Math 4527 (Number Theory 2)

Lecture #37 of 37 $\sim$ April 17, 2021

Binary Quadratic Forms, Part 3

- Composition of Quadratic Forms
- The Class Group (Again)
- Other Results About Class Groups
- Elliptic Curves With Complex Multiplication

This material represents §9.2.4 from the course notes.

Recall, I

Using reduced forms we showed that there were finitely many equivalence classes and gave a method for calculating them all:

Theorem (Reduced Forms)

Let Δ be a nonsquare integer congruent to 0 or 1 modulo 4 and suppose $f(x, y) = ax^2 + bxy + cy^2$ is a reduced form of discriminant Δ. Then the following hold:

1. *There are finitely many reduced forms of discriminant Δ.*
2. *Every equivalence class of quadratic forms of discriminant Δ contains at least one reduced form.*
3. *There are finitely many equivalence classes of binary quadratic forms of discriminant Δ.*
4. *Every equivalence class of binary quadratic forms of negative discriminant Δ is represented by a unique reduced form.*

Composition 101: Spelling and Grammar

We also have a composition law for quadratic forms, due to Dirichlet.

Definition

Let $f(x,y) = ax^2 + bxy + cy^2$ *and* $g(x,y) = a'x^2 + b'xy + c'y^2$ *be positive-definite binary quadratic forms of discriminant* $\Delta < 0$*. Suppose that* $\gcd(a, a', (b+b')/2) = 1$*. Then the* *<u>Dirichlet composition</u> of* $f(x,y)$ *and* $g(x,y)$ *is the binary quadratic form* $h(x,y) = Ax^2 + Bxy + Cy^2$ *where* $A = aa'$*,* B *is the unique integer in* $(-A, A]$ *satisfying* $B \equiv b \pmod{2a}$*,* $B \equiv b' \pmod{2a'}$*, and* $B^2 \equiv \Delta \pmod{4aa'}$*, and* $C = \dfrac{B^2 - \Delta}{4aa'}$.

This composition law takes in two quadratic forms of discriminant Δ and outputs a new one. It is well defined on equivalence classes and yields composition identities.

Composition 102: Words

Dirichlet's composition law makes the collection of equivalence classes of forms of discriminant Δ into an abelian group:

Theorem (Composition of Quadratic Forms)

Suppose Δ is the discriminant of a quadratic integer ring and let $\mathcal{F}$ be the set of equivalence classes of quadratic forms of discriminant Δ. Then $\mathcal{F}$ has the structure of an abelian group under Dirichlet composition. The identity of $\mathcal{F}$ is the norm form on the quadratic integer ring Δ and the inverse of the class containing $ax^2 + bxy + cy^2$ is the class containing $ax^2 - bxy + cy^2$.

Dirichlet composition is well-defined on equivalence classes, so we need to show associativity, commutativity, and that the identity and inverses are as claimed.

Composition 103: Sentences

Proof:

- Associativity = tedious; we skip it.
- Commutativity is immediate, because the definition of the Dirichlet composition is symmetric in f and g.
- For the identity, we want to compose the norm form on $\mathcal{O}_{\sqrt{D}}$ with a reduced form $ax^2 + bxy + cy^2$. Clearly the gcd condition is satisfied, since the norm form has leading coefficient 1.
- Then $A = a$ and we require B to be the unique integer in $(-A, A]$ satisfying $B \equiv b \pmod{2a}$ with $B^2 \equiv \Delta \pmod{4a}$, but clearly $B = b$ satisfies this condition so since $b \in (-|a|, |a|]$ is reduced, we simply have $B = b$.
- Then $C = \frac{B^2 - \Delta}{4a} = c$, and so the result of the composition is again just $ax^2 + bxy + cy^2$.

Composition 104: Paragraphs

Proof (continued):

- For inverses, we want to compose $ax^2 + bxy + cy^2$ with $ax^2 - bxy + cy^2$, but the gcd condition might fail, so instead we apply S to the second form to obtain $cx^2 + bxy + ay^2$.
- Then $\gcd(a, c, (b+b)/2) = \gcd(a, b, c) = 1$ because Δ is squarefree except for a factor of 4. Then the Dirichlet composition of $ax^2 + bxy + cy^2$ with $cx^2 + bxy + ay^2$ has $A = ac$, $B \equiv b \pmod{2a}$, $B \equiv b \pmod{2c}$, and $B^2 \equiv \Delta \pmod{4ac}$, but clearly $B = b$ satisfies this condition.
- Then $C = \frac{b^2-(b^2-4ac)}{4ac} = 1$, so the resulting composition is $acx^2 + bxy + y^2$. Applying S and then a power of T reduces this to a form $x^2 + (\Delta/4)y^2$ if Δ is even, or $x^2 + xy + \frac{1-\Delta}{4}y^2$ if Δ is odd, and this is precisely the norm form, as claimed.

