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

Sounak Bagchi

Euler Circle

07/04/2024

Introduction

The Central Question

What odd primes p can be expressed in the form $x^2 + ny^2$ for positive integers n and integers x, y?

$n = 1$

We first consider the canonical example of $n = 1$ for $p = x^2 + y^2$ where x and y are integers and p is an odd prime.

Fermat's Two Squares Theorem

For an odd prime p, we have

$$p \equiv 1 \pmod 4 \iff p = x^2 + y^2 \quad (x, y \in \mathbb{Z}).$$

Note that the quadratic residues in modulo 4 are $0, 1$. Since p can be written as a sum of two squares, it follows that $p \equiv 0, 1, 2 \pmod 4$. Since p is an odd prime, we must have

$$p = x^2 + y^2 \implies p \equiv 1 \pmod 4. \qquad (1)$$

The converse is true as well, albeit much harder to prove. We'll show it in a two-step process.

Descent

If $p \mid a^2 + b^2$ for $\gcd(a, b) = 1$, then p can be written as a sum of two squares.

Reciprocity

If $p \equiv 1 \pmod 4$, then $p \mid a^2 + b^2$ with $\gcd(a, b) = 1$.

Combining these two steps, along with (1), gives the proof of Fermat's Two Squares Theorem. (The proofs are quite instructive, and can be found in my paper.)

Other Examples

Euler used a similar method to tackle the cases of $n = 2$ and $n = 3$. He found that

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

In particular, the Descent steps that he used were:

If $p \mid x^2 + 2y^2, \gcd(x, y) = 1$ then p is of the form $a^2 + 2b^2$ for $a, b \in \mathbb{Z}$
If $p \mid x^2 + 3y^2, \gcd(x, y) = 1$ then p is of the form $a^2 + 3b^2$ for $a, b \in \mathbb{Z}$

The Reciprocity steps that he used were:

If $p \equiv 1, 3 \pmod 8$, then $p \mid x^2 + 2y^2, \gcd(x, y) = 1$
If $p \equiv 1 \pmod 3$, then $p \mid x^2 + 3y^2, \gcd(x, y) = 1$

Are we done? No!

The natural question to ask is: does this easily generalize for all n? If it did, this presentation would be much shorter. Unfortunately, I'm not done yet, so we'll have to show that this doesn't generalize.

The problem that arises is that the Descent conjecture just isn't true for general n.

Generalized Descent Conjecture

If $p \mid x^2 + ny^2$ with $\gcd(x, y) = 1$, then p is of the form $a^2 + nb^2$ for $a, b \in \mathbb{Z}$.

Consider the case for $n = 5$:

$$\text{If } p \mid x^2 + 5y^2, \gcd(x, y) = 1 \text{ then } p \text{ is of the form } a^2 + 5b^2 \text{ for } a, b \in \mathbb{Z}$$

Taking $x = 1$ and $y = 2$, note that $3 \mid 1^2 + 5 \cdot 2^2 = 21$. However, 3 cannot be written in the form of $a^2 + 5b^2$ for integers a, b.

Generalizing

As it turns out, to fix this "Descent" step, we will need more advanced tools, namely Lagrange's Theorem on binary quadratic forms, which we'll cover later.

For now, let's focus on perfecting the Reciprocity Step. We essentially want a set of residues $a_1, a_2, \ldots$ so that the following statement holds:

$$p \equiv a_1, a_2, \ldots \pmod{n} \iff p \mid x^2 + ny^2, \gcd(x, y) = 1$$

This is rather easily generalizable. Define the standard **Legendre Symbol** $\left(\frac{a}{p}\right)$ to be

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a \text{ and a is a quadratic residue modulo p} \\ -1 & p \nmid a \text{ and a is a quadratic nonresidue modulo p} \end{cases}$$

General Reciprocity

For $n > 0$ and odd primes $p \nmid n$, we have

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

Proof: The forward direction is fairly elementary. Note that

$$x^2 + ny^2 \equiv 0 \pmod{\text{p}} \iff -n \equiv \frac{x^2}{y^2} \equiv \left(\frac{x}{y}\right)^2 \pmod{p}.$$

This is legal since $y \not\equiv 0 \pmod{\text{p}}$, as otherwise $x \equiv 0 \pmod{p}$ and $\gcd(x, y) \neq 1$. So, $-n$ is a square modulo p, hence the forward direction is proved.

