Durham University

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

Steven Charlton
Rising Stars 2012
Supervisor: Dr Jens Funke

The Sum of Two Squares

Question: Which numbers can be written as the sum of two squares?

More fundamental: Which *primes* are the sum of two squares?

Prime	Two Squares?	Prime	Two Squares?
2	$1^2 + 1^2$	31	No
3	No	37	$1^2 + 6^2$
5	$1^2 + 2^2$	41	$4^2 + 5^2$
7	No	43	No
11	No	47	No
13	$2^2 + 3^2$	53	$2^2 + 7^2$
17	$1^2 + 4^2$	59	No
19	No	61	$5^2 + 6^2$
23	No	67	No
29	$2^2 + 5^2$	71	No

What patterns can *you* see in the results of this table?

Fermat's Two Squares Theorem

Fermat noticed that the odd primes which can be written as the sum of two squares seem to be the primes which exceed a multiple of 4 by 1.

He claimed this was always the case, that is:

$$p = x^2 + y^2 \text{ if and only if } p \equiv 1 \pmod 4$$

The 'congruence' notation $p \equiv a \pmod d$, meaning p and a differ by a multiple of d, gives a concise way of writing Fermat's criterion.

In later years Fermat found related results, claiming for $p > 3$:

$$p = x^2 + 2y^2 \text{ if and only if } p \equiv 1, 3 \pmod 8$$
$$p = x^2 + 3y^2 \text{ if and only if } p \equiv 1 \pmod 3$$

Unfortunately he did not provide proofs of any of these claims. It took Euler forty years to give complete proofs.

How can they be proved, and how can they be extended?

Gauss's Theory of Quadratic Forms

A quadratic form is a polynomial:

$$ax^2 + bxy + cy^2$$

Its discriminant is $D = b^2 - 4ac$.

A suitable change of variables gives equivalent forms which have the same discriminant and represent the same integers.

Under this equivalence there are a finite number of different forms with discriminant D, which can be listed algorithmically.

This leads to the first simple criterion and some proofs:

Theorem. *If p is an odd prime which doesn't divide D, then: p is represented by some quadratic form of discriminant D if and only if D is a square modulo p.*

A Useful Criterion . . .

There is one form of discriminant $D = -4$, given by $x^2 + y^2$.

To find which primes the forms of discriminant $D = -4$ represent, look for when -4 is a square modulo p.

Quadratic reciprocity relates 'p is a square modulo q' and 'q is a square modulo p'.

It tells us -4 is a square modulo p if and only if $p \equiv 1 \pmod 4$, proving Fermat's first claim.

Since there is one form of each discriminant $D = -8$ and -12, the same works to prove Fermat's other claims.

. . . But Rarely Sufficient

Usually there are many forms of discriminant D, and the criterion can't separate them.

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

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

The criterion would tell us that together they represent the primes:

$$p \equiv 1, 3, 7, 9 \pmod{20}$$

but it can't say what they represent individually.

Lagrange's Genus Theory

To try to distinguish the forms discriminant D Lagrange considered what values the forms represent modulo D.

Substituting the possible values modulo 20 into the two quadratic forms of discriminant $D = -20$ shows:

$$x^2 + 5y^2 \text{ represents } 1, 9 \text{ modulo } 20$$
$$2x^2 + 2xy + 3y^2 \text{ represents } 3, 7 \text{ modulo } 20$$

With this we identify which form represents which primes:

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

Convenient Numbers

Using genus theory similar conditions can be found in several other cases.

Keeping in mind the 'usual' exclusions, we get results like:

$$p = x^2 + 6y^2 \text{ if and only if } p \equiv 1, 7 \pmod{24}$$
$$p = x^2 + 15y^2 \text{ if and only if } p \equiv 1, 19, 31, 49 \pmod{60}$$
$$p = x^2 - 7y^2 \text{ if and only if } p \equiv 1, 9, 25 \pmod{28}$$

When congruences describe primes of the form $x^2 + ny^2$, then the positive integer n is called a convenient number.

There are 65 known convenient numbers, and possibly one more. As some numbers aren't convenient, congruences can't describe the primes.

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

Euler originally discovered the convenient numbers, in a different guise, when searching for large primes.

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 $y = 100$.

Class Field Theory and the Langlands Program

When genus theory stops working we need more sophisticated techniques from algebraic number theory.

Using techniques from class field theory we can find criteria like:

$$p = x^2 + 23y^2 \text{ if and only if } \begin{cases} -23 \text{ is a square modulo } p \text{ and} \\ x^3 - x^2 + 1 \text{ has a root modulo } p \end{cases}$$

But even this only works for particular types of quadratic forms.

The quest to find similar solutions for more general polynomial equations is the theme of non-abelian class field theory and the eminent and 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.