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

Isaac Chan-Osborn
(TA: Jacob Swenberg)

July 7, 2025

Introduction

Question (The Driving Question)

For a positive integer n, what primes p can be expressed as $x^2 + ny^2$ for some integer x and y?

Theorem

For a positive integer n and a prime p not dividing n, there is a polynomial $f_n(x)$ such that

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ and} \\ f_n(x) \equiv 0 \bmod p \text{ has a solution in the integers.} \end{cases}$$

This is a very powerful theorem, and proving it brings insight into many different places. The nature of $f_n(x)$ is mysterious and comes from class field theory.

History

A well known theorem of Fermat states that

Theorem (Fermat's Sum of Two Squares Theorem)

Let p be an odd prime. Then $p = x^2 + y^2$ for some integers x and y if and only if $p \equiv 1 \bmod 4$.

This is the case when $n = 1$. Much less common are the two theorems for $n = 2, 3$.

Theorem (Fermat)

Let p be an odd prime that isn't 3. Then,

$$p = x^2 + 2y^2 \iff p \equiv 1, 3 \bmod 8$$
$$p = x^2 + 3y^2 \iff p \equiv 1 \bmod 3.$$

Sum of Squares

We look at the proof of

Theorem (Fermat's Sum of Two Squares Theorem)

Let p be an odd prime. Then $p = x^2 + y^2$ for some integers x and y if and only if $p \equiv 1 \bmod 4$.

The first published proof of this theorem was by Euler and proceeds with two steps, the descent step and the reciprocity step.

- Descent: If $p | x^2 + y^2, \gcd(x, y) = 1$ then $p = x^2 + y^2$ for some x, y.
- Reciprocity: If $p \equiv 1 \bmod 4$ then $p | x^2 + y^2, \gcd(x, y) = 1$.

Descent Step

Lemma (Descent)

If $p | x^2 + y^2, \gcd(x, y) = 1$ *then* $p = x^2 + y^2$ *for some* x, y.

Proof.

The crucial fact is the following:

Proposition

If M *is the sum of two relatively prime squares, and a prime divisor* q *of* M *is the sum of two relatively prime squares, then so is* M/q.

Then, we can use descent by the smallest prime divisor of M. ■

Reciprocity Step

Lemma

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

Proof.

Let $p = 4k + 1$, so the polynomial

$$(x^{2k} - 1)(x^{2k} + 1) \equiv x^{4k} - 1 \equiv 0 \bmod p$$

whenever $x \not\equiv 0 \bmod p$. Then, the left factor has at most $2k < 4k$ roots, so there is some x such that $(x^k)^2 + 1 \equiv 0 \bmod p$, as desired. ∎

Generalizing Descent

The previous method seems quite promising. In fact, the descent steps for $n = 2, 3$ are

- If $p | x^2 + 2y^2$ for relatively prime x, y then $p = x^2 + 2y^2$ for some x, y
- If $p | x^2 + 3y^2$ for relatively prime x, y then $p = x^2 + 3y^2$ for some x, y.

This inspires us to conjecture the following:

Conjecture (Generalized Descent)

If p is a prime not dividing n then $p | x^2 + ny^2 \implies p = x^2 + ny^2$.

Generalizing Descent

The previous method seems quite promising. In fact, the descent steps for $n = 2, 3$ are

- If $p | x^2 + 2y^2$ for relatively prime x, y then $p = x^2 + 2y^2$ for some x, y
- If $p | x^2 + 3y^2$ for relatively prime x, y then $p = x^2 + 3y^2$ for some x, y.

This inspires us to conjecture the following:

Conjecture (Generalized Descent)

If p is a prime not dividing n then $p | x^2 + ny^2 \implies p = x^2 + ny^2$.

Sadly, this is false. When $n = 5$ we have that $7 | 1^2 + 5 \cdot 2^2 = 21$ but 7 is not represented as $x^2 + 5y^2$.

Generalizing Reciprocity

Turning to reciprocity, we are prompted to ask where $p \equiv 1 \bmod 4, p \equiv 1, 3 \bmod 8$, and $p \equiv 1 \bmod 3$ come from. To do this, we use quadratic reciprocity. We have that

Lemma

For a positive integer n and a prime p not dividing n, it holds that

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

using the Legendre symbol. The proof is simple: $x^2 + ny^2 \equiv 0 \bmod p \implies x^2 \equiv -ny^2 \bmod p$, from which it is clear that $-n$ is a quadratic residue, and that is sufficient.

Quadratic Forms

We can generalize using Lagrange's notion of quadratic forms, which include $x^2 + ny^2$.

Definition

A *quadratic form* $f(x, y)$ is a polynomial of the form $ax^2 + bxy + cy^2$ for some integers a, b, c. It represents a number m if $ax^2 + bxy + cy^2 = m$ has an integer solution, and properly represents m if $\gcd(x, y) = 1$.

Definition

The *discriminant* of a quadratic form is $D = b^2 - 4ac$.

