Durham University

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

Steven Charlton
SET Awards 2012
Supervisor: Dr Jens Funke

Fermat's Sum of Two Squares

In December 1640, Pierre de Fermat announced his theorem on when a prime is expressible as the sum of two squares. He claimed that for a prime p:

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

Fourteen years later, in September 1654, he added two related results:

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

Typically, Fermat neglected to prove these claims, and this responsibility fell to subsequent generations of mathematicians. How can they be proved, and how can they be generalised?

The consistent form of these three claims demands a unified explanation, and it hints at a deeper level of structure underlying these results.

Gauss's Theory of Quadratic Forms

A major milepost on this quest comes from Gauss's theory of quadratic forms.

A **(binary) quadratic form** is a polynomial of the form:

$$f(x, y) = ax^2 + bxy + cy^2$$

For our purposes we are mostly interested in **primitive integral** binary quadratic forms, those where the coefficients a, b and c are coprime integers.

A quadratic form $f(x, y)$ **represents** the integer m if $m = f(x, y)$ has a solution in integers. The intention is to construct a criterion which classifies all primes a given quadratic forms represents.

An **equivalence** between quadratic forms is defined according to the orbits of the set of quadratic forms under the following group action of $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$:

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \cdot f(x, y) = f(px + ry, qx + sy)$$

Under this, equivalent forms represent the same integers and have the same **discriminant**:

$$D = b^2 - 4ac$$

The set of quadratic forms of discriminant D breaks up into a finite number of equivalence classes, called the **form class number** $h(D)$ of the discriminant. Gauss gave a method to list these classes algorithmically by using the so-called *reduced* forms.

Theorem. *An odd prime $p \nmid D$ is represented by some quadratic form of discriminant D if and only if D is a quadratic residue modulo p, which can be expressed, using the Legendre symbol, as $(D/p) = 1$.*

An immediate Corollary of this Theorem: if the class number $h(D) = 1$, then there is only one form of discriminant D and the Legendre symbol tells us exactly which primes it represents.

Class Number One

For which discriminants is the class number $h(D) = 1$? When is $x^2 + ny^2$ the only form of discriminant $D = -4n$, up to equivalence?

For so-called positive-definite forms $D < 0$, and the *Baker-Heegner-Stark Theorem* completely classifies all the discriminants with class number one. For even discriminants $D = -4n$, this occurs for $n = 1, 2, 3, 4$, and 7.

Using the Theorem, and applying quadratic reciprocity to $(-4n/p) = 1$ in the cases $n = 1, 2$, and 3, we get a proof of Fermat's three claims.

When $n = 4$, we find $p = x^2 + 4y^2 \iff p \equiv 1 \pmod 4$, but this already follows trivially from the case $n = 1$, which is the statement of Fermat's Two Squares Theorem.

When $n = 7$, we can take a small step beyond Fermat. Except for the even prime $p = 2$, and the odd primes p dividing $D = -28$, we have: $p = x^2 + 7y^2 \iff (-28/p) = 1$. But $(-28/p) = (-7/p)$, and by quadratic reciprocity $(-7/p) = (p/7)$. This means p is a square modulo 7, and so for $p \neq 2, 7$:

$$p = x^2 + 7y^2 \iff p \equiv 1, 2, 4 \pmod 7$$

No such classification for class number one is known in the indefinite case, $D > 0$. But the class number can be calculated, so we can start *listing* which discriminants have class number $h(D) = 1$, and use the Theorem to find criteria in these cases. For even discriminants $D = 4n$, this list begins $n = 2, 5, 13, 17, 29, \ldots$

$$p = x^2 - 2y^2 \iff p \equiv 1, 7 \pmod 8$$
$$p = x^2 - 5y^2 \iff p \equiv 1, 4 \pmod 5$$
$$p = x^2 - 13y^2 \iff p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$$

The Theorem applies equally well to find criteria when the discriminant is odd:

$$p = x^2 + xy + 3y^2 \iff p \equiv 1, 3, 4, 5, 9 \pmod{11}$$
$$p = x^2 + xy - y^2 \iff p \equiv 1, 4 \pmod 5$$

Lagrange's Genus Theory

What can we do when the class number is greater than one? A partial answer is provided by Lagrange's genus theory. The basic idea of genus theory is simple but elegant, and is best illustrated with an example.

