Primes of the form $x^2 + ny^2$:

Representing integers by quadratic forms

Sommersemester 2017

Steven Charlton

C5A38, Fachbereich Mathematik, Universität Tübingen

E-mail address: steven.charlton@uni-tuebingen.de or charlton@math.uni-tuebingen.de

URL: https://www.math.uni-tuebingen.de/user/charlton/teaching/primes_17/

Contents

CHAPTER 1

Introduction and Motivation

Lecture 1
19/04/2017

Our motivating results are the following claims due to Pierre de Fermat. The first result was announced by Fermat in a letter to Marin Mersenne, dated 25 December 1640. The other results were announced by Fermat fourteen years later, in a letter to Blaise Pascal.

Fermat did not provide proofs of these results; considerable effort was required by Leonhard Euler to find the proofs. After first reading about the results, it took Euler 40 years to finally discover full proofs of Fermat's claims. Euler also spent much time thinking about how to generalise these results.

Fermat's claims are the following:

Theorem 1.1 (Fermat 1640 (conjectured), Euler 1747–1749, and 1752–1755 (published))**.** *A prime number p can be written as $x^2 + y^2$, with $x, y \in \mathbb{Z}$, if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

Example 1.2. We have $p = 1\,000\,003$ is prime, and $p \equiv 3 \pmod 4$. Therefore p cannot be written as $x^2 + y^2$. With brute force, you can directly check this!

On the other hand, $p = 5\,617\,237$ is prime and $p = 1 \pmod 4$. Therefore we should be able to write p as $x^2 + y^2$. Indeed

$$5\,617\,237 = 1959^2 + 1334^2\,.$$

(Notice Fermat's claim does not tell us how to find such a representation, only that it should exist. Constructing solutions is an interesting topic by itself!)

Theorem 1.3 (Fermat 1654 (conjectured), Euler 1772))**.** *Let p be a prime number. Then we can write*

$$p = x^2 + 2y^2, \text{ with } x, y \in \mathbb{Z} \iff p = 2, \text{ or } p \equiv 1, 3 \pmod 8$$
$$p = x^2 + 3y^2, \text{ with } x, y \in \mathbb{Z} \iff p = 3, \text{ or } p \equiv 1 \pmod 3\,.$$

Our main question and goal is the following

Problem 1.4. What primes p can be expressed in the form

$$p = x^2 + ny^2$$

for integers x, y? How can we prove these results? How general can we make our results?

1.1. Overview of main topics and results

Here we give an overview of the main results and topics we will see in this course. This section is intended to be deliberately vague: during the semester we will explain the details and theory! We are only trying to chart our course at the moment.

Quadratic forms and quadratic reciprocity: We begin by discussing Euler's proofs of Fermat's claims. We will try to give proofs that are close in spirit to Euler's proofs. There are two main steps: reciprocity and descent which lead us into more abstract theory.

- Descent is somehow easier for Euler to prove. It tells us about the form of p if p divides an number of the form x^2+ny^2. Generally is leads us to study 'binary quadratic forms' $ax^2+bxy+cy^2$, and to understand when two quadratic forms are equivalent.
- Reciprocity is harder. It gives us conditions for when p divides a number of the form x^2+ny^2. It leads us to the beautiful result that is quadratic reciprocity, which relates the existence of solutions of $\pm p \equiv x^2 \pmod{q}$ and $\pm q \equiv y^2 \pmod{p}$.

Our first big general result is

Theorem 1.5. *Let p be prime not dividing D. Then $\left(\frac{D}{p}\right) = 1$, (meaning D is a square modulo p) if and only if p is represented by some quadratic form $ax^2+bxy+cy^2$ of* discriminant $D = b^2 = 4ac$.

Class number 1: When the *class number* $h^+(D)$ (number of non-equivalent quadratic forms of discriminant D) is 1, we can use quadratic reciprocity and the theory of reduced quadratic forms to derive results. This happens when $D = -4, -8, -12$, and so we can recover Fermat's results. But it happens in other cases too, and we get new results.

Example 1.6 ($D = 8$)**.** For $p \neq 2$ we have

$$p = x^2 - 2y^2 \text{ if and only if } p \equiv 1, 7 \pmod{8}$$

Example 1.7 ($D = -11$)**.** For $p \neq 2, 11$, we have

$$p = x^2 + xy + 3y^2 \text{ if and only if } p \equiv p \equiv 1, 3, 4, 5, 9 \pmod{11}$$

Try to think about some of the following examples. We will see how to find conditions for p during the course of the semester, but you can start to 'get a feel' for the results by playing around yourself!

Exercise 1.8. Similar 'nice' criteria exist for the following cases (and many more!)

- $x^2 + 7y^2$ where $D = -28$,
- $x^2 - 5y^2$ where $D = 20$,
- $x^2 - 13y^2$ where $D = 52$,
- $x^2 + xy + 5y^2$ where $D = -19$,
- $x^2 + xy - y^2$ where $D = 5$,
- $x^2 + xy - 4y^2$ where $D = 13$.

Try to discover these conditions in one or two of the cases: which primes p can be written in these forms? What patterns do these p satisfy?

Perhaps you can write a computer program to investigate, or use a computer algebra system like Mathematica, Maple or Sage? Or even just a spreadsheet?

Genus theory, beyond class number 1. When $h^+(D) > 1$, we can't immediately get such conditions. All we can say is

Example 1.9 ($D = -20$)**.** For $p \neq 2, 5$ we have

$$p = \left\{ \begin{matrix} x^2 + 5y^2, \text{ or} \\ 2x^2 + 2xy + 3y^2 \end{matrix} \right\} \text{ if and only if } p \equiv 1, 3, 7, 9 \pmod{20}$$

But if these two quadratic forms are in different *genera*, the congruence condition 'splits up' into separate conditions for the two forms. Being in the same genera means the two forms take the same values modulo D. Since $x^2 + 5y^2$ takes only values $1, 9 \pmod{20}$ and $2x^2 + 2xy + 3y^2$ takes only values $3, 7 \pmod{20}$ we can argue for the following.

Example 1.10 ($D = -20$)**.** For $p \neq 2, 5$ we have

$$p = x^2 + 5y^2 \text{ if and only if } p \equiv 1, 9 \pmod{20}$$
$$p = 2x^2 + 2xy + 3y^2 \text{ if and only if } p \equiv 3, 7 \pmod{20}$$

This allows us to handle many more cases, with only a little more work.

Unfortunately, genus theory is not powerful enough to solve our question completely. Generally there are many quadratic forms in the same genera, and we can only obtain partial results like

Example 1.11 ($D = -56$)**.** For $p \neq 2, 7$ we have

$$p = \left\{x^2 + 14y^2, \text{ or } 2x^2 + 7y^2\right\} \text{ if and only if } p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$$
$$p = \left\{3x^2 \pm 2xy + 5y^2\right\} \text{ if and only if } p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$$

No amount of congruence conditions will *ever* able to separate the two quadratic forms $x^2 + 14y^2$ and $2x^2 + 7y^2$! We need a genuinely new idea here.

Composition of quadratic forms. In studying examples like the above, involving criteria which 'mix' many different quadratic forms, we encounter a curious phenomenon.

Example 1.12 ($D = -20$)**.** For p, q primes we have

$$p \equiv 3, 7 \pmod{20} \text{ implies } 2p = x^2 + 5y^2$$
$$p, q \equiv 3, 7 \pmod{20} \text{ implies } pq = x^2 + 5y^2$$

Example 1.13 ($D = -56$)**.** Let $p, q \neq 2, 7$ be primes. While we have no condition like

$$p \equiv a_1, \ldots, a_k \pmod{N} \text{ implies } p = x^2 + 14y^2\,,$$

we *can* say

$$p \equiv 3, 5, 13, 19, 27, 45 \pmod{56} \text{ implies } 3p = x^2 + 14y^2$$
$$p, p \equiv 3, 5, 13, 19, 27, 45 \pmod{56} \text{ implies } pq = x^2 + 14y^2\,.$$

Where does 2 come from in the first example, and why does instead 3 work in the second example?

The first example follows immediately from the identity

$$(2x^2+2xy+3y^2)(2z^2+2zw+3w^2) = (2xz+xw+yz+3yw)^2+5(xw-yz)^2\,.$$

How common are such identities? How can we find them? What is the structure/deeper reason behind them?

This identity is an example of *composition of quadratic forms*. Given two binary quadratic forms of the same discriminant, their product can *always* be expressed as a quadratic form of the same discriminant, with a bilinear combination of the two original pairs of variables.

This even gives the set of binary quadratic forms of discriminant D the structure of an abelian group! This group structure also gives us an alternative way to characterise the *genus* of a quadratic form.

Exercise 1.14. Can you find a similar identity for

$$(3x^2+2xy+5y^2)(3z^2+2zw+5w^2) = (\cdots)^2+14(\cdots)^2\,?$$

[Binary quadratic forms of discriminant D can be related directly to idea classes in (orders in) quadratic number fields $\mathbb{Q}(\sqrt{-D})$. The composition of binary quadratic forms is exactly the multiplication in the *ideal class group*!]

Cubic and biquadratic reciprocity, towards class field theory. Genus theory does not allow us to separate x^2+14y^2 and $2x^2+7y^2$. We can start to see how to tackle this problem by looking at some of Euler's other conjectures.

Conjecture 1.15 (Euler)**.** *Let p be a prime, then*

$$p = x^2+27y^2 \text{ if and only if } \begin{cases} p \equiv 1 \pmod 3 \text{ , and} \\ 2 \equiv z^3 \pmod p \text{ has a solution} \end{cases}.$$

Conjecture 1.16 (Euler)**.** *Let p be a prime, then*

$$p = x^2+64y^2 \text{ if and only if } \begin{cases} p \equiv 1 \pmod 4 \text{ , and} \\ 2 \equiv z^4 \pmod p \text{ has a solution} \end{cases}.$$

Gauss was able to prove these results using his work on cubic and biquadratic reciprocity. In much the same way as quadratic reciprocity gives us a solution to easier cases.

It turns out that the equivalent result for x^2+14y^2 is the following

Example 1.17 ($D=-56$)**.** Let $p \neq, 2, 7$ be a prime, then

$$p = x^2+14y^2 \text{ if and only if } \begin{cases} \left(\frac{-14}{p}\right) = 1, \text{ and} \\ (z^2+1)^2 \equiv 8 \pmod p \text{ has a solution} \end{cases}.$$

We will aim to prove Gauss's results using (relatively) elementary techniques. The general theory which subsumes Gauss's results, and the x^2+14y^2 result, is *class field theory* and *Artin reciprocity*

Fact 1.18. The primes $p = x^2 + ny^2$ are determined by the behaviour of p in the *Hilbert class field* (or more generally the *ring class field*) of $\mathbb{Z}[\sqrt{-n}] \subset \mathbb{Q}(\sqrt{-n})$.

This leads to the 'ultimate' theorem in the study of $x^2 + ny^2$

Theorem 1.19. *Let n be a (non-square) integer. Then there exists a polynomial $f_n(z)$ of degree $h^+(-4n)$ (the class number of discriminant $D = -4n$), such that*

$$p = x^2 + ny^2 \text{ if and only if } \begin{cases} \left(\frac{-n}{p}\right) = 1, \text{ and} \\ f_n(z) \equiv 0 \pmod{p} \text{ has a solution.} \end{cases}$$

Exercise 1.20. Test out the conditions given above for $x^2 + 14y^2$, $x^2 + 27y^2$ and $x^2 + 64y^2$. A good selection is $p = 23, 31, 43, 73, 89, 109, 113, 127, 137, 151, 157$.

1.2. Extra topics

In the last few lectures, I would like to discuss some other related topics which study the question of $p = x^2 + ny^2$ or more generally $m = ax^2 + bxy + cy^2$, from other perspectives.

These extra topics are intended to be for fun[1] and provide some glimpses into deeper/more advanced topics. They will **NOT** be examined.

- Polynomial conditions are not sufficient for $ax^2 + bxy + cy^2$, but we can use *modular forms*.
- Modular forms and L-functions can count the *number* of different ways of writing $m = ax^2 + bxy + cy^2$.
- We can study higher arity forms like $x^2 + y^2 + z^2$ using *local-global* methods, and using *modular forms*.

1.3. Recommended books

The main book for this course is:

- David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Vol. 34. John Wiley & Sons, 2011

This covers all the main topics in detail, and provides a historical perspective for the results.

Other useful books which may present the material in different ways (more general, alternative viewpoints, ...) include

- John William Scott Cassels. *Rational quadratic forms*. Courier Dover Publications, 2008
- John Horton Conway and Francis YC Fung. *The sensual (quadratic) form*. 26. MAA, 1997
- Don Bernard Zagier. *Zetafunktionen und quadratische Körper: eine Einführung in die höhere Zahlentheorie*. Springer-Verlag, 2013

I will try to indicate the appropriate sections, when we cover the relevant material.

[1] At least for my fun(!)

Part 1

Elementary theory of binary quadratic forms

CHAPTER 2

Fermat's Three Claims

Lecture 2
26/04/2017

We will first try to prove Fermat's claims, using as elementary methods as possible. This will lay the foundations for more abstract analysis later.

2.1. Recap of $\bmod n$ notation

First, let us give a reminder of the meaning of the notation $a \equiv b \pmod{n}$, and the properties of the associated ring $\mathbb{Z}/n\mathbb{Z}$.

Definition 2.1. We write $a \equiv b \pmod{n}$ to mean $n \mid a - b$. That is n divides $a - b$.

The operations of $+$ and $\times$ are well defined under $\equiv \pmod{n}$. That is

$$a \equiv a' \pmod{n} \text{ and } b \equiv b' \pmod{n}$$

means

$$a \pm b \equiv a' \pm b' \pmod{n}$$
$$a \times b \equiv a' \times b' \pmod{n}$$

Write $[x] \coloneqq \{ r \in \mathbb{Z} \mid r \equiv x \pmod{n} \}$ for the equivalence class of integers with the same remainder as x, modulo n.

Then the set

$$\mathbb{Z}/n\mathbb{Z} \coloneqq \{ [x] \mid x \in \mathbb{Z} \} = \{ [0], [1], \dots, [n-1] \}$$

forms a commutative ring, with unity $[1]$, under the operations of $+, \times$.

We can find y such that $[x] \cdot [y] = [1]$ (meaning $[x]$ is a unit in $\mathbb{Z}/n\mathbb{Z}$, and $[x]^{-1} = [y]$), if and only if $\gcd(x, n) = 1$. Therefore, if $n = p$ prime, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field and $(\mathbb{Z}/p\mathbb{Z})^* = \{ [1], [2], \dots, [n-1] \}$ is a group of order $p - 1$.

Fact 2.2. It is known that the group of units of a finite field is cyclic. More generally: any finite subgroup of the group of units of any field is cyclic.

Fact 2.3 (Lagrange)**.** In a finite group G, the order of any element $g \in G$ divides the order of the group. Alternatively, $g^{\#G} = 1_G$ the identity.

2.2. Fermat's two squares theorem

Here we present Euler's elementary proof of Fermat's two squares theorem.

Theorem 2.4 (Fermat's two squares)**.** *Let p be a prime. Then*

$$p = x^2 + y^2, \text{ with } x, y \in \mathbb{Z} \iff p = 2, \text{ or } p \equiv 1 \pmod{4}.$$

Proof. We prove each direction separately.

'⇒': Modulo 4, we see the squares are $0^2, 1^2, 2^2, 3^2 \equiv 0, 1 \pmod 4$. So if $p = x^2 + y^2$, then we obtain $p \equiv 0 + 0, 0 + 1, 1 + 0, 1 + 1 \equiv 0, 1, 2 \pmod 4$.

Since p is prime, $p \equiv 0 \pmod 4$ is not possible, and $p \equiv 2 \pmod 4$ means $p = 2$. So indeed $p = x^2 + y^2 \Rightarrow p = 2$ or $p \equiv 1 \pmod 4$.

'⇐': This direction requires two steps.

Descent. If $p \mid x^2 + y^2$, $\gcd(x, y) = 1$, then p is a sum of two squares.

Reciprocity. If $p \equiv 1 \pmod 4$, then $p \mid x^2 + y^2$, $gcd(x, y) = 1$.

We deal with each in turn. □

Descent. Euler was able to prove *Descent* first, in 1747, using the classical identity $(x^2 + y^2)(z^2 + w^2) = (xz \pm yw)^2 + (xw \mp yz)^2$, and the following lemma.

Lemma 2.5. *Suppose $N = a^2 + b^2$ is a sum of two relative prime squares* $\gcd(a, b) = 1$. *If $q = x^2 + y^2$ is a prime divisor of N, then N/q is also a sum of two relatively prime squares.*

Proof. We have $N = a^2 + n^2$ and $q = x^2 + y^2$. So q divides

$$x^2N - a^2q = x^2(a^2 + b^2) - a^2(x^2 + y^2) = (xb - ay)(xb + ay)\,.$$

Since q is prime, it divides one of the two factors. We can assume (by changing $a \leftrightarrow -a$) that $q \mid xb - ay$, so $xb - ay = dq$ for some $d \in \mathbb{Z}$.

Claim: $x \mid a + dy$. Since $\gcd(x, y) = 1$, this is equivalent to $x \mid (a + dy)y$. But

$$\begin{aligned}(a + dy)y &= ay + dy^2\\ &= xb - dq + dy^2\\ &= xb - d(x^2 + y^2) + dy^2\\ &= xb - dx^2\end{aligned}$$

is certainly divisible by x.

Set $a + dy = cx$. Then we obtain $a = cx - dy$ and $b = dx + cy$. [The $b = dx + cy$ follows by writing

$$\begin{aligned}&xb - dx^2 = (a + dy)y\\ &\Rightarrow xb - dx^2 = cxy\\ &\Rightarrow b - dx = cy\\ &\Rightarrow b = dx + cy\end{aligned}$$

using the equation above.]

Now we have

$$\begin{aligned}N = a^2 + b^2 &= (cx - dy)^2 + (dx + cy)^2\\ &= (x^2 + y^2)(c^2 + d^2)\\ &= q(c^2 + d^2)\,.\end{aligned}$$

So see that $N/q = c^2 + d^2$ is a sum of squares. Moreover, we must have $\gcd(c, d) = 1$, as $\gcd(a, b) = 1$. □

How to use this to complete the *Descent* step? Suppose p is an odd prime dividing $N = a^2 + b^2$, $\gcd(a, b) = 1$.

We can change $a \to a' = a + pk$, and $b \to b' = b + p\ell$, to assume $|a|, |b| < \frac{1}{2}p$, giving $N < \frac{1}{2}p^2$. If $\gcd(a', b') > 1$, we can also divide by it. So we can assume $p \mid N = a^2 + b^2$, with $\gcd(a, b) = 1$ and $N \leq \frac{1}{2}p^2$.

Any prime divisor $q \neq p$ of N is necessarily $< p$. If it is $> p$, then $N > pq > p^2$, contradicting our bound $N < \frac{1}{2}p^2$. Moreover, $p^2 \nmid N$, so p only appears with exponent 1.

Suppose that all such $q \mid N$ are the sum of two squares. By repeatedly applying Lemma 2.5, then we conclude $p = N/(\prod q_i^{n_i})$ is also sum of two squares. Now if p is *not* a sum of two squares, we can produce a smaller counterexample q; we can repeat this indefinitely to obtain an infinite decreasing sequence of prime numbers. This is a contradiction, and completes the *Descent* step.

Reciprocity. The reciprocity step caused Euler more problems; he only completed it in 1749. Euler's proof used finite differences. We can appeal to our knowledge of groups, and of the field $\mathbb{Z}/p\mathbb{Z}$ instead.

If $p \equiv 1 \pmod 4$, then $p = 4k + 1$ for some positive integer k. Then $(\mathbb{Z}/p\mathbb{Z})^*$ is a group of order $4k$. By Lagrange's theorem on the orders of elements in groups, we have

$$\alpha^{4k} \equiv 1 \pmod 4$$

for every $\alpha \in \mathbb{Z}/p\mathbb{Z}$.

View this as saying the polynomial $x^{4k} - 1$ has $4k$ roots in $\mathbb{Z}/p\mathbb{Z}$. Factor this polynomial over $\mathbb{Z}/p\mathbb{Z}$ to get $x^{4k} - 1 = (x^{2k} - 1)(x^{2k} + 1)$. We know a polynomial $f(x)$ over a field (even integral domain!) has $\leq \deg f(x)$ roots. Since $x^{2k} - 1$ can only have $2k$ roots, the other $2k$ elements must be roots of $x^{2k} + 1$. Let $\beta = [b] \in \mathbb{Z}/p\mathbb{Z}$ be such a root, then $b^{2k} + 1 \equiv 0 \pmod p$, meaning $p \mid b^{2k} + 1$. (Can choose $b > 0$ by adding multiples of p.) So $p \mid (b^k)^2 + 1^2$, and $\gcd(b^k, 1) = 1$. This completes the *Reciprocity* step, and so completes the proof of the theorem.

2.3. When an integer $N = x^2 + y^2$

Lecture 3
03/05/2017

Without much more work, we can establish a criterion on which integers are the sum of two squares.

Theorem 2.6. *A positive integer N is the sum of two squares if and only if the exponent of $p \equiv 3 \pmod 4$ in the prime factorisation of N is even.*

Proof. There are two directions to the proof. The first follows from what we know above.

'$\Leftarrow$': Write $N = 2^c p_1^{e_1} \cdots p_k^{e_k} q_1^{2f_1} \cdots q_l^{2f_l}$, where each $p_i \equiv 1 \pmod 4$, and each $q_j \equiv 3 \pmod 4$.

We can write $p_i = a_i^2 + b_i^2$ from the result above, $2 = 1^2 + 1^2$ and $q_j^{2f_j} = (q_j^{f_j})^2 + 0^2$. Then repeatedly use the identity

$$(x^2 + y^2)(z^2 + w)^2 = (xz \pm yw)^2 + (xw \mp yz)^2$$

to write N as the sum of two squares.

'⇒': Now suppose we can write $N = x^2 + y^2$, for some $x, y \in \mathbb{Z}$. We can factor N into primes, and write

$$N = ts^2\,,$$

where t is square-free, i.e. all primes in t appear with exponent 1. We want to show that if an odd prime $p \mid t$, then $p \equiv 1 \pmod 4$.

Suppose $\gcd(x, y) = d$, write $x = x_0 d$, $y = y_0 d$. Since d^2 divides the right hand side of $ts^2 = x^2 + y^2$, and t is square free, d^2 must divide s^2. So write $s^2 = s_0^2 d^2$. Then we can divide through by d^2 on both sides, we get

$$\begin{aligned} ts^2 &= x^2 + y^2 \\ \Rightarrow ts_0^2 d^2 &= (x_0^2 + y_0^2)d^2 \\ \Rightarrow s_0^2 t &= x_0^2 + y_0^2\,, \end{aligned}$$

where $\gcd(x_0, y_0) = 1$.

Since $p \mid t$, we have $p \mid x_0^2 + y_0^2$, $\gcd(x_0, y_0) = 1$. By the *Descent* step, this means p is the sum of two squares, hence $p \equiv 1 \pmod 4$, by Fermat's two-squares theorem. □

Exercises: Fermat's $p = x^2 + 2y^2$ and $p = x^2 + 3y^2$ claims

Euler was able to prove Fermat's other two claims using similar techniques. The following exercises guide you through the process.

