/75), Paper No. 7, 7 pp. California Inst. Tech., Pasadena, Calif., 1976

[Ca1966] J.W.S. Cassels, *Diophantine Equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291

[Cas1978] J.W.S. Cassels, *Rational Quadratic Forms*, Academic Press 1978; Russian transl. 1982

[CB2006] C. Castaño-Bernard, *A level N reduction theory of indefinite binary quadratic forms*, preprint 2006

[Cat1867] E. Catalan, *Rectification et addition à la note sur un problème d'analyse indéterminée*, Atti dell'Accad. Pont. Nuovi Lincei **20** (1867), 1ff; 77ff

[Cay1845] A. Cayley, *On the theory of linear transformations*, Cambridge Math. J. **4** (1845), 1–16; Coll. Math. Papers I (1889), 80–94

[Cay1846] A. Cayley, *Mémoire sur les hyperdéterminants*, J. Reine angew. Math. **30** (1846), 1–37

[Cay1850] A. Cayley, *Note sur un système de certaines formules*, J. Reine angew. Math. **39** (1850), 14–15

[Cay1855] A. Cayley, *Note sur les covariants d'une fonction quadratique, cubique, ou biquadratique à deux indédterminées*, J. Reine angew. Math. **50** (1855), 285–287

[Cay1857] A. Cayley, Quart. J. Math. **1** (1857), 85; 90; Coll. Math. Papers III, 9; 11

[CR1988a] L. Charlap, D. Robbins, *An elementary introduction to elliptic curves*, CRD expos. report **31**, Dec. 1988

[CR1988b] L. Charlap, D. Robbins, *An elementary introduction to elliptic curves II*, CRD expos. report **34**, Dec. 1988

[Cha1837] M. Chasles, *Sur les équations indéterminées du second degré*, J. Math. Pures Appl. **2** (1837), 37–55

[Cha1911] A. Châtelet, *Sur certains ensembles de tabléaux et leur application à la théorie des nombres*, Ann. Ecole Norm. Sup. **28** (1911), 105–202

[Cha1924] A. Châtelet, *Groupes Abelians Finis*, 1924

[Che1851] M.P. Chebyshev (Tchebichef), *Sur les formes quadratiques*, J. Math. Pures Appl. **16** (1851), 257–282

[CP1989] Y.J. Choie, L.A. Parson, *Rational period functions and indefinite binary quadratic forms* I, Math. Ann. **286** (1989), 697–708

[CP1991] Y.J. Choie, L.A. Parson, *Rational period functions and indefinite binary quadratic forms* II, Ill. J. Math. **35** (1991), 374–400

[Chu2008] K.S. Chua, *Inverting the wedge product and Gauss' composition*, preprint 2008

[Cip1903] M. Cipolla, *Un metodo fer la risoluzione della congruenza di secondo grado*, Rend. Acad. Sci. Fis. Mat. Napoli **9** (1903), 154–163

[Cle1865a] A. Clebsch, *Über diejenigen ebenen Kurven, deren Koordinaten rationale Funktionen eines Parameters sind*, J. Reine Angew. Math. **64** (1865), 43–65

[Cle1865b] A. Clebsch, *Über diejenigen Kurven, deren Koordinaten sich als elliptische Funktionen eines Parameters darstellen lassen*, J. Reine Angew. Math. **64** (1865), 210–270

[Coh1962] H. Cohn, *A second course in number theory*, Dover 1962; 2nd ed. as *Advanced number theory*, Dover 1980

[Coh1985] H. Cohn, *Introduction to the Construction of Class Fields*, Cambridge 1985

[CL1981] H. Cohn, J. Lagarias, *Is there a density for the set of primes p such that the class number of $\mathbb{Q}(\sqrt{-p}\,)$ is divisible by 16?*, Colloqu. Math. Soc. Bolyai **34** (1981), 257–280

[CL1983] H. Cohn, J. Lagarias, *On the existence of fields governing the 2-invariants of the class group of $\mathbb{Q}(\sqrt{dp}\,)$ as p varies*, Math. Comp. **41** (1983), 711–730

[Col1817] H.T. Colebrooke, *Algebra, with arithmetic and mensuration, from the sanscrit of Brahmegupta and Bhascara*, London 1817

[CG1995] A. Costa, F. Gerth, *Densities for 4-class ranks of totally complex quadratic extensions of real quadratic fields*, J. Number Theory **54** (1995), no. 2, 274–286

[Co1989] D.A. Cox, *Primes of the form x^2+ny^2. Fermat, Class Field Theory, and Complex Multiplication*, John Wiley 1989

[Cr1973] M. Craig, *A type of class group for imaginary quadratic fields*, Acta Arith. **22** (1973), 449–459

[Cr1977] M. Craig, *A construction for irregular discriminants*, Osaka J. Math. **14** (1977), 365–402

[CO1989] J.E. Cremona, R.W.K. Odoni, *Some density results for negative Pell equations; an application of graph theory*, J. Lond. Math. Soc. (2) **39** (1989), 16–28

[Czu1894] E. Czuber, *Über einen symbolischen Kalkul auf Trägern vom Geschlecht Eins*, Jahresber. DMV **4** (1894), 100–107

[DPY2001] Z.-D. Dai, D.-Y. Pei, J.H. Yang, D.-F. Ye, *Cryptanalysis of a public key cryptosystem based on conic curves*, Electronics Letters **37** (2001), 426–??

[DP1970] P. Damey, J.-J. Payan, *Existence et construction des extensions galoisiennes et non-abéliennes de degré 8 d'un corps de caractéristique differente de 2*, J. Reine Angew. Math. **244** (1970), 37–54

[Da1997] H. Darmon, *Wiles' theorem and the arithmetic of elliptic curves*, in: Modular Forms and Fermat's Last Theorem, G. Cornell et al. (eds.), Springer Verlag 1997, 549–569; cf. p.

[DL1996] H. Darmon, C. Levesque, *Sommes infinies, équations diophantiennes et le dernier théorème de Fermat*, Gazette des Sciences Mathématiques du Québec, Vol. XVIII, Avril 1996; cf. p.

[Daw1994] B. Dawson, *The ring of Pythagorean triples*, Missouri J. Math. Sci. **6** (1994), 72–77; cf. p.

[Dec2005] I. Déchène, *Generalized Jacobians in Cryptography*, Ph.D. thesis McGill 2005

[Dec2005] I. Déchène, *Arithmetic of generalized Jacobians*, preprint 2006

[Ded1857] R. Dedekind, *Abriss einer Theorie der höheren Congruenzen in Bezug auf einen reellen Primzahl-Modulus*, J. Reine Angew. Math. **54** (1857), 1–26

[Ded1905] R. Dedekind, *Über trilineare Formen und die Komposition der binären quadratischen Formen*, J. Reine Angew. Math. **129** (1905), 1–34

[Deg1958] G. Degert, *Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **22** (1958), 92–97

[Den1975] Ch. Denenberg, *Periodic expansions and units in quadratic and cubic number fields*, J. Reine Angew. Math. **278/279** (1975), 266–277

[Des1878a] A. Desboves, *Sur l'emploi des identités algebriques dans la résolution en nombres entiers, des equations d'un degré supérieur au second*, C. R. Acad. Sci. Paris **87** (1878), 321–322

[Des1878b] A. Desboves, *Sur un point de l'historie des mathématiques*, C. R. Acad. Sci. Paris **87** (1878), 925

[Des1878c] A. Desboves, *Deuxième note sur la résolution en nombres entiers de l'équation* $ax^4 + by^4 = cz^2$, C. R. Acad. Sci. Paris **88** (1878), 522–523

[Des1879] A. Desboves, *Mémoire sur la résolution en nombres entiers de l'équation* $aX^m + bY^m = cZ^n$, Nouv. Ann. Math. (2) **18** (1879), 265–279; 398–410; 433–444; 481–499

[Des1880] A. Desboves, *Théorème sur les équations cubiques et biquadratiques*, C. R. Acad. Sci. Paris **90** (1880), 1069–1070

[Des1886] A. Desboves, *Résolution, en nombres entiers et sous sa forme la plus générale, de l'équation cubique, homogène, à trois inconnues*, Nouv. Ann. Math. (3) **5** (1886), 545–579

[Des1945] P. Despujols, *Norme de l'unité fondamentale du corps quadratique absolu*, C. R. Acad. Sci. Paris **221** (1945), 684–685

[Deu1935] M. Deuring, *Algebren*, Springer-Verlag 1935; Chelsea 1948

[Dic1920] L.E. Dickson, *History of the Theory of Numbers*, vol I (1920); vol II (1920); vol III (1923); Chelsea reprint 1952

[Dic1930] L.E. Dickson, *Studies in the Theory of numbers*, Chicago 1930

[Dir1834] G.P.L. Dirichlet, *Einige neue Sätze über unbestimmte Gleichungen*, Abh. Kön. Akad. Wiss. Berlin 1834, 649–664; Gesammelte Werke I, 221–236

[Dir1839] P.G.L. Dirichlet, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew. Math. **19** (1839), 324–369; Werke I, 411–496

[Dir1842] P.G.L. Dirichlet, *Recherches sur les formes quadratiques à coéfficients et à indéterminées complexes*, J. Reine Angew. Math. **24** (1842), 291–371; Werke I, 533–619

[DD1893] P.G.L. Dirichlet, *Vorlesungen über Zahlentheorie*, herausgegeben und mit Zusätzen versehen von R. Dedekind; 4th ed. Braunschweig 1893

[DD1999] P. G. L. Dirichlet, *Lectures on number theory* (R. Dedekind, ed.). Translated from the 1863 German original and with an introduction by John Stillwell. LMS 1999

[Due1991] S. Düllmann, *Ein Algorithmus zur Bestimmung der Klassengruppe positiv definiter quadratischer Formen*, Diss. Univ. d. Saarlandes Saarbrücken, 1991

[DB1972] B.J. Dulin, H.S. Butts, *Composition of binary quadratic forms over integral domains*, Acta Arith. **20** (1972), 223–251

[Eck1984] E. Eckert, *The group of primitive Pythagorean triangles*, Math. Mag. **54** (1984), 22–27; cf. p.

