LMS Undergraduate Summer School
Binary quadratic forms

Alex Bartel

25–26 August 2022

1 Introduction: sums of two squares

Which prime numbers p can be expressed in the form $p = x^2 + y^2$ for x, $y \in \mathbb{Z}$? Try it yourself before reading further: we have $2 = 1^2 + 1^2$, 3 cannot be written this way, we have $5 = 1^2 + 2^2$, ... Check all primes up to, say, $p = 61$. Can you see a pattern?

The following theorem was first proved by Fermat.

Theorem 1.1. *Let p be a prime number. Then there exist x, $y \in \mathbb{Z}$ such that $p = x^2 + y^2$ if and only if $p \equiv 1$ or $2 \pmod 4$.*

One of the directions is easy: every square is either 0 or $1 \pmod 4$, so the only possible values for the sum of two squares are 0, 1, and $2 \pmod 4$. Of these, $0 \pmod 4$ can never be a prime number, so one direction of the above equivalence follows. It is the other direction that is the real content of the theorem, namely that for every prime number that satisfies the "obvious" necessary condition, there really exist suitable x and y.

Over the centuries, many different proofs of this result have been discovered. The following "one-sentence-proof", which we present in an expanded version, is due to Zagier, building on ideas of Heath-Brown who, in turn, credits Liouville with some of the ideas. None of the ideas in this proof will be used in the rest of the course, we only show it as what chess players call a study, a little gem of mathematical magic.

Proof. Let $p = 4k + 1$ be a prime number, where $k \in \mathbb{Z}_{>0}$. Consider the set $S = \{(x, y, z) \in \mathbb{Z}^3_{\geq 0} : x^2 + 4yz = p\}$. Then we can define two *involutions* on S, meaning maps $\iota \colon S \to S$ such that $\iota \circ \iota = \mathrm{id}$. The first one stares one in the face:

$$\iota_1 \colon (x, y, z) \mapsto (x, z, y).$$

The second one, umm ..., not exactly:

$$\iota_2 \colon (x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z, \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y, \\ (x - 2y, x - y + z, y) & \text{if } x > 2y. \end{cases}$$

The involution ι_2 has exactly one fixed point, namely $(x, y, z) = (1, 1, k)$, so $\#S$ must be odd, hence ι_1 must also have at least one fixed point, (x, y, y). But $(x, y, y) \in S$ means that we have $x^2 + (2y)^2 = p$, as required. □

More generally, one can completely determine which natural numbers are sums of two squares.

Theorem 1.2. *Let $n = \prod_p p^{e_p} \in \mathbb{Z}_{\geq 1}$, where the product runs over distinct prime numbers, and $e_p \in \mathbb{Z}_{\geq 0}$ for all p. Then there exist x, $y \in \mathbb{Z}$ with $n = x^2 + y^2$ if and only if for all $p \equiv 3 \pmod 4$ the exponent e_p is even.*

Proof. This will eventually follow from the theory we will develop, but for now you can think about the "if" direction. Hint: for all x, y, z, $w \in \mathbb{Z}$ one has $(x^2 + y^2)(z^2 + w^2) = (xz - yw)^2 + (xw + yz)^2$. □

Lagrange obtained several variants of Fermat's result.

Theorem 1.3 (Lagrange)**.** *Let p be a prime number. Then*

- *there exist x, $y \in \mathbb{Z}$ such that $p = x^2 + 2y^2$ if and only if either $p = 2$ or $p \equiv 1$ or $3 \pmod 8$,*
- *there exist x, $y \in \mathbb{Z}$ such that $p = x^2 + 3y^2$ if and only if either $p = 3$ or $p \equiv 1 \pmod 3$,*
- *there exist x, $y \in \mathbb{Z}$ such that $p = x^2 + 5y^2$ if and only if either $p = 5$ or $p \equiv 1$ or $9 \pmod{20}$,*
- *there exist x, $y \in \mathbb{Z}$ such that $2p = x^2 + 5y^2$ if and only if $p \equiv 3$ or $7 \pmod{20}$.*

2 Binary quadratic forms

Definition 2.1. A *binary quadratic form (over $\mathbb{Z}$)* is a polynomial in x, y of the form $ax^2 + bxy + cy^2$ for some a, b, $c \in \mathbb{Z}$. We will often abbreviate this to (a, b, c).

Definition 2.2. Let (a, b, c) be a binary quadratic form and let $n \in \mathbb{Z}$. We say that (a, b, c) *represents* n (*properly*) if there exist x, $y \in \mathbb{Z}$ satisfying $ax^2 + bxy + cy^2 = n$ (and $\gcd(x, y) = 1$).