Exercise 2.7. Find a generalisation of the identity

$$(x^2 + y^2)(z^2 + w^2) = (xz \pm yw)^2 + (xw \mp yz)^2$$

to

$$(x^2 + ny^2)(z^2 + nw^2) = (\cdots)^2 + n(\cdots)^2\,,$$

and

$$(ax^2 + cy^2)(az^2 + cw^2) = (\cdots)^2 + ac(\cdots)^2\,.$$

Exercise 2.8.
i) Formulate a version of Lemma 2.5 when a prime $q = x^2 + ny^2$ divides $N = a^2 + nb^2$. Show also the statement holds when $n = 3$ and $q = 4$.
ii) Suppose a prime p divides $N = a^2 + nb^2$, $\gcd(a, b) = 1$. Is it true that $p = x^2 + ny^2$, for some $\gcd(x, y) = 1$? Give a proof or a counterexample. What does this say about our ability to complete the *Descent* step in general?

Exercise 2.9 (Primes of the form x^2+2y^2)**.** In this exercise you will prove Fermat's theorem for primes $p = x^2 + 2y^2$.

i) Suppose that prime $p = x^2 + 2y^2$. By reducing modulo 8, show that $p = 2$ or $p \equiv 1, 3 \pmod 8$.
ii) (Descent for $x^2 + 2y^2$) Suppose prime p divides $x^2 + 2y^2$, with $\gcd(x, y) = 1$. Adapt the proof of Theorem 2.4 to show that $p = a^2 + 2b^2$. Hint: the previous exercise might be useful.
iii) (Reciprocity for $x^2 + 2y^2$) Suppose prime $p \equiv 1, 3 \pmod 8$. Show that $p \mid x^2 + 2y^2$, for some $\gcd(x, y) = 1$, by completing the following steps.
   i) For $p \equiv 1 \pmod 8$, make use of the identity:
   $$x^{8k} - 1 = (x^{4k} - 1)[(x^{2k} - 1)^2 + 2x^{2k}]$$
   ii) For $p \equiv 3 \pmod 8$, argue as follows.

a) (Optional) Show descent works for $x^2 - 2y^2$.
b) Use descent for $x^2 - 2y^2$, to show p does not divide any $N = x^2 - 2y^2$. Conclude that $2 \not\equiv a^2 \pmod{p}$.
c) Show p does not divide any $N = x^2 + y^2$.
d) Write $p = 2m + 1$, and show that no two of the following are congruence, modulo p

$$1^2, 2^2, \ldots, m^2, -1^2, -2^2, \ldots, -m^2 .$$

Hence conclude exactly one of $-a$ and a is a square, modulo p. In particular, show -2 is a square, modulo p.
e) Show that $p \mid x^2 + 2y^2$, with some $\gcd(x, y) = 1$. (Take $x = 1$.)
f) (Optional/research) Is it possible to more directly show $p \equiv 3 \pmod 8$ divides some $x^2 + 2y^2$, $\gcd(x, y) = 1$? For example, by using a polynomial identity like above?

Hence conclude that Fermat's claim about $p = x^2 + 3y^2$ holds.

iv) Find (with proof!) a condition on when a positive integer N can be written in the form $N = x^2 + 2y^2$, $x, y \in \mathbb{Z}$.

Exercise 2.10 (Primes of the form x^2+3y^2)**.** In this exercise you will prove Fermat's theorem for primes $p = x^2 + 3y^2$.

i) Suppose that prime $p = x^2 + 3y^2$. By reducing modulo 3, show that $p = 3$, or $p \equiv 1 \pmod 3$.
ii) (Descent for $x^2 + 3y^2$) Suppose prime p divides $x^2 + 3y^2$, with $\gcd(x, y) = 1$. Show that $p = a^2 + 3b^2$. Warning: the descent step doesn't work for $p = 2$, so if $p \neq a^2 + 3b^2$ you need to produce an *odd* prime $q < p$ not of this form.
iii) (Reciprocity for x^2+3y^2) Suppose prime $p \equiv 1 \pmod 3$. Show that $p \mid x^2+3y^2$, for some $\gcd(x, y) = 1$. Hint:

$$4(x^{3k} - 1) = (x^k - 1)[(2x^k + 1)^2 + 3] .$$

Hence conclude that Fermat's theorem claim about $p = x^2 + 3y^2$ holds.

iv) Find (with proof!) a condition on when a positive integer N can be written in the form $N = x^2 + 3y^2$, $x, y \in \mathbb{Z}$.

CHAPTER 3

Quadratic residues, and quadratic reciprocity

We should try to explain the meaning of 'reciprocity' in the *Reciprocity* steps above. This leads us to the notion of quadratic residues, and quadratic reciprocity.

3.1. Definition

We introduce the Legendre symbol, and prove some of its properties.

Definition 3.1 (Legendre symbol)**.** Let $a \in \mathbb{Z}$ be an integer, and p be an odd prime. Define

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \text{ and } a \equiv m^2 \pmod{p} \\ -1 & \text{if } p \nmid a \text{ and } a \not\equiv m^2 \pmod{p} \end{cases}.$$

So $\left(\frac{a}{p}\right)$ is telling us whether or not a is a square, modulo p.

Example 3.2. Since the squares modulo 17 are

$$(0)^2, (\pm 1)^2, \ldots, (\pm 8)^2 \equiv 0, 1, 2, 4, 8, 9, 13, 15, 16 \pmod{17},$$

we see

$$\left(\frac{15}{17}\right) = 1 \text{ since } 15 \equiv 7^2 \pmod{17},$$
$$\left(\frac{12}{17}\right) = -1.$$

3.2. Alternative criterion

We can give a different description of $\left(\frac{a}{p}\right)$, but first we need to recall a little group theory.

Fact 3.3. If p is an (odd) prime, then $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p-1$. It is generated by some *primitive* element g with order $p-1$.

Lemma 3.4. *Let $a \in \mathbb{Z}$ be an integer, and p be an odd prime. Assume $p \nmid a$, and that $a \equiv g^k \pmod{p}$, where g is the primitive element mentioned above. Then a is a quadratic residue modulo p, i.e. $\left(\frac{a}{p}\right) = 1$, if and only if k is even.*

Proof. We check both directions separately.

'$\Leftarrow$': If $k = 2\ell$ is even, then clearly $a \equiv (g^\ell)^2 \pmod{p}$ is a square.

'⇒': Suppose now that $a \equiv y^2 \pmod{p}$. Write $y = g^m$, some m to see $g^k \equiv a \equiv y^2 \equiv g^{2\ell} \pmod{p}$. Multiplying both sides by g^{-k} gives $g^{2\ell-k} \equiv 1 \pmod{p}$. In the group $(\mathbb{Z}/p\mathbb{Z})^*$, g has order $p-1$, so $p-1 \mid 2\ell-k$. But since p is odd, we also have $2 \mid p-1$. Therefore $2 \mid 2\ell-k$, which implies $2 \mid k$ as required. □

From this lemma, we have the following alternative description of $\left(\frac{a}{p}\right)$, due to Euler.

Theorem 3.5 (Euler's criterion)**.** *Let $a \in \mathbb{Z}$, and let p be an odd prime. Then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}\,.$$

Proof. We split this into the three possible cases as in the definition of $\left(\frac{a}{p}\right)$.

Case $p \mid a$: If $p \mid a$, then both sides reduce to $0 \equiv 0 \pmod{p}$.

Case $a \equiv \square \pmod{p}$: Write $a \equiv m^2 \pmod{p}$. Then we compute

$$a^{(p-1)/2} \equiv m^{2(p-1)/2} \equiv m^{p-1} \equiv 1\,,$$

by Fermat's Little Theorem (or Lagrange's theorem on orders of elements in a group). So both sides reduce to $1 \equiv 1 \pmod{p}$.

Case $a \not\equiv \square \pmod{p}$: Since a is not a square modulo p, we can write $a \equiv g^{2k+1} \pmod{p}$ using the previous lemma. Then

$$a^{(p-1)/2} \equiv g^{(2k+1)(p-1)/2} \equiv g^{(p-1)k} g^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p}\,.$$

What is the value of $b \equiv g^{(p-1)/2}$? Certainly $b^2 \equiv g^{(p-1)} \equiv 1 \pmod{p}$, so $b \equiv \pm 1 \pmod{p}$. But since $p-1 \nmid \frac{1}{2}(p-1)$, it cannot be the case that $b \equiv 1$; the element g has order $p-1$ in the group $(\mathbb{Z}/p\mathbb{Z})^*$. Therefore $b \equiv -1 \pmod{p}$, which completes the proof. □

Remark 3.6. Since $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$, congruence modulo $p \geq 3$ is enough to give *equality* in calculations. We will exploit this fact later.

One useful property of the Legendre symbol, is that it is multiplicative in the top argument.

Proposition 3.7. *The Legendre symbol $\left(\frac{\cdot}{p}\right)$ is multiplicative. That is, for $a, b \in \mathbb{Z}$, and p an odd prime, we have*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\,.$$

Proof. Using Euler's criterion, we have

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}\,.$$

Both sides are in $\{-1, 0, 1\}$, so congruence modulo p implies equality on the level of integers. □

3.3. Solution of the *Reciprocity* step

We can restate the condition $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$ as follows.

Lemma 3.8 (Reciprocity step)**.** *Let n be a non-zero integer, and let p be an odd prime not dividing n. Then*

$$p \mid x^2 + ny^2, \gcd(x, y) = 1 \iff \left(\frac{-n}{p}\right) = 1 .$$

Proof. We prove the two directions separately.

'$\Leftarrow$': Suppose $\left(\frac{-n}{p}\right) = 1$, then we can write $-n \equiv x^2 \pmod p$, for some $x \in \mathbb{Z}$. Now we obtain $x^2 + n \cdot 1^2 \equiv 0 \pmod p$, so $p \mid x^2 + n \cdot 1^2$ and $\gcd(x, y) = 1$.

'$\Rightarrow$': Conversely, suppose $p \mid x^2 + ny^2$, some $\gcd(x, y) = 1$. Then I claim $\gcd(y, p) = 1$. Otherwise $\gcd(y, p) = p$, meaning $p \mid y$. Then $p \mid x^2 + ny^2$ and $p \mid y$ implies $p \mid x$, so $\gcd(x, y) \geq p$, contrary to our assumption. Since $\gcd(y, p) = 1$, we can find $y^{-1} \pmod p$. Then $x^2 + ny^2 \equiv 0 \pmod p$ implies $-n \equiv (xy^{-1})^2 \pmod p$. So $\left(\frac{-n}{p}\right) = 1$. (Since we assumed $p \nmid n$, at the beginning.) □

This means the *Reciprocity* step of the previous proofs boils down to finding congruence conditions on p, which make $\left(\frac{-n}{p}\right) = 1$. This can be done with *quadratic reciprocity*, hence the name!

3.4. Quadratic reciprocity

Lecture 4
10/05/2017

Quadratic reciprocity relates the behaviour of $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ for (distinct) odd primes p, q. Somehow, whether p is a square modulo q is reflected by a related question about whether q is a square modulo p.

Theorem 3.9 (Quadratic Reciprocity)**.** *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} .$$

We will prove this theorem using a lemma of Eisenstein, giving an alternative criterion for $\left(\frac{p}{n}\right)$. (The traditional way to approach to quadratic reciprocity is by way of Gauss's lemma - somehow similar to Eisenstein's lemma, but less elegant(?) to state and prove. Eisenstein's lemma leads to a more geometric argument.)

Lemma 3.10 (Eisensetin)**.** *Let p be an odd prime, and let $n \in \mathbb{Z}$, with $\gcd(n, p) = 1$. Then*

$$\left(\frac{n}{p}\right) = (-1)^s ,$$

where

$$s = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2kn}{p} \right\rfloor$$

PROOF (SKETCH): For $1 \leq k \leq \frac{p-1}{2}$, define

$$r_k \coloneqq 2kn - p\left\lfloor \frac{2kn}{p} \right\rfloor \equiv \left\lfloor \frac{2kn}{p} \right\rfloor .$$

This is the least positive residue of $2nk$, modulo p.

Then

$$\begin{aligned} n^{(p-1)/2} \prod_{k=1}^{(p-1)/2} (2k) &\equiv \prod_{k=1}^{(p-1)/2} r_k \\ &= (-1)^{\sum_k r_k} \prod_{k=1}^{(p-1)/2} (-1)^{r_k} r_k \\ &\equiv (-1)^{\sum_k r_k} \prod_{k=1}^{(p-1)/2} (2k) \pmod{p} . \end{aligned}$$

Can divide out by $\prod_{k=1}^{(p-1)/2}(2k) \pmod{p}$, to obtain

$$(-1)^{\sum_k r_k} \equiv n^{(p-1)/2} \equiv \left(\frac{n}{p}\right) \pmod{p} ,$$

using Euler's criterion, and hence equality $(-1)^{\sum_k r_k} = \left(\frac{n}{p}\right)$ since both sides are in $\{ -1, 0, 1 \}$.

⟦The last congruence follows from the claim that

$$\{ (-1)^{r_k} r_k \}$$

is simply a rearrangement of $\{ 2, 4, \ldots, p-1 \}$. View $(-1)^{r_k} r_k$ as the least positive residue, modulo p. They are all even, and they are distinct because if

$$(-1)^{r_k} r_k = (-1)^{r_\ell} r_\ell ,$$

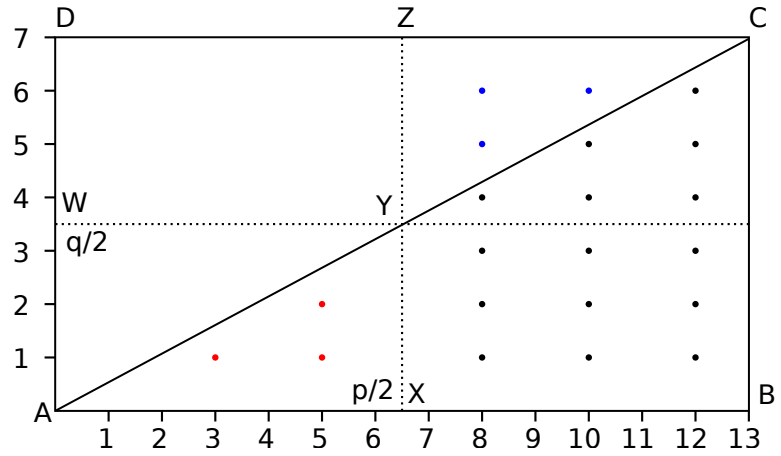
then divide out by n to obtain

$$2k \equiv \pm 2\ell \pmod{p}$$

Since p is odd, this forces $2k \equiv 2\ell \pmod{p}$. Since we have $\frac{p-1}{2}$ even integers in the range $2, \ldots, p-1$, they must just be a rearrangement of $2, \ldots, p-1$.⟧ □

From this, we can prove the law of quadratic reciprocity.

PROOF OF QUADRATIC RECIPROCITY (SKETCH). Consider the following $p \times q$ rectangle



The sum

$$\sum_k \left\lfloor \frac{2qk}{p} \right\rfloor$$

counts the number of lattice points with even x-coordinate in ABC. (The black points.) But since each column $x =$ even has an even number of entries, this is the same, modulo 2, as the number of lattice points with even x-coordinate in ZYC (blue). By rotating, this is the same as the number of lattice points with odd x-coordinate in AXY (red).

So we obtain

$$\left(\frac{q}{p}\right) = (-1)^{\mu},$$

where μ is the total number of lattice points in AXY.

Similarly, $\left(\frac{p}{q}\right) = (-1)^{\nu}$, where ν is the number of lattice points inside AYW.

Finally

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu+\nu} = (-1)^{(p-1)/2\cdot(q-1)/2}$$

since $\mu+\nu$ is just the total number of lattice points inside $AXYW$. (Since $\gcd(p,q) = 1$, the line does not pass through any lattice here.) □

In order to evaluate $\left(\frac{n}{p}\right)$, we also need to know what $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ are. We can use Euler's criterion to evaluate $\left(\frac{-1}{p}\right)$ as a function of p, in terms of congruence conditions on p.

Proposition 3.11 (First supplement to Quadratic Reciprocity)**.** *For p an odd prime, we have*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. By Euler's criterion we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p,$$

but since $\left(\frac{-1}{p}\right), (-1)^{(p-1)/2} \in \{ -1, 0, 1 \}$, congruence modulo $p \geq 3$ implies equality as integers.

Moreover, when $p = 4k+1$, we see $(-1)^{(p-1)/2} = (-1)^{2k} = 1$. When $p = 4k+3$, we see $(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$. Any odd prime p must have exactly one of these two forms. □

We can also evaluate $\left(\frac{2}{p}\right)$, in terms of congruence conditions on p.

Proposition 3.12 (Second supplement to Quadratic Reciprocity)**.** *For p an odd prime, we have*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \end{cases}$$

Proof. It is easy to check that $(-1)^{(p^2-1)/8}$ evaluates as indicated for the different cases modulo 8. We therefore show how $\left(\frac{2}{p}\right)$ evaluates to this.

We use Eisenstein's lemma. Note that

$$s = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{4k}{p} \right\rfloor = \#\{ k \in Z \mid p/4 < k \leq p/2 \} = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor ,$$

since each summand is ≤ 1.

Then just substitute $p = 8m+1, 8m+3, 8m+5, 8m+7$ respectively.

$$p = 8m+1\colon\ s = \lfloor 4m + 1/2 \rfloor - \lfloor 2m + 1/4 \rfloor = 2m \rightsquigarrow \left(\frac{2}{p}\right) = 1^0 = 1$$

$$p = 8m+3\colon\ s = \lfloor 4m + 3/2 \rfloor - \lfloor 2m + 3/4 \rfloor = 2m+1 \rightsquigarrow \left(\frac{2}{p}\right) = (-1)^1 = -1 ,$$

similarly for $p = 8m+5, 8m+7$. □

With quadratic reciprocity, and these two supplements, we can describe when $\left(\frac{a}{p}\right) = 1$, in terms of congruence conditions on p. Factor $a = \pm 2^{e_2} \prod q_i^{e_i}$, and use this to write

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{e_2} \prod_i \left(\frac{q_i}{p}\right)^{e_i} .$$

Use quadratic reciprocity to 'flip' $\left(\frac{q_i}{p}\right)$ to $(-1)^{(p-1)/2}\left(\frac{p}{q_i}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{q_i}\right)$ or to $\left(\frac{p}{q_i}\right)$, as appropriate. Each $\left(\frac{p}{q_i}\right)\pm$ is described by a congruence modulo q_i. Moreover $\left(\frac{-1}{p}\right) = \pm 1$ is described by a congruence modulo 4, and $\left(\frac{2}{p}\right) = \pm 1$ is described by a congruence modulo 8. Select all the possible combinations $\left(\frac{p}{q_i}\right) = \pm 1, \left(\frac{-1}{p}\right) = \pm, \left(\frac{2}{p}\right) = \pm 1$ which give result $\left(\frac{a}{p}\right) = 1$, and find the congruence for each case. Overall, we see that $\left(\frac{a}{p}\right) = 1$ can be described by a congruence modulo $8q_1 \cdots q_n \leq 4a$, at most.

Example 3.13 (Reciprocity for x^2+3y^2)**.** We can use quadratic reciprocity to show $p \equiv 1 \pmod 3$ implies $p \mid x^2 + 3y^2$, for some $\gcd(x, y)$. This gives a different proof of the *Reciprocity* step for $x^3 + 3y^2$.

By Lemma 3.8, we know that for p odd, $p \nmid 3$, we have

$$p \mid x^2 + 3y^2, \gcd(x, y) \iff \left(\frac{-3}{p}\right) = 1\,.$$

By quadratic reciprocity we know

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(p-1)/2\cdot(3-1)/2} = (-1)^{(p-1)/2} = \left(\frac{-1}{p}\right).$$

By rearranging (and realising $\left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$, for $a \nmid p$, since $\left(\frac{a}{p}\right) = \pm 1$), we obtain

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right).$$

Now the non-zero squares modulo 3 are exactly $1^2, 2^2 \equiv 1 \pmod 3$. So $\left(\frac{-3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod 3$.

We now have some sense of why Euler had so much difficulty in proving (the *Reciprocity* steps for) Fermat's $x^2 + 2y^2$ and $x^2 + 3y^2$ claims. He was in the process of discovering/working out quadratic reciprocity!

Exercises

Exercise 3.14. Use (the supplements to) Quadratic Reciprocity to find congruence conditions on p such that $\left(\frac{-2}{p}\right) = 1$. This gives an alternate proof of the *Reciprocity* step for $p \mid x^2 + 2y^2$. How does this compare with Exercise 2.9?

Exercise 3.15. Find congruence conditions on p such that $\left(\frac{a}{p}\right) = 1$ for

i) $a = \pm 5$,
ii) $a = \pm 7$,
iii) $a = \pm 6$,
iv) $a = \pm 10$,
v) $a = \pm 21$.

Hence state the corresponding *Reciprocity* steps for these $x^2 + ny^2$, in these cases.

Exercise 3.16. (Easy cases of Dirichlet's theorem on primes in arithmetic progressions)

i) By directly imitating Euclid's classical proof that there are infinitely many primes, show that there are infinite many primes $p \equiv 3 \pmod 4$. Hint: consider $N_k = 2^2 p_1 p_2 \dots p_k - 1$, where $p_1 = 3, p_2 = 7, \dots$ are the primes of the form $4n + 3$.
ii) By using Lemma 3.8, with $n = 1$, adapt the above proof, to show there are infinitely many primes $p \equiv 1 \pmod 4$.
iii) Show that there are infinitely many primes $p \equiv 1 \pmod 3$ and infinitely many primes $p \equiv 2 \pmod 3$.

Exercise 3.17 (Primes of the form $x^2 - 2y^2$)**.**

i) Show directly that the descent step holds for $x^2 - 2y^2$.
ii) Use quadratic reciprocity to determine when $p \mid x^2 - 2y^2$.

iii) Give a condition on when a prime $p = x^2 - 2y^2$.

Exercise 3.18. In this exercise you will evaluate $\left(\frac{2}{p}\right)$ in a different way, using Euler's criterion.

Consider $(\mathbb{Z}/p\mathbb{Z})$, and suppose we extend it to $F = (\mathbb{Z}/p\mathbb{Z})[\overline{\zeta_8}]$ which includes (the image of) $\zeta_8 = e^{2\pi i/8}$, a primitive 8-th root of 1. Then any element $x \in F$ can be written

$$x \equiv \sum_{i=0}^{7} a_i \zeta_8^i \pmod{p},$$

with addition and multiplication given in the 'natural ways' using the rule $\zeta_8^8 = 1$. (Similar to $\mathbb{C} = \mathbb{R}[i]$, where we write element $x \in \mathbb{R}[i]$ as $x = a + bi$, and use the rule $i^2 = 1$.)

i) Write $\tau = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \zeta_8^7$. Show that $\tau^2 = 2$, hence show

$$\tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{p}.$$

ii) Using the binomial theorem, show that

$$\tau^p \equiv \zeta_8^p + \zeta_8^{-p} \pmod{p}$$

iii) For $p \equiv \pm 1, \pm 3 \pmod 8$, evaluate τ^p, and check the result can be written as

$$\tau^p = (-1)^{(p^2-1)/8}\tau \pmod{p}$$

iv) Conclude that

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

CHAPTER 4

Quadratic forms, definitions and properties

Lecture 5
17/05/2017

Using quadratic reciprocity, we have a systematic way of completing the *Reciprocity* set in Euler's proofs. However, the descent step fails in general.

