4. BINARY QUADRATIC FORMS

4.1. What integers are represented by a given binary quadratic form?.

An integer n is represented by the *binary quadratic form* $ax^2+bxy+cy^2$ if there exist integers r and s such that $n=ar^2+brs+cs^2$. In the seventeenth century Fermat showed the first such result, that the primes represented by the binary quadratic form x^2+y^2 are 2 and those primes $\equiv 1 \pmod 4$, and thence determined all integers that are the sum of two squares (see exercises 4.1a and 4.1b). One can similarly ask for the integers represented by x^2+2y^2, or x^2+3y^2, or $2x^2+3y^2$, or any binary quadratic form $ax^2+bxy+cy^2$. For the first few examples, an analogous theory works but things get less straightforward as the discriminant $d:=b^2-4ac$ gets larger (in absolute value).

The integers n that are represented by $x^2+2xy+2y^2$ are the same as those represented by x^2+y^2, for if $n=u^2+2uv+2v^2$ then $n=(u+v)^2+v^2$, and if $n=r^2+s^2$ then $n=(r-s)^2+2(r-s)s+2s^2$. Thus we call these two forms *equivalent* and, in general, binary quadratic form f is equivalent to $F(X,Y)=f(\alpha X+\beta Y,\gamma X+\delta Y)$ whenever $\alpha,\beta,\gamma,\delta$ are integers with $\alpha\delta-\beta\gamma=1$,[1] and so f and F represent the same integers. Therefore to determine what numbers are represented by a given binary quadratic form, we can study any binary quadratic form in the same equivalence class. If $f(x,y)=ax^2+bxy+cy^2$ and $F(X,Y)=AX^2+BXY+CY^2$ above, note that $A=f(\alpha,\gamma)$, $C=f(\beta,\delta)$ and $B^2-4AC=b^2-4ac$ (in fact $B-b=2(a\alpha\beta+b\beta\gamma+c\gamma\delta)$).

For now we will study the case where the discriminant $d<0$ (since it is easier), following ideas of Gauss. First note that if $f(x,y)=ax^2+bxy+cy^2$ then $4af(x,y)=(2ax+by)^2+|d|y^2$ and so is either always positive (if $a>0$), else always negative. Replacing f by $-f$ in the latter case we develop the theory of positive definite quadratic forms, and one can then easily deduce all the analogous results for negative definite f. Note that if $f(u,v)=0$ with u,v real then $u=v=0$ since the discriminant is negative, and thus the ratio of non-zero ordinates of a zero is never real. The integers represented by the quadratic form $gf(x,y)$ are of the form gn where n is represented by $gf(x,y)$, so we assume that $\gcd(a,b,c)=1$.

Gauss observed that it is possible to find a unique *reduced* binary quadratic form in each equivalence class, that is with

$$-a<b\le a<c \quad\text{or}\quad 0\le b\le a=c. \tag{4.1.1}$$

To prove that there is such a reduced binary quadratic form in each equivalence class Gauss provided the following simple algorithm. If one is given a form $aX^2+bXY+cY^2$ which is not reduced then

[1] If our main objective is to determine which forms obviously represent the same integers then we should also allow $\alpha\delta-\beta\gamma=-1$. However the theory is more complicated when we allow this.

Typeset by $\mathcal{AMS}$-TEX

• If $c < a$, or if $c = a$ and $b < 0$, then let $a' = c,\ b' = -b,\ c' = a$ so that $aX^2 + bXY + cY^2 \sim a(-y)^2 + bx(-y) + cx^2 = a'x^2 + b'xy + c'y^2$,

• Otherwise $a \le c$ and b is not in the range $-a < b \le a$. Now let $b' \equiv b \pmod{2a}$ be that residue with $-a < b' \le a$. Write $b' = b + 2ak$ and $c' = f(k, 1)$ so that $aX^2 + bXY + cY^2 \sim a(x + ky)^2 + b(x + ky)y + cy^2 = ax^2 + b'xy + c'y^2$.

In either case the binary quadratic form $aX^2 + bXY + cY^2$ is equivalent to $a'X^2 + b'XY + c'Y^2$, and we now repeat the algorithm with this latter form. Note that (a', b') is a pair of integers with $|b'| + a' \le |b| + a$, with equality only when $c = a$ or $b = -a$, respectively. One can therefore deduce that the algorithm must end in a finite number of steps; and when it ends, we have a reduced binary quadratic form.

Now if $ax^2 + bxy + cy^2$ is reduced with $b^2 - 4ac = d < 0$ then $-d = 4ac - b^2 \ge 4aa - a^2 = 3a^2$ so that $a \le \sqrt{|d|/3}$. Hence there are only finitely many reduced binary quadratic forms of any given negative discriminant d, since $a \le \sqrt{|d|/3}$ then $-a < b \le a$ and c is given by $(b^2 - d)/4a$. For example, for $d = -4$, $a \le 1$ so that $a = 1$, and $-a < b \le a$ with $b^2 + 4$ divisible by 4, so that $b = 0$ and hence $c = 1$. That is, there is exactly one reduced binary quadratic forms of discriminant -4, namely $x^2 + y^2$, and hence just one equivalence class of binary quadratic forms of discriminant -4. The *class number*, $h(d)$, denotes the number of equivalence classes of binary quadratic forms of discriminant d.

We say that n is *properly* represented by $aX^2 + bXY + cY^2$ if there exist coprime integers α and γ such that $n = a\alpha^2 + b\alpha\gamma + c\gamma^2$. (Hence, above, A and C are properly represented by f.) In this case select integers β and δ for which $\alpha\delta - \beta\gamma = 1$ and then, letting $X = \alpha x + \beta y, Y = \gamma x + \delta z$, we have that $f(x, y) = aX^2 + bXY + cY^2$ is equivalent to $f'(x, y) = nx^2 + b'xy + c'y^2$, for certain integers b', c', and f' represents n. But f' has the same discriminant as f, so that $d = (b')^2 - 4nc'$; in particular d is a square mod $4n$.

On the other hand suppose that d is a square mod $4n$. Then select b so that $b^2 \equiv d \pmod{4n}$ and $c = (b^2 - d)/4n$, to obtain a binary quadratic form $nx^2 + bxy + cy^2$ which properly represents n. Therefore we have proved:

Proposition 4.1. *Integer n is properly represented by some binary quadratic form of discriminant d if and only if d is a square mod $4n$.*

This gives another proof of Fermat's result: A prime p can be represented by a binary quadratic form of discriminant -4 if and only if -4 is a square mod $4p$, and therefore $p = 2$ or $\left(\frac{-1}{p}\right) = 1$ so that $p \equiv 1 \pmod 4$. We have proved that there is just one equivalence class of binary quadratic forms of discriminant -4, and therefore any representative, such as $x^2 + y^2$, properly represents 2 and any prime $\equiv 1 \pmod 4$.

Exercises

4.1a.a) Prove that if prime $p \equiv 1 \pmod 4$ then there exists a residue class $m \pmod p$ for which $m^2 \equiv -1 \pmod p$.

b) Consider the set of integers $\{i + jm :\ 0 \le i, j \le [\sqrt{p}]\}$. Show that there are two elements of this set, say $i + jm$ and $I + Jm$, which are congruent mod p.

c) Deduce that $p = (i - I)^2 + (j - J)^2$.