[Edw1977] H.G. Edwards, *Fermat's Last Theorem. A genetic introduction to algebraic number theory*, Springer-Verlag 197?; reprint 1996

[Edw2005] H.G. Edwards, *Essays in constructive mathematics*, Springer-Verlag 2005

[Edw2007a] H.G. Edwards, *Composition of binary quadratic forms and the foundations of mathematics*, in: [GSS2007, p. 129–144]

[Edw2007b] H.G. Edwards, *A normal form for elliptic curves*, Bull. Am. Math. Soc. **44** (2007), 393–422

[Edw2008] H.G. Edwards, *Higher arithmetic. An algorithmic introduction to number theory*, AMS 2008

[Eis1844] G. Eisenstein, *Théorèmes sur les formes cubiques et solution d'une équation du quatrième degré indéterminée*, J. Reine Angew. Math. **27** (1844), 75–79

[Eis1852] G. Eisenstein, *Über die Vergleichung von solchen ternären quadratischen Formen, welche verschiedene Determinanten haben*, Bericht (1852), 350–389; Mathematische Werke II, 722–761

[Elk2007] N. Elkies, *Pythagorean triples and Hilbert's Theorem 90*, `http://www.math.harvard.edu/~elkies/Misc/index.html`

[Els1994] Ch. Elsholtz, *Primzahlen der Form* $4k+1$ *sind Summe von zwei Quadratzahlen*, Mathematik Lehren **62** (1994), 58–61

[Els2003] Ch. Elsholtz, *Kombinatorische Beweise des Zweiquadratesatzes und Verallgemeinerungen*, Math. Sem.ber. (2003), 1–17

[Eps1934] P. Epstein, *Zur Auflösbarkeit der Gleichung* $x^2 - Dy^2 = -1$, J. Reine Angew. Math. **171** (1934), 243–252; cf. p.

[Esc1905] E.B. Escott, *Solution de l'équation* $x^2 - Dy^2 = -1$, L'Interméd Math. **12** (1905), 53; cf. p.

[Eu1747] L. Euler, *Theorematum quorumdam arithmeticorum demonstrationes*, Comm. Acad. Sci. Petrop. **10** (1738) 1747, 125–146; Opera Omnia Ser. I vol. II, Commentationes Arithmeticae, 38–58

[Eul1762] L. Euler, *De resolutione formularum quadraticarum indeterminatarum per numeros integros*, Novi. Comm. Acad. Petrop. **9** (1762/63) 1764, 3–33; Opera Omnia I_2, 576–602

[Eul1765] L. Euler, *De usu novi algorithmi in problemate Pelliano solvendo*, Novi Acad. Sci. Petropol. **11** (1765) 1767, 28–66; Opera Omnia I-3, 73–111

[Eul1773] L. Euler, *Nova subsidia pro resolutione formulae* $axx + 1 = yy$, Sept. 23, 1773; Opusc. anal. **1** (1783), 310; Comm. Arith. Coll. **II**, 35–43; Opera Omnia I-4, 91–104

[Eul1775a] L. Euler, *De insigni promotione scientiae numerorum*, (E 598), Oct. 26, 1775; Opuscula analytica **2** (1785), 275–314; Opera Omnia I-4, 163–196

[Eul1775b] L. Euler, *Novae demonstrationes circa divisores numerorum formae xx+nyy*, (E 610), Nov. 20, 1775; Nova Acta Acad. Sci. Petropol. **1** (1783), 47–74; Opera Omnia I-4, 197–220

[Eu1776] L. Euler, *Extrait d'une lettre de M. Euler à M. Beguelin, en mai 1778*, Opera Omnia I-3, 418–420

[Eu1770] L. Euler, *Vollständige Anleitung zur Algebra*, Petersburg 1770; Russ. Transl. Petersburg 1768/69; Opera Omnia I **1**, 1–498

[EG1965] L. Euler, C. Goldbach, *Briefwechsel 1729 – 1764*, A.P. Juskevic, E. Winter (eds.), Akademie-Verlag 1965

[Fai1991] A. Faisant, *L'équation diophantienne du second degré*, Hermann 1991

[Far1994] R. Farwick, *Kettenbrüche und enge Klassen in reell quadratischen Funktionenkörpern über* $\mathbb{F}_p$, diploma thesis Münster 1994

[Fen1996] K. Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith. **75** (1996), 71–83

[FX2004] K. Feng, M. Xiong, *On elliptic curves* $y^2 = x^3 - n^2x$ *with rank zero*, J. Number Theory **109** (2004), 1–26

[FX2006] K. Feng, Y. Xue, *New series of odd non-congruent numbers*, Science in China, 2006

[FS2007] D.D. Fenster, J. Schwermer, *Composition of quadratic forms: am algebraic perspective*, in [GSS2007, p. 145–158]

[Fla1989] D. Flath, *Introduction to number theory*, Wiley & Sons, New York, 1989

[Fri1918] H. Frick, *Über den Zusammenhang der Perioden quadratischer Formen positiver Determinante mit der Zerlegung einer Zahl in die Summe zweier Quadrate*, Diss. ETH Zürich, 1918

[Fri2004] M. Frick, Addition und Berechnung von Punkten auf rationalen Kegelschnitten, Diploma thesis, Siegen 2004

[Fro1912] F.G. Frobenius (unter Benutzung einer Mitteilung des Herrn Dr. R. Remak), *Über quadratische Formen, die viele Primzahlen darstellen*, Sitz. Kön. Preuß. Akad. Wiss. Berlin (1912), 966–980; Ges. Abh. III, Springer 1968, 573–587

[Fro1954a] A. Fröhlich, *The generalization of a theorem of L. Rédei's*, Quart. J. Math. (2) **5** (1954), 130–140

[Fue1941] R. Fueter, *Vorwort des Herausgebers*, Euler's Opera Omnia I-4 (1941), VII–XXX

[Fur1959] Y. Furuta, *Norm of units of quadratic fields*, J. Math. Soc. Japan **11** (1959), 139–145

[Gau1990] M.-L. Gaunet, *Formes cubiques polynomiales*, C. R. Acad. Sci. Paris Sér. I **311** (1990), no. 9, 491–494

[Gau1801] C.F. Gauss, *Disquisitiones Arithmeticae*, Leipzig 1801; French transl. by Poullet Delisle (1807); reprints 1910, 1953; German transl. by H. Maser (1889); English transl. by A.A. Clarke (1965); 2nd rev. ed. Waterhouse et al. (1986); Spanish transl. by H. Barrantes Campos, M. Josephy and Á. Ruiz Zúñiga (1995)

[Gau1900a] C.F. Gauss, *Zwei Notizen über die Auflösung der Congruenz* $xx+yy+zz \equiv 0 \pmod p$, Werke VIII (1900), 3–4

[Gau1900b] C.F. Gauss, *Werke VIII*, 1900

[GKZ1994] I.M. Gelfand, M.M. Kapranov, A.V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, Birkhäuser Boston, 1994

[Ger1917] A. Gérardin, *Sur l'èquation* $x^2 - Ay^2 = 1$, L'Ens. math. **19** (1917), 316–318; Sphinx-Œdipe **12** June 15, 1917, 1–3; cf. p.

[Ger1990] I.-Kh. I. Gerasim, *On the genesis of Rédei's theory of the equation* $x^2 - Dy^2 = -1$ (Russian), Istor.-Mat. Issled. No. **32-33** (1990), 199–211

[Ger1984] F. Gerth, *The* 4*-class ranks of quadratic fields*, Invent. Math. **77** (1984), no. 3, 489–515

[Ger1989] F. Gerth, *The* 4*-class ranks of quadratic extensions of certain real quadratic fields*, J. Number Theory **33** (1989), no. 1, 18–31

[Goi2001] E. Goins, *A ternary algebra with applications to binary quadratic forms*, Sixth conference for African American Researchers in the mathematical sciences (2000), G.M. N'Guérékata et al. (eds.), Contemp. Math. **284** (2001), 7–12

[GSS2007] , C. Goldstein, N. Schappacher, J. Schwermer, *The shaping of arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*, Springer-Verlag 2007

[Gos1910] Th. Gosset, *On irregular determinants*, Messenger Math. (2) **40** (1910), 135–137

[Gra1973] G. Gras, *Sur les* l*-classes d'idéaux dans les extensions cycliques relatives de degré premier* l I, II, Ann. Inst. Fourier **23** (1973), 1–48; ibid. **23** (1973), 1–44

[Gra1992] G. Gras, *Sur la norme du groupe des unités d'extensions quadratiques relatives*, Acta Arith. **61** (1992), 307–317

[Gra1910] D. Gravé, *Sur une identité dans la théorie des formes binaires quadratiques*, C. R. Acad. Sci. Paris **149** (1910), 770–772

[Gro2003] B. Gross, *An elliptic curve test for Mersenne primes*, preprint 2003; cf. p.

[Gru1874] F. Grube, *Über einige Eulersche Sätze aus der Theorie der quadratischen Formen*, Zeit. Math. Phys. **19** (1874), 492–519

[GH1978] Griffiths, Harris, *Principles of Algebraic Geometry*, Wiley 1978

[Gry1997] A. Grytczuk, *Note on a Pythagorean ring*, Missouri J. Math. Sci. **9** (1997), 83–89; cf. p.

[GLW2000] A. Grytczuk, F. Luca, M. Wojtowicz, *The negative Pell equation and Pythagorean triples*, Proc. Japan Acad. **76** (2000), 91–94; cf. p.

[Gue1882] S. Günther, *Ueber einen Specialfall der Pell'schen Gleichung*, Blätter für das Bayerische Gymnasial- und Realschulwesen **17** (1882), 19–24; cf. p.

[Hae1913a] E. Haentzschel, *Euler und die Weierstraßsche Theorie der elliptischen Funktionen*, Jahresber. DMV **22** (1913), 278–284

[Hae1913b] E. Haentzschel, *Herleitung der Bedingungen für die Lösbarkeit des Fermatschen Problems, die Gleichung $y^3 = a_0x^3+3a_1x^2+3a_2x+a_3$ durch rationale Zahlen zu erfüllen*, Jahresber. DMV **22** (1913), 319–329

[Hae1913c] E. Haentzschel, *Rationale Tetraeder mit kongruenten Seiten*, Sitzungsberichte Berlin **12** (1913), 101–108

[Hae1914a] E. Haentzschel, *Theorie der Heronischen Parallelogramme*, Sitzungsberichte Berlin **13** (1914), 80–89

[Hae1914b] E. Haentzschel, *Die rationalen Vierecke des Inders Brahmagupta*, Sitzungsberichte Berlin **14** (1915), 23–31

[Hae1914c] E. Haentzschel, J. Reine Angew. Math. **144** (1914), 275–283

[Hae1915] E. Haentzschel, *Lösung einer Aufgabe aus der Arithmetik des Diophant*, Jahresber. DMV **24** (1915), 467–471

[Hae1916a] E. Haentzschel, *Theorie der Dreiecke mit rationalen Maßzahlen der Seiten und der Seitenhalbierenden*, Jahresber. DMV **25** (1916), 333–351

[Hae1916b] E. Haentzschel, *Bemerkungen zu der vorstehenden Notiz des Herrn v. Schaewen*, Jahresber. DMV **25** (1916), 357–359

[HK1984] F. Halter-Koch, *Über den 4-Rang der Klassengruppe quadratischer Zahlkörper*, J. Number Theory **19** (1984), 219–227

[HaK1987] F. Halter-Koch, *Über Pellsche Gleichungen und Kettenbrüche*, Arch. Math. **49** (1987), 29–37

[Ha2010] S. Hambleton, F. Lemmermeyer, *A family of groups on the integer points of Pell surfaces*, preprint 2009

[Han1981] P. Hanlon, *Applications of the quaternions to the study of imaginary quadratic ring class groups*, Diss. Pasadena, 1981

[HW1986] K. Hardy, K. Williams, *On the solvability of the diophantine equation $dV^2 - 2eVW - dW^2 = 1$*, Pac. J. Math. **124** (1986), 145–158; cf. p.

