A talk written at the
Swiss Federal Institute of Technology In Zurich
on the topic of

Quadratic Binary Forms

---

by Karlo Jerkovic and Ryan Rueger
for the seminar *L-Functions* held by
Dr. M. Schwagenscheidt in
Zurich, October 2021

1 Initial definitions

(Presented and written by Karlo)

Quadratic forms might at first glance not have much in common with L-functions, however historically Dirichlet defined Dirichlet series and characters to analyse quadratic forms and to calculate their so called class numbers. The theory of binary quadratic forms and the calculation of their class number through Dirichlet series will be the subject of this talk.

Definition 1.1 (Binary Quadratic Form)**.** A binary quadratic form is a quadratic homogeneous polynomial in two variables

$$f(x, y) = ax^2 + bxy + cy^2 \tag{1.1}$$

For our purposes, we will assume that the coefficients a, b, c are integers.

An important example of a binary quadratic form is the "Pell equation"

$$t^2 - Du^2 = 4 \tag{1.2}$$

It has been shown that this equation has non-trivial integer solutions for $D > 0$ as long as D is not a square. This is however only one binary quadratic form of many. One might ask for integer solutions (x, y) for any binary quadratic form f and integer n such that $f(x, y) = n$. To that end we can introduce a definition of equivalence among binary quadratic forms.

Definition 1.2 (Equivalence)**.** Two binary quadratic forms f and f' are equivalent if there exists[1] $(\alpha, \beta; \gamma, \delta)$ such that for

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{1.3}$$

it holds $f'(x, y) = f(x', y')$. The coefficients of f' are

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 \tag{1.4}$$

$$b' = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta \tag{1.5}$$

$$c' = a\beta^2 + b\beta\delta + c\delta^2 \tag{1.6}$$

[1] Using the usual inline-matrix notation, where commas indicate the next column, and semicolons the next row starting at the top left.

This definition of equivalence allows us to automatically find the solutions of f' if we already know them for f. This relation definitely helps the pursuit of integer solutions of binary quadratic forms.

Now one might ask whether this relation is an equivalence relation? The answer is "Yes". The properties of $\mathrm{SL}_2(\mathbb{Z})$ as a group directly imply the properties of an equivalence relation. The existence of the identity matrix in $\mathrm{SL}_2(\mathbb{Z})$ implies reflectivity, the existence of the inverse element implies symmetry and the closure implies transitivity. With this definition of equivalence being an equivalence relation, we can take a look at the equivalence classes of f.

A simple fact (that is tedious to prove) is that the discriminant $D = b^2 - 4ac$ of a binary quadratic equation is invariant under transformations of matrices in $\mathrm{SL}_2(\mathbb{Z})$. This allows us to look at equivalence classes of f through their discriminant D. This might lead some to believe that there are infinitely many equivalence classes. However for that to work, we must first check whether there exists for any given integer discriminant D a binary quadratic form f. It turns out that for integers $D = 0 \pmod 4$ or $D = 1 \pmod 4$ there is always the binary quadratic form

$$f(x,y) = \begin{cases} x^2 - \dfrac{D}{4}y^2, & \text{if } D = 0 \pmod 4 \\ x^2 + xy + \dfrac{1-D}{4}y^2, & \text{if } D = 1 \pmod 4 \end{cases} \tag{1.7}$$

As for $D = 2 \pmod 4$ and $D = 3 \pmod 4$ there are no valid integer coefficients a, b, c that would satisfy these conditions - the proof is a fun little exercise. So there are indeed infinitely many equivalence classes, which is a bit unfortunate. We can however narrow the scope of this problem and only look at equivalence classes of binary quadratic forms f with a set discriminant D.

2 Counting equivalence classes

Theorem 2.1. *Let $D \in \mathbb{Z}$ not a square. Then there exist at most finitely many equivalence classes of binary quadratic forms with discriminant D.*

Proof. There are two claims that together prove the theorem.

(i) (Claim 1) Every binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ is equivalent to a binary quadratic form $f'(x,y) = a'x^2 + b'xy + c'y^2$ such that

$$|b'| \leq |a'| \leq |c'| \tag{2.1}$$

(ii) (Claim 2) For a binary quadratic form f' as described in Claim 1 there are only finitely many triples (a', b', c') that satisfy the inequality 2.1 for a set value $b'^2 - 4a'c' = D$.

First we prove Claim 1. We set $a' = \min_{(x,y)\in\mathbb{Z}^2}(|f(x,y)|)$. Then we know there are integers α and γ that satisfy

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 \tag{2.2}$$

We note that the greatest common divisor r of α and γ is 1, because otherwise a'/r^2 would be the minimum mentioned above since it can also be represented by f. Furthermore we can choose β and δ such that $\alpha\delta - \beta\gamma = 1$. This means that

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \tag{2.3}$$

and thus the form f is equivalent to some form $\tilde{f} = a'x^2 + \tilde{b}xy + \tilde{c}y^2$ where a' as in 2.2. From here we define $b' = \tilde{b} - 2a'n$ for $n \in \mathbb{N}$ such that $|a'| \geq |b'|$. Now

$$a'(x - ny)^2 + \tilde{b}(x - ny)y + \tilde{c}y^2 = a'x^2 + (\tilde{b} - 2a'n)xy + (a'n^2 - \tilde{b}n + \tilde{c})y^2 \tag{2.4}$$

has the form of yet another equivalent binary quadratic form $f'(x,y) = a'x^2 + b'xy + c'y^2$. Finally we observe that $|c'| \geq |a'|$ necessarily holds because of the definition of a' itself. This proves the first claim.

The second claim follows by consideration of the following inequalities.

$$|D| = |b'^2 - 4a'c'| \geq |4a'c'| - |b'|^2 \geq 4|a'|^2 - |a'|^2 = 3|a'| \tag{2.5}$$

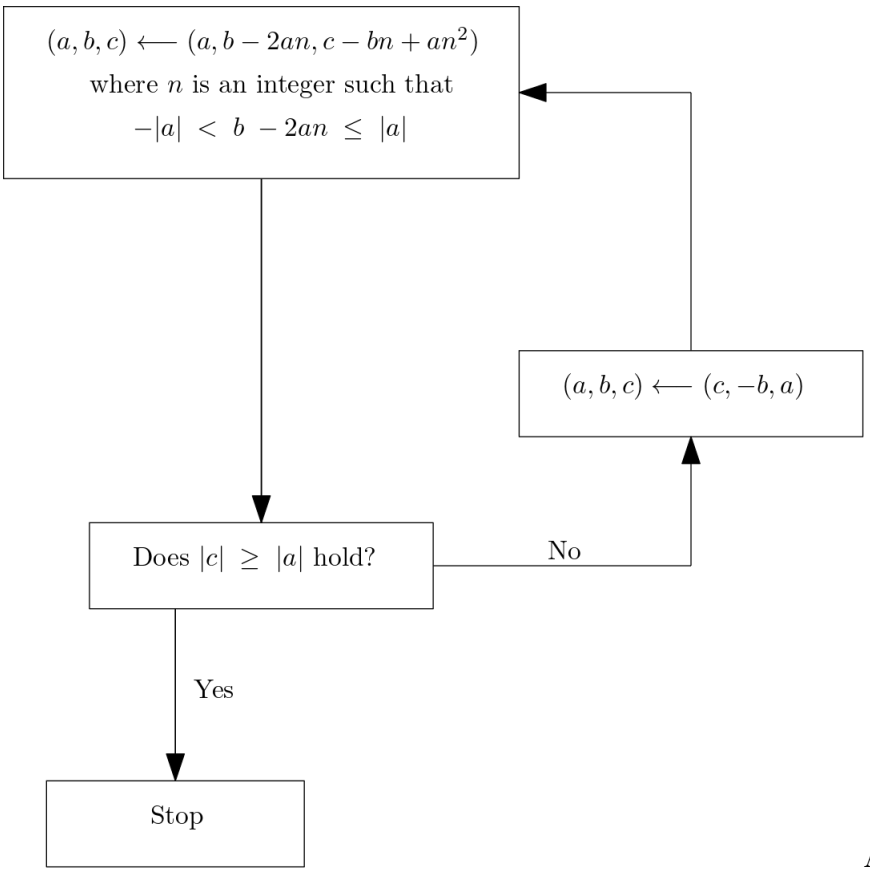
This inequality implies

$$\begin{cases} |a'| \leq \sqrt{\dfrac{|D|}{3}} \\ |b'| \leq |a'| \\ c' = \dfrac{b'^2 - D}{4a'} \end{cases} \tag{2.6}$$

From that we can deduce that the values of a', b', c' are bounded from below and above and thus there are only finitely many binary quadratic forms f' with the above condition. This concludes the proof. □

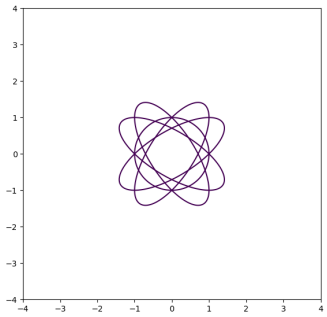
The following diagram describes an algorithm that can find equivalent binary quadratic forms using key steps in the proof of Theorem 2.1 above. Note that the algorithm always

terminates since for each loop $|a|$ decreases by at least 1.