Example 4.1. We have that $2, 3 \mid 1^2 + 5 \times 1^2$, yet we cannot write $2 = x^2 + 5y^2$, and we cannot write $3 = x^2 + 5y^2$. (You should have discovered something like this in Exercise 2.8 ii).) However, we can say

$$p \mid x^2 + 5y^2 \Rightarrow p = x^2 + 5y^2 \text{ or } p = 2x^2 + 2xy + 3y^2 \,.$$

We need a more systematic method of studying the *Descent* step, and 'classifying' the failures like above. For that purpose, we introduce and study quadratic forms.

4.1. General definitions around quadratic forms

We try to state the definitions rather generally, at first. But we will focus mainly on the case of 'integral binary quadratic forms', so think about $n = 2$ and $R = \mathbb{Z}$ if you prefer.

Let R be some ring (with unity $1 \in R$) inside some field K.

Definition 4.2 (Quadratic Form)**.** A quadratic form over R is a homogeneous polynomial

$$\begin{aligned} f(x_1, \ldots, x_n) &\coloneqq \sum_{1 \le i \le j \le n} r_{i,j} x_i x_j \\ &= r_{1,1}x_1^2 + r_{1,2}x_1x_2 + \cdots \end{aligned}$$

of degree 2, with coefficients $r_{i,j} \in R$.

- If $f(x_1, \ldots, x_n)$ is a quadratic form in n variables, we call it an *n-ary* quadratic form (binary, ternary, quaternary, ...)

Representations: Given a quadratic form $f(x_1, \ldots, x_n)$ over some ring R, we can substitute values $a_i \in R$ to evaluate $f(a_1, \ldots, a_n)$.

- Fix some $r \in R$. If there exists values $\underline{\mathbf{a}} = (a_1, \ldots, a_n) \in R^n$, such that $f(a_1, \ldots, a_n) = r$, we say f *represents* r.

Matrix: Given a quadratic form $f(\underline{\mathbf{x}}) = f\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) \coloneqq f(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} f_{i,j} x_i x_j$, we can write $f(\underline{\mathbf{x}})$ as a matrix equation

$$f(\underline{\mathbf{x}}) = \underline{\mathbf{x}}^\top \underbrace{\begin{pmatrix} f_{1,1} & \cdots & \frac{1}{2}f_{i,j} \\ \vdots & \ddots & \vdots \\ \frac{1}{2}f_{i,j} & \cdots & f_{n,n} \end{pmatrix}}_{=: F} \underline{\mathbf{x}} \,.$$

(View $\underline{\mathbf{x}}$ as a column vector!) We call F the *(Gram) matrix* of the form f.

Notice that the matrix may contain coefficients in $\frac{1}{2}R$, not just R. (We assume $\operatorname{char} K \neq 2$, for simplicity!)

Now from F, we can make the following definitions

- We call $\det(F)$, the *determinant* $\det(f)$ of f.
- If $f(x, y) = ax^2 + bxy + cy^2$ is a binary quadratic form, with
$$F = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix},$$
then $\det(M) = ac - \frac{1}{4}b^2$. The *discriminant* of f is $-4\det(M) = b^2 - 4ac$.
- If $\det(M) \neq 0$, we call f *regular*, *non-singular*, or *non-degenerate*.

4.2. Defintions around integral quadratic forms

We focus mainly on the case $R = \mathbb{Z}$, and within this on binary quadratic forms, at least in the first part of this course. Later we may look at quadratic forms in more variables: ternary quadratic forms, 4-ary quadratic forms, ...

- We call quadratic forms over $R = \mathbb{Z}$ *integral*.
- If $\frac{1}{2}f_{i,j} \in \mathbb{Z}$, so the 'off-diagonal' terms $f_{i,j}x_ix_j$ have '*even*' coefficient, and the matrix has entries in $\mathbb{Z}$, then we call the form *classically* integral.

Remark 4.3. This distinction is the source of much debate and consternation. The notion of classically integral does back to Gauss, who assumed the 'off-diagonal' coefficients were even. For qualitative results, this distinction is not so important because we have the following result

$$f \text{ integral} \Rightarrow 2f \text{ classically integral}$$

Over $R = \mathbb{Z}$, we can impose extra conditions involving gcd

- If $\gcd(r_{i,j}) = 1$, we say f is primitive.
- If $r \in \mathbb{Z}$, and there exists $\underline{\mathbf{a}} \in \mathbb{Z}^n$ such that $f(\underline{\mathbf{a}}) = r$, and $\gcd(\underline{\mathbf{a}}) = 1$, we say f represents a *properly*.

We can look at all the (sign of) values f attains.

- If $f(\underline{\mathbf{a}}) \geq 0$, for all $\underline{\mathbf{a}} \in \mathbb{Z}^n$, we say f is *positive semi-definite*.
- If $f(\underline{\mathbf{a}}) > 0$, for all $\underline{\mathbf{a}} \neq \underline{\mathbf{0}} \in \mathbb{Z}^n$, we say f is *positive definite*.
- Similarly, for *negative (semi-)definite*.
- If $f(\underline{\mathbf{a}}) > 0$ for some $\underline{\mathbf{a}} \neq 0 \in \mathbb{Z}^n$, and $f(\underline{\mathbf{a}}') < 0$ for some $\underline{\mathbf{a}}' \neq 0 \in \mathbb{Z}^n$, we say f is *indefinite*.

For integral binary quadratic forms, we have the following result connecting definiteness and the discriminant.

Proposition 4.4. *Suppose $f(x, y) = ax^2 + bxy + cy^2$ is a binary quadratic form, with discriminant $D = b^2 - 4ac$.*

i) Then f is indefinite iff $D > 0$.
ii) Then f is positive (respectively negative) definite iff $D < 0$ and $a > 0$ (respectively $a < 0$).

Proof. Exercise. Hint: complete the square. □

4.3. Equivalence of quadratic forms

As with (almost) all mathematical objects, we want to notion that two such quadratic forms are 'equivalent'. What should equivalence look like here? The most obvious thing we can do is a change of variables $x_i \mapsto F_i(x_1, \dots, x_n)$. The result of this should be another quadratic form with R coefficients, so the function F_i should be linear, i.e. $x_i \mapsto \sum_j b_{i,j}x_j$, with $b_{i,j} \in R$. So we can represent this change of variables by a matrix $B \in M_{n\times n}(R)$, and $\underline{\mathbf{x}} \mapsto B\underline{\mathbf{x}}$. Moreover, we want to be able to undo this change of variables (to get an equivalence relation!), so B should be invertible, i.e. $B \in \mathrm{GL}_n(R)$.

Definition 4.5 (Equivalence)**.** Let f, g be two n-ary quadratic forms over R. Suppose that there is some matrix $B \in \mathrm{GL}_n(R)$, such that $f(B\underline{\mathbf{x}}) = g(\underline{\mathbf{x}})$. Then we say f is ($\mathrm{GL}_n(R)$-)*equivalent* or just R-*equivalent* to g.

On the level of matrices, we have that

$$f(B\underline{\mathbf{x}}) = (B\underline{\mathbf{x}})^\top F(B\underline{\mathbf{x}}) = \underline{\mathbf{x}}^\top (B^\top FB)\underline{\mathbf{x}}\,,$$

so the matrix G of g is related to the matrix F of f by $G = B^\top FB$.

4.3.1. Examples of equivalence. The qualitative behaviour of quadratic forms, under $\mathrm{GL}_n(R)$-equivalence depends very strongly on the ring R

Example 4.6 (Over $\mathbb{R}$)**.** Every n-ary quadratic form over $\mathbb{R}$ is equivalence to a unique form

$$x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2\,.$$

This is (basically) Sylvester's law of inertia in linear algebra. It comes from repeatedly completing the square.

For example, consider

$$x^2 + xy + 2y^2 + 2xz + 3yz - z^2\,.$$

We complete the square in x, to obtain

$$\begin{aligned}
&= (x + \tfrac{1}{2}y + z)^2 + \tfrac{7}{4}y^2 + 3yz - 2z^2 \\
&= (x + \frac{1}{2}y + z)^2 + (\tfrac{\sqrt{7}}{2}y + \tfrac{2}{\sqrt{7}}z)^2 - (\tfrac{3\sqrt{2}}{\sqrt{7}}z)^2 \\
&\rightsquigarrow X_0^2 + X_1^2 - X_3^2
\end{aligned}$$

using the change of variables

$$\begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} & 1 \\ 0 & \frac{\sqrt{7}}{2} & \frac{2}{\sqrt{7}} \\ 0 & 0 & \frac{3\sqrt{2}}{\sqrt{7}} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}\,.$$

By construction, this change of variables matrix is upper triangular with non-zero diagonal entries. So it is invertible. This shows the forms are equivalent. (More precisely, this shows that $X_1^2 + X_2^2 - X_3^2$ is $\mathrm{GL}_3(\mathbb{R})$-equivalent to $x^2 + xy + 2y^2 + 2xz + 3yz - z^2$.

Example 4.7 (Over $\mathbb{C}$)**.** Over $\mathbb{C}$, every n-ary quadratic form is equivalent to

$$x_1^2 + x_2^2 + \cdots + x_r^2\,,$$

since we can change $-x_k^2 = (ix_k)^2$, to obtain a plus sign.

Lecture 6
24/05/2017

So the situation of quadratic forms over $\mathbb{R}$, and over $\mathbb{C}$ is (in some sense) completely understood. The situation over $\mathbb{Z}$ is *much* more interesting!

Example 4.8 (Over $\mathbb{Z}$)**.** We cannot always convert to 'diagonal' form, so it becomes more difficult to determine when two quadratic forms are equivalent.

- Consider the following.
$$x^2 + 5y^2 \text{ and } 9x^2 + 32xy + 29y^2$$
are equivalent via $B = \left(\begin{smallmatrix} 2 & 3 \\ 1 & 2 \end{smallmatrix}\right)$. But $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ are not equivalent. How can we see this? Suppose
$$f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)) = 2x^2 + 2xy + 3y^2\,.$$
Expand out and gather coefficients to get
$$(a^2 + 5c^2)x + (2ab + 10cd)xy + (b^2 + 5d^2) = 2x^2 + 2xy + 3y^2$$
We have to find integers a, b, c, d such that (in particular) $a^2 + 5c^2 = 2$. But this is not possible.
- Consider the following.
$$f(x, y) = x^2 - 3y^2 \text{ and } g(x, y) = -x^2 + 3y^2$$
are not equivalent. Suppose
$$f\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)\right) = g(x, y)\,,$$
then we obtain
$$(a^2 - 3c^2)x^2 + (2ab - 6cb)xy + (b^2 - 3d^2)y^2 = -x^2 + 3y^2\,.$$
So we need $a^2 - 3c^2 = -1$, with $a, c \in \mathbb{Z}$. It turns out that there is no solution to this, but this is not so obvious. We can see this by reducing modulo 3, giving $a^2 \equiv -1 \equiv 2 \pmod 3$. But the squares modulo 3 are $0^2, (\pm 1)^2 \equiv 0, 1 \pmod 3$.

4.3.2. Properties of $\mathrm{GL}_n(R)$-equivalence. Some properties of $\mathrm{GL}_n(R)$-equivalence can help answer questions about when two quadratic forms are equivalent. Here we give some of the properties. The proofs are (relatively straightforward) exercises.

Proposition 4.9. *$\mathrm{GL}_n(R)$-equivalence is an equivalence relation on n-ary quadratic forms over R.*

- *The form f is equivalent to f,*
- *If f is equivalent to g, then g is equivalent to f, and*
- *If f equivalent to g, and g equivalent to h, then f equivalent to h.*

Proposition 4.10. *Suppose f and g are $\mathrm{GL}_n(R)$-equivalent quadratic forms.*

- *Then $\det(f)$ and $\det(g)$ differ by a square:*
$$\det(f) = \lambda^2 \det(g)\,,$$
for some $\lambda \neq 0 \in R^*$.
- *If $R = \mathbb{Z}$, then*
$$\det(f) = \det(g)\,,$$
and so $\mathrm{GL}_n(\mathbb{Z})$-equivalent integral binary quadratic forms have the same discriminant.

Proposition 4.11. *Suppose f and g are $\mathrm{GL}_n(R)$-equivalent quadratic forms.*

- *Then f represents $r \in R$ if and only if g represents $r \in R$.*
- *If $R = \mathbb{Z}$, then f represents $n \in \mathbb{Z}$ properly, if and only if g represents $n \in \mathbb{Z}$ properly.*

Proposition 4.12. *Suppose f and g are $\mathrm{GL}_n(\mathbb{Z})$-equivalent quadratic forms.*

- *Then f is primitive if and only if g is primitive, and*
- *f is classically integral if and only if g is classically integral.*

Proposition 4.13. *Suppose f and g are integral n-ary quadratic forms. Then $2f$ and $2g$ are classically integral, and*

$$f \text{ } \mathrm{GL}_n(\mathbb{Z})\text{-equivalent to } g \text{ if and only if } 2f \text{ } \mathrm{GL}_n(\mathbb{Z})\text{-equivalent to } 2g.$$

4.3.3. Proper equivalence for integral quadratic forms. When $R = \mathbb{Z}$, we can further refine the notion of equivalence. Any matrix in $\mathrm{GL}_n(\mathbb{Z})$ has determinant $+1$ or -1. These lead to the notions of proper and improper equivalence.

Definition 4.14. If there exists $B \in \mathrm{SL}_n(\mathbb{Z})$ (with $\det(B) = 1 > 0$) and $f(B\underline{\mathbf{x}}) = g(\underline{\mathbf{x}})$, we say f and g are *properly* equivalent. Otherwise, they are *improperly* equivalent.

Example 4.15. The forms $f(x, y) = 3x^2 + 2xy + 5y^2$ and $g(x, y) = 3x^2 - 2xy + 5y^2$ improperly equivalent via $B = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Are they properly equivalent? This is perhaps a more subtle question, and we will develop better techniques for dealing with it shortly. Nevertheless: expand out

$$f(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\underline{\mathbf{x}}) = 3x^2 - 2xy + 5y^2$$

The x^2 coefficient requires $3a^2+2ac+5c^2 = 3$. The only solutions are $a = \pm 1, c = 0$. Similarly, the y^2 coefficient requires $3b^2 + 2bd + 5d^2 = 5$, and the only solutions are $b = 0, d = \pm 1$.

Only 2 of these 4 choices give $\mathrm{SL}_2(\mathbb{Z})$ matrices, namely

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Both of which send f to f. So f and g are not properly equivalent.

Remark 4.16. Since $\mathrm{SL}_n(\mathbb{Z}) < \mathrm{GL}_n(\mathbb{Z})$ is a subgroup, $\mathrm{SL}_n(\mathbb{Z})$-equivalence is also an equivalence relation. The properties above all have corresponding versions for $\mathrm{SL}_n(\mathbb{Z})$-equivalence.

Remark 4.17. Proper equivalence is the better notion of equivalence when we study integral quadratic forms. (It has better properties in terms of composition, and connections ot ideals in quadratic number fields.) If we speak of equivalent integral quadratic forms, we always mean *proper* equivalence, unless otherwise specified.

Proposition 4.18. *Suppose f, g, h are integral quadratic forms. If f and g are improperly equivalent, and g and h are improperly equivalent. Then f and h are properly equivalent.*

4.4. Solution to the *Descent* step

With our knowledge of quadratic forms, we can now give a 'solution' to the descent step of the proof in general. This is a solution, in so much as it gives us a result in all cases, but since we have generally $p \mid x^2 + ny^2$ does not imply p is of the form $x^2 + ny^2$ (e.g. $p = 3 \mid 6 = 1^2 + 5 \cdot 1^2$, but $p \neq x^2 + 5y^2$), we still do not solve the our problem *completely*. From now on we restrict to integral binary quadratic forms.

4.4.1. Proper equivalence and proper representation. There is a close relationship between proper representation, and proper equivalence of binary quadratic forms.

Lemma 4.19. *A binary quadratic form $ax^2+bxy+cy^2$ properly represents an integer m if and only if $f(x, y)$ is properly equivalence to the form $mx^2 + b'xy + c'y^2$, for some $b', c' \in \mathbb{Z}$.*

Proof. We show the two directions separately.

'$\Leftarrow$': Certainly $mx^2 + b'xy + c'y^2$ properly represents m by taking $(x, y) = (1, 0)$.

'$\Rightarrow$'. Now, let $f(p, q) = m$ be a proper representation of m. Since $\gcd(p, q) = 1$, we can find (by the Euclidean algorithm/Bezout) r, s so that $ps - qr = 1$. THen

$$\begin{aligned} f\left(\left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)\right) &= (ap^2 + bpq + cq^2)x^2 + (2apr + bqr + bps + 2cqs)xy \\ &\quad + (ar^2 + brs + cs^2)y^2 \\ &= \underbrace{f(p, q)}_{=m} x^2 + b'xy + c'y^2 \,. \end{aligned}$$

□

4.4.2. Representation by a binary quadratic form of discriminant D. We finally now can finally give a condition on which determines which primes certain integral binary quadratic forms represent.

Lemma 4.20. *Let D be a discriminant, and m an odd integer relatively prime to D. Then m is properly represented by a primitive binary quadratic form of discriminant D if and only if D is a square modulo m.*

Proof. We show the two directions separately.

'$\Rightarrow$'. Let $m = f(x, y)$ be a proper representation of m. Then by Lemma 4.19, we can assume $f(x, y) = mx^2 + bxy + cy^2$. Then $D = b^2 - 4mc$, and so $D \equiv b^2 \pmod{m}$.

'$\Leftarrow$': Suppose $D \equiv b^2 \pmod{m}$. Since m is odd, one can assume D and b have the same parity: change $b \mapsto b + m$ if necessary.

Notice that the discriminant of a quadratic form necessarily satisfies $D \equiv 0, 1 \pmod{4}$, as $D = b^2 - 4ac \equiv b^2 \equiv 0, 1 \pmod{4}$. We therefore have $D \equiv b^2 \pmod{4m}$. (We must have $D \equiv b^2 + km \pmod{4m}$, but reducing modulo 4 shows that $k \equiv 0 \pmod{4}$.)

So write $D = b^2 - 4mc$, for some c. Then $mx^2 + bxy + cy^2$ properly represents m, and has discriminant D. Moreover, it is primitive, since m was assumed to be relatively prime to D. □

And as a corollary, if we restrict to primes, we obtain.

Corollary 4.21 (Descent step)**.** *Let D be a discriminant, and let p be an odd prime not dividing D. Then*

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

if and only if p is represented by a primitive binary quadratic form of discriminant D.

Proof. Modulo an odd prime p, we know D if a square if and only if $\left(\frac{D}{p}\right) = 1$. Any representation of a prime is proper, otherwise $\gcd(x, y) = q > 1$, meaning $q^2 \mid f(x, y) = p$. □

For this corollary to be useful for explicit results, we need more knowledge of the (equivalence classes of) primitive integral binary quadratic forms of discriminant D. We study this problem in more detail next: we show that the number of equivalence classes is finite, and give procedures to list representatives of these equivalence classes.

Example 4.22. In the next chapter, we will show that $x^2 + 3y^2$ is the only binary quadratic form of discriminant $D = -12$ up to (proper) equivalence. We can therefore easily prove Fermat's $x^2 + 3y^2$ theorem as follows.

From a computation in Example 3.13, using Quadratic reciprocity Theorem 3.9, we established that for a prime p

$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \pmod 3 .$$

From Corollary 4.21, we know that for an odd prime $p \nmid D = -12$

$$\left(\frac{-12}{p}\right) = 1 \iff \begin{array}{c} p \text{ is represented by a primitive binary} \\ \text{quadratic form of discriminant } D = -12 \end{array}$$

But $\left(\frac{-12}{p}\right) = \left(\frac{2}{p}\right)^2\left(\frac{-3}{p}\right) = \left(\frac{-3}{p}\right)$. And since $x^2 + 3y^2$ is the only primitive binary quadratic form of discriminant $D = -12$, we see p is represented by some form if and only if it is represented by $x^2 + 3y^2$.

Thus for $p \neq 2, 3$ we have

$$p \equiv 1 \pmod 3 \overset{\text{QR}}{\iff} \left(\frac{-3}{p}\right) = 1 \overset{\text{Cor}}{\iff} p = x^2 + 3y^2 .$$

Exercises

Exercise 4.23. Let $f(x_1, \ldots, x_n)$ be a quadratic form (with coefficients over some ring $R \supset \mathbb{Z}$). Show that

$$f \text{ is integral implies } 2f \text{ is } \textit{classically} \text{ integral.}$$

Exercise 4.24. Suppose that $f(x_1, \ldots, x_n)$ is a non-primitive integral quadratic form. Show that $f(x_1, \ldots, x_n)$ can represent at most one prime.

Exercise 4.25. Suppose $f(x,y) = ax^2 + bxy + cy^2$ is an integral binary quadratic form, with discriminant $D = b^2 - 4ac$.

i) Show that f is indefinite if $D > 0$.
ii) Show that f is positive (respectively negative) definite if $D < 0$ and $a > 0$ (respectively $a < 0$).
iii) What happens when $D = 0$? What happens if $D > 0$ is a perfect square?

Hint: Complete the square!

Exercise 4.26. Let $f(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form, of discriminant $D = b^2 - 4ac$. Show that $D \equiv 0, 1 \pmod 4$, and that every such D occurs.

Exercise 4.27. Show that R-equivalence is an equivalence relation on n-ary quadratic forms over R. Show

- The form f is equivalent to f,
- If f is equivalent to g, then g is equivalent to f, and
- If f equivalent to g, and g equivalent to h, then f equivalent to h.

Check also for $\mathrm{SL}_n(\mathbb{Z})$-equivalence, when $R = \mathbb{Z}$.

Exercise 4.28. Suppose f and g are $\mathrm{GL}_n(R)$-equivalent quadratic forms. Show

- $\det(f)$ and $\det(g)$ differ by a square
$$\det(f) = \lambda^2 \det(g)\,,$$
for some $\lambda \neq 0 \in R^*$. How does λ arise from the equivalence of f to g?
- For $R = \mathbb{Z}$, conclude $\det(f) = \det(g)$, and explain why $\mathrm{GL}_n(\mathbb{Z})$-equivalent integral binary quadratic forms have the same discriminant.

Exercise 4.29. Suppose f and g are $\mathrm{GL}_n(R)$-equivalent quadratic forms. Show

- f represents $r \in R$ if and only if g represents $r \in R$.
- For $R = \mathbb{Z}$, f represents $n \in \mathbb{Z}$ properly, if and only if g represents $n \in \mathbb{Z}$ properly. Check also for $\mathrm{SL}_n(\mathbb{Z})$-equivalence.

Use this to show that
$$x^2 + 14y^2 \ , \ 2x^2 + 7y^2 \text{ and } 3x^2 + 2xy + 5y^2$$
are not $\mathrm{GL}_n(\mathbb{Z})$-equivalent.

Exercise 4.30. Suppose f and g are integral n-ary quadratic forms. Then $2f$ and $2g$ are classically integral. Show that

f is $\mathrm{GL}_n(\mathbb{Z})$-equivalent to g if and only if $2f$ is $\mathrm{GL}_n(\mathbb{Z})$-equivalent to $2g$.

Check also for $\mathrm{SL}_n(\mathbb{Z})$-equivalence.

Exercise 4.31. Suppose f, g, h are integral quadratic forms. Suppose f and g are improperly equivalent, and g and h are improperly equivalent. Show that f and h are *properly* equivalent.

