Gauss' Theory of Binary Quadratic Forms

Aniruddha Nadiga

Last updated: October 27, 2019

0 Introduction

These are my notes for the lecture series called Gauss' Theory of Binary Quadratic Forms by Alex Bartel from the Fall of 2019. The abstract for the series is below:

A prime number can be written as a sum of two squares if and only if it is congruent to 1 modulo 4. This theorem was first conjectured by Fermat and proved by Euler. Ok, so let's do some variations on the theme: which primes can be written as a square plus twice a square? And how about a square plus 3 times a square? Fermat also conjectured answers to these two questions (which he of course, being Fermat, called theorems rather than conjectures), but the actual proofs were given by Lagrange over 100 years later. Then Gauss came along, and showed us that these simple minded elementary questions actually form a gateway to a beautiful algebraic theory, the theory of binary quadratic forms. It continues to be of great relevance today, not only by virtue of still presenting us with many embarrassingly basic but hard questions, but also e.g. in some of Manjul Bhargava's Fields Medal winning work. I will give an introduction to Gauss's theory. Eventually those who are interested will turn it into a study group on some of Bhargava's work, but initially there will be almost no prerequisites

1 Background

Theorem 1.0.1
Let p be a prime number. Then there exist integers x and y such that $x^2 + y^2 = p$ if and only if $p \equiv 1$ or $2 \pmod 4$

Example 1.0.2
$5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, but you can not do this with 3, 7 or 11.

The proof that is given is particularly short and also slick, but it is not the most illuminating.

Proof. First suppose that there exist x and y such that $x^2 + y^2 = p$. Since all squares are 0 or 1 mod 4, we know that $x^2 + y^2$ is congruent to 1 or 2 mod 4 (if both were zero mod 4 then their sum is divisible by 4 which makes p not prime).
Now suppose that $p = 4k + 1$ is a prime. Then et $S = \{(x, y, z) \mid x^2 + 4yz = p\}$. Now we will define two involutions on S. The first is $i_1 : S \to S$ by $(x, y, z) \mapsto (x, z, y)$. The second involution is $i_2 : S \to S$ defined be

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

In the cases that are not covered then the sum in $x^2 + 4yz$ can not be prime. It is easy to check that this is a involution. Now note that i_2 has a unique fixed point, $(1, 1, k)$. Since involutions pair up elements that are not fixed points, this tells us that there is an odd number of elements of S. This means that for i to be an involution there is an odd number of fixed points, specifically, there is at least one fixed point. Fixed points of i_1 are of the form (x, y, y), and in this case $x^2 + (2y)^2 = p$, which proves the theorem. □

From this idea we can deduce a more general assertion.

Theorem 1.0.3
Let $n = \prod_p p^{e_p}$ where the product is over distinct prims and $e_p \in \mathbb{Z}_{>0}$. Then there exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = n$ if and only if for all $p \equiv 3 \pmod 4$, e_p is even.

Proof. Left as a exercise. Hint for the "if" direction: $(x^2+y^2)(z^2+w^2) = (xz+yw)^2 + (xw+yz)^2$. This can be read as "products of numbers that are the sum of squares are the sum of squares". □

Theorem 1.0.4
Let p be an odd prime. Then there exists $x, y \in \mathbb{Z}$ such that
- $x^2 + 2y^2 = p$ if and only if $p \equiv 1$ or $3 \pmod 4$.
- $x^2 + 3y^2 = p$ if and only if $p \equiv 1 \pmod 3$
- $x^2 + 5y^2 = p$ if and only if $p \equiv 3$ xor $9 \pmod{20}$
- $x^2 + 5y^2 = 2p$ if and only if $p \equiv 3$ xor $7 \pmod{20}$

Results of this type get more and more difficult as the coefficients grow (the conditions get more complicated).