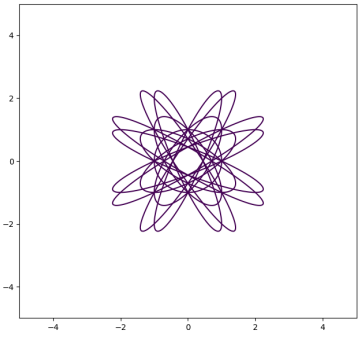


Algorithm 1

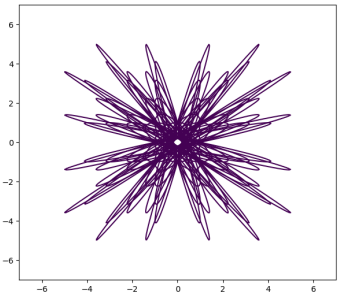
We can also note that it is possible by brute force computation that one can find all equivalence classes of binary quadratic forms with a given discriminant D by using the equations in 2.6. One will for example find that for the discriminant $D = -3$ the only equivalence class is given by the representative $f(x, y) = x^2 + y^2$ i.e. the unit circle. How does the equivalence class itself look like? On might reverse engineer the algorithm above to get many equivalent binary quadratic forms. The following image however was generated by computing matrices in $\mathrm{SL}_2(\mathbb{Z})$ with entries that are within a certain range for instance if we set the range r, then we seek any matrices in $\mathrm{SL}_2(\mathbb{Z})$ for which $|\alpha|, |\beta|, |\gamma|, |\delta| \leq r$. This algorithm produces the following images if all the binary quadratic forms were to be graphed on the same plane. Note the symmetry of these figures are a result of the "symmetries" of the entries in the matrices.



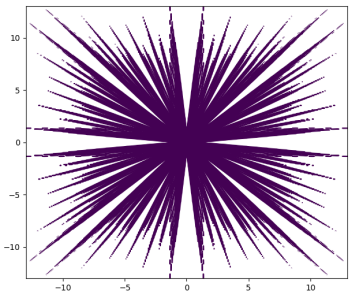
r=1



r=2



r=4



r=10

The reason this algorithm, instead of the reverse engineered algorithm from Algorithm 1, was chosen is precisely because of the symmetry of these pictures which makes them appealing to the eye. Reverse engineering the algorithm in Algorithm 1 when implemented would require the use recursion which brings with it a range of technical difficulties, when trying to create such symmetrical images.

3 Invariants under the $\mathrm{SL}_2(\mathbb{Z})$ action

(Presented and written by Ryan)

Lemma 3.1. *Aside from the determinant, other invariants within classes of quadratic binary forms under the* $\mathrm{SL}_2(\mathbb{Z})$ *action are:*

(i) The greatest common divisor of the coefficients of the forms; and

(ii) when their discriminant is negative, the sign of the coefficients of the x^2 *(*y^2*) term between any two forms. That is, if* a, a' *are the coefficients of* x^2 *of any two equivalent binary quadratic forms which have negative discriminant, then* $\mathrm{sign}(a) = \mathrm{sign}(a')$.

Remark. Note that if the discriminant of a quadratic binary form $f(x, y) = ax^2+bxy+cy^2$ is negative, a and c have the same sign. Indeed, $b^2 - 4ac < 0$ is true if and only if $0 \leq b^2 < 4ac$, and $0 < ac$ is true if and only if a, c have the same sign.

These two invariants are of interest, as they allow us to classify binary quadratic forms even further. First we

Define 3.2 (Primitve binary quadratic forms)**.** A binary quadratic form is said to be *primitive* if the coefficients are globally coprime[2] (that is, the g.c.d. of the coefficients is 1).

and note that a form whose coefficients have g.c.d. r, is r times a primitive form with discriminant D/r^2. Indeed, if $r = \gcd(a, b, c)$, then $f(x, y) = (a/r)x^2+(b/r)xy+(c/r)y^2$ is a primitive quadratic binary form with determinant $(b/r)^2 - 4(a/r)(c/r) = (b^2 - 4ac)/r^2$.

As such, the primitive forms are the building blocks of *all* forms. Moreover, we see from the lemma, that if a class of forms has a primitive representative, then *all* representatives are primitive. As such, it makes sense to speak of "classes of primitive forms".

Proof of the Lemma. In this proof, let f, f' be binary quadratic forms, representatives of the same class under the $\mathrm{SL}_2(\mathbb{Z})$ action, with coefficients a, b, c and a', b', c' respectively. Let Γ in $\mathrm{SL}_2(\mathbb{Z})$ relate f' with f via $f' = \Gamma \cdot f$ and denote by D their discriminant

[2] As opposed to being pairwise coprime.

$b^2 - 4ac = b'^2 - 4a'c'$. Then we have the relation

$$\begin{aligned} a' &= a\Gamma_{11}^2 + b\Gamma_{11}\Gamma_{22} + c\Gamma_{22}^2 \\ b' &= 2a\Gamma_{11}\Gamma_{12} + b(\Gamma_{11}\Gamma_{21} + \Gamma_{12}\Gamma_{22}) + 2c\Gamma_{21}\Gamma_{22} \\ c' &= a\Gamma_{12}^2 + b\Gamma_{12}\Gamma_{21} + c\Gamma_{21}^2 \end{aligned}$$

(and the same relation, expressing a, b, c as functions of a', b', c' using the inverse of Γ).

(i) If r is a divisor of a, b and c, then r clearly also divides a', b' and c'; hence $\gcd(a,b,c) \mid \gcd(a',b',c')$. Yet by symmetry, we have $\gcd(a',b',c') \mid \gcd(a,b,c)$ so $\gcd(a',b',c') = \gcd(a,b,c)$.

(ii) Now assume that $D = b^2 - 4ac < 0$. Note that this forces $a, c \neq 0$. From

$$\begin{aligned} aa' &= a^2\Gamma_{11}^2 + ab\Gamma_{11}\Gamma_{22} + ac\Gamma_{22}^2 \\ &= \left(a\Gamma_{11} + \frac{1}{2}b\Gamma_{22}\right)^2 - \left(\frac{1}{2}b\Gamma_{22}\right)^2 + ac\Gamma_{22}^2 \\ &= \left(a\Gamma_{11} + \frac{1}{2}b\Gamma_{22}\right)^2 - \frac{1}{4}b^2\Gamma_{22}^2 + ac\Gamma_{22}^2 \\ &= \left(a\Gamma_{11} + \frac{1}{2}b\Gamma_{22}\right)^2 - \frac{1}{4}\Gamma_{22}^2(4ac - b^2) \\ &= \left(a\Gamma_{11} + \frac{1}{2}b\Gamma_{22}\right)^2 + \frac{1}{4}\Gamma_{22}^2(-D) \\ &> 0 \end{aligned}$$

we can conclude that a, a' have the same sign. Using the same "complete the square" method, we can make the same observation for c, c':

$$cc' = \cdots = \left(c\Gamma_{21} + \frac{1}{2}b\Gamma_{12}\right)^2 + \frac{1}{4}\Gamma_{12}^2(-D) > 0.$$

□

Corollary 3.3. *If the coefficient of x^2 in a binary quadratic form with negative discriminant is positive, then the form is positive on all non-zero integer pairs.*