[Har1875] A. Harnack, *Über die Verwerthung der elliptischen Functionen für die Geometrie der Curven dritten Grades*, Math. Ann. **9** (1875) 1–54

[Har1878a] D.S. Hart, *Solution of an indeterminate problem*, Analyst **5** (1878), 118–119; cf. p.

[Har1878b] D.S. Hart, *A new method for solving equations of the form $x^2 - Ay^2 = 1$*, Educat. Times **28** (1878), 29

[Has1927] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil Ia, Beweise zu I.*, Jahresber. DMV **36** (1927), 233–311

[Has1934] H. Hasse, *Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern*, Abh. Math. Semin. Hamburg **10** (1934), 325–348

[Has1965] H. Hasse, *Über mehrklassige, aber eingeschlechtige reell-quadratische Zahlkörper*, Elem. Math. **20** (1965), 49–59

[Has1951] H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3** (1951), 45–51

[Has1967] H. Hasse, *Vorlesungen über Klassenkörpertheorie*, Physica Verlag 1967

[Hay1987] D.R. Hayes, *Real quadratic function fields*, CMS Conf. Proc. **7** (1987), 203–236
[Haz1997] F. Hazama, *Pell equations for polynomials*, Indag. Math. **8** (1997), 387–397
[HB1984] D.R. Heath-Brown, *Fermat's two squares theorem*, Invariant (1984)
[HB1993] D.R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), 171–195
[Hee1952] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253; cf. p.
[Hei1854] Heine, *Fernere Untersuchungen über ganze Functionen*, J. Reine Angew. Math. **48** (1854), 243–266
[Hel1986] Y. Hellegouarch, *Elliptic Curves*, unpublished lecture notes 1986
[Hel1989] Y. Hellegouarch, *Positive definite binary quadratic forms over* $k[X]$, Number theory (Ulm, 1987), 93–119, Springer-Verlag 1989
[Her1848] C. Hermite, *Sur un théorème relatif aux nombres entiers*, J. Math. Pures Appl. **13** (1848), ??; Œuvres I, p. 264
[Her1849] C. Hermite, *Démonstration élémentaire d'une proposition relative aux diviseurs de* $x^2 + Ay^2$, J. Math. Pures Appl. **14** (1849), ??; Œuvres I, p. 274–275
[Her1851] C. Hermite, *Sur l'introduction des variables continues dans la théorie des nombres*, J. Reine Angew. Math. **41** (1851), 191–216; euvres I (1905), 164–192
[Her1857] C. Hermite, *Lettre à Cayley "Sur les formes cubiques"*, Quart. J. Math. **1** (1857), 88–89; ŒuvresI, 437–439
[Her1859] C. Hermite, *Sur Théorie des equations modulaires*, C.R.Acad. Sci. Paris **48** (1859), 940; 1079; 1096; ibid. **49** (1859), p. 16; 110; 141; Œuvres II, 38–82
[Her1957] C. S. Herz *Construction of Class Fields*, Seminar on complex multiplication (Chowla et al. eds.) (1957), Lecture Notes Math. 21, Springer Verlag
[Hew1902] L.I. Hewes, *Note on irregular determinants*, Bull. Amer. Math. Soc. **9** (1902), 141–142
[HH1891] D. Hilbert, A. Hurwitz, *Über die diophantischen Gleichungen vom Geschlecht Null*, Acta Math. **14** (1891), 217–224
[Hir1973] F. Hirzebruch, *Hilbert modular surfaces*, L'Ens. Math. **19** (1973), 183–281
[Hla2000] E. Hlawka, *Pythagorean triples*, Number theory, Birkhäuser, Basel (2000), 141–155; cf. p.
[HM2000] J.W. Hoffman, J. Morales, *Arithmetic of binary cubic forms*, Enseign. Math. (2) **46** (2000), 61–94
[Hof1944] J.E. Hofmann, *Studien zur Zahlentheorie Fermats*, Abh. Preuss. Akad. Wiss. 1944, 19 pp.
[Ho1958] L. Holzer, *Zahlentheorie* Teil I, Teubner 1958
[Hou2007] Ch. Houzel, *Elliptic functions and arithmetic*, in: [GSS2007, 291–314]
[Hu1915] G. Humbert, C. R. Acad. Sci. Paris **160** (1915), 647–650
[Hur1994] J. Hurrelbrink, *Circulant graphs and 4-ranks of ideal class groups*, Canad. J. Math. **46** (1994), no. 1, 169–183
[Hur1889] Hurwitz, *Über eine besondere Art der Kettenbruch-Entwickelung reeller Größen*, Acta Math. **12** (1889), 367
[Hur1917] A. Hurwitz, *Über ternäre diophantische Gleichungen dritten Grades*, Vierteljahrschrift d. Naturf. Ges. Zürich **62** (1917), 207–229; Werke II, 446–468
[Ili1982] C.S. Iliopoulos, *Analysis of an algorithm for composition of binary quadratic forms*, J. Algorithms **3** (1982), 157–159
[Ina1940] E. Inaba, *Über die Struktur der* l*-Klassengruppe zyklischer Zahlkörper vom Primzahlgrad* l, J. Fac. Sci. Imp. Univ. Tokyo. Sect. I. **4** (1940), 61–115
[Iwa2005] A. Iwaomoto, Masters thesis (Japan.), Kyoto University, 2005
[Iya1935] S. Iyanaga, *Sur les classes d'idéaux dans les corps quadratiques*, Actual. scient. et industr. 1935, Nr. 197 (Exposés math. VIII), 15 p. (1935)

[Jac2000a] T. Jackson, *A short proof that every prime* $p \equiv 3 \bmod 8$ *is of the form* x^2+2y^2, Amer. Math. Monthly **107** (2000), 447

[Jac2000b] T. Jackson, *Automorphs and Involutions*, Tatra Mt. Math. Publ. **20** (2000), 59–63

[Jac1835] C.G. Jacobi, *De usu theoriae integralium ellipticorum et integralium abelianorum in analysi Diophantea*, J. Reine Angew. Math. **13** (1835), 353–355; Werke 2 (1882), 51–55

[JW2009] M.J. Jacobson, H.C. Williams, *Solving the Pell Equation*, Springer-Verlag 2009

[Jak1995] B. Jakob, *Pythagoreische Tripel, algebraische Kurven und Diophantische Gleichungen*, Didaktik d. Math. **23** (1995), 99-105

[Jen1935] E.D. Jenkins, *On the composition of quadratic forms*, Bull. Amer. Math. Soc. (1935), 719–726

[Jen1962a] Ch. U. Jensen, *On the solvability of a certain class of non-Pellian equations*, Math. Scand. **10** (1962), 71–84

[Jen1962b] Ch. U. Jensen, *On the Diophantine equation* $\xi^2 - 2m^2\eta^2 = -1$, Math. Scand. **11** (1962), 58–62

[Jen1962c] Ch. U. Jensen, *Über eine Klasse nicht-Pellscher Gleichungen*, J. Reine Angew. Math. **209** (1962), 36–38

[Ji1995] C.G. Ji, *Norms of fundamental units in real quadratic function fields*, J. Nanjing Norm. Univ. Nat. Sci. Ed. **18** (1995), no. 4, 7–12

[Ji1997] C.G. Ji, *The norms of fundamental units in real quadratic function fields* J. Math. (Wuhan) **17** (1997), no. 2, 173–178

[Jon1950] B.W. Jones, *The Arithmetic Theory of Quadratic Forms*, MAA 1950

[Jon1898] E. de Jonquières, *Formules générales donnant des valeurs de D pour lesquelles l'équation* $t^2 - Du^2 = -1$ *est résoluble en nombres entiers*, C. R. Acad. Sci. Paris **126** (1898), 1837

[Jou18??] Joubert, *Sur les fonctions elliptiques et sur son application à la théorie des nombres*,

[Joy2009] M. Joye,

[Jue1896] C. Juel, *Ueber die Parameterbestimmung von Punkten auf Curven zweiter und dritter Ordnung. Eine geometrische Einleitung in die Theorie der logarithmischen und elliptischen Funktionen*, Math. Ann. **47** (1896), 72–104; cf. p.

[Ju1916] G. Julia, C. R. Acad. Sci. Paris **162** (1916), 151–154

[Ju1936] H.W.E. Jung, *Einführung in die Theorie der quadratischen Zahlkörper*, Leipzig 1936

[Kah1970] D. Kahle, *Bestimmung der pythagoreischen Zahlentripel mit Hilfe linearer Transformationen*, Math.-phys. Semesterber. **17** (1970), 193–195

[Kap1930] H. Kapferer, *Über das Kriterium der Rationalität einer algebraischen Kurve*, Sitz.-ber. (1930), 123–128

[Kap1976] P. Kaplan, *Sur le* 2*-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. **283/284** (1976), 313–363

[Ka1977] P. Kaplan, *Cycles d'ordre au moins* 16 *dans le* 2*-groupe des classes d'idéaux de certains corps quadratiques*, Mém. Bull. Soc. Math. France **49/50** (1977), 113–124

[Kap1983] P. Kaplan, *À propos des équations antipelliennes*, Enseign. Math. (2) **29** (1983), 323–327

[KW1994] P. Kaplan, K.S. Williams, *An elementary remark on the distribution of integers representable by a positive-definite integral binary quadratic form*, Arch. Math. **62** (1994), 38–42

[Kap1968] I. Kaplansky, *Composition of binary quadratic forms*, Studia Math. **31** (1968), 523–530

[Kat1991] S. Katayama, *On fundamental units of real quadratic fields with norm* -1, Proc. Japan Acad. **67** (1991), 343–345

[Kat1992] S. Katayama, *On fundamental units of real quadratic fields with norm* $+1$, Proc. Japan Acad. **68** (1992), 18–20

[Kat2001] S. Katok, *Continued fractions, hyperbolic geometry and quadratic forms*, lecture notes 2001

[Kha1990] S.P. Khare, *Ramanujan's function* $\tau(n)$ *and binary quadratic form* $x^2 + 23y^2$, J. Bihar Math. Soc. **13** (1990), 31–34

[KP1999] Kh. Khessami Pilerud, *On the Diophantine equation* $x^2 - Ny^2 = -1$, (Russian) Vestnik Moskov. Univ. Ser. I Mat. Mekh. (1999), no. 2, 65–67; Engl. transl. Moscow Univ. Math. Bull. **54** (1999), no. 2, 48–49; cf. p.