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

$$x^2 + 5y^2 \quad \text{and} \quad 2x^2 + 2xy + 3y^2$$

Applying the Theorem to this discriminant, we find $p \neq 2, 5$ is represented by *some* quadratic form of discriminant $D = -20$ if and only if $(-20/p) = 1$. With quadratic reciprocity this is just $p \equiv 1, 3, 7, 9 \pmod{20}$. Yet all we can say now is:

$$\left.\begin{array}{l} p = x^2 + 5y^2 \text{ or} \\ p = x^2 + 2xy + 3y^2 \end{array}\right\} \iff p \equiv 1, 3, 7, 9 \pmod{20}$$

But look at what values each form represents in $(\mathbb{Z}/20\mathbb{Z})^*$; substitute in the possible x and y modulo 20:

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

Now pick a prime $p \equiv 1, 9 \pmod{20}$. Then p is represented by one of the forms of discriminant $D = -20$. But since $p \not\equiv 3, 7 \pmod{20}$ reducing modulo 20 shows $p \neq 2x^2 + 2xy + 3y^2$. Leaving the only possibility as $p = x^2 + 5y^2$. The same argument gives the corresponding result for the other form:

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

Generally: two quadratic forms of discriminant D are in the same **genus** if they represent the same set of values H in $(\mathbb{Z}/D\mathbb{Z})^*$.

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

When a genus contains one quadratic form, we know exactly what primes the form represents and can describe them by congruences.

Euler's Convenient Numbers

Which genera contain only one quadratic form? When is $x^2 + ny^2$ the only form in its genus?

For a fixed discriminant, each genus contains the same number of forms. There is a criterion in terms of the structure of the 'form class group', or equivalently on the class number and the discriminant, which detects when there is one form per genus.

There are 65 known positive n for which the genus of $x^2 + ny^2$ contains only one form, these are Euler's **convenient numbers**. The entire list *is* finite and includes $n = 6, 8, 9, 10, 12, \ldots$; the largest convenient number known is $n = 1848$. Making the needed exclusions, we get results like:

$$p = x^2 + 6y^2 \iff p \equiv 1, 7 \pmod{24}$$
$$p = 2x^2 + 3y^2 \iff p \equiv 5, 11 \pmod{24}$$
$$p = x^2 + 8y^2 \iff p \equiv 1, 9, 17, 25 \pmod{32}$$
$$p = x^2 + 9y^2 \iff p \equiv 1, 13, 25 \pmod{36}$$

Since there are no obvious bounds on the variables, determining whether or not a prime is represented by an indefinite form is not straight-forward; finding criteria for indefinite forms is advantageous. Genus theory applies equally well for indefinite forms, finding criteria for $x^2 - ny^2$, when $n = 3, 6, 7, 8, 10, \ldots$

$$p = x^2 - 3y^2 \iff p \equiv 1 \pmod{12}$$
$$p = x^2 - 6y^2 \iff p \equiv 1, 19 \pmod{24}$$
$$p = x^2 - 7y^2 \iff p \equiv 1, 9, 25 \pmod{28}$$

and it produces results for the odd discriminants:

$$p = x^2 + xy + 4y^2 \iff p \equiv 1, 4 \pmod{15}$$
$$p = x^2 + xy - 5y^2 \iff p \equiv 1, 4, 16 \pmod{21}$$

But surprisingly genus theory shows congruence conditions are not enough in general!

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

Euler originally discovered the convenient numbers, in a different guise, when searching for large primes. To him a number n is convenient if: $m = x^2 + ny^2$ has one solution in positive integers implies m is prime.

Using that $n = 1848$ is a convenient number, Euler proved that $p = 18\,518\,809$ is prime by showing the only solution to:

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

in positive integers is $x = 197$, and $y = 100$. A large prime, and a major accomplishment for the time!

Nowadays this is reduced to a few milliseconds of computer time, and the results dwarfed by 'Titanic' primes.

Quadratic Forms and Quadratic Fields

When genus theory fails to work we need more sophisticated techniques.

If $D = d_K < 0$ is the discriminant of some imaginary quadratic number field $K = \mathbb{Q}(\sqrt{d})$ there is a bijective correspondence:

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

between the ideal class group $\mathcal{C}(K)$ of K, and the set of classes of positive-definite quadratic forms of discriminant D. There is a similar correspondence between narrow ideal classes in a real quadratic field and indefinite forms of discriminant $D = d_K > 0$.