Proof. Let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form with discriminant $D < 0$ and $a > 0$. Further, let α, β be arbitrary integers. Then the matrix

$$\Gamma = \begin{pmatrix} \alpha & \alpha\beta - 1 \\ 1 & \beta \end{pmatrix} \quad \text{with} \quad \det(\Gamma) = \alpha\beta - 1(\alpha\beta - 1) = 1$$

lies in $\mathrm{SL}_2(\mathbb{Z})$. Now let $f' = \Gamma \cdot f$ with coefficients a', b', c'. We can now write

$$0 < aa' = a(a\alpha^2 + b\alpha\beta + c\beta^2) = af(\alpha, \beta)$$

to conclude that $f(\alpha, \beta) > 0$ for all integral α, β not both zero. □

Corollary 3.4. *If the coefficient of y^2 in a binary quadratic form with negative discriminant is positive, then the form is positive on all non-zero integer pairs.*

Proof. This proof is entirely analogous to the x^2 case, using the matrix

$$\Gamma = \begin{pmatrix} \alpha\beta + 1 & \alpha \\ \beta & 1 \end{pmatrix} \quad \text{with} \quad \det(\Gamma) = (\alpha\beta + 1) - \alpha\beta = 1$$

instead. □

Remark. Here we also see the importance of the remark following the lemma. If it were possible for a, c to have different signs (w.l.o.g. assume $a > 0$, $c < 0$), we would have a contradiction: since on the one hand all values of $f(x, y)$ (on integral values of x, y) are positive because $a > 0$, yet on the other hand, all values of $f(x, y)$ are negative because $c < 0$.

These findings lead to the

Definition 3.5 (Positive-definite, Negative-definite)**.** If a quadratic binary form has negative discriminant, then the previous lemma showed that either all values are positive or all values are negative. Then we call such a form *positive-definite* or *negative-definite* respectively. Looking at the sign of the coefficients of x^2 (or y^2) will tell us whether the form is positive-definite or negative-definite.

In fact, we see that for every class of positive-definite binary quadratic forms, there is a corresponding class of negative-definitive binary quadratic forms with exactly the same representatives up to multiplication with -1. Indeed, let $f(x, y) = ax^2 + bxy + cy^2$ be a positive-definite form (with negative discriminant D). Then $g(x, y) = -f(x, y)$ also has discriminant

$$(-b)^2 - 4(-a)(-c) = b^2 - 4ac = D < 0$$

but is clearly negative-definite.

Finally, this all allows us to

Define 3.6 (the Class number)**.** Given an integer D we define the *class number* $h(D)$ (of the binary quadratic forms under the $\mathrm{SL}_2(\mathbb{Z})$ action) as follows:

(i) if $D > 0$, then we define $h(D)$ to be the number of classes whose representatives are primitive binary quadratic forms of discriminant D;

(ii) if $D < 0$, then we define $h(D)$ to be the number of classes whose representatives are *positive-definite* primitive binary quadratic forms of discriminant D.

By Theorem 2.1, this class number is always finite.

Lemma 3.7. *If $D \equiv 2, 3 \pmod 4$, then $h(D) = 0$. Else, we have seen there is a fundamental form with discriminant D.*

Proof. Note that for any choice of a, b, c, $b^2 - 4ac \equiv b^2 \pmod 4$. Consequently, any $D = b^2 - 4ac$ can only be

$$D \equiv \begin{cases} 0 & \text{if} \quad b \equiv 0 \pmod 4 \\ 1 & \text{if} \quad b \equiv 1 \pmod 4 \\ 0 & \text{if} \quad b \equiv 2 \pmod 4 \\ 1 & \text{if} \quad b \equiv 3 \pmod 4 \end{cases}$$

Hence, any value $D \equiv 2, 3 \pmod 4$ cannot be the discriminant of any binary quadratic form. □

4 Counting representations of integers

Now we will move on to study the number of solutions (x, y) of $f(x, y) = n$ there are for a given n. We call these solutions *representations of n under f*. Before we define the "representations-number" which encapsulates this problem, we will perform some reductions.

Example 4.1 (Ramanujan, sums of cubes)**.** *A very famous example — in the realm of binary **cubic** forms — is one of Ramanujan: what is the smallest number which can be represented as the sum of two (positive) cubes in more than one way? In the context of our work: what is the smallest n so that $f(x, y) = x^3 + y^3 = n$ has more than one (with x, y positive) solution? Ramanujan claimed this number to be* $1729 = 10^3 + 9^3 = 12^3 + 1^3$.

This example is historically attributed to an anecdote of Hardy: When visiting Ramanujan in hospital, Hardy mentioned in to Ramanujan that he found the number of the cab that he had arrived in, 1729, to be quite boring; adding that he hoped it not to be a bad omen for Ramanujan's health. Ramanujan retorted, that indeed 1729 is an interesting number, for it is the smallest number that can be written as the sum of two cubes in two different ways.

Example 4.2 (Fermat, sums of squares)**.** *Fermat formulated the following result for primes: a prime p is the sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

This second example, essentially states that any prime $p \equiv 1 \pmod 4$ has at least one representation under the quadratic binary form $f(x, y) = x^2 + y^2$.

There is a natural equivalence relation on the set of solutions of the equation $f(x, y) = n$: the subgroup U_f of matrices in $\mathrm{SL}_2(\mathbb{Z})$ that fix the coefficients of $f(x, y) = ax^2 + bxy + cy^2$ send solutions of $f(x, y) = n$ to other solutions, hence naturally induces an equivalence relation.

More precisely, let U_f be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which fixes the coefficients of $f = f(x, y) = ax^2 + bxy + cy^2$. That is, for all Ψ in U_f we have that $\Psi \cdot f(x, y) = f(x, y)$. Equivalently,

$$U_f = \left\{ \Psi \in \mathrm{SL}_2(\mathbb{Z}) \mid \text{such that } \begin{cases} a = a\Psi_{11}^2 + b\Psi_{11}\Psi_{22} + c\Psi_{21}^2 \\ b = 2a\Psi_{11}\Psi_{12} + b(\Psi_{11}\Psi_{22} + \Psi_{12}\Psi_{21}) + 2c\Psi_{21}\Psi_{22} \\ c = a\Psi_{12}^2 + b\Psi_{12}\Psi_{22} + c\Psi_{22}^2 \end{cases} \right\}.$$

We call elements of the set U_f *automorphisms* of f. It is readily seen that this is indeed a (non-empty) group.

Now, if (x, y) is a solution of $f(x, y) = n$, then $\Psi \cdot (x, y)$ is also a solution of $f(x, y) = n$. Hence we obtain a well-defined group action of U_f acting on the set of solutions of $f(x, y) = n$. This group action in turn defines an relation, where $(x, y) \sim (x', y')$ if there exists a Ψ in U_f such that $(x, y) = \Psi \cdot (x', y')$. This relation is clearly reflexive, symmetric and transitive by properties of a group action, hence we have an equivalence relation.

So now, we can

Define 4.3 (the Representations-number)**.** The *representations-number $R(n, f)$ of n under f* is the number under U_f invariant solutions of $f(x, y) = n$. That is, $R(n, f)$ counts the number of times $f(x, y)$ takes the value n up to transformations of (x, y) under U_f.

and note that this is well defined. Indeed, if f, f' are representatives of the same class under the $\mathrm{SL}_2(\mathbb{Z})$ action, related via Γ, then Γ will take representations of n under f and map them to representations of n under f'. Furthermore, we will see that $R(n, f)$ is finite.

Definition 4.4 (Total representations-number)**.** We define the *total representations-number* $R(n)$ *of* n *under forms of discriminant* D to be the sum

$$R(n) = \sum_{i=1}^{h(D)} R(n, f_i)$$

whereby the f_i are representatives of the (different) classes of primitive binary quadratic forms of discriminant D.

We know of no closed form for the representations-number $R(n, f_i)$, however we *can* calculate the value $R(n)$ in a closed form.