Composition 105: Five-Paragraph Essays

In fact, the abelian group we obtain by composing binary quadratic forms of discriminant Δ is essentially just the ideal class group of the quadratic integer ring $\mathcal{O}_{\sqrt{D}}$:

Theorem (Quadratic Forms and Ideal Class Groups)

Suppose $\Delta < 0$ is the discriminant of a quadratic integer ring $\mathcal{O}_{\sqrt{D}}$. Then the group $\mathcal{F}$ of equivalence classes of binary quadratic forms of discriminant Δ under composition is isomorphic to the group $\mathcal{I} \times \{\pm 1\}$ of equivalence classes of ideals of $\mathcal{O}_{\sqrt{D}}$ under ideal multiplication, together with a sign ± 1.

The isomorphism is very explicit, but the whole statement wouldn't fit on this slide. But the point is, we have fairly natural ways to convert between ideals and binary quadratic forms.

Composition 106: Persuasive Writing

Here is the explicit version:

Definition

Define the map $\varphi_{FI} : \mathcal{F} \to \mathcal{I} \times \{\pm 1\}$ *sending a quadratic form* $ax^2 + bxy + cy^2$ *to the pair* $((a, \frac{-b + \sqrt{\Delta}}{2}), \mathrm{sign}(a))$.

Definition

Define the map $\varphi_{IF} : \mathcal{I} \times \{\pm 1\} \to \mathcal{F}$ *that takes an ideal* $I = (n, \omega)$ *of norm* n *(with* $\omega \notin \mathbb{Z}$*) along with a sign* $s \in \{\pm 1\}$ *to the quadratic form* $s \cdot \frac{N(nx - s\omega y)}{N(I)}$.

Theorem (Quadratic Forms and Ideal Class Groups, Explicitly)

The map φ_{FI} *is a group isomorphism with inverse given by* φ_{IF}.

Composition 107: Pointless Literary Analysis Essays

What this result says is that, up to some minor business with ± signs, we obtain an isomorphism between the group of binary quadratic forms under composition with the ideal class group.

- In particular, when $\Delta < 0$, the positive-definite forms have a $+$ sign and the negative-definite forms have a $-$ sign: thus, the theorem gives an isomorphism between classes of positive-definite forms (which are uniquely represented by reduced positive-definite forms) and classes in the ideal class group.
- For positive Δ, the nonuniqueness of reduced forms in a given equivalence class causes issues with the ± 1. However, one can essentially salvage this result by restricting the definition of reduced forms and accounting for the sign ambiguity, which depends on whether the fundamental unit of $\mathcal{O}_{\sqrt{D}}$ has positive or negative norm.

Composition 108: Sci-Fi Short Stories

Examples:

1. For $D = -1$, with $\Delta = -4$, we have two reduced binary quadratic forms $x^2 + y^2$ and $-x^2 - y^2$.
    - Applying the map φ_{FI} to them yields the same ideal $(1, i) = \mathbb{Z}[i]$ along with a sign ± 1.
    - Conversely, applying φ_{IF} to $I = (1, i)$ and the sign $+1$ yields the quadratic form $\dfrac{N(x + iy)}{N(1)} = x^2 + y^2$, while applying φ_{IF} to $I = (1, i)$ and the sign -1 yields the quadratic form $-\dfrac{N(x - iy)}{N(1)} = -x^2 - y^2$.

Composition 109: Historical Nonfiction

Examples:

2. For $D = -10$, with $\Delta = -40$, we have two reduced positive-definite forms $x^2 + 10y^2$ and $2x^2 + 5y^2$.
   - Applying φ_{FI} to $x^2 + 10y^2$ yields the ideal $(1, \sqrt{-10}) = (1)$ representing the trivial ideal class.
   - Applying φ_{FI} to $2x^2 + 5y^2$ yields the ideal $(2, \sqrt{-10})$ which represents the nontrivial ideal class.
   - Conversely, applying φ_{IF} to $I = (1, \sqrt{-10})$ and the sign $+1$ yields the form $\dfrac{N(x + y\sqrt{-10})}{1} = x^2 + 10y^2$.
   - Applying φ_{IF} to $I = (2, \sqrt{-10})$ and the sign $+1$ yields the quadratic form $\dfrac{N(2x + y\sqrt{-10})}{2} = 2x^2 + 5y^2$.

