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

Steven Charlton

1 Title

I'm going to talk about primes of the form $x^2 + ny^2$, or more generally representing numbers by binary quadratic forms. I'm going to be looking more at the class field theory side of things.

2 Introduction

I'll start by giving you some motivating examples, which will hopefully pique your curiosity, and make you wonder what happens in general.

Then I'll go on to define property a binary quadratic form, and some of the other notions we'll make use of, before giving a quick proof of Fermat's theorem on the sum of two squares.

Then I'll briefly introduce the Hilbert class field, and use it to find a condition for which primes $x^2 + 23y^2$ represents.

I'll end with a run down of what we can and can't do so far, and some possible extensions to the question.

3 Motivating Examples

So now the promised examples. On the first line we have Fermat's theorem on sums of two squares: an prime p is the sum of two squares if and only if the prime is equal to 2, or the prime is congruent to 1 mod 4.

And the next line is another one of Fermat's results. You can see the structure of it is quite similar to the first: a prime is represented by $x^2 + 2y^2$ if and only if it satisfies some congruence, or is in a list of exceptions. Similar for the next two examples. You begin to wonder if this sort of thing happens in general?

Then when you get told something like this for $x^2 + 17y^2$..., you have to wonder where it comes from and how it fits in the grand scheme of things. What the difference between 17 and the others, that means the criterion is so different? I hope to explain some of the theory behind this.

4 Binary Quadratic Forms

A binary quadratic form is a degree two (quadratic) homogeneous polynomial in two variables (binary), something of the form $ax^2 + bxy + cy^2$. We take a, b, c, integers and assume that they are coprime, otherwise divide through by the GCD and get a simpler quadratic form.

The discriminant is $D = b^2 - 4ac$, and tells us what type of numbers the quadratic form represents. Using the identity

$$4aQ(x, y) = (2ax + by)^2 - Dy^2$$

you can see that if $D > 0$, then Q represents both positive and negative values: it is indefinite, and if $D < 0$, then Q represents only positive values or only negative values depending on the sign of a, and then is positive/negative definite.

There is a notion of equivalence between quadratic forms: change of basis, changing x, y by a matrix in $\mathrm{SL}(2, \mathbb{Z})$. Equivalent forms represents the same values, and have the same discriminant. So we can group all equivalent forms together, and just look at one representative.

For a fixed discriminant there are a finite number of equivalence classes. For $D < 0$, Gauss gave a method to list a canonical representative of each class, the so-called reduced forms.

If D is the discriminant of an imaginary quadratic number field $\mathbb{Q}(\sqrt{d})$, then there is a correspondence between the quadratic forms of discriminant D and ideals in the number field. The correspondence means that a number m is represented by the form Q if and only if there is an ideal of norm m in the class $[\mathfrak{a}]$ corresponding to Q.

$$\begin{array}{ccc} \{ \text{ classes of quadratic forms } Q \ \} & \overset{1:1}{\longleftrightarrow} & \{ \text{ ideal classes } [\mathfrak{a}] \ \} \\ \text{representations of } m \text{ by } Q & \longleftrightarrow & \text{ideals of norm } m \text{ in } [\mathfrak{a}] \end{array}$$

So the question of when $p = x^2 + ny^2$ can be rephrased as asking when there is a principal ideal of norm p in the number field.

Lastly we have a theorem, telling us when some quadratic form of discriminant $D = -4n$ represents a given prime p. So what is there is only one quadratic form of that discriminant? Then if $(-n/p) = 1$, p must be represented by this form, and vice versa.

5 Fermat and the Sum of Two Squares

When is a prime the sum of two squares?

Here we want to represent p by a binary quadratic form of discriminant -4, so we should start by listing all of them. We can do this either by listing the reduced forms à la Gauss, or by using the link to the quadratic field $\mathbb{Q}(i)$. Either way, we find there is only one quadratic form of discriminant -4, and (a representative of) it is $x^2 + y^2$.