5 The structure of the Automorphism group

(Presented and written by Karlo)

Theorem 5.1. *Let $f(x,y) = ax^2 + bxy + y^2$ a primitive binary quadratic form with a non-square discriminant D. Then the map*

$$(t,u) \mapsto \begin{pmatrix} \frac{t-bu}{2} & -cu \\ au & \frac{t+bu}{2} \end{pmatrix} \tag{5.1}$$

is a bijection between the set of solution of the Pell equation 1.2 and U_f. If we consider the group $(U_f, \circ)$ with

$$(t_1,u_1) \circ (t_2,u_2) = \left(\frac{t_1t_2+Du_1u_2}{2}, \quad \frac{t_1u_2+u_1t_2}{2}\right) \tag{5.2}$$

then the above mentioned map is also a group isomorphism. Furthermore the group U_f is finite for $D<0$ and cyclical of order

$$w = \begin{cases} 6, & \text{for } D=-3 \\ 4, & \text{for } D=-4 \\ 2, & \text{for } D<-4 \end{cases} \tag{5.3}$$

Whereas for $D>0$ it holds $U_f \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. From the definition of U_f we get that for $(\alpha,\beta;\gamma,\delta) \in U_f$

$$\begin{aligned} \alpha\beta &= \beta(a\alpha^2 + b\alpha\gamma + c\gamma^2) && (5.4)\\ &= \alpha(a\alpha\beta + b\beta\gamma) + c\beta\gamma^2 && (5.5)\\ &= \alpha(-c\gamma\delta) + c\beta\gamma^2 && (5.6)\\ &= -c\gamma && (5.7) \end{aligned}$$

5.6 follows from

$$2(a\alpha\beta + b\beta\gamma + c\gamma\delta) = b(1 - \alpha\delta + \beta\gamma) = 0 \tag{5.8}$$

and 5.7 follows from

$$\alpha\delta - \beta\gamma = 1 \tag{5.9}$$

and similarly

$$\begin{aligned} c(\alpha-\delta) &= \alpha(a\beta^2+b\beta\gamma\delta+c\delta^2)-c\delta && (5.10)\\ &= \beta(a\alpha\beta+c\gamma\delta)+b\alpha\beta\delta && (5.11)\\ &= -\beta(b\beta\gamma)+b\alpha\beta\delta && (5.12)\\ &= b\beta && (5.13) \end{aligned}$$

Thus we get the following

$$\frac{\gamma}{a}=\frac{\delta-\alpha}{b}=\frac{-\beta}{c} \tag{5.14}$$

Now since f is primitive the greatest common divisor is 1, meaning that either side of the equation above is some integer u. We define $t=\alpha+\delta$ and get

$$\begin{cases} \alpha = \frac{t-bu}{2} \\ \delta = \frac{t+bu}{2} \beta = -cu\gamma = au \end{cases} \tag{5.15}$$

Combined with $\alpha\delta-\beta\gamma=1$ we get Pell's equation and thus we have shown for any matrix in U_f we can find a solution to Pell's equation. For the opposite direction we just have to show that the matrix in 5.1 is in U_f and that the matrix multiplication yields the same result as the map in 5.2. This can be done by direct computation.

To prove the second claim of the theorem we let $D<0$. We get that

$$t^2-Du^2 \geq t^2 \qquad , \qquad t^2-D^2 \geq |D|u^2 \tag{5.16}$$

Which means that Pell's equation only has solutions for $|t|,|u|\leq 2$ which are

$$\begin{cases} (t,u)=(\pm 2,0) \text{ or } (\pm 1,\pm 1) & \text{for } D=-3 \\ (t,u)=(\pm 2,0) \text{ or } (0,\pm 1) & \text{for } D=-4 \\ (t,u)=(\pm 2,0) & \text{for } D<-4 \end{cases} \tag{5.17}$$

This also proves with our previous result that the order of U_f for $D<0$ is given by w as described in the statement of the theorem. Now we want to show the cyclical nature of U_f. We consider for each solution (t,u) of 1.2 the following

$$\epsilon=\frac{t+u\sqrt{D}}{2} \ , \qquad \epsilon'=\frac{t+u\sqrt{D}}{2} \tag{5.18}$$

We note that $\epsilon\epsilon' = 1$ and that for any solution (t, u) that $(t, -u)$ is also a solution. So the ϵ of (t, u) is precisely the ϵ' of $(t, -u)$. We also consider the following map

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \epsilon = \frac{\alpha + \delta}{2} + \frac{\gamma}{2a}\sqrt{D} \tag{5.19}$$

The image of this map is (together with the multiplication) a group, because of the definition of ϵ and the fact that it is closed under multiplication. This map is thus a homomorphism from U_f onto $\mathbb{C}^*$. It is also injective since its kernel is trivial. With the result from 5.17 we get

$$\begin{cases} \epsilon = \pm 1 \text{ or } \frac{\pm 1 \pm i\sqrt{(3)}}{2} & \text{for} \quad D = -3 \\ \epsilon = \pm 1 \text{ or } \pm i & \text{for} \quad D = -4 \\ \epsilon = \pm 1 & \text{for} \quad D < -4 \end{cases} \tag{5.20}$$

These are precisely the w-th unit roots which shows us that U_f is indeed cyclical.

For $D > 0$ the map 5.19 gives us an injection on $\mathbb{R}^*$. The image is a subgroup that contains ± 1 since $(t, u) = (\pm 2, 0)$ is always a solution. However for $u, t \neq 0$ we get that $|\epsilon| > 1$. So we either get $U_f = \left\{\pm \mathrm{id}_{\mathrm{Mat}_{2\times 2}}\right\}$ for the subgroup $\{\pm 1\} \subseteq \mathbb{R}^*$ or we get $U_f \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ since for the smallest solution (t_0, u_0) the so called fundamental unit $\epsilon_0 = (t_0 + u_0\sqrt{D})/2$ (which is only depends on D) is the generator of $\{\epsilon_0^n | n \in \mathbb{Z}\}$ a subgroup of the image of 5.19 onto $\mathbb{R}^*$. It will be shown later on that $U_f = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is the only possibility. This concludes the proof. □

6 Calculating total representations numbers

(Presented and written by Ryan)

Theorem 6.1. *Let D be a fundamental discriminant and n a non-zero integer. Then the total representations number $R(n)$ of n under the (primitive) forms of discriminant D is given by*

$$R(n) = \sum_{m|n} \chi_D(m)$$

where $\chi_D(m)$ is the Dirichlet character modulo $|D|$ characterised by

$$\chi_D(p) = \left(\frac{D}{p}\right) = \begin{cases} 0 & \text{if} \quad p \mid D \\ 1 & \text{if} \quad p \nmid D, \exists x \in \mathbb{Z} : D \equiv x^2 \pmod{p} \\ -1 & \text{else.} \end{cases}$$

$$\chi_D(2) = \begin{cases} 0 & \text{if} \quad D \equiv 0 \pmod{4}, \\ 1 & \text{if} \quad D \equiv 1 \pmod{8}, \\ -1 & \text{if} \quad D \equiv 5 \pmod{8}, \end{cases}$$

In particular, all values of $R(n)$ are finite.

Definition 6.2 ((Recall) Fundamental discriminant)**.** A *fundamental discriminant* or *fundamental number* is an integer D that either satisfies

$$D \equiv 1 \pmod{4} \quad \text{and} \quad D \text{ squarefree}$$

or

$$D \equiv 0 \pmod{4}; \quad \frac{D}{4} \text{ squarefree; and } \quad \frac{D}{4} \equiv 2 \text{ or } 3 \pmod{4}.$$

Corollary 6.3. *The expectation of $R(n)$ is the value of the L-function $L(s, \chi_D)$ at $s = 1$. That is*

$$\lim_{N \to \infty} \left(\frac{1}{N} \sum_{n=1}^{N} R(n) \right) = L(1, \chi_D).$$

Remark. This has a "probabilistic" interpretation as the expected number of representation of a number n: even though calculating individual values of $R(n)$ for a given D might be cumbersome, we know what the value should be on average.

