Binary Quadratic Forms and the Class Number Formula

Robert Meier and Paul Seidel

May 29, 2019

1 Binary Quadratic Forms

This part of the talk follows the book *A primer of analytic number theory: from Pythagoras to Riemann by Stopple* [2] closely. We consider the *binary quadratic forms* in two variables

$$Q(x, y) = ax^2 + bxy + cy^2$$

of *discriminant* $b^2 - 4ac = d$. Here, a, b, c are integers. Additionally, we only consider the case $\gcd(a, b, c) = 1$. These forms are called *primitive*. A form Q *represents* an integer m if there are integers x_0 and y_0 such that $Q(x_0, y_0) = m$. We will write forms compactly as $Q = (a, b, c)$. These forms were already studied in the seventeenth and eighteenth centuries by Fermat and Euler among others. Later, Gauss put the theory of forms onto solid footing in his book *Disquisitiones Arithmeticae*. They investigated questions like:

- What integers can be represented by a given form?
- What forms can represent a given integer?
- Additionally, if the integer is representated by the form, how many representations exist and how do we find them?

In the mid-nineteenth century it became clear that studying binary quadratic forms is essentially the same as studying the class groups of quadratic fields. Here, we focus on the forms, as this allows us to derive a version of the class number formula in the scope of this talk. In the first part of the talk, we will derive some facts about the binary quadratic forms. In the second part, we prove the class number formula, which connects analytic and algebraic number theory.

Whether m is represented by $2x^2 + 3y^2$ is clearly the same question as asking whether $3x^2 + 2y^2$ represents m. In a similar fashion, though less obvious, it is also the same as considering the form $2x^2 + 4xy + 5y^2$. As $2x^2 + 4xy + 5y^2 =$

$2(x+y)^2+3y^2$, we just changed the variables (x,y) to $(x+y,y)$. This change of variables corresponds to the matrix

$$M = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

as $(x,y)M = (x+y,y)$. Gauss introduced an equivalence relation between forms to avoid this redundancy.

Definition 1.1. Two forms $Q = (a,b,c)$ and $Q' = (a',b',c')$ are equivalent, $Q \sim Q'$, if there is a matrix $M \in SL_2(\mathbb{Z})$ such that

$$Q'(x,y) = Q((x,y)M).$$

Since it is straight forward to show that this actually defines a proper equivalence relation, we omit that here. The point of this equivalence relation is that if $Q \sim Q'$ they represent the same integers.

We restrict ourselves to the case $d < 0$. As

$$4a(ax^2+bxy+cy^2) = (2ax+by)^2 + (4ac-b^2)y^2$$

we get that the right hand side is always positive. We additionally restrict ourselves to $a > 0$. This means we only talk about forms which take only positive values. We call them *positive definite*. The case $a < 0$ is closely connected. In that case, the forms take only negative values. With $M = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ we change (a,b,c) to $(c,-b,a)$ and thus we also have $c > 0$.

We can also write

$$Q(x,y) = (x,y)\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

and if $Q' \sim Q$ via M, then

$$Q'(x,y) = (x,y)M\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}M^T\begin{pmatrix} x \\ y \end{pmatrix}.$$

From this it easily follows that Q' has the same discriminant as Q.

A natural question to ask is how many equivalence classes there are?

Definition 1.2. We call the number of equivalence classes for discriminant $d < 0$ the class number $h(d)$.

Now we will prove that the class number is always finite.

Theorem 1.3. *For each $d < 0$, the class number $h(d)$ is finite. In fact, every form is equivalent to a form (a,b,c) with*

$$|b| \leq a \leq c.$$

Proof. Take any positive definite form with determinant d. If the inequality already holds, we are done. In the other case, we will show that we can find an equivalent form Q' with $a' + c' < a + c$. We iterate this procedure. As the first an last coefficients are positive and there are only finitely many positive integers smaller than $a + c$, the process will stop at some point and we are done.

Let $\sigma(b)$ be the sign of b. We iterate the following until the inequalities are satisfied:

- If $a < |b|$, the matrix

$$\begin{bmatrix} 1 & 0 \\ -\sigma(b) & 1 \end{bmatrix} \qquad \text{changes } (x, y) \text{ to } (x - \sigma(b)y, y).$$

  We get the form

$$ax^2 + (b - 2\sigma(b)a)xy + (a + c - |b|)y^2.$$

  As $a < |b|$ we get that

$$a' + c' = 2a + c - |b| < a + c.$$

  We managed to decrease the sum.

