QUADRATIC FORMS

ISHAN LEVY

1. Introduction

When is a prime p of the form x^2+ny^2? More generally, when is it represented by the binary quadratic form $ax^2+bxy+cy^2$ for $a,b,c\in\mathbb{Z}$, meaning $p=ax^2+bxy+cy^2$ has a solution? We can ask which numbers are represented by which quadratic forms and how many representations are there? We will be especially in the case that a number is of the form $ax^2+bxy+cy^2$ with x,y relatively prime, in which case we will say it is **properly represented** by the form. We will explore Lagrange's theory of reduced positive definite forms to get a better grasp on this problem.

We can view $ax^2+bxy+cy^2$ as the product $\begin{pmatrix}x & y\end{pmatrix}\begin{pmatrix}a & \frac{b}{2}\\ \frac{b}{2} & c\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}$ First note that we can replace x,y with linear functions in x and y and the result will still be a quadratic form. If this linear transformation is invertible, then we can say that the two quadratic forms are **isomorphic**. Isomorphic quadratic forms represent the same numbers. In the matrix form, if Q represents the quadratic form and A is the matrix representing the linear transformation, then the new matrix is represented by A^TQA. Since $\det(A^TQA)=\det Q$ as $\det A=\pm1$, $4\det A=b^2-4ac$ is an isomorphism invariant of the quadratic form called its discriminant, denoted $\operatorname{disc}(Q)$. Note that it is $\equiv 0,1 \pmod 4$, and that $b\equiv D \pmod 2$. More generally the discriminant changes by $\det(A)^2$ if A has coefficients in $\mathbb{C}$. We will like to consider **primitive** quadratic forms, namely those where $(a,b,c)=(1)$. The problem of determining what the isomorphism classes of quadratic forms are and how many representations of a number a quadratic form has reduces easily to the case where it is primitive.

The discriminant greatly affects which primes are represented by the form Q. We can complete the square to get $4aQ=(2ax+by)^2-\operatorname{disc}Qy^2$. This means that if $\operatorname{disc}Q>0$, the form is **definite**, meaning that it takes on either nonnegative (positive definite) or nonpositive (negative definite) values depending on the sign of a. If $\operatorname{disc}Q<0$, it takes on both positive and negative values, so is **indefinite**. If $\operatorname{disc}Q=0$, it is **degenerate**, and the equation above makes it easy to determine what numbers are represented by the form. Here all of our forms will be primitive, and positive definite. Note that any discriminant $\equiv 0,1 \pmod 4$ is attained by some quadratic form.

A slightly different equivalence relation that will be important is by requiring the matrix A to be in $\mathrm{SL}_2(\mathbb{Z})$. In this case we will say that Q is **equivalent** to A^TQA.

It is easy to tell when two forms of the class are equivalent as we will soon see. Say that a form is reduced if $|b| \leq a \leq c$ and if either of the inequalities are equalities, then we require b to be nonnegative as well.

Theorem 1.1. *Every quadratic form is equivalent to a unique reduced quadratic form.*

Proof. For existence of an equivalent reduced form, if $|b| > a$, we can consider the map $x, y \mapsto x, y - \mathrm{sign}(b)x$, which will make $|b|$ smaller. If $c \leq a$, we can swap a, c via $x, y \mapsto y, -x$. Finally when $|b| \leq a \leq c$, if $-b = a$, it is easy to see that one of the previous transformations used will force b to be positive while preserving the inequalities.

Now to show that this is unique, we can first observe that for a reduced form, a can be recovered as being the smallest element represented by the form. Then, observe that we can recover whether $a = c$ or not be looking at whether the value a is attained twice or more than twice by the quadratic form. If $a = c$, then b can be recovered from the equation of the discriminant and the fact that it is nonnegative. If $a < c$, then the value a is only obtained by $(x, y) = (1, 0), (-1, 0)$ so the only automorphisms of the quadratic form that fix the coefficient a are $x, y \mapsto \pm x, \mp y + cx$. One only needs to check then that for any reduced form, applying any of these doesn't yield a reduced form. □

Exercise 1.1.1. *The matrices* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *generate* $\mathrm{SL}_2(\mathbb{Z})$.

Let's find all equivalence class of quadratic forms of discriminants -12. For a reduced form, $a \leq \sqrt{12/3} = 2$. and b is an even number with $b \leq a$. So either $(a, b) = (1, 0), (2, 0), (2, 2)$. $c = \frac{b^2 - D}{/} 4a$, giving the forms $x^2 + 3y^2, 2x^2 + \frac{3}{2}y^2, 2x^2 + 2xy + 2y^2$. The only one that is primitive is $x^2 + 3y^2$, so there is only one equivalence class.

Question 1.2. *Is there a notion of reduced form for indefinite forms? Is it unique?*

For $D < 0$ a discriminant, let $\mathrm{Cl}(D)$ be the set of equivalence classes of quadratic forms of a particular discriminant. It is called the class group (though for now it is only a set).

Theorem 1.3. $\mathrm{Cl}(D)$ *is finite.*

Proof. We only need to show there are finitely many reduced forms. For a reduced form, $D = b^2 - 4ac \leq a^2 - 4a^2 = -3a^2$, so $|b| \leq a \leq \sqrt{-\frac{D}{3}}$, and c is determined by a, b via the formula for D. Thus there are only finitely many possibilities. □

We define $h(D)$ to be the size of $\mathrm{Cl}(D)$, and call it the **class number** of D.

When is a number properly represented by a particular quadratic form? Here is a necessary and sufficient condition for this given a fixed discriminant.