For the backwards direction, write

$$-n \equiv a^2 \pmod{p}.$$

Thus, we must find a solution (x, y) in modulo p such that

$$x^2 - a^2y^2 \equiv 0 \pmod{p} \iff (x - ay)(x + ay) \equiv 0 \pmod{p},$$

where $x, y \not\equiv 0 \pmod{p}$. Then, it suffices to fix $x = 1$ and choose y to be the inverse of a modulo p, though many other solutions exist, of course.

Both directions have been proved, hence we're done. ■

Quadratic Forms

Lagrange first introduced the concept of Quadratic Forms in two variables

$$f(x, y) = ax^2 + bxy + cy^2, a, b, c \in \mathbb{Z}$$

Along with quadratic forms, Lagrange introduced discriminants, reduced forms, and equivalence.

As it turns out, Lagrange's Theory on reduced forms gives us a solution for the Descent Step looking for. Then, along with the Reciprocity Step, this will give the answer to our central question for some cases n.

For the sake of time, we won't introduce definitions relating to binary quadratic forms.

Equivalence

Two quadratic forms $f(x, y)$ and $g(x, y)$ are **equivalent** if there are integers p, q, r, s for which

$$f(x, y) = g(px + qy, rx + sy) \qquad ps - qr = \pm 1.$$

If $ps - qr = 1$, then f and g are properly equivalent, and if $ps - qr = -1$, then f and g are improperly equivalent.

There is a relationship between proper representation and proper equivalence, that we uncover in the next lemma.

Lemma 2

A form $f(x, y)$ properly represents an integer m if and only if $f(x, y) = ax^2 + bxy + cy^2$ is properly equivalent to a quadratic form $g(x, y) = mx^2 + b'xy + c'y^2$.

Lemma 3

Let $D \equiv 0, 1 \pmod 4$ be an integer and let m be an odd integer relatively prime to D. Then m is properly represented by a primitive form with discriminant D if and only if D is a quadratic residue modulo m.

Corollary 1

Let n be an integer and p be an odd prime that does not divide n. Then

$$\left(\frac{-n}{p}\right) = 1 \iff p \text{ is represented by a primitive form with discriminant -}4n.$$

Proof. This is a result of Lemma 2 along with basic properties of the Legendre Symbol, as $\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)$. Since p being represented by a primitive form with discriminant $-4n$ is equivalent to $\left(-\frac{4n}{p}\right) = 1$, the result follows. ■

Reduced Forms

We can do this using the next type of quadratic forms:

Reduced Quadratic Forms

A primitive positive definite form $f(x, y) = ax^2 + bxy + cy^2$ (i.e. $f(x, y) > 0$ for all $(x, y) \neq (0, 0)$) is said to be **reduced** if

$$|b| \leq a \leq c, \text{ and } b \geq 0 \text{ if either } |b| = a \text{ or } a = c.$$

Corollary 2

The quadratic form $f(x, y) = x^2 + ny^2$ is always reduced.

Proof: Check! ■

Theorem 1

Every primitive positive definite quadratic form is properly equivalent to a unique reduced one.

To demonstrate the use of this theorem, consider the primitive positive definite forms $f(x, y) = 3x^2 + 2xy + 5y^2$ and $g(x, y) = 3x^2 - 2xy + 5y^2$. These forms are obviously equivalent since $f(x, y) = g(x, -y)$, and moreover they are both reduced. So, Theorem 1 implies that these forms are not properly equivalent.

On the other hand, consider $f(x, y) = 2x^2 + 2xy + 3y^2$ and $g(x, y) = 2x^2 - 2xy + 3y^2$. Note that only $f(x, y) = 2x^2 + 2xy + 3y^2$ is reduced, since for both f and g, $a = |b|$. Hence, using Theorem 1, it follows that f and g are properly equivalent to each other.

Class Number

Class Number

Let $h(D)$, the **class number**, denote the number of equivalence classes of primitive positive definite forms with discriminant D, with the equivalence relation being proper equivalence among quadratic forms.

Corollary 3

$h(D)$ counts the number of reduced forms of discriminant D, and is finite.

Proof: This is true because of Theorem 1 - the finiteness part can be proved by bounding the coefficients of the quadratic form by some expression in D. ■

Class Number Table

Table 1: Reduced Forms for Certain Discriminants D.

