Journal of the Indian Math Soc.
39 (1975) 167–172

2 AS A NINTH POWER (MOD p)

By KENNETH S. WILLIAMS*

[Received July 10, 1974]

1. Introduction. Let p be a prime $\neq 2,3$. We consider the problem of giving a necessary and sufficient condition for 2 to be a ninth power (mod p), analogous to those known for 2 to be a k *th* power (mod p) for $k=3$ [3], $k=5$ [4], $k=7$ [5] and $k=11$ [6]. If $p \equiv 2 \pmod 3$ then 2 is always a ninth power (mod p) so we may restrict our attention to primes $p \equiv 1 \pmod 3$. For such primes, Gauss showed that there are integers L, M such that

$$4p = L^2 + 27M^2,\ L \equiv 1 \pmod 3 \tag{1.1}$$

Indeed there are just two solutions of (1.1), namely $(L, \pm M)$. Jacobi [3] proved that 2 is a cube (mod p) if and only if $L \equiv 0 \pmod 2$. Clearly 2 cannot be a ninth power (mod p) without being a cube (mod p). If 2 is a cube (mod p) and $p \not\equiv 1 \pmod 9$ then 2 will also be a ninth power (mod p). However if 2 is a cube (mod p) and $p \equiv 1 \pmod 9$ then 2 may or may not be a ninth power (mod p). In this case, using a result of Dickson [2], we prove that 2 is a ninth power (mod p) if and only if $x_1 \equiv 0 \pmod 2$, where x_1 is uniquely determined by the diophantine system

$$\left.\begin{aligned}
&8p = 2x_1^2 + 3x_2^2 + 18x_3^2 + 18x_4^2 + 27x_5^2 + 54x_6^2,\\
&x_2^2 - 9x_5^2 - 2x_1x_2 + 4x_1x_3 + 2x_1x_5 - 2x_2x_3 + 2x_2x_4\\
&\quad + 6x_2x_6 + 12x_3x_4 + 6x_3x_5 + 12x_3x_6 + 6x_4x_5 + 24x_4x_6\\
&\quad + 18x_5x_6 = 0,\\
&x_1x_2 - 2x_1x_4 + x_1x_5 + 2x_2x_3 - 2x_2x_4 - 3x_2x_6 - 6x_3x_5\\
&\quad - 12x_3x_6 - 6x_4x_5 - 6x_4x_6 + 9x_5x_6 = 0,
\end{aligned}\right\} \tag{1.2}$$

with $(x_1, x_2, x_3, x_4, x_5, x_6) \neq (L, 0, 0, 0, 0, \pm M)$ and $x_1 \equiv 1 \pmod 3$ (compare [3], [4], [5] and [6]).

---

*Research supported under a National Research Council of Canada grant (No. A—7233).

2. A Preliminary Lemma. We prove

LEMMA. *Let p be a prime $\equiv 1 \pmod 9$. Then any solution* $(x_1, x_2, x_3, x_4, x_5, x_6)$ *of* (1.2) *satisfies*

$$x_1 + x_6 \equiv x_2 + x_5 \equiv x_2 + x_3 + x_4 \equiv 0 \pmod 2 \tag{2.1}$$

and

$$x_2 + 2x_3 + 3x_5 \equiv 0 \pmod 4. \tag{2.2}$$

PROOF. Reducing the first equation in (1.2) modulo 2 we obtain

$$x_2 + x_5 \equiv 0 \pmod 2, \tag{2.3}$$

which is part of the assertion (2.1). Next we reduce the same equation modulo 4 obtaining

$$2x_1^2 + 3x_2^2 + 2x_3^2 + 2x_4^2 + 3x_5^2 + 2x_6^2 \equiv 0 \pmod 4. \tag{2.4}$$

