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

In a letter to Marin Mersenne, dated December 25, 1640, Pierre de Fermat observed that an odd prime p can be written as the sum of two squares exactly when p surpasses a multiple of 4 by 1. That is:

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

In later years he wrote of related results, giving conditions which describe when a prime is the sum of a square and twice a square, or a prime is the sum of a square and thrice a square. Essentially Fermat was determining which primes are represented by the quadratic forms:

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

Fermat, typically, neglected to provide proofs for these claims, and this responsibility fell to later mathematicians. Obtaining complete proofs of these required a full forty years of work and effort on the part of Leonhard Euler, leading him to many results and conjectures of his own about other special cases.

Generally one can ask if there is condition which describes all the primes a given quadratic form represents, and if there is how can we find it?

Carl Friedrich Gauss's theory of quadratic forms and their equivalence leads to a simple and elegant criterion to describe which primes certain groups of quadratic forms represent. This simplicity comes at a price; usually the groups contain many forms representing different primes and this condition is not powerful enough to separate them further.

Genus theory, an idea by Joseph-Louis Lagrange which breaks the forms in a group up into 'genera', refines the results of this criterion. Now it is almost effortless to produce criterion like:

$$p = x^2 + 5y^2 \text{ if and only if } p \equiv 1, 9 \pmod{20}$$
$$p = x^2 - 7y^2 \text{ if and only if } p \equiv 1, 9, 25 \pmod{28}$$

But this is only the beginning. Things continue to work for a while, and then abruptly stop. These methods fail to find criteria in cases like $x^2 + 11y^2$, $x^2 + 14y^2$ and almost all others. More strikingly, this shows that congruence condition describing the primes do not always exist. What goes wrong?

In order to explain this, and to have a generally applicable theorem giving criterion, we must push quadratic forms to the background, and study more algebraic objects.

A correspondence between quadratic forms and ideals builds a dictionary between these two notions. Using it questions about one are translated to the other where they can be studied and answered using powerful techniques from number theory such as the Hilbert class field of class field theory. From this we get a general form for such criteria: "a certain polynomial has a root modulo p". This can be made explicit to obtain criterion like:

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