Definite and Indefinite Forms

Note that

$$4af(x, y) = (2ax + by)^2 - Dy^2.$$

Thus, we call a form indefinite if $D > 0$ and positive or negative definite if $D \leq 0$ and a is positive or negative, respectively.

Equivalence and Proper Equivalence

Two forms $f(x, y)$ and $g(x, y)$ are equivalent if

$$f(x, y) = g(px + qy, rx + sy)$$

where $ps - qr = \pm 1$. When $ps - qr = 1$, we say they are properly equivalent. Otherwise, they are improperly equivalent. Equivalence preserves determinant and represented values.

Definition

A form $f(x, y)$ is reduced if $|b| \leq a \leq c$ and $b > 0$ if $|b| = a$ or $a = c$.

Theorem

There are finitely many proper equivalence classes of positive definite forms of discriminant D. Moreover, no two reduced forms are properly equivalent. This number is class number of D, or $h(D)$.

Note that $x^2 + ny^2$ is always reduced.

Class Numbers

Theorem

When m is an odd number relatively prime to $D \equiv 0, 1 \bmod 4$. Then m is properly represented by a form of discriminant D if and only if D is a quadratic residue $\bmod\ m$.

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

When $h(-4n) = 1$, we are done from reciprocity and the previous theorem.

Class Number 1

Unfortunately, we find the result

Theorem

If $h(-4n) = 1$ *then* $n = 1, 2, 3, 7$.

Separating these reduced forms further when $h(-4n) > 1$ uses genus theory, which is capable of fully solving 65 values of n. We will now look at Euler's conjectures for $n = 27$ and $n = 64$.

Eisenstein Integers

The set of Eisenstein integers is the ring $\mathbb{Z}[\omega]$ where $\omega = e^{2i\pi/3} = \dfrac{-1 + i\sqrt{3}}{2}$. We can define the norm of $\alpha = a + b\omega$ as

$$N(\alpha) = a^2 - ab + b^2 = (a + b\omega)(a + b\omega^2).$$

This allows us to study cubic reciprocity and $n = 27$. The invertible Eisenstein integers are $\pm 1, \pm\omega$, and $\pm\omega^2 = \pm(-1 - \omega)$, and these are called units. Two Eisenstein integers are associates if their ratio is a unit. An Eisenstein prime is an irreducible element.

Cubic Reciprocity

We can define the Cubic Legendre symbol the same way we define the regular one:

$$\left(\frac{\alpha}{\pi}\right)_3 = \alpha^{(N(\pi)-1)/3} \in \{1, \omega, \omega^2\}.$$

Theorem (Law of Cubic Reciprocity)

For Eisenstein primes π *and* θ *that are congruent to* $\pm 1 \bmod 3$ *and have unequal norm, then*

$$\left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3.$$

Solving $n = 27$

Using cubic reciprocity one can find that

Theorem

When p is a prime then $p = x^2 + 27y^2$ if and only if $p \equiv 1 \bmod 3$ and 2 is a cubic residue mod p.

For details on the proof, see my paper!

Gaussian Integers

The Gaussian integers is the ring $\mathbb{Z}[i]$ where $i^2 = -1$. The norm function for $z = a + bi$ is

$$N(z) = a^2 + b^2 = (a + bi)(a - bi).$$

Similarly the invertible Gaussian integers are $\pm 1, \pm i$. The primes in $\mathbb{Z}[i]$ are the irreducible elements.

Biquadratic/Quartic Reciprocity

Define the biquadratic Legendre symbol as

$$\left(\frac{\alpha}{\pi}\right)_4 = \alpha^{(N(\pi)-1)/4} \in \{\pm 1, \pm i\}.$$

Then, the Law of Biquadratic Reciprocity states that

Theorem (Law of Biquadratic Reciprocity)

If π and θ are distinct primes congruent to $1 \bmod 2+2i$ then

$$\left(\frac{\theta}{\pi}\right)_4 = \left(\frac{\pi}{\theta}\right)_4 (-1)^{(N(\pi)-1)(N(\theta)-1)/16}.$$

Solving $n = 64$

Using Biquadratic Reciprocity and its supplements, one can show that

Theorem

Let p be a prime. Then, p can be expressed as $x^2 + 64y^2$ if and only if $p \equiv 1 \bmod 4$ and 2 is a biquadratic residue $\bmod\ p$.

Conclusion

We go back to our result

Theorem

For a positive integer n and a prime p not dividing n, there is a polynomial $f_n(x)$ such that

$$p = x^2 + ny^2 \iff \begin{cases} \left(\frac{-n}{p}\right) = 1 \text{ and} \\ f_n(x) \equiv 0 \bmod p \text{ has a solution in the integers.} \end{cases}$$

Through quadratic reciprocity, quadratic forms and some special rings, we have solved the cases where $n = 1, 2, 3, 27, 64$ and genus theory allows us to solve 62 more. Note that $n = 27, 64$ give insight on $f_n(x)$, as $f_{27}(x) = x^3 - 2$ and $f_{64}(x) = x^4 - 2$. The methods used to obtain this result have applications to Class Field Theory, Elliptic Curves, and more.