When is $p = x^2 + ny^2$?

David Cox wrote a book

Primes of the form $x^2 + ny^2$.

The main theme is, given n, which primes can be written as $x^2 + ny^2$.

1 Conditions for $p = x^2 + ny^2$

1. $p = x^2 + y^2$ iff $p \equiv 1 \pmod 4$.
2. $p = x^2 + 2y^2$ iff $p = 2$ or $p \equiv 1, 3 \pmod 8$.
3. $p = x^2 + 3y^2$ iff $p = 3$ or $p \equiv 1 \pmod 8$.
4. $p = x^2 + 5y^2$ iff $p = 5$ or $p \equiv 1, 9 \pmod{20}$.
5. $p = x^2 + 6y^2$ iff $p \equiv 1, 7 \pmod{24}$.
6. $p = x^2 + 10y^2$ iff $p \equiv 1, 9, 11, 19 \pmod{40}$.
7. $p = x^2 + 13y^2$ iff $p = 13$ or $p \equiv 1, 9, 17, 25, 29, 49 \pmod{52}$.
8. Assume $p \neq 7$. $p = x^2 + 14y^2$ iff $\left(\frac{-14}{p}\right) = 1$ and $(x^2 + 1)^2 \equiv 8 \pmod p$.
9. $p = x^2 + 15y^2$ iff $p \equiv 1, 9, 31, 49 \pmod{60}$.
10. $p = x^2 + 21y^2$ iff $p \equiv 1, 25, 37 \pmod{84}$.
11. $p = x^2 + 22y^2$ iff $p \equiv 1, 9, 15, 23, 25, 31, 47, 49, 71, 81 \pmod{88}$.
12. $p = x^2 + 27y^2$ iff $p \equiv 1 \pmod 3$ and 2 is a cubic residue mod p.
13. $p = x^2 + 30y^2$ iff $p \equiv 1, 31, 49, 79 \pmod{120}$.
14. $p = x^2 + 64y^2$ iff $p \equiv 1 \pmod 4$ and 2 is a quartic residue mod p.

ARE THERE ANY n SUCH THAT THE CONDITION IS SIMPLE BUT IS NOT ON THIS LIST.

2 General Theorem

Def 2.1 Let $n, m \in \mathbb{N}$ with $n, m \geq 1$. Let

$$f(z) = f_m z^m + \cdots + f_0$$

$$g(z) = g_n z^n + \cdots + g_0$$

The *Sylvester Matrix associated to* f, g is the $(n+m) \times (n+m)$ matrix constructed as follows

1. The first row is
   $(f_m\ f_{m-1}\ \cdots\ f_1\ f_0\ 0\ \cdots\ 0)$
   (There are zero 0's on the left and $n-1$ 0's at the right end.)
2. The second row is
   $(0\ f_m\ f_{m-1}\ \cdots\ f_1\ f_0\ \cdots\ 0)$
   (There is one 0 on the left end and $n-2$ 0's on the right end.)
3. Let $1 \leq i \leq n$. The ith row is
   $(0\ \cdots 0\ f_m\ f_{m-1}\ \cdots\ f_1\ f_0\ 0\ \cdots\ 0)$
   (There are $i-1$ 0's on the left end and $n-i$ 0's on the right end.)
4. The $n+1$st row is
   $(g_n\ g_{n-1}\ \cdots\ g_1\ g_0\ 0\ \cdots\ 0)$
   (There are zero 0's on the left and $m-1$ 0's at the right end.)
5. The $n+2$th row is
   $(0\ g_n\ g_{n-1}\ \cdots\ g_1\ g_0\ \cdots\ 0)$
   (There is one 0 on the left end and $m-2$ 0's on the right end.)
6. Let $1 \leq i \leq n$. The $n+i$th row is
   $(0\ \cdots 0\ g_n\ g_{n-1}\ \cdots\ g_1\ g_0\ 0\ \cdots\ 0)$
   (There are $i-1$ 0's on the left end and $m-i$ 0's on the right end.)

Example If $m = 4$ and $n = 3$ then the matrix is

$$\begin{pmatrix} f_4 & f_3 & f_2 & f_1 & f_0 & 0 & 0 \\ 0 & f_4 & f_3 & f_2 & f_1 & f_0 & 0 \\ 0 & 0 & f_4 & f_3 & f_2 & f_1 & f_0 \\ g_3 & g_2 & g_1 & g_0 & 0 & 0 & 0 \\ 0 & g_3 & g_2 & g_1 & g_0 & 0 & 0 \\ 0 & 0 & g_3 & g_2 & g_1 & g_0 & 0 \\ 0 & 0 & 0 & g_3 & g_2 & g_1 & g_0 \end{pmatrix}$$

Def 2.2 The *Resultant* of two polynomials f, g is the determinant of the Sylvester Matrix associated to f, g. We denote this $\mathrm{Res}(f, g)$.

Def 2.3 Let f be a polynomial of degree n. Let f_n be its lead coefficient. Let f' be the derivative of f. The *Discriminat* of f is

$$\frac{(-1)^{n(n-1)/2}}{f_n}\mathrm{Res}(f, f').$$

We denote this $\mathrm{Disc}(f)$.

Theorem 2.4 *Let $n \equiv 0, 2 \pmod 4$ be a positive squarefree integer. Then there exists an irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ such that the following happens: Let p be a prime that does not divide n and does not divide $\mathrm{Disc}(f_n)$. Then*

$p = x^2 + ny^2$ iff the following both hold.

1. $\left(\frac{-n}{p}\right) = 1$ *and*
2. $f_n(x) \equiv 0 \pmod p$.

THE ABOVE THEOREM SEEMS STRANGE SINCE THERE A CONDITION ON x. THIS DOES NOT SEEM TO LEAD TO AN ALGORITHM FOR, GIVEN PRIME p, n DETERMINE IF THERE EXISTS x, y WITH $p = x^2 + ny^2$.

THE BOOK ONLY EVER GIVES THE POLY IN THE CASE OF $n = 14$. ARE OTHER POLYS KNOWN? COMPLICATED?

Theorem 2.5 *Let $n \geq 1$. Then there exists a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ [I DO NOT KNOW WHAT THAT IS] such that the following happens: Let p be a prime that does not divide n and does not divide $\mathrm{Disc}(f_n)$. Then*

$p = x^2 + ny^2$ iff the following both hold.

1. $\left(\frac{-n}{p}\right) = 1$ *and*
2. $f_n(x) \equiv 0 \pmod{p}$.

Theorem 2.6 *Let n, m be positive integers. Then there exists a monic irreducible polynomial $f_{n,m}(x) \in \mathbb{Z}[x]$ such that the following happens: Let p be a prime that does not divide mn or and does not divide $\mathrm{Disc}(f_{n,m})$. Then the following are equivalent*

1. $p = x^2 + ny^2$ *with* $x \equiv 1 \pmod{m}$ *and* $y \equiv 0 \pmod{m}$.
2. $\left(\frac{-n}{p}\right) = 1$ *and* $f_{n,m} \equiv 0 \pmod{p}$ *has an integer solution.*