4.1b. As any square r^2 is represented as $r^2 + 0^2$, and as the product of two integers that are the sum of two squares, can be represented using the formula $(r^2 + s^2)(t^2 + u^2) = (rt + uv)^2 + (ru - tv)^2$, use exercise 4.1a to describe with proof all integers that can be written as the sum of two squares

4.1c. Show that the product of two integers that can be represented by $x^2 + dy^2$, is always another integer that can be represented by $x^2 + dy^2$.

4.1d. Show that the equivalence defined above is indeed an equivalence relation, and deduce that two equivalent binary quadratic forms represent the same integers.

4.1e. Prove that Gauss's reduction algorithm does indeed terminate with a reduced binary quadratic form.

4.1f.a) Show that if $ax^2 + bxy + cy^2$ is reduced then the smallest four values that the form properly represents are $0 < a \leq c \leq a - |b| + c$. (Hint: Begin by observing that if $|x| > |y|$ then $ax^2 + bxy \leq |x|(a|x| - |by|) \geq |x|^2(a - |b|)$.) Find *all* of the proper representations of a and c by f.

b) Deduce that reduced forms $ax^2 + bxy + cy^2$ and $ax^2 - bxy + cy^2$ cannot be equivalent. (Hint: Remember that, if they are equivalent, then the transformation of variables involves proper representations of both a and c.)

c) Deduce that distinct reduced forms are inequivalent. (Hint: Use part a.)

d) Evidently every reduced form has the *automorphism*[2] given by $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, and the automorphisms form a group. Show that if other non-trivial automorphisms occur then $a = b$ or c. Deduce that either $a = c$ and $b = 0$ so that if $(a, b, c) = 1$ then our form is $x^2 + y^2$ of discriminant $d = -4$, and the "extra" automorphism is $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ of order 2; or that $a = b = c$ so that if $(a, b, c) = 1$ then our form is $x^2 + xy + y^2$ of discriminant $d = -3$, and an"extra" automorphism is $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ of order 3. (Hint: Use part a.)

4.1g. Find all reduced quadratic forms of discriminant d with $0 > d > -30$. Show that there is just one reduced quadratic forms for each of the following discriminants: $-3, -4, -7, -8, -11, -19, -43, -67$ and -163.

4.1h. Determine what primes are represented by $x^2 + 2y^2$, then by $x^2 + 3y^2$, then by $2x^2 + 3y^2$, etc.

4.2 Quadratic forms, Ideals, and Transformations.

If we follow the transformations on our variables in (4.1.2) then the two cases are

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \tag{4.1.2}$$

Therefore the transformation of the original variables to the variables at the end of Gauss's algorithm, may be written as a product of the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. These both have determinant 1, and together generate $\mathrm{SL}(2, \mathbb{Z})$, the 2-by-2 matrices with integer entries and determinant 1: that is, one knows that any matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ where $\alpha, \beta, \gamma, \delta$ are integers satisfying $\alpha\delta - \beta\gamma = 1$, may be written as a product of our two generating matrices.

An action of $M \in \mathrm{SL}(2, \mathbb{Z})$ on complex number z, is given by the map $\begin{pmatrix} z \\ 1 \end{pmatrix} \to M \begin{pmatrix} z \\ 1 \end{pmatrix}$. Now consider the complex number $z = \frac{b+\sqrt{d}}{2a}$, which is in the upper half of the complex plane. Since $\frac{1}{z} = \frac{b-\sqrt{d}}{2c}$ we know that $|z| > 1$ if and only if $c > a$. In the first part of

[2] That is, an $\mathrm{SL}(2, \mathbb{Z})$ transformation of the variables which leaves the quadratic form unchanged.

Gauss's algorithm, if $|z| < 1$ or if $|z| = 1$ and $\mathrm{Re}(z) < 0$, then we map $z \to z' = -1/z$ so that $|z'| > 1$, or $|z'| = 1$ and $\mathrm{Re}(z') \geq 0$.

In the second part of Gauss's algorithm we have $|z| \geq 1$ and we map $z \to z' = z + k$ so that $-\frac{1}{2} < \mathrm{Re}(z') \leq \frac{1}{2}$. The algorithm terminates when z is in the *fundamental domain* $\mathcal{D}$

$$(4.2.1) \qquad -\frac{1}{2} < \mathrm{Re}(z) \leq \frac{1}{2} \text{ with } |z| > 1, \quad \text{or} \quad 0 \leq \mathrm{Re}(z) \leq \frac{1}{2} \text{ with } |z| = 1$$

(as in Figure 1). The uniqueness of the reduced binary quadratic form in its equivalence class implies that every point $\frac{b+\sqrt{d}}{2a}$ in the upper half of the complex plane has some unique element of $\mathcal{D}$ in its orbit. It can be proved that this is true for any point in the upper half of the complex plane.

There is a third way to view Gauss's algorithm, involving imaginary quadratic fields, due to Dirichlet. If $d \equiv 0$ or $1 \pmod 4$ and is squarefree other than perhaps a factor of 4 or 8, then we say that d is a *fundamental* discriminant. An *algebraic integer* is a number that is the root of a monic polynomial with integer coefficients; the algebraic integers in $\mathbb{Q}(\sqrt{d})$ take the form $\mathbb{Z}[\tau_d] := \{m + n\tau_d : \ m, n \in \mathbb{Z}\}$, where

$$\tau_d = \begin{cases} \frac{\sqrt{d}}{2} & \text{if } d \equiv 0 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

An A is the ring of algebraic integers of a field K then an *ideal* I of A is a subset of A that is closed under addition, and under scalar multiplication by elements of A.

For every ideal in $\mathbb{Z}[\tau_d]$ there exist integers a, B, g such that every element of the ideal is of the form $g(ax + (B + \tau_d)y)$ for some integers x and y (see exercise 4.2a). In Gauss's algorithm we begin with an ideal $2(a, B + \tau_d) = (2a, b + \sqrt{d})$ in $\mathbb{Z}[\tau_d]$, for fundamental discriminant $d < 0$, where $B = [b/2]$. Ideals I and J are *equivalent* if there exist algebraic integers α and β for which $\alpha I = \beta J$. In the first step of the algorithm we have $(2a, b+\sqrt{d}) \sim (2c, -b + \sqrt{d})$, since

$$(b - \sqrt{d}) \times (2a, b + \sqrt{d}) = (2a(b - \sqrt{-d}), b^2 - d) = (2a) \times (b - \sqrt{-d}, 2c);$$

and in the second step that $(2a, b + \sqrt{d}) \sim (2a, b' + \sqrt{d})$, replacing b by $b' = b + 2ak$. Therefore Gauss's algorithm shows that every ideal of $\mathbb{Z}[\tau_d]$ is equivalent to a *reduced ideal*, that is one with a basis $(2a, b + \sqrt{d})$ satisfying (4.1.1), where $c = (b^2 - d)/4a$.

