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

Advaith Mopuri

July 2023

Table of Contents

A Classic Theorem of Fermat

It is well known that for $x, y \in \mathbb{Z}$ and an odd prime p,

$$p = x^2 + y^2 \iff p \equiv 1 \bmod 4. \tag{1}$$

[1] Here we are only considering odd primes p, as they make up the actually interesting parts of this problem

A Classic Theorem of Fermat

It is well known that for $x, y \in \mathbb{Z}$ and an odd prime p,

$$p = x^2 + y^2 \iff p \equiv 1 \bmod 4. \tag{1}$$

This begs the question – is there a similar way that we can classify which primes[1] can be expressed in the form $x^2 + ny^2$?

[1] Here we are only considering odd primes p, as they make up the actually interesting parts of this problem

Brief History

Mathematicians like Fermat, Euler, Legendre, Lagrange, and Gauss all contributed to the creation of such a classification, and developed techniques such as quadratic forms, reciprocity, and genus theory in the process.

Proving Fermat's Theorem

Recall equation 1

$$p = x^2 + y^2 \iff p \equiv 1 \bmod 4.$$

Proving Fermat's Theorem

Recall equation 1

$$p = x^2 + y^2 \iff p \equiv 1 \bmod 4.$$

In order to prove this theorem, Euler used an approached based off of two steps, descent and reciprocity.

Descent and Reciprocity

Descent and Reciprocity

Descent:

$$\text{If } p | x^2 + y^2, \gcd(x, y) = 1, \text{ then } p \text{ can be written as } x^2 + y^2$$

$$\text{for some possibly different } x, y.$$

Descent and Reciprocity

Descent and Reciprocity

Descent:

$$\text{If } p | x^2 + y^2, \gcd(x, y) = 1, \text{ then } p \text{ can be written as } x^2 + y^2$$

$$\text{for some possibly different } x, y.$$

Reciprocity:

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

Note: $p = x^2 + y^2 \implies p \equiv 0, 1, 2 \bmod 4$ since $x^2 \equiv 0, 1 \bmod 4$. But, for odd primes p the first and third options are clearly impossible.

Why Reciprocity?

As Euler continued using the descent and reciprocity steps for different values of n, he found that the reciprocity step became increasingly difficult to prove.

Why Reciprocity?

As Euler continued using the descent and reciprocity steps for different values of n, he found that the reciprocity step became increasingly difficult to prove.

Three main types of reciprocity are:

1. Quadratic Reciprocity
2. Cubic Reciprocity ($\mathbb{Z}[\omega]$)
3. Biquadratic Reciprocity ($\mathbb{Z}[i]$).

Quadratic Reciprocity

Define

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

Quadratic Reciprocity

Define

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

We then have

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

Cubic Reciprocity

Define

$$\alpha^{\frac{N(\pi)-1}{3}} = \left(\frac{a}{\pi}\right)_3 \bmod \pi$$

for a prime π not dividing 3, and norm $N(\pi) = \pi\bar{\pi}$.

This can take on the values $1, \omega$, and ω^2.

Cubic Reciprocity

Define

$$\alpha^{\frac{N(\pi)-1}{3}} = \left(\frac{a}{\pi}\right)_3 \bmod \pi$$

for a prime π not dividing 3, and norm $N(\pi) = \pi\bar{\pi}$.

This can take on the values $1, \omega$, and ω^2. Similar to before, we have

$$\left(\frac{a}{\pi}\right)_3 = 1 \iff x^3 \equiv \alpha \bmod \pi \text{ has a solution.}$$

Cubic Reciprocity

This definition of cubic reciprocity can be used to prove the following:

$$x^3 \equiv a \bmod p \text{ is solvable in } \mathbb{Z} \iff \left(\frac{a}{\pi}\right) = 1, p = \pi\bar{\pi}$$

$$p = x^2 + 27y^2 \iff p \equiv 1 \bmod 3, 2 \text{ is a cubic residue modulo } p$$

Ramification, Inertial Degree, and Splitting

The *ramification index* of a prime in a field L is a property defined by the exponent of that prime in the product of the factorization of the ring of integers of L with a prime ideal $\mathfrak{p}$.

Ramification, Inertial Degree, and Splitting

The *ramification index* of a prime in a field L is a property defined by the exponent of that prime in the product of the factorization of the ring of integers of L with a prime ideal $\mathfrak{p}$. The *inertial degree* of $\mathfrak{p}$ is the degree of the residue field extension of the ring of integers of L over said prime.

Ramification, Inertial Degree, and Splitting

The *ramification index* of a prime in a field L is a property defined by the exponent of that prime in the product of the factorization of the ring of integers of L with a prime ideal $\mathfrak{p}$. The *inertial degree* of $\mathfrak{p}$ is the degree of the residue field extension of the ring of integers of L over said prime.

If the ramification index and the inertial degree of a prime are both equal to 1, then we say that the prime *splits completely* in L.

Ramification, Inertial Degree, and Splitting

The *ramification index* of a prime in a field L is a property defined by the exponent of that prime in the product of the factorization of the ring of integers of L with a prime ideal $\mathfrak{p}$. The *inertial degree* of $\mathfrak{p}$ is the degree of the residue field extension of the ring of integers of L over said prime.

If the ramification index and the inertial degree of a prime are both equal to 1, then we say that the prime *splits completely* in L.

In fact, in the case of a Galois extension, the inertial degree and ramification indices of all primes in the factorization are equal, so we say that $\mathfrak{p}$ splits completely in L.

The Hilbert Class Field

Using some group theory and the Hilbert class field, it turns out that we can derive the following theorem:

$$p = x^2 + ny^2 \iff p \text{ splits completely in } L.$$