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

Yucong Chen

University of California, Los Angeles

April 6, 2023

Basic Question

Given a positive integer n, which primes p can be expressed in the form $p = x^2 + ny^2$, where $x, y \in \mathbb{Z}$?

Motivating Examples

Three theorems of Fermat for odd primes p, where $x, y \in \mathbb{Z}$:

$p = x^2 + y^2 \Leftrightarrow p \equiv 1 \pmod 4$

$p = x^2 + 2y^2 \Leftrightarrow p \equiv 1, 3 \pmod 8$

$p = x^2 + 3y^2 \Leftrightarrow p = 3$ or $p \equiv 1 \pmod 3$

Main Theorem

Let $n > 0$ be an integer. Then there is a monic irreducible 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

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

Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer a for which $L = K(\alpha)$ is the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-n})$.

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 the ring class field L described above.

Quadratic Reciprocity

Definition (Legendre symbol)

$$(a/p) = \begin{cases} 0 \text{ if } p|a \\ 1 \text{ if } p \not| a \text{ and } a \text{ is a quadratic residue modulo } p \\ -1 \text{ if } p \not| a \text{ and } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Lemma

Let n be a nonzero integer, and let p be an odd prime not dividing n. Then $p|x^2 + ny^2$, $gcd(x, y) = 1 \Leftrightarrow (-n/p) = 1$.

Related Definitions

Number field K is a finite extension of $\mathbb{Q}$ in $\mathbb{C}$.
Ring of integers O_K is the algebraic integers of K, i.e., the set of all $\alpha \in K$ which are roots of a monic integer polynomial.
A **prime ideal** is a subset of a ring that shares many important properties of a prime number in the ring of integers.
A **Galois extension** is an algebraic field extension E/F that is normal and separable, and an **abelian extension** is a Galois extension whose Galois group is abelian.
For a field extension L/K, consider the ring of integer O_L that has a factorization into prime ideals $p \cdot O_L = p_1^{e_1} ... p_k^{e_k}$ where the p_i are distinct prime ideals of O_L. Then p is said to **ramify** in L if $e_i > 1$ for some i; otherwise it is **unramified**.

Hilbert Class Field

Definition

The **Hilbert class field** of a number field K is the maximal unramified abelian extension of K.

Theorem

Let L be the Hilbert class field of a number field K, and let p be a prime ideal of K. Then p splits completely in $L \Leftrightarrow p$ is a principal ideal. Moreover, p splits completely in $L \Leftrightarrow f_n(x) \equiv 0 \pmod{p}$ is solvable in O_K $\Leftrightarrow f_n(x) \equiv 0 \pmod{p}$ is solvable in $\mathbb{Z}$.

Definitions

A **modulus m** is a product of primes and distinct real embeddings.
A **congruence subgroup** for m is a subgroup of the fractional ideals $I_K(m)$ coprime to m, containing the principal ideals $P_{K,1}(K)$.
The **Artin map** of a Galois extension L/K, sending a prime ideal p to its Frobenius element in $Gal(L/K)$, defines a homomorphism:
$(\frac{L/K}{\cdot}) : I_K(m) \to Gal(L/K)$. ($m$ is a prime divisor.)

Theorem (Existence)

For a modulus m of K and a congruence subgroup H, there is a unique abelian extension of K such that H is the kernel of the Artin map.

Ring Class Field

By the Existence Theorem, there is a unique abelian extension L of K, which is called the **ring class field**.

Theorem

Let $n \in \mathbb{Z}_{>0}$ and L be the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in the field $K = \mathbb{Q}(\sqrt{-n})$. Then L is Galois over $\mathbb{Q}$, and if p is an odd prime not dividing n, then $p = x^2 + ny^2 \Leftrightarrow p$ splits completely in L.

Remark

The ring of integers of a number field is given by $O_K = \mathbb{Z}[\sqrt{-n}]$, which happens whenver n is squarefree and $n \not\equiv 3 \bmod 4$, the conductor equals 1. So, $I_K(1) = I_K$ and $P_{K,\mathbb{Z}}(1) = P_{K,1}(1) = P_K$, and the ring class field is equal to the Hilbert class field.

Rest of Proof for Main Theorem

There exists a real algebraic integer α such that $L = K(\alpha)$. Since L is Galois over $\mathbb{Q}$, $[L \cap \mathbb{R} : \mathbb{Q}] = [L : K]$. For $\alpha \in L \cap \mathbb{R}$, $L \cap \mathbb{R} = \mathbb{Q}(\alpha) \Leftrightarrow L = K(\alpha)$. So α is a real integral primitive element of L over K. Then its monic minimal polynomial $f_n(x)$ over $\mathbb{Q}$ is also the minimal polynomial of α over K.
Therefore, we can describe the field L by finding a monic integer polynomial $f_n(x)$, which will be the minimal polynomial of a primitive element of the extension $K = \mathbb{Q}(\sqrt{-n}) \subset L$. Any polynomial of the given form satisfying the equivalence is the minimal polynomial of some primitive element of this extension.

Example 1

For odd prime $p \neq 7$,

$$p = x^2 + 14y^2 \Leftrightarrow \begin{cases} (-14/p) = 1 \\ \text{and } (x^2+1)^2 \equiv 8 \pmod{\text{p}} \text{ has an integer solution.} \end{cases}$$

Proof: $\alpha = \sqrt{2\sqrt{2}-1}$ is a real integer primitive element of Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$. Its minimal polynomial can be chosen to be $f_{14}(x)$. The discriminant is $-2^{14} \cdot 7$, so we need to exclude primes 2 and 7.

Example 2

For prime $p > 3$,

$$p = x^2 + 27y^2 \Leftrightarrow \begin{cases} (-27/p) = 1 \\ \text{and } x^3 \equiv 2 \pmod{p} \text{ has an integer solution.} \end{cases}$$

Proof: The ring class field of $\mathbb{Z}[\sqrt{-27}]$ is $L = K(\sqrt[3]{2})$, where $K = \mathbb{Q}(\sqrt{-3})$. Since $\sqrt[3]{2}$ is a real algebraic integer, $f_{27}(x)$ can be $x^3 - 2$. The discriminant of $x^3 - 2$ is $-2^3 \cdot 3^3$, so $p > 3$.

References

Daniel Marcus's *Number Fields*
David Cox's *Primes of the form* $x^2 + ny^2$