The ideal $(2a, b + \sqrt{d}) = \{2ax + (b + \sqrt{d})y : \ x, y \in \mathbb{Z}\}$. Multiplying this linear form with its complex conjugate, and dividing by 4, we obtain

$$(4.2.3) \qquad \left(ax + \left(\frac{b+\sqrt{d}}{2}\right) y\right) \left(ax + \left(\frac{b-\sqrt{d}}{2}\right) y\right) = a(ax^2 + bxy + cy^2).$$

This gives an isomorphism between equivalence classes of ideals of $\mathbb{Z}[\tau_d]$ presented in the form $(2a, b + \sqrt{d})$ where $4a$ divides $b^2 - d$, and binary quadratic forms of discriminant d.

A *unit* α is an algebraic integer which divides 1; in other words both α and $1/\alpha$ are algebraic integers. The units of $\mathbb{Q}$ are 1 and -1 which are thus contained in any $\mathbb{Q}(\sqrt{d})$. We wish to determine whether there are any other units in $\mathbb{Q}(\sqrt{d})$: Evidently if $m+n\tau_d$, with $n\neq 0$, is a unit then $(m,n)=1$ and so

$$m^2-(d/4)n^2=\pm 1 \ \text{ or } \ (2m+n)^2-dn^2=\pm 4,$$

if $d\equiv 0$ or $1 \pmod 4$, respectively. If $d<0$ then "±" must be +, and $|d|n^2\leq 4$ so that $d=-3$ or -4 and $n=\pm 1$. We deduce that the only possibilities are the units i and $-i$ in $\mathbb{Q}(\sqrt{-4})$, and the units $\frac{\pm 1\pm\sqrt{-3}}{2}$ in $\mathbb{Q}(\sqrt{-3})$.

Now suppose that $\frac{u+\sqrt{d}v}{2}$ is a unit (note that $u-dv$ is even). If we write

$$aX+\left(\frac{b+\sqrt{d}}{2}\right)Y=\frac{u+\sqrt{d}v}{2}\left(ax+\left(\frac{b+\sqrt{d}}{2}\right)y\right) \tag{4.2.4}$$

then $aX^2+bXY+cY^2=\pm(ax^2+bxy+cy^2)$ by (4.2.3) where $u^2-dv^2=\pm 4$, an automorphism of our form.

Exercises

4.2a.a) Let I be an ideal of the ring of integers of $\mathbb{Z}[\tau_d]$ and let $g=\gcd\{v: u+v\tau_d\in I\}$. Prove that there exists some $h+g\tau_d\in I$, and that every element of I can be written as an integer plus an integer multiple of $h+g\tau_d$.

b) Let k be the generator of $\mathbb{Z}\cap I$ so that $I=\{mk+n(h+g\tau_d):\ m,n\in\mathbb{Z}\}$. By constructing elements of I, prove that g divides k and that g divides h, so that $I=g[a,B+\tau_d]_{\mathbb{Z}}$ for some integers a,B,g for which $4a$ divides b^2-d, where $b=2B$ or $2B+1$ so that $d\equiv b \pmod 2$. (Hint: I is closed under scalar multiplication by any element of $\mathbb{Z}[\tau_d]$.)

4.2b. Prove that there is a 1-to-1 correspondence between the units of $\mathbb{Q}(\sqrt{d})$ and the automorphisms of a binary quadratic form of discriminant d, whether $d<0$ or $d>0$ (see, e.g., exercise 4.1f.d, to help with the $d<0$ case).

4.3. The class group. The equivalence classes of ideals form an abelian group called the *ideal class group* (where multiplication of ideals is defined by $IJ=\{ij:\ i\in I, j\in J\}$), and the identity element is the equivalence class of *principal ideals*, that is ideals generated by just one element. If $K=\mathbb{Q}(\sqrt{d})$ with $d<0$ then the product of any ideal with its complex conjugate[3] gives a principal ideal. If the class number $h(d)=1$, then all of the ideals are principal, so we have a *principal ideal domain*, which implies that we have unique factorization of the algebraic integers of the field. If $h(d)\neq 1$ then factorization is not unique. However we always have unique factorization of the ideals, which allows us to do arithmetic in any number field, much as in the rational integers.

One can, correspondingly, multiply together two quadratic forms to get a third (as in exercises 4.1b and 4.1c). This was originally done in general by Gauss's *composition*, and any known method to do so is complicated, which is part of what motivated Dirichlet's development of the theory of ideals. Recently Bhargava gave a beautiful description of Gauss's composition, which we will outline in section 4.8.

[3] The *complex conjugate* of an ideal I is the ideal $\overline{I}:=\{\overline{z}:\ z\in I\}$.

For any discriminant $d = b^2 - 4ac$ we have $d \equiv 0$ or $1 \pmod 4$. In fact there is a binary quadratic form for every such d, which corresponds to the identity element of the class group (that is, the class of principal ideals). This *principal form* is

$$x^2 - \frac{d}{4}y^2 \text{ if } d \equiv 0 \pmod 4 \text{ and } x^2 + xy - \frac{(d-1)}{4}y^2 \text{ if } d \equiv 1 \pmod 4.$$

Note that the principal form is reduced and is the only reduced binary quadratic form of discriminant d with $a = 1$. Therefore $h(d) \geq 1$ and we ask how big is $h(d)$ typically? Much depends on what type of field that $\mathbb{Q}(\sqrt{d})$ is. If d is negative then $h(d)$ is typically around $\sqrt{|d|}$, but $h(d)$ is typically bounded when d is positive. Gauss asked an important question in each case:

- Is it true that there are infinitely many squarefree $d > 0$ for which the class number, $h(d)$, is one?
- Are there negative squarefree d for which the class number is one, other than the nine values given in the list $-1, -2, -3, -7, -11, -19, -43, -67, -163$?

The first question remains completely open. The quest to resolve the second question set the tone for twentieth century number theory perhaps more than any other problem. In the 1930s it was shown that there are no more than ten elements on the list, though the proof, by its very nature, cannot be modified to determine whether there is indeed a missing tenth d. We shall prove this in chapter 12. In the 1950s, Heegner showed that there is no tenth field by a proof that was not fully believed at the time; though nowadays we know that Heegner was correct and the technique he created to prove this result, suitably reformulated, is now central to arithmetic geometry (see section 4.10). In the 1960s Baker and Stark came up with quite different, and widely accepted, proofs that there is no tenth field.[4] In the 1980s Goldfeld, Gross and Zagier showed how one can find all squarefree $d < 0$ with any given class number, be it 1, 2 or whatever (see section 12.* for more details).

In the case $d = -163$ above, the principal form is $x^2 + xy + 41y^2$. Taking $y = 1$ we obtain the polynomial $n^2 + n + 41$ which is prime for $n = 0, 1, 2, \dots, 39$ (we already encountered this in section 1.4). Is it a co-incidence that this polynomial should arise again here?

Rabinowicz's theorem. *Let $A \geq 2$ be an integer. The polynomial $n^2 + n + A$ is prime for $0 \leq n \leq A - 2$ if and only if $h(1 - 4A) = 1$.*

Remark. We have the examples $A = 2, 3, 5, 11, 17$ and 41, and we know that these are all thanks to Heegner's result.

