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

Steven Charlton
MATH4072: Project IV
Supervisor: Dr Jens Funke

Fermat and the Sum of Two Squares

In December 1640, Fermat announced when a prime is the sum of two squares. He claimed:

$$p = x^2 + y^2 \iff p = 2, \text{ or } p \equiv 1 \pmod 4$$

and fourteen years later he added that:

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

These examples must make you wonder what happens in general. Which primes does a quadratic form represent?

Quadratic Forms

A quadratic form is a polynomial of the form $ax^2+bxy+cy^2$. We take $a, b, c \in \mathbb{Z}$, and can assume they are coprime.

The discriminant is $D = b^2 - 4ac$, and it tell us what type of numbers the quadratic form can represent. If $D < 0, a > 0$, then it only represents positive values; if $D < 0, a < 0$, negative values; if $D > 0$, both negative and positive values.

Two quadratic forms are equivalent if they differ by an orientation preserving change of basis: changing x and y by a matrix in $\mathbf{SL}(2, \mathbb{Z})$.

For a given discriminant there are only finitely many equivalence classes of forms. This number the called the class number $h(D)$ of the discriminant D. Gauss gave a way to list a representative of each class, when $D < 0$.

Theorem. *For p an odd prime not dividing integer n, the Legendre symbol $(n/p) = 1$ if and only if p is represented by a quadratic form of discriminant $4n$.*

Class Number One

If $h(-4n) = 1$, so the only quadratic form is $x^2 + ny^2$, the Legendre symbol tells us exactly which primes it represents.

The only time $h(-4n) = 1$ is when $n = 1, 2, 3, 4,$ or 7. Using quadratic reciprocity on $(-n/p)$ we can work out exactly which primes the form $x^2 + ny^2$ represents. Fermat's original results come from this with $n = 1, 2,$ and 3.

For $n = 7$, we take a small step beyond Fermat. By quadratic reciprocity $(-7/p) = 1$ iff $(p/7) = 1$, and the squares modulo 7 are $1, 2, 4$. Tweaking this to avoid $p = 2$ gives:

$$p = x^2 + 7y^2 \iff p = 7 \text{ or } p \equiv 1, 9, 11 \pmod{14}$$

Genus Theory

If $h(-4n) > 1$ we need some way to distinguish and separate the quadratic forms of that discriminant.

Group quadratic forms of discriminant D together into a genus according to what set of values H they represent in $(\mathbb{Z}/D\mathbb{Z})^*$.

Theorem. *If a genus of quadratic forms of discriminant D represents the set H in $(\mathbb{Z}/D\mathbb{Z})^*$, then an odd prime $p \nmid D$ is represented by a quadratic form in that genus if and only if $[p] \in H$.*

If a genus contains only one form, we know what primes it represents.

There are two quadratic forms of discriminant $D = -20$:

$$x^2 + 5y^2 \text{ represents } 1, 9 \text{ in } (\mathbb{Z}/20\mathbb{Z})^*$$
$$2x^2 + 2xy + 3y^2 \text{ represents } 3, 7 \text{ in } (\mathbb{Z}/20\mathbb{Z})^*$$

so each genus contains one form and now we know:

$$p = x^2 + 5y^2 \iff p = 5, \text{ or } p \equiv 1, 9 \pmod{20}$$
$$p = 2x^2 + 2xy + 3y^2 \iff p = 2, \text{ or } p \equiv 3, 7 \pmod{20}$$

There are 65 known n for which the genus of $x^2 + ny^2$ contains only one form, the largest of which is $n = 1848$. These are Euler's convenient numbers. The entire list *is* finite, and there is at most one more convenient number.

$p = 18\,518\,809$ is Prime

Euler used that $n = 1848$ is a convenient number to show $p = 18\,518\,809$ is prime by finding that the only solution in positive integers to

$$18\,518\,809 = x^2 + 1848y^2$$

is $x = 197$, and $y = 100$.

Quadratic Forms and Quadratic Fields

When D is the discriminant of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$, then there is a bijective correspondence:

$$\{ \text{ classes of quadratic forms } \} \overset{1:1}{\longleftrightarrow} \{ \text{ ideal classes } \}$$
$$ax^2 + bxy + cy^2 \longmapsto [a, (-b + \sqrt{D})/2]$$

between the ideal class group $\mathcal{C}(K)$ of K, and the set of classes of quadratic forms of discriminant D.

If the quadratic form Q and ideal class $[\mathfrak{a}]$ correspond, then ways of representing an integer m by the form Q correspond to ideals of norm m in the class $[\mathfrak{a}]$.

Since x^2+ny^2 maps to the trivial ideal class, the question of when $p = x^2+ny^2$ becomes the question of when is there an ideal of norm p. The Legendre symbol $(-n/p)$ tells us when there is an ideal of norm p. But is it principal?

The Hilbert Class Field

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

The Artin symbol links the structure of the Hilbert class field L to the ideal structure of the number field K. It defines a surjective map from the fractional ideals $\mathcal{I}(K)$ of K:

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{I}(K) \to \mathrm{Gal}(L/K)$$

with the kernel being the principal ideals $\mathcal{P}(K)$. Then by the First Isomorphism Theorem:

$$\mathcal{C}(K) = \mathcal{I}(K)/\mathcal{P}(K) \cong \mathrm{Gal}(L/K)$$

so the degree of the extension is $[L : K] = h(K)$.

The Artin symbol helps us to tell when a prime ideal $\mathfrak{p}$ in K is principal:

Theorem. *Let L be the Hilbert class field of K. Then a prime $\mathfrak{p}$ of K is principal $\iff$ $\mathfrak{p}$ splits completely in L.*

This gives us an abstract condition for solving $p = x^2 + ny^2$:

Theorem. *Let L be the Hilbert class field of $K = \mathbb{Q}(\sqrt{-n})$, and assume $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$, then for an odd prime $p \nmid n$:*

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

Dedekind's Theorem tell us how a prime ideal $\mathfrak{p}$ splits in a field extension, thus we can find an explicit criterion if we know the Hilbert class field.

Primes of the Form $p = x^2 + 14y^2 \ldots$

The Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$ is $L = K(\sqrt{2\sqrt{2} - 1})$.

We need (p) to split in $K = \mathbb{Q}(\sqrt{-14})$ and $F = \mathbb{Q}(\sqrt{2\sqrt{2} - 1})$. So we need $(-14/p) = 1$, and by Dedekind's Theorem the polynomial x^4+2x^2-7, which generates F, has a root modulo p

This gives a criterion for $p \neq 2, 7$:

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

. . . And Beyond

This theory allows us to solve the question $p = x^2 + ny^2$ for infinitely many n but not all. To deal with cases when $\mathcal{O}_K \neq \mathbb{Z}[\sqrt{-n}]$, we can use the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$.

Much of this works for indefinite quadratic forms as well. The narrow class field can tell whether an ideal is principal and if it is generated by an element of positive norm. This gives a way of finding when $p = x^2 - ny^2$ as well.