Question 2.3. Given a binary quadratic form, what is the set of integers that it represents (properly)?

Definition 2.4. A binary quadratic form (a, b, c) is called *primitive* if it satisfies $\gcd(a, b, c) = 1$.

Notice that Question 2.3 can always be reduced to primitive binary quadratic forms. From now on, we will tacitly assume all our forms to be primitive.

Observe that, for example, $2x^2 + 7y^2$ and $7x^2 + 2y^2$ clearly represent the same integers. Less clearly, the form $2x^2 + 4xy + 9y^2$ also represents the same integers as the other two. Indeed, $(2, 4, 9)$ can be obtained from $(2, 0, 7)$ via the substitution $x = X + Y$, $y = Y$, with inverse $X = x - y$, $Y = y$. As x, y run through all integers, so do X, Y, and one has $2x^2+7y^2 = 2X^2 + 4XY + 9Y^2$.

How does this generalise? Consider an affine change of variable $X = rx + sy$, $Y = tx + uy$. We want to choose r, s, t, u such that as x, y run through all integers, so do X, Y, and conversely. Note: if $(x, y) = (1, 0)$, then $(X, Y) = (r, t)$; and if $(x, y) = (0, 1)$, then $(X, Y) = (s, u)$. Thus, we certainly need r, s, t, $u \in \mathbb{Z}$. Conversely, this is sufficient to ensure that $(x, y) \in \mathbb{Z}^2 \Rightarrow (X, Y) \in \mathbb{Z}^2$. For the converse, solve for x, y: we get

$$\begin{aligned} x &= \frac{u}{ur - st}X - \frac{s}{ur - st}Y, \\ y &= \frac{-t}{ur - st}X + \frac{r}{ur - st}Y. \end{aligned}$$

By the same argument as before, we need $\frac{u}{ur-st}, \ldots \in \mathbb{Z}$. It is not hard to see that this forces $ur - st \in \{\pm 1\}$; and conversely, this additional requirement is sufficient to guarantee that $(x, y) \mapsto (X, Y)$ defines a bijection between $\mathbb{Z}^2$ and $\mathbb{Z}^2$.

Here is a better, more conceptual, explanation: the above conditions are equivalent to the condition that $\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, i.e. that $r, s, t, u \in \mathbb{Z}$ and $\det \left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right) \in \{\pm 1\}$. This makes sense, since performing a change of coordinates as above corresponding to $\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right)$, and then another one corresponding to $\left(\begin{smallmatrix} r' & t' \\ s' & u' \end{smallmatrix}\right)$, then this corresponds to a change of coordinates by

$$\begin{pmatrix} rr' + ts' & rt' + tu' \\ \cdots & \cdots \end{pmatrix} = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \cdot \begin{pmatrix} r' & t' \\ s' & u' \end{pmatrix}.$$

Therefore, such a change of variables can be reversed if and only if the corresponding matrix is invertible.

Summary. The group $\mathrm{GL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms via

$$\begin{pmatrix} r & t \\ s & u \end{pmatrix} \cdot f(x, y) = f\left((x, y) \cdot \left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right)\right).$$

The set of integers that a binary quadratic form represents (properly) depends merely on the orbit of the form under this action, not really on the form itself.

It will turn out to be more convenient to restrict to matrices with determinant 1. In particular, we will not allow the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, which would

swap x and y, and transform $ax^2 + cy^2$ to $cx^2 + ay^2$. We can still transform $(a, 0, c)$ to $(c, 0, a)$ by using the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, which generally transforms (a, b, c) to $(c, -b, a)$.

Definition 2.5. We define two binary quadratic forms f and g to be equivalent, and write $f \sim g$, if there exists $\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $g(x, y) = f\left((x, y) \cdot \left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right)\right)$.

The set of integers that a form represents (properly) only depends on the equivalence class of a form. For example by Fermat's theorem, a prime number p can be written as $p = 10x^2 + 14xy + 5y^2$ if and only if $p \equiv 1$ or $2 \pmod 4$. Indeed, we have $10x^2 + 14xy + 5y^2 = (3x + 2y)^2 + (x + y)^2$, or in the notation above, $(10, 14, 5) = \left(\begin{smallmatrix} 3 & 1 \\ 2 & 1 \end{smallmatrix}\right) \cdot (1, 0, 1)$, so that we have $(10, 14, 5) \sim (1, 0, 1)$.

Question 2.6. How do we (quickly) tell whether or not two given forms are equivalent?

Definition 2.7. The *discriminant* of (a, b, c) is defined by $\Delta(a, b, c) = b^2 - 4ac$.

Proposition 2.8. *Suppose that we have $(a, b, c) \sim (a', b', c')$. Then we have $b^2 - 4ac = b'^2 - 4a'c'$.*

Proof. The proof is a direct calculation: write $f = (a, b, c)$, and let $\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then we have

$$\begin{aligned} &f\left((x, y) \cdot \left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right)\right) \\ &\quad = a(rx + sy)^2 + b(rx + sy)(tx + uy) + c(tx + uy)^2 \\ &\quad = (ar^2 + brt + ct^2)x^2 + \cdots, \end{aligned} \tag{2.1}$$

so if the matrix $\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right)$ takes (a, b, c) to (a', b', c'), then we have $a' = ar^2 + brt + ct^2$, etc. Expressing b' and c' this way, substituting into the formula for the discriminant, and simplifying gives the result. □

Example 2.9. If $b \neq \pm b'$, then $(a, b, c) \not\sim (a, b', c)$, since then $b^2 - 4ac \neq b'^2 - 4a'c'$.

But caution: the implication goes in only one direction, in other words, there exist non-equivalent forms with the same discriminant. For example let $f_1 = 2x^2 + 3y^2$, $f_2 = x^2 - 2xy + 7y^2$. The discriminants of both forms are $-4 \cdot 2 \cdot 3 = -24 = 2^2 - 4 \cdot 7$, but we claim that the two forms are not equivalent. Indeed, f_2 represents 1 (take $x = 1$, $y = 0$), but it is easy to see that f_1 does not represent 1, since if $x \neq 0$ or $y \neq 0$, then $f_1(x, y) > 1$.

The sign of the discriminant tightly controls the behaviour of the binary quadratic form: given $f = ax^2 + bxy + cy^2$, multiply by $4a$ and complete the square to obtain

$$4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 - (b^2 - 4ac)y^2.$$

Case 0: $b^2 - 4ac = 0$**.** Then $4a \cdot f$ is the square of a linear form – not interesting.
Case 1: $b^2 - 4ac < 0$**.** Then for all $x, y \in \mathbb{Z}$ we have $4a \cdot f(x, y) \geq 0$. If $a > 0$, then for all $x, y \in \mathbb{Z}$ we have $f(x, y) \geq 0$, and we call such an f *positive definite*. If $a < 0$, then for all $x, y \in \mathbb{Z}$ we have $f(x, y) \leq 0$, and we call such an f *negative definite*.
Case 2: $b^2 - 4ac > 0$**.** If $a = 0$, then $f = y(bx + cy)$ is a product of two distinct linear forms, also not as interesting. If, on the other hand, $a \neq 0$, then $4a \cdot f$, and hence also f, represent both positive and negative integers. We call such an f *indefinite*.

In this course we will eventually focus on positive definite forms, but first we prove some results that are valid for all binary quadratic forms.

Proposition 2.10. *Let (a, b, c) be a binary quadratic form, and let $n \in \mathbb{Z}$. Then (a, b, c) properly represents n if and only if (a, b, c) is equivalent to a form (n, k, l) for some k, $l \in \mathbb{Z}$.*

Proof. One direction is easy: if (a, b, c) is equivalent to a form (n, k, l) for some k, $l \in \mathbb{Z}$, then these two forms properly represent the same integers; and the latter represents n by setting $x = 1$, $y = 0$.

Let us prove the converse: suppose that there exist r, $t \in \mathbb{Z}$ such that $n = ar^2 + brt + ct^2$ and such that $\gcd(r, t) = 1$. By Bézout's identity, there exist s, $u \in \mathbb{Z}$ such that $ru - st = 1$. Thus, the matrix $\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right)$ is in $\mathrm{SL}_2(\mathbb{Z})$, and by Equation (2.1) it transforms the form (a, b, c) to a form $(n, \ldots)$, as claimed. □

The proposition shows that Question 2.3 can be essentially reduced to a suitable version of Question 2.6.

Proposition 2.11. *Let d, $n \in \mathbb{Z}$, and suppose that either*

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

Then n is properly representable by some *form of discriminant d if and only if d is a square modulo $4|n|$.*

Proof. By Proposition 2.10, n is properly representable by some form of discriminant d if and only if there exists a form (n, k, l) of discriminant d, i.e. satisfying $k^2 - 4nl = d$. The existence of k, l satisfying $k^2 - 4nl = d$ is clearly equivalent to d being a square modulo $4|n|$. We leave it as an exercise to show that the specific conditions on d ensure that for all k, l satisfying $k^2 - 4nl = d$ we have $\gcd(n, k, l) = 1$, so that the form (n, k, l) is automatically primitive. □

Example 2.12. Let $f = x^2 + y^2$. The discriminant is -4. We will soon show that all forms of discriminant -4 are equivalent to each other, so by Proposition 2.11, f properly represents a given integer $n > 0$ if and only if -4 is a square modulo $4n$. This, in turn, is equivalent to -1 being a square modulo n. If we write $n = \prod_p p^{e_p}$, where the product runs over distinct primes, and e_p are non-negative integers, then by the Chinese Remainder Theorem, -1 is a square modulo n if and only if for all p, -1 is a square modulo p^{e_p}. Now, -1 is a square modulo 2, but not modulo 4; next, if $p \equiv 3 \pmod 4$, then -1 is not a square modulo p, so also not a square modulo p^{e_p} for any $e_p \geq 1$; while if $p \equiv 1 \pmod 4$, then -1 is a square modulo p^{e_p} for all $e_p \geq 1$ (this is typically proven in an elementary number theory course; here we will omit the proof). In summary, $x^2 + y^2$ properly represents n if and only if

$$n = 2^\delta \prod_{p \equiv 1 \pmod 4} p^{e_p}$$

with $\delta \in \{0, 1\}$ and with $e_p \in \mathbb{Z}_{\geq 0}$ for all $p \equiv 1 \pmod 4$.

3 Reduction theory of positive definite forms

We will describe an algorithm that, given a positive definite binary quadratic form, "reduces" it to an equivalent form with smaller coefficients. Repeating the reduction step, the algorithm will terminate in a so-called "reduced" form. It will allow us to prove that for every $d \in \mathbb{Z}_{<0}$ there are only finitely many equivalence classes of forms with discriminant d, and will give us a quick algorithm to decide whether two given forms are equivalent.

The reduction algorithm. Let (a, b, c) be a positive definite binary quadratic form. In particular, we have a, $c > 0$. Apply one of the following operations if possible:

(A) if $c < a$, apply the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ to obtain the equivalent form $(c, -b, a)$.

(B) if $|b| > a$, apply the matrix $\left(\begin{smallmatrix} 1 & 0 \\ s & 1 \end{smallmatrix}\right)$ for suitable $s \in \mathbb{Z}$ to obtain the equivalent form (a, b', c'), where $b' = b + 2as$. Choose s such that $|b'| \leq a$.

Step (A) preserves b and decreases a, while step (B) preserves a and decreases $|b|$, so if we keep applying these steps, eventually we must reach a form to which we can apply neither step, i.e. a form (a, b, c) satisfying $c \geq a$ and $|b| \leq a$.

Example 3.1. Start with the form $(10, 13, 5)$. Notice that both the conditions of steps (A) and (B) are satisfied, so we may apply either of the two steps. If we start with (A) we get the chain

$$(10, 13, 5) \xrightarrow{\text{(A)}} (5, -13, 10) \xrightarrow[s=1]{\text{(B)}} (5, -3, 2) \xrightarrow{\text{(A)}} (2, 3, 5) \xrightarrow[s=-1]{\text{(B)}} (2, -1, 4).$$

If, instead, we start with (B), we get

$$(10, 13, 5) \xrightarrow[s=-1]{\text{(B)}} (10, -7, 2) \xrightarrow{\text{(A)}} (2, 7, 10) \xrightarrow[s=-2]{\text{(B)}} (2, -1, 4).$$

Even if neither condition applies, we can use the operations (A) and (B) for further disambiguation:

- if $b = -a$, then use operation (B) with $s = 1$ to preserve a and change b to $+a$;
- if $a = c$, then use operation (A), if necessary, to ensure that $b \geq 0$.

Definition 3.2. A positive definite binary quadratic form (a, b, c) is called *reduced* if

- either $c > a$ and $-a < b \leq a$,
- or $c = a$ and $0 \leq b \leq a$.

Theorem 3.3. *Every positive definite binary quadratic form is equivalent to a unique reduced form.*

Proof. As noted above, applying the steps of the reduction algorithm repeatedly either decreases a while preserving b, or decreases $|b|$ while preserving a. Since we have $a, |b| \geq 0$, this must terminate; and by definition, applying applying the final disambiguation if necessary, the final form is reduced.

It remains to prove uniqueness. Let (a, b, c) be reduced. First, we claim that a is the smallest positive integer properly represented by (a, b, c). Indeed, suppose that $0 \neq n = ar^2 + brt + ct^2$ for some $r, t \in \mathbb{Z}$. If we have $|r| \geq |t|$, then $r^2 \geq |rt|$, and since the form is reduced, we deduce that $ar^2 \geq |brt|$, so that $ar^2 + brt \geq 0$. Hence $n \geq ct^2 \geq at^2$. If $t \neq 0$, then this is $\geq a$, while if $t = 0$, then $n = ar^2 \geq a$. Similarly, if $|r| < |t|$, then we can use $c \geq a \geq |b|$ to show that $brt + ct^2 \geq 0$, and hence $n \geq ar^2 \geq a$.

Next, we claim that b is the unique integer satisfying $|b| \leq a$ and ($b \geq 0$ if $a = c$) that appears as the xy-coefficient among all forms $(a, \ldots)$ that are equivalent to (a, b, c). Indeed, suppose that the matrix $\left(\begin{smallmatrix} r & t \\ s & u \end{smallmatrix}\right)$ transforsm (a, b, c) to (a, b', c') for some b', $c' \in \mathbb{Z}$. Then by equation 2.1 we have $a = ar^2 + brt + ct^2$. Carefully inspecting the argument in the previous paragraph, one finds that this is only possible if either $r = 1$, $t = 0$, or ($a = c$, $r = 0$, $t = 1$). In the former case the matrix is of the form $\left(\begin{smallmatrix} 1 & 0 \\ s & 1 \end{smallmatrix}\right)$, and we saw above that such a matrix changes b by multiples of $2a$, which proves the claim. The parenthetical case is left as an exercise to the reader. □

Lemma 3.4. *Let (a, b, c) be a reduced binary quadratic form, and let $d < 0$ be its discriminant. Then we have $|b| \leq a \leq \sqrt{|d|/3}$.*

Proof. Since we have $|b| \leq a \leq c$, we deduce that $d = b^2 - 4ac \leq a^2 - 4a^2 = -3a^2$, so that $|b| \leq a \leq \sqrt{|d|/3}$, as claimed. □

Theorem 3.5. *Let $d < 0$. Then there exist only finitely many equivalence classes of binary quadratic forms with discriminant d.*

Proof. By Theorem 3.3, the assertion is equivalent to the claim that there exist only finitely many reduced forms with discriminant d. By Lemma 3.4, there exist only finitely many a and b (and therefore c) such that (a, b, c) is a reduced form with discriminant d, whence the result follows. □

Example 3.6. Let us classify positive definite reduced binary quadratic forms of discriminant -4. If (a, b, c) is such a form, then by Lemma 3.4 we have $|b| \leq a \leq \sqrt{4/3}$, so we have $a = 1$, and $b \in \{-1, 0, 1\}$. Since the parity of b is the same as that of d, we must, in fact, have $b = 0$, so the only reduced positive definite form of discriminant -4 is $x^2 + y^2$. This is the missing step in Example 2.12, so that we have now proved (for a second time) Fermat's theorem.

Example 3.7. Let $d = -8$. If (a, b, c) is a positive definite reduced binary quadratic form of discriminant d, then by Lemma 3.4 we have $|b| \leq a \leq \sqrt{8/3}$, so by the same argument as in the previous example we necessarily have $a = 1$ and $b = 0$, hence $c = 2$. Thus, by Theorem 3.3 all binary quadratic forms of discriminant -8 are equivalent to $x^2 + 2y^2$, and therefore the set of integers that a form of discriminant -8 properly represents does not depend on the form, it is the same as the set of integers that are properly represented by $x^2 + 2y^2$. By Proposition 2.11 a prime number p is properly representable by $x^2 + 2y^2$ if and only if -8 is a square modulo $4p$, which is equivalent to -2 being a square modulo p. That condition can be shown to be equivalent to $p \equiv 1$ or $3 \pmod 8$, which proves one of Lagrange's theorems.

Example 3.8. Let $d = -15$. If (a, b, c) is a positive definite reduced binary quadratic form of discriminant d, then by Lemma 3.4 we have $|b| \leq a \leq \sqrt{15/3} < 3$. Moreover, since d is odd, so is b, so we have $b = 1$, and $a = 1$ or 2. Therefore, there are exactly two equivalence classes of positive definite binary quadratic forms of discriminant -15, represented by $(1, 1, 4)$ and $(2, 1, 2)$. Proposition 2.11 implies that an integer n is properly representable by one of these forms if and only if -15 is a square modulo $4n$. This condition can be made explicit, like in the previous examples, but which integers are representable by $x^2+xy+4y^2$, and which ones by $2x^2+xy+2y^2$? Notice that if we have $n = r^2 + rt + 4t^2$ for some r, $t \in \mathbb{Z}$, then we have $4n = (2r + t)^2 + 15t^2 \equiv (2r + t)^2 \pmod{15}$, so if $15 \nmid n$, then this forces n to be a square modulo 15, i.e. $n \equiv 1, 4, 6, 9,$ or $10 \pmod{15}$; while if $n = 2r^2 + rt + 2t^2$, then $8n = (4r + t)^2 + 15t^2$, which implies that if $15 \nmid n$, then we have $n \equiv 2, 3, 5, 8,$ or $12 \pmod{15}$.

We see that when $d = -15$, the set

$$\{n \not\equiv 0 \pmod{15} : n \text{ is representable by a given form of discr. } d\}$$

is describable by congruence conditions. This is an instance of Gauss's *genus theory*. The $|d|$ for which this property holds are called *idoneal numbers*. There are many equivalent definitions, and these numbers crop up in rather unexpected places in number theory.

Gauss conjectured that there are only finitely many idoneal numbers, and wrote down a conjecturally complete list. Chowla proved the finiteness conjecture in 1934. Weinberger proved in 1973 that Gauss's list is missing at most one number. Actual completeness of Gauss's list is still open!

4 Class numbers

This and the next section are only intended to sketch where the theory goes next, and link it up with modern developments.

For $d \in \mathbb{Z}$, the class number $h(d)$ is the number of equivalence classes of binary quadratic forms of discriminant d. This number is always finite, even when $d > 0$. Let us restrict attention to those d that satisfy the hypotheses of Proposition 2.11, the so-called *fundamental discriminants*. As we mentioned in the proof of that proposition, all such d have the property that every binary quadratic form of discriminant d is primitive. Gauss compiled extensive tables of all reduced forms of discriminant d for hundreds, if not thousands, of values of d, and based on these computations made several conjectures:

(A) For every $n \in \mathbb{Z}_{\geq 1}$ there are only finitely many fundamental discriminants $d < 0$ such that $h(d) = n$. In other words, we have $h(d) \to \infty$ as $d \to -\infty$.

(B) The complete list of all fundamental $d < 0$ with $h(d) = 1$ is

$$\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

(C) There exist infinitely many fundamental discriminants $d > 0$ such that $h(d) = 1$.

Part (A) was proven by Heilbronn in 1934.

Part (B) is known as Gauss's class number 1 problem. Heilbronn and Linfoot proved in 1934 that Gauss's list is missing at most one other value. Heegner, an amateur mathematician, submitted in 1952 a proof of completeness of Gauss's list, but the paper was poorly written und contained some small mistakes (some of which could be traced back to mistakes in Weber's "Algebra", the standard text at the time). Heegner died without receiving

recognition for his solution. In 1967, Stark and Birch showed that Heegner's proof had been essentially correct, all mistakes being easily fixable. Today, so-called "Heegner points" are one of the most important techniques for studying elliptic curves.

Part (C) is still open!

5 Class groups

The next major step taken by Gauss was to define a binary operation, so-called composition, on the set of equivalence classes of forms of given discriminant. Gauss showed that this operation gave the set of equivalence classes of binary quadratic forms of a given discriminant d the structure of a finite abelian group, the so-called "class group" $\mathrm{Cl}(d)$. Thus, one can refine Gauss's conjectures by asking questions about the group structure of $\mathrm{Cl}(d)$: as d varies, how often is this group cyclic? How often does the 3-torsion have size at least 9? What is the average size of the 5-torsion of $\mathrm{Cl}(d)$? Etc.

In 1984, Cohen and Lenstra proposed a unifying framework that predicts answers to any such statistical questions about class group, the so-called *Cohen–Lenstra heuristics*. In 2014 Bhargava received a Fields Medal, to a large degree for proving special cases of (generalisations of) these conjectures. In 2020, jointly with Lenstra, we have *disproved* the Cohen–Lenstra heuristics, and proposed a corrected version in a somewhat restricted setting. In a recent preprint with Johnston and Lenstra we have proposed a correction to the heuristics in their "unrestricted" original scope.

Essentially all instances of the Cohen–Lenstra heuristics are wide-open.