Proof. We can verify this by hand for $A \leq 7$, so assume $A \geq 8$.

Suppose that $h(d) = 1$ where $d = 1 - 4A$, so that $x^2 + xy + Ay^2$ is the only binary quadratic form of discriminant d, up to equivalence. If $m := n^2 + n + A$ is composite for some $0 \leq n \leq A - 2$ then the smallest prime factor p of m satisfies $p \leq \sqrt{n^2 + n + A} < A$. Moreover m is properly represented by $x^2 + xy + Ay^2$, so that d is a square mod $4m$ by Proposition 4.1, and hence d is a square mod $4p$. But then, p must be properly

[4] There have now been about a dozen different proofs of this fact. All profound, all interesting, none of them easy.

represented by some binary quadratic form of discriminant d by Proposition 4.1, and hence by $x^2+xy+Ay^2$, since this is the only one. Therefore if $p=u^2+uv+Av^2$ with $(u,v)=1$ then $(2u+v)^2+(4A-1)v^2=4p\le 4(A-1)$. Hence $v=0$ and $u=\pm 1$ which gives a contradiction, and therefore n^2+n+A cannot be composite.

If $h(d)>1$ then there exists another reduced binary quadratic form $ax^2+bxy+cy^2$ with $2\le a\le \sqrt{|d|/3}$. Note that a is properly represented by this form, so that d is a square mod $4a$ by Proposition 4.1, and therefore d is a square mod $4p$ where p is the smallest prime factor of a. If $p=2$ then $d\equiv 1 \pmod 8$ (as d is odd) so that A is even and therefore 0^2+0+A is composite. Hence we may assume that p is odd, and let n_1 be the smallest non-negative integer for which $(2n_1+1)^2\equiv d \pmod p$, so that $n_1\le p-1$. Therefore p divides $n_1^2+n_1+A$, so if this is prime then it must equal p, and so $(p+n_1)^2+(p+n_1)+A=p(p+2n_1+2)$ is composite. This proves the result since $p+n_1\le 2p-1\le 2a-1\le 2\sqrt{|d|/3}-1\le A-2$.

Exercises

4.3a. Prove that the principal form is the only reduced form with $a=1$.

4.3b. An algebraic integer α is called *irreducible* if it cannot be written as $\beta\gamma$ where β and γ are both algebraic integers with norm >1. Show that if $h(d)>1$ if and only if there exists algebraic integers $\alpha\in\mathbb{Q}(\sqrt{d})$ which is irreducible but such that (α) is not prime.

4.3c. (Davenport's open question) If algebraic integer $\alpha\in\mathbb{Q}(\sqrt{d})$ is irreducible then what is the maximum number of prime factors that (α) can have?

4.4. The local-global principal, and counting representations. Determining whether n has a representation by binary quadratic form $ax^2+bxy+cy^2$ in rational numbers x,y is a far easier problem than determining whether it has a representation in integers: Replacing $2ax+by$ by z, this is equivalent to representing $4an$ by z^2-dy^2 in rational numbers y,z; that is finding a solution to

$$Au^2+Bv^2=Cw^2, \tag{4.4.1}$$

in integers u,v,w, where we multiply through by the common denominator of y and z, taking $A=4an$, $B=d$, $C=1$. The *local-global principle* tells us that (4.4.1) has a solution in non-zero integers if and only if it does in the reals, and mod q, for every prime power q. In fact one can show that if there is a solution to (4.4.1) in non-zero integers u,v,w, then there is a non-zero solution with $|Au^2|,|Bv^2|,|Cw^2|\le|ABC|$.[5] We also know that if there is one non-zero solution then there are infinitely many (see exercise 4.4b.h).

Proposition 4.1 is a similarly simple criterion to determine whether there exists a binary quadratic form of discriminant d which represents n in integers, but it does not help us with representation in integers by a particular, given binary quadratic form. It would be helpful to have some congruence conditions that could help us decide whether or not an integer is representable by f. For example, Proposition 4.1 tells us that prime $p>5$ can be represented by some binary quadratic form of discriminant -15 if and only if -15 is a

[5] Therefore if there are non-zero rational solutions to $n=ax^2+bxy+cy^2$ then there is one with $(x,y)=(r/t,s/t)$ where $|t|\le\sqrt{|d|}$, $|s|\le 2\sqrt{|an|}$ and $|r|\le(|b|+\sqrt{|d|})\sqrt{|n|/|a|}$.

square mod p, that is if $p \equiv 1, 2, 4$ or $8 \pmod{15}$. Now $h(-15) = 3$ with reduced binary quadratic forms $f_1 = x^2+xy+4y^2$, $f_2 = 2x^2+xy+2y^2$, $f_3 = 2x^2-xy+2y^2$. If prime p is represented by f_1 then $4p = (2x+y)^2+15y^2$ and so $4p$ is a square mod 15, hence $p \equiv 1$ or $2 \pmod{15}$; whereas if prime p is represented by f_2 or f_3 then $8p = (4x \pm y)^2+15y^2$ and so $8p$ is a square mod 15, hence $p \equiv 4$ or $8 \pmod{15}$. Therefore a simple congruence criterion allows us to determine which quadratic form of discriminant -15, represents which primes. On the other hand Proposition 4.1 tells us that odd prime $p \neq 11$ can be represented by some binary quadratic form of discriminant -44 if and only if -11 is a square mod p, which holds if and only if p is a square mod 11. If p is represented by x^2+11y^2, or if p is represented by $3x^2+2xy+4y^2$ so that $3p = (3x+y)^2+11y^2$, then we can only deduce in either case that p is a square mod 11 (since 3 is a square mod 11), and thus we cannot distinguish which primes are represented by which form. The discriminants for which we can decide which forms represent which primes by simple congruence conditions are Euler's *idoneal numbers*. It is conjectured that there are only 65 idoneal numbers, the largest being -5460.

Suppose that $f_1, f_2, \dots, f_h$ are representatives of the $h = h(d)$ distinct classes of binary quadratic forms of discriminant d. Let $r_f(n)$ be the number of distinct representations of n by f, and $r(n) := \sum_{i=1}^h r_{f_i}(n)$, the total number of distinct representations of n by binary quadratic forms of discriminant d.[6] Although there is no simple way, in general, to determine each $r_{f_i}(n)$ (since there is no local-global principle for this question), we will be able to evaluate $r(n)$ (since we have a suitable local-global principle given by Proposition 4.1). The isomorphism between ideals and binary quadratic forms given at the end of section 4.2 implies that if $\mathcal{I}_1, \dots, \mathcal{I}_h$ are the ideal classes corresponding to $f_1, f_2, \dots, f_h$, respectively, then $r_{f_j}(n)$ is the number of factorizations of the ideal (n) as $A\overline{A}$ with $A \in \mathcal{I}_j$. One gets this simple correspondence because the indistinct representations of n differ, multiplicatively, by a unit (as in (4.2.4)), and the units are naturally discarded when considering factorization into ideals. Therefore $r(n)$ equals the number of factorizations of (n) as $A\overline{A}$, so that $r(n)$ is a multiplicative function. Now if p is a prime then the ideal (p) can factor into prime ideals in $\mathbb{Q}(\sqrt{d})$ in three different ways:

$$(p) = \begin{cases} \mathcal{P}\,\overline{\mathcal{P}} \text{ with } (\mathcal{P}, \overline{\mathcal{P}}) = 1, & \text{if } (d/p) = 1, \\ \mathcal{P}^2, & \text{if } (d/p) = 0, \\ (p) & \text{if } (d/p) = -1. \end{cases}$$

Therefore $r(p^k) = k+1$ if $(d/p) = 1$, also $r(p^k) = 1$ if $(d/p) = 0$, and $r(p^k) = 0$ or 1 if $(d/p) = -1$, depending on whether k is odd or even. In each case we find that $r(p^k) = \sum_{j=0}^k (d/p^j)$, and so, by multiplicativity,

$$r(n) = \sum_{m|n} \left(\frac{d}{m}\right). \tag{4.4.2}$$

[6] By "distinct representations" we mean those that are inequivalent under an automorphism of f. See exercise 4.2b.