[Kin1995] R.J. Kingan, *Tournaments and ideal class groups*, Canad. Math. Bull. **38** (1995), no. 3, 330–333

[Kis1976] H. Kisilevsky, *The Rédei-Reichardt theorem—a new proof*, Selected topics on ternary forms and norms (Sem. Number Theory, California Inst. Tech., Pasadena, Calif., 1974/75), Paper No. 6, 4 pp. California Inst. Tech., Pasadena, Calif., 1976

[Kit1993] Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge University Press 1993

[Kle1893] F. Klein, *Ueber die Composition der binären quadratischen Formen*, Gött. Nachr. (1893), 106–1O9

[Kne1982a] M. Kneser, *Komposition binärer quadratischer Formen*, Abh. Braunschweig. Wiss. Ges. **33** (1982), 41–42

[Kne1982b] M. Kneser, *Composition of binary quadratic forms*, J. Number Theory **15** (1982), no. 3, 406–413

[Koe1987] M. Koecher, *On endomorphisms of degree* 2, Proc. Indian Acad. Sci. **97** (1987), 179–188

[KN1993] Y. Kohno, T. Nakahara, *Oriented graphs of* 2*-class group constructions of quadratic fields* (Japanese), Combinatorial structure in mathematical models (Kyoto, 1993), RIMS Kokyuroku **853**, (1993), 133–147

[KKN1992] Y. Kohno, S. Kitamura, T. Nakahara, 2*-rank component evaluation for class groups of quadratic fields using graphs* (Japanese), Optimal combinatorial structures on discrete mathematical models (Kyoto, 1992) Surikaisekikenkyusho Kokyuroku No. **820** (1993), 1–15

[Kol1982] A. Koller, *Primfaktorsuche mit der Pellschen Gleichung*, Siemens Forsch. Entwickl. 11 (1982), no. 1, 51–61, iv.

[Kon1901] H. Konen, *Geschichte der Gleichung* $t^2 - Du^2 = 1$, Leipzig (1901), 132 pp

[Koe1911] R. König, *Zur arithmetischen Theorie der auf einem algebraischen Gebilde existierenden Funktionen*, Ber. Math. Phys. Kl. Ges. d. Wiss. Leipzig **63** (1911), 348–368

[Koe1912] R. König, *Über die quadratischen Formen mit rationalen Funktionen als Koeffizienten*, Monatsh. Math. Phys. **23** (1912), 321–346

[Ko1913a] R. König, *Beiträge zur Arithmetik der hyperelliptischen Funktionenkörper*, J. Reine angew. Math. **142** (1913), 191–210

[Koe1913b] R. König, *Über quadratische Formen und Zahlkörper, sowie zwei Gruppensätze*, J.ber. DMV **22** (1913), 239–254 239–254

[Koe1895] E. Kötter, *Note über ebene Curven dritter Ordnung*, J. Reine Angew. Math. **114** (1895), 170–180

[Kor1916] A. Korselt, *Über eine diophantische Aufgabe*, Jahresber. DMV **25** (1916), 138–139, 351–353

[Kor1981] U. Korte, *Binäre quadratische Formen über Zahlkörpern und Funktionenkörpern einer Unbestimmten mit endlichem Konstantenkörper*, Diss. Univ. Münster, 1981

[Kro1864] L. Kronecker, *Über den Gebrauch der Dirichletschen Methoden in der Theorie der quadratischen Formen*, Monatsber. Akad. Wiss. Berlin 1864, 285–303

[Kum1848] E. Kummer, *Über die Vierecke, deren Seiten und Diagonalen rational sind*, J. Reine Angew. Math. **37** (1848), 1–20; Coll. Papers I, 253–273

[Kut1974] M. Kutsuna, *On the fundamental units of real quadratic fields*, Proc. Japan Acad. **50** (1974), 580–583

[Lac1984] G. Lachaud, *Calibre et fonction Zéta des corps quadratiques réels*, Univ. Nice, L.A. **168** (1984), 23pp

[Lac1988] G. Lachaud, *Continued fractions, binary quadratic forms, quadratic fields, and zeta functions*, Proc. Math. Workshop 1988, 1–56

[Lag1980a] J.C. Lagarias, *On the computational complexity of determining the solvability or unsolvability of the equation* $X^2 - DY^2 = -1$, Trans. Amer. Math. Soc. **260** (1980), no. 2, 485–508

[Lag1980b] J.C. Lagarias, *On determining the* 4*-rank of the ideal class group of a quadratic field* J. Number Theory **12** (1980), 191–196

[Lag1980c] J.C. Lagarias, *Worst-case complexity bounds for algorithms in the theory of integral quadratic forms*, J. Algorithms **1** (1980), no. 2, 142–186

[Lag2003] J. Lagarias, private communication, 2003–2004

[Lag1774] J. L. Lagrange, *Additions aux éléments d'Algèbre d'Euler*; Lyon 1774; Œuvres **7/8** (1973); Engl. Transl. in *Elements of Algebra*, Springer-Verlag 1972; German Transl.: *Lagrange's Zusätze zu Euler's Elementen der Algebra. Unbestimmte Analysis*, Ostwald's Klassiker No. 103, Leipzig 1898

[Lag1773] J. L. Lagrange, *Recherches d'Arithmétique*, Nouv. Mém. Acad. Sci. Berlin (1773), 2ème partie (1775); Œuvres III

[Lal1907] T. Lalesco, *Sur la représentation des nombres par les classes de formes appartenant à un déterminant donné*, Bull. Soc. Math. France **35** (1907), 248–252

[LMD1933] C.G. Latimer, C.C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. Math. **74** (1933), 313–316

[Lav2002] T. Lavrinenko, *Solving an indeterminate third degree equation in rational numbers*, Rev. Hist. Math. **8** (2002), 67–111

[Leg1798] A.M. Legendre, *Essais sur la théorie des nombres*, 1798; 2nd. ed. 1808

[Leg1808] A.M. Legendre, *Théorie des Nombres*, second edition 1808

[Leg1830] A.M. Legendre, *Théorie des Nombres*, third edition 1830

[Leh1967] D.H. Lehmer, *Technology applied to the theory of numbers*, in: Studies in Number Theory, vol. 6, MAA 1967, 117–151

[Le1999] F. Lemmermeyer, *A note on Pépin's counter examples to the Hasse principle for curves of genus* 1, Abh. Math. Sem. Hamburg **69** (1999), 335–345

[Le2000a] F. Lemmermeyer, *Kreise und Quadrate modulo p*, Math. Sem. Ber. **47** (2000), 51–73; cf. p.

[Le2000b] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer Verlag 2000

[Le2000c] F. Lemmermeyer, *On Tate-Shafarevich groups of some elliptic curves*, Proc. Conf. Graz 1998, (2000), 277–291

[Le2003a] F. Lemmermeyer, *Higher Descent on Pell Conics. I. From Legendre to Selmer*, preprint 2003; cf. p.

[Le2003b] F. Lemmermeyer, *Higher Descent on Pell Conics. II. Two Centuries of Missed Opportunities*, preprint 2003; cf. p.

[Le2003c] F. Lemmermeyer, *Higher Descent on Pell Conics. III. The First* 2*-Descent*, preprint 2003; cf. p.

[Le2003d] F. Lemmermeyer, *Some families of non-congruent numbers*, Acta Arith. **110** (2003), 15–36

[Len1982] H.W. Lenstra, *On the calculation of regulators and class numbers of quadratic fields*, Number theory days, 1980 (Exeter, 1980), 123–150, Cambridge 1982

[Len2002] H. Lenstra, *Solving the Pell equation*, Notices AMS **49** (2002), 182–192

[LeV1969] W.J. LeVeque, *A brief survey of diophantine equations*, Studies in Number Theory vol. 6, MAA 1969, p. 4–24

[Lev1988] C. Levesque, *Continued fraction expansions and fundamental units*, J. Math. Phys. Sci. **22** (1988), no. 1, 11–44

[Lev1988] C. Levesque, G. Rhin, *A few classes of periodic continued fractions*, Utilitas Math. **30** (1986), 79–107

[Lev1914] Levi, Leipziger Ber. **66** (1914), 26–37

[LT2000] D. Li, Y. Tian, *On the Birch-Swinnerton-Dyer conjecture of elliptic curves* $E_D : y^2 = x^3 - D^2x$, Acta Math. Sin. **16** (2000), no. 2, 229–236

[Lin1940] C.E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht eins*, Ph.D. thesis Uppsala 1940

[Lin1999] S. Lindhurst, *An analysis of Shanks's algorithm for computing square roots in finite fields*, CRM Proc. Lecture Notes **19** (1999), 231–242

[Lip1857] R. Lipschitz, *Einige Sätze aus der Theorie der quadratischen Formen*, J. Reine Angew. Math. **53** (1857), 238–259

[Lub1961] S. Lubeslki, *Unpublished results on number theory II. Composition theory of binary quadratic forms*, Acta Arith. **7** (1961), 9–17

[Luc1877] E. Lucas, *Recherches sur plusieurs ouvrages de Léonard de Pise et sur diverses questions d'arithmétique superieure*, Bull. Bibl. Stor. Sci. Mat. Fis. **10** (1877), 129–193; 239–293

[Luc1878a] E. Lucas, *Sur l'analyse indéterminée du troisième degré et sur la question 802 (Sylvester)*, Nouv. Ann. Math. (2) **17** (1878), 507–514

[Luc1878b] E. Lucas, *Sur l'équation indéterminée* $x^3 + y^3 = az^3$, Nouv. Ann. (2) **17** (1878), 425–426

[Lut1937] E. Lutz, *Sur l'équation* $y^2 = x^3 - Ax - B$ *dans les corps p-adiques*, J. Reine Angew. Math. **177** (1937), 237–247

[Mad2001] D.J. Madden, *Constructing families of long continued fractions* Pac. J. Math. **198** (2001), 123–147

[Mab1879] N. Malebranche, cf. C. Henry, Bull. Bibl. Storia Sc. Mat. Fis. **12** (1879), 696–698

[Mal1906] E. Malo, *Solution de l'équation* $x^2 - Dy^2 = -1$, L'Interméd. Math. **13** (1906), 246

[Mat1891] G.B. Mathews, *Irregular determinants and subtriplicate forms*, Messenger Math. **20** (1891), 70–74

[Man1972] Y. Manin, *Cubic Forms* (Russian), Moscow 1972; Engl. transl. Amsterdam 1986

[Man1896] P. Mansion, *Rapport*, Belg. Bull. (3) **30** (1896), 189–193

[Mar1962] J. Mariani, *The group of the pythagorean numbers*, Amer. Math. Mon. **69** (1962), 125–128; cf. p.