- If $a \geq |b|$ and $c < a$, we change the form to $(c, -b, a)$ with the matrix $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. After this step we either have $a < |b|$ or we are done.

We proved that each form is equivalent to a form with $|b| \leq a \leq c$. Now we prove that for each d there are only finitely many forms with this property. We have

$$3a^2 = 4a^2 - a^2 \leq 4ac - b^2 = -d = |d|.$$

Thus $|b| \leq a \leq \sqrt{|d|/3}$. Therefore there are only finitely many possible choices for a and b. As $b^2 - 4ac = d$ choosing a and b also fixes c. This finishes the proof. □

With this theorem we get an upper bound on the class number. For fixed d, we can now search for all forms satisfying the inequalities. To actually get the exact class number, we need to answer another question: Are there forms which satisfy the inequalities that are equivalent to each other? The following Lemma will help us:

Lemma 1.4. *Suppose that the quadratic form $Q(x, y) = ax^2+bxy+cy^2$ satisfies $|b| \leq a \leq c$. Then, a is the minimum of Q; that is, for all $(x, y) \neq (0, 0)$,*

$$Q(x, y) \geq a$$

Furthermore, ac is the minimum of products of values of Q. In other words, if (x, y) and (u, v) do not lie on the same line through the origin, then

$$Q(x, y)Q(u, v) \geq ac$$

Proof. Clearly, $Q(1,0) = a$, so Q represents a. Similarily $Q(1,0)Q(0,1) = ac$. In fact, $Q(x,0) = ax^2 \geq a$ and $Q(0,y) = cy^2 \geq y$. If both x and y are nonzero, we get

$$\begin{aligned} Q(x,y) &= ax^2 + bxy + cy^2 \\ &\geq ax^2 - |b||x||y| + cy^2 \\ &\geq ax^2 - |b||x||y| + cy^2 - a(x-y)^2 \\ &= (2a - |b|)|x||y| + (c-a)y^2 \\ &\geq (2a - |b|) + (c-a) = a + c - |b| \geq c \end{aligned}$$

This gives us that a is the minimum value. Additionally, if the point is not on the x-axis, the value is at least c. In the second part we look at points which are not collinear, which means at most one point is on the horizontal axis. Thus one of the values is at least c. The other value we can bound from below by a to get $Q(x,y)Q(u,v) \geq ac$. □

With this Lemma we are able to find out exactly which forms satisfying the inequalities are equivalent to each other.

Theorem 1.5. *Every form with discriminant d is equivalent to exactly one form satisfying the inequalities*

$$\{|b| \leq a \leq c\} \quad \textit{and} \quad \{b \geq 0 \textit{ if either } |b| = a \quad \textit{or} \quad a = c.\}$$

Remark 1.6. We call these forms *reduced*. The theorem says that each equivalence class contains exactly one reduced form.

Proof. First we show that we still can find a representative of each class. If $a = c$ and $b < 0$, we can use $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ to get $(a,b,c) \sim (c,-b,a)$. The second form has $b \geq 0$ and also satisfies the inequalities. In the second case, if $|b| = a$ and $b < 0$, we use $\begin{bmatrix} 1 & 0 \\ -\sigma(b) & 1 \end{bmatrix}$ to get

$$(a,b,c) \sim (a, b - 2\sigma(b)a, a + c - |b|) = (a,-b,c).$$

Now we only look at the set of forms satisfying all inequalities of the theorem statement. We want to show that we do not have two forms in the same class anymore. We look at $Q = (a,b,c) \sim Q' = (a',b',c')$ where both Q and Q' satisfy the inequalities and show that their coefficients are the same. As they are equivalent, they represent the same integers. Thus they have the same minimum. Together with the previous Lemma 1.4 we get $a = a'$. Similarily, the second part of the Lemma 1.4 gives us $c' = c$. As they have the same discriminant, we also get that $b' = \pm b$. If $b' = b$ we are done. So assume the contrary. Without loss of generality $b < 0$. As Q satisfies the inequalities in the theorem, we have both $|b| \neq a$ and $a \neq c$, i.e.

$$0 < |b| < a < c.$$

As one can see in the proof of the Lemma 1.4, we actually have

$$Q(x, y) > c > a$$

if both variables are nonzero. Equivalence allows us to find a change of variables, i.e.

$$Q'(x, y) = Q(rx + ty, sx + uy).$$

Then $a = Q'(1, 0) = Q(r, s)$. Because of the strict version of the Lemma, we get that (r, s) is on the x-axis and $r = \pm 1$. Similarily, $c = Q'(0, 1) = Q(t, u)$, gives us $t = 0$ and $u = \pm 1$. As the determinant of the change of variables matrix is 1, r and u have the same sign. Thus the matrix of the change is either I or $-I$. But as these change of variables result in the same form, we get $b' = b$. This finishes the proof. □

This theorem gives us an algorithmic procedure to find out the class number. We have bounds on a and b, so we can just try out all possibilities to find all forms satisfying the inequalities of the last theorem. We could actually be more efficient, for example b has to have the same parity as d, as $b^2 - d = 4ac$. We actually also see that if d is not 0 or 1 mod 4, there are no forms of discriminant d. This is as b^2 is either 0 or 1 mod 4 and $d \equiv b^2$ mod 4. There are other conditions on the coefficients which would make this even faster, but the main point is that we are able to calculate the class number.

Example 1.7. *We illustrate this with $d = -35$. As $\sqrt{|d|/3} = 3.415...$, we know that $1 \leq a \leq 3$ and $-3 \leq b \leq 3$. As d is odd, so is b, we have $b \in \{-3, -1, 1, 3\}$. First, if $b = \pm 1$, we have $c = (b^2 - d)/4a = 9/a$. As c is an integer, we get $a = 1$ or 3. We get the forms $\{1, \pm 1, 9\}$ and $\{3, \pm 1, 3\}$. In both cases the two forms with $b = -1$ are not reduced. If $b = \pm 3$, we also need $a = 3$ as $a \geq |b|$. But then $c = 44/12$ is not an integer. Hence the class number $h(-35) = 2$.*

We now turn our attention to the question: Which integers are represented?

Definition 1.8. A form Q represents an integer n **properly** if there are two relatively prime integers r and s such that $Q(r, s) = n$.

Restricting our attention to proper representation will be useful. If Q represents n properly, it represents all integers of the form $m^2 n$. We can just multiply both variables with m to get a representaion of $m^2 n$. The point of equivalence is that equivalent forms represent the same integers. The following Theorem allows us to say something in the other direction.

Theorem 1.9. *If a form Q properly represents an integer n, Q is equivalent to a form (n, m, l).*

Proof. Assume r and s are relatively prime and $Q(r, s) = n$. Bézout's Identity gives us $-t$ and u such that $ru - ts = 1$, i.e.

$$M = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL_2(\mathbb{Z}).$$

With $Q'(x,y) = Q((x,y)M)$ we get

$$Q'(1,0) = Q((1,0)M) = Q(r,s) = n.$$

Thus $a' = n$ and we are done. □

Remark 1.10. This does not imply that different forms which properly represent the same integer are always equivalent, as m and l can be different.

The next theorem we will only state and not prove:

Theorem 1.11. *A form Q of discriminant d properly represents an integer n if and only if Q is equivalent to a form (n,m,l) where*

$$m^2 \equiv d \mod 4n \qquad \textit{and} \qquad 0 \leq m < 2n.$$

The proof can be found in [2] on the pages $304-5$.The main ideas are that as $m^2 - 4nl = d$ we get that $m^2 \equiv d \mod 4n$ is needed and the bound on m holds because we can use change of variables to make m smaller similar as we did earlier. The next question we are asking ourselves is, how many different proper representations of an integer does a form have? Suppose two pairs (r,s) and (r',s') give us the same form in the theorem above, i.e. we have two matrices

$$M = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \qquad \textit{and} \qquad M' = \begin{bmatrix} r' & s' \\ t' & u' \end{bmatrix},$$

such that

$$Q((x,y)M) = nx^2 + mxy + ly^2 = Q'((x,y)M').$$

This also gives us $Q(x,y) = Q((x,y)M'M^{-1})$. The matrix $M'M^{-1}$ is called an *automorphism* of Q. These automorphisms form a subgroup of $SL_2(\mathbb{Z})$. We have the following theorem, whose proof we also omit, it is mostly tedious algebraic computations.

Theorem 1.12. *For a binary quadratic form $Q = (a,b,c)$ of discriminant d, the automorphisms N of Q are in one-to-one correspondence with solutions (t,u) of the Pell equation $t^2 - du^2 = 4$ via*

$$(t,u) \leftrightarrow N = \begin{bmatrix} \frac{t-bu}{2} & cu \\ cu & \frac{t+bu}{2} \end{bmatrix}.$$

For $d > 0$, there are infinitely many solutions. For $d = -3$ there are six solutions, for $d = -4$ four, and for $d < -4$ there are only two solutions.

Remark 1.13. For $d < -4$ we only have the trivial solutions $(\pm 2, 0)$ which correspond to the automorphisms I and $-I$. This means that if a proper representation (r,s) gives us a form (m,n,l), the only other proper representation giving us that form is $(-r,-s)$. From now on we restrict ourselves to $d < -4$.

Now we know that there are only finitely many proper representations of n by Q. Hence the following definition makes sense:

Definition 1.14. Let Q be a binary quadratic form with $d < -4$. The **representation number** of n by Q is

$$r_Q(n) = \frac{1}{2}\#\{(x, y) \text{ relatively prime with } Q(x, y) = n\}.$$

Additionally we define

$$r_d(n) = \sum_{\text{reduced forms } Q} r_Q(n).$$

We can't say too much about $r_Q(n)$ for a fixed Q, but we can say the following about $r_d(n)$ by combining the last two theorems:

Theorem 1.15. *For $d < -4$, $r_d(n)$ is the number of m which satisfy*

$$0 \leq m < 2n \qquad \text{and} \qquad m^2 \equiv d \mod 4n.$$

As a final remark in this section, we remind you of the first talk. We saw the identification of the upper half plane as the group of symmetric positive definite 2×2 square matrices with determinant 1. This gives us a binary quadratic form for each point. Namely each point corresponds to the quadratic form which has this point as a zero if we set $y = 1$. Then the modular group acts on the forms by translating these roots with the Möbius Transform. Here we only talked about forms with integer coefficients, but this is just a special case. It turns out that a form is reduced if and only if the corresponding root is in the fundamental domain. This means that finding the reduced form is the same as translating the root into the fundamental domain. This finishes the first part of the talk, after the break we will connect this to L-functions.

2 The Class Number Formula

In 1837 Dirichlet proved the following famous theorem on primes in arithmetic progressions.

Theorem 2.1. *Let a and b be positive integers. The sequence*

$$a, \quad a + b, \quad a + 2b, \quad a + 3b, \quad \ldots$$

contains infinitely many primes if and only if $\gcd(a, b) = 1$.

An important step of the proof consisted in showing that his *Dirichlet L-series* do not vanish at 1 (provided that they do not arise from a principal character). They are defined as follows.

Definition 2.2. Let k be a non-zero integer. A function $\chi : \mathbb{Z} \to \mathbb{C}$ is called a Dirichlet character modulo k if the following three properties hold:

1. For all $n \in \mathbb{N}$, $\chi(n + k) = \chi(n)$.

2. If $\gcd(n,k) > 1$, then $\chi(n) = 0$ and if $\gcd(n,k) = 1$, then $\chi(n) \neq 0$.

3. For all $m, n \in \mathbb{Z}$, $\chi(mn) = \chi(m)\chi(n)$.

If $\chi(n) = 1$ for all n with $\gcd(n,k) = 1$, then χ is called principal. Finally, if χ is a Dirichlet character, then the function

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

is called a Dirichlet L-series.

For example if we take $k = 1$ in this definition, then we obtain the principal character $\chi \equiv 1$ and the corresponding L-series is the Riemann zeta function. We already know that it has a simple pole at 1.

In 1839 Dirichlet found the exact value at 1 for certain types of L-series which are connected to binary quadratic forms. This result is known as the *class number formula*. Using methods from algebraic number theory, it has since been generalized to a relation between the residue at 1 of the Dedekind zeta function of some number field K and algebraic data of K. The proof we will give today corresponds to the case where K is an imaginary quadratic number field. If you want to learn more about this topic, a good reference is for example [1].

The definitions imply that if χ is a Dirichlet character modulo k, then χ can also be viewed as a group homomorphism $(\mathbb{Z}/k\mathbb{Z})^\star \to \mathbb{C}^\star$. From a representation theoretic viewpoint, this means that χ is a character of the group $(\mathbb{Z}/k\mathbb{Z})^\star$. If we let $\varphi(k) = |(\mathbb{Z}/k\mathbb{Z})^\star|$ denote the Euler totient function, then for all n with $\gcd(n,k) = 1$ we have

$$\chi(n)^{\varphi(k)} = \chi(n^{\varphi(k)}) = \chi(1) = 1.$$

This implies that all non-zero values of χ lie on the unit circle. Combining the fact that $|\chi| \leq 1$ with the multiplicativity of χ, one can prove, in exactly the same manner as for the Riemann zeta function, that $L(s,\chi)$ is an analytic function for $\Re(s) > 1$ and that it has the Euler product

$$L(s,\chi) = \prod_p \frac{1}{1 - \chi(p)p^{-s}}.$$

A proof for the case of the Riemann zeta function can be found in chapter VII of [1].

We are only interested in a particular Dirichlet character, whose definition requires the Kronecker symbol, which is a generalization of the Legendre symbol.

Definition 2.3. Let p be an odd prime and a an integer. Then a is called a quadratic residue modulo p if a has a square root in $\mathbb{Z}/p\mathbb{Z}$, that is the equation $x^2 = a$ has a solution $x \in \mathbb{Z}/p\mathbb{Z}$. The Legendre symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \text{if } a \text{ is not a quadratic residue modulo } p, \\ 0, & \text{if } p \mid a, \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p. \end{cases}$$

Now we define the Jacobi symbol, which allows for an odd natural number n in place of the odd prime p. If we have the prime factorization $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Lastly, we extend the definition to even natural numbers, which yields the Kronecker symbol. For this we define the case $n = 2$ first.

$$\left(\frac{a}{2}\right) = \begin{cases} -1, & \text{if } a \equiv 3, 5 \pmod 8, \\ 0, & \text{if } 2 \mid a, \\ 1, & \text{if } a \equiv 1, 7 \pmod 8. \end{cases}$$

Then if $n = 2^\alpha m$ with m odd, let

$$\left(\frac{a}{n}\right) = \left(\frac{a}{2}\right)^\alpha \left(\frac{a}{m}\right).$$

Before we define the Dirichlet character of interest, we restrict the discriminants which we look at to *fundamental discriminants* in order to make the results to come a bit simpler to write down.

Definition 2.4. A discriminant d of a binary quadratic form is called a fundamental discriminant if either of the following holds:

- $d \equiv 0 \pmod 4$, $d/4$ is square free and $d/4 \equiv 2, 3 \pmod 4$.
- $d \equiv 1 \pmod 4$ and d is square free.

Definition 2.5. Let $d < 0$ be a fundamental discriminant. We use the Kronecker symbol to define the Dirichlet character χ_d by

$$\chi_d(n) = \left(\frac{d}{n}\right).$$

It is not obvious that χ_d actually defines a Dirichlet character. While the third property in Definition 2.2 is clear from the definition of the Kronecker symbol, it is not obvious whether a k as in the first property exists. For the Legendre symbol, one clearly has

$$\left(\frac{a}{p}\right) = \left(\frac{a+p}{p}\right).$$

This holds analogously for the Jacobi symbol, and for the Kronecker symbol we can use

$$\left(\frac{a}{2}\right) = \left(\frac{a+8}{2}\right)$$

to obtain

$$\left(\frac{a}{n}\right) = \left(\frac{a+8n}{n}\right)$$

in general. This suggests that the period of χ_d is a multiple of $|d|$. However, the definition of $\chi_d(n)$ uses n as the lower variable in the symbol, so we cannot use our observation immediately. The idea can be saved by using a version of the celebrated quadratic reciprocity theorem for the Kronecker symbol, which relates

$$\left(\frac{d}{n}\right) \quad \text{and} \quad \left(\frac{n}{|d|}\right)$$

in a controlled manner. Going through the computations, one obtains that if d is a fundamental discriminant, then χ_d is a Dirichlet character modulo $|d|$.

Now we have defined the main object of interest of this part of the talk, the Dirichlet L-series

$$L(s, \chi_d) = \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s}.$$

The goal for the remainder of this talk will be to prove the class number formula.

Theorem 2.6 (The class number formula)**.** *Let $d < -4$ be a fundamental discriminant and let h denote its class number. Then*

$$L(1, \chi_d) = \frac{\pi h}{\sqrt{|d|}}.$$

The left side will only make sense once we have shown that $L(s, \chi_d)$ is well defined at $s = 1$. For the proof of the class number formula we need to relate binary quadratic forms to χ_d, which is the content of the following result.

Theorem 2.7. *Let $d < 0$ be a fundamental discriminant. Then*

$$r_d(n) = \begin{cases} 0, & \text{if } p^2 \mid n \text{ for some prime factor } p \text{ of } d, \\ \prod\limits_{p \mid n,\ p \nmid d} (1 + \chi_d(p)), & \text{otherwise,} \end{cases}$$

where each p is a prime factor of n.

Proof. We only prove some special cases and not the full theorem.

Consider first the case where the square of a prime factor p of d divides n. We show that $r_d(n) = 0$ using Theorem 1.15. If p is odd and $m^2 \equiv d \pmod{4n}$, then $m^2 \equiv d \pmod{p^2}$. Since p divides d, it also divides m^2 and thus $p^2 \mid m^2$. But then $d \equiv m^2 \equiv 0 \pmod{p^2}$ which contradicts the fact that d is a fundamental discriminant, because fundamental discriminants are not divisible by an odd prime squared. In the case $p = 2$ we must have $4 \mid d$ and $d/4 \equiv 2, 3 \pmod 4$. One can check that then $d \equiv 8, 12 \pmod{16}$. If $m^2 \equiv d \pmod{16}$ we immediately obtain a contradiction, because 8 and 12 are not quadratic residues modulo 16.

In the case that there is a prime factor p of n with $(\frac{d}{p}) = -1$ we also want to show $r_d(n) = 0$. If the equation $m^2 \equiv d \pmod{4n}$ has a solution m, then d is a quadratic residue modulo p, contradiction.

In the remaining cases we have $(\frac{n}{p}) = 1$ for all primes p which divide n but not d. If we let k denote the number of such primes, we want to show that $r_d(n) = 2^k$. We prove the case where n is odd and $d \equiv 0 \pmod 4$. According to Theorem 1.15, we must count the number of solutions m, with $0 \leq m < 2n$, of the equation

$$m^2 \equiv d \pmod{4n}.$$

Since d is a multiple of 4, so is m^2, and there are integers $\widetilde{d}, \widetilde{m}$ with $4\widetilde{d} = d$ and $2\widetilde{m} = m$. This transforms the counting problem into finding solutions to

$$\widetilde{m}^2 \equiv \widetilde{d} \pmod{n}$$

with $0 \leq \widetilde{m} < n$. Now let q be a prime divisor of both n and d, which also implies $q^2 \nmid n$ by our case distinction. The congruence $\widetilde{m}^2 \equiv \widetilde{d} \pmod q$ has the unique solution $\widetilde{m} \equiv 0 \pmod q$. If p is a (necessarily odd) prime divisor of n with $(\frac{d}{p}) = 1$, then $\widetilde{m}^2 \equiv \widetilde{d} \pmod p$ has at least one solution $\widetilde{m}$. Furthermore, $-\widetilde{m} \not\equiv \widetilde{m} \pmod p$ is another solution, so we get exactly two solutions modulo p. If the prime factorization of n is $q_1 \cdots q_l p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, we can apply Hensel's Lemma to conclude that the congruences

$$\widetilde{m}^2 \equiv \widetilde{d} \pmod{p_i^{\alpha_i}}$$

have exactly two solutions each. We record the statement of the special case of Hensel's Lemma which we need here for convenience. See also [2] chapter 14.

Theorem 2.8 (Hensel's Lemma)**.** *Suppose p is an odd prime, a is not divisible by p and $\alpha \geq 1$. If there is a solution x to the congruence*

$$x^2 \equiv a \pmod{p^\alpha},$$

then there is a unique solution $\widetilde{x}$ to the congruence

$$\widetilde{x}^2 \equiv a \pmod{p^{\alpha+1}}$$

satisfying $\widetilde{x} \equiv x \pmod{p^\alpha}$.

Finally, we can apply the Chinese Remainder Theorem to conclude that there are precisely 2^k solutions to the congruence $\widetilde{m}^2 \equiv \widetilde{d} \pmod n$. □

For the proof of the class number formula we will also need the following function, which connects the class number to the L-series which we defined earlier.

