PACIFIC JOURNAL OF MATHEMATICS
Vol. 52, No. 1, 1974

THE SEPTIC CHARACTER OF 2, 3, 5 AND 7

PHILIP A. LEONARD AND KENNETH S. WILLIAMS

Necessary and sufficient conditions for 2, 3, 5, and 7 to be seventh powers (mod p) (**p a prime** $\equiv 1 \pmod 7$) **are determined.**

1. Introduction. Let p be a prime $\equiv 1 \pmod 3$. Gauss [5] proved that there are integers x and y such that

$$4p = x^2 + 27y^2,\ x \equiv 1 \pmod 3\ . \tag{1.1}$$

Indeed there are just two solutions $(x, \pm y)$ of (1.1). Jacobi [6] (see also [2], [9], [16]) gave necessary and sufficient conditions for all primes $q \leqq 37$ to be cubes (mod p) in terms of congruence conditions involving a solution of (1.1), which are independent of the particular solution chosen. For example he showed that 3 is a cube (mod p) if and only if $y \equiv 0 \pmod 3$. For p a prime $\equiv 1 \pmod 5$, Dickson [3] proved that the pair of diophantine equations

$$\begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2\ , \\ xw = v^2 - 4uv - u^2,\ x \equiv 1 \pmod 5\ , \end{cases} \tag{1.2}$$

has exactly four solutions. If one of these is (x, u, v, w) the other three are $(x, -u, -v, w)$, $(x, v, -u, -w)$ and $(x, -v, u, -w)$. Lehmer [7], [8], [10], [11], Muskat [14], [15], and Pepin [17] have given necessary and sufficient conditions for 2, 3, 5, and 7 to be fifth powers (mod p) in terms of congruence conditions on the solutions of (1.2) which do not depend upon the particular solution chosen. For example Lehmer [8] proved that 3 is a fifth power (mod p) if and only if $u \equiv v \equiv 0 \pmod 3$.

In this note, making use of results of Dickson [4], Muskat [14], [15] and Pepin [17], and the authors [12], [13] we obtain the analogous conditions for 2, 3, 5, and 7 to be seventh powers modulo a prime $p \equiv 1 \pmod 7$. The appropriate system to consider is the triple of diophantine equations

$$\begin{cases} 72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2)\ , \\ 12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 \\ \qquad + 48x_3x_4 + 98x_5x_6 = 0\ , \\ 12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 \\ \qquad + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0,\ x_1 \equiv 1 \pmod 7\ , \end{cases} \tag{1.3}$$

considered by the authors in [12] (see also [20]). It was shown there that (1.3) has six nontrivial solutions in addition to the two trivial