[Mat1891] G.B. Mathews, Mess. Math. **20** (1891), 70–74

[Mat1892] G.B. Mathews, *Theory of numbers*, Cambridge 1892; reprint Chelsea 1961

[Mat1911] G.B. Mathews, Proc. London Math. Soc. (2) **9** (1911), 200–204

[McL2003] J. Mc Laughlin, *Polynomial solutions of Pell's equation and fundamental units in real quadratic fields*, J. London Math. Soc. (2) **67** (2003), 16–28

[McL2003] J. Mc Laughlin, *Multi-variable polynomial solutions to Pell's equation and fundamental units in real quadratic fields*, Pacific J. Math. **210** (2003), 335–349

[Lau2003] K.E. Lauter, *The equivalence of the geometric and alebraic gropus law for Jacobians of genus* 2 *curves*, Contemp. Math. **324** (2003), 165–171

[Mer1880] F. Mertens, *Zur Lehre von den quadratischen Formen mit positiver Determinante*, J. Reine Angew. Math. **99** (1880), 332–338

[Mer1894] F. Mertens, *Über die Äquivalenz der reducirten binären quadratischen Formen von positiver Determinante*, Wien. Ber. **103** (1894), 995–1004

[Mer1895] F. Mertens, *Ueber die Composition der binären quadratischen Formen*, Wien. Ber. **104** (1895), 103–143

[Mer1906] F. Mertens, *Ein Beweis des Satzes, dass jede Klasse von ganzzahligen primitiven binären quadratischen Formen des Hauptgeschlechts durch Duplikation entsteht*, J. Reine Angew. Math. **129** (1906), 181–186

[Mer1918a] F. Mertens, *Die Äquivalenz der reduzierten binären quadratischen Formen von positiver Determinante*, Wien. Ber. **127** (1918), 1019–1034

[Mer1918b] F. Mertens, *Herleitung eines vollständigen Systems von ganzzahligen primitiven binären quadratischen Formen σ-ter Art der Determinante Dp^2 aus einem ebensolchen System einer Determinante D, wo p eine Primzahl bezeichnet*, Wien. Ber. **127** (1918), 1799–1828

[MR1993] J. Minac, C. Reis, *Trigonometry over finite fields*, Expos. Math. (1993),

[Min1996] Zh. MingZhi, *Factoring Integers with conics*, J. Sichuan Univ. **33** (1996), 356–359

[Min1873a] B. Minnigerode, *Über die Vertheilung der quadratischen Formen mit complexen Coefficienten und Veränderlichen in Geschlechter*, Gött. Nachr. 1873, 160–180

[Min1873b] B. Minnigerode, *Über eine neue Methode, die Pellsche Gleichung aufzulösen*, Gött. Nachr. **12** (1873), 619–653

[Mit1997] D.A. Mitkin, *On some diophantine equations connected with Pellian equation*, Proc. Int. Conf. in honour of J. Kubilius; New Trends in Probab. Stat. **4** (1997), 27–32

[Moe1830] A.F. Möbius, *Beiträge zur Lehre von den Kettenbrüchen nebst einem Anhange dioptrischen Inhalts*, J. Reine Angew. Math. **6** (1830), 215–243; Werke IV

[Mol1996] R. Mollin, *Quadratics*, CRC 1996

[Mol1997] R.A. Mollin, *Polynomial solutions for Pell's equation revisited*, Indian J. Pure Appl. Math. **28** (1997), 429–438

[Mol2001a] R. Mollin, *Polynomials of Pellian type and continued fractions*, Serdica Math. J. **27** (2001), 317–342

[Mol2001b] R. Mollin, *Proof of some conjectures by Kaplansky*, C.R. Math. Rep. Sci. Canada **23** (2001), 60–64

[Mol2007] R. Mollin, *On a generalized Kaplansky conjecture*, Int. J. Contemp. Math. Sciences **2** (2007), 411–416

[MW1991] R. Mollin, H.C. Williams, *On a determination of real quadratic fields of class number one and related continued fraction period length less than* 25, Proc. Japan Acad. **67** (1991), no. 1, 20–25

[Mor1912] L.J. Mordell, *Note on irregular determinants*, Messenger Math. (2) **42** (1912), 124.

[Mor1914] L.J. Mordell, Proc. London Math. Soc. (2) **13** (1914), 60–80; ibid. **18** (1919), v

[Mor1922] L.J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambr. Phil. Soc. **21** (1922), 179–192

[Mor1873] C. Moreau, *Solution de la question 1055*, Nouv. Ann. (2) **12** (1873) 330–331

[Mor1986] J. Morita, *A transformation group of the Pythagorean numbers*, Tsukuba J. Math. **10** (1986), no. 1, 151–153; cf. p.

[Mor1979] P. Morton, *On Rédei's theory of the Pell equation*, J. Reine Angew. Math. **307/308** (1979), 373–398

[Mor1982a] P. Morton, *Density results for the* 2*-classgroups and fundamental units of real quadratic fields*, Studia Sci. Math. Hungar.**17** (1982), no. 1-4, 21–43
[Mor1982b] P. Morton, *Density result for the* 2*-classgroups of imaginary quadratic fields*, J. Reine Angew. Math. **332** (1982), 156–187
[Mor1983] P. Morton, *The quadratic number fields with cyclic* 2*-classgroups*, Pac. J. Math. **108** (1983), 165–175
[Mor1990a] P. Morton, *Governing fields for the* 2*-class group of* $\mathbb{Q}(\sqrt{-q_1q_2p}\,)$ *and a related reciprocity law*, Acta Arith. **55** (1990), 267–290
[Mor1990b] P. Morton, *On the nonexistence of abelian conditions governing solvability of the* -1 *Pell equation*, J. Reine Angew. Math. **405** (1990), 147–155
[Mul2004] S. Müller, *On the computation of square roots in finite fields*, Designs, Codes and Cryptography **31** (2004), 301–312
[Nag1925] T. Nagell, *Om den unbestemte ligning* $x^2 - Dy^2 = 1$, Norsk. Mat. Tidskr. **7** (1925), 33–46
[Nag1933] T. Nagell, *Über die Lösbarkeit der Gleichung* $x^2-Dy^2 = -1$, Ark. Mat. Astron. Fys. B **23**, No.6 (1933), 1–5
[Nag1952] T. Nagell, *Un théorème arithmétique sur les coniques*, Arkiv f. Mat. **2** (1952), 247–250; cf. p.
[Nag1954] T. Nagell, *On a special class of Diophantine equations of the second degree*, Ark. Mat. **3** (1954), 51–65
[Nag1909] J. v. Sz. Nagy, *Über ein Theorem von Jacobi und seine Verallgemeinerung*, Jahresber. DMV **18** (1909), 4–7
[Nag1915] J. v. Sz. Nagy, *Über den symbolischen Kalkul von Emil Weyr auf den elliptischen Kurven*, Jahresber. DMV **24** (1915), 457–460
[Nat1976] M.B. Nathanson, *Polynomial Pell's equations*, Proc. Amer. Math. Soc. **56** (1976), 89–92
[Nek2003] J. Nekovar, *Elliptic curves and modular forms*, lecture notes DEA 2003/04, Paris VI; cf. p.
[Neu1981] M. Neubrand, *Scharen quadratischer Zahlkörper mit gleichgebauten Einheiten*, Acta Arith. **39** (1981), 125–132
[New1977] M. Newman, *A note on an equation related to the Pell equation*, Amer. Math. Monthly (1977), 365–366
[New1971] I. Newton, *The Mathematical Papers of Isaac Newton*, vol. IV, Cambridge 1971
[Nie1908] B. Niewenglowski, *Note sur les equations* $x^2 - ay^2 = 1$ *et* $x^2 - ay^2 = -1$, Bull. Soc. Math. France **35** (1907), 126–131; cf. also Wiadomi Mat. Warsaw **12** (1908), 1–26 (Polish); cf. p.
[Nor1974] H.-U. Nordhoff, *Explizite Darstellungen von Einheiten und ihre Anwendung auf Mehrklassigkeitsfragen bei reell-quadratischen Zahlkörpern. I*, J. Reine Angew. Math. **268/269** (1974), 131–149
[Nor2002] S. Northshield, *Associativity of the Secant Method*, Amer. Math. Monthly **109** (2002), 246–257
[Olv1999] P.J. Olver, *Classical Invariant Theory*, LMS Student Texts, CUP 1999 LMS
[Olt1853] Oltramare, *Considérations générales sur les racines des nombres premiers*, J. Reine Angew. Math. **45** (1853), 303–344
[OM1973] O. T. O'Meara, *Introduction to quadratic forms*, Springer Verlag 1973; reprint 2000
[Ono1994] K. Ono, *Variations on a theme of Euler. Quadratic forms, elliptic curves, and Hopf maps*, Plenum Press 1994
[Ono1985] T. Ono, *A generalization of Gauss's theorem on the genera of quadratic forms*, Proc. Japan Acad. **61** (1985), 109–111
[Ori1977a] B. Oriat, *Rélations entre les 2-groupes des classes d'idéaux des extensions quadratiques* $k(\sqrt{d}\,)$ *et* $k(\sqrt{-d}\,)$, Ann. Inst. Fourier **27** (1977), No.2, 37–59

[Ori1977b] B. Oriat, *Rélations entre les 2-groupes des classes d'ideaux de $k(\sqrt{d})$ et $k(\sqrt{-d})$*, Astérisque **41-42** (1977), 247–249

[Ori1976] B. Oriat, *Rélation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres*, Bull. Soc. Math. Fr. **104** (1976), 301–307

[Pal1936] G. Pall, *Note on irregular determinants*, J. London Math. Soc. **11** (1936), 34–35; sh. S.