D	$h(D)$	Reduced Forms of Discriminant D
-4	1	$x^2 + y^2$
-8	1	$x^2 + 2y^2$
-12	1	$x^2 + 3y^2$
-20	2	$x^2 + 5y^2, 2x^2 + 2xy + 3y^2$
-28	1	$x^2 + 7y^2$
-56	4	$x^2 + 14y^2, 2x^2 + 7y^2, 3x^2 \pm 2xy + 5y^2$
-108	3	$x^2 + 27y^2, 4x^2 \pm 2xy + 7y^2$
-256	4	$x^2 + 64y^2, 4x^2 + 4xy + 17y^2, 5x^2 \pm 2xy + 13y^2$

Class number

As can be seen in the table above, for the values $n = 1, 2, 3$, the quadratic forms $x^2 + y^2, x^2 + 2y^2, x^2 + 3y^2$ are the only reduced forms with discriminant $-4n$. Hence, by using quadratic reciprocity, we can immediately find when the values $(-1/p)$, $(-2/p)$, $(-3/p)$ are equal to 1, and from there we can determine what primes are represented as $x^2 + ny^2$.

However, this only works because $h(-4n) = 1$ for the values $n = 1, 2, 3, 7$, as the only reduced form is $x^2 + ny^2$ in these cases.

Theorem 2

If n is a positive integer, then

$$h(-4n) = 1 \iff n = 1, 2, 3, 4, \text{ or } 7$$

Corollary 1

Let n be an integer and p be an odd prime that does not divide n. Then

$$\left(\frac{-n}{p}\right) = 1 \iff p \text{ is represented by a primitive form with discriminant -4}n.$$

As an example, for $n = 5$, we have

$$p \equiv 1, 3, 7, 9 \pmod{20} \iff \left(\frac{-5}{p}\right) = 1 \iff p = x^2 + 5y^2 \text{ or } p = 2x^2 + 2xy + 3y^2.$$

We need to find another way to separate these two forms. This is precisely where genus theory comes into play. Consider our example with $n = 5$ as above. Note that

$$\begin{aligned} x^2 + 5y^2 \quad &\text{represents} \quad 1, 9 \quad \pmod{20} \\ 2x^2 + 2xy + 3y^2 \quad &\text{represents} \quad 3, 7 \quad \pmod{20} \end{aligned}$$

Genus

We say that two primitive positive definite forms, both with discriminant D, are part of the same **genus** if they represent the same values modulo D.

So, for example, in the above case for $D = -56$, $x^2 + 14y^2$ and $2x^2 + 7y^2$ would belong to the same genus, and in total there are two genera.

Now, consider the case $n = 5$ again. Using what we know about genera, we can conclude that

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

The top line, indeed, does give a full class of solutions for $n = 5$, as expected.

This is still not entirely sufficient since each genus can have more than one class of forms. In fact, it's not known how many such n exist where each genus has one class.

While we won't go over the proof of a final result, as it requires heavy machinery such as class field theory that takes time to establish, genus theory is one of the ways in which we can effectively deal with this problem. Once again, for more elaboration (and a final solution), take a look at my paper.

Special Conjectures

Euler made conjectures for the special cases $n = 27$ and $n = 64$, which were proved using cubic reciprocity and biquadratic reciprocity. For the sake of time we won't prove them here (a proof can be found in my paper), but they are below:

Euler's Conjecture for $n = 27$

Let p be a prime in $\mathbb{Z}$. Then $p = x^2 + 27y^2$ for $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 3$ and 2 is a cubic residue modulo p.

Euler's Conjecture for $n = 64$

- If $\pi = a + bi$ is a primary prime in $\mathbb{Z}[i]$, then

$$\left(\frac{2}{\pi}\right)_4 = i^{ab/2}.$$

- If p is prime, then $p = x^2 + 64y^2$ if and only if $p \equiv 1 \pmod 4$ and 2 is a biquadratic residue modulo p.

For all n

The Main Result

Let $n > 0$ be an integer. Then there is an irreducible monic polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that, if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \pmod{p} \\ \text{has an integer solution} \end{cases}$$

Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $L = K(\alpha)$ is the Hilbert Class Field of $K = \mathbb{Q}(\sqrt{-n})$. Finally, if $f_n(x)$ is any monic integer polynomial of degree $h(-4n)$ for which the above equivalence holds, then $f_n(x)$ is irreducible over $\mathbb{Z}$ and is the minimal polynomial of a primitive element of L.

Acknowledgements & Sources

I'd like to thank Dr. Simon Rubinstein-Salzedo and Emma Cardwell for their continual guidance in helping me study this topic. I'd also like to thank Justin Cheong and Siddharth Kothari for giving me suggestions on how to improve this presentation and the paper accompanying it.
Practically all of my research was done from David Cox's excellent book "Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication".