Primes of the Form $x^2 + ny^2$ and Quadratic Forms

Atharva Gawde
Mentor: Simran Khunger

University of Michigan

November 28, 2023

Fermat's Theorems

Theorem (Fermat)

For an odd prime p and $x, y \in \mathbb{Z}$,
$p = x^2 + y^2 \iff p \equiv 1 \pmod 4$

Fermat's Theorems

Theorem (Fermat)

For an odd prime p and $x, y \in \mathbb{Z}$,

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

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

$p = x^2 + 3y^2 \iff p = 3 \text{ or } p \equiv 1 \pmod 3$

Euler's Approach: Infinite Descent

Lemma

Suppose that N is a sum of two relatively prime squares, and that $q = x^2 + y^2$ is a prime divisor of N. Then $\frac{N}{q}$ is also a sum of relatively prime squares.

Euler's Approach: Infinite Descent

Lemma

Suppose that N is a sum of two relatively prime squares, and that $q = x^2 + y^2$ is a prime divisor of N. Then $\frac{N}{q}$ is also a sum of relatively prime squares.

Idea of Infinite Descent:

Descent Step

If $p \mid x^2 + y^2$, $\gcd(x, y) = 1$, then p can be written as $x^2 + y^2$ for some possibly different x, y.

Euler's Approach: Infinite Descent

Lemma

Suppose that N is a sum of two relatively prime squares, and that $q = x^2 + y^2$ is a prime divisor of N. Then $\frac{N}{q}$ is also a sum of relatively prime squares.

Idea of Infinite Descent:

Descent Step

If $p \mid x^2 + y^2$, $\gcd(x, y) = 1$, then p can be written as $x^2 + y^2$ for some possibly different x, y.

Reciprocity Step

If $p \equiv 1 \pmod 4$, then $p \mid x^2 + y^2$, $\gcd(x, y) = 1$

Euler's Approach: Infinite Descent

Lemma

Suppose that N is a sum of two relatively prime squares, and that $q = x^2 + y^2$ is a prime divisor of N. Then $\frac{N}{q}$ is also a sum of relatively prime squares.

Idea of Infinite Descent:

Descent Step

If $p \mid x^2 + y^2$, $\gcd(x, y) = 1$, then p can be written as $x^2 + y^2$ for some possibly different x, y.

Reciprocity Step

If $p \equiv 1 \pmod 4$, then $p \mid x^2 + y^2$, $\gcd(x, y) = 1$

Euler solved this for $n = 2, 3$ as well, but where do these congruences come from?

Quadratic Reciprocity and Legendre Symbols

Definition (Legendre Symbol)

For an odd prime p and an integer a not divisible by p,

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

Quadratic Reciprocity and Legendre Symbols

Definition (Legendre Symbol)

For an odd prime p and an integer a not divisible by p,

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

Lemma

Let n be a nonzero integer, and let p be an odd prime not dividing n. Then $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$ if and only if $\left(\frac{-n}{p}\right) = 1$

Connection to $p = x^2 + ny^2$

Quadratic Reciprocity and Legendre Symbols

Definition (Legendre Symbol)

For an odd prime p and an integer a not divisible by p,

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

Lemma

Let n be a nonzero integer, and let p be an odd prime not dividing n. Then $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$ if and only if $\left(\frac{-n}{p}\right) = 1$

Connection to $p = x^2 + ny^2$

About Quadratic Reciprocity

Rephrasing the Reciprocity Step

Reciprocity Step

If $p \equiv 1 \pmod 4$, then $p \mid x^2 + y^2$, $\gcd(x, y) = 1$

Lemma

Let n be a nonzero integer, and let p be an odd prime not dividing n. Then $p \mid x^2 + ny^2$, $\gcd(x, y) = 1$ if and only if $\left(\frac{-n}{p}\right) = 1$

$$\left(\frac{-3}{p}\right) = 1 \iff p = 1, 7 \pmod{12}$$
$$\left(\frac{-5}{p}\right) = 1 \iff p = 1, 3, 7, 9 \pmod{20}$$
$$\left(\frac{-7}{p}\right) = 1 \iff p = 1, 9, 11, 15, 23, 25 \pmod{28}$$
$$\left(\frac{3}{p}\right) = 1 \iff p = \pm 1 \pmod{12} \text{ is the same as } \pm 1^2 \pmod{12}$$
$$\left(\frac{5}{p}\right) = 1 \iff p = \pm 1, \pm 11 \pmod{20} \text{ is the same as } \pm 1^2, 3^2 \pmod{20}$$
$$\left(\frac{7}{p}\right) = 1 \iff p = \pm 1, \pm 3, \pm 9 \pmod{28} \text{ is the same as } \pm 1^2, 5^2, 3^2 \pmod{28}$$

Special Cases of Quadratic Reciprocity

Conjecture

For q an odd prime and p any integer, $\left(\frac{q}{p}\right) = 1 \iff p \equiv \pm\beta^2 \pmod{4q}$, where β is an odd integer. Euler generalizes this in his conjectures for $N > 0$,
$\left(\frac{N}{p}\right) = 1 \iff p \equiv \alpha^2 \pmod{4N}$, for certain odd values of α.