[Pal1935] G. Pall, *Binary quadratic discriminants differing by square factors*, Amer. J. Math. **57** (1935), 789–799

[Pal1948] G. Pall, *Composition of binary quadratic forms*, Bull. Amer. Math. Soc. **54** (1948), 1171–1175

[Pal1969] G. Pall, *Discriminantal divisors of binary quadratic forms*, J. Number Theory **1** (1969), 525–533

[Pal1973] G. Pall, *Some aspects of Gaussian composition*, Acta Arith. **24** (1973), 401–408

[Pal1976] G. Pall, *Pythagorean triples, Gaussian composition, and spinor genera*, Adv. Math. **19** (1976), 1–5

[dPa1906] L. du Pasquier, *Zahlentheorie der Tettarionen*, Vierteljahresschrift Naturf. Ges. Zürich **51** (1906), 55–130

[Pen1996] R.C. Penner, *The geometry of the Gauss product*, J. Math. Sci. **81** (1996), no. 3, 2700–2718

[Per1986] R. Peralta, *A simple and fast probabilistic algorithm for computing square roots modulo a prime number*, IEEE Trans. Inf. Theory **32** (1986), 846–847

[Per1913] O. Perron, *Die Lehre von den Kettenbrüchen*, 1913; 2nd ed. 1929; 3rd. ed. 1954/1957; Engl. Transl. *The Theory of continued fractions* by C. Snyder, 2010

[Pep1874] Th. Pépin, *Théorèmes d'analyse indéterminée*, C. R. Acad. Sci. Paris **78** (1874), 144–148

[Pep1876] T. Pépin, *Nouvelles formules pour réduire à un carré la valeur d'un polynôme rationnel du quatrième degré*, Atti Accad. Pont. Nuovi Lincei **30** (1876/77), 211–237

[Pep1879] Th. Pépin, *Théorèmes d'analyse indéterminée*, C. R. Acad. Sci. Paris **88** (1879), 1255–1257

[Pep1880a] Th. Pépin, *Nouveaux théorèmes sur l'équation indéterminée $ax^4 + by^4 = z^2$*, C. R. Acad. Sci. Paris **91** (1880), 100–101

[Pep1880b] Th. Pépin, *Composition des formes quadratiques binaires*, Atti Acad. Pont. Nuovi Lincei **33** (1879/80), 6–73

[Pep1882a] Th. Pépin, *Nouveaux théorèmes sur l'équation indéterminée $ax^4 + by^4 = z^2$*, C. R. Acad. Sci. Paris **94** (1882), 122–124

[Pep1882b] Th. Pépin, *Sur la classification des formes quadratiques binaires*, Acc. P. d. N. L. **33** (1882), 354–391

[Pep1883] Th. Pépin, Atti Accad. Pont. Nuovi Lincei **37** (1883/84), 227–294

[Pep1885] Th. Pépin, Atti Accad. Pont. Nuovi Lincei **39** (1885/86), 23–87

[Per1913] O. Perron, *Die Lehre von den Kettenbrüchen*, Teubner 1913

[Pet1926] K. Petr, *Über die Pellsche Gleichung*, Rozpravy **35** (1926), 7pp

[Pet1927] K. Petr, *On Pell's equation* (Czech), Casopis **56** (1927), 57–66

[Pet1928] K. Petr, *On the composition of binary quadratic forms* (Czech), Rozpravy **38**, Nr. 17 (1928)

[Per1887] J. Perott, *Sur l'équation $t^2 - Du^2 = -1$. Premier mémoire*, J. Reine Angew. Math. **102** (1887), 185–225

[Pfa1867] Pfaff, *Neuere Geometrie*, Erlangen 1867

[Pic1882] G. Pick, *Über die Integration hyperelliptischer Differentiale durch Logarithmen*, Wiener Ber. **85** (1882), [Ple1982] W. Plesken, *Automorphs of ternary quadratic forms*, in: Ternary quadratic forms and norms (O. Taussky, ed.), Lect. Notes Pure Appl. Math. **79** (1982), 5–30

[Poi1901] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, J. Math. Pures Appl. (5) **7** (1901), 161–233; Œuvres 5 (1950), 483–548

[vdP2001] A. van der Poorten, *The Hermite-Serret Algorithm and* 12^2+33^2, in: Cryptography and computational number theory, K.-Y. Lam et al. (eds.) Proceedings of the workshop CCNT'99, Singapore, November 22-26, 1999. Prog. Comput. Sci. Appl. Log. 20 (2001), 129–136

[vdP2003a] A. van der Poorten, *Review 2003i:11040*, MathSciNet; cf. p.

[vdP2003b] A. van der Poorten, *A Note on NUCOMP*, Math. Comput. **72** (2003), 1935–1946

[PW1999] A. van der Poorten, H.C. Williams, *On certain continued fraction expansions of fixed period length*, Acta Arith. **89** (1999), no. 1, 23–35

[PS1997] V. Prasolov, Y. Solovyev, *Elliptic Functions and Elliptic Integrals*, Transl. Math. Monographs **170**, AMS 1997; cf. p.

[Pta1909] J. Ptaszycki, *Sur un théorème d'analyse indéterminée, énoncé par Jacobi*, Jahresber. DMV **18** (1909), 1–3

[Pum1968] D. Pumplün, *Über die Klassenzahl und die Grundeinheit des reellquadratischen Zahlkörpers*, J. Reine Angew. Math. **230** (1968), 177–210

[Rab1913a] Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, Proc. 5. Intern. Math. Congr. 1912 **1** (1913), 418–421

[Rab1913b] Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*, J. Reine Angew. Math. **142** (1813), 153–164

[Rad1956] Rademacher, *Zur Theorie der Dedekindschen Summen*, Math. Z. **63** (1956), 445–463

[Ram1994] A.M.S. Ramasamy, *Polynomial solutions for the Pell's equation*, Indian J. Pure Appl. Math. **25** (1994), no. 6, 577–581

[Red1932] L. Rédei, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, Math. Naturwiss. Anz. Ungar. Akad. d. Wiss. **49** (1932), 338–363

[Red1935a] L. Rédei, *Über die Pellsche Gleichung* $t^2 - du^2 = -1$, J. Reine Angew. Math. **173** (1935), 193–221; transl. from Mat. Termeszett. Ertes. **54** (1936), 1–44

[Red1935b] L. Rédei, *Über einige Mittelwertfragen im quadratischen Zahlkörper*, Journ. Reine Angew. Math. **174** (1935), 15–55

[Red1935c] L. Rédei, *Ein asymptotisches Verhalten der absoluten Klassengruppe des quadratischen Zahlkörpers und die Pellsche Gleichung*, Jahresbericht D. M. V. **45** (1935), 78 kursiv

[Red1937] L. Rédei, *Über die D-Zerfällungen zweiter Art* (Hungarian; German summary), Math.-nat. Anz. Ungar. Akad. Wiss. **56** (1937), 89–125

[Red1943] L. Rédei, *Über den geraden Teil der Ringklassengruppe quadratischer Zahlkörper, die Pellsche Gleichung und die diophantische Gleichung* $rx^2+sy^2 = z^{2^n}$ *I, II, III*, Math. Naturwiss. Anz. Ungar. Akad. d. Wiss. **62** (1943), 13–34, 35–47, 48–62

[Red1953] L. Rédei, *Die* 2*-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung*, Acta Math. Acad. Sci. Hungaricae **4** (1953), 31–87

[RR1933] L. Rédei, H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1933), 69–74

[Reh1982] H.P. Rehm, *On a theorem of Gauss concerning the number of integral solutions of the equation* $x^2 + y^2 + z^2 = m$, in: Ternary quadratic forms and norms (O. Taussky, ed.), Lect. Notes Pure Appl. Math. **79** (1982), 31–38

[Reh2006] H.P. Rehm *Binäre ganzzahlige quadratische Formen*, lecture notes Univ. Karlsruhe, 2006

[Re1942] H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18

[Rei1963] H. Reichardt, *Über Dirichlet's zahlentheoretische Arbeiten*, Bericht von der Dirichlet-Tagung, Akademie-Verlag Berlin 1963

[Rei1999] G. Reißner, *Zur Komposition binärer quadratischer Moduln über kommutativen Ringen*, Ph.D. Diss. Univ. Bochum, 1999

[Ri1901] G. Ricalde, Interméd. Math. **8** (1901), 256

[Ric1864] C. Richaud, *Énoncés de quelques théorèmes sur la possibilité de l'équation $x^2 - Ny^2 = -1$ en nombres entiers*, J. Math. Pures Appl. (2) **9** (1864), 384–388

[Ric1865a] C. Richaud, *Démonstrations de quelques théorèmes concernant la résolution en nombres entiers de l'équation $x^2 - Ny^2 = -1$*, J. Math. Pures Appl. (2) **10** (1865), 235–292

[Ric1865b] C. Richaud, *Sur la résolution des équations $x^2 - Ay^2 = \pm 1$*, Atti Accad. Pont. Nuovi Lincei **19** (1865), 177–182

[Ric1866] C. Richaud, *Démonstrations de quelques théorèmes concernant la résolution en nombres entiers de l'équation $x^2 - Ny^2 = -1$*, J. Math. Pures Appl. (2) **11** (1866), 145–176

[Ric1971] B. Rice, *Quaternions and binary quadratic forms*, Proc. Amer. Math. Soc. **27** (1971), 1–7

[Ris1978] J. Riss, *La composition des formes quadratiques binaires (d'après Gauss)*, Sém. Théor. Nombr. Bordeaux (1978), exp. 18, 16pp

[Rob1878] S. Roberts, *On the decomposition of certain numbers into sums of two square integers by continued fractions*, Proc. London Math. Soc. **9** (1877/78), p. 187

[Rob1879] S. Roberts, *On forms of numbers determined by continued fractions*, Proc. London Math. Soc. **10** (1878/79), 29–41

[Sal1879] G. Salmon, *A tratise on the higher plane curves*, 3rd ed. 1879

[Sam1988] P. Samuel, *Projective Geometry*, Sprinver-Verlag 1988

[San1925a] G. Sansone, *Sulle equazioni indeterminate delle unità di norma negativa dei corpi quadratici reali*, Rend. Acad. d. L. Roma (6) **2** (1925), 479–484; cf. p.