Definition 2.9. Given a binary quadratic form Q, the Epstein Zeta function is defined for all $\Re(s) > 1$ by

$$\zeta(s, Q) = \frac{1}{2} \sum_{(x,y) \neq (0,0)} Q(x, y)^{-s}.$$

Note that since equivalent binary quadratic forms represent a given integer equally often, the Epstein Zeta function is independent of the choice of Q within its equivalence class. We can use the following trick to rewrite $\zeta(s, Q)$ as a sum over pairs of relatively prime integers: If x, y are integers we can write $(x, y) = m(u, v)$ where $m = \gcd(x, y)$ and $\gcd(u, v) = 1$. Then

$$Q(x, y) = Q(m(u, v)) = m^2 Q(u, v)$$

and consequently

$$\zeta(s, Q) = \frac{1}{2} \sum_{m=1}^{\infty} \sum_{\gcd(u,v)=1} m^{-2s} Q(u, v)^{-s} = \zeta(2s) \sum_{n=1}^{\infty} r_Q(n) n^{-s}.$$

The last equality follows directly from the definition of r_Q in the case that $d < -4$. Finally we obtain another function by summing over all equivalence classes:

$$\zeta(s, d) = \sum_{\text{classes } [Q]} \zeta(s, Q) = \zeta(2s) \sum_{n=1}^{\infty} r_d(n) n^{-s}. \tag{1}$$

Now we prove a lemma which establishes the connection between binary quadratic forms and our L-series.

Lemma 2.10. *Let $d < 0$ be a fundamental discriminant. Then*

$$\sum_{n=1}^{\infty} r_d(n) n^{-s} = \prod_p \frac{1 + p^{-s}}{1 - \chi_d(p) p^{-s}} = \zeta(2s)^{-1} L(s, \chi_d) \zeta(s).$$

Proof. We begin with the first equality. We claim that for a single factor of the Euler product we get

$$\frac{1 + p^{-s}}{1 - \chi_d(p) p^{-s}} = \begin{cases} 1, & \text{if } \chi_d(p) = -1, \\ 1 + p^{-s}, & \text{if } \chi_d(p) = 0, \\ 1 + 2 \sum_{k=1}^{\infty} p^{-ks}, & \text{if } \chi_d(p) = 1. \end{cases}$$

If $\chi_d(p) = 0$ or -1, this is clear. If $\chi_d(p) = 1$, we expand the geometric series:

$$\frac{1 + p^{-s}}{1 - p^{-s}} = (1 + p^{-s}) \sum_{k=0}^{\infty} p^{-ks} = 1 + \sum_{k=1}^{\infty} (1 + 1) p^{-ks}.$$

Now we multiply all these factors and analyse how often some given n^{-s} will appear in the product, depending on the prime factorisation of n. By comparing this with Theorem 2.7, we will obtain the desired result. So let $p_1, \ldots, p_k$ be the prime factors of n.
Case 1: There is some p_i with $p_i^2 \mid n$ and $p_i \mid d$. Then $\chi_d(p_i) = 0$. In the product, there will be no instance of p_i^{-2s} and so n^{-s} cannot be obtained by multiplying the factors together. Thus the coefficient of n^{-s} is 0, which agrees

with Theorem 2.7.
Case 2: There is some p_i with $\chi_d(p_i) = -1$. Then p_i^{-s} will not appear in the product and so the coefficient of n^{-s} is 0, which again agrees with Theorem 2.7.
Case 3: In the remaining cases we have $\chi_d(p_i) \neq -1$ and $p_i^2 \nmid n$ for all prime factors p_i. This means that we get at least one n^{-s} after multiplying out the product. Now consider a fixed p_i. If $p_i \nmid d$, then $\chi_d(p_i) = 1$ and in the Euler product we see that the coefficient of n^{-s} is multiplied by 2. The same thing happens in the product from Theorem 2.7. If $p_i \mid d$, then $\chi_d(p_i) = 0$ and the factor $(1 + p_i^{-s})$ in the Euler product will multiply the coefficient of n^{-s} by 1, exactly as in Theorem 2.7. Thus the first equality is proven.

The second equality follows immediately from the Euler products for $L(s, \chi_d)$ and the Riemann zeta function:

$$\begin{aligned}\zeta(2s)^{-1}L(s,\chi_d)\zeta(s) &= \prod_p (1-p^{-2s}) \prod_p \frac{1}{1-\chi_d(p)p^{-s}} \prod_p \frac{1}{1-p^{-s}} \\ &= \prod_p \frac{(1-p^{-s})(1+p^{-s})}{(1-\chi_d(p)p^{-s})(1-p^{-s})} \\ &= \prod_p \frac{1+p^{-s}}{1-\chi_d(p)p^{-s}}.\end{aligned}$$

□

Together with (1) we immediately obtain the following.

Corollary 2.11.

$$\zeta(s,d) = L(s,\chi_d)\zeta(s).$$

We still pursue our goal of finding out more about $L(1, \chi_d)$, so we want to investigate the above equation at $s = 1$. We have already seen that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1, but we do not know much about $\zeta(s, d)$ and $L(s, \chi_d)$ yet. For this we consider $\zeta(s, Q)$ with a particular binary quadratic form Q and relate it to the non-holomorphic Eisenstein series

$$E(s,z) = \frac{1}{2}\pi^{-s}\Gamma(s) \sum_{(m,n)\neq(0,0)} \frac{\Im(z)^s}{|mz+n|^{2s}}$$

from the last talk. Then we can just use the properties of E which were proven by the last group.

Propostion 2.12. *Let $Q(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form with discriminant $d < 0$ and let*

$$z_Q = \frac{-b+\sqrt{d}}{2a} \in \mathbb{H}$$

denote one of the complex roots of the polynomial $Q(x, 1)$. Then

$$\zeta(s,Q) = \left(\frac{|d|}{4}\right)^{-\frac{s}{2}} \frac{\pi^s}{\Gamma(s)} E(s, z_Q).$$

Proof. Straightforward computations show

$$\Im(z_Q) = \frac{1}{a}\left(\frac{|d|}{4}\right)^{\frac{1}{2}}$$

and

$$\begin{aligned} a|mz_Q + n|^2 &= a\left(\left(n - \frac{bm}{2a}\right)^2 + \left(\frac{m\sqrt{|d|}}{2a}\right)^2\right) \\ &= a\left(n^2 - \frac{bmn}{a} + \frac{b^2m^2}{4a^2} + \frac{m^2(4ac - b^2)}{4a^2}\right) \\ &= an^2 - bmn + cm^2 \\ &= Q(m, -n). \end{aligned}$$

Thus

$$\begin{aligned} \left(\frac{|d|}{4}\right)^{-\frac{s}{2}} \frac{\pi^s}{\Gamma(s)} E(z_Q, s) &= \frac{1}{2}\left(\frac{|d|}{4}\right)^{-\frac{s}{2}} \sum_{(m,n)\neq(0,0)} \frac{\Im(z_Q)^s}{|mz_Q + n|^{2s}} \\ &= \frac{1}{2} \sum_{(m,n)\neq(0,0)} \frac{1}{a^s|mz_Q + n|^{2s}} \\ &= \frac{1}{2} \sum_{(m,n)\neq(0,0)} \frac{1}{Q(m,-n)^s} \\ &= \zeta(s, Q). \end{aligned}$$

□

From the last talk we know that the non-holomorphic Eisenstein series can be extended to a holomorphic function on $\mathbb{C}$ except for simple poles at $s = 0$ and $s = 1$. Since $s \mapsto (|d|/4)^{-s/2}\pi^s\Gamma(s)^{-1}$ is holomorphic everywhere, has a zero at $s = 0$ and is non-zero at $s = 1$, we conclude that $\zeta(s, Q)$ is holomorphic except for a simple pole at $s = 1$. Furthermore, the residue of $E(s, z)$ at $s = 1$ is independent of z and equal to $1/2$, so $\zeta(s, Q)$ has residue $\pi/\sqrt{|d|}$ at $s = 1$. Since this is independent of the choice of equivalence class of the quadratic form Q, we can sum the $\zeta(s, Q)$ over the equivalence classes to conclude that $\zeta(s, d)$ also has a simple pole at $s = 1$. If we let h denote the class number of d, the corresponding residue is

$$\frac{\pi h}{\sqrt{|d|}}.$$

Recall that the Riemann zeta function has a simple pole of residue 1 at $s = 1$. The equation $\zeta(s, d) = L(s, \chi_d)\zeta(s)$ then implies that $L(1, \chi_d)$ is defined and not equal to 0. In that case we obtain

$$L(1, \chi_d) = \operatorname*{Res}_{s=1} L(s, \chi_d)\zeta(s) = \operatorname*{Res}_{s=1} \zeta(s, d) = \frac{\pi h}{\sqrt{|d|}}.$$

References

[1] Juergen Neukirch. *Algebraic Number Theory.* Springer, 1999.

[2] Jeffrey Stopple. *A primer of analytic number theory: from Pythagoras to Riemann.* Cambridge University Press, 2003.