CHAPTER 5

The class number, and reduction of binary quadratic forms

Lecture 7
31/05/2017

It is a *remarkable* fact that for a fixed number of variables n, and a fixed determinant d, the number of equivalence classes of equivalent integral n-ary quadratic form of determinant d is *finite*! (This holds for proper equivalence, or improper equivalence. And for integral or classically integral. And for primitive, or not-necessarily primitive.)

Definition 5.1. Write $h(D)$ for the number of proper equivalence classes of positive definite primitive integral binary quadratic forms of discriminant $D < 0$.

Write $h^+(D)$ for the number of proper equivalence classes of indefinite primitive integral binary quadratic forms of discriminant $D > 0$.

Remark 5.2. The plus in the notation refers to the fact that we (sort of have) a 'narrower' notion of equivalence in the indefinite case: we do not identify $-ax^2 + bxy - cy^2$ and $ax^2 + bxy + cy^2$ unless they are properly equivalent. Whereas in the positive definite case, we always ignore the negative-definite forms (so we can think of identifying the positive definite form $ax^2 + bxy + cy^2$ and negative definite forms $-ax^2 + bxy - cy^2$.

In the indefinite case, we can write $h(D)$ to mean always identify these forms. Sometimes we have $h(D) = h^+(D)$ and sometimes only $h^+(D) = 2h(D)$.

Whether we have $= 1\times$ or $= 2\times$ depends on whether a solution to the equation $x^2 - ny^2 = -4$ exists. If we focus on the case $D = -4n$, then this is equivalent to whether a solution to $x^2 - ny^2 = -1$ exists. If such a solution exists, then we have $= 1\times$, otherwise we have $= 2\times$.

The existence of a solution to $x^2 - ny^2 = -1$ means that the *fundamental unit* of the order $\mathbb{Z}[\sqrt{n}] \subset \mathcal{O}_K$ has negative norm. This is only the tip of the connection between quadratic forms and quadratic number fields. (See handout 2)

Example 5.3. We know that $x^2 - 3y^2$ and $-x^2 + 3y^2$ are not equivalent, and we proved this by seeing that $x^2 - 3y^2 = -1$ has no solution. But since $x^2 - 5y^2 = -1$ has solution $(x, y) = (2, 1)$, we can write

$$\left(\begin{smallmatrix} 2 & -5 \\ 1 & -2 \end{smallmatrix}\right) \cdot (x^2 - 5y^2) = -x^2 + 5y^2 \,.$$

This can be generalised.

We will prove this finiteness in the case of $n = 2$ by means of *reduced* forms. We will give a procedure which lists a representative of each proper-equivalence class. The case of positive-definite forms is qualitatively different from the case of indefinite forms, so we treat them separately. We also say perhaps a few words about the general case of n-ary forms.

5.1. Reduction of positive definite forms

We introduce a notion of a positive-definite binary quadratic form being reduced. It may be convenient to write $(a,b,c) = ax^2+bxy+cy^2$. We shall also write $B \circ f$ to mean the action of matrix B on form f, i.e. $(B\circ f)(\underline{\mathbf{x}}) = f(B\underline{\mathbf{x}})$.

Definition 5.4. Let $f(x,y) = ax^2+bxy+cy^2$ be a positive-definite binary quadratic form of discriminant $D<0$. We say that $f(x,y)$ is *reduced* if

- $|b| \le a \le c$, and
- if $|b| = a$ then $b \ge 0$, and
- if $a = c$, then $b \ge 0$.

The claim now is that every positive-definite binary quadratic form of fixed discriminant $D<0$ is properly equivalent to a unique reduced form.

Theorem 5.5. *In every proper equivalence class of positive-definite binary quadratic forms of fixed discriminant $D<0$, there is a unique reduced form.*

Proof. Firstly we show there is a reduced form, secondly we show it is unique.

Existence: Since the form is positive-definite, we have $a>0$. By the well-ordering principle, each proper equivalence class of binary quadratic forms contains a form with minimal a.

Suppose $ax^2+bxy+cy^2$ is such a form. We have $a \le c$, otherwise $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ sending $x \mapsto -y$ and $y \mapsto x$ changes $ax^2+bxy+cy^2$ into $cx^2-bxy+ay^2$, with smaller x^2-coefficient.

The matrix $T^k = \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ sends $x \mapsto x+ky$, and $y \mapsto y$. So transforms $ax^2+bxy+cy^2$ into $ax^2+(2ak+b)xy+(ak^2+bk+c)y^2$. This lets us put the xy-coefficient into the range $(-a,a]$, giving $-a < b \le a$, so $|b| \le a$.

We need to check whether the edge cases as satisfied. By construction, if $|b| = a$, then $b = a > 0$. Moreover, if $a = c$, we can ensure $b \ge 0$ by transforming with $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ sending $ax^2+bxy+cy^2$ to $cx^2-bxy+ay^2$.

⟦We can obtain an explicit algorithm for reduction, as follows. If $c<a$, use S to get smaller a coefficient. Then use T^k to put $-a < b \le a$. By keeping track of which matrices T^k, S we use, and in which order, we can give an explicit $\mathrm{SL}_2(\mathbb{Z})$-matrix which shows f is equivalent to the reduced form $\widetilde{f}$. If you know about modular forms, this reduction procedure is closely connected with finding fundamental domain for $\mathfrak{H}/\mathrm{SL}_2(\mathbb{Z})$. ⟧

Uniqueness: Now we need to show that if two reduced forms $ax^2+bxy+cy^2$ and $a'x^2+b'xy+c'y^2$ are equivalent, then $a'=a$, $b'=b$, and $c'=c$.

Firstly we show that a is minimal for a reduce form. Acting by $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ sends $a \mapsto ap^2+bpr+cr^2$. Since $|b| \le a \le c$, we can write

$$ap^2+bpr+cr^2 = ap^2\big(1+\underbrace{\tfrac{b}{a}}_{-1<\frac{b}{c}\le 1}\tfrac{r}{p}\big)+cr^2 = ap^2+cr^2\big(1+\underbrace{\tfrac{b}{c}}_{-1<\frac{b}{c}\le 1}\tfrac{p}{r}\big),$$

Moreover, we must have $\gcd(p,r)=1$, to get $\det=1$. So $p=0$ implies $r=\pm1$, and $r=0$ implies $p=\pm1$.

If $p=0$, we get $a\mapsto c\geq a$.

If $r=0$, we get $a\mapsto a\geq a$.

So we can assume $p,r\neq 0$. Then one of $\frac{r}{p}$ and $\frac{p}{r}$ is in $(-1,1]$. If the former, we get

$$a\mapsto ap^2(1+\underbrace{\frac{b}{a}\frac{r}{p}}_{\in(-1,1]})+cr^2>ap^20+cr^2\geq a.1^2=a\,,$$

if the latter, we get

$$a\mapsto ap^2+cr^2(1+\underbrace{\frac{b}{c}\frac{p}{r}}_{\in(-1,1]})>ap^2+cr^20\geq a.1^2=a\,.$$

This shows that the x^2-coefficient is minimal for a reduced form. So $a=a'$.

Which forms are equivalent to $ax^2+bxy+cy^2$, and have x^2-coefficient also a? We read off the possibilities from the inequalities above:

- $(p,r)=(0,\pm1)$ with $a=c$.
- Or $(p,r)=(\pm1,0)$

This gives matrices

$$\begin{pmatrix}0&\pm1\\ \pm1&k\end{pmatrix},\begin{pmatrix}\pm1&k\\ 0&\pm1\end{pmatrix}$$

Since $-I_2$ acts as the identity on $f(x,y)$, i.e. $f(-x,-y)=f(x,y)$, we can assume the signs are $+$. The matrix $\left(\begin{smallmatrix}0&1\\1&k\end{smallmatrix}\right)$ is only a valid possibility if $a=c$. But if $a=c$, then its affect on b is exactly the same as for the other matrix. So without loss of generality, the only transformation we need to consider is

$$\begin{pmatrix}0&\pm1\\ \pm1&k\end{pmatrix}$$

sending $x\mapsto x+ky$, and $y\mapsto y$ and $b\mapsto b+2ak$. To get another reduced form, we must take $k=0$, else $b+2ak$ is outside the required range. So we have only the identity matrix. Hence $b=b'$, and $c=c'$. □

From this, we obtain a bound on x^2-coefficient in terms of the discriminant $D<0$, for reduced positive-definite binary quadratic forms.

Corollary 5.6. *Let $f(x,y)=ax^2+bxy+cy^2$ be a reduced positive-definite binary quadratic form of discriminant $D<0$. Then*

$$a\leq\sqrt{\tfrac{-D}{3}}$$

Proof. Since $f(x,y)$ is reduced, we know $c\geq a\geq|b|$. So $a^2\geq b^2$. Substituting this into the formula for the discriminant, we find

$$-D=4ac-b^2\geq 4a^2-a^2=3a^2\,,$$

giving the required bound. □

From this, we obtain the easy corollary that there are only a finite number of proper equivalence classes of positive-definite binary quadratic forms of fixed discriminant $D < 0$.

Corollary 5.7 (Finiteness of the 'class number')**.** *The number $h(D)$ of proper equivalence classes of positive-definite binary quadratic forms of fixed discriminant $D < 0$ is finite.*

PROOF. Each proper equivalence class contains a unique reduced form $ax^2 + bxy + cy^2$, with $|b| \leq a \leq c$. If D is fixed, we can compute $c = \frac{b^2-D}{4a}$ in terms of a and b.

Moreover, the number of possible a, b is finite, using the bound $|b| \leq a \leq \sqrt{-D/3}$ from the previous corollary. Hence the number of possible reduce forms of discriminant D is finite, and so is the number of proper equivalence classes. □

We can now easily list a representative of the proper equivalence class of positive-definite binary quadratic forms of discriminant $D < 0$. Since primitive forms are only equivalent to primitive forms, we can restrict to equivalence classes of primitive positive-definite binary quadratic forms by throwing away any non-primitive ones from our final result.

Example 5.8. List the primitive positive-definite binary quadratic forms of discriminant $D = -12$.

We have the bound $1 \leq a \leq \sqrt{-D/3} = 2$. We list all $|b| \leq a$, for $a = 1, 2$. Then compute $c = \frac{b^2+12}{4a}$ to get the following table.

a	b	c	Integral?	Reduced?	Primitive?
1	-1	$\frac{13}{4}$			
1	0	3	✓	✓	✓
1	1	$\frac{13}{4}$			
2	-2	2	✓		
2	-1	$\frac{13}{8}$			
2	0	$\frac{3}{2}$			
2	1	$\frac{13}{8}$			
2	2	2	✓	✓	

So there are two classes of positive-definite binary quadratic forms of discriminant $D = -12$.

$$x^2 + 3y^2\,, \text{ and } 2x^2 + 2xy + 2y^2$$

Only the first class is primitive, so $h(-12) = 1$.

A calculator is available online at `http://www.numbertheory.org/php/classnoneg.html` to compute the class number, and reduced equivalence classes of (primitive) positive-definite binary quadratic forms of discriminant $D < 0$.

5.2. Reduction of indefinite forms

With indefinite forms, the notion of a reduced form is more subtle. We have a definition of *reduced*, but it turns out that there is not (necessarily) a single unique reduced form in each proper equivalence class. However, the reduced forms are arranged naturally in a cycle structure. We only sketch the details of this reduction.

We can imitate the proof of Theorem 5.5 to see immediately the first part of the following proposition.

Proposition 5.9. *Every indefinite quadratic form of some discriminant D is equivalent to one of the form $ax^2+bxy+cy^2$ with $|b| \leq |a| \leq |c|$. Moreover, such a form has $ac<0$ and $|a| \leq \frac{1}{2}\sqrt{D}$.*

Proof. Exercise! □

An immediate corollary is that the number of proper equivalence classes of indefinite binary quadratic forms of discriminant $D>0$ is finite

Corollary 5.10. *For a given discriminant $D>0$, the class number $h^+(D)$ of proper equivalence classes of binary quadratic forms of discriminant D is finite.*

Proof. Every equivalence class contains a form $ax^2+bxy+cy^2$ with $|a| \leq \frac{1}{2}\sqrt{D}$, and $|b| \leq |a|$. There are only finitely many such choices. We compute $c = \frac{b^2-D}{2a}$, so there are only finitely many forms of discriminant D. □

Our notion of a reduced indefinite form, in particular the bounds involved, differ somewhat from the above result.

Definition 5.11 (Reduced indefinite form)**.** Let $f(x,y) = ax^2+bxy+cy^2$ be a binary quadratic form of discriminant $D>0$. We call f *reduced* if

$$\left|\sqrt{D}-2|a|\right| < b < \sqrt{D}\,.$$

Now we have the following properties of reduced forms.

Proposition 5.12. *If $ax^2+bxy+cy^2$ is a reduced indefinite binary quadratic form, then*

- $|a|+|c|<D$
- $|a|, b, |c| < \sqrt{D}$
- $ac<0$.

Proof. Exercise! □

Definition 5.13 (Reduction operator)**.** Let $D>0$ be a discriminant. For $a \neq 0, b$ integer, define $r(b,a)$ to be the unique integer r such that

$$r \equiv b \pmod{2a}\,,$$

and

$$\begin{cases} -|a| < r \leq |a| & \text{if } |a| > \sqrt{D} \\ \sqrt{D}-2|a| < r < \sqrt{D} & \text{if } |a| < \sqrt{D} \end{cases}.$$

Then the reduction operator ρ is defined on $ax^2+bxy+cy^2$ of discriminant $D>0$ by

$$\rho(ax^2+bxy+cy^2) = cx^2 + r(-b,c)xy + \frac{r(-b,c)^2-D}{4c}y^2\,.$$

We then have the following proposition.

Proposition 5.14 (Proposition 5.6.6 in [Coh13, p. 264])**.** *i) Iterating ρ a finite number of times on any indefinite form $ax^2+bxy+cy^2$, eventually produces a reduced form,*

ii) If $f(x,y)=ax^2+bxy+cy^2$ is a reduced form, then $\rho(f(x,y))$ is again a reduced form,

iii) The reduced forms equivalent to f are exactly the forms $\rho^n(f)$, n sufficiently large, which are reduced.

Proof. See [Coh13]. □

Remark 5.15. In particular, we can give a method to list a representative of every proper equivalence class of indefinite binary quadratic forms of fixed discriminant D.

Step 1: Produce a list $\mathcal{L}$ of all reduced forms of discriminant $D>0$.
Step 2: Select a reduced form f remaining in $\mathcal{L}$, and iteratively apply ρ to compute the reduced forms $\mathcal{F}$ equivalent to f.
Step 3: Record f (or any other reduced form from $\mathcal{F}$) on the list $\mathcal{R}$ of representatives, then replace $\mathcal{L}$ with $\mathcal{L}\setminus\mathcal{F}$. If $\mathcal{L}\neq\emptyset$, go to Step 2.
Step 4: Output list $\mathcal{R}$ of representatives of the reduced forms of discriminant $D>0$.

Example 5.16. We find representatives of the equivalence classes of primitive indefinite binary quadratic forms of discriminant $D=20$. To get a reduced form, we have bounds $\left|\sqrt{D}-2|a|\right| < b < \sqrt{D}$. And We have bounds $|a| \le \sqrt{20} = 4.47\ldots$, so $-4 \le a \le 4$. We list these, and compute $c=\frac{b^2-D}{2a}$ (Notice that we always get D pairs (a,b), before discarding non-integral forms!)

a	b	c	Integral?	Primitive?
-2	2	2	✓	
-1	4	1	✓	✓
1	4	-1	✓	✓
2	2	-2	✓	

So reduced forms of discriminant $D=20$ are $-2x^2+2xy+2y^2, -x^2+4xy+y^2, x^2+4xy-y^2, 2x^2+2xy-2y^2$. The primitive ones are $-x^2+4xy+y^2$ and $x^2+4xy-y^2$.

We now compute the ρ-orbits to see if any of the primitive reduced forms are equivalent. To compute $\rho(-x^2+4xy+y^2)$, we need to know $r(-4,1)$.

We have $r(-4,1)=r$, where $r\equiv -4 \pmod 2$. Since $|1|=1<\sqrt{20}=4.47\ldots$, we need $\sqrt{20}-2|1|<r<\sqrt{20}$, so that $2.47\ldots<r<4.47\ldots$. This means $r(-4,1)=4$. We get

$$\rho(-x^2+4xy+y^2) = x^2+4xy+\frac{4^2-20}{4}y^2 = x^2+4xy-y^2$$

So the ρ-orbit of $-x^2+4xy+y^2$ is $\{-x^2+4xy+y^2, x^2+4xy-y^2\}$. This deals with all ρ-orbits of primitive reduced forms. Therefore the two primitive reduced forms are equivalent, so the is only a single equivalence class of binary quadratic forms of discriminant $D=20$, and $h^+(20)=1$.

Upshot: Every binary quadratic form of discriminant $D=20$ is equivalent to $x^2+4xy-y^2$. In particular x^2-5^2 and $-x^2+5y^2$ both must be equivalent to $x^2+4xy-y^2$. By applying our results, we can say for $p \neq 2,5$:

$$\begin{aligned} p \equiv 1,4 \pmod 5 &\overset{\text{QR}}{\iff} \left(\frac{20}{p}\right) = 1 \\ &\overset{\text{Cor}}{\iff} p = x^2 - 5y^2 \\ &\overset{\text{Reduction}}{\iff} p = -x^2 + 5y^2 \\ &\overset{\text{Reduction}}{\iff} p = x^2 + 4xy - y^2 \end{aligned}$$

Example 5.17. Repeating the same example for $D=12$ leads to the primitive reduced forms $-2x^2+2xy+y^2, -x^2+2xy+2y^2, x^2+2xy-2y^2, 2x^2+2xy-y^2$. Under ρ, these split into the orbits

$$\left\{-2x^2+2xy+y^2, x^2+2xy-2y^2\right\}, \left\{-x^2+2xy+2y^2, 2x^2+2xy-y^2\right\}.$$

So there are two non-equivalent classes of primitive indefinite binary quadratic forms of discriminant $D=12$. So $h^+(D)=2$. Identifying $ax^2+bxy+cy^2$ and $-ax^2+bxy+cy^2$ leads to one class containing $x^2+2xy-2y^2$. So $h(12)=2$.

Applying ρ to x^2-3y^2 produces eventually (after ρ^2) $x^2+2xy-2y^2$. Applying ρ to $-x^2+3y^2$ produces eventually (after ρ^2) $-x^2+2xy+2y^2$. Since these are in different ρ-orbits, we see that the forms $-x^2+3y^2$ and x^2-3y^2 are not equivalent.

Exercise: check the details here!

A calculator is available online at `http://www.numbertheory.org/php/classnopos0.html` to compute the class number, and representatives of the equivalence classes of primitive indefinite binary quadratic forms of discriminant $D>0$.

5.3. Finiteness of the class number in general

In this section we say a few words about the finiteness of the class number in general, for n-ary quadratic forms of fixed determinant d. For simplicity, we assume that the quadratic forms are *classically* integral, but since $f \sim g$ if and only if $2f \sim 2g$, this is not a serious restriction.

Lemma 5.18 ([Cas08], Lemma 3.1)**.** *For each $n \geq 1$, there is a constant C_n so that for any regular integral quadratic form in n-variables, there is a vector $\underline{\mathbf{a}} \in \mathbb{Z}^n$ with $f(\underline{\mathbf{a}}) \neq 0$, and*

$$|f(\underline{\mathbf{a}}| \leq C_n |\det(f)|^{1/n}.$$

With this we can take an arbitrary (classically) integra ln-ary quadratic form of determinant d, find $h = f(\underline{\mathbf{a}}) < C_n|\det(f)|^{1/n}$. Then we can find an equivalent form where the x^2-coefficient is h. (Compare Lemma 4.19, we can assume $\underline{\mathbf{a}}$ is primitive.) This means the x^2-coefficient lies in a finite set.

Completing the square means we can write

$$hf(\underline{\mathbf{x}}) = (hx_1 + r_{12}x_2 + r_{13}x_3 + \cdots)^2 + g(x_2, \ldots, x_n)\,.$$

By induction, we can transform $g(x_2, \ldots, x_n)$ to one of a finite number of non-equivalent forms, modulo $\mathrm{SL}_{n-1}(\mathbb{Z})$. We can also substitute $x_1 \to x_1 - u_2x_2 - u_3x_3 - \cdots$, to ensure the $|r_{1j}| < h$. This means the RHS above lies in a finite set of possibilities. Hence $f(\underline{\mathbf{x}})$ lies in a finite set of possibilities, itself. So the class number $h(n, d)$ of n-ary quadratic forms, of determinant d is finite.

One can produce tables

- Of equivalence classes of ternary quadratic forms `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/Brandt_1.html`, `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/Brandt_2.html`,
- Of quaternary quadratic forms `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/nipp.html`, and higher.

Exercises

Positive-definite.

Exercise 5.19. Apply the algorithm in the existence step of the proof of Theorem 5.5 to find reduced forms equivalent to the following, also give matrices which show the equivalence:

- $6x^2 - 2xy + y^2$
- $10x^2 - 10x + 3y^2$
- $5x^2 - 10xy + 6y^2$
- $5x^2 + 6xy + 3y^2$
- $2x^2 + 4xy + 5y^2$
- $x^2 + 2xy + 7y^2$
- $8x^2 - 2xy + y^2$

Exercise 5.20. Check that the following, for discriminant $D < 0$ are always reduced forms

- For $D \equiv 0 \pmod 4$, the form $x^2 - \frac{D}{4}y^2$,
- For $D \equiv 1 \pmod 4$, the form $x^2 + xy + \frac{1-D}{4}y^2$.

These are called the *principal forms*. For $D > 0$, these forms are not reduced, but we still call them the *principal forms*. (These forms correspond to the principal ideal class in quadratic number fields. See handout 2.)

Exercise 5.21. Suppose that $f(x) = ax^2 + bxy + cy^2$ is a positive-definite binary quadratic form of discriminant $D < 0$. Suppose $a < \sqrt{-D/4}$ and $-a < b \leq a$. Show that f is reduced.

Exercise 5.22. • Verify the following table of class numbers (in the positive definite case), by listing all reduced forms of the given discriminant.

D	$h(D)$	D	$h(D)$
-3	1	-4	1
-7	1	-8	1
-11	1	-12	1
-15	2	-16	1
-19	1	-20	2
-23	3	-24	2
-27	1	-28	1
-31	3	-32	2
-35	2	-36	2
-39	4	-40	2

- Write a computer program to extend this to all discriminants $-32768 < D < 0$. Hint: $h(-32767)$ is divisible by 13. (Runtime of about 30 minutes, is fine)

Exercise 5.23. The entries above for $D = -4, -8, -12$ correspond to Fermat's $x^2 + y^2$, $x^2 + 2y^2$ and $x^2 + 3y^2$ theorems, which we now have powerful techniques to prove. Since $h(D) = 1$ for $D = -3, -7, -11, -16, -19, -27$ and -28, we obtain corresponding results for these cases.

i) State and prove congruence conditions on when a prime p can be represented by
   - $x^2 + xy + y^2$, of discriminant -3,
   - $x^2 + xy + 2y^2$, of discriminant -7,
   - $x^2 + xy + 3y^2$, of discriminant -11,
   - $x^2 + 4y^2$, of discriminant -16,
   - $x^2 + xy + 5y^2$, of discriminant -19,
   - $x^2 + xy + 7y^2$, of discriminant -27,
   - $x^2 + 7y^2$, of discriminant -28.

ii) Show directly that the result $p = x^2 + 4y^2$ where $D = -16$ is (trivially) equivalent to result for $p = x^2 + y^2$ where $D = -4$.

iii) Similarly show the result for $p = x^2+7y^2$ with $D = -28$ is (trivially) equivalent to the result for $p = x^2 + xy + 2y^2$ with $D = -7$. Hint: reduce modulo 2 to show y is even in $x^2+xy+2y^2$, then write $x^2+xy+2y^2 = (x+y/2)^2+7(y/2)^2$.