From (2.3) we have $x_2^2 \equiv x_5^2 \pmod 4$ and using this in (2.4) we obtain

$$2(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_6^2) \equiv 0 \pmod 4,$$

that is

$$x_1 + x_2 + x_3 + x_4 + x_6 \equiv 0 \pmod 2. \tag{2.5}$$

Now reducing the second equation in (1.2) modulo 8 we get

$$x_2^2 - x_5^2 - 2x_1x_2 + 4x_1x_3 + 2x_1x_5 - 2x_2x_3 + 2x_2x_4 - 2x_2x_6 + 4x_3x_4 - 2x_3x_5 + 4x_3x_6 - 2x_4x_5 + 2x_5x_6 \equiv 0 \pmod 8. \tag{2.6}$$

By (2.3) we may define an integer t by $x_2 = x_5 + 2t$ and substituting this in (2.6) yields

$$t(x_1 + x_3 + x_4 + x_5 + x_6) + t^2 + x_3(x_1 + x_4 + x_5 + x_6) \equiv 0 \pmod 2,$$

which appealing to (2.3) and (2.5) gives
$t \equiv x_3 \pmod 2$, that is, $\frac{1}{2}(x_2 - x_5) \equiv x_3 \pmod 2$ or $x_2 + 2x_3 + 3x_5 \equiv 0 \pmod 4$, which is the assertion of (2.2). Finally reducing the third equation in (1.2) modulo 4 we get using (2.3)

$$(x_1 + x_6)(x_2 + 2x_4 + x_5) \equiv 0 \pmod 4,$$

that is

$$(x_1 + x_6)(x_3 + x_4 + x_5) \equiv (x_1 + x_6)(t + x_4 + x_5) \equiv 0 \pmod 2, \tag{2.7}$$

so that

$$x_1 + x_6 \equiv x_3 + x_4 + x_5 \equiv 0 \pmod 2,$$

follows from (2.3), (2.5) and (2.7), completing the ~~proof of the rest of~~ the assertion of (2.1).

3. A Theorem of Dickson. Our results depend upon the following result of Dickson ([2] Theorem 3, p. 193).

THEOREM 1 (DICKSON) *Let p be a prime $\equiv 1$ (mod 9). The triple of diophantine equations*

$$\left.\begin{array}{l} p = c_0^2 + c_1^2 + c_2^2 + c_3^2 + c_4^2 + c_5^2 - c_0c_3 - c_1c_4 - c_2c_5, \\ c_0c_1 + c_1c_2 + c_2c_3 + c_3c_4 + c_4c_5 - c_0c_4 - c_1c_5 - c_0c_5 = 0, \\ c_0c_2 + c_1c_3 + c_2c_4 + c_3c_5 - c_0c_4 - c_1c_5 - c_0c_5 = 0, \end{array}\right\} \quad (3.1)$$

has exactly six integral solutions $(c_0, c_1, c_2, c_3, c_4, c_5) \neq (\tfrac{1}{2}(L \pm 3M), 0, 0, \pm 3M, 0, 0)$ (*upper signs together or lower signs together*) *satisfying*

$$c_0 \equiv -1,\ c_1 \equiv c_2 \equiv -c_4 \equiv -c_5,\ c_3 \equiv 0 \pmod 3) \qquad (3.2)$$

If $(c_0, c_1, c_2, c_3, c_4, c_5)$ is one of these six solutions, the other five are given by

$$\left.\begin{array}{l} (c_0 - c_3, c_5, c_1 - c_4, -c_3, c_2, -c_4), \\ (c_0, -c_4, c_5 - c_2, c_3, c_1 - c_4, -c_2), \\ (c_0 - c_3, -c_2, -c_1, -c_3, c_5 - c_2, c_4 - c_1), \\ (c_0, c_4 - c_1, -c_5, c_3, -c_1, c_2 - c_5), \\ (c_0 - c_3, c_2 - c_5, c_4, -c_3, -c_5, c_1). \end{array}\right\} \quad (3.3)$$