For $d < -4$, the only automorphisms of f correspond to the map $(x, y) \to \pm(x, y)$, and so $r_f(n)$ counts the number of pairs of integers x, y for which $n = f(x, y)$ with $x > 0$, or $x = 0$ and $y > 0$, for $n \geq 1$. Therefore $2r_f(n)$ denotes the total number of representation of n by f. In general, if $d < 0$ then $wr_f(n)$ counts the total number of representations of n by f where w, the number of automorphisms of f, is given (see section 4.2) by

$$w = 2 \text{ if } d < -4, \quad w = 4 \text{ if } d = -4, \quad \text{and} \quad w = 6 \text{ if } d = -3.$$

Now, by exercise 3.4c we know that the number of pairs of integers x, y for which $ax^2 + bxy + cy^2 \leq N$ is given by $2\pi N/\sqrt{|d|} + O(\sqrt{N})$ for any reduced form f. Therefore

$$\sum_{n \leq N} r_f(n) = \frac{1}{w} \sum_{\substack{x,y \in \mathbb{Z} \\ f(x,y) \leq N}} 1 = \frac{1}{w} \frac{2\pi N}{\sqrt{|d|}} + O(h(d)\sqrt{N}). \tag{4.4.3}$$

We deduce, since every reduced form gives a distinct representation of some integer $a \leq \sqrt{|d|/3}$, that

$$h(d) \leq \sum_{a \leq \sqrt{|d|/3}} r(a) \leq w \sum_{a \leq \sqrt{|d|/3}} \tau(a) \ll \sqrt{|d|} \log d \tag{4.4.4}$$

where τ is the divisor function (see section 2.14).

Exercises

4.4a. Determine what primes are represented by $x^2 + 2y^2$, then by $x^2 + 3y^2$, then by $2x^2 + 3y^2$, etc.

4.4b. At first sight it appears one must check infinitely many local criteria to use the local-global principle in (4.4.1). We shall show that we only need verify a finite number of such criteria.

a) Show that without loss of generality we may assume that A, B, C are squarefree and pairwise coprime.

b) Show that there is a non-zero solution in the reals if and only if A, B and $-C$ do not all have the same sign.

c) Show that if p is an odd prime and there is a non-zero solution to (4.4.1) mod p, then there is a non-zero solution to (4.4.1) mod p^k for all $k \geq 1$. (Hint: Given a solution x, y, z mod p^k look for one $x + up^k, y + vp^k, z + wp^k$ mod p^{k+1}.)

d) Show that if there is a non-zero solution to (4.4.1) mod 8, then there is a non-zero solution to (4.4.1) mod 2^k for all $k \geq 3$.

e) Show that if odd prime p divides C then there is a non-zero solution to (4.4.1) mod p if and only if $(-AB/p) = 1$. Concoct similar criteria for the odd prime divisors of A and B.

f) Show that if odd prime p does not divide ABC then there is a non-zero solution to (4.4.1) mod p. (Show that there exists a non-zero solution with $z = 0$ if $(-AB/p) = 1$. By generalizing this, deduce that if there is non non-zero solution then $(A/p) = (B/p) = -(C/p)$ and $p \equiv 3 \pmod 4$. Multiply the equation through by $A^{-1} \pmod p$, and replace v and w by appropriate multiples, to deduce that there is then no solution to $x^2 + y^2 \equiv -1 \pmod p$ in non-zero $x, y \pmod p$. Now be ingenious!).

g) Write down a finite algorithm to test whether (4.4.1) is solvable.

h) Show that if there is one non-zero solution over the integers then there are infinitely many. (Hint: Divide through by z to get a solution $u, v, 1 \in \mathbb{Q}$. Now look for a solution $u + r, v + rt, 1 \in \mathbb{Q}$ and solve for r.) Translate this back to show that if we have a solution to $n = ax^2 + bxy + cy^2$ in rationals x, y then $X = \frac{-(ax+by)m^2 - 2cymn + cxn^2}{am^2+bmn+cn^2}, Y = \frac{aym^2 - 2axmn - (bx+cy)n^2}{am^2+bmn+cn^2}$ is a solution in rationals for all integers m, n.

4.5. Dirichlet's class number formula for imaginary quadratic fields. By (4.4.3) we have

$$\sum_{n\leq N} r(n) = \sum_{j=1}^{h(d)} \sum_{n\leq N} r_{f_j}(n) = h(d)\frac{2\pi N}{w\sqrt{|d|}} + O(h(d)\sqrt{N}). \tag{4.5.1}$$

On the other hand, we can use (4.4.2) to deduce

$$\sum_{n\leq N} r(n) = \sum_{n\leq N}\sum_{m|n}\left(\frac{d}{m}\right) = \sum_{m\leq N}\left(\frac{d}{m}\right)\left[\frac{N}{m}\right].$$

We would like to approximate the right side by $\sum_{m\leq N}\left(\frac{d}{m}\right)\frac{N}{m}$ which is roughly $NL(1,(\frac{d}{.}))$, but the error term could be as large as $\sum_{m\leq N} 1$, which is unacceptable. Thus we have to do something different for the large values of m: Since (d/m) is a non-principal character to the modulus $|d|$ we have $|\sum_{A<m\leq B}\left(\frac{d}{m}\right)| \leq |d|$ for any A and B, and so

$$\left|\sum_{N/K<m\leq N}\left(\frac{d}{m}\right)\left[\frac{N}{m}\right]\right| = \left|\sum_{k=1}^{K}\sum_{N/K<m\leq N/k}\left(\frac{d}{m}\right)\right| \leq K|d|,$$

whereas

$$\sum_{m\leq N/K}\left(\frac{d}{m}\right)\left[\frac{N}{m}\right] = \sum_{m\leq N/K}\left(\frac{d}{m}\right)\left(\frac{N}{m}+O(1)\right) = N\sum_{m\leq N/K}\frac{1}{m}\left(\frac{d}{m}\right) + O(N/K).$$

Selecting $K=\sqrt{N/|d|}$ we deduce, from exercise 3.3b, that

$$\sum_{n\leq N} r(n) = N\ L\left(1,\left(\frac{d}{\cdot}\right)\right) + O(\sqrt{|d|N}),$$

since the method used to prove (3.3.6) implies that $\sum_{m\geq \ell|d|}\frac{1}{m}\left(\frac{d}{m}\right) \ll 1/\ell$, for any integer $\ell\geq 1$. Equating this with (4.5.1), and then letting $N\to\infty$ with d fixed we deduce *Dirichlet's class number formula for imaginary quadratic fields*:

$$h(d) = \frac{w}{2\pi}\sqrt{|d|}\ L\left(1,\left(\frac{d}{\cdot}\right)\right) \qquad \text{whenever } d<0. \tag{4.5.2}$$

Exercises

4.5a. Use (4.5.2) to show that if $d<0$ then $L(1,(d/.)) \geq 2\pi/w\sqrt{|d|}$ and hence $L(1,(d/.)) \geq \pi/\sqrt{|d|}$ if $d<-4$.