Special Cases of Quadratic Reciprocity

Conjecture

For q an odd prime and p any integer, $\left(\frac{q}{p}\right) = 1 \iff p \equiv \pm\beta^2 \pmod{4q}$, where β is an odd integer. Euler generalizes this in his conjectures for $N > 0$, $\left(\frac{N}{p}\right) = 1 \iff p \equiv \alpha^2 \pmod{4N}$, for certain odd values of α.

Euler was really solving special cases of quadratic reciprocity!

Building Correspondences

Lemma

If $D \equiv 0, 1 \pmod 4$ *is a nonzero integer, then there is a unique homomorphism* $\chi : (\mathbb{Z}/D\mathbb{Z})^* \longrightarrow \{\pm 1\}$ *such that* $\chi([p]) = \left(\frac{D}{p}\right)$ *for odd primes p not dividing D. Furthermore,* $\chi([-1]) = 1$ *when* $D > 0$ *and* $\chi([-1]) = -1$ *when* $D < 0$.

Corollary

Let n be a nonzero integer, and let $\chi : (\mathbb{Z}/4n\mathbb{Z})^* \longrightarrow \{\pm 1\}$ *be the homomorphism above when* $D = -4n$. *If p is an odd prime not dividing n, then the following are equivalent:*

(i) $p \mid x^2 + ny^2, \gcd(x, y) = 1$

(ii) $\left(\frac{-n}{p}\right) = 1$

(iii) $[p] \in \ker(\chi) \subseteq (\mathbb{Z}/4n\mathbb{Z})^*$

Quadratic Forms and Reciprocity

Definition (Quadratic Forms)

A quadratic form is a function of the form $f(x, y) = ax^2 + bxy + cy^2$ for $a, b, c \in \mathbb{Z}$.

Equivalent and Proper Equivalent Forms

Two quadratic forms $f(x, y)$ and $g(x, y)$ are said to be equivalent if there exist integers p, q, r, s such that

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

and $ps - qr = \pm 1$. They are properly equivalent if $ps - qr = 1$.

Definition (Discriminant)

The discriminant of a quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is given by $D = b^2 - 4ac$.

More on Quadratic Forms and Reciprocity

Definition (Reduced Form)

A primitive positive definite form $ax^2 + bxy + cy^2$ is said to be reduced if $|b| \leq a \leq c$, and $b \geq 0$ if either $|b| = a$ or $a = c$.

Theorem

Let $D < 0$ be fixed. Then the number $h(D)$ of classes of primitive positive definite forms of discriminant D is finite, and furthermore $h(D)$ is equal to the number of reduced forms of discriminant D.

Reduced Forms of Discriminant D

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

Connection to $p = x^2 + ny^2$

Theorem

Let $D \equiv 0, 1 \pmod 4$ be negative, and consider $\chi : (\mathbb{Z}/D\mathbb{Z})^* \to \{\pm 1\}$ from before. Then for an odd prime p not dividing D, $[p] \in \ker(\chi)$ if and only if p is represented by on of the $h(D)$ reduced forms of discriminant D.

Theorem

Let n be a positive integer. Then

$$h(-4n) = 1 \iff n = 1, 2, 3, 4, 7$$

Genus Theory

Definition (Genus)

We say two primitive positive definite forms of discriminant D are in the same genus if they represent the same values in $(\mathbb{Z}/D\mathbb{Z})^*$

For $D = -20$

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

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

Composition and Genera

Lemma

Give a negative integer $D \equiv 0, 1 \pmod 4$

(i) *The values in* $(\mathbb{Z}/D\mathbb{Z})^*$ *represented by the principal form of discriminant* D *for a subgroup* $H \subseteq \ker(\chi)$.

(ii) *The values in* $(\mathbb{Z}/D\mathbb{Z})^*$ *represented by* $f(x, y)$ *forms a coset of* H *in* $\ker(\chi)$

Definition (Dirichlet Composition)

Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be primitive positive definite forms of discriminant $D < 0$ which satisfy $\gcd(a, a', (b + b')/2) = 1$. Then the Dirichlet composition of $f(x, y)$ and $g(x, y)$ is the form

$$F(x, y) = aa'x^2 + Bxy + \frac{B^2 - D}{2}(4aa')y^2$$

More Composition and Genera

Theorem

Let $D \equiv 0, 1 \pmod 4$ be negative, and let $C(D)$ be the set of classes of primitive positive definite forms of discriminant D. Then Dirichlet composition induces a well-defined binary operation on $C(D)$ which makes $C(D)$ into a finite Abelian group whose order is the class number $h(D)$.

Since all forms in a given class represent the same numbers, sending the class to the coset of $H \subseteq \ker(x)$ it represents defines a map

$$\varphi : C(D) \longrightarrow \ker(\chi)/H$$

Note that a given fiber $\varphi^{-1}(H')$ in $\ker(\chi)/H$ consists of all classes in a given genus, and the image of φ can be identified with the set of genera.

Future Steps

With the rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$, where ω is a third root of unity we can solve special cases:

Theorem

Let p be a prime. Then $p = x^2 + 27y^2 \iff p \equiv 1 \pmod 3$ and 2 is cubic residue modulo p.

Theorem

Let p be a prime. Then $p = x^2 + 64y^2 \iff p \equiv 1 \pmod 4$ and 2 is biquadratic residue modulo p.

Generalizing work we did using the Legendre symbol is necessary. These generalizations lead us to formulating theories of Galois theory and further Class Field Theory.