Exercise 5.24. Suppose that the positive-definite form $f(x, y)$ represents the value 1. Show that $f(x, y)$ is equivalent to the principal form (recall this is: either x^2+ny^2, for discriminant $D = -4n$, or $x^2 + xy + ny^2$,for discriminant $D = -4k + 1$).

What about if $f(x, y)$ is an indefinite form?

Exercise 5.25. Suppose p is a prime number, represented by two forms $f(x, y)$ and $g(x, y)$ of discriminant D (positive-definite, or indefinite). Show that $f(x, y)$ and $g(x, y)$ are equivalent (possibly improperly equivalent). Hint: use Lemma 4.19, and examine the middle coefficient modulo p.

Exercise 5.26. By considering reduced forms, of the form $ax^2 + cy^2$. Show that the class number of discriminant D can be arbitrarily high. Hint: consider $D = -4p_1p_2 \cdots p_k$, where p_i are distinct primes.

Indefinite.

Exercise 5.27. Imitate the proof of Theorem 5.5 to show that every indefinite quadratic form of some discriminant D is equivalent to one of the form $ax^2+bxy+cy^2$ with $|b| \leq |a| \leq |c|$. Moreover, show that such a form has $ac < 0$ and $|a| \leq \frac{1}{2}\sqrt{D}$.

Exercise 5.28. If $ax^2 + bxy + cy^2$ is a reduced indefinite binary quadratic form, show that

- $|a| + |c| < \sqrt{D}$,
- $|a|, b, |c| < \sqrt{D}$, and
- $ac < 0$.

Exercise 5.29.

- Verify the following table of class numbers (in the indefinite case), by listing all reduced forms of the given discriminant and partitioning them into ρ-orbits.

D	$h^+(D)$	D	$h^+(D)$
5	1	8	1
12	2	13	1
17	1	20	1
21	2	24	2
28	2	29	1
32	2	33	2
37	1	40	2
41	1	44	2
45	2	48	2
52	1	53	1
56	2	57	2
60	4		

- Write a computer program to extend this to all non-square discriminants $0 < D < 32768$.

Exercise 5.30. The entry for $D = 8$ corresponds to the result for $p = x^2 - 2y^2$, as given in Problem Sheet 2. The entry for $D = 20$ corresponds to our result above for $p = x^2 - 5y^2$. Since $h^+(D) = 1$ for $D = 5, 13, 17, 20, 29, 7, 41, 52, 53$, we obtain corresponding results for these cases.

i) State and prove congruence conditions on when a prime p can be represented by
   - $x^2 + xy - y^2$ of discriminant $D = 5$,
   - $x^2 + xy - 3y^2$ of discriminant 13,
   - $x^2 + xy - 4y^2$ of discriminant 17,
   - $x^2 + xy - 7y^2$ of discriminant 29,
   - $x^2 + xy - 9y^2$ of discriminant 37,
   - $x^2 + xy - 10y^2$ of discriminant 41,
   - $x^2 - 13y^2$ of discriminant 52,
   - $x^2 + xy - 1y^2$ of discriminant 53.

ii) Derive a result for $x^2 - 17y^2$ using the result for $x^2 + xy - 4y^2$. Hint: reduce $x^2 + xy - 4y^2$ modulo 2 to show y is even, and write $x^2 + xy - 4y^2 = (x + \frac{y}{2})^2 - 17(\frac{y}{2})^2$.

iii) Derive a result for $x^2 - 41y^2$ using the result for $x^2 + xy - 10y^2$.

Exercise 5.31. Suppose that $D = 8k + 1$ is a discriminant, and that $h^+(D) = 1$. By considering the primes which $x^2 + xy - 2ky^2$ represents, show that every binary quadratic form of discriminant $4D$ is equivalent to $x^2 - 2ky^2$. Hence conclude $h^+(4D) = 1$. (You may assume that any primitive integral binary quadratic form attains a prime value - this follows from the Chebotarev density theorem.)

CHAPTER 6

Class number 1 and genus theory

Lecture 8
14/06/2017

While the techniques we have so far are relatively powerful (reducing Fermat's conjectures to algorithmic exercises!), we can only obtain results in the case of class number 1. But as we already know, class number 1 does not always occur (and in fact the situation is quite dire). With genus theory we can obtain further results, beyond class number 1.

6.1. Class number 1

If the class number is one, then we can use Corollary 4.21 to completely solve our question of when $p = x^2 + ny^2$. We therefore wish to study when $h(D) = 1$ and $h^+(D) = 1$. Unfortunatey, I claim that in the positive definite case, $h(D) = 1$ is very rare. In fact only finitely many times does it occur.

Theorem 6.1. *Suppose that $D = -4n < 0$ is a discriminant. Then $h(D) = 1$ if and only if*

$$n = 1, 2, 3, 4, 7\,.$$

Proof. It is easy to check that $h(D) = 1$ these cases. The proof that these are the only cases is given via an exercise, where we explicitly construct reduced forms other than $x^2 + ny^2$, showing that $h(D) \geq 2$. □

A more much difficult theorem to prove is a classification of all negative discriminants $D \equiv 0, 1 \pmod 4$ for which $h(D) = 1$.

Theorem 6.2 (Baker-Heegner-Stark)**.** *Suppose that $D < 0$ is a discriminant. Then $h(D) = 1$ if and only if*

$$D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\,.$$

Proof. We will *not* prove this theorem. A proof requires modular functions and complex multiplication. □

Basically this means we can only solve finitely many $p = x^2+ny^2$ with the techniques we have currently. And the only interesting case beyond Fermat is:

- For $p \neq 2, 7$:

$$\begin{aligned} p = x^2 + 7y^2 &\overset{\text{Cor}}{\iff} \left(\frac{-28}{p}\right) = 1 \\ &\iff \left(\frac{-7}{p}\right) = 1 \end{aligned}$$

$$\begin{aligned} &\overset{\text{QR}}{\iff} \left(\frac{p}{7}\right) = 1 \\ &\iff p \equiv \square \pmod 7 \\ &\iff p \equiv 1, 2, 4 \pmod 7 \end{aligned}$$

Plus we get some results for the corresponding $p = x^2 + xy + ny^2$, where $D = 1 - 4n$, such as:

- for $p \neq 2, 67$:

$$\begin{aligned} p = x^2 + xy + 31y^2 &\overset{\text{Cor}}{\iff} \left(\frac{-67}{p}\right) = 1 \\ &\overset{\text{QR}}{\iff} \left(\frac{p}{67}\right) = 1 \\ &\iff p \equiv \square \pmod{67} \\ &\iff p \equiv 1, 3, 4, 5, \ldots, 64, 65 \pmod{67}. \end{aligned}$$

If we turn to indefinite forms instead, then there are infinitely many cases where $h(D)^+ = 1$, although there is a 'trick' to constructing them.

Claim 6.3. For each $n > 0$, we have

$$h^+(4 \cdot 169^n \cdot 13) = 1,$$

so that every binary quadratic form of discriminant $D = 4 \cdot 169^n \cdot 13$ is equivalent to the principle form

$$x^2 - 169^n \cdot 13y^2.$$

Therefore, for $p \neq 2, 13$ we have

$$\begin{aligned} p = x^2 - 169^n \cdot 13y^2 &\overset{\text{Cor}}{\iff} \left(\frac{169^n \cdot 13}{p}\right) = 1 \\ &\iff \left(\frac{13}{p}\right) = 1 \\ &\overset{\text{QR}}{\iff} p \equiv 1, 3, 4, 9, 10, 12 \pmod{13} \end{aligned}$$

If we disallow this 'trick', and focus only on so-called fundamental discriminants $D = 4k + 1$ square-free or $D = 4k$, k square-free and, $k \equiv 2, 3 \pmod 4$. I.e. discriminants D which are not of the form $D = m^2 D_0$, with D_0 a discriminant. Then the question of whether there are infinitely many such discriminants with class number $h^+(D) = 1$ remains open, but the it appears that $h^+(D) = 1$ much more frequently that in the positive-definite case. And the list appears to continue indefinitely.

Proposition 6.4. *For discriminant D equal to*

$$D = \begin{cases} 5, 8, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, \\ 109, 113, 137, 149, 157, 173, 181, 193, 197, \ldots \end{cases},$$

the class number $h^+(D) = 1$.

(Notice that these are all prime, and congruence to 1 (mod 4), except for $D = 8$. This is provable!) So we get various conditions like

$$\begin{aligned} p = x^2 + xy - 15y^2 &\overset{\text{Cor}}{\iff} \left(\frac{p}{61}\right) = 1 \\ &\overset{\text{QR}}{\iff} p \equiv \square \pmod{61} \\ &\iff p \equiv 1, 3, 4, 5, \ldots, 57, 58, 60 \pmod{61} \end{aligned}$$

Conjecture 6.5. *There are infinitely many fundamental discriminants $D > 0$ such that $h(D) = 1$. [Equivalently, using the link between quadratic forms and quadratic numbe rfields: infinite many real quadratic fields $K = \mathbb{Q}(\sqrt{D})$ have class number $h_K^+ = 1$. It is not even known whether $h_K = 1$ occurs infinitely often.]*

If the class number is > 1, can we do anything?

6.2. Elementary aspects of genus theory

Let us study the first case of $x^2 + ny^2$ where the class number is > 1. This is $D = -20$, with $x^2 + 5y^2$.

Example 6.6. Using our theory, we have for $p \neq 2, 5$:

$$p \equiv 1, 3, 7, 9 \pmod{20} \overset{\text{QR}}{\iff} \left(\frac{-20}{p}\right) = 1 \underset{\text{Reduction}}{\overset{\text{Cor} +}{\iff}} p = \begin{cases} x^2 + 5y^2 \text{ or} \\ 2x^2 + 2xy + 3y^2 \end{cases}$$

But let us consider the values that $p = x^2 + 5y^2$ attains in $(\mathbb{Z}/20\mathbb{Z})^*$ (since we only care abut primes $p \nmid 20$, in particular coprime to 20). Look modulo 5, and combine with the result that $p \equiv 1, 3, 7, 9 \pmod{20}$. We have

$$x^2 + 5y^2 \equiv x^2 \equiv 0, (\pm 1)^2, (\pm 2)^2 \pmod 5 \equiv 0, 1, 4 \pmod 5$$

For $p \neq 2, 5$ prime, only $p \equiv 1, 4 \pmod 5$ is possible, which means from our mod 20 list, we have $p \equiv 1, 9 \pmod{20}$.

Similarly

$$\begin{aligned} 2x^2 + 2xy + 3y^2 &\equiv 2(x^2 + xy + 4y^2) \\ &\equiv 2(x + 3y)^2 \\ &\equiv 0, 2 \cdot (\pm 1)^2, 2 \cdot (\pm 2)^2 \\ &\equiv 0, 2, 3 \pmod 5 \end{aligned}$$

For $p \neq 2, 5$ prime, only $p \equiv 2, 3 \pmod 5$ is possible. This means from out mod 20 list, we must have $p \equiv 3, 7 \pmod{20}$.

Thus we have

$$\begin{aligned} p = x^2 + 5y^2 &\Rightarrow p \equiv 1, 9 \pmod{20} \\ p = 2x^2 + 2xy + 3y^2 &\Rightarrow p \equiv 3, 7 \pmod{20}. \end{aligned}$$

Now let us make the following argument to show the reverse implications. Let

Let $p \equiv 1, 9 \pmod{20}$. Then certainly $p \equiv 1, 3, 7, 9 \pmod{20}$, so we can write

$$p = \begin{cases} x^2 + 5y^2 \text{ or} \\ 2x^2 + 2xy + 3y^2 \end{cases} .$$

If $p \neq x^2 + 5y^2$, then it must be represented by the other form. But this means $p = 2x^2 + 2xy + 3y^2$, and so $p \equiv 3, 7 \pmod{20}$, a contradiction. Hence $p \equiv 1, 9 \pmod{20} \Rightarrow p = x^2 + 5y^2$.

Similarly, if $p \equiv 3, 7 \pmod{20}$, then $p = x^2 + 5y^2$ or $p = 2x^2 + 2xy + 3y^2$. If $p \neq 2x^2 + 2xy + 3y^2$, then $p = x^2 + 5y^2$, so $p \equiv 1, 9 \pmod{20}$, contradiction. Hence $p \equiv 3, 7 \pmod{20} \Rightarrow p = 2x^2 + 2xy + 3y^2$.

Upshot: For $p \neq 2, 5$ we have

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$$
$$p = 2x^2 + 2xy + 3y^2 \iff p \equiv 3, 7 \pmod{20} .$$

Let's take a moment to identify some of the (potential) key properties which made this argument work. Each quadratic form represents a certain set of congruence classes ni $(\mathbb{Z}/D\mathbb{Z})^*$ (since we only focus on odd primes $p \nmid D$, so satisfy $\gcd(p, D) = 1$). Different forms represent disjoint sets of values, and so these values characterise which primes the given form represents. We want to see that this is not an accident, and so to justify the following definition.

Definition 6.7 (Genus)**.** Let $f(x, y)$ and $g(x, y)$ be two primitive integral binary quadratic forms of discriminant D. We say that $f(x, y)$ and $g(x, y)$ are in the same *genus* if they represent the same values in $(\mathbb{Z}/D\mathbb{Z})^*$.

To answer this, it is helpful to introduce an alternative description of Corollary 4.21, by means of a certain group homomorphism.

Lemma 6.8. *If $D \equiv 0, 1 \pmod{4}$ is a non-zero integer (in particular a discriminant!), then there is a unique group homomorphism*

$$\chi \colon (\mathbb{Z}/D\mathbb{Z})^* \to \{ \pm 1 \} ,$$

such that $\chi([p]) = \left(\frac{D}{p}\right)$ for odd primes $p \nmid D$.

Proof. See handout 3 for a sketch of the proof. This uses the Jacobi symbol, a generalisation fo the Legendre symbol. □

In particular, we can restate Corollary 4.21 in the following ways

Corollary 6.9 (Descent)**.** *Let D be a discriminant, and let p be an odd prime not dividing D. Then p is represented by a primitive binary quadratic form of discriminant D if and only if $[p] \in \ker \chi \subset (\mathbb{Z}/D\mathbb{Z})^*$.*

Remark 6.10. This more rigorously establishes the result $\left(\frac{4n}{p}\right) = 1$ is characterised by a congruence condition modulo $D = 4n$, that I mentioned for $\left(\frac{n}{p}\right) = \left(\frac{4n}{p}\right) = 1$ after the proof of Quadratic Reciprocity Theorem 3.9. It also deals with the case $D = 4n + 1$. Moreover, we see extra structure in the set of congruence classes: they form a subgroup of $(\mathbb{Z}/D\mathbb{Z})^*$.

We can now give a characterisation of the values in $(\mathbb{Z}/D\mathbb{Z})^*$ that binary quadratic forms of discriminant D represents. We also define the *principal form* of discriminant D:

$$x^2 - \frac{D}{4}y^2 \text{for } D \equiv 0 \pmod 4$$
$$x^2 + xy + \frac{1-D}{4}y^2 \text{for } D \equiv 1 \pmod 4$$

Theorem 6.11. *Given an integer $D \equiv 0, 1 \pmod 4$, and $\ker \chi \subset (\mathbb{Z}/D\mathbb{Z})^*$ as above. Let $f(x, y)$ be a primitive integral binary quadratic form of discriminant D. Then*

i) THe values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by the principal form of discriminant D form a subgroup $H \subset \ker \chi$.
ii) The values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$ form a coset of H in $\ker \chi$.

In particular, the values represented in $(\mathbb{Z}/D\mathbb{Z})^*$ by two binary quadratic forms of discriminant D are either disjoint, or identical.

Sketch. Firstly, to see $H \subset \ker \chi$, we need to check that if $m = f(x_0, y_0)$, with $\gcd(m, D) = 1$, then $[m] \in \ker \chi$. But $m = d^2m'$, where m' is properly represented by $f(x, y)$, and $d = \gcd(x_0, y_0)$. Then $\chi([m]) = \chi([d])^2\chi([m']) = \chi([m'])$, so we can assume m itself is properly represented by $f(x, y)$. Hence $D = b^2 - 4mk$, using Lemma 4.20. Now if m odd, the Jacobi symbol (not Legendre symbol) gives

$$\left(\frac{D}{m}\right) = \left(\frac{b^2 - 4km}{m}\right) = \left(\frac{b^2}{m}\right) = \left(\frac{b}{m}\right)^2 = 1$$

(The case m even requires a little more work: show $D \equiv 1 \pmod 8$, then use property $\left(\frac{2}{8k+1}\right) = 1$.)

For i) Using $(x^2 + ny^2)(w^2 + nz^2) = (xw - nzy)^2 + n(xz + wy)^2$, we see H is a subgroup for $D \equiv 0 \pmod 4$. For $D \equiv 1 \pmod 4$, we can use

$$4(x^2 + xy + \frac{1-D}{4}y^2) \equiv (2x + y)^2 \pmod D,$$

so that H is the subgroup of squares in $(\mathbb{Z}/D\mathbb{Z})^*$.

For ii), if $D = -4n$, and $f(x, y) = ax^2 + bxy + cy^2$ then b is even and we can write

$$af(x, y) = (ax + \tfrac{b}{2}y)^2 + ny^2,$$

so that the values of $f(x, y)$ in $(\mathbb{Z}/D\mathbb{Z})^*$ lie in the coset $[a]^{-1}H$. Then given $[c] \in [a]^{-1}H$, we have $ac \equiv z^2 + nw^2 \pmod{4n}$, for some w, z. Now take $y_0 \equiv w \pmod D$, and solve $ax + \frac{b}{2}y \equiv z \pmod D$, to obtain $x_0 \equiv a^{-1}(z - \frac{b}{2}y_0) \pmod D$. This shows that $f(x_0, y_0) \equiv c \pmod D$, so $f(x, y)$ represents exactly the coset $[a]^{-1}H$. The result for $D \equiv 1 \pmod 4$ is similar. □

Given a coset H' of $H \in \ker \chi$, we can define the *genus* of H' be consist of all forms of discriminant D which represents the values of H' in $(\mathbb{Z}/D\mathbb{Z})^*$.

Remark 6.12. We might ask whether every coset of H in $\ker \chi$ occurs as the values represented by some quadratic form. It does, but a quick proof of this relies on a

rather difficult theorem. Dirichlet's theorem on primes in arithmetic progressions tells us that for $\gcd(m,b)=1$, there are infinitely many primes

$$p \equiv b \pmod{m},$$

in particular there is an odd prime $p \nmid D$ such that $p \equiv b \pmod{D}$. Then $[p] \in \ker\chi$ means $\left(\frac{D}{p}\right) = 1$, so that p is represented by a form of discriminant D, and in particular arbitrary $b \in \ker\chi$ is represented by some quadratic form of discriminant D. Thus any coset bH does arise.

We then obtain

Lecture 9 21/06/2017

Theorem 6.13. *Let D be a discriminant, and $H \subset \ker\chi$ be the subgroup of values represented by the principal form. IF H' is a coset of H in $\ker\chi$, and $p \nmid D$ is an odd prime. THen*

$$[p] \in H' \iff p \text{ is represented by a (reduced)} \text{ form of discriminant } D \text{ in the genus of } H'.$$

In particular, if every genus of discriminant D consists of a single quadratic form, then we obtain congruence for when $p = f(x,y)$, for every quaratic form of dicriminant D. Unfortunately, this (also!) does not always happen.

Example 6.14. The (reduced) primitive forms of discriminant -56 are

$$x^2+14y^2, 2x^2+7y^2, 3x^2 \pm 2xy + 5y^2 .$$

We have that

$$\left(\frac{-56}{p}\right) = 1 \iff 1,3,5,9,13,15,19,23,25,27,39,45 \pmod{56}.$$

(Either by just checking for $\ker\chi\colon (\mathbb{Z}/56\mathbb{Z})^* \to \{\pm 1\}$, or by using quadratic reciprocity.)

We find (necessary conditions on the) values which the principal form represents in $(\mathbb{Z}/56\mathbb{Z})^*$ by reducing modulo 7, to see

$$x^2+14y^2 \equiv x^2 \equiv 1,2,4 \pmod{7}.$$

So the represented values H must be contained in

$$\{1,9,15,23,25,39\} \subset (\mathbb{Z}/56\mathbb{Z})^* .$$

(These are the classes in $\ker\chi$ which map to $1,2,4$ when taken modulo 7.) Similarly, $2x^2+7y^2 \equiv 2x^2 \equiv 2,4,1 \pmod{7}$, so the values it represents must also be contained in

$$\{1,9,15,23,25,39\} \subset (\mathbb{Z}/56\mathbb{Z})^* .$$

By changing $x \to -x$, it is clear that the other forms represent the same values, so the cosets of H they determine must be equal. Now if $\#H < 6$, we cannot cover the remaining > 6 values $\{3,5,13,19,27,45\}$ with a single coset. This is a problem, since cosets of a subgroup $H \subset \ker\chi$ must partition the group $\ker\chi$. So $\#H = 6$, and we have the following

$$\begin{cases} x^2+14y^2 \\ 2x^2+7y^2 \end{cases} \xrightarrow{\text{represents}} \{1,9,15,23,25,39\} \subset (\mathbb{Z}/56\mathbb{Z})^*$$

$$\left\{3x^2 \pm 2xy + 5y^2 \quad \xrightarrow{\text{represents}} \{\, 3, 5, 13, 19, 27, 45 \,\} \subset (\mathbb{Z}/56\mathbb{Z})^*\right.$$

So the genus of $H = \{\, 1, 9, 15, 23, 25, 39 \,\}$ consists of $\{\, x^2 + 14y^2, 2x^2 + 7y^2 \,\}$. And the genus of $\{\, 3, 5, 13, 19, 27, 45 \,\}$ consists of $\{\, 3x^2 \pm 2xy + 5y^2 \,\}$.

By Theorem 6.11, we immediately obtain for $p \neq 2, 7$:

$$p = \begin{cases} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{cases} \iff p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$$

$$p = 3x^2 \pm 2xy + 5y^2 \iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}.$$

Moreover, since $3x^2 \pm 2xy + 5y^2$ obviously represent the same values (they are $\mathrm{GL}_2(\mathbb{Z})$-equivalent via $x \mapsto -x$), we even get

$$p = 3x^2 + 2xy + 5y^2 \iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}.$$

In order to study genus theory more deeply (to figure out when it works, and to understand some further properties), we need to first study the composition of binary quadratic forms.

Exercises

Class number 1.

Exercise 6.15. Suppose $m > 1$ is an integer, and $m \neq p^r$ is not a prime power. Show that we can write $m = ac$, where $1 < a < c$, and $\gcd(a, c) = 1$.

Exercise 6.16. In this exercise we will prove that $h(-4n) = 1$, for $n > 0$ if and only if $n = 1, 2, 3, 4, 7$.

- Show that $h(-4n) = 1$ for these n, by listing the reduced forms.
- Suppose that n is not a prime power. Use the previous exercises to write down a second reduced form of discriminant $-4n$. Hint: $b = 0$.
- Suppose that $n = 2^r$. If $r \geq 4$, show that
$$4x^2 + 4xy + (2^{r-2} + 1)y^2$$
is reduced, and is primitive. Check that $h(-4n) > 1$, for $r = 3$, also.
- Suppose now that $n = p^r$, p an odd prime. Suppose $n + 1 = ac$, where $2 \leq a < c$, and $\gcd(a, c) = 1$. Show that
$$ax^2 + 2xy + cy^2$$
is reduced of discriminant $-4n$.
- Finally, suppose that $n = p^r$, but that $n + 1 = 2^s$. If $s \geq 6$, show that
$$8x^2 + 6xy + (2^{s-3} + 1)y^2$$
is a reduced form of discriminant $-4n$. What happens for $s = 1, 2, 3, 4, 5$?
- Conclude that $h(-4n) = 1$ if and only if $n = 1, 2, 3, 4, 7$.

Elementary genus theory.

Exercise 6.17. Apply the idea from $p = x^2 + 5y^2$ from Example 6.6, or the general result from Theorem 6.11, to obtain congruence conditions for

- $p = x^2 + 6y^2$ and the other form of discriminant -24,
- $p = x^2 + 8y^2$ and the other form of discriminant -32,
- $p = x^2 + 21y^2$, and the other 3 forms of discriminant -84,
- $p = x^2 - 3y^2$, and the other form of discriminant 12,
- $p = x^2 - 10y^2$ and the other form of discriminant 40.
- $p = x^2 - 15y^2$ and the other 7 forms of discriminant 60.

Exercise 6.18. It is not possible to obtain a congruence condition for $p = x^2+56y^2$, even by using the genus theory Theorem 6.11. What is the best result you can obtain for $p = x^2 + 56y^2$, and the other 5 forms of discriminant -224? Hint: it *is* possible to give congruence conditions for some of the forms.

Exercise 6.19. Show that the values in $(\mathbb{Z}/D\mathbb{Z})^*$ represented by $f(x, y)$, a form of discriminant $D \equiv 1 \pmod 4$ form a coset of H (the values of the principal form), in $\ker \chi$.

Exercise 6.20. Suppose that $f(x, y)$ and $g(x, y)$ are two binary quadratic forms of discriminant D. Suppose that $f(x, y)$ and $g(x, y)$ are $\mathrm{GL}_2(\mathbb{Q})$-equivalent, via a matrix whose entries have denominators all coprime to $2D$. Show that $f(x, y)$ and $g(x, y)$ represent the same values in $(\mathbb{Z}/N\mathbb{Z})^*$, for all non-zero N. Conclude that $f(x, y)$ and $g(x, y)$ are in the same genus.

Exercise 6.21. Recall that x^2+14y^2 and $2x^2+7y^2$ are in the same genus, since they both represent $\{ 1, 9, 15, 23, 25, 39 \} \subset (\mathbb{Z}/56\mathbb{Z})^*$. Show that $x^2 + 14y^2$ and $2x^2 + 7y^2$ are $\mathrm{GL}_2(\mathbb{Q})$-equivalent, as forms over the rational numbers. (Hint: denominator 5 works.) Conclude, in particular, that congruence conditions can never separate the primes represented by $x^2 + 14y^2$ and $2x^2 + 7y^2$.

Exercise 6.22. Show that $2x^2 + 9x^2$ and $x^2 + 18y^2$ are $\mathrm{GL}_2(\mathbb{Q})$-equivalent, as forms over the rational numbers. (Hint: denominator 9 works.) Show however, that $2x^2 + 9y^2$ and $x^2 + 18y^2$ are in different genera. (If they represent the same vaues in $(\mathbb{Z}/72\mathbb{Z})^*$, then the same holds for any divisor of 72.) What differs from the previous exercise?

CHAPTER 7

Composition of binary quadratic forms

In this chapter we introduce the composition of binary quadratic forms. This allows us to give the set of all proper equivalence classes of binary quadratic forms a group stucture. This group structure is useful both to further study genus theory, and to obtain other results about representations of (multiples) of primes by binary quadratic forms.

We have already seen some examples of this composition, namely the identities

$$(x^2+ny^2)(w^2+nz^2) = (xw-nzy)^2+n(xz+yw)^2\,,$$

which we read as saying the form x^2+ny^2 composed with itself, is itself. Similarly, we have the identity

$$(3x^2+2xy+5y^2)(3z^2+2zw+5w^2) = (wx+5wy+3xz+yz)^2+14(wx-yz)^2$$

composing the form $3x^2+2xy+5y^2$ with itself to get the form x^2+14y^2. How do we understand and generalise these identities?

7.1. Definition and setup

Definition 7.1 (Composition of quadratic forms)**.** Let $f(x,y)$ and $g(x,y)$ be two primitive binary quadratic forms of discriminant D. We say that a form $F(x,y)$ of discriminant D is the composition of f and g provided that

$$f(x,y)g(z,w) = F(B_1(x,y;z,w),B_2(x,y;z,w))\,,$$

where

$$B_i(x,y;z,w) = a_ixz+b_ixw+c_iyz+d_iyw$$

is an integral bilinear form. $a_i,\dots,d_i\in\mathbb{Z}$.

We would like, ideally, that whenever we compose f and g using different B_i, we obtain a properly equivalent form. Unfortunately this does not happen, not even up to improper equivalence.

$$\begin{aligned}
&(14x^2+10xy+21y^2)(9w^2+2wz+30z^2) = \\
&\quad 126(-wx+wy+2xz+3yz)^2+\\
&\quad 38(-9wy-14xz-6yz)(-wx+wy+2xz+3yz)\\
&\quad +5(-9wy-14xz-6yz)^2\\
&(14x^2+10xy+21y^2)(9w^2+2wz+30z^2) = \\
&\quad 126(-wx-3wy+4xz-yz)^2+\\
&\quad 74(9wy-14xz-4yz)(-wx-3wy+4xz-yz)+\\
&\quad 13(9wy-14xz-4yz)^2+
\end{aligned}$$

One can then check that $(126, 38, 5)$ and $(126, 74, 13)$ are in different equivalence classes (proper, or improper)! (Check that the first doesn't represent 13, for example.)

Fortunately, we can fix this situation. Given any composition data, as above, Gauss proved that we have

$$a_1b_2 - a_2b_1 = \pm f(1, 0),$$
$$a_1c_2 - a_2c_1 = \pm g(1, 0)\,.$$

By restricting to the case where both signs are + we obtain

Definition 7.2 (Direct composition, Gauss)**.** Given F a composition of f and g, as above. We say F is the *direct composition* provided that

$$a_1b_2 - a_2b_1 = +f(1, 0),$$
$$a_1c_2 - a_2c_1 = +g(1, 0)\,.$$

It turns out that $(126, 38, 5)$ is the direct composition, in the previous case. We now have some questions. Is it always possible find the (direct) composition of two quadratic forms? If so, how can we do this explicitly?

Dirichlet gives an explicit construction of the composition of (a, b, c) and (a', b', c'), subject to some assumptions on $\gcd(a, a', \frac{1}{2}(b + b')) = 1$. We follow a version of this given in [Cas08], which makes it clear that this restriction is not a problem.

7.2. Dirichlet composition

We will use the notation $(a, b, c) = ax^2 + bxy + cy^2$ for integral (primitive) binary quadratic forms, and write $(a, b, c) \sim (p, q, r)$ to mean (a, b, c) and (p, q, r) are properly equivalent. If we fix the discriminant D, we may write $(a, b, *)$ to mean the (unique) form $(a, b, \frac{b^2-D}{4a})$ of discriminant D.

Lemma 7.3. *Let $f = (a, b, c)$ be a primitive form, and M any integer. Then f represents some integer coprime to M. By dividing through by the gcd, we can assume it properly represents an integer coprime to M.*

Proof. Exercise. □

Lemma 7.4. *Suppose (a_1, b, c_1) and (a_2, b, c_2) are two equivalent, primitive forms with the same middle coefficient. Let l be an integer such that $l \mid c_1, c_2$, and $\gcd(a_1, a_2, l) = 1$. Then*

$$(la_1, b, l^{-1}c_2) \sim (la_2, b, l^{-1}c_2)\,.$$

Proof. From the matrix $T = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ converting from (a_1, b, c_1) to (a_2, b, c_2), one obtains the equations

$$a_1s + c_2t = 0$$
$$a_2s + c_1t = 0\,,$$

whence $l \mid s$. So the matrix

$$\begin{pmatrix} r & l^{-1}s \\ lt & u \end{pmatrix}$$

gives the equivalence $(la_1, b, l^{-1}c_2) \sim (la_2, b, l^{-1}c_2)$. □

Definition 7.5. Given two primitive forms $f_i = (a_i, b_i, c_i)$ of discriminant D, we shall say f_1 and f_2 are *concordant* if $a_1 a_2 \neq 0$ and $b_1 = b_2 =: b$, and the form $(a_1 a_2, b, *)$ of discriminant D is integral.

Observe that $(a_1 a_2, b, *)$ is primitive: otherwise $p \mid a_1 a_2, b, \frac{b^2 - D}{4 a_1 a_2}$. Without loss of generality, $p \mid a_1$. So we get $p \mid a_1, b$. Finally $p \mid a_2 \cdot \frac{b^2 - D}{4 a_1 a_2} = c_1$ since it divides the second factor.

Given two concordant forms $f_i = (a_i, b_i, c_i)$, we will show (afterwards) that $(a_1 a_2, b, *)$ is the direct composition $f_1 \circ f_2$s of f_1 and f_2. Whence we can take this as the definition of composition of quadratic forms. We will also show that given any two primitive quadratic forms, one can find equivalent concordant forms with $\gcd(a_1, a_2) = 1$, so that the this composition always works.

Lecture 10
28/06/2017

Lemma 7.6. *Let C_1, C_2 be two classes of primitive forms of discriminant D. Then we can find concordant forms $f_i = (a_i, b, *)$ in C_i. Moreover, we may choose these concordant forms so that a_1, a_2 are coprime, and are coprime to any integer M, given in advance.*

Proof. By the first lemma, f_1 properly represents some integer a_1 coprime to M. So f_1 $(a_1, b_1, *)$. Then f_2 properly represents some a_2 prime to $a_1 M$, so $f_2 \sim (a_2, b_2, *)$. The $\mathrm{SL}_2(\mathbb{Z})$-change of variables $x \mapsto x + l_i y$ sends $b_i \to b_i^* = b_i + 2 a_i l_i$. We have $b_1 \equiv b_2 \pmod 2$ and since a_1, a_2 coprime we can choose l_1, l_2 so that $b_1^* = b_2^* = b$ by solving the system of equations

$$\begin{aligned} b &\equiv b_1 \pmod{2a_1} \\ b &\equiv b_2 \pmod{2a_2}. \end{aligned}$$

We can assume a_1 is odd, and so write the system as

$$\begin{aligned} b &\equiv b_1 \pmod 2 \\ b &\equiv b_1 \pmod{a_1} \\ b &\equiv b_2 \pmod{2a_2}. \end{aligned}$$

Reducing the last mod 2 shows that $b \equiv b_2 \equiv b_1 \pmod 2$, so the first is a consequence, and we can drop it. Then we can directly apply Chinese Remainder Theorem to write $b = b_2 a_1 \lambda + b_1 2 a_2 \mu$, where $1 = \gcd(a_1, 2a_2) = a_1 \lambda + 2 a_2 \mu$.

Thus $f_1 \sim (a_1, b, *)$ and $f_2 \sim (a_2, b, *)$ are (equivalent to) concordant forms, as required. □

Thus we can always find the composition of two quadratic forms by choosing a pair of equivalent concordant forms. We still need to check that this is well defined, so that by choosing a second equivalent pair of concordant forms, we obtain an equivalent composition.

Lemma 7.7. *Suppose that C_1 and C_2 are two classes of quadratic forms. Suppose that $f_1' = (a_1', b', *)$ and $f_2' = (a_2', b', *)$ are a pair of concordant forms with $f_i' \in C_i$. Suppose that $f_1'' = (a_1'', b'', *)$ and $f_2'' = (a_2'', b'', *)$ are another pair of concordant forms with $f_i'' \in C_i$. Then the composition $f_1' \circ f_2'$ and $f_1'' \circ f_2''$ are in the same class.*

PROOF. Using the first lemma with $M = a_1'a_2'a_1''a_2''$, we can find a concordant pair $f_1 = (a_1, b, *), f_2 = (a_2, b, *)$ so that

$$f_1 \sim f_1', f_2 \sim f_2'$$

with

$$\gcd(a_1, a_2) = 1 = \gcd(a_1a_2, a_1'a_2'a_1''a_2'')\,.$$

It is sufficient to show that $f_1 \circ f_2 = (a_1a_2, b, *) \sim (a_1'a_2', b', *) = f_1' \circ f_2'$, since the same argument applies to get $\sim (a_1''a_2'', b'', *) = f_1'' \circ f_2''$.

The gcd above means $\gcd(a_1a_2, a_1'a_2') = 1$, so as before we can find B such that

$$B \equiv b \pmod{2a_1a_2}$$
$$B \equiv b' \pmod{2a_1'a_2'}\,.$$

Then we have

$$(a_i, B, *) \sim (a_i, b, *) = f_i \sim f_i' = (a_i', b', *) \sim (a_i', B, *)$$

Consider

$$(a_1, B, \tfrac{B^2-D}{4a_1}) \sim (a_1', B, \tfrac{B^2-D}{4a_1'})$$

Notice that $B^2 - D$ is divisible by $4a_1'a_2'$ since $(a_1', b', *)$ and $a_2', b', *)$ are concordant. Also it is divisible by $4a_1$, where $\gcd(a_1, a_1'a_2') = 1$ by construction. Hence it is divisible by $4a_1a_2'$. Taking $l = a_2'$ and using the second lemma, we get

$$(a_1a_2', B, *) \sim (a_1'a_2', B, *)$$

Similarly using $l = a_1$ we get

$$(a_2, B, *) \sim (a_2', B, *) \Rightarrow (a_1a_2, B, *) \sim (a_1a_2', B, *)\,.$$

From this, the required equivalence follows as

$$(a_1'a_2', B, *) \sim (a_1a_2', B, *) \sim (a_1a_2, B, *)\,.$$

□

Theorem 7.8 (Class group)**.** *The composition discussed above endows the set of equivalence classes of primitive binary quadratic forms, of discriminant D with the structure of a finite abelian group. This is called the* class group $\mathcal{C}(D)$ *(for positive-definite) or $\mathcal{C}^+(D)$ for indefinite forms.*

SKETCH. The identity element is the principal form $(1, 0, *) \sim (1, b, *)$ or $(1, 1, *) \sim (1, b, *)$ according to $D \pmod 4$. The indicated equivalent forms are concordant with (a, b, c), and the definition of composition shows the principal form is the identity.

Commutativity follows immediately by definition $(a_1, b, *) \circ (a_2, b, *) = (a_1a_2, b, *) = (a_2, b, *) \circ (a_1, b, *)$.

Associativity holds because the class of $f_1 \circ (f_2 \circ f_3)$ and $(f_1 \circ f_2) \circ f_3$ both contain $(a_1a_2a_3, b, *)$.

The inverse of (a, b, c) is $(a, -b, c) \sim (c, b, a)$, improperly equivalent form to (a, b, c). This is because the composition is $(ac, b, 1)$, which represents 1, so it belongs to the principal class. □

Finally, we show that the composition using concordant forms gives us direct compositions in Gauss's sense. Since the direct composition involves bilinear forms, a $\mathrm{SL}_2(\mathbb{Z})$-change of variabiesl in any of the 3 forms still produces a composition law. (See Exercise!) Thus we can change to a more convenient choice of forms.

Proposition 7.9. *Let f_1, f_2 be two primitive binary quadratic forms. And suppose that the following concordant forms are equivalent to f_1, f_2*

$$(a, B, a'C) \text{ and } (a', B, aC)$$

where $C = \frac{B^2-D}{4a'a'}$). The composition (aa', B, C) is the direct composition of the concordant forms above.

Proof. We have the following composition law

$$(ax^2 + Bxy + a'Cy^2)(a'z^2 + Bzw + aCw^2) = aa'X^2 + BXY + CY^2\,,$$

where $X = xz - Cyw$ and $Y = axw + a'yz + Byw$.

This is direct since

$$f_1(1,0) = a = \underbrace{a_1}_{xz\in X:1}\underbrace{b_2}_{xw\in Y:a} - \underbrace{a_2}_{xz\in Y:0}\underbrace{b_1}_{xw\in X:0}$$
$$f_2(1,0) = a' = \underbrace{a_1}_{xz\in X:1}\underbrace{c_2}_{yz\in Y:a'} - \underbrace{a_2}_{xz\in Y:0}\underbrace{c_1}_{yz\in X:0}$$

□

Aside from needing to finding an explicit change of variables to a pair of concordant forms, we can in principle produce such identities for any choice of primitive quadratic forms.

Example 7.10. Let us find the composition of the reduced forms $(3, 2, 16)$ and $(7, -6, 8)$. We have

$$(3, 2, 16) \sim (3, 2 + 2 \cdot 3, 21) \text{ via } x \mapsto x + y$$
$$(7, -6, 8) \sim (7, -6 + 2 \cdot 7, 9) \text{ via } x \mapsto x + y\,.$$

These two forms are concordant and the composition is $(21, 8, 3)$. We have the explicit direct composition law

$$(3x^2 + 8xy + 21y^2)(7z^2 + 8zw + 9w^2) = 21X^2 + 8XY + 3Y^2\,,$$

with $X = xz - 3yw$, and $Y = 3xw + 7yz + 8yw$.

Finally, we can observe that $(21, 8, 3)$ is equivalent to $(3, -8, 21)$ via $X \mapsto -Y, Y \mapsto X$ which is a proper equivalence, and the result is equivalent to the reduced form $(3, -2, 16)$ via $X \mapsto X - Y$. So inverting these we get

$$\begin{aligned}
&(3x^2 + 8xy + 21y^2)(7z^2 + 8zw + 9w^2)\\
&= 3(X + Y)^2 - 2(X + Y)(-X) + 16(-X)^2\\
&= 3(xz + 3xw + 7yz + 5yw)^2 +\\
&\quad - 2(xz + 3xw + 7yz + 5yw)(-xz + 3yw) +\\
&\quad + 16(-xz + 3yw)^2)\,.
\end{aligned}$$

Finally, we put $x \mapsto x - y$ and $z \mapsto z - w$ to recover the two original forms, and obtain

$$\begin{aligned}
&(3x^2 + 2xy + 16y^2)(7z^2 - 6wz + 8w^2) \\
&= 3(xz + 2xw + 6yz - 4yw)^2 + \\
&\quad - 2(xz + 2xw + 6yz - 4yw)(-xz + wx + yz + 2yw) + \\
&\quad + 16(-xz + wx + yz + 2yw)^2
\end{aligned}$$

This is still direct since

$$\begin{aligned}
f_1(1,0) = 3 &= \underbrace{a_1}_{xz \in X:1}\ \underbrace{b_2}_{xw \in Y:1} - \underbrace{a_2}_{xz \in Y:-1}\ \underbrace{b_1}_{xw \in X:2} \\
f_2(1,0) = 7 &= \underbrace{a_1}_{xz \in X:1}\ \underbrace{c_2}_{yz \in Y:1} - \underbrace{a_2}_{xz \in Y:-1}\ \underbrace{c_1}_{yz \in X:6}
\end{aligned}$$

The following web pages have calculators to compute the composition of two quadratic forms of discriminant D, for positive-definite and indefinite forms:

- Positive-definite: `http://www.numbertheory.org/php/composeneg.html`
- Indefinite: `http://www.numbertheory.org/php/composepos.html`

Example 7.11. We can also prove some non-trivial results about which fixed multiples of primes, and when products of two primes can be written as certain quadratic forms.

We have that for $p \neq 2, 7$:

$$3p = x^2 + 14y^2 \iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}.$$

Since 3 is represented by $3x^2 + 2xy + 5y^2$, the direction $\Leftarrow$ follows from the composition $(3, 2, 5) \circ (3, -2, 5) = (3, 2, 5) \circ (5, 2, 3) = (15, 2, 1) \sim (1, 0, 14)$. For $\Rightarrow$, we see that $3p = x^2 + 14y^2$ implies $p \mid x^2 + 14y^2$, so $p = x^2 + 14y^2, 2x^2 + 7y^2,$ or $3x^2 \pm 2xy + 5y^2$. If $p = x^2 + 14y^2, 2x^2 + 7y^2$, then $p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$, so that $3p \equiv 3, 5, 13, 19, 27, 45$ meaning $3p \neq x^2 + 14y^2$. Hence $p = 3x^2 \pm 2xy + 5y^2$ which implies $p \equiv 3, 5, 13, 1927, 45 \pmod{56}$.

More generally, the same argument show that if we have $q \neq 2, 7$ is any prime represented by $3x^2 + 2xy + 5y^2$, then for $p \neq 2, 7$:

$$pq = x^2 + 14y^2 \iff p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}.$$

However, if q is represented by one of the other forms, and not $3x^2 + 2xy + 5y^2$, then

$$pq = x^2 + 14y^2 \iff \begin{cases} p \text{ and } q = 2x^2 + 7y^2 \text{ or} \\ p \text{ and } q = x^2 + 14y^2 \end{cases}.$$

This is somehow intuitively clear, but is requires a little work to prove directly.

Overall this says that for odd primes p, q with $\left(\frac{14}{p}\right) = \left(\frac{14}{q}\right) = 1$, then

$$pq = x^2 + 14y^2 \iff p, q \text{ are represented by the same form}$$

Exercises

Exercise 7.12. Let $f = (a, b, c)$ be a primitive form, and M any integer. Show that f represents some integer coprime to M. Show also that we can assume f properly represents some integer coprime to M.

Exercise 7.13. Suppose that F is (a) direct composition of f and g. If $f \sim f'$ and $g \sim g'$, and $F' \sim F$, show that F' is a direct composition of f' and g'. So we can use the Dirichlet composition to find the direct composition with explicit bilinear forms.

Exercise 7.14. Suppose that $pq = X^2 + 14Y^2$ and $q = 2a^2 + 7b^2$. By considering the composition

$$\begin{aligned} p(2a^2 + 7b^2)(2a^2 + 7b^2) &= (X^2 + 14Y^2)(2a^2 + 7b^2) \\ &= 2(aX + 7bY)^2 + 7(-bX + 2aY)^2 \,. \end{aligned}$$

By reducing $2a^2 + 7b^2$, and $X^2 + 14Y^2$ modulo q, show that we may choose the sign $\pm a, \pm b, \pm X, \pm Y$, so that

$$q \mid aX + 7bY, -bX + 2aY \,,$$

hence conclude that p is represented by $2x^2 + 7y^2$.

