10.48047/jocaaa.2024.32.01.71

Primes of the form $x^2 + ny^2$ and Class Fields

Dr. Siddaramu R

Government First Gade College, Holenarasipur. Hassan (dist) 573211.

Abstract:

We give a complete Characterization of the Quadratic Reciprocity Law and sums of squares. A primes number p can be written as a sum of two squares of integers if and only if $p = 2\ or\ p \equiv 1(mod\ 4)$. The Law of Quadratic Reciprocity established by Gauss.

Introduction: It is a well-known theorem of Fermat, that a prime number p can be written as a sum of two squares of integers if and only if $p = 2\ or\ p \equiv 1(mod\ 4)$.Fermat also stated that for an odd prime p,$p = x^2 + 2y^2$ if and only if $p \equiv 1,3(mod\ 8)$ and $p = x^2 + 3y^2$ if and only if $p = 3\ of\ p \equiv 1(mod\ 3)$. Euler gave a complete proof of these statements and made similar conjectures on $p = x^2 + ny^2$, for various special values of n. Some of these conjectures were proved by later mathematicians like Gauss, ete., Historically, the solution to this problem became more and more complete as Algebraic Number Theory developed. It is interesting to note that as in the case of the famous 'Fermat's Last Theorem, it joins hand with deeper theorems of modern Algebraic Number Theory. In fact, one can provide a very satisfactory answer for general n, in terms of Class Fields of orders in imaginary quadratic elds. There are also explicit methods for computing such Class Fields.

Theorem 1: Let p be an odd prime. Then, $p = x^2 + y^2$ for some integers x, y if and only if $p \equiv 1(mod\ 4)$.

Proof: The only if part is trivial, looking at congruence classes (mod 4). Let us sketch a proof of the converse. This can be done in two steps:

1. The Reciprocity step: If $p \equiv 1(mod\ 4)$, then $p|(x^2 + y^2)$ for some integers x, y with $(x, y) = 1$.
2. The Descent Step: If $p|(x^2 + y^2)$, for some integers x, y with $(x, y) = 1$, then $p = x^2 + y^2$ for some $x, y \in Z$.

Let us begin by proving Step 1. For a prime p, the congruence classes modulo p, viz., Z/pZ form a field and the nonzero elements of Z/pZ form a cyclic group of order $p - 1 = 4k$. Therefore, there exist an element x of order $4k$ in $Z/pZ - \{0\}$. Let $y = x^k$. Then $y^4 = 1$ and$y^2 = -1$. Thus-1 is a square in Z/pZ. This is the same as saying that there exist $x, y \in Z$ such that$x^2 + y^2 \equiv 0(mod\ p)$ i.e.$p|(x^2 + y^2)$. Thus Step 1. Follows.

For proving Step 2, we need the following lemma.

Lemma 2: Suppose that N is a sum of two squares, which are relatively prime, and $q = x^2 + y^2$ is a prime divisor of N. Then N/q is also a sum of two squares, which are relatively prime.

Proof: The proof is essentially based on the fact that the product of sums of two squares is a sum of two squares:

10.48047/jocaaa.2024.32.01.71

$(x^2 + y^2)(z^2 + w^2) = (xz \pm yz)^2 + (xw \mp yz)^2 \ldots\ldots\ldots\ldots\ldots\ldots (1)$

Let $N = a^2 + b^2$ with $(a, b) = 1$. Since $q|N$, we have $q|(x^2N - a^2q)$.

But,$x^2N - a^2q = x^2(a^2 + b^2) - a^2(x^2 + y^2) = x^2b^2 - a^2y^2 = (xb - ay)(xb + ay)$. Since q is a prime, $q|(xb - ay)$ *or* $q|(xb + ay)$. By changing the sigh of a if necessary, we may assume that $q|(xb - ay)$. Thus $xb - ay = qd$ for some integer d.Now,

$$xb - ay = dq = d(x^2 + y^2) = dx^2 + dy^2 \Rightarrow xb - dx^2 = ay + dy^2 = (a + dy)y.$$

This implies that $x|(a + dy)y$. Since $(x, y) = 1$, we get $x|(a + dy)$. Thus $a + dy = cx$ i.e., $a = cx - dy$ for some integer c. Again, from the same equation $(a + dy)y = x(b - dx)$, we also get, $b = dx + cy$. Now using (1) we get

$$N = a^2 + b^2 = (cx - dy)^2 + (dx + cy)^2 = (x^2 + y^2)(c^2 + d^2) = q(c^2 + d^2).$$

Therefore $N/q = c^2 + d^2$. Clearly $(c, d) = 1$. This completes the proof of the lemma.