Composition 110: Non-Ridiculous Poetry

Examples:

3. For $D = \Delta = -31$, we have three reduced positive-definite forms $x^2 + xy + 8y^2$, $2x^2 + xy + 4y^2$, and $2x^2 - xy + 4y^2$.
   - Applying the map φ_{FI} to $x^2 + xy + 8y^2$ yields the ideal $(1, \frac{-1+\sqrt{-31}}{2}) = (1)$ representing the trivial ideal class.
   - Applying the map φ_{FI} to $2x^2 + xy + 4y^2$ yields the ideal $(2, \frac{-1+\sqrt{-31}}{2})$ which is one of the two ideal factors of (2), while applying it to $2x^2 + xy + 4y^2$ yields $(2, \frac{1+\sqrt{-31}}{2})$, which is the other ideal factor of (2).

Composition 111: Satire and Parody

Proof (of Theorem):

- First we show that the maps are well defined.
- If we start with a quadratic form $ax^2 + bxy + cy^2$ of discriminant Δ, then as we have observed numerous times, $b \equiv \Delta \bmod 2$, and so $\frac{-b+\sqrt{\Delta}}{2} \in \mathcal{O}_{\sqrt{D}}$. Then the result of applying φ_{FI} to $ax^2 + bxy + cy^2$ is indeed an ideal of $\mathcal{O}_{\sqrt{D}}$.
- Furthermore, if we apply S or T to the quadratic form, the resulting ideal class is not changed: applying T leaves the ideal alone, while applying S changes $(a, \dfrac{-b+\sqrt{\Delta}}{2})$ to $(c, \dfrac{b+\sqrt{\Delta}}{2})$, and these are the same ideal class because $\dfrac{b+\sqrt{\Delta}}{2} \cdot (a, \dfrac{-b+\sqrt{\Delta}}{2}) = a \cdot (c, \dfrac{b+\sqrt{\Delta}}{2})$.
- So φ_{FI} is well defined.

Composition 112: Getting That Screenplay Written

Proof (deuxième parti):

- For φ_{IF}, suppose that (n, ω) is an ideal of $\mathcal{O}_{\sqrt{D}}$ and $s \in \{\pm 1\}$. Then $N(nx + s\omega y) = (nx + s\omega y)(nx + s\overline{\omega}y) = n^2x^2 + sn(\omega + \overline{\omega})xy + s^2\omega\overline{\omega}y^2$ is a quadratic form. Furthermore, all of its coefficients are divisible by the norm of I since $(N(I)) = I \cdot \overline{I} = (n^2, n(\omega + \overline{\omega}), \omega\overline{\omega})$, so the quotient $s\frac{N(nx - s\omega y)}{N(I)} = snx^2 + (\omega + \overline{\omega})xy + s\frac{\omega\overline{\omega}}{n}y^2$ is still a quadratic form with integer coefficients. Its discriminant is $\frac{n^2(\omega+\overline{\omega})^2 - 4n^2\omega\overline{\omega}}{N(I)^2} = (\omega - \overline{\omega})^2 = \Delta$ since we may assume ω is of the form $\frac{-b+\sqrt{\Delta}}{2}$ by changing basis for I.
- Furthermore, if we scale the ideal I by a principal factor, the resulting quadratic form is not changed, since the ratio $s\frac{N(nx - s\omega y)}{N(I)}$ if we scale n, ω by the same constant.
- So φ_{IF} is well defined.

Composition 113: Steampunk Urban Fantasy

Proof (continué):

- Now we check that the maps are inverses. If we apply φ_{IF} to $\varphi_{FI}(ax^2+bxy+cy^2) = ((a, \frac{-b+\sqrt{\Delta}}{2}), s)$ where $s = \mathrm{sign}(a)$, we obtain the quadratic form $s \cdot \frac{1}{|a|}(ax - s\frac{-b+\sqrt{\Delta}}{2}y)(ax - s\frac{-b-\sqrt{\Delta}}{2}y) =$ $\frac{1}{a}(a^2x^2 - sabxy + s^2acy^2) = ax^2+bxy+cy^2$. Thus, $\varphi_{IF} \circ \varphi_{FI}$ is the identity.
- Oppositely, if we apply φ_{FI} to the ideal $I = (n, \omega)$ and sign s, we obtain $snx^2 + (\omega+\overline{\omega})xy + s\frac{\omega\overline{\omega}}{n}y^2$ as noted above. Then since $n > 0$, we see $\mathrm{sign}(sn) = s$, and the underlying ideal is generated by sn and $\dfrac{-(\omega+\overline{\omega})+\sqrt{\Delta}}{2} = \omega$, hence is simply $I = (n, \omega)$. Thus, $\varphi_{FI} \circ \varphi_{IF}$ is the identity as well, so the maps φ_{FI} and φ_{IF} are inverses.

Composition 114: Legalese and Bureaucracy

Proof (fin):

- Finally, φ_{IF} is multiplicative on ideals, since both the numerator and denominator are multiplicative.
- Thus, φ_{IF} is a group isomorphism and its inverse is φ_{FI}, which is the desired result.

We will remark that it is harder to check directly that φ_{FI} is an isomorphism since the description of Dirichlet composition is more complicated, but this fact is embedded in the results we have already shown.

Applications, I: College Applications

We will remark that in some situations, it is easier to compute the ideal class group by finding factorizations of prime ideals and using the Minkowski bound, and in other situations it is easier to compute reduced forms.

- As an application of computing the class group, we can give characterizations (in certain cases) of the primes, and sometimes of the integers, represented by a quadratic form.
- The idea is first to analyze primes represented by all the forms of the given discriminant, and then to use the structure of the class group to multiply all of the results together.

Applications, II: Co-Op Applications

Example: Classify the integers represented by the two quadratic forms $x^2 + 10y^2$ and $2x^2 + 5y^2$.

- We have shown already that these are the two inequivalent positive-definite forms with discriminant $\Delta = -40$.
- From our results earlier, we see that a prime p is represented by one of these forms if and only if -40 is a quadratic residue modulo p.
- We can ignore $p = 2, 5$ for the moment, since they are both clearly represented by the second form and not the first.

Applications, III: REU Applications

Example: Classify the integers represented by the two quadratic forms $x^2 + 10y^2$ and $2x^2 + 5y^2$.

- For $p \neq 2, 5$ by quadratic reciprocity we have $\left(\frac{-40}{p}\right) = \left(\frac{-10}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{5}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{p}{5}\right)$.
- Since $\left(\frac{-2}{p}\right) = +1$ for $p \equiv 1, 3 \pmod 8$ and $\left(\frac{p}{5}\right) = +1$ for $p \equiv 1, 4 \pmod 5$, we see that $\left(\frac{-40}{p}\right) = +1$ for $p \equiv 1, 9, 11, 19 \pmod{40}$ (both symbols are $+1$) and for $p \equiv 7, 13, 23, 37 \pmod{40}$ (both symbols are -1).
- Thus, a prime $p \neq 2, 5$ is represented by one of $x^2 + 10y^2$ and $2x^2 + 5y^2$ if and only if $p \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40}$.

Applications, IV: Grad School Applications

Example: Classify the integers represented by the two quadratic forms $x^2 + 10y^2$ and $2x^2 + 5y^2$.

- But if p is represented by $x^2 + 10y^2$, then $p \equiv x^2 \pmod 5$, so p must be a quadratic residue modulo 5 and so $p \equiv 1, 9, 11, 19 \pmod{40}$.
- Likewise, if p is represented by $2x^2 + 5y^2$, then $p \equiv 2x^2 \pmod 5$ so p must be a quadratic nonresidue modulo 5 and so $p \equiv 7, 13, 23, 37 \pmod{40}$.
- Since these cases partition the primes, we conclude that the primes represented by $x^2 + 10y^2$ are precisely the primes $p \equiv 1, 9, 11, 19 \pmod{40}$, while the primes represented by $2x^2 + 5y^2$ are precisely 2, 5, and the primes $p \equiv 7, 13, 23, 37 \pmod{40}$.

Applications, V: Job Applications

Example: Classify the integers represented by the two quadratic forms $x^2 + 10y^2$ and $2x^2 + 5y^2$.

- Now we can use the structure of the class group to identify the integers represented by these forms. We may take out all square factors to obtain a product of distinct primes.
- The remaining primes p must be 2, 5, or have $p \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40}$.
- Then, when we multiply these together, since $x^2 + 10y^2$ represents the trivial element of the class group, we see that the form representing n will be $x^2 + 10y^2$ when the total number of primes dividing n to an odd power among $2, 5$ and $p \equiv 7, 13, 23, 37 \pmod{40}$ is even, while the form will be $2x^2 + 5y^2$ when the total number of such primes is odd.

Some History, I: American History

There are many open problems regarding class groups of quadratic fields. A natural immediate question is to determine which quadratic integer fields have class number n for each fixed n.

- The case $n = 1$ is known as the class number 1 problem, and (per our earlier discussion) it is equivalent to asking which quadratic integer rings have unique factorization. It was conjectured by Gauss in 1801 that there are only finitely many imaginary quadratic fields of class number 1.
- It was proven by Heilbronn in 1934 that there are only finitely many imaginary quadratic fields of any fixed class number (so that in particular the class number $h(-d) \to \infty$ as $d \to \infty$). This result was sharpened by Siegel to obtain an ineffective bound $h(-d) \geq c\sqrt{d}$ for a positive constant c whose value was not effectively known.

Some History, II: European History

Heilbronn also showed that there were at most 10 imaginary quadratic fields of class number 1.

- Since 9 such fields, corresponding to $D = -1$, -2, -3, -7, -11, -19, -43, -67, and -163 were already known, this meant there could exist at most one more.
- The nonexistence of this 10th field was essentially proven by Heegner in 1952 using modular forms, but his proof had some minor gaps and it was not accepted[1] until Stark gave a full proof of the result in 1967. Baker also gave a proof, using an entirely different method (linear forms in logarithms), in 1966.

[1] Heegner was not a professional mathematician (he was in fact a radio engineer and high school teacher, though he did have mathematical training), which certainly contributed to the mathematical community's lack of credence for his claim that he had settled a 150-year-old conjecture of Gauss. Sadly, he died in 1965, before his results gained general acceptance.

Some History, III: Canadian History

For real quadratic fields, the results are quite different: Gauss conjectured in this case that there are infinitely many real quadratic fields of class number 1.

- This problem of determining whether there actually are infinitely many real quadratic fields of class number 1 is still open (as of 2021). In fact, it is not known definitively whether there are infinitely many real quadratic fields of class number greater than 1 either!
- Many small values of D do yield real quadratic fields of class number 1. In fact, the only squarefree values of D less than 100 that do not are $D = 10, 15, 26, 30, 34, 35, 39, 42, 51, 55, 58, 65, 66, 70, 74, 78, 85, 87, 91, 95$ which all have class number 2 along with $D = 79$ which has class number 3 and $D = 82$ which has class number 4.

Some History, IV: Venezuelan History

There are various conjectures about various aspects of the class groups of real and imaginary quadratic fields.

- One set of such results are the Cohen-Lenstra heuristics, which give precise predictions, for odd primes p, about the density with which any given abelian p-group will appear as the p-power torsion part of a class group (i.e., the Sylow p-subgroup) of a real or imaginary quadratic field.
- For the prime $p = 2$, the structures of p-power torsion subgroups of class groups are fully understood, and are consequences of what is called genus theory, which is a name due to Gauss (as is the term "equivalence class", first used in Gauss's analysis of quadratic forms) that has nothing to do with other uses[2] of the word "genus", e.g., in topology.

[2] Gauss's organization of forms into classes, orders, and then genera was clearly a reference to Linnaeus's taxonomic nomenclature, which first appeared 40 years prior – and this is where our word "class" from set theory comes from!

Some History, V: Kyrgyzstani History

Intuitively, the Cohen-Lenstra heuristics say that the probability, in an appropriate sense, that a given abelian p-group P will occur as the p-part of the class group of an imaginary quadratic field should be proportional to $1/\#\mathrm{Aut}(P)$.

- This may initially seem to be a rather unnatural weighting, but in fact it is quite sensible in the appropriate context.
- Specifically, given a group acting on a set X, if we wish to select a random orbit of the group uniformly at random, we should weight each of the elements of X by 1 over the size of its orbit and then pick an element of X at random with that weighting.
- As a side-comment, if you do this for "picking a random finite set of size n", the resulting probability distribution is the Poisson distribution.

Some History, VI: Martian History

One can use the Cohen-Lenstra heuristics to make predictions about p-parts of class groups by comparing $1/\#\mathrm{Aut}(P)$ to the sum of all these values over all abelian p-groups.

- Some various predictions for imaginary quadratic fields: the probability that the class number is divisible by 3 (i.e., that the 3-part of the class group is not trivial) is approximately 43.99%, the probability that it is divisible by 5 is approximately 23.97%, and the probability that it is divisible by 7 is approximately 16.32%.
- A similar heuristic holds for real quadratic fields, although the weighting is slightly different: the probability that a prime p divides the class number is predicted as $1 - \prod_{k \geq 2}(1 - p^{-k})$, which for $p = 3$ is approximately 15.98%, for $p = 5$ is approximately 4.96%, and for $p = 7$ is approximately 2.37%.

These results agree very well with numerical data.

Complex Multiplication, I

For fun in the last few minutes, I thought I'd try to pack in a very brief discussion of elliptic curves with complex multiplication.

- For an arbitrary elliptic curve E, we say that a function $f : E \to E$ is an endomorphism of E if f is a group homomorphism on the points of E, and is also a rational function when written down in coordinates.
- The endomorphisms naturally form a ring (addition is pointwise, multiplication is via function composition).
- The typical examples are the multiplication-by-m maps. For most curves, these maps are the only endomorphisms.
- But some elliptic curves have "extra" endomorphisms: over $\mathbb{C}$, these will be "complex multiplications", which behave like multiplication by a complex number. (Over finite fields, one can also get quaternion rings, but we won't worry about that.)

Complex Multiplication, II

As we discussed, an elliptic curve E over $\mathbb{C}$ corresponds to a lattice Λ in the complex plane.

- The endomorphisms of E then act on the lattice Λ via complex number arithmetic. Suppose Λ has basis $\{1, \tau\}$.
- Then if we have an element $z \in \mathbb{C}$ that corresponds to a complex multiplication, multiplying Λ by z must land back inside Λ.
- In particular, $z \cdot 1$ and $z \cdot \tau$ are both in Λ, so $z = a\tau + b$ and $z\tau = c\tau + d$ for some integers a, b, c, d.
- But this means $c\tau + d = \tau(a\tau + b)$, so τ is the root of a quadratic polynomial with integer coefficients, which is to say, it lies in some (necessarily) imaginary quadratic field $\mathbb{Q}(\sqrt{D})$.
- Moreover, eliminating τ yields $z^2 - (b + c)z + ad = 0$, so in fact $z \in \mathcal{O}_{\sqrt{D}}$.

Complex Multiplication, III

This tells us that the possible complex multiplications on the lattice Λ are given by a (nonzero) ideal of $\mathcal{O}_{\sqrt{D}}$.

- On the other hand, as we have already seen, we can view any nonzero ideal of $\mathcal{O}_{\sqrt{D}}$ as yielding a lattice λ_I inside $\mathbb{C}$ via the Minkowski embedding.
- Then, because ideals are closed under arbitrary R-multiplication, we obtain complex multiplication by $\mathcal{O}_{\sqrt{D}}$ on the elliptic curve E corresponding to λ_I.
- Furthermore, scaling the lattice λ_I by a constant does not affect the isomorphism class of the curve E. So in fact, up to isomorphism, the elliptic curves E with endomorphism ring $\mathcal{O}_{\sqrt{D}}$ are in bijection with the elements of the ideal class group of $\mathcal{O}_{\sqrt{D}}$.

Complex Multiplication, IV

This result actually tells us quite a lot about the j-invariants of these possible curves E.

- In fact, for an elliptic curve with complex multiplication by $\mathcal{O}_{\sqrt{D}}$, the j-invariant is necessarily an algebraic integer (i.e., a root of a monic polynomial with integer coefficients) whose degree is equal to the degree of the class number of $\mathcal{O}_{\sqrt{D}}$.
- The degree part of this statement follows because of this bijection between elliptic curves E with endomorphism ring $\mathcal{O}_{\sqrt{D}}$ and the elements of the class group of $\mathcal{O}_{\sqrt{D}}$. (Then one uses a bit of Galois theory: all of the elliptic curves are Galois conjugates, so applying this to the j-invariant shows that it has the same number of Galois conjugates over $\mathbb{Q}$, and this gives the degree. The hard part is showing all of the curves are actually Galois conjugates.)

Complex Multiplication, V

In particular, if we choose $\mathcal{O}_{\sqrt{D}}$ to have class number 1, then its j-invariant satisfies a monic polynomial with integer coefficients of degree 1: in other words, it is an integer.

- We can use this fact to make a very mysterious observation: the real number $e^{\pi\sqrt{163}} \approx 262537412640768743.99999999999925\ldots$ is extremely close to an integer.

Complex Multiplication, VI

The mysterious observation is, in fact, related to what I was just talking about.

- The connection is that the j-invariant is actually what is called a modular function: this is a meromorphic function f on the complex upper half-plane such that
  1. $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and all z in the upper half-plane
  2. The function f has a Fourier expansion at $i\infty$ of the form $f(z) = \sum_{n=0}^{\infty} c_n q^n$ for $q = e^{2\pi i z}$.

  The integer k is called the weight of the modular function.

Complex Multiplication, VII

The j-invariant is a modular function of weight 0 that is holomorphic on the upper half-plane.

- One can then compute its Fourier expansion at ∞, which is $j(z) = \frac{1}{q} + 744 + 196884q + \cdots$.
- Now, apply this to an elliptic curve with complex multiplication by $z = \sqrt{-163}$, so that $q = e^{2\pi i \sqrt{-163}} = e^{\pi\sqrt{-163}}$.
- Since $\mathcal{O}_{\sqrt{-163}}$ has class number 1, its j-invariant is an integer.
- But the Fourier series says $j(z) = \frac{1}{q} + 744 + 196884q + \cdots = e^{\pi\sqrt{163}} + 744 + 196884e^{-\pi\sqrt{163}} + \cdots$, and the terms after the first two are very, very small.
- Hence, our numerical coincidence.

Complex Multiplication, VIII

Another mystery: the Fourier series of the j-invariant is $j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$.

- If M is the monster group (the largest sporadic simple group, of order $808017424794512875886459904961710757005754368000000000$ $= 2^{46}3^{20}5^{9}7^{6}11^{2}13^{3}17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$), then the dimensions of the irreducible representations of M are 1, 196883, 21296876, 842609326, ...

Complex Multiplication, VIII

Another mystery: the Fourier series of the j-invariant is $j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$.

- If M is the monster group (the largest sporadic simple group, of order $808017424794512875886459904961710757005754368000000000 = 2^{46}3^{20}5^{9}7^{6}11^{2}13^{3}17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$), then the dimensions of the irreducible representations of M are 1, 196883, 21296876, 842609326, ...
- It was conjectured by McKay, Thompson, Conway, and Norton that these suspiciously close values are not a coincidence: this was called the Moonshine Conjecture.
- In 1992, using some very deep results like the no-ghost theorem from string theory, Borcherds proved that there is a graded module whose automorphism group is exactly M, from which these comparisons arise.

Wrap-Up

So, of course, I hope all of this discussion has convinced you that there are lots more amazing results in number theory out there to learn, and that all of the topics from the course really are connected, often in surprising and unexpected ways.

- I really had fun designing and teaching this course, and I hope you enjoyed taking it.
- I didn't cover quite everything I was hoping to cover, but I think we got through quite a lot of great things.
- If you did enjoy the course, please do make sure to fill out the TRACE evaluations. The department really does use them to decide who gets to teach what, and I'm really hoping to be able to teach other courses like this one in the future.

Also, the due date for HW13 is extended to Friday evening, and I will have office hours from noon-3pm on that day.

Summary

We established that the composition of binary quadratic forms yields a group structure that is the same as the ideal class group.

We discussed some examples of classifying integers represented by quadratic forms.

We discussed some open problems about class groups, including the Cohen-Lenstra heuristics.

We briefly discussed elliptic curves with complex multiplication.

Next lecture: There isn't one, the class is over :-(

Wrap-Up, II: The Finaling

Finally, I know you're all dreading the prospect of taking an actual exam in this course.

- Since essentially everyone has worked quite hard all semester, I am announcing a change to the course grade policy: if
  1. you have finished all 13 homework assignments (no slacking off this week, sorry), and
  2. your total score on the 13 assignments is at least 330/400 (which for those who have completed the first 12 assignments, requires at most 20/35 on HW13)

  then you are excused from taking the final exam as you are already receiving an A in the course.
- If these conditions do not apply to you, I will email you the final exam and it will be due on Friday, April 30th.
- Otherwise, good luck on your other exams, have a great summer, and stay safe!