4.6. Positive discriminants and fundamental units. When $d > 0$, Gauss defined $ax^2 + bxy + cy^2$ to be *reduced* when

$$0 < \sqrt{d} - b < 2|a| < \sqrt{d} + b. \tag{4.6.1}$$

This implies that $0 < b < \sqrt{d}$ so that $|a| < 2\sqrt{d}$ and therefore there are only finitely many reduced forms of positive discriminant d. Note that $ax^2 + bxy + cy^2$ is reduced if and only if $cx^2 + bxy + ay^2$ is. The first inequality implies that $ac = (b^2 - d)/4 < 0$.

Let $\rho_1 := \frac{-b+\sqrt{d}}{2a}$ and $\rho_2 := \frac{-b-\sqrt{d}}{2a}$ be the two roots of $at^2 + bt + c = 0$. Then (4.6.1) holds if and only if $|\rho_1| < 1 < |\rho_2|$ and $\rho_1\rho_2 < 0$.

Forms $ax^2 + bxy + cy^2$ and $cx^2 + b'xy + c'y^2$ are *neighbours* (and equivalent) if they have the same discriminant and $b + b' \equiv 0 \pmod{2c}$, since $a(-y)^2 + b(-y)(x + \frac{b+b'}{2c}y) + c(x + \frac{b+b'}{2c}y)^2 = cx^2 + b'xy + c'y^2$. The reduction algorithm proceeds as follows: Given $ax^2 + bxy + cy^2$ we select a neighbour as follows: Let b_0' be the least residue in absolute value of $-b \pmod{2c}$ so that $|b_0'| \leq c$.

- If $|b_0'| > \sqrt{d}$ then let $b' = b_0'$. Note that $0 < (b')^2 - d \leq c^2 - d$ so that $|c'| = ((b')^2 - d)/4|c| < |c|/4$.
- If $|b_0'| < \sqrt{d}$ then select $b' \equiv -b \pmod{2c}$ with b' as large as possible so that $|b'| < \sqrt{d}$. Note that $-d \leq (b')^2 - d = 4cc' < 0$. If $2|c| > \sqrt{d}$ then $|c'| \leq |d/4c| < |c|$.

Otherwise $\sqrt{d} \geq 2|c|$ and $\sqrt{d} - 2|c| < |b'| < \sqrt{d}$, and therefore the neighbour is reduced. Thus we see that the absolute values of the coefficients a and c of the binary quadratic form are reduced at each step of the algorithm until we obtain a reduced form.

There is one major difference between this, the $d > 0$ case, and the $d < 0$ case: In a given class of binary quadratic forms of positive discriminant there is not necessarily a unique reduced form. Rather, when we run Gauss's algorithm we eventually obtain a *cycle* of reduced forms, which must happen since every reduced form has a unique right and a unique left reduced neighbouring form, and there are only finitely many reduced forms. Given a quadratic form $a_0x^2 + b_0xy + a_1y^2$ we define a sequence of forms, in the following notation:

$$a_0 \;{}^{b_0}\; a_1 \;{}^{b_1}\; a_2 \;{}^{b_2}\; a_3 \;\ldots\;.$$

This represents, successively, the forms $a_0x^2 + b_0xy + a_1y^2$, $a_1x^2 + b_1xy + a_2y^2$, $a_2x^2 + b_2xy + a_3y^2$, $\ldots$, of equal discriminant, where a form is the unique reduced right neighbour of its predecessor, and then $a_{i+1} = (b_i^2 - d)/4a_i$. For example, when $d = 816$,

$$5 \;{}^{26}\; -7 \;{}^{16}\; 20 \;{}^{24}\; -3 \;{}^{24}\; 20 \;{}^{16}\; -7 \;{}^{26}\; 5 \;{}^{24}\; -12 \;{}^{24}\; 5 \;{}^{26}\; -7 \;\ldots$$

which is a cycle of period 8.

In section 4.2 we discussed the units of $\mathbb{Q}(\sqrt{d})$, and showed that they are in 1-to-1 correspondence with the solutions to *Pell's Equation*:

$$v^2 - dw^2 = \pm 4. \tag{4.6.2}$$

This yields the map $\begin{pmatrix} X \\ Y \end{pmatrix} \to \begin{pmatrix} \frac{v-bw}{2} & -cw \\ aw & \frac{v+bw}{2} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$, so that $aX^2 + bXY + cY^2 = \pm(ax^2 + bxy + cy^2)$, which is an automorphism only when $v^2 - dw^2 = 4$. In exercise 4.6b we show that there is a solution to Pell's equation (4.6.2) for all positive non-square integers d. Pell's equation has a long and interesting history (see [Weil]), and there has long been an efficient method known to find solutions, which are sometimes very large: Any solution to (4.6.2) yields a good rational approximation $\frac{v}{w}$ to $\sqrt{d}$, in fact with $|\frac{v}{w}-\sqrt{d}|<\frac{1}{2w^2}$ if $d \geq 19$. This implies that $\frac{v}{w}$ is a convergent for the continued fraction of $\sqrt{d}$:[7] For $\alpha \in \mathbb{R}$ let $\alpha_0=\alpha$ and then, for each $j \geq 0$, let $a_j=[\alpha_j]$ and $\alpha_{j+1}=1/\{\alpha_j\}$. The *continued fraction* of α is given by

$$\alpha=[a_0,a_1,a_2,a_3,\dots]:=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{\cdots}}}}$$