Up to units of K, representations of m by a quadratic form Q correspond to ideals of norm m in the (narrow) ideal class $[\mathfrak{c}]$ corresponding to Q.

The form $x^2 + ny^2$ maps to the trivial (narrow) ideal class. So the question of representing primes p by $x^2 + ny^2$ becomes the question: When is there a (totally positive) principal ideal of norm p? The splitting of (p) tells us if there is an ideal of norm p, how can we determine if it is *principal*?

Class Field Theory

With an understanding of class field theory we will be in a position to determine when an ideal is principal.

Class field theory seeks to classify and construct all the abelian extensions of a number field, those extensions which are Galois and have abelian Galois group.

A **modulus** $\mathfrak{m}$ of a number field K is a formal product of prime ideals and distinct *real* embeddings $K \hookrightarrow \mathbb{C}$.

A **congruence subgroup** for $\mathfrak{m}$ is a subgroup of the fractional ideals $\mathcal{I}_K(\mathfrak{m})$ coprime to $\mathfrak{m}$, containing the principal ideals $\mathcal{P}_{K,1}(K)$.

The **Artin map** of a Galois extension L/K, sending a prime ideal $\mathfrak{p}$ to its '*Frobenius*' element in $\mathrm{Gal}(L/K)$, defines a homomorphism:

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

The theory culminates in the *Existence Theorem*, allowing us to construct field extensions with useful properties:

Theorem (Existence). *For a modulus $\mathfrak{m}$ 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.*

The Hilbert Class Field

The class field of primary importance to us is the Hilbert class field.

The **Hilbert class field** L of a number field K arises from applying the existence theorem to the modulus $\mathfrak{m} = 1$, and the congruence subgroup $\mathcal{P}_{K,1}(1) = \mathcal{P}(K)$. An equivalent definition is:

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

The Artin map of L/K becomes a *surjective* homomorphism from the fractional ideals $\mathcal{I}(K) = \mathcal{I}_K(1)$:

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

which has kernel $\mathcal{P}(K)$, the principal ideals. The First Isomorphism Theorem implies $\mathrm{Gal}(L/K) \cong \mathcal{P}(K)/\mathcal{I}(K) = \mathcal{C}(K)$, so the Hilbert class field has degree $[L : K] = h(K)$.

The order of the Artin map of a prime ideal tells us the 'inertial degree' of the prime. Since L/K is unramified, it follows that the Artin map of $\mathfrak{p}$ is trivial if and only if $\mathfrak{p}$ splits completely. This means a prime ideal splits completely in L/K if and only if it is principal!

With the correspondence between forms and ideals this leads to the abstract criterion:

Theorem. *If the quadratic form Q corresponds to the principal ideal class in K, then:*

$$p \text{ is represented by } Q \iff (p) \text{ splits completely in the Hilbert class field of } K$$

With *Dedekind's Theorem* on splitting of prime ideals in an extension this can be made explicit.

The form $x^2 + 29y^2$ corresponds to the principal ideal class in the quadratic field $K = \mathbb{Q}(\sqrt{-29})$

The Hilbert class field of K is $L = K(\alpha)$, where α is a root of $t^6 - 2t^3 + t^2 + 2t + 2$.

Dedekind's Theorem excludes primes dividing the discriminant of the polynomial, so for $p \neq 2, 29$:

$$p = x^2 + 29y^2 \iff \begin{cases} (-29/p) = 1 \text{ and} \\ t^6 - 2t^3 + t^2 + 2t + 2 \text{ has a root modulo } p \end{cases}$$

With tables of Hilbert class fields, or a computer algebra system, these criteria can be constructed plentifully:

$$p = x^2 + 23y^2 \iff \begin{cases} (-23/p) = 1 \text{ and} \\ t^3 - t^2 + 1 \text{ has a root modulo } p \end{cases}$$

$$p = x^2 + 34y^2 \iff \begin{cases} (-34/p) = 1 \text{ and} \\ t^4 + t^3 - 3t^2 - 8t - 4 \text{ has a root modulo } p \end{cases}$$

The Narrow Class Field

Since the Hilbert class field cannot detect the narrow ideal class, we bring in another class field to investigate indefinite forms.