Moreover, if g is a primitive root (mod p), then for some solution $(c_0, c_1, c_2, c_3, c_4, c_5) \neq (\tfrac{1}{2}(L \pm 3M), 0, 0, \pm 3M, 0, 0)$ of (3.1) and (3.2) we have

$$81(0,0)_9 = \begin{cases} p - 26 + L + 54c_0 - 27c_3, \text{ if } \operatorname{ind}_g(3) \equiv 0 \pmod 3), \\ p - 26 + L - 27c_3, \text{ if } \operatorname{ind}_g(3) \equiv 1 \pmod 3), \\ p - 26 + L + 27c, \text{ if } \operatorname{ind}_g(3) \equiv 2 \pmod 3), \end{cases} \qquad (3.4)$$

where $(h, k)_9$ denotes the cyclotomic number of order nine, that is, the number of solutions (s, t) of $g^{9s+h} + 1 \equiv g^{9t+k} \pmod p$, and $\operatorname{ind}_g(l)$ ($l \not\equiv 0 \pmod p$)) denotes the unique integer m such that $l \equiv g^m \pmod p$, $0 \leqslant m \leqslant p-2$.

Diagonalizing the first equation in (3.1) and absorbing the conditions (3.2) into the equations in (3.1) we obtain

COROLLARY. *Let p be a prime $\equiv 1$ (mod 9). The triple of diophantine equations* (1.2) *has exactly six solutions* $(x_1, x_2, x_3, x_4, x_5, x_6) \neq (L, 0, 0, 0, 0, \pm M)$ *satisfying* $x_1 \equiv 1$ (*mod* 3). *If* $(x_1, x_2, x_3, x_4, x_5, x_6)$ *is one of these solutions, the other five solutions are given by*

$$(x_1, x_2, x_3, x_4, x_5, x_6)\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -\frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & \frac{3}{2} & -\frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & -\frac{9}{4} & -\frac{3}{4} & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}^k, \tag{3.5}$$

where $k = 0, 1, 2, 3, 4, 5$, *so that* $x_1 \equiv 1 \pmod 3$ *is uniquely determined by* (1.2). *Moreover, if* g *is a primitive root* $\pmod p$, *then for some solution* $(x_1, x_2, x_3, x_4, x_5, x_6) \neq (L, 0, 0, 0, 0, \pm M)$ *of* (1.2) with $x_1 \equiv 1$ $\pmod 3$ *we have*

$$81(0, 0)_9 = \begin{cases} p - 26 + L + 27x_1, \text{ if } \operatorname{ind}_g(3) \equiv 0 \pmod 3, \\ p - 26 + L - 81x_6, \text{ if } \operatorname{ind}_g(3) \equiv 1 \pmod 3, \\ p - 26 + L + 81x_6, \text{ if } \operatorname{ind}_g(3) \equiv 2 \pmod 3, \end{cases} \tag{3.6}$$

PROOF. For any solution $(c_0, c_1, c_2, c_3, c_4, c_5)$ of (3.1) and (3.2) we obtain a solution $(x_1, x_2, x_3, x_4, x_5, x_6)$ of (1.2) by setting

$$\left.\begin{aligned} x_1 &= 2c_0 - c_3, \\ x_2 &= c_4 + c_5, \\ 3x_3 &= 2c_1 - c_4, \\ 3x_4 &= 2c_2 - c_5, \\ 3x_5 &= c_4 - c_5, \\ 3x_6 &= c_3, \end{aligned}\right\} \tag{3.7}$$

with $x_1 \equiv 1 \pmod 3$. Conversely if $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a solution of (1.2) with $x_1 \equiv 1 \pmod 3$ then, by the Lemma, we may define a solution $(c_0, c_1, c_2, c_3, c_4, c_5)$ of (3.1) by setting