Proof of corollary. Consider[3]

$$\begin{aligned}
\sum_{n=1}^{N} R(n) &= \sum_{n\le N}\sum_{m\mid n}\chi_D(m) \\
&= \sum_{\substack{1\le k,m\le N\\ km\le N}}\chi_D(m) \\
&= \sum_{1\le k,m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k) \\
&= \sum_{1\le k,m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x\le\sqrt{N}\right\}}(m) \\
&\quad + \sum_{1\le k,m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x>\sqrt{N}\right\}}(m)
\end{aligned}$$

Here, we have simply rewritten the sum using different notation, and split it into two sub-sums. Let us turn to each sum separately. On the one hand we can rather crudely write

$$\begin{aligned}
\sum_{1\le k,m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x\le\sqrt{N}\right\}}(m) &= \sum_{1\le m\le N}\sum_{1\le k\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x\le\sqrt{N}\right\}}(m) \\
&= \sum_{1\le m\le N}\sum_{1\le k\le N/m}\chi_D(m)\,\mathbb{1}_{\left\{x\le\sqrt{N}\right\}}(m) \\
&= \sum_{1\le m\le\sqrt{N}}\sum_{1\le k\le N/m}\chi_D(m) \\
&= \sum_{1\le m\le\sqrt{N}}\chi_D(m)\sum_{1\le k\le N/m}1 \\
&= \sum_{m\le\sqrt{N}}\chi_D(m)\left(\frac{N}{m}+O(1)\right).
\end{aligned}$$

On the other hand we have

$$\begin{aligned}
\sum_{1\le k,m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x>\sqrt{N}\right\}}(m) &= \sum_{1\le k\le N}\sum_{1\le m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x>\sqrt{N}\right\}}(m) \\
&= \sum_{1\le k\le N}\sum_{1\le m\le N/k}\chi_D(m)\,\mathbb{1}_{\left\{x>\sqrt{N}\right\}}(m) \\
&= \sum_{1\le k\le N}\sum_{\sqrt{N}<m\le N/k}\chi_D(m) \\
&= \sum_{1\le k\le\sqrt{N}}\sum_{\sqrt{N}<m\le N/k}\chi_D(m).
\end{aligned}$$

[3]Here the notation $\mathbb{1}_A(x)$ is the usual indicator function on whether x lies in the set A.

Now we will look at the inner sum $\sum_{\sqrt{N}<m\leq n/k}\chi_d(m)$: for any given k, let

$$r_1 = \min\left(\left\{r\in\mathbb{N} \mid rD > \sqrt{N}\right\}\right)$$
$$r_2 = \max\left(\left\{r\in\mathbb{N} \mid rD < \frac{N}{k}\right\}\right)$$

then

$$\begin{aligned}
\sum_{\sqrt{N}<m\leq n/k}\chi_D(m) &= \sum_{\sqrt{N}<m<r_1D}\chi_D(m) + \sum_{m=Dr_1}^{Dr_2}\chi_D(m) + \sum_{Dr_2<m<N/k}\chi_D(m)\\
&= \sum_{\sqrt{N}<m<r_1D}\chi_D(m) + \sum_{r=r_1}^{r_2}\sum_{l=1}^{D}\chi_D(rD+l) + \sum_{Dr_2<m<N/k}\chi_D(m)\\
&= \sum_{\sqrt{N}<m<r_1D}\chi_D(m) + \sum_{r=r_1}^{r_2}\sum_{l=1}^{D}\chi_D(rD+l) + \sum_{Dr_2<m<N/k}\chi_D(m)\\
&= \sum_{\sqrt{N}<m<r_1D}\chi_D(m) + \sum_{r=r_1}^{r_2}\underbrace{\sum_{l=1}^{D}\chi_D(l)}_{=0} + \sum_{Dr_2<m<N/k}\chi_D(m)\\
&= \sum_{\sqrt{N}<m<r_1D}\chi_D(m) + \sum_{Dr_2<m<N/k}\chi_D(m)\\
&= O(1)
\end{aligned}$$

Here we used that χ_D is a non-principal Dirichlet character modulo $|D|$. Hence

$$\begin{aligned}
\sum_{n=1}^{N}R(n) &= \sum_{m\leq\sqrt{N}}\chi_D(m)\left(\frac{N}{m}+O(1)\right)+O(\sqrt{N})\\
&= N\sum_{m\leq\sqrt{N}}\chi_D(m)\left(\frac{1}{m}+O\left(\frac{1}{N}\right)\right)+O(\sqrt{N})\\
&= N\sum_{m\leq\sqrt{N}}\frac{\chi_D(m)}{m}+\sum_{m\leq\sqrt{N}}O\left(\frac{1}{N}\right)+O(\sqrt{N})\\
&= N\sum_{m\leq\sqrt{N}}\frac{\chi_D(m)}{m}+O\left(\frac{1}{\sqrt{N}}\right)+O(\sqrt{N}).
\end{aligned}$$

So

$$\begin{aligned}\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}R(n) &= \lim_{N\to\infty}\left(\sum_{m\le\sqrt{N}}\frac{\chi_D(m)}{m}+O\left(\frac{1}{N^{3/2}}\right)+O\left(\frac{1}{\sqrt{N}}\right)\right)\\ &= \sum_{m=1}^{\infty}\frac{\chi_D(m)}{m}\\ &= L(1,\chi_D)\end{aligned}$$

□

Remark. Note that the trick of splitting the sum into intervals of length $|D|$ to conclude that

$$\sum_{1\le k,m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x>\sqrt{N}\right\}}(m)=O(\sqrt{N})$$

does not work for the first sum

$$\sum_{1\le k,m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x\le\sqrt{N}\right\}}(m)$$

using the same steps, we obtain

$$\begin{aligned}\sum_{1\le k,m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x\le\sqrt{N}\right\}}(m) &= \sum_{1\le k\le N}\sum_{1\le m\le N}\chi_D(m)\,\mathbb{1}_{\{xy\le N\}}(m,k)\,\mathbb{1}_{\left\{x\le\sqrt{N}\right\}}(m)\\ &= \sum_{1\le k\le N}\sum_{1\le m\le N/k}\chi_D(m)\,\mathbb{1}_{\left\{x\le\sqrt{N}\right\}}(m)\\ &= \sum_{1\le k\le N}\sum_{m\le\min\left(\sqrt{N},N/k\right)}\chi_D(m)\end{aligned}$$

and there is little we can do with the $\min\left(\sqrt{N},N/k\right)$ condition.

To prove the Theorem, we will need the following auxiliary

Lemma 6.4. *Let G be a group that acts on the finite sets X,Y. Define the diagonal group action $G\times(X\times Y)\to X\times Y$ by $(g,(x,y))\mapsto(g\cdot x,g\cdot y)$. Further, let $S\subseteq X\times Y$*

be a G-invariant subset (that is, $G \cdot S \subseteq S$). Finally, define

$$\begin{aligned} Y_x &= \{y \in Y \mid (x,y) \in S\} \\ X_y &= \{x \in X \mid (x,y) \in S\} \\ G_x &= \mathrm{Stab}_G(x) = \{g \in G \mid gx = x\} \end{aligned}$$

Then

$$\left|S/G\right| = \sum_{x \in X/G} \left|Y_x/G_x\right| = \sum_{y \in Y/G} \left|X_y/G_y\right|$$

where, as usual, the "quotient" notation of a set by a group is the set of orbits within the set under the group action of the group.

Proof of the Theorem. Let $R^*(n)$ be the number of non-equivalent primitive representation of n by forms of discriminant D. We call a representation $f(x_0, y_0) = n$ primitive, if x_0 and y_0 are coprime. Now we have

$$R(n) = \sum_{\substack{g \geq 1 \\ g^2 | n}} R^*\left(\frac{n}{g^2}\right)$$

Indeed, suppose $f(x_1, y_1)$ is a non-primitive representation with $x_1 = gx_0$ and $y_1 = gy_0$ for x_0, y_0 coprime. Then $f(x_1, y_1) = g^2 f(x_0, y_0) = n$. Hence $f(x_0, y_0)$ is a representation of n/g^2. Now we want to prove an easier way to calculate $R^*(n)$. We claim that

$$R^*(n) = \left|\left\{b \in \{0, \ldots, 2n-1\} \mid b^2 \equiv D \pmod{4n}\right\}\right|.$$

and prove this claim using the Auxiliary lemma with

$$\begin{aligned} G &= \mathrm{SL}_2(\mathbb{Z}) \\ X &= \left\{f(x,y) = ax^2 + bxy + cy^2 \mid b^2 - 4ac = D\right\} \\ Y &= \left\{(x,y) \in \mathbb{Z}^2 \mid \gcd(x,y) = 1\right\} \\ S &= \{(f,(x,y)) \in X \times Y \mid f(x,y) = n\} \end{aligned}$$

In this notation

- The action of G on Y is defined by $\Gamma \cdot (x,y) = \Gamma(x,y)^T$ (where the product is the usual matrix-vector multiplication and we abuse notation and interpret the result

of $\Gamma(x,y)^T = (x',y')^T$ as a tuple (x',y') so that $\Gamma \cdot (x,y)$ lies in Y again). Indeed

$$\Gamma \cdot (x,y) = \Gamma(x,y)^T = \Gamma \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \Gamma_{11} & \Gamma_{12} \\ \Gamma_{21} & \Gamma_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \Gamma_{11}x + \Gamma_{12}y \\ \Gamma_{21}x + \Gamma_{22}y \end{pmatrix}$$

is consistent with our previous definitions of the $\mathrm{SL}_2(\mathbb{Z})$ action.