[San1925b] G. Sansone, *Ancora sulle equazioni indeterminate delle unità di norma negativa dei corpi quadratici reali*, Rend. Acad. d. L. Roma (6) **2** (1925), 548–554; cf. p.

[Sas1986] R. Sasaki, *A characterization of certain real quadratic fields*, Proc. Japan Acad. **62** (1986), 97–100

[Sch1909] P. v. Schaewen, *$Ax^3 + Bx^2y + Cxy^2 + Dy^3 = z^3$ in rationalen Zahlen zu lösen*, Jahresber. DMV **18** (1909), 7–14

[Sch1916] P. v. Schaewen, *Bemerkungen zu den Abhandlungen des Herrn Haentzschel im 24. Bande S. 467 ff. und im 25. Bande S. 139 ff.*, Jahresber. DMV **25** (1916), 354–357

[Sch1990] N. Schappacher, *Développement de la loi de groupe sur une cubique*, Séminaire Théor. Nombres, Paris 1988–1989, 159–184; Progr. Math. **91** (1990); cf. p.

[Sch1932] D. Schepel, *Over de Vergelejking van Pell*, Ph. D. thesis Groningen, 1932

[Sch1869] E. Schering, *Die Fundamental-Classen der zusammensetzbaren arithmetischen Formen*, Abh. Gött. Ges. Wiss. **14** (1869)

[Sch1908] L. Schlesinger, *Über ein Problem der Diophantischen Analysis bei Fermat, Euler, Jacobi und Poincaré*, Jahresber. DMV **17** (1908), 57–67

[Sch1839] Th. Schönemann, *Ueber die Congruenz $x^2 + y^2 \equiv 1 \pmod p$*, J. Reine Angew. Math. **19** (1839), 93–112; cf. p.

[Sch1934] A. Scholz, *Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$*, Math. Z. **39** (1934), 95–111

[Sch1939] A. Scholz, *Einführung in die Zahlentheorie*, Göschen 1939
[Sch1982] R. Schoof, *Quadratic fields and factorization*, Computational methods in number theory, Part II, 235–286, Math. Centre Tracts **155**, Amsterdam 1982
[Sch1985] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), 483–494
[Sch1898] K. Schwering, *Geometrische Aufgaben mit rationalen Lösungen*, Pr. **458** Gymn. Düren, 1898, 15 pp;
[Sch1902] K. Schwering, *Anwendungen des Abelschen Theorems auf die Lösung der diophantischen Gleichungen* $x^3 + Ay^3 = z^3$ *und* $x^3 + y^3 = z^2$, Arch. Math. Phys. (3) **2** (1902), 285–288
[Scr1984] C. Scriba, *Zur Geschichte der Bestimmung rationaler Punkte auf elliptischen Kurven – Das Problem von Behā-Eddin 'Amūli*, Ber. Sitz. Joachim Jungius-Ges. Wiss., Hamburg **1** (1982/83), No.6, 52 S. (1984)
[See1831] L.A. Seeber, *Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen*, Math. Abh. **1**, Freiburg 1831
[Seg1894] J.A. de Séguier, *Formes quadratiques et multiplication complexe*, 1894
[Sel1963] C.-O. Selenius, *Kettenbruchtheoretische Erklärung der zyklischen Methode zur Lösung der Bhaskara-Pell-Gleichung*, Acta Acad. Aboensis **23** (1963), no. 10
[Sel1975] C.-O. Selenius, *Rationale of the chakravala process of Jayadeva and Bhaskara II*, Hist. Math. **2** (1975), 167–184
[Sha1970] D. Shanks, *Class number, a theory of factorization, and genera*, Proc. Symp. Pure Math. **20** (1970), 415–440
[Sha1971] D. Shanks, *Gauss's Ternary form reduction and the* 2*-Sylow subgroup*, Math. Comp. **25** (1971), 837–853; Corr.: ibid. **32** (1978), 1328–1329
[Sha1972a] D. Shanks, *Five number-theoretic algorithms*, Proc. 2nd Manitoba Conf. Numer. Math., Manitoba, Canada (1972), 51–70
[Sha1972b] D. Shanks, *The infrastructure of a real quadratic field and its applications*, Proc. Number Theory Conf. Boulder 1972, pp. 217–224.
[Sha1978] D. Shanks, *A matrix underlying the composition of quadratic forms and its implications for cubic extensions*, Notices Amer. Math. Soc. **25** (1978), p. A305
[Sh1989a] D. Shanks, *On Gauss and Composition I*, in *Number Theory and Applications* (R. Mollin, ed.), 1989, 163–178
[Sh1989b] D. Shanks, *On Gauss and Composition II*, in *Number Theory and Applications* (R. Mollin, ed.), 1989, 179–204
[SW1972] D. Shanks, P. Weinberger, *A quadratic field of prime discriminant requiring three generators for its class group, and related theory*, Acta Arith. **21** (1972), 71–87; sh. S.
[Sha2001] P. Shastri, *Integral points on the unit circle*, J. Number Theory **91** (2001), 67–70; cf. p.
[Shi1996] P. Shiu, *Involutions associated with sums of two squares*, Publ. Inst. Math. (Beograd) **59** (1996), 18–30
[SMD1931] G. Shover, C.C. MacDuffee, , Bull. Amer. Math. Soc. **37** (1931), 434–438
[Shy1975] J.M. Shyr, *On relative class numbers of certain quadratic extensions*, Bull. Amer. Math. Soc. **81** (1975), 500–502
[Shy1979] J.M. Shyr, *Class numbers of binary quadratic forms over algebraic number fields*, J. Reine Angew. Math. **307/308** (1979), 353–364
[Sie1846] H. Siebeck, , J. Reine Angew. Math. **33** (1846), 71
[ST1992] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag 1992; cf. p.
[Sim2006] D. Simon, *Sur la paramétrisation des solutions des équations quadratiques*, J. Théor. Nombres Bordeaux **18** (2006), 265–283

[Smi1864] H.J.S. Smith, *On complex binary quadratic forms*, Proc. Roy. Soc. London **13** (1864), 278–298; Coll. Math. Papers I (1894), 418–442

[Smi18??] H.J.S. Smith, *On the orders and genera of ternary quadratic forms*, Phil. Trans. London Math. Soc. **157**, 255–298; Coll. Math. Papers I (1894), 455–509

[Smi1865] H.J.S. Smith, *Report on the theory of numbers*, 1859–1865; reprint Chelsea 1965

[Smo1991] C. Smorynski, *Logical Number Theory I. An Introduction*, Springer-Verlag 1991

[Sol1994] R. Soleng, *Homomorphisms from the group of rational points on elliptic curves to clas groups of quadratic number fields*, J. Number Theory **46** (1994), 214–229

[Spe1895] G. Speckman, *Über die Auflösung der Pell'schen Gleichung*, Archiv Math. Phys. (2) **13** (1895), 330

[Spe1912] A. Speiser, *Über die Komposition der binären quadratischen Formen*, Weber-Festschrift (1912), 375–395

[Sta1896] P. Stäckel, *Review JFM 27.0337.02*, Jahrbuch Fortschritte der Mathematik **27** (1896), p. 337; cf. p.

[vSt1846] von Staudt, *Beiträge zur Geometrie der Lage*, 1846, 1856, 1857

[Ste1966] Steinig, *On Euler's idoneal numbers*, Elemente Math. **21** (1966), 73–88

[Ste1899] E. Steinitz, *Zur Theorie der Moduln*, Math. Ann. **52** (1899), 1–57

[Ste1834] M.A. Stern, *Theorie der Kettenbrüche und ihre Anwendung*, J. Reine Angew. Math. **11** (1834), 311–350

[Ste1857] M.A. Stern, *Zur Theorie der periodischen Kettenbrüche*, J. Reine Angew. Math. **8** (1857), 1–102

[Ste1866] M.A. Stern, *Über die Eigenschaften der periodischen negativen Kettenbrüche, welche die Wuadratwurzel aus einer ganzen positiven Zahl darstellen*, Abh. Königl. Akad. Wiss. Göttingen **12** (1866), 3–48

[Ste1988] P. Stevenhagen, *Class groups and governing fields*, Ph. D. thesis, Berkeley 1988

[Ste1989] P. Stevenhagen, *Ray class groups and governing fields*, Théorie des nombres, Années 1988/89, Publ. Math. Fac. Sci. Besançon (1989)

[Ste1993a] P. Stevenhagen, *Rédei-matrices and applications*, Number theory (Paris, 1992–1993), 245–259, London Math. Soc. Lecture Note Ser., 215

[Ste1993b] P. Stevenhagen, *Divisibility by 2-powers of certain quadratic class numbers*, J. Number Theory **43** (1993), 1–19

[Ste1993c] P. Stevenhagen, *The number of real quadratic fields having units of negative norm*, Exp. Math. **2** (1993), 121–136

[Str1979] A.E. Stratton, *The curious substitution $z = \tan\theta/2$ and the Pythagorean theorem*, Amer. Math. Monthly **86** (1979), 584–585

[Stu1875] R. Sturm, *Über die v. Staudt'schen Würfe*, Math. Ann **9** (1875), 333–346

[Sue1995] Y. Sueyoshi, *Comparison of the 4-ranks of the narrow ideal class groups of the quadratic fields $\mathbb{Q}(\sqrt{m}\,)$ and $\mathbb{Q}(\sqrt{-m}\,)$* (Japanese), Algebraic number theory and Fermat's problem (Kyoto, 1995), Surikaisekikenkyusho Kokyuroku No. **971** (1996), 134–144

[Sue1997] Y. Sueyoshi, *On a comparison of the 4-ranks of the narrow ideal class groups of $\mathbb{Q}(\sqrt{m}\,)$ and $\mathbb{Q}(\sqrt{-m}\,)$*, Kyushu J. Math. **51** (1997), 261–272

[Sue2000] Y. Sueyoshi, *Relations betwen the narrow 4-class ranks of quadratic number fields*, Adv. Stud. Contemp. Math. **2** (2000), 47–58

[Sue2001] Y. Sueyoshi, *On Rédei matrices with minimal rank*, Far East J. Math. Sci. (FJMS) **3** (2001), no. 1, 121–128

[Syl1858] J.J. Sylvester, *Note on the algebraic theory of derivative points of curves of the third degree*, Phil. Mag. **16** (1858), 116–119; Mathem. Papers II, 107–109

[Syl1880] J.J. Sylvester, *On certain ternary cubic-form equations*, Amer. J. Math. **2** (1879), 280–285, 357–393; ibid. **3** (1880), 58–88, 179–189; Math. Papers III, 312–391

[Syl1881] J.J. Sylvester, *Mathematical Question 6243*, Educational Times **34** (1881), 21–22; cf. p.

