MATH. SCAND. 35 (1974), 309–317

3 AS A NINTH POWER (MOD p)

KENNETH S. WILLIAMS*

1. Introduction.

Let p be a prime $\neq 3$. If $p\equiv 2 \pmod 3$ then 3 is always a ninth power $\pmod p$ 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

$$(1.1)\qquad 4p = L^2+27M^2,\quad L\equiv 1 \pmod 3\,.$$

Indeed there are just two solutions of (1.1), namely $(L, \pm M)$. Jacobi proved that 3 is a cube $\pmod p$ if and only if $M\equiv 0 \pmod 3$. As 3 cannot be a ninth power $\pmod p$ without being a cube $\pmod p$ we assume from now on that $M\equiv 0 \pmod 3$, say $M=3N$. If $p\not\equiv 1 \pmod 9$, as it is a cube $\pmod p$, 3 will also be a ninth power $\pmod p$, so we need only consider primes $p\equiv 1 \pmod 9$, in which case, 3 may or may not be a ninth power $\pmod p$. It is the purpose of this note to give a simple necessary and sufficient condition for 3 to be a ninth power $\pmod p$ in this case. This condition takes the form of a simple linear congruence (mod 3) in the variables of a certain triple of diophantine equations (see (3.5)–(3.7)). This theorem is proved using a new expression for the index of 3 modulo 9 in terms of the cyclotomic numbers of order 9 (see Lemma 6) and certain classical results concerning these cyclotomic numbers proved by Dickson in [2].

2. Preliminary results.

From this point on we emphasize that p is assumed (unless otherwise stated) to be a prime $\equiv 1 \pmod 9$ such that 3 is a cube $\pmod p$, so that $M\equiv 0 \pmod 3$, say $M=3N$, and $L\equiv 7 \pmod 9$. First of all we wish to fix the sign of N. Let g be a fixed (once and for all) primitive root $\pmod p$ and for any integer $n\not\equiv 0 \pmod p$ we define $\operatorname{ind}(n)\equiv\operatorname{ind}_g(n)$ to be the least non-negative integer l such that

$$n \equiv g^l \pmod p\,.$$

* Research supported by the National Research Council of Canada under grant no. A-7233.

Received February 20, 1974.

We set $\beta = \exp(2\pi i/9)$, so that

$$\beta^6+\beta^3+1 = 0\,,$$

and define a primitive 9th order character χ by

$$\chi(n) = \beta^{\operatorname{ind}(n)}, \quad n \not\equiv 0 \pmod{p}\,.$$

For completeness we set $\chi(n)=0$, if $n\equiv 0 \pmod{p}$. For any integers r and s the Jacobi sum $J(r,s)$ is defined by

$$J(r,s) = \sum_{n=0}^{p-1} \chi^r(n)\chi^s(1-n)\,.$$

If Q denotes the field of rational numbers, $J(r,s)$ is clearly an integer of the sextic field $Q(\beta)$. As $J(3,3)$ is invariant under the transformation $\beta \to \beta^4$, it is an element of $Q(\beta^3)=Q(\sqrt{-3})$ $(\subset Q(\beta))$, and Dickson [2, equation (6)] has noted that we may fix the sign of N by

$$J(3,3) = \tfrac{1}{2}(L+9N\sqrt{-3})\,. \tag{2.1}$$

Also following Dickson [2, equation (14)] we define integers

$$c_0, c_1, c_2, c_3, c_4, c_5$$

by

$$J(1,1) = \sum_{i=0}^{5} c_i \beta^i\,. \tag{2.2}$$

Dickson [2, equation (25)] showed that (for *any* prime $p\equiv 1 \pmod{9}$)

$$c_0 \equiv -1, \quad c_1 \equiv c_2 \equiv -c_4 \equiv -c_5, \quad c_3 \equiv 0 \pmod{3}\,. \tag{2.3}$$

In view of our additional assumption that $M\equiv 0 \pmod{3}$ we are able to prove more, namely,

LEMMA 1. $c_1\equiv c_2\equiv c_3\equiv c_4\equiv c_5\equiv 0 \pmod{3}$.