- The action of G on X is defined by $\Gamma \cdot f(x,y) = f(\Gamma^{-1}(x,y)^T)$ (where we abuse notation and write $f((x,y))$ to mean $f(x,y)$). Note that the inverse is necessary for the associativity property of a well-defined group action to be satisfied:

$$\begin{aligned} (\Gamma\Delta) \cdot f(x,y) &= f((\Gamma\Delta)^{-1} \cdot (x,y)) \\ &= f((\Delta^{-1}\Gamma^{-1}) \cdot (x,y)) \\ &= f(\Delta^{-1} \cdot (\Gamma^{-1} \cdot (x,y))) \\ &= \Delta \cdot f((\Gamma^{-1} \cdot (x,y))) \\ &= \Gamma \cdot (\Delta \cdot f(x,y)). \end{aligned}$$

  Without the inverse, we get

$$\begin{aligned} (\Gamma\Delta) \cdot f(x,y) &= f((\Gamma\Delta) \cdot (x,y)) \\ &= f(\Gamma(\Delta \cdot (x,y))) \\ &= \Gamma \cdot f(\Delta \cdot (x,y)) \\ &= \Delta \cdot (\Gamma \cdot f(x,y)) \\ &\neq \Gamma \cdot (\Delta \cdot f(x,y)) \end{aligned}$$

- X/G are the equivalence classes of quadratic binary forms of discriminant D under the $\mathrm{SL}_2(\mathbb{Z})$-action.
- Y_f is the set of primitive representations of n by f.
- Y_f/G_f is the set of primitive non-equivalent representations of n by f.

Now verifying that S really is G-invariant is easy: let $(f,(x,y))$ lie in $X \times Y$, and Γ in $\mathrm{SL}_2(\mathbb{Z})$ then

$$\Gamma \cdot (f,z) = (\Gamma \cdot f, \Gamma \cdot (x,y))$$

and

$$(\Gamma \cdot f)(\Gamma \cdot (x,y)) = f(\Gamma^{-1}(\Gamma \cdot (x,y))) = f((\Gamma^{-1}\Gamma) \cdot (x,y)) = f((x,y)) = f(x,y)$$

so if $f(x,y) = n$ (that is, $(f,(x,y))$ lies in S) then $\Gamma \cdot (f,(x,y))$ will also lie in S.

So, we are permitted to apply the lemma. On the one hand, we get

$$\left|S/G\right| = \sum_{f \in X/G} \left|Y_x/G_f\right| = \sum_{f \in X/G} R^*(n,f) = R^*(n)$$

and on the other hand we get

$$\left|S/G\right| = \sum_{z \in Y/G} \left|X_z/G_z\right|.$$

For this we note for all (x,y) in Y, $(1,0) \sim (x,y)$ via

$$\begin{pmatrix} x & -b \\ y & a \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \qquad \text{with} \quad \det \begin{pmatrix} x & -b \\ y & a \end{pmatrix} = ax + by$$

whereby a, b are the Bezout-coefficients with $ax + by = 1$ (which exist, because x, y are coprime) making the matrix[4] $(x, -b; y, a)$ an element of $\mathrm{SL}_2(\mathbb{Z})$. Hence Y/G has only one orbit, which is represented by $(1,0)$. Hence

$$\left|S/G\right| = \sum_{z \in Y/G} \left|X_z/G_z\right| = \left|X_{(1,0)}/G_{(1,0)}\right|.$$

For this element, we have

$$G_{(1,0)} = \{g \in G \mid g \cdot (1,0) = (1,0)\} = \left\{ \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \mid r \in \mathbb{Z} \right\} \subseteq \mathrm{SL}_2(\mathbb{Z})$$

[4] Using the usual inline-matrix notation, where commas indicate the next column, and semicolons the next row starting at the top left.

and

$$\begin{aligned}
X_{(1,0)} &= \{f \in X \mid (f,(1,0)) \in S\} \\
&= \{f \in X \mid f(1,0) = n\} \\
&= \left\{f(x,y) = ax^2 + bxy + cy^2 \in X \mid f(1,0) = a = n\right\} \\
&= \left\{f \in X \mid f(x,y) = nx^2 + bxy + \frac{b^2-D}{4n}y^2\right\} \\
&= \left\{nx^2 + bxy + \frac{b^2-D}{4n}y^2 \mid \frac{b^2-D}{4n} \in \mathbb{Z}\right\} \\
&= \left\{nx^2 + bxy + \frac{b^2-D}{4n}y^2 \mid b \in \mathbb{Z}, b^2 \equiv D \pmod{4n}\right\} \subseteq X
\end{aligned}$$

Now, for any $(1,r;0,1)$ in $G_{(1,0)}$ acting on f in $X_{(1,0)}$ we obtain

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \cdot f(x,y) = nx^2 + (b+2nr)xy + \frac{(b+2nr)^2 - D}{4n}y^2$$

and see that any two $nx^2 + bxy + ((b^2-D)/4n)y^2$, $nx^2 + b'xy + (((b')^2-D)/4n)y^2$ are equivalent under $G_{(1,0)}$ if and only if $b \equiv b' \pmod{2n}$. So

$$\begin{aligned}
\left|S/G\right| &= \sum_{z \in Y/G} \left|X_z/G_z\right| \\
&= \left|X_{(1,0)}/G_{(1,0)}\right| \\
&= \left|\left\{b \in \{0,\dots,2n-1\} \mid b^2 \equiv D \pmod{4n}\right\}\right|.
\end{aligned}$$

and conclude

$$R^*(n) = \left|\left\{b \in \{0,\dots,2n-1\} \mid b^2 \equiv D \pmod{4n}\right\}\right|.$$

Now, by using the Chinese remainder theorem, we obtain

$$R^*(n) = \prod_{p \text{ prime}} R^*(p^{v_p(n)})$$

where $v_p(n)$ is the p-adic valuation[5] of n. Now, we would like to get a cleaner representation of

$$R^*(p^k) = \left|\left\{b \in \left\{0,\dots,2p^k-1\right\} \mid b^2 \equiv D \pmod{4p^k}\right\}\right|.$$

[5] This counts the number of times p divides n, as such $n = \prod_{(p \text{ prime})} p^{v_p(n)}$.

Our first step is to note that

$$R^*(p^k) = \frac{1}{2}\left|\left\{b \in \left\{0,\dots,4p^k-1\right\} \mid b^2 \equiv D \pmod{4p^k}\right\}\right|$$

because every solution of $b^2 \equiv D \pmod{4p^k}$ in $\{0,\dots,2p^k-1\}$ corresponds to a solution in $\{2p^k,\dots,4p^k-1\}$ by adding $2p^k$. Indeed, for b in $\{0,\dots,2p^k-1\}$ we have

$$b^2 \equiv (b+2p^k)^2 \equiv b^2 + 4p^k(b+p^k) \equiv D \pmod{4p^k}.$$

So if we look at all $\{0,\dots,4p^k-1\}$ we get twice the number of solutions as are contained in $\{0,\dots,2p^k-1\}$. Now, assuming $p \neq 2$, we can apply the Chinese remainder theorem again, to obtain

$$\begin{aligned} R^*(p^k) &= \frac{1}{2}\left|\left\{b \in \left\{0,\dots,4p^k-1\right\} \mid b^2 \equiv D \pmod{4p^k}\right\}\right| \\ &= \frac{1}{2}\left|\left\{b \in \left\{0,\dots,p^k-1\right\} \mid b^2 \equiv D \pmod{p^k}\right\}\right| \\ &\quad \cdot \left|\left\{b \in \{0,\dots,4\} \mid b^2 \equiv D \pmod{4}\right\}\right| \end{aligned}$$

To calculate

$$\left|\left\{b \in \{0,\dots,4\} \mid b^2 \equiv D \pmod{4}\right\}\right|$$

we need to perform a case distinction for possible values of the fundamental discriminant D

(i) (Case 1: $D \equiv 1 \pmod 4$) Here, there are two possible solutions for $b = 1, 3$.