The continued fraction is finite in length if and only if α is rational, and it is periodic if and only if α is a quadratic irrational. The *convergents* to α are given by $\frac{p_n}{q_n}=[a_0,a_1,\dots,a_n]$ for each $n \geq 0$. We have $\frac{p_1}{q_1}>\frac{p_3}{q_3}>\cdots>\alpha>\cdots>\frac{p_2}{q_2}>\frac{p_0}{q_0}$ and $|\alpha-\frac{p_n}{q_n}| \leq \frac{1}{q_nq_{n+1}}$ for all $n \geq 0$. When $\alpha=\sqrt{d}$ we have, for $c_n:=p_n^2-dq_n^2$, that $c_nc_{n+1}<0$ and $|c_n|<2\sqrt{d}+1$, and that there is a cycle of reduced forms $c_0 \ {}^{b_0}\ c_1 \ {}^{b_1}\ c_2 \ {}^{b_2}\ c_3 \ \dots$ of discriminant d. For example for $d=60$ we have $\sqrt{60}=[7,\overline{1,2,1,14}]$ (the terms under the line form the period of the continued fraction), and gives rise to the cycle $-11\ {}^{4}\ 4\ {}^{4}\ -11\ {}^{7}\ 1\ {}^{7}\ -11\ {}^{4}\ 4$, and the first 4 corresponds to the unit $\frac{8+\sqrt{60}}{2}=4+\sqrt{15}$. In general if (4.6.1) is satisfied and $\frac{p_n}{q_n}$ is the nth convergent to $\frac{\sqrt{d}-b}{2|a|}$ then define $c_n=ap_n^2 \pm bp_nq_n+cq_n^2$ where $\pm$ represents the sign of a, and we have such a cycle. For example $\frac{\sqrt{97}-9}{8}=[0,\overline{9,2,2,1,4,4,1,2,2}]$, which gives the cycle
$-1\ {}^{9}\ 4\ {}^{7}\ -3\ {}^{5}\ 6\ {}^{7}\ -2\ {}^{9}\ 2\ {}^{7}\ -6\ {}^{5}\ 3\ {}^{7}\ -4\ {}^{9}\ 1\ {}^{9}\ -4\ {}^{7}\ 3\ {}^{5}\ -6\ {}^{7}\ 2\ {}^{9}\ -2\ {}^{7}\ 6\ {}^{5}\ -3\ {}^{7}\ 4\ {}^{9}\ -1\ {}^{9}\ 4\dots.$

The *fundamental unit* is that solution $\epsilon_d:=\frac{v_0+\sqrt{d}w_0}{2}$ which is minimal and >1. We call $\frac{v^2-dw^2}{4}$ the *norm* of ϵ_d. All other solutions of (4.6.2) take the form

$$\frac{v+\sqrt{d}w}{2}=\pm\epsilon_d^k, \tag{4.6.3}$$

for some $k \in \mathbb{Z}$ (for a proof see exercise 4.6c). We let ϵ_d^+ be the smallest unit >1 with norm 1. One can deduce from (4.6.3) that $\epsilon_d^+=\epsilon_d$ or ϵ_d^2, depending on whether the norm of ϵ_d is 1 or -1.

The plan now is to copy over the argument of section 4.5, though we have the problem that there may be infinitely many different representations of n that are not distinct from a given representation of n. We deal with this by selecting a region in which there is exactly one representative from each such class of representations of n: By (4.2.4) we know that any two such representations differ by a unit, in fact of the form $\pm(\epsilon_d^+)^k$, so if x,y give one representation, then all of the others that are not distinct from this representation are given by X,Y where X and Y are determined by the equations $X-\rho_1Y=\pm(\epsilon_d^+)^k(x-\rho_1y)$

[7] For proofs of the discussion in the rest of this paragraph see [Ba], Chapters 6 and 8.

and $X - \rho_2 Y = \pm(\epsilon_d^+)^{-k}(x - \rho_2 y)$. Now we see that $|(X-\rho_1 Y)/(X-\rho_2 Y)| = (\epsilon_d^+)^{2k}|(x-\rho_1 y)/(x-\rho_2 y)|$, so there is a unique choice of k for which this quantity satisfies

$$1 \le \left| \frac{X-\rho_1 Y}{X-\rho_2 Y} \right| < (\epsilon_d^+)^2. \tag{4.6.4}$$

We must again worry about the sign ±, so we select it so that $X - \rho_1 Y > 0$. Therefore $r_f(n)$ equals the number of pairs of integers X, Y with $n = aX^2 + bXY + cY^2$ and $X - \rho_1 Y > 0$ for which (4.6.4) holds; and so we want to determine $\sum_{n \le N} r_f(n)$ which equals the number of lattice points $x, y \in \mathbb{Z}$ with $|ax^2 + bxy + cy^2| \le N$ and $x - \rho_1 y > 0$ for which (4.6.4) holds. To do so we need to get an idea of the shape of the region inside which we are counting lattice points:

If $a > 0$ then $\rho_2 < 0 < \rho_1$. As $a(x-\rho_1 y)(x-\rho_2 y) = n > 0$ therefore $x - \rho_2 y > 0$. Thus our domain becomes $y < 0$ and $x > (-y)(\rho_1 - \rho_2(\epsilon_d^+)^2)/((\epsilon_d^+)^2 - 1)$ (since this is $> (-y)(-\rho_2) > (-y)(-\rho_1)$) with $0 < ax^2 + bxy + cy^2 \le N$.

If $a < 0$ then $\rho_1 < 0 < \rho_2$. As $a(x-\rho_1 y)(x-\rho_2 y) = n > 0$ therefore $x - \rho_2 y < 0$. Thus our domain becomes $y > 0$ and $(-b/a)y \le x < y(\rho_1 + \rho_2(\epsilon_d^+)^2)/(1 + (\epsilon_d^+)^2)$ (since this is $< \rho_2 y$, and before, since $-b/a = (\rho_1+\rho_2)/2 > \rho_1$) with $0 < ax^2 + bxy + cy^2 \le N$.

In both cases the number of lattice points will be the area of the domain plus an error bounded by a constant multiple of the perimeter (since the perimeter is part the arc of the original curve, part straight lines), which has length $O_d(\sqrt{N})$.[8] Now the area can be worked out in a straightforward manner by making the substitution $u = x - \rho_1 y$ followed by $v = \pm(u + (\rho_1 - \rho_2)y)$ where the ± is chosen so that $\pm a > 0$. We then have that our area is $1/|\rho_1 - \rho_2|$ times the area of the region defined by $0 \le v \le u < v(\epsilon_d^+)^2$ with $0 \le uv \le N/|a|$; an elementary calculation then yields $(N/\sqrt{d})\log(\epsilon_d^+)$.

Now combining this information as in section 4.5 reveals that

$$NL\left(1, \left(\frac{d}{\cdot}\right)\right) = h(d)\frac{N}{\sqrt{d}}\log(\epsilon_d^+) + O_d(\sqrt{N}).$$

Letting $N \to \infty$ we deduce *Dirichlet's class number formula for real quadratic fields*:

$$h(d)\log(\epsilon_d^+) = \sqrt{d}\, L\left(1, \left(\frac{d}{\cdot}\right)\right) \qquad \text{whenever } d > 0. \tag{4.6.5}$$

Exercises

4.6a. Prove that every reduced form of positive discriminant has a unique right and a unique left reduced neighbouring form.

4.6b. In this exercise we will prove that there is always a solution to (4.6.2).

a) Suppose that we are given a real number α. By considering the numbers $\{\alpha n\}$, $0 \le n \le Q-1$, show that for any Q, there exist integers p, q with $q < Q$ for which $|q\alpha - p| \le 1/Q$.

b) Deduce that if α is irrational then there are infinitely many pairs of integers p, q, with $|q\alpha - p| \le 1/q$.

