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

Description of Poster – SET Awards 2012

Steven Charlton

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

More fundamental: Which *primes* can be written as 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

Answer: This intrigued Fermat (1601–1665) who noticed a simple pattern in the results of the table. Primes surpassing a multiple of four by one are the sum of two squares, primes surpassing a multiple of four by three are not.

Fermat claimed this to always be the case, announcing his Two Squares Theorem[1]:

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

But not one for proving his claims, Fermat left this for subsequent mathematicians to supply. How can this be proved and generalised?

Claims: Fourteen years after making this claim, Fermat announced two further tantalising results related to it. He found conditions describing when a prime is the sum of a square and twice or thrice a square:

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

It would take four decades of work and effort from Euler (1707–1783) before these claims would finally concede to proof. But this only served to raise more questions, and lead Euler to many results and conjectures of his own.

Out of this several questions naturally arise:

[1] The 'congruence' notation $a \equiv b \pmod n$, meaning a and b differ by a multiple of n, provides a concise way to write the claim.

- Do conditions describing which primes are represented always exist?
- How can we find or construct these conditions?
- Are such conditions always similar to those Fermat found?

Elementary Solutions: Gauss's (1777–1855) theory of quadratic forms leads to a simple and elegant condition describing the primes *certain groups* of quadratic forms represent. It gives a unified explanation for Fermat's claims and their similar structure. But this simplicity is at the expense of generality. It provides a complete solution in only a few cases, and cannot separate groups containing many forms.

Lagrange's (1736–1813) genus theory *refines* the results of this condition, breaking the forms in one group up into 'genera'. It gives a more fundamental reason for the appearance of congruence conditions in Fermat's claims, and allows similar conditions to be derived effortlessly:

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$$
$$p = x^2 - 3y^2 \iff p \equiv 1 \pmod{12}$$

Unfortunately, it severely limits when congruence conditions are sufficient. Two forms in the same genus can *never* be separated with congruences.

Sophisticated Solutions: When genus theory fails we are forced to reach for more sophisticated techniques. By relating quadratic forms to more algebraic objects we can unleash the full power of class field theory on the problem. This produces a *complete* solution to primes of the form $x^2 + ny^2$, and sets a general form for the criteria: "a certain polynomial has a root modulo p". This can be made explicit in examples:

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

But *even* this only applies to special types of quadratic form. Currently, the quest to find similar solutions for more general equations is the theme of eminent Langlands (1936) program.

The poster takes the reader on a tour through a cross-section of the history and results of number theory, sparked by Fermat's observations. Throughout, we introduce and apply increasingly powerful and general techniques to study the problem of representing primes by quadratic form. Pushing these techniques to their limits, I concoct a multitude of original criteria describing the primes represented by an eclectic range of forms.