(ii) (Case 2: $D \equiv 0 \pmod 4$) Here, there are two possible solutions for $b = 0, 2$.

Alas, in both cases, we get 2 solutions and we can conclude that

$$R^*(p^k) = \left|\left\{b \in \left\{0,\dots,p^k-1\right\} \mid b^2 \equiv D \pmod{p^k}\right\}\right|.$$

Now we will prove the Theorem for $p \neq 2$. We note that

(i) If $p \nmid D$, then $D \not\equiv 0 \pmod{p^k}$ and

$$\left|\left\{b \in \left\{0,\dots,p^k-1\right\} \mid b^2 \equiv D \pmod{p^k}\right\}\right| = \begin{cases} 2, & \text{if } \exists b : b^2 \equiv D \pmod{p^k} \\ 0, & \text{if } \nexists b : b^2 \equiv D \pmod{p^k} \end{cases}$$

It is clear, that if we have one solution b to $b^2 \equiv D \pmod{p^k}$, then $-b$ is also a solution. Since $b^2 \equiv D \not\equiv 0 \pmod{p^k}$ we see that $b \not\equiv -b \pmod{p^k}$ and we have two distinct solutions.

We now want to prove that there are no more than 2 solutions. Let b, c be two solutions $b^2 \equiv c^2 \equiv D \pmod{p^k}$ then $(b-c)(b+c) \equiv 0 \pmod{p^k}$. Then we have the following case distinction: If p^k divides $(b-c)$, then $b \equiv c \pmod{p^k}$ (i.e. they are the same solution) and if p^k divides $(b+c)$ then $b \equiv -c \pmod{p^k}$ (i.e. they are the same solution but with a different sign). These are the two solutions above, in the case that D is a quadratic residue modulo p.

We are left with the case in which $p \leq p^l < p^k$ divides $(b-c)$, and p^{l-k} divides $(b+c)$. That is, the case in which the factors of p^k split amongst $(b+c)$ and $(b-c)$. In particular, we see that p divides both $(b+c)$ and $(b-c)$ and as such, p divides $(b+c)+(b-c) = 2b$. Assuming $p \neq 2$, we have that p divides b, and by extension that p divides D. This is in direct contradiction to our assumption that $p \nmid D$. Indeed, if p divides b then $b = \lambda p$ for some integral λ; combined with $b^2 \equiv D \pmod{p^k}$ implying the existence of some integral μ such that $b^2 - D = (\lambda p)^2 - D = \mu p^k$ we have $D = p(\mu p^{k-1} - \lambda^2 p)$.

(ii) If $p \mid D$, then $D \equiv 0 \pmod{p^k}$ and

$$\left|\left\{b \in \left\{0, \ldots, p^k - 1\right\} \mid b^2 \equiv D \equiv 0 \pmod{p^k}\right\}\right| = \begin{cases} 1, & \text{if} \quad k = 1 \\ 0, & \text{else.} \end{cases}$$

If b is a solution to $b^2 \equiv D \pmod{p^k}$ then there exists an integral μ such that $b^2 - D = \mu p^k$. Moreover, if p divides D, we have an integral δ such that $D = p\delta$. Now we rearrange to obtain $b^2 = D + \mu p^k = \delta p + \mu p^k = p(\delta + \mu p^{k-1})$. So p divides b^2 and as such b, hence there is an integral β such that $b = \beta p$. Substituting this back, we obtain $b^2 - D = (\beta p)^2 - D = \mu p^k$. Hence $D = p(\beta^2 p - \mu p^{k-1})$. If $k > 1$, then we have shown that p^2 divides D, which cannot be, since D is a fundamental discriminant. If $k = 1$, then $b = 0$ is the only valid solution.

Finally, we can substitute these results into

$$R(p^k) = \sum_{\substack{g \geq 1 \\ g^2 \mid n}} R^*\left(\frac{p^k}{g^2}\right)$$

We must now perform another case distinction.

(i) Case

$$\left(\frac{D}{p}\right) = 1$$

Here, D is a non-trivial quadratic reside. So,

$$\begin{aligned}
R(p^k) &= \sum_{\substack{g\geq 1\\ g^2|n}} R^*\left(\frac{p^k}{g^2}\right) \\
&= \sum_{l=0}^{\lfloor k/2\rfloor} R^*\left(\frac{p^k}{p^{2l}}\right) \\
&= \begin{cases} \sum_{l=0}^{k/2} R^*\left(p^k/p^{2l}\right), & \text{if } k \text{ even} \\ \sum_{l=0}^{(k-1)/2} R^*\left(p^k/p^{2l}\right), & \text{if } k \text{ odd} \end{cases} \\
&= \begin{cases} R^*(p^k/p^k) + \sum_{l=0}^{(k/2)-1} R^*\left(p^k/p^{2l}\right), & \text{if } k \text{ even} \\ \sum_{l=0}^{(k-1)/2} R^*\left(p^k/p^{2l}\right), & \text{if } k \text{ odd} \end{cases} \\
&= \begin{cases} R^*(1) + \sum_{l=1}^{k/2} R^*(p^{2l}), & \text{if } k \text{ even} \\ \sum_{l=0}^{(k-1)/2} R^*(p^{2l+1}), & \text{if } k \text{ odd} \end{cases} \\
&= \begin{cases} 1 + \sum_{l=1}^{k/2} 2, & \text{if } k \text{ even} \\ \sum_{l=0}^{(k-1)/2} 2, & \text{if } k \text{ odd} \end{cases} \\
&= k+1 \\
&= \sum_{l=0}^{k} \chi_D(p^l)
\end{aligned}$$

(ii) Case

$$\left(\frac{D}{p}\right) = -1$$

here D is a non-quadratic reside modulo p, so (using the same rearrangements as above)

$$\begin{aligned} R(p^k) &= \dots \\ &= \begin{cases} 1 + \sum_{l=1}^{k/2} 0, & \text{if } k \text{ even} \\ \sum_{l=0}^{(k-1)/2} 0, & \text{if } k \text{ odd} \end{cases} \\ &= \begin{cases} 1, & \text{if } k \text{ even} \\ 0, & \text{if } k \text{ odd} \end{cases} \\ &= \sum_{l=0}^{k} \chi_D(p^l) \end{aligned}$$

(iii) Case

$$\left(\frac{D}{p}\right) = 0$$

here p divides D, so

$$\begin{aligned} R(p^k) &= \dots \\ &= \begin{cases} R^*(1) + \sum_{l=1}^{k/2} R^*(p^{2l}), & \text{if } k \text{ even} \\ \sum_{l=0}^{(k-1)/2} R^*(p^{2l+1}), & \text{if } k \text{ odd} \end{cases} \\ &= \begin{cases} R^*(1) + \sum_{l=1}^{k/2} R^*(p^{2l}), & \text{if } k \text{ even} \\ R^*(p) + \sum_{l=1}^{(k-1)/2} R^*(p^{2l+1}), & \text{if } k \text{ odd} \end{cases} \\ &= \begin{cases} 1 + \sum_{l=1}^{k/2} 0, & \text{if } k \text{ even} \\ 1 + \sum_{l=1}^{(k-1)/2} 0, & \text{if } k \text{ odd} \end{cases} \\ &= 1 \\ &= \sum_{l=0}^{k} \chi_D(p^l) \end{aligned}$$

The proof for the case $p = 2$ involves similar case distinctions. □

Theorem 6.5. *Let f be a binary quadratic form of discriminant D, which is positive-definite if $D < 0$. Then the expected value of $R(n, f)$ is given by*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} R(n, f) = \begin{cases} \frac{2\pi}{w\sqrt{-D}} & \text{if} \quad D < 0, \\ \frac{\log(\varepsilon_0)}{\sqrt{D}} & \text{if} \quad D > 0 \end{cases}$$

where w is the order of U_f and ε_0 is the fundamental value of f.

Proof. In this proof, we must distinguish between the cases $D > 0$ and $D < 0$. Let us begin with $D < 0$.

We begin with two observations

(i) The automorphism group of f is finite, of order w; and

(ii) The automorphism group $U_f \setminus \{\mathrm{id}\}$ of f has no fixed points when operating on $(\mathbb{Z} \setminus \{0\})^2$.