Lemma 1.4. *f is properly represented by a quadratic form iff the form is equivalent to a form $fx^2 + bxy + cy^2$*

Proof. Suppose f is properly represented by some quadratic form $ax^2+bxy+cy^2$ for $x = r, y = s$. Then there is a solution to $rp - sq = 1$, so consider the transformation $(x, y) \to (rx+qy, sx+py)$, and we will get an equivalent form with the x^2 coefficient f. Conversely, if the x^2 coefficient is f, then $x = 1, y = 0$ will yield f. □

Theorem 1.5. *f is properly represented by a quadratic form of discriminant D iff D is a square mod $4f$.*

Proof. By the previous theorem we can assume that the form is $fx^2 + bxy + cy^2$. Then $D = b^2 - 4fc$ iff $D \equiv b^2 \pmod{4f}$. Conversely, if we can solve $D = b^2 - 4fc$, Then $fx^2 + bxy + cy^2$ is a form that works. □

Exercise 1.5.1. *-4 is a square mod 5. Find a form $5x^2+bxy+cy^2$ for some $b, c \in \mathbb{Z}$ with discriminant -4, and then show explicitly that it is equivalent to $x^2 + y^2$.*

Now according to this calculation and the above theorem above, a prime p is represented by $x^2 + 3y^2$ iff -12 is a square mod $4p$. If p is odd, This is equivalent to -3 being a square mod p, $(\frac{-3}{p}) = (\frac{p}{3})$ by quadratic reciprocity so we see that this holds iff $p \equiv 1 \pmod 3$.

Exercise 1.5.2. *When is a prime of the form $x^2 + ny^2$ for $n = 1, 2, 3, 4, 7$? When is a prime of the form $x^2 + xy + ny^2$ for $n = 1, 2, 3, 5, 7, 11, 17, 41$*

Exercise 1.5.3. *Construct reduced quadratic forms that are not $x^2 + ny^2$ of discriminant $-4n$ to show that $h(-4n) > 1$ unless $n = 1, 2, 3, 4, 7$. How far does this technique work for discriminants $-4n + 1$?*

For $D = -20$, There are two reduced forms, $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$. -20 is a square mod $4p$ iff it is a square mod p iff $1 = (\frac{-20}{p}) = (\frac{-5}{p}) = (-1)^{\frac{p-1}{2}}(\frac{p}{5})$. This gives the condition $p \equiv 1, 3, 7, 9 \pmod{20}$. The relatively prime squares mod 20 are $1, 9 \pmod{20}$, so a of the form $x^2 + 5y^2$ must be $\equiv 1, 9 \bmod 20$. Similarly, note that $3(2x^2 + 2xy + 3y^2) = 5x^2 + (x + 3y)^2$, so a prime of the form $2x^2 + 2xy + 3y^2$ is $3, 7 \pmod{20}$. So if $(\frac{-20}{4p}) = 1$, then p is represented by some quadratic form of discriminant -20, but we can tell exactly which one it is by the congruence class of p! Thus we get the theorem:

Theorem 1.6. *p is of the form $x^2 + 5y^2$ iff $p \equiv 1, 9 \pmod{20}$, and of the form $2x^2 + 2xy + 3y^2$ iff $p \equiv 3, 7 \pmod{20}$.*

So as long as all the reduced forms represent different different congruence classes for which $(\frac{D}{4p}) = 1$, then we can find out when a prime is represented by a particular form of discriminant D.

We can divide the quadratic forms of a particular discriminant up based on which elements mod D they represent, and we call the set of quadratic forms representing a number a **genus**. So the techniques we have used show that if every genus contains only one quadratic form for a fixed discriminant, we can determine which primes are represented by any quadratic form of that discriminant.

Exercise 1.6.1. *When is p of the form $x^2 + ny^2$ for $n = 6, 10, 13, 15, 21, 22, 30$?*

When is $2p$ is of the form $x^2 + 5y^2$?

Exercise 1.6.2. *If $2p$ is of the form $x^2 + 5y^2$, then $p \equiv 3, 7 \pmod{20}$.*

Is the converse true? Well we know that p is of the form $2x^2 + 2xy + 3y^2$, and the same holds for 2, so we can appeal to the identity that holds for any quadratic form of discriminant $-4n$: $(ax^2 + 2bxy + cy^2)(az^2 + 2bzw + cw^2) = (axz + bxw + byz + cyw)^2 + n(xw - yz)^2$. Thus we get:

Theorem 1.7. *$2p$ is of the form $x^2 + 5y^2$ iff $p \equiv 3, 7 \pmod{20}$.*

This identity is quite amazing! It shows that the congruence classes represented by $x^2 + 5y^2$ are exactly the squares of those represented by $2x^2 + 2xy + 3y^2$. It turns out that given any two quadratic forms of equal discriminant, there is always an identity of the form above, where the forms are on the left hand side of the equation. Thus we can think of the form on the right hand side as a **composite** of the other two. Unfortunately, two forms may have many composites, but by being a little more careful, one can produce a well defined operation that actually turns the set $\mathrm{Cl}(D)$ into an abelian group (hence the name class *group*)! This was first shown in Gauss's *Disquisitiones Arithmeticae*, and is an amazing feat.

Finally I will remark that the quadratic forms $x^2 + 14y^2$ and $2x^2 + 7y^2$ represent the same numbers mod 56. And indeed, examples seem to show that about half of the primes in those congruence classes belong to each, and it is unclear which belong to which. Can we come up with a condition that tells us exactly which primes are represented by x^2+14y^2 and which ones are not? This, and the more general problem of determining when a prime is represented by a quadratic form can be solved using the more modern tools of class field theory.