The **narrow class field** L of a number field K arises from applying the existence theorem to the modulus $\mathfrak{m}$ consisting of all real embeddings $K \hookrightarrow \mathbb{C}$, and the congruence subgroup $\mathcal{P}_{K,1}(\mathfrak{m}) = \mathcal{P}^+(K)$ of totally positive principal fractional ideals.

The Artin map of L/K again becomes a surjective homomorphism:

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

but for this class field the kernel is now $\mathcal{P}^+(K)$, the totally positive principal fractional ideals.

The narrow class field is unramified at all finite primes, so a prime ideal $\mathfrak{p}$ splits completely if and only if the Artin map of $\mathfrak{p}$ is trivial. This means $\mathfrak{p}$ splits completely if and only if $\mathfrak{p}$ is a totally positive principal ideal.

Theorem. *If the quadratic form Q corresponds to the totally positive principal ideal class in K, then:*

$$p \text{ is represented by } Q \iff (p) \text{ splits completely in the narrow class field of } K$$

Again with Dedekind's Theorem this criterion can be made explicit.

The form $x^2 - 142y^2$ corresponds to the totally positive principal ideal class in $K = \mathbb{Q}(\sqrt{142})$.

The narrow class field of K is $L = K(\alpha)$, where α is a root of $t^6 - 2t^5 - 5t^4 + 56t^2 + 64t + 128$.

For $p \neq 2, 5, 71$:

$$p = x^2 - 142y^2 \iff \begin{cases} (142/p) = 1 \text{ and} \\ t^6 - 2t^5 - 5t^4 + 56t^2 + 64t + 128 \text{ has a root modulo } p \end{cases}$$

So whilst it is not obvious whether or not the Diophantine equation $19 = x^2 - 142y^2$ has a solution, the condition tells us it doesn't. A brute-force check shows the polynomial has no roots modulo 19. The criterion does not hold, and so we should not bother to look for a solution – there is none.

Similar results can be found for other indefinite quadratic forms:

$$p = x^2 - 321y^2 \iff \begin{cases} (321/p) = 1 \text{ and} \\ t^6 - 2t^5 + 2t^4 - 2t^3 + 47t^2 - 20t + 163 \text{ has a root modulo } p \end{cases}$$

Cubic Forms

With finesse, class fields and the theory developed can be used to investigate higher forms.

Let's investigate the cubic form $a^3 + 11b^2 + 121c^2 - 33abc$. What primes does it represent?

This is the norm-form on the ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{11}]$ of the cubic field $K = \mathbb{Q}(\sqrt[3]{11})$.

This form represents a prime p if and only if there is an element of norm p in $\mathcal{O}_K$. Since -1 has norm -1, this happens if and only if there is a principal ideal of norm p.

The Hilbert class field of $K = \mathbb{Q}(\sqrt[3]{11})$ is $L = \mathbb{Q}(\alpha)$ where α is a root of $t^6 - 15t^4 + 9t^2 - 4$.

If there is a principal ideal $\mathfrak{a} \subset K$ of norm p, then $\mathfrak{a}$ splits completely in the Hilbert class field, and so $t^6 - 15t^4 + 9t^2 - 4$ has a root modulo p. Conversely if $t^6 - 15t^4 + 9t^2 - 4$ has a root modulo p, there is an ideal $\mathfrak{a} \subset K$, above (p), which splits completely in L. This is a principal ideal of norm p.

So we have the following condition:

For $p \neq 2, 3, 11$:

$$p = a^3 + 11b^3 + 121c^3 - 33abc \iff t^6 - 15t^4 + 9t^2 - 4 \text{ has a root modulo } p$$

Conditions like this allow us to determine easily whether certain more complicated Diophantine equations have solutions or not:

The equation
$$5 = a^3 + 11b^3 + 121c^3 - 33abc$$
has no solutions in integers, because $t^6 - 15t^4 + 9t^2 - 4$ has no roots modulo 5

In a similar way such conditions can be found for other cubic forms:

$$p = a^3 + 7b^3 + 49c^3 - 21abc \iff \begin{cases} t^9 - 9t^7 - 69t^6 + 27t^5 + 414t^4 + 1560t^3 - \\ 621t^2 - 4761t - 1583 \text{ has a root modulo } p \end{cases}$$

The Langlands Program

The quest to find similar solutions for more general polynomial equations can be studied using *automorphic forms*, and is the theme of non-abelian class field theory and the eminent, far-reaching Langlands program.

In recent decades this has become the central unifying theme of modern number theory and is at the forefront of current research.