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 solutions $(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$, where t and u are given by

$$p = t^2 + 7u^2,\ t \equiv 1 \pmod 7\ . \tag{1.4}$$

If $(x_1, x_2, x_3, x_4, x_5, x_6)$ is one of the six nontrivial solutions of (1.3) the other five nontrivial solutions are

$$\begin{cases} \left(x_1, -x_3, x_4, x_2, -\frac{1}{2}(x_5 + 3x_6), \frac{1}{2}(x_5 - x_6)\right), \\ \left(x_1, -x_4, x_2, -x_3, -\frac{1}{2}(x_5 - 3x_6), -\frac{1}{2}(x_5 + x_6)\right), \\ (x_1, -x_2, -x_3, -x_4, x_5, x_6) \\ \left(x_1, x_3, -x_4, -x_2, -\frac{1}{2}(x_5 + 3x_6), \frac{1}{2}(x_5 - x_6)\right), \\ \left(x_1, x_4, -x_2, x_3, -\frac{1}{2}(x_5 - 3x_6), -\frac{1}{2}(x_5 + x_6)\right). \end{cases} \tag{1.5}$$

We prove

THEOREM. (a) *2 is a seventh power* (mod p) *if and only if* $x_1 \equiv 0 \pmod 2$.

(b) *3 is a seventh power* (mod p) *if and only if* $x_5 \equiv x_6 \equiv 0 \pmod 3$.

(c) *5 is a seventh power* (mod p) *if and only if either*

$$x_2 \equiv x_3 \equiv -x_4 \pmod 5 \quad \textit{and} \quad x_5 \equiv x_6 \equiv 0 \pmod 5$$

or

$$x_1 \equiv 0 \pmod 5 \quad \textit{and} \quad x_2 + x_3 - x_4 \equiv 0 \pmod 5\ .$$

(d) *7 is a seventh power* (mod p) *if and only if* $x_2 - 19x_3 - 18x_4 \equiv 0 \pmod{49}$.

In view of (1.5) it is clear that none of the conditions given in the theorem depends upon the particular nontrivial solution of (1.3) chosen. Moreover, in connection with (d) we remark that any solution of (1.3) satisfies $x_2 + 2x_3 + 3x_4 \equiv 0 \pmod 7$ (see [12]) so that $x_2 - 19x_3 - 18x_4 \equiv 0 \pmod 7$.

We remark that since this paper was written a paper has appeared by Helen Popova Alderson [1] giving necessary and sufficient conditions for 2 and 3 to be seventh powers (mod p). Her conditions are not as simple as (a) and (b) above.

2. *Proof of* (a). Let g be a primitive root (mod p), where p is an odd prime. Let $e > 1$ be an odd divisor of $p - 1$ and set $p -$

$1 = ef$. The cyclotomic number $(h, k)_e$ is defined to be the number of solutions s, t of the trinomial congruence

$$g^{es+h} + 1 \equiv g^{et+k} \pmod{p}\,, \quad 0 \leqq s, t \leqq f - 1\,.$$

It is well-known [8], [18] that 2 is an eth power $(\bmod\, p)$ if and only if $(0, 0)_e \equiv 1 \pmod 2$. From [4], [13] we have $49(0, 0)_7 = p - 20 - 12t + 3x_1$, so that 2 is a seventh power $(\bmod\, p)$ if and only if $x_1 \equiv 0 \pmod 2$.

Alternatively this result can be proved using a result of Pepin [17] (see also [14]) or by using the representation of x_1 in terms of a Jacobsthal sum (see [7] and [12]).

3. *Proof of* (b). The Dickson-Hurwitz sum $B_e(i, j)$ is defined by

$$B_e(i, j) = \sum_{h=0}^{e-1} (h, i - jh)_e\,.$$

In [13] it was shown that

$$(3.1) \qquad \begin{cases} 84B_7(0, 1) = 12x_1 + 12p - 24\,, \\ 84B_7(1, 1) = -2x_1 + 42x_2 + 49x_5 + 147x_6 + 12p - 24\,, \\ 84B_7(2, 1) = -2x_1 + 42x_3 + 49x_5 - 147x_6 + 12p - 24\,, \\ 84B_7(3, 1) = -2x_1 + 42x_4 - 98x_5 + 12p - 24\,, \\ 84B_7(4, 1) = -2x_1 - 42x_4 - 98x_5 + 12p - 24\,, \\ 84B_7(5, 1) = -2x_1 - 42x_3 + 49x_5 - 147x_6 + 12p - 24\,, \\ 84B_7(6, 1) = -2x_1 - 42x_2 + 49x_5 + 147x_6 + 12p - 24\,, \end{cases}$$

for some nontrivial solution $(x_1, x_2, x_3, x_4, x_5, x_6)$ of (1.3). Muskat [14], Pepin [17] have shown that 3 is a seventh power $(\bmod\, p)$ if and only if

$$B_7(1, 1) \equiv B_7(2, 1) \equiv B_7(4, 1) \pmod 3\,,$$
$$B_7(3, 1) \equiv B_7(5, 1) \equiv B_7(6, 1) \pmod 3\,.$$

This condition using (3.1) is easily shown to be equivalent to $x_5 \equiv x_6 \equiv 0 \pmod 3$. In verifying this it is necessary to observe that if $x_5 \equiv x_6 \equiv 0 \pmod 3$ then $x_1 \equiv x_5 \equiv x_6 \equiv 0 \pmod 3$, $x_2 \equiv x_3 \equiv -x_4 \pmod 3$ follow from (1.3).

4. *Proof of* (c). Muskat [14] has shown that 5 is a seventh power $(\bmod\, p)$ if and only if either

$$B_7(1, 1) \equiv B_7(2, 1) \equiv B_7(4, 1) \pmod 5$$
$$B_7(3, 1) \equiv B_7(5, 1) \equiv B_7(6, 1) \pmod 5$$

or

$$B_7(1, 1) + B_7(2, 1) + B_7(4, 1) \equiv B_7(3, 1) + B_7(5, 1) + B_7(6, 1) \equiv 0 \pmod 5 ,$$

which by (3.1) is equivalent to

$$x_2 \equiv x_3 \equiv -x_4 \pmod 5 \quad \text{and} \quad x_5 \equiv x_6 \equiv 0 \pmod 5 ,$$

or

$$x_1 \equiv 0 \pmod 5 \text{ and } x_2 + x_3 - x_4 \equiv 0 \pmod 5 .$$

5. *Proof of* (d). Muskat [15] has shown that 7 is a seventh power (mod p) if and only if

$$B_7(1, 1) - B_7(6, 1) - 19(B_7(2, 1) - B_7(5, 1)) - 18(B_7(3, 1) - B_7(4, 1)) \equiv 0 \pmod{49} ,$$

which by (3.1) is easily seen to be equivalent to

$$x_2 - 19x_3 - 18x_4 \equiv 0 \pmod{49} .$$

6. **Application of theorem to primes $p \equiv 1 \pmod 7$, $p < 1000$.** One of us (K.S.W.) has prepared a table of solutions [19] of (1.3) for all primes $p \equiv 1 \pmod 7$, $p < 1000$. For these primes the table shows that

(a) $x_1 \equiv 0 \pmod 2$ only for $p = 631, 673, 693$,
(b) $x_5 \equiv x_6 \equiv 0 \pmod 3$ only for $p = 757, 883$,
(c) (i) $x_2 \equiv x_3 \equiv -x_4 \pmod 5$ and $x_5 \equiv x_6 \equiv 0 \pmod 5$ not satisfied,
(ii) $x_1 \equiv 0 \pmod 5$ and $x_2 + x_3 - x_4 \equiv 0$ only for $p = 71, 827, 883$,
(d) $x_2 - 19x_3 - 18x_4 \equiv 0 \pmod{49}$ only for $p = 43, 281$,

so that by the theorem, for primes $p \equiv 1 \pmod 7$, $p < 1000$,

2 is a seventh power (mod p) only for $p = 631, 673, 953$,
3 is a seventh power (mod p) only for $p = 757, 883$,
5 is a seventh power (mod p) only for $p = 71, 827, 883$,
7 is a seventh power (mod p) only for $p = 43, 281$.