$$\left.\begin{aligned} 2c_0 &= x_1 + 3x_6, \\ 4c_1 &= x_2 + 6x_3 + 3x_5, \\ 4c_2 &= x_2 + 6x_4 - 3x_5, \\ c_3 &= 3x_6, \\ 2c_4 &= x_2 + 3x_5, \\ 2c_5 &= x_2 - 3x_5, \end{aligned}\right\} \tag{3.8}$$

which satisfies (3.2). Clearly the excluded solutions $(\frac{1}{2}(L \pm 3M), 0, 0, \pm 3M, 0, 0)$ and $(L, 0, 0, 0, 0, \pm M)$, (3.3) and (3.5), (3.4) and (3.6), correspond under the transformations (3.7) and (3.8). This completes the proof of the corollary.

4. Necessary and sufficient condition for 2 to be A Ninth power (mod p). We are now in a position to prove the main result of this paper.

THEOREM 2. *Let p be a prime* $\equiv 1 \pmod 9$ *for which* 2 *is a cube* $(\text{mod } p)$. *Let* $x_1 \equiv 1 \pmod 3$ *be the unique integer determined by the system* (1.2) (*see corollary*). *Then* 2 *is a ninth power* $(\text{mod } p)$ *if and only if* $x_1 \equiv 0 \pmod 2$.

PROOF. Using a well-known result (see for example [4] or [7]) 2 is a ninth power $(\text{mod } p)$ if and only if $(0, 0)_9 \equiv 1 \pmod 2$, that is, by the corollary if and only if $x_1 \equiv 0 \pmod 2$, since $L \equiv 0 \pmod 2$ as 2 is a cube $(\text{mod } p)$.

5. Numerical Examples. The only primes $p < 1000$, $p \equiv 1 \pmod 9$, for which 2 is a cube $(\text{mod } p)$ are

$$p = 109, 127, 307, 397, 433, 739, 811, 919. \tag{5.1}$$

Mr. Barry Lowe, using Carleton University's Sigma-9 computer, found solutions of (1.2) for these values of p as follows:

p	x_1	x_2	x_3	x_4	x_5	x_6
109	−5	10	4	2	2	−1
127	4	−8	−2	2	—	−2
307	7	24	−2	2	4	−1
397	−14	2	4	6	−6	4
433	−23	4	−2	2	8	3
739	−5	4	−4	16	−4	3
811	−41	16	10	2	−4	1
919	−11	0	−10	−14	−4	5

Thus, by Theorem 2, of these primes only $p = 127$ and 397 have 2 as a ninth power $(\text{mod } p)$. Indeed it is easy to check directly that

$$2 \equiv 84^9 \pmod{127}, \quad 2 \equiv 32^9 \pmod{397}.$$

We close by remarking that elsewhere [8] the author has obtained a similar necessary and sufficient condition for 3 to be a ninth power $(\text{mod } p)$.

References

1. L.D. Baumert and H. Fredricksen, The cyclotomic numbers of order eighteen with applications to difference sets. *Math. Comp.* 21 (1967), 204–219.
2. L.E. Dickson, Cyclotomy when *e* is composite, *Trans. Amer. Math. Soc.*, 38 (1935), 187–200.
3. K.G.J. Jacobi, De residuis cubicis commentatio numerosa, *J. für die reine und angew. Math.*, 2 (1827), 66–69.
4. Emma Lehmer, The quintic character of 2 and 3, *Duke Math. J.* 18 (1951), 11–18.
5. P.A. Leonard and K.S. Williams, The septic character of 2, 3, 5, and 7, *Pacific J. Math.* 52 (1974) 143–147.
6. P.A. Leonard, B.C. Mortimer and K.S. Williams, The eleventh power character of 2, *to appear in Jour. für reine und angew Math.*
7. T. Storer, *Cyclotomy and difference sets*, Markham Publishing Co. (Chicago).
8. K.S. Williams, 3 as a ninth power, *Math. Scand* 35 (1974), 309–317.

Carleton University
Ottawa, Ontario, Canada