Now, to complete the proof of the Descent Step, let p be an odd prime such that $p|N = a^2 + b^2$, where a, b are relatively prime. By replacing a by $a + rp$ and b by $b + sp$ for suitable integers r and s, we may assume that $N = a^2 + b^2$ with$|a| < p/2$ and $|b| < p/2$, so that $N = a^2 + b^2 < p^2/2$. By dividing out by the common factors, we may further assume that, these new a, b are also relatively prime. As$p|N$ and $N < p^2/2$, all prime divisors $q \neq p$ of N are less than p. If q is a sum of two squares, then by the lemma N/q is also s sum of two squares, which are relatively prime. If all the prime divisors $q \neq p$ of N are sums of two squares, then by repeatedly applying the lemma, we get that p itself is a sum of two squares.Therefore, if p is not a sum of two squares, then there exists a prime $q_1 < p, q_1|N = a^2 + b^2$ such that q_1 is not a sum of two squares. Repeating the process, we produce an infinite sequence of primes $> q_1 > q_2 \cdots$, which is absurd. Therefore p is itself a sum of two squares. This completes the proof of the Descent Step and hence also the theorem.

Let us now consider Euler's proof of Fermat's generalizations. For an odd prime p,

$p = x^2 + 2y^2$, for some $x, y \in Z \Longleftrightarrow p \equiv 1,3(mod\ 8)\ldots\ldots\ldots (2)$

And

$p = x^2 + 3y^2, for\ some\ x, y \in Z \Longleftrightarrow p = 3\ or\ p \equiv 1(mod\ 3)\ldots\ldots (3)$ Euler gave a complete proof of these statements, using the same two-step strategy. The Descent Step works just as in the previous case. However, the Reciprocity Step required a theorem, viz., the Quadratic Reciprocity Law, which was not established at the time of Euler. In fact, as remarked by D. Cox (cf. [COX]p.13-14), Euler discovered the Quadratic Reciprocity Law, while trying to prove these conjectures. Let usfirst recall the Legendre symbol:

Let us first recall the Legendre symbol: If p is an odd prime and a is any integer, then the Legendre symbol $(\frac{a}{p})$ is defined as follows:

10.48047/jocaaa.2024.32.01.71

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \quad if\ p|a, \\ 1 \quad if\ p \nmid a\ and\ a\ is\ a\ quadratic\ residue\ (mod\ p). \\ -1\ if\ p \nmid a\ and\ a\ is\ a\ quadratic\ non\ residue\ (mod\ p). \end{cases}$$

So, in terms of the Legendre symbol, we may now formulate the Reciprocity Step as follows: $p|(x^2 + y^2)$ for some $x, y \in Z$ with $(x, y) = 1 \Leftrightarrow \left(\frac{-2}{p}\right) = 1$ for equation (2) and $p|(x^2 + 3y^2)$ for some $x, y \in ZZ$ with $(x, y) = 1 \Leftrightarrow \left(\frac{-3}{p}\right) = 1$ for equation (3). The equation is how to describe all those for which $\left(\frac{-2}{p}\right) = 1$ and $\left(\frac{-3}{p}\right) = 1$ in terms of congruence classes of p modulo a fixed integer. This is exactly what prompted Euler to come up with the Law of Quadratic Reciprocity which was later established by Gauss.

References:

1. David Cox, Primes of the form $x^2 + ny^2$; Fermat, Class Field Theory and Complex Multiplication, John Wiley & Sons, New York Singapore, 1989.
2. Parvati Shastri, Integral points on the circle $x^2 + y^2 = c$, to appear in the Proceedings of the International Conf. on Alg. Number Theory Harish-Chandra Res. Institute, Allahabad, Nov. 2000.
3. Dipendra Prasad, Elliptic Curves with Complex Multiplication, Introduction to Class field Theory, Lecture Notes of the Instructional School in Algebraic Number Theory held at the Department of Mathematics, University of Mumbai, 1995.
4. Eknath Ghate, Complex Multiplication, Proceedings of the Workshop on Advanced Algebraic Number Theory, Harish-Chandra. Research Institute, Allahabad, 2000.