Exercise 7.15. Suppose that $F = (A, B, C)$ is the composition of $f = (a, b, c)$ and $g = (a', b', c')$ via

$$\begin{aligned} f(x, y)g(z, w) = F(&a_1xz + b_1xw + c_1yz + d_1yw, \\ &a_2xz + b_2xw + c_2yz + d_2yw) \,. \end{aligned}$$

Suppose all 3 forms have the same discriminant $D \neq 0$.

i) By specialising variables x, y, w, z prove that

$$\begin{aligned} aa' &= Aa_1^2 + Ba_1a_2 + Ca_2^2 \\ ac' &= Ab_1^2 + Bb_1b_2 + Cb_2^2 \\ ab' &= 2Aa_1b_1 + B(a_1b_2 + a_2b_1) + 2Ca_2b_2 \,. \end{aligned}$$

Hint: try $x = z = 1, y = w = 0$ for the first.

ii) Prove that $a^2(b'^2 - 4ac') = (a_1b_2 - a_2b_1)^2(B^2 - 4AC)$, henc econcude

$$f(1, 0) = a = \pm(a_1b_2 - a_2b_1) \,.$$

iii) Prove that

$$g(1, 0) = a' = \pm(a_1c_2 - a_2c_1)$$

Exercise 7.16. Recall that a group of order 4 is is isomorphic to either $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, or to $\mathbb{Z}/4\mathbb{Z}$. Determine the class group $\mathcal{C}(D)$ for $D = -56$, $D = -68$, $D = -84$, $D = -96$. Do you see any connection between $\mathcal{C}(D)$ and when genus theory works? Hint: to distinguish between $\mathbb{Z}/\mathbb{Z}2\times\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ you only need to check whether some form is not properly equivalent to its inverse. Why? This is easy to see using reduced forms.

Exercise 7.17. It is known that any *ternary* quadratic form $f(x, y, z)$ of determinant $\det(f) = 1$ is properly equivalent to $x^2 + y^2 + z^2$. (See Corollary 2 [Cas08, p. 138].) Assuming this, show that there is no (nice!) notion of composition of integral ternary quadratic forms of fixed determinant. Hint: we would (want to) have

$$(x^2+y^2+z^2)(u^2+v^2+w^2) = (B_1(x,y,z;u,v,w))^2+(B_2(x,y,z;u,v,w))^2+(B_3(x,y,z;u,v,w))^2\,,$$

where $B_i(x, y, z; u, v, w) = a_{1,1}xu + \cdots + a_{3,3}zw$ are integral bilinear forms. Consider representations of $15 = 3 \times 5$ by $x^2 + y^2 + z^2$.

Exercise 7.18. Suppose $D < 0$ is a discriminant, and that q is a prime such that $\left(\frac{D}{q}\right) = 1$. Show that

$$h(D) \geq \log\left(\frac{1}{4}(|D|)\right) / \log q\,.$$

Hint: some $g(x, y)$ of discriminant D represents q. If g has order M in the class group, then q^M is represented by the principal form. Put a bound on q^M.

Remark: With slightly stronger analysis, one can prove the bound

$$h(D) - 1 \geq \log\left(\frac{1}{4}(|D| + 1)\right) / \log(q)\,.$$

For this, see the paper "Über die Klassenzahl imaginär-quadratischer Zahlkörper", Nagel 1922.

CHAPTER 8

The class group, and advanced aspects of genus theory

With the now established composition of binary quadratic forms, we can now study genus theory in more detail. We will be able to prove some non-trivial facts about the number of genera, and the number of classes per genera.

8.1. Relation between class group and genera

We can relate he class group $\mathcal{C}(D)$ to genus theory by way of the following map. Recall the map $\chi\colon (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$, and the subgroup H of values represented by the principal form. We also know that the values represented by other forms are cosets of H in $\ker\chi$. Since all quadratic forms in a given class represent the same values, we can define the following map

$$\Phi\colon \mathcal{C}(D) \twoheadrightarrow \ker\chi/H\,,$$

sending the class C to the coset of values it represents. This map is a group homomorphism:

Proof. Suppose that $f \mapsto H'$ and $g \mapsto H''$. The composition $f\circ g$ in the class group represents values in $H'H''$, as seen using the Gauss direct composition definition. Thus $\Phi(f\circ g) = HH'' = \Phi(f)\Phi(g)$. So Φ is a group homomorphism. □

Notice that $\Phi^{-1}(H')$, for $H' \in \ker\chi/H$ consists of all classes in a given genus, and $\operatorname{im}\Phi = \ker\chi/H$ may be identified with the set of genera.

Theorem 8.1. *Let D be a discriminant. Then*

- *All genera of forms of discriminant D consist of the same number of classes*
- *The number of genera is a power of 2*

Proof. For i) it is a standard fact in group theory that all 'fibres' (preimages $\phi^{-1}(x)$, $x \in \operatorname{im}(\phi)$) contain the name number of elements. The fibre $\phi^{-1}(x)$ is a coset of $\ker\phi = \phi^{-1}(0)$, and we know cosets have the same cardinality.

For ii) we note that H contains all squares in $(\mathbb{Z}/D\mathbb{Z})^*$, since principal form $f(x,y) = x^2 + \cdots$ takes value $f(x,0) = x^2$. Thus every element in $\ker\chi/H$ has order ≤ 2, whence

$$\ker\chi/H \cong (\mathbb{Z}/2\mathbb{Z})^m$$

for some m, (by the classification of finitely generated abelian groups). Since $\Phi(\mathcal{C}(D)) = \ker\phi/H$ is the set of genera, we see that the number of genera is 2^m, for some m. □

Lecture 11
05/07/2017

8.2. Structure of $\mathcal{C}^{(+)}(D)$

With deeper understanding of the class group, we can produce further results about the genera. We focus on the positive-definite case $D < 0$, and in particular on $D = -4n$ for simplicity. But most of the results hold for any discriminant.

Lemma 8.2. *A reduced form of discriminant $D < 0$ has order ≤ 2 in the class group if and only if $b = 0, a = b$ or $a = c$.*

Proof. We know that the inverse of $f = (a, b, c)$ is the class of the improperly equivalent form $f' = (a, -b, c)$. The element f has order ≤ 2 if and only if f is properly equivalent to its opposite.

Case 1: $|b| < a < c$. Then f' is also reduced, and so the two forms are equivalent if and only if $b = 0$.

Case 2: $a = b$ or $a = c$ then our study of reduced forms shows that (a, b, c) and $(a, -b, c)$ are properly equivalent. □

Theorem 8.3. *Let D be a discriminant. Write r for the number of odd primes dividing D, and define μ as follows.*

If $D \equiv 1 \pmod 4$, then $\mu = r$. Otherwise, $D \equiv 0 \pmod 4$, so $D = -4n$ with $n > 0$. Define μ by the table

n	μ
$n \equiv 3 \pmod 4$	r
$n \equiv 1, 2 \pmod 4$	$r + 1$
$n \equiv 4 \pmod 8$	$r + 1$
$n \equiv 0 \pmod 8$	$r + 2$

Then the class group $\mathcal{C}^{(+)}(D)$ has exactly $2^{\mu-1}$ elements of order ≤ 2.

Sketch. We treat the case $D = -4n < 0$ where $n \equiv 1 \pmod 4$ only. Since $D \equiv 0 \pmod 4$, b is even. We count the number of reduced forms satisfying $2b = 0$, $a = 2b$ or $a = c$. Then since n is odd, r is the number of prime divisors of n, and we want to show $\mu = r + 1$.

For $2b = 0$, we require $ac = n$, with a, c relatively prime and $a < c$. There are 2^r choices for (a, c) relatively prime, and half of these have $a < c$. So there are 2^{r-1} reduced forms of type $ax^2 + cy^2$.

Now consider $a = 2b$ or $a = c$. Write $n = bk$, where b, k coprime and $0 < b < k$. There are 2^{r-1} such $b's$. Set $c = \frac{1}{2}(b + k)$. Then $2bx^2 + 2bxy + cy^2$ has discrimiannt $-4n$, and is reduced since $n \equiv 1 \pmod 4$.

This gives 2^{r-1} reduced forms

$$2b < c : 2bx^2 + 2by + cy^2 \text{ is reduced}$$

$$2b > c : 2bx^2 + 2by + cy^2 \text{ is equivalent to}$$

$$cx^2 + 2(c - b)xy + cy^2 \text{ via } (x, y) \mapsto (-y, x + y)$$

Latter is reduced since $2b > c \Rightarrow 2(c - b) < c$.

I claim this gives all reduced forms with $a = 2b$, or $a = c$. Thus we get $2^{r-1} + 2^{r-1} = 2^r$ elements of order ≤ 2. Hence $\mu = r + 1$. □

This also holds for $D > 0$, but requires much more work since reduced forms can be properly equivalent amongst themselves, making it difficult to enumerate elements of order ≤ 2.

8.3. Structure of the genera

Theorem 8.4. *Let D be a discriminant.*

i) There are $2^{\mu-1}$ genera of forms of discriminant D, where μ is defined above.
ii) The principal genus (containing the principal form) consists of $\mathcal{C}^{(+)}(D)^2$, the subgroup of squares in $\mathcal{C}^{(+)}(D)$. So every form in the principal genus arises by squaring.

In order to sketch the proof of this theorem, we introduce a more efficient method for determining when two forms are in the same genus. Let $p_1, \ldots, p_r$ be the distinct odd primes dividing D. Define the following functions ('characters')

$$\chi_i(a) = \left(\frac{a}{p_i}\right) \text{ for } a \text{ coprime to } p_i$$
$$\delta(a) = (-1)^{(a-1)/2} \text{ for } a \text{ odd}$$
$$\epsilon(a) = (-1)^{(a^2-1)/8} \text{ for } a \text{ odd}$$

For $D \equiv 1 \pmod 4$ we use the characters $\chi_1, \ldots, \chi_r$. For $D \equiv 0 \pmod 4$, write $D = -4n$, and use the following characters

n	characters
$n \equiv 3 \pmod 4$	χ_i
$n \equiv 1 \pmod 4$	χ_i, δ
$n \equiv 2 \pmod 8$	$\chi_i, \delta\epsilon$
$n \equiv 6 \pmod 8$	χ_i, ϵ
$n \equiv 4 \pmod 8$	χ_i, δ
$n \equiv 0 \pmod 8$	χ_i, δ, ϵ

The number of characters assigned is exactly the number μ given above. Then define a map

$$\Psi \colon (\mathbb{Z}/D\mathbb{Z})^* \to (\mathbb{Z}/2\mathbb{Z})^\mu .$$

Lemma 8.5. *The homomorphism $\Psi \colon (\mathbb{Z}/D\mathbb{Z})^* \to (\mathbb{Z}/2\mathbb{Z})^\mu$ is surjective, and its kernel is the subgroup H of values represented by the principal form. Thus*

$$(\mathbb{Z}/D\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^\mu .$$

Sketch of Theorem. For i) Since $\ker\chi$ has index 2 in $(\mathbb{Z}/D\mathbb{Z})^*$ (because $(\mathbb{Z}/D\mathbb{Z})^* \xrightarrow{\chi} \mathbb{Z}/2\mathbb{Z}$ is surjective, so $(\mathbb{Z}/D\mathbb{Z})^*/\ker\chi \cong \mathbb{Z}/2\mathbb{Z}$), we find

$$\ker\chi/H \overset{\text{index } 2}{\subset} (\mathbb{Z}/D\mathbb{Z})^*/H ,$$

so $\ker\chi/H \cong (\mathbb{Z}/2\mathbb{Z})^{\mu-1}$. Since $\ker\chi/H$ is the set of genera, we conclude there are $2^{\mu-1}$ such genera.

To prove ii) We recall that $\Phi\colon \mathcal{C}^{(+)}(D) \to \ker\chi/H \cong (\mathbb{Z}/2\mathbb{Z})^{\mu-1}$ is a group homomorphism. Thus $\mathcal{C}^{(+)}(D)^2 \subset \ker\Phi$, as $\phi(x^2) = \phi(x)^2 = (\pm 1)^2 = 1$. So we have a map

$$\mathcal{C}^{(+)}(D)/\mathcal{C}^{(+)}(D)^2 \to (\mathbb{Z}/2\mathbb{Z})^{\mu-1}\,.$$

What is the order of $\mathcal{C}^{(+)}(D)/\mathcal{C}^{(+)}(D)^2$? Notice $\mathcal{C}^{(+)}(D)/\mathcal{C}^{(+)}(D)^2$ can be identified with the elements of order ≤ 2 in $\mathcal{C}^{(+)}(D)$, so it has order $2^{\mu-1}$, by an earlier result. But this map is surjective, since the original map Φ was. Since the two sides have the same order, we see it is injective, and thus is a group isomorphism. □

Definition 8.6 (Genus, Gauss)**.** Given a form $f(x,y)$ of discriminant D, find a number a coprime to D which $f(x,y)$ represents. Evaluate the μ-tuple of characters ,as defined above. This gives the *complete* character of $f(x,y)$.

Two forms are in the same genus, if they have the same complete character.

Lemma 8.7. *The complete character depends only on the form $f(x,y)$, and this definition of genus agrees with the previous.*

Proof. The complete character is the map $\Psi(a)$, where $\Psi\colon (\mathbb{Z}/D\mathbb{Z})^* \to (\mathbb{Z}/2\mathbb{Z})^\mu$, as before. The possible a's lie in a coset H' of H in $(\mathbb{Z}/D\mathbb{Z})$. The complete character is uniquely determined by the coset H. □

Example 8.8. We can use Gauss's definition to determine the genera for $D = -164$. Since $D = -164 = -4 \times 41$, has $r = 1$ odd prime divisor, $n = 41 \equiv 1 \pmod 4$ and have $\mu = r + 1$. We assign characters $\chi_1 = \left(\frac{\cdot}{41}\right)$, $\delta = (-1)^{(a-1)/2}$. We find

Form	Represents	χ_1	δ
(1, 0, 41)	1	1	1
(2, 2, 21)	21	1	1
(3, -2, 14)	3	-1	-1
(3, 2, 14)	3	-1	-1
(5, -4, 9)	5	1	1
(5, 4, 9)	5	1	1
(6, -2, 7)	7	-1	-1
(6, 2, 7)	7	-1	-1

using

$$\left(\frac{3}{41}\right) = \left(\frac{41}{3}\right)(-1)^{(41-1)(3-1)/4} = -1$$
$$\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right)(-1)^{(41-1)(5-1)/4} = 1$$
$$\left(\frac{7}{41}\right) = \left(\frac{41}{7}\right)(-1)^{(41-1)(7-1)/4} = -1\,.$$

So we see that the following forms are in the same genus

$$\{\,(1,0,41),(2,2,21),(5,-4,9),(5,4,9)\,\}\,\{\,(3,-2,14),(3,2,14),(6,-2,7),(6,2,7)\,\}\,.$$

We compute that

$$\ker(\chi_1,\delta) = \{\,1,5,9,21,25,33,3745,49,57,61,73,77,81,105,113,121,125,133,141\,\} \subset (\mathbb{Z}/164\mathbb{Z})^*$$

meaning these are the values represented by the genera containing $(1, 0, 41)$. Therefore the other genus represents, say $3\times$ these, giving

$$\{\, 3, 7, 11, 15, 19, 27, 35, 47, 55, 63, 67, 71, 75, 79, 95, 99, 111, 135, 147, 151 \,\} \,.$$

Theorem 8.9. *Let D be a discriminant. Then the following are equivalent*

i) Every genus of forms of discriminant D contains a single class
ii) The class group $\mathcal{C}^{(+)}(D)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$ for some integer m
iii) The class number $h^{(+)}(D)$ equals $2^{\mu-1}$

Sketch. i) implies ii) If every genus contains a single class, then $\mathcal{C}^{(+)}(D)^2 = \{\, 1 \,\}$ as this is the principal genus. So every element of $\mathcal{C}^{(+)}(D)$ has order ≤ 2. The only finite abelian groups with this property are of the form $(\mathbb{Z}/2\mathbb{Z})^m$. (There can be no $\mathbb{Z}$-summand by by finiteness, and no $\mathbb{Z}/(> 2\mathbb{Z})$-summand).

ii) implies iii) We know $h^{(+)}(D) = \mathcal{C}^{(+)}(D) = \#(\mathcal{C}^{(+)}(D)/\mathcal{C}^{(+)}(D)^2) \cdot \#(\mathcal{C}^{(+)}(D)^2) = 2^{\mu-1} \cdot 1$.

iii) implies i). Using the above equation, $h^{(+)}(D) = 2^{\mu-1}$ implies $\#(\mathcal{C}^{(+)}(D)^2) = 1$, hence the principal genus (and so all genera) contain a single class. □

Theorem 8.10. *Let $f(x, y)$ and $g(x, y)$ be primitive forms of discriminant D. The the following are equivalent:*

i) $f(x, y)$ and $g(x, y)$ are in the same genus, so represent the same values in $(\mathbb{Z}/D\mathbb{Z})^*$,
ii) $f(x, y)$ and $g(x, y)$ represent the same values in $(\mathbb{Z}/m\mathbb{Z})^*$ for all non-zero m, so congruence can never distinguish f and g,
iii) $f(x, y)$ and $g(x, y)$ are $\mathrm{GL}_2(\mathbb{Q})$-equivalent over $\mathbb{Q}$ via a matrix whose denominators are coprime to $2D$.

Exercises

Exercise 8.11. Let $p \equiv 1 \pmod 8$ be prime.

i) Let $\mathcal{C}(-4p)$ be the class group of discriminant $D = -4p < 0$. Use genus theory to prove that
$$\mathcal{C}(-4p) \cong (\mathbb{Z}/2^a\mathbb{Z}) \times G \,,$$
where $\#G$ is odd, and $a \geq 1$. And hence $2 \mid h(-4p)$. Hint: recall the fundamental theorem for finitely generated abelian groups. How many elements of order 2 are in $\mathcal{C}(-4p)$?
ii) Use Gauss's definition of genus to show that
$$2x^2 + 2xy + ((p + 1)/2)y^2$$
is in the principal genus. Hint: it is easier to use the Jacobi symbol, not the Legendre symbol.
iii) Use Theorem 8.4 to show $\mathcal{C}(-4p)$ has en element of order 4, hence conclude $4 \mid h(-4p)$.

Part 2

Advanced topics in quadratic forms (NON-EXAMINABLE)

CHAPTER 9

Cubic reciprocity and $p = x^2 + 27y^2$

Lecture 12
12/07/2017
Exam!

Lecture 13
19/07/2017

Here we briefly sketch the introductory ideas involved in establishing results for $p = x^2 + ny^2$, when genus theory begins to fail.

9.1. The ring $\mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{-3}}{3}$

The law of cubic reciprocity is connected closely with the ring $\mathbb{Z}[\omega]$, where $\omega = \frac{-1+\sqrt{-3}}{2}$. We state some of the important properties of this ring.

Definition 9.1 (Norm)**.** The norm $N\colon \mathbb{Z}[\omega] \to \mathbb{Z}$ is defined by

$$\begin{aligned} N\colon \mathbb{Z}[\omega] &\to \mathbb{Z} \\ a + b\omega &\mapsto (a + b\omega)(a + b\overline{\omega}) = a^2 - ab + b^2\,, \end{aligned}$$

where $\bar{\cdot}\colon \sqrt{-3} \leftrightarrow -\sqrt{-3}$ is the complex conjugate.

With the norm, one can define a division algorithm in $\mathbb{Z}[\omega]$, which makes $\mathbb{Z}[\omega]$ into a Euclidean ring. In particular, it is a unique factorisation domain: every element factors uniquely into a product of (suitably generalised) prime elements.

Proposition 9.2. *The units (elements with multiplicative inverses) in $\mathbb{Z}[\omega]$ are $\pm 1, \pm\omega, \pm\omega^2$.*

Proposition 9.3. *The prime elements of $\mathbb{Z}[\omega]$ are determined as follows. Let p be a prime of $\mathbb{Z}$, then*

- *If $p = 3$, then $1 - \omega$ is prime in $\mathbb{Z}[\omega]$, and $3 = -\omega^2(1 - \omega)^2$.*
- *If $p \equiv 1 \pmod 3$, then $p = a^2 - ab + b^2$, and $\pi = a + b\omega$ is prime in $\mathbb{Z}[\omega]$, where π and $\overline{\pi}$ do not differ by a unit.*
- *If $p \equiv 2 \pmod 3$, then p is prime in $\mathbb{Z}[\omega]$.*

This accounts for all primes of $\mathbb{Z}[\omega]$.

Proposition 9.4. *Given a prime π of $\mathbb{Z}[\omega]$, then the quotient field $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ (compare with $\mathbb{Z}/p\mathbb{Z}$!) is a finite field with $N(\pi)$ elements. Moreover $N(\pi) = p$, or p^2 for some prime integer p.*

- *If $p = 3$, or $p \equiv 1 \pmod 3$, then $N(\pi) = 3$ and $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] \cong \mathbb{Z}/p\mathbb{Z}$.*
- *If $p \equiv 3$, then $N(\pi) = p^2$, and $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ is a field with p^2 elements, containing $\mathbb{Z}/p\mathbb{Z}$ as a unique subfield.*

Corollary 9.5. *If π is prime in $\mathbb{Z}[\omega]$, and $\pi \nmid \alpha \in \mathbb{Z}[\omega]$, then*

$$\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$$

because $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ is a finite group with $N(\pi) - 1$ elements.

9.2. Cubic residue symbol and cubic reciprocity

We can use these properties to define a generalised Legendre symbol, $\left(\frac{\alpha}{\pi}\right)_3$ dealing with cubic residues. Let π be a prime of $\mathbb{Z}[\omega]$ not dividing 3 (i.e. not associae to $1-\omega$). Then $3 \mid N(\pi) - 1$, so

$$x = \alpha^{(N(\pi)-1)/3}$$

is a root of $x^3 \equiv 1 \pmod{\pi}$. By factoring $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$, it follows that

$$\alpha^{(N(\pi)-1)/3} \equiv 1, \omega, \omega^2 \pmod{\pi}.$$

We define the Legendre symbol $\left(\frac{\alpha}{\pi}\right)_3$ to be the unique cube root of 1 such that

$$\alpha^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}.$$

(Compare with Euler's criterion for the quadratic residue symbol!)

We get some properties, very similar to that for the quadratic residue symbol.

Proposition 9.6. *The Legendre symbol $\left(\frac{\alpha}{\pi}\right)_3$ is multipliative in the top argument*

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3.$$

The Legendre symbol only depends on $\alpha \pmod{\pi}$, so $\alpha \equiv \beta \pmod{\pi}$ implies

$$\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$$

We can connect the Legendre symbol with cubic residues as follows. Since $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])$ is a finite field, the group of units is (necessarily) cyclic. So we obtain the following.

Proposition 9.7. *The following are equivalent*

i) The congruence $x^3 \equiv \alpha \pmod{\pi}$ has a solution in $\mathbb{Z}[\omega]$
ii) The symbol $\left(\frac{\alpha}{\pi}\right)_3 = 1$.

Proof. Both are equivalent to $\alpha^{(N(\pi)-1)/3} \equiv 1 \pmod{\pi}$. □

To state the law of cubic reciprocity, we also need the notion of a primary prime. A prime π is called *primary* if $\pi \equiv \pm 1 \pmod{3}$. Exactly 2 of the associates $\pm\pi, \pi\omega\pi, \pm\omega^2\pi$ are primary.

Theorem 9.8 (Cubic reciprocity)**.** *Let π and θ be primary primes in $\mathbb{Z}[\omega]$ with $N(\pi) \neq N(\theta)$. Then*

$$\left(\frac{\pi}{\theta}\right)_3 = \left(\frac{\theta}{\pi}\right)_3.$$

Like quadratic reciprocity, there are supplementary laws for $\left(\frac{\omega}{\pi}\right)_3$ and $\left(\frac{1-\omega}{\pi}\right)_3$. Namely for $\pi \equiv -1 \pmod 3$ (can assume this), write $\pi = -1 + 3m + 3n\omega$. Then

$$\left(\frac{\omega}{\pi}\right)_3 = \omega^{m+n}$$
$$\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2m}$$

What does cubic reciprocity and $\mathbb{Z}[\omega]$ have to do with cubic residues in $\mathbb{Z}/p\mathbb{Z}$, and solving $x^3 \equiv a \pmod p$?