From these we can conclude that

$$R(n, f) = \frac{1}{w} \left|\left\{(x, y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 = n\right\}\right|.$$

Therefore

$$\sum_{n=1}^{N} R(n, f) = \frac{1}{w} \left|\left\{(x, y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 \leq N\right\}\right|$$

Now,

$$\left|\left\{(x, y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 \leq N\right\}\right|$$

describes the number of integral points inscribed by a tilted ellipse. In turn, the area

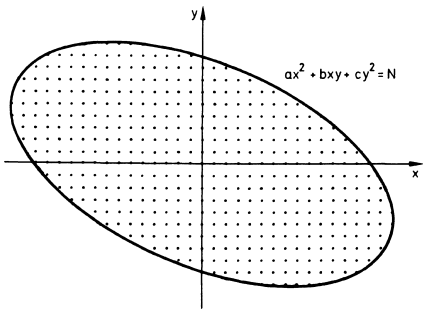


Figure 6.1: The area inscribed within the ellipse gives an estimation of the number of integral points within the ellipse

within the ellipse asymptotically counts the number of integer pairs inscribed by the ellipse. This area inscribed by an ellipse with a major axis length of α and a minor axis length of β is given by $\pi\alpha\beta$. Intuitively, this result can be seen by beginning with a circle of radius α, whose area is $\pi\alpha^2$ and then scaling the y-axis by β/α to obtain the area $\pi\alpha^2 \cdot (\beta/\alpha) = \pi\alpha\beta$ of the ellipse with axis lengths of α, β. In our case, this amounts to an area of

$$2\pi \frac{N}{\sqrt{|D|}}$$

(Calculating the axis lengths isn't necessarily trivial in the tilted ellipse case). Hence

$$\lim_{N\to\infty} \left(\frac{1}{N} \left| \left\{ (x,y) \in \mathbb{Z}^2 \mid ax^2 + bxy + cy^2 \leq N \right\} \right| \right) = 2\pi \frac{1}{\sqrt{D}}$$

which is our desired result.

Now, we must show the result for $D > 0$. Although we will use a similar method, we can no longer use the fact that U_f is finite. So, instead of counting all solutions and dividing by the number of equivalent ones, we will simply find a bounded representative of every solution. This approach is somewhat similar to the reduction in the proof of Theorem 2.1.

To that end, let f be a binary quadratic form of discriminant D, Γ in the automorphism group U_f and (x, y) a representation of n under f (i.e. $f(x, y) = n$). Then $\Gamma \cdot (x, y) = (x', y')$ also has $f(x', y') = n$. Now we will perform some manipulations to obtain a new "reduced" form. With

$$\varepsilon_\Gamma = \frac{\Gamma_{11} + \Gamma_{22}}{2} + \frac{\Gamma_{21}}{2a}\sqrt{D}$$

we get

$$x' + \frac{b - \sqrt{D}}{2a} y' = \varepsilon_\Gamma \cdot \left(x + \frac{b - \sqrt{D}}{2a} y \right)$$

and using the substitutions

$$\theta = \frac{-b + \sqrt{D}}{2a}\,, \qquad \theta' = \frac{-b - \sqrt{D}}{2a}$$

so that

$$ax^2 + bxy + cy^2 = a(x - \theta y)(x - \theta' y)$$

and so that

$$x' - \theta y' = \varepsilon_\Gamma \cdot (x - \theta y) \ , \qquad x - \theta' y = \varepsilon_\Gamma \cdot (x' - \theta' y')$$

we finally get

$$\frac{x' - \theta' y'}{x' - \theta y'} = \frac{1}{\varepsilon_\Gamma^2} \cdot \frac{x - \theta' y}{x - \theta y} = \frac{1}{\varepsilon_0^{2k}} \cdot \frac{x - \theta' y}{x - \theta y}$$

since every ε_Γ is of the form $\pm\varepsilon_0^k$, for some k. From the proof of Theorem 5.1, we see that $U_f \cong \mathbb{Z} \times \mathbb{Z}/2\,\mathbb{Z}$ via the map

$$\Gamma \mapsto \varepsilon_\Gamma = \frac{\Gamma_{11} + \Gamma_{22}}{2} + \frac{\Gamma_{21}}{2a}\sqrt{D} = \pm\varepsilon_0^k$$

hence, for every k we can find a Γ such that $\varepsilon_\Gamma^2 = \varepsilon_0^{2k}$. Moreover, from the proof of Theorem 5.1, we see that $\varepsilon_0 > 1$, so by choosing Γ carefully from U_f we can force ε_Γ^{-2k} to be arbitrarily small. Moreover, we can dictate the sign of $(x' - \theta' y')/(x' - \theta y')$ by potentially multiplying Γ by -1. As such, we can choose a Γ with corresponding $\varepsilon_\Gamma = \varepsilon_0^{2k}$ such that the to (x, y) equivalent solution $(x', y') = \Gamma \cdot (x, y)$ satisfies

$$1 < \frac{x' - \theta' y'}{x' - \theta y'} = \frac{1}{\varepsilon_\Gamma^2} \cdot \frac{x - \theta' y}{x - \theta y} = \frac{1}{\varepsilon_0^{2k}} \cdot \frac{x - \theta' y}{x - \theta y} \leq \varepsilon_0^2$$

In fact, there can only be one such Γ (and as a consequence, only one equivalent solution (x', y')) for which $(x' - \theta' y')/(x' - \theta y')$ lies in the interval $(1, \varepsilon_0^2]$. For any other Γ', we would obtain a different $k' = k + l$ value for which $\varepsilon_{\Gamma'}^2 = \varepsilon_0^{2k'}$, which would push the quotient

$$\varepsilon_0^{-2l} < \frac{x'' - \theta'' y''}{x'' - \theta y'} = \frac{1}{\varepsilon_{\Gamma'}^2} \cdot \frac{x - \theta' y}{x - \theta y} = \frac{1}{\varepsilon_0^{2k'}} \cdot \frac{x - \theta' y}{x - \theta y} = \frac{1}{\varepsilon_0^{2(k+l)}} \cdot \frac{x - \theta' y}{x - \theta y} \leq \varepsilon_0^{2-2l}$$

of the equivalent solution $\Gamma' \cdot (x, y) = (x'', y'')$ out of the interval $(1, \varepsilon_0^2]$ into $(\varepsilon_0^{-2l}, \varepsilon_0^{2-2l}]$.

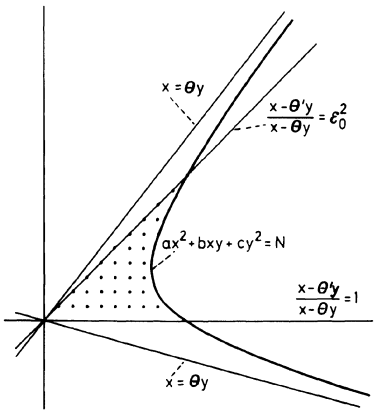
In conclusion, for every representation (x, y) of n under f we have found exactly one equivalent representation (x', y') of n under f that satisfies

$$1 < \frac{x' - \theta' y'}{x' - \theta y'} \leq \varepsilon_0^2$$

Hence

$$R(n, f) = \left| \left\{ (x, y) \in \mathbb{Z}^2 : ax^2 + bxy + cy^2 = n, x - \theta y > 0, 1 < \frac{x - \theta' y}{x - \theta y} \leq \varepsilon_0^2 \right\} \right|$$

Analogously to earlier, this is asymptotically the area inside a (tilted) parabola.



Which amounts to the area

$$\frac{\log(\varepsilon_0)}{\sqrt{D}}N$$

We conclude that

$$\lim_{N\to\infty}\left(\frac{1}{N}\sum_{n=1}^{N}R(n,f)\right)=\frac{\log(\varepsilon_0)}{\sqrt{D}}$$

□

Finally, we can demonstrate the class number theorem.

Theorem 6.6. *Let D be a discriminant, then*

$$h(D)=\begin{cases}\frac{w\sqrt{-D}}{2\pi}L(1,\chi_D) & \text{if} \quad D<0,\\ \frac{\sqrt{D}}{\log(\varepsilon_0)}L(1,\chi_D) & \text{if} \quad D>0,\end{cases}$$