[8] When we use O_d we mean "bounded by a constant that depends only on d".

c) Taking $\alpha = \sqrt{d}$ deduce that there are infinitely many pairs of integers p, q with $|p^2 - dq^2| \leq 2\sqrt{d} + 1$.

d) Deduce that there exist integers N, r, s such that there are infinitely many pairs of integers p, q with $p^2 - dq^2 = N$ and $p \equiv r \pmod N$, $q \equiv s \pmod N$.

e) Given two solutions p, q, p', q' in part d, show that $v := (pp' - dqq')/N$, $w := (p'q - pq')/N$ are integers satisfying $v^2 - dw^2 = 1$.

4.6c.a) Prove that if $\pm v, \pm w \neq 0$ satisfy (4.6.2) then $\frac{v+\sqrt{d}w}{2} > 1$ if and only if v and w are both positive.

b) Suppose that $x^2 - dy^2 = \pm 4$ where $\alpha := \frac{x+\sqrt{d}y}{2} > 1$ is the minimal solution which is not an integer power of $\epsilon_d = \frac{v_0+\sqrt{d}w_0}{2}$. Obtain a contradiction by considering $\alpha\epsilon_d^{-1}$.

c) Deduce that all solutions to (4.6.2) are of the form (4.6.3). The units thus form a group, under multiplication, which is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$.

4.6d. Do the "elementary calculation" that yields $(N/\sqrt{d})\log(\epsilon_d)$.

4.6e. Use (4.6.2) to show that $\epsilon_d > \sqrt{d}$. Then use (4.6.5) to show that if $d > 1$ then $L(1, (d/.)) \geq \log(\sqrt{d})/\sqrt{d}$.

4.7. Upper and lower bounds on $L(1, \chi)$. In exercises 4.5a and 4.6d we returned to the topic of section 3.4 but, armed with Dirichlet's class number formula, we did a lot better, getting the lower bounds

$$L(1, (d/.)) \geq \begin{cases} \pi/\sqrt{|d|} & \text{if } d < -4 \\ \log(\sqrt{d})/\sqrt{d} & \text{if } d \geq 2 \end{cases}. \tag{4.7.1}$$

We will see in section 12 that one can significantly improve both of these lower bounds for almost all d. Let us now study upper bounds by being more precise in (3.3.5):

$$\left| \sum_{n=rq}^{(r+1)q-1} \frac{\chi(n)}{n} \right| = \left| \sum_{n=rq}^{(r+1)q-1} \chi(n) \left(\frac{1}{n} - \frac{1}{rq} \right) \right| \leq \sum_{\substack{0 \leq j \leq q-1 \\ (j,q)=1}} \frac{j}{(rq)^2} = \frac{\phi(q)}{2qr^2}$$

adding the j and $q - j$ terms. Hence

$$|L(1, \chi)| \leq \sum_{n=1}^{q-1} \frac{1}{n} + \frac{\phi(q)}{2q} \sum_{r \geq 1} \frac{1}{r^2} \leq \log q + 2 \tag{4.7.2}$$

using exercises 2.2a and 2.2b. We also bound the derivative $L'(1, \chi) = -\sum_{n \geq 1} \chi(n) \log n/n$, so that

$$\begin{aligned} |L'(1, \chi)| &\leq \sum_{n=1}^{q-1} \frac{\log n}{n} + \left| \int_q^\infty \frac{\log t}{t} \left(\sum_{n \leq t} \chi(n) \right) dt \right| \\ &\leq \int_{n=1}^{q-1} \frac{\log t}{t} dt + q \int_q^\infty \frac{\log t - 1}{t^2} dt \\ &\leq \frac{1}{2}(\log q)^2 + q\frac{\log q}{q} < \frac{1}{2}(1 + \log q)^2, \end{aligned} \tag{4.7.3}$$

using the bound in exercise 3.2g.

Exercises

4.7a. a) Improve the bound in (4.7.2) to include a factor $\phi(q)/q$ in front of the main term, perhaps at the expense of a larger secondary term.

b) Prove (4.7.2) using partial summation on the terms with $n \geq q$, using the bound in exercise 3.2g.

4.7b.a) Modify the method of (4.7.3) to show that if $0 < \sigma < 1$ then $|L(\sigma, \chi)|$, $|L'(\sigma, \chi)|/\log q$ are both $\leq (2-\sigma)q^{1-\sigma}/(1-\sigma)$.

b) This bound is not much good if σ is very close to 1. If $1 - 1/\log q \leq \sigma < 1$ then use the fact that $1/n^{\sigma} < e/n$ if $n < q$ to prove that $|L(\sigma, \chi)|$, $|L'(\sigma, \chi)|/\log q$ are both $\leq e(\log q + 2)$.

4.8. Bhargava's composition law. Given a 2-by-2-by-2 array of integers we define quadratic forms from the three pairs of opposite faces: If the numbers on the two faces get put, in order, into two 2-by-2 matrices M and N (where the same corner is always used for the top right element of M), then we define the quadratic form to be minus the determinant of $Mx + Ny$. Bhargava has shown that these three quadratic forms have the same discriminant and that their product equals the identity in the class group. (And, indeed any three binary quadratic forms whose product is the identity, must arise in this way). For example the cube with faces

$$\boxed{\begin{matrix} 1 & 4 \\ 7 & -4 \end{matrix}} \text{ and } \boxed{\begin{matrix} -1 & -2 \\ 4 & -3 \end{matrix}}$$

gives rise to the three quadratic forms $-32x^2 - xy + 11y^2$, $2x^2 - 37xy - 5y^2$, $11x^2 + 23xy - 20y^2$ of discriminant 1409, whose product is the identity.

4.9. Quadratic Forms. We have seen that it is important to know which integers are represented by a given binary quadratic form; and it is still of interest to determine which integers are represented by a given quadratic form in no matter how many variables. For example Lagrange proved that every integer is the sum of four squares, and Ramanujan asked which quadratic forms represent all integers. Quite recently Bhargava and Hanke gave the easily applied criterion that a quadratic form with integer coefficients represents all the positive integers if and only if it represents each of the twenty-nine integers $1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203$ and 290. To check whether a quadratic form represents all the primes, Bhargava showed that one only needs to check that it represents all of the primes up to 73.

4.10. Heegner's proof. Heegner showed that if $d < 0$ is a fundamental discriminant with $h(d) = 1$, and $\tau = \frac{-1+\sqrt{d}}{2}$ or $\frac{\sqrt{d}}{2}$ depending on whether $d \equiv 0$ or $1 \pmod 4$ then there is a solution in integers x, y to the equation

$$j(\tau) = x^3 = dy^2 + 1728$$

where j is the classical j-function so that $j(\tau) = (-1)^d e^{\pi\sqrt{|d|}} + 744 + 196884(-1)^d e^{-\pi\sqrt{|d|}} + \dots$. Therefore for such d we know that $e^{\pi\sqrt{|d|}}$ is very close to an integer. For example if $d = -163$ then $x = -640320$, $y = 40133016$ and $0 < x^3 + 744 - e^{\pi\sqrt{163}} < 10^{-12}$.

4.11. Plus. In 4.9 we might add Add discuss general representation by qfs, Ramanujan conjecture etc.

Unit and class groups in arbitrary number fields.

Class number formula in arbitrary number fields.

Generalization to elliptic curves and the B-Sw D conjecture.