Using the previous theorem, and observation: for an odd prime not dividing 1, $p = x^2 + y^2$ if and only if $(-1/p) = 1$, and using a supplement to quadratic reciprocity, we know $(-1/p) = 1 \iff p \equiv 1 \pmod 4$. Then we just check the few excluded cases: $p = 2$, and p dividing 1. $p = 2$ is clearly of this form, and there are no primes dividing 1, so putting this together we get Fermat's lovely result on when a prime is the sum of two squares.

You might then wonder when there is only one binary quadratic form of discriminant $-4n$, and so when something similar works. This only happens for $n = 1, 2, 3, 4,$ and 7. So we do get some more results but nothing as general as we would hope. Notice this doesn't even work for $n = 5$.

6 The Hilbert Class Field

Now we introduce the class field theory side of things. The Hilbert class field is defined to be the maximal unramified abelian extension of a number field, but for us the actual definition is not as important as its properties. One of these properties is it can tell when a prime ideal $\mathfrak{p}$ of K is principal. The Artin symbol links the field structure of L to the ideal structure of K, and gives the following theorem. A prime of K is principal if and only if it splits completely in L.

Using Dedekind's theorem we can give a criterion for this splitting in terms of the polynomial generating the extension having a root modulo $\mathfrak{p}$.

Now we have a way to tell when an ideal is principal, and linking quadratic fields back to quadratic forms, we can use this to answer the question in many more cases.

7 Primes of the Form $x^2 + 23y^2$

To answer this, first let's consider $\mathbb{Q}(\sqrt{-23})$. The discriminant of this is -23, rather than $-4 \cdot 23$ as the ring of integers isn't $\mathbb{Z}[\sqrt{-23}]$, so we can't directly find which primes are of this form. Firstly the quadratic form corresponding to the principal ideal class in K is $x^2 + xy + 6y^2$, and so using the Hilbert class field we can find which primes are of this form.

The Hilbert class field is $K(\alpha)$, where $\alpha^3 - \alpha - 1 = 0$. Now $p = x^2 + xy + 6y^2$ iff there is a principal ideal of norm p in K, which is iff (p) splits into principal ideals in K. These principal ideals split completely in L, and so (p) splits completely in L, and conversely if p splits completely in L, then p splits into principal ideals in K. So $p = x^2 + xy + 6y^2$ iff p splits completely in L.

Splitting completely in L is equivalent to splitting in F, and K, and so using Dedekind's theorem and the Legendre symbol we get the condition, for $p \neq 23$...

Now use the identity

$$x^2 + xy + 6y^2 = (x + y/2)^2 + 23(y/2)^2$$

Now that 2 isn't represented by either quadratic form, and for other primes p is odd. Working modulo 2, you can see that y must be even. So if $p = x^2 + xy + 6y^2$, then $p = x^2 + 23y^2$, and vice versa. So being represented by one form is equivalent to being represented by the other, and putting this together we get the same condition on when $p = x^2 + 23y^2$.

8 Going Further?

The Hilbert class field gives a quite general method for finding such conditions for a lot of n, but not all. In particular we need that $\mathbb{Z}[\sqrt{-n}]$ is the ring of integers of $\mathbb{Q}(\sqrt{-n})$, so n is square-free, and $n \equiv 1, 2 \pmod 4$. Occasionally we can tweak things to get a condition for other n, like when $n = 23$.

The ring class field can deal with all the remaining cases of $x^2 + ny^2$, for positive definite forms. So we can answer the question for all n.

We can play similar games with indefinite forms, although we need to look at the narrow class field in place of the Hilbert class field, to tell when an ideal is generated by an element of positive norm.

These ideas can be extended somewhat to finding which primes certain ternary cubic forms or higher represent.

This still leaves some problems unsolved; we can't say which primes an arbitrary binary quadratic form represents, nor have we looked at quadratic forms in 2 or more variables. Some of these questions can be studied using modular forms.

9 Any Questions?