If $p = 3$, then $a^3 \equiv a \pmod 3$, by Fermat's little Theorem. So this the equation always has a solution. If $p \equiv 2 \pmod 3$, then $3 \nmid p - 1$ and so the map $a \mapsto a^3$ is an automorphism of $(\mathbb{Z}/p\mathbb{Z})^*$. So $x^3 \cong a \pmod p$ also always has a solution.

For $p \equiv 1 \pmod 3$, we have to deal with the cubic residue symbol. We have $p = \pi\overline{\pi}$ in $\mathbb{Z}[\omega]$, and an isomorphism

$$(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/[\omega]/\pi\mathbb{Z}[\omega])$$

So for $p \nmid a$, we get

$$x^3 \equiv a \pmod p \text{ solvble in } \mathbb{Z} \iff \left(\frac{a}{\pi}\right)_3 = 1.$$

9.3. Application to $p = x^2 + 27y^2$

We can now prove (or at least sketch the proof of) Euler's conjecture about primes of the form $x^2 + 27y^2$.

Theorem 9.9. *Let p be a prime. Then $p = x^2 + 27y^2$ if and only if $p \equiv 1 \pmod 3$ and 2 is a cube modulo p.*

Proof. We show both directions separately.

'$\Rightarrow$': Suppose that $p = x^2 + 27y^2$. Then, in particular $p = x^2 + 3(3y)^2$, so is of the form $a^2 + 3b^2$, and hence $p \equiv 1 \pmod 3$. So need to show 2 is a cube modulo p.

Let $\pi = x + 3\sqrt{-3}y$, so that $p = \pi\overline{\pi}$, whence π is prime in $\mathbb{Z}[\omega]$. So

$$2 = x^3 \pmod p \iff \left(\frac{2}{\pi}\right)_3 = 1\,.$$

Both 2 and $x + 3\sqrt{-3}y$ are primary primes, so cubic reciprocity implies

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3.$$

Then

$$\left(\frac{\pi}{2}\right)_3 \equiv \pi^{(N(2)-1)/3} = \pi \pmod 2\,.$$

We need to show that $\pi \equiv 1 \pmod 2$.

But $\pi = x + 3\sqrt{-3}y = x + 3(1 + 2\omega)y = x + 3y + 6\omega y \equiv x + y \pmod 2$. Since $p = x^2 + 27y^2$, x and y have opposite parity, so $\pi \equiv 1 \pmod 2$.

'$\Leftarrow$': Suppose that $p \equiv 1 \pmod 3$ prime and $2 \equiv a^3 \pmod p$. We can write $p = \pi\overline{\pi}$ in $\mathbb{Z}[\omega]$, where $\pi = a + b\omega$. We can assume (by going to an associate), that π is primary. So $\pi = a + 3b\omega$, for some $a, b \in \mathbb{Z}$.

Thus

$$4p = 4\pi\overline{\pi} = 4(a^2 - 3ab + 9b^2) = (2a - 3b)^2 + 27b^2 \,.$$

Since 2 is a cube modulo p, we have that $\left(\frac{2}{\pi}\right) = 1$, so that cubic reciprocity says $\left(\frac{\pi}{2}\right) = 1$, and hence $\pi \equiv 1 \pmod 2$. So $a + 3b\omega \equiv 1 \pmod 2$, so a is odd, and b is even.

Then

$$p = (a - 3\tfrac{b}{2})^2 + 27(\tfrac{b}{2})^2 \,,$$

showing p has the required form. □

9.4. Artin reciprocity, and class field theory

This introduction of 'cubic reciprocity' and the similar biquadratic reciprocity for $x^4 \equiv p \pmod q$, using $\mathbb{Z}[i]$, sparked the search for more and more general reciprocity laws. This is the Artin reciprocity law, which relates ideals/ideal classes to elements of the Galois group of an abelian extension L/K of number fields. One can use the Artin symbol and the class fields to study how a prime ideal $\mathfrak{p}$ in K factorises when lifted to L. In particular the Hilbert class field H can be used to detects when a prime ideal p factors into principal ideals $K = \mathbb{Q}(\sqrt{-d})$, and hence give a condition on when $p = x^2 + ny^2$. This detection is based on the factorisation modulo p, of the polynomial f describing the extension how the H/K is generated.

One obtains the abstract result that

Theorem 9.10. *Let $D = -4n < 0$ be a discriminant, then there exists a polynomial $f_{-4n}(x)$ of degree $h(-4n)$ such that for $p \nmid \operatorname{disc}(f_{-4n})$*

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{D}{p}\right) = 1 \text{ and,} \\ f_{-4n}(x) \equiv 0 \pmod p \text{ has a solution.} \end{cases}$$

The polynomial $f_{-4n}(x)$ can be made explicit for each choice of n, but requires advanced computational techniques.

Example 9.11. When $D = -4 \cdot 27$, one finds that $f_{-4\cdot 27}(x) = x^3 - 2$ works, and $\left(\frac{-27}{p}\right) = \left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \pmod 3$, recovering the result above. Notice $h(-4 \cdot 27) = 3$, since there are 3 reduced forms of discriminant $D = -4 \cdot 27$ namely:

$$x^2 + 27y^2, 4x^2 \pm 2xy + 7y^2$$

We also obtain the following condition for the other forms $4x^2 \pm 2xy + 7^2$, by negating the condition above

$$p = 4x^2 \pm 2xy + 7y^2 \iff \begin{cases} p \equiv 1 \pmod 3 \\ 2 \text{ is not a cube modulo } p. \end{cases}$$

Exercises

Exercise 9.12. With cubic reciprocity, we can handle another one of Euler's conjectures:

$$4p = x^2 + 243y^2 \iff \begin{cases} p \equiv 1 \pmod 3 \text{ and} \\ 3 \equiv a^3 \pmod p \end{cases}$$

Let $p \equiv 1 \pmod 3$ be prime.

i) Use the proof of $p = x^2 + 27y^2$ to show that
$$4p = a^2 + 27b^2$$
where we can take $a \equiv 1 \pmod 3$.

ii) Conclue that $\pi = (a + 3\sqrt{-3}b)/2$ is a primary prime of $\mathbb{Z}[\pi]$, and that $p = \pi\overline{\pi}$.

iii) For $\pi = (a + 3\sqrt{-3}b)/2$, show that the supplementary laws can be written as
$$\left(\frac{\omega}{\pi}\right)_3 = \omega^{2(a+2)/3}$$
$$\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{(a+2)/3+b}$$

iv) Conclude $\left(\frac{3}{\pi}\right)_3 = \omega^{2b}$.

v) Use this to prove Euler's conjecture, above.

CHAPTER 10

Modular forms and theta series

10.1. Definition and properties of modular forms

Lecture 14
26/07/2017

A (classical) modular form for $\mathrm{SL}_2(\mathbb{Z})$ is a 'nice' function $f\colon \mathbb{H} \to \mathbb{C}$, which satisfies a certain symmetry law when transformed by $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Definition 10.1 (Upper half plane)**.** The upper half-plane is

$$\mathbb{H} \coloneqq \{\, z = x + iy \in \mathbb{C} \mid y > 0 \,\} \,.$$

Definition 10.2 (Modular form of weight k)**.** A function $f\colon \mathbb{H} \to \mathbb{C}$ is said to be modular, of weight k the following conditions hold

i) f is holomorphic on $\mathbb{H}$,
ii) For $z \in \mathbb{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we have

$$f(\gamma \cdot z) \coloneqq f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)\,,$$

and
iii) f is holomorphic at $i\infty$.

We write M_k for the $\mathbb{C}$-vector space of weight k modular forms.

Fact 10.3. Since $f(z+1) = f(z)$, using $\gamma = T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we see that any modular form is $\mathbb{Z}$-periodic. Hence it has a Fourier expansion:

$$f(z) = \sum_{i=0}^{\infty} a_n q^n \,,$$

where $q = \exp(2\pi i z)$. The expansion starts at $n = 0$, since f is 'holomorphic at $z = i\infty \leftrightarrow q = 0$'.

If $a_0 = 0$, then the modular form $f(z)$ is said to vanish at the cusp $i\infty$. Then $f(z)$ is called a *cusp form*. Write S_k for the space of cusp forms (*Spitzenformen*).

Often, one *defines* a modular form by giving the coefficients a_n in the *q-expansion*. This becomes important when we study quadratic forms using theta series. Regardless, these coefficients a_n hold a lot of *arithmetic* information.

Definition 10.4 (Eisenstein series)**.** The *Eisenstein series* of weight $2k$ is defined by

$$G_{2k}(z) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus (0,0)} \frac{1}{(m+\tau)^{2k}} \,.$$

It is modular of weight $2k$, for $k \geq 2$.

Fact 10.5. The q-expansion of $G_{2k}(z)$ has the following form

$$G_{2k}(z) = 2\zeta(2k)\Big(1 + \underbrace{\frac{(2\pi i)^{2k}}{(2k-1)!\zeta(2k)}}_{\text{rational}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n\Big),$$

where

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

is the sum of α-th power of divisors function. *Very arithmetical!*

$$\begin{aligned} G_4(z) &= \tfrac{\pi^4}{45}(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n) \\ G_6(z) &= \tfrac{2\pi^4}{945}(1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n) \\ &\vdots \end{aligned}$$

For notational ease, one often writes

$$E_{2k}(z) = \frac{G_{2k}(z)}{2\zeta(2k)} = 1 + \underbrace{\frac{(2\pi i)^{2k}}{(2k-1)!\zeta(2k)}}_{\text{rational}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

10.2. Applications of modular forms

Why should we care these objects? One reason is the ease by which one can extract highly-non-trivial arithmetic identities by comparing the coefficients of relations between modular forms. This is based on the following fact

Fact 10.6. The space M_k of weight k modular forms is *finite* dimensional. Specifically

$$\dim_{\mathbb{C}} M_k = \begin{cases} \lfloor k/12 \rfloor & k \equiv 2 \pmod{12} \\ \lfloor k/12 \rfloor + 1 & \text{otherwise.} \end{cases}$$

Moreover, any modular form is a polynomial in G_4 and G_6.

This means it is sufficient to compare only finitely many coefficients, to prove that all coefficients are equal.

Example 10.7. Since $\dim_{\mathbb{C}} M_8 = \lfloor 8/12 \rfloor + 1 = 1$, we must have $E_4^2 = \lambda E_8$ since both are modular forms of weight 8. The leading coefficient of both sides is 1, so we must have $\lambda = 1$. This gives the identity

$$(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n)^2 = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n \,.$$

Extracting the coefficient of q^n from both sides, we obtain the non-trivial identity

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{i=1}^{n-1} \sigma_3(i)\sigma_3(n-i)$$

10.3. Theta series

To use modular forms in the study of quadratic forms, we need to generalise various notions/weaken various conditions. We only require the transformation

$$f(\gamma \cdot z) \coloneqq f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

hold for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. For example

$$\Gamma_0(N) \coloneqq \{\, \gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod N \,\}$$
$$\Gamma_1(N) \coloneqq \{\, \gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \pmod N \,\}\,.$$

We can also generalise the transformation law allowed, to include an automorphic factor $\varepsilon(a,b,c,d)$, with absolute value 1, namely requiring

$$f(\gamma \cdot z) \coloneqq f\left(\frac{az+b}{cz+d}\right) = \varepsilon(a,b,c,d)(cz+d)^k f(z)\,.$$

Then we can have modular forms of odd weight, say if $\varepsilon(a,b,c,d) = \chi(d)$, some character, and $\chi(-1) = -1$.

Write

$$M_k(\Gamma, \varepsilon)$$

for the $\mathbb{C}$-vector space of modular forms of weight k, for subgroup Γ, and automorphic factor ε.

Definition 10.8 (Theta series)**.** Let Q be a positive-definite integral quadratic form in n-variables. Let

$$r_Q(m) = \#\{\, \underline{\mathbf{x}} \in \mathbb{Z}^n \mid Q(\underline{\mathbf{x}}) = m \,\}$$

be the representation numbers of Q. Then the *theta series* of Q is defined by

$$\Theta_Q(z) \coloneqq \sum_{\underline{\mathbf{x}} \in \mathbb{Z}^n} q^{Q(\underline{\mathbf{x}})} = \sum_{m=0}^{\infty} r_Q(m) q^m\,.$$

Fact 10.9 (Hecke, Schoenberg, Pfetzer, Shimura)**.** Let Q be a positive-definite integral quadratic form in n variabies, of level N and discriminant D. Then Θ_Q is modular on $\Gamma_0(N)$, of weight $n/2$, and character $\chi_\Delta(\cdot) = \left(\frac{\Delta}{\cdot}\right)$.

If Q has matrix $A = \frac{1}{2}M$, then discriminant D is defined as $(-1)^n \det(A)$. The level of Q is the smallest N such that NA^{-1} is a matrix with integer entries, and even diagonals.

Example 10.10. The series

$$\Theta_{x^2+y^2}(z) = \sum_{n=0}^{\infty} r_{x^2+y^2}(n) q^n = 1 + 4q + 4q^2 + 4q^4 + 8q^5 + 4q^8 + \cdots$$

is a modular form of weight 1, and character $\chi_{-4} = \left(\frac{-4}{\cdot}\right)$ on $\Gamma_0(4)$.

Let *chi*: $(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}$ (extended to $\mathbb{Z}$, in the natural way) be a character. Then the Eisensteinseries $G_{k,\chi}$ defined by

$$G_{k,\chi}(z) = a_0 + \sum_{n=1}^{\infty} \left(\sum_{d \mid n} \chi(d) d^{k-1} \right) q^n$$

is a modular form of weight k, and character χ on $\Gamma_0(N)$. Here a_0 is some suitable constant, which must be determined explicitly.

One finds

$$G_{1,\chi_{-4}}(z) = \frac{1}{4} + \sum_{n=1}(\sum_{d|n} \chi_{-4}(d))q^n = \frac{1}{4} + q + q^2 + q^4 + 2q^5 + q^8 + \cdots$$

is a modular form of weight 1, and character $\chi_{-4} = \left(\frac{-4}{\cdot}\right)$. One can prove that $M_1(\Gamma_0(4), \chi_{-4})$ is a 1-dimensional vector space. Thus by comparing the constant coefficient, we must have

$$\Theta_{x^2+y^2}(z) = 4G_{1,\chi_{-4}}(z)\,,$$

and by comparing the q^n coefficient, we find

$$r_{x^2+y^2}(n) = 4\sum_{d|n}\left(\frac{-4}{n}\right).$$

For an odd prime $n = p$, we see

$$r_{x^2+y^2}(p) = 4(1 + \left(\tfrac{-4}{p}\right))\,,$$

so that

$$p = x^2 + y^2 \iff \left(\frac{-4}{p}\right) = 1 \iff p \equiv 1 \,(\mathrm{mod}\ 4)\,,$$

and we recover Fermat's theorem, along with a precise count for the *number* of representations. Namely for $p \equiv 1 \pmod 4$, we have $r_{x^2+y^2}(p) = 8$, i.e. up to $\pm$, and $x \leftrightarrow y$, there is a unique way of writing $p = x^2 + y^2$.

Example 10.11. One can also study forms with *higher* arity. We find that

$$\Theta_{x_1^2+x_2^2+x_3^2+x_4^2}(z) = 1 + 8q + 24q^2 + 32q^3 + 24q^4 + \cdots$$

is modular of weight 2, for $\Gamma_0(4)$. This space $M_2(\Gamma_0(4))$ is 2 dimensional, and a basis is given by

$$G_2(z) - 2G_2(2z), G_2(2z) - 2G_2(4z)\,,$$

where

$$G_2(z) = -\frac{1}{24} + \sum_{n=1}^{\infty}\sigma_1(n)q^n = -\frac{1}{24} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + \cdots\,.$$

(Note: G_2 itself is not modular, but the non-holomorphic combination $G_2(z) + \frac{1}{8\pi y}$ is otherwise modular of weight 2. The non-holomorphic part cancels in the above combinations.)

One then finds

$$\Theta_{x_1^2+x_2^2+x_3^2+x_4^2}(z) = 8(G_2(z) - 2G_2(2z)) + 16(G_2(2z) - 2G_2(4z))$$

by comparing the first 2 Fourier coefficients. Hence, by comparing q^n, we find

$$r_{x_1^2+x_2^2+x_3^2+x_4^2}(n) = 8\sigma_1(n) - 32\underbrace{\sigma(n/4)}_{0 \text{ if } 4 \nmid n}$$

$$= 8\sum_{\substack{d|n\\ 4\nmid d}} d$$

In partiular, for $n = p$ prime

$$r_{x_1^2+x_2^2+x_3^2+x_4^2}(p) = 8(1+p) > 0\,,$$

so every prime can be written as the sum of 4 squares.

Corollary: every integer can be written as the sum of 4 squares, by using the identity

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) = \\ (a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2 + \\ +(a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2 + \\ +(a_1b_3-a_2b_4-a_3b_1+a_4b_2)^2 + \\ +(a_1b_4+a_2b_3-a_3b_2-a_4b_1)^2\,.\end{aligned}$$

10.4. Class number ≥ 5

Class field theory works to give conditions for all forms of discriminant D, whenever the class number $h(D)$ is 1, 2, 3, 4 or 6. For class number 5, we cannot distinguish the forms $Q(x,y), Q^2(x,y), Q^3(x,y), Q^4(x,y)$ (the exponent means composition, since $\mathcal{C}(D) \cong \mathbb{Z}/5\mathbb{Z}$).

This first occurs for $D = -47$, where we have the forms $(1,1,12), (2,\pm1,6), (3,\pm1,4)$. We obtain 3 distinct Θ-series

$$\begin{aligned}\Theta_0 &= \Theta_{x^2+xy+12y^2}(z) = 1+2q+2q^4+2q^9+4q^{12}+\cdots\\ \Theta_1 &= \Theta_{2x^2+xy+6y^2}(z) = 1+2q^2+2q^6+2q^7+2q^8+2q^9+2q^{12}+\cdots\\ \Theta_2 &= \Theta_{3x^2+xy+4y^2}(z) = 1+2q^3+2q^4+2q^6+2q^8+2q^{12}+\cdots\end{aligned}$$

These are modular of weight 1 for $\Gamma_0(47)$ with character $\varepsilon_{-47} = (-47/\cdot)$. An 'obvious' element of $M_1(\Gamma_0(47), \varepsilon_{-47}$ is $\eta(z)\eta(47z)$ where

$$\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$$

is the Dedekind η-function. It turns out that

$$\frac{1}{2}(\Theta_1-\Theta_2) = \eta(z)\eta(47z)\,.$$

This means that the coefficient a_n of the modular form

$$\eta(z)\eta(47z) \coloneqq q^2\prod_{n=1}^{\infty}(1-q^n)(1-q^{47n}) =: \sum_{n=1}^{\infty}a_nq^n$$

This series already contains enough information to completely characterise the primes represented by $Q_0,\ldots,Q_4$ using the coefficient a_n. If we have $\left(\frac{-47}{p}\right) = 1$, then p is represented by exactly one of Q_0, Q_1, Q_2. If $a_p = 0$, it must be Q_0 since this Θ-series does not contribute to $\eta(z)\eta(47z)$. If $a_p = 1$ it must be Q_1, and if $a_p = -1$ it must be Q_2. So we obtain the criterion

$$p = x^2+xy+12y^2 \iff \begin{cases}(-47/p) = 1, \text{ and}\\ a_p = 0\end{cases}$$

$$p = 2x^2 \pm xy + 6y^2 \iff \begin{cases} (-47/p) = 1, \text{ and} \\ a_p = 1 \end{cases}$$

$$p = 3x^2 \pm xy + 4y^2 \iff \begin{cases} (-47/p) = 1, \text{ and} \\ a_p = -1 \end{cases}$$

By reducing $\eta(z)\eta(47z)$ modulo 47, we can obtain a more explicit version of this criterion. Notice that

$$(1 - q^{47n}) \equiv (1 - q^n)^{47} \pmod{47},$$

since 47 is prime. Thus

$$\eta(z)\eta(47z) \equiv q^2 \prod_{n=1}^{\infty} (1 - q^n)^{48} \pmod{24}.$$

But the function

$$\Delta(z) \coloneqq q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \eta(z)^{24}$$

is a 'well-known' modular form (actually cusp form) called the discriminant function. It is a weight 12 modular form for $\mathrm{SL}_2(\mathbb{Z})$ with no character. Its Fourier coefficients define the Ramanujan-τ function. This $\tau(n)$ function which satisfies some amazing, very deep properties

- τ is multiplicative: $\gcd(m, n) = 1$ implies $\tau(mn) = \tau(m)\tau(n)$.
- $\tau(p^{m+1}) = \tau(p)\tau(p^m) - p^{11}\tau(p^{m-1})$
- $|\tau(p)| \leq 2n^{11/2}$ or more generally $|\tau(n)| \leq \sigma_0(n)n^{11/2}$.

The first two properties follow because $\Delta(z)$ is a 'Hecke-eigenform'. The third property is a related to deep results called the Weil conjecture's, concerned with *zeta functions of curves/varieties over finite fields*. This was proven by Deligne.

A table of the first few values is given below.

n	1	2	3	4	5	6	7	8	9	10
$\tau(n)$	1	-24	252	-1472	4830	-6048	-16744	84480	-113643	-115920

So by reducing modulo 47, we obtain

$$\eta(z)\eta(47z) \equiv \Delta^2(z) \pmod{47}$$

$$a_n \equiv \sum_{i+j=n} \tau(i)\tau(j) \pmod{47},$$

and so can rewrite the condition on $a_p = -1, 0, 1$ in terms of the following 'convolution' of τ with itself:

$$\sum_{i+j=p} \tau(i)\tau(j) \equiv -1, 0, 1 \pmod{47}.$$

Alternatively, we can read this as a congruence theorem for τ, the value depending on which quadratic form represents p. Modulo any other prime, this convolution seems to take all values in all residue classes!

Exercises

Exercise 10.12. Recall that M_k denotes the space of weight k modular forms.

i) Show that M_k is a $\mathbb{C}$-vector space.
ii) If k is odd, show that $M_k = \{ 0 \}$. Hint: consider $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.
iii) Let $f \in M_k$ and $g \in M_\ell$ be two modular forms. Show that fg is also a modular form, and that $fg \in M_{k+\ell}$.

Remark: Don't worry too much about the holomorphic at $i\infty$ condition!

Exercise 10.13. Find a relation between E_4E_6 and E_{10}. Hence derive an identity for σ_9 as a 'convolution' of σ_3 and σ_5 of the form

$$\sigma_9(n) = a\sigma_5(n) + b\sigma_3(n) + c\sum_{i=1}^{n} \sigma_3(i)\sigma_5(n-i)\,.$$

(Here a, b, c are certain rational numbers you should find.)

Bibliography

[Cas08] John William Scott Cassels. *Rational quadratic forms*. Courier Dover Publications, 2008.

[CF97] John Horton Conway and Francis YC Fung. *The sensual (quadratic) form*. 26. MAA, 1997.

[Coh13] Henri Cohen. *A course in computational algebraic number theory*. Vol. 138. Springer Science & Business Media, 2013.

[Cox11] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Vol. 34. John Wiley & Sons, 2011.

[Zag13] Don Bernard Zagier. *Zetafunktionen und quadratische Körper: eine Einführung in die höhere Zahlentheorie*. Springer-Verlag, 2013.