2 Binary Quadratic Froms

Definition 2.0.1
A *binary quadratic form* (over $\mathbb{Z}$) in x and y is a polynomial of the form $ax^2+bxy+cy^2$ where $a, b, c \in \mathbb{Z}$. We can abbreviate these polynomial to (a, b, c).
We say that (a, b, c) *represents* (properly) an integer n if there are some integer values x_0 and y_0 such that $ax_0^2 + bx_0y_0 + cy_0^2 = n$ (and the values are coprime).

Big Question: Given a BQF, what integers does it represent (properly)?

We have the following observations:

1. If $2x^2 + 7y^2$ represents n then so does $7x^2 + 2y^2$.
2. If $2x^2 + 7y^2$ represents n, then we can show that $2x^2 + 4xy + 9y^2$ does as well. To see this let $X = x + y$ and $Y = y$ then $2X^2 + 7Y^2 = 2x^2 + 4xy + 9y^2$. The inverse of this transformation is $X = x - y$ and $Y = y$. Thus if some values of x_0, y_0 make one of the equations equal to n, we can find some values that make the other equation equal to n.

In general we can consider linear changes of variable of the form $x = rX + sY$ and $y = tX + uY$. We want it to be the case that $x, y \in \mathbb{Z}$ when ever $X, Y \in \mathbb{Z}$. This will force $r, s, t, u \in \mathbb{Z}$. We also want the implication in the other direction. If we invert the transformations this will imply that $ru - st \in \{-1, 1\}$.

Both of these conditions together will result in $x, y \in \mathbb{Z} \iff X, Y \in \mathbb{Z}$.

Now note that we can write any binary quadratic form as

$$\begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix},$$

meaning that we can represent any binary quadratic form as a 2×2 integer valued matrix. Then we can have the linear changes in variables described above be written as

$$\begin{bmatrix} r & s \\ t & u \end{bmatrix}^T \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

Given the constrants on r, s, t, u from above, this will force the matrix to be in $\mathrm{GL}_2(\mathbb{Z})$. We can see that this is a right action on the set of binary quadratic forms (because C_1C_2 applied to a binary quadratic form is the same as applying C_1 first and then C_2).

For our purposes it will end up being more convenient to consider the restriction to matrices with determinant 1, so we consider the action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of binary quadratic forms.

Definition 2.0.2
Two binary quadratic forms (a, b, c) and (a', b', c') are said the be *equivalent*, denoted $(a, b, c) \equiv (a', b', c')$, if there is an element of $\mathrm{SL}_2(\mathbb{Z})$ that takes one to the other.

Proposition 2.0.3
If two forms are equivalent then they represent the same integers.

Proof. Let (a, b, c) be a binary quadratic form (represented by $\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$). Then let $C \in \mathrm{SL}_2(\mathbb{Z})$. If $(a, b, c) \cdot C$ (represented by $C^T \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} C$ represents n, we want to show that (a, b, c) represents n as well. Let x_0 and y_0 be integers that make $(a, b, c) \cdot C(x_0, y_0)$ equal n. Then the integers $\begin{bmatrix} x_0 & y_0 \end{bmatrix} C^T$ will make (a, b, c) be n as well. This follows from the matrix representations. □

Thus the integers that a form represents depends only on its orbit under the action of $\mathrm{SL}_2(\mathbb{Z})$, and we have simplified the original big question. This leads to the following:

Question: Given two binary quadratic forms how do we quickly tell if they are equivalent?

Definition 2.0.4
Thee *discriminant* of a binary quadratic form (a, b, c) is $b^2 - 4ac$. This can also be understood as -4 times the determinant of the matrix that represents (a, b, c).

Proposition 2.0.5
Two equivalent forms have the same discriminant.

Proof. This follows simply by considering the matrix characterization of the discriminant. □

However, it can still be the case that two forms with the same discriminant are not equivalent.

Example 2.0.6
Let $f_1 = 2x^2 + 3y^2$ and $f_2 = x^2 + 2xy + 7y^2$. They have the same disciminant. However, f_2 represents 1, since $f_2(1, 0) = 1$, but it us clearly impossible that f_1 represents 1.