Indeed we can show directly that

$$2 \equiv 196^7 \pmod{631},\ 2 \equiv 128^7 \pmod{673},\ 2 \equiv 120^7 \pmod{953} ,$$
$$3 \equiv 81^7 \pmod{757},\ 3 \equiv 207^7 \pmod{883} ,$$
$$5 \equiv 58^7 \pmod{71},\ 5 \equiv 561^7 \pmod{827},\ 5 \equiv 432^7 \pmod{883} ,$$
$$7 \equiv 28^7 \pmod{43},\ 7 \equiv 264^7 \pmod{281} .$$

References

1. Helen Popova Alderson, *On the septimic character of* 2 *and* 3, Proc. Camb. Phil. Soc., **74** (1973), 421–433.

2. A.J.C. Cunningham and T. Gosset, *On 4-tic and 3-bic residuacity tables*, Messinger of Mathematics, **50** (1920), 1-30.

3. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math., **57** (1935), 391-424.

4. ———, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc., **37** (1935), 363-380.

5. K. F. Gauss, *Disquisitiones Arithmeticae*, Yale University Press, 1966, Art. 358, 440-445.

6. K. G. J. Jacobi, *De residuis cubicis commentatio numerosa*, J. für die reine und angew. Math., **2** (1827), 66-69.

7. E. Lehmer, *On the quintic character of* 2, Bull. Amer. Math. Soc., **55** (1949), 62-63.

8. ———, *The quintic character of* 2 *and* 3, Duke Math. J., **18** (1951), 11-18.

9. ———, *Criteria for cubic and quartic residuacity*, Mathematika, **5** (1958), 20-29.

10. ———, *Artiads characterized*, J. Math. Anal. Appl., **15** (1966), 118-131.

11. ———, *On the divisors of the discriminant of the period equation*, Amer. J. Math., **90** (1968), 375-379.

12. P. A. Leonard and K. S. Williams, *A diophantine system of Dickson*, to appear.

13. ———, *The cyclotomic numbers of order seven*, Proc. Amer. Math. Soc., (to appear).

14. J. B. Muskat, *Criteria for solvability of certain congruences*, Canad. J. Math., **16** (1964), 343-352.

15. ———, *On the solvability of* $x^e \equiv e \pmod p$, Pacific J. Math., **14** (1964), 257-260.

16. T. Nagell, *Sur quelques problèmes dans la théorie dans restes quadratiques et cubiques*, Arkiv för Mat., **3** (1956), 211-222.

17. T. Pepin, *Mémoire sur les lois de reciprocité relatives aux résidues de puissances*, Pontif. Accad. Sci., Rome **31** (1877), 40-148.

18. T. Storer, *Cyclotomy and Difference Sets*, Markham Publishing Co., 1967.

19. K. S. Williams, *A quadratic partition of primes* $p \equiv 1 \pmod 7$, Math. of Computation (to appear).

20. ———, *Elementary treatment of a quadratic partition of primes* $p \equiv 1 \pmod 7$, Illinois J. Math. (to appear).

Received October 2, 1973 and in revised form December 17, 1973. The research of both authors was supported by the National Research Council of Canada under Grant A-7233. The second author's sabbatical leave at the University of British Columbia was supported by N.R.C. Travel Grant T-0259.

ARIZONA STATE UNIVERSITY
AND
CARLETON UNIVERSITY