[Sze2007] T.-W. Sze, *On taking square roots and constructing quadratic nonresidues over finite fields*, preprint 2007

[TY1993] A. Takaku, S.-I. Yoshimoto, *Fundamental unit of the real quadratic field* $\mathbb{Q}(\sqrt{v(v^3+1)(v^6+3v^3+3)})$, Ryukyu Math. J. **6** (1993), 57–67

[Tan1996] L. Tan, *The group of rational points on the unit circle*, Math. Mag. **69** (1996), 163–171; cf. p.

[Ta1997] B. Tangedal, *A question of Stark*, Pac. J. Math. **180** (1997), 187–199; cf. p.

[Tan1889] F. Tano, *Sur quelques théorèmes de Dirichlet*, J. Reine Angew. Math. **105** (1889), 160–169

[Tau1949] O. Taussky, *On a theorem of Latimer and MacDuffee*, Can. J. Math. 1, 300-302 (1949)

[Tau1970] O. Taussky, *Sums of squares*, Amer. Math. Monthly **77** (1970), 805–830; cf. p.

[Tau1981] O. Taussky, *Composition of binary integral quadratic forms via integral* 2×2-*matrices and composition of matrix classes*, Linear and Multilinear Algebra **10** (1981), no. 4, 309–318

[Tau1981] O. Taussky, *The many aspects of the Pythagorean triangles*, Linear Algebra Appl. **43** (1982), 285–295

[Tau1982] O. Taussky (ed.), *Ternary quadratic forms and norms*, Marcel Dekker 1982

[vTh1926] M. von Thielmann, *Zur Pellschen Gleichung*, Math. Ann. **95** (1926), 635–640

[Tik1994] V. Tikhomirov, *Three paths to Mt. Fermat. Let Lagrange, Zagier and Minkowski be your guides*, Quantum **4** (1994), 5–7

[Tom1995] K. Tomita, *Explicit representation of fundamental units of some real quadratic fields*, Proc. Japan Acad. **71** (1995), 41–43

[Tom1997] K. Tomita, *Explicit representation of fundamental units of some real quadratic fields. II*, J. Number Theory **63** (1997), no. 2, 275–285

[Ton1891] A. Tonelli, *Bemerkungen über die Auflösung quadratischer Congruenzen*, Gött. Nachr. 1891, 344–346

[Tow1980] J. Towber, *Composition of oriented binary quadratic form-classes over commutative rings*, Adv. Math. **36** (1980), 1–107

[Tro1969] H. F. Trotter, *On the norms of units in quadratic fields*, Proc. Amer. Math. Soc. **22** (1969), 198–201

[Tur1915] E. Turrière, *Le problème de Jean de Palerme et de Léonard de Pise*, Ens. Math. **17** (1915), 315–324; cf. p.

[Tur1994] S.M. Turner, *Square roots mod p*, Amer. Math. Monthly **101** (1994), 443–449

[Tur1916] E. Turrière, *Notions d'arithmogéométrie*, Ens. math. **18** (1916), 81–110, 397–428; cf. p.

[Tur1917] E. Turrière, *Notions d'arithmogéométrie*, Ens. math. **19** (1917), 159–191, 233–272; cf. p.

[Tur1918] E. Turrière, *Notions d'arithmogéométrie*, Ens. math. **20** (1918), 161–174; cf. p.

[Ueh1989] T. Uehara, *On the* 4*-rank of the narrow ideal class group of a quadratic field*, J. Number Theory **31** (1989), 167–1731

[VaP1895] C. de la Vallée Poussin, *Recherches arithmétiques sur la composition des formes binaires quadratiques*, Mém. Acad. Belgique **53** (1895/96), mem. no. 3, 59pp.

[Vau1985] Th. P. Vaughan, *The construction of unramified cyclic quartic extensions of* $\mathbb{Q}(\sqrt{-m})$, Math. Comp. **45** (1985), 233–242

[Vaz1997a] A. Vazzana, *On the* 2*-primary part of* K_2 *of rings of integers in certain quadratic number fields*, Acta Arith. **80** (1997), 225–235

[Vaz1997b] A. Vazzana, *Elementary abelian* 2*-primary parts of* $K_2\mathcal{O}$ *and related graphs in certain quadratic number fields*, Acta Arith. **81** (1997), No.3, 253–264

[VY1910] O. Veblen, J.W. Young, *Projective Geometry I*, Ginn & Co. 1910; cf. p.

[Ven1922] B.A. Venkow, *On the arithmetic of quaternions*, Bull. Acad. Sci. URSS **16** (1922), 205–246

[Ven1970] B.A. Venkov, *Elementary Number Theory*, Engl. Transl. 1970

[Vie1631] Viète, *Ad logisticam speciosam Notae Priores*, 1631

[Wal1952] A. Walfisz, *Pell's Equation* (Russian), Tbilisi 1952; 90 pp

[Wal1988] G. Walsh, *The Pell equation and powerful numbers*, M. Sc. thesis, Univ. Calgary 1988

[Wal2002] G. Walsh, *On a question of Kaplansky*, Amer. Math. Monthly **109** (2002), no. 7, 660–661

[Wal2007] G. Walsh, *On a question of Kaplansky II*,

[Wan2008] S. Wang, *On certain triple systems, elliptic curves, and Gauss theory of quadratic forms*, Ph.D. thesis Johns Hopkins Univ. 2008

[Wat1994] W.C. Waterhouse, *A counterexample for Germain*, Amer. Math. Monthly **101** (1994), 140–150

[WY2003] W.A. Webb, H. Yokota, *Polynomial Pell's equation*, Proc. Amer. Math. Soc. **131** (2003), 993–1006

[Web1907] H. Weber, *Über die Komposition der quadratischen Formen*, Gött. Nachr. (1907), 86–100

[Web1939] W. Weber, *Die Pellsche Gleichung*, Deutsche Math., Beiheft 1 (1939), 151 pp.

[Wei1977] A. Weil, *Fermat et l'équation de Pell*, Prismata (1977), 441–448; Coll. Papers, 413–419

[We1928] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1928), 281–315

[We1930] A. Weil, *Sur un théorème de Mordell*, Bull. Sci. Math. (2) **54** (1930), 182–191

[Wei1981] A. Weil, *Sur les origines de la géométrie algébrique*, Compos. Math. **44** (1981), 395–406

[Wei1984] A. Weil, *Number Theory. An approach through history from Hammurapi to Legendre*, Birkhäuser 1984

[Wei1986] A. Weil, *Gauss et la composition des formes quadratiques binaires*, Aspects of mathematics and its applications, Collect. Pap. Hon. L. Nachbin, 895–912 (1986).

[Wei1989] A. Weil, *On Eisenstein's copy of the Disquisitiones*, Algebraic number theory, 463–469, Adv. Stud. Pure Math. **17**, 1989

[Wei1986] B. Weis, *Zur Berechnung der Einheitengruppe und der Klassengruppen in quadratischen Kongruenzfunktionenkörpern*, diploma thesis Saarbrücken 1986

[Wer1907] A.S. Werebrusow, Math. Soc. Moscow **26** (1907), 115–129

[Whi1912] E.E. Whitford, *The Pell equation*, New York 1912, 193 pp

[Wil2002] H.C. Williams, *Some generalizations of the S_n sequence of Shanks*, Acta Arith. **69** (1995), no. 3, 199–215

[Wil2002] H.C. Williams, *Solving the Pell equation*, Proc. Millenial Conference on Number Theory (Urbana 2000), Peters 2002, 397–435

[WL1994] K. S. Williams, D. Liu, *Representation of primes by the principal form of negative discriminant Δ when $h(\Delta)$ is* 4, Tamkang J. Math. **25** (1994), 321–334

[Woi2001] M. Wojtowicz, *Algebraic structures on some sets of Pythagorean triples. II*, Missouri J. Math. Sci. **13** (2001), 17–23; cf. p.

[Yam1970] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76

[Yam1971] Y. Yamamoto, *Real quadratic number fields with large funamental units*, Osaka J. Math. **8** (1971), 261–270

[Yok1968] H. Yokoi, *On real quadratic fields containing units with norm* -1, Nagoya Math. J. **33** (1968), 139–152

[Yok1970] H. Yokoi, On the fundamental unit of real quadratic fields with norm 1. J. Number Theory **2** (1970), 106–115

[Yu2001] J. Yu, *On arithmetic of hyperelliptic curves*, Aspects of Mathematics, HKU 2001, 395–415

[Zag1975a] D. Zagier, *Nombres de classes et fractions continues*, Journ. Arithm. Bordeaux, Astérisque **24–25** (1975), 81–97

[Zag1975b] D. Zagier, *A Kronecker limit formula for real quadratic fields*, Math. Ann. **213** (1975), 153–184

[Zag1981] D. Zagier, *Zetafunktionen und quadratische Körper*, Springer-Verlag 1981

[Zag1990] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \bmod 4$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990), 144

[Zag1991] D. Zagier, *The Birch-Swinnerton-Dyer conjecture from a naive point of view*, Arithmetic algebraic geometry (Texel, 1989), 377–389, Progr. Math., **89** 1991

[ZZ1991] P. Zanardo, U. Zannier, *The group of Pythagorean triples in number fields*, Ann. Mat. Pura Appl. (4) **159** (1991), 81–88; cf. p.

[Zha1997] Ch. Zhao, *A criterion for elliptic curves with lowest* 2*-power in* $L(1)$, Math. Proc. Cambridge Philos. Soc. **121** (1997), no. 3, 385–400

[Zha2001] Ch. Zhao, *A criterion for elliptic curves with second lowest 2-power in* $L(1)$, Math. Proc. Cambridge Philos. Soc. **131** (2001), no. 3, 385–404

[Zhe1998] Ch. ZhengFu, *A public key cryptosystem based on conic curves over finite fields* $\mathbb{F}_p$, Chinacrypt 1998, 45–49

[Zin1974] E. W. Zink, *Über die Klassengruppe einer absolut zyklischen Erweiterung*, Diss. Humboldt Univ. Berlin (1974)

[Zur1936] E. Zurl, *Theorie der reduziert regelmäßigen Kettenbrüche*, Math. Ann. **110** (1936), 679–717

Author Index

Subject Index