ILLINOIS JOURNAL OF MATHEMATICS
Volume 27, Number 2, Summer 1983

# SETS OF PRIMES DETERMINED BY SYSTEMS OF POLYNOMIAL CONGRUENCES

BY

J. C. LAGARIAS

## 1. Introduction

Fermat considered the problem of characterizing the set $\Sigma_Q$ of primes $p$ for which

$$Q(x, y) = ax^2 + bxy + cy^2 = \pm p \tag{1.1}$$

for some integers $x$, $y$. In a letter to Mersenne dated December 26, 1640, he asserted that the form $x^2 + y^2$ represented all primes $p \equiv 1 \pmod 4$ and no primes $p \equiv 3 \pmod 4$. In a letter to Pascal written in 1654, he asserted that for the forms $x^2 + 2y^2$, $x^2 + 3y^2$ the sets $\Sigma_Q$ consisted of all primes in certain arithmetic progressions. He conjectured the same for $x^2 + 5y^2$ (see [7, p. 3]). It is plausible that Fermat had proofs of his assertions, although he never revealed them [17, p. 104]. Some of Fermat's assertions were subsequently proved by Euler in 1761. Euler had already observed that for other forms, e.g., $x^2 + 11y^2$, there was no obvious characterization of the set $\Sigma_Q$ in terms of primes in arithmetic progressions [7, p. 3].

The problem of characterizing the sets $\Sigma_Q$ motivated many subsequent investigations. Gauss considered two binary quadratic forms $Q_1$ and $Q_2$ to be equivalent if one can be obtained from the other by a unimodular integer transformation of variables. Equivalent forms represent the same sets of primes. A form can represent infinitely many primes only if it is *primitive*, i.e., $(a, b, c) = 1$. The set of all primitive forms having the same *discriminant* $D = b^2 - 4ac$ fall into a finite set of equivalence classes, which we denote $\mathrm{Cl}(D)$. Gauss developed a theory of *genera* which restricted the values that could be represented by a given binary quadratic form to be those for which certain auxiliary quadratic congruences were solvable or unsolvable in specified ways. For example, for $D = -164 = -4.41$, there are eight classes in $\mathrm{Cl}(D)$. There are two auxiliary quadratic congruences:

$$\text{(A)} \quad x_1^2 \equiv 41 \pmod p, \tag{1.2}$$

$$\text{(B)} \quad x_2^2 \equiv -1 \pmod p. \tag{1.3}$$

Received April 20, 1982.