PROOF. We use the notation $(h,k)_9$ for a cyclotomic number of order 9, that is, the number of solutions x,y of the congruence

$$g^{9x+h}+1\equiv g^{9y+k} \pmod{p}$$

with $0\leqq x,y<\frac{1}{9}(p-1)$, and the notation $(h,k)_3$ for a cyclotomic number of order 3, that is, the number of solutions x,y of the congruence

$$g^{3x+h}+1 \equiv g^{3y+k} \pmod{p}$$

with $0\leqq x,y<\frac{1}{3}(p-1)$. These numbers are related by the equation

$$(h,k)_3 = \sum_{r,s=0}^{2} (h+3r,k+3s)_9\,, \tag{2.4}$$

(see Dickson [2, equation (2)]. Gauss showed that for any prime $p\equiv 1$ (mod 3)

$$\begin{aligned} &9(0,0)_3 = p-8+L, \quad 18(0,1)_3 = 2p-4-L+9M\,, \\ (2.5)\quad &9(1,2)_3 = p+1+L, \quad 18(0,2)_3 = 2p-4-L-9M\,, \\ &(1,0)_3 = (0,1)_3 = (2,2)_3,\ (1,1)_3 = (2,0)_3 = (0,2)_3,\ (2,1)_3 = (1,2)_3\,, \end{aligned}$$

and Dickson [2] evaluated the $(h,k)_9$ implicitly in terms of L, $M, c_0, \ldots, c_5$. The explicit expressions for the $(h,k)_9$ have been given by Baumert and Fredricksen [1, Tables 1 and 2]. From Dickson's work [2, p. 189] we have modulo 3

$$\begin{aligned} c_1 &= (0,1)_9+(0,4)_9-2(0,7)_9+2(1,3)_9-4(1,6)_9+2(2,5)_9 \\ &\equiv (0,1)_9+(0,4)_9+(0,7)_9+2(1,3)_9+2(1,6)_9+2(2,5)_9 \\ &= (0,1)_9+(0,4)_9+(0,7)_9+(3,1)_9+(3,4)_9+(3,7)_9+ \\ &\quad +(6,1)_9+(6,4)_9+(6,7)_9 = (0,1)_3\,, \end{aligned}$$

by (2.4), so that by (2.5), as $M \equiv 0 \pmod 3$, we have

$$(2.6)\qquad 18c_1 \equiv 2p-4-L \pmod{27}\,.$$

As $p \equiv 1 \pmod 9$, $L \equiv 7 \pmod 9$, we can define integers u and v by $p = 9u+1$, $L = 9v+7$, so that (2.6) becomes

$$(2.7)\qquad c_1 \equiv u+v+1 \pmod 3\,.$$

Finally as $M \equiv 0 \pmod 3$ we have (see [1, Table 2])

$$81(3,6)_9 = p+1+L\,,$$

so that

$$(2.8)\qquad u+v+1 \equiv 0 \pmod 9\,.$$

(2.7) and (2.8) show that $c_1 \equiv 0 \pmod 3$. This completes the proof of the lemma in view of (2.3).

Lemma 1 enables us to define integers $d_0, d_1, d_2, d_3, d_4, d_5$ by

$$(2.9)\qquad c_0 = d_0,\ c_1 = 3d_1,\ c_2 = 3d_2,\ c_3 = 3d_3,\ c_4 = 3d_4,\ c_5 = 3d_5\,,$$

with (by (2.3))

$$(2.10)\qquad d_0 \equiv -1 \pmod 3\,.$$

We next relate N to the d_i modulo 3 by proving

LEMMA 2. $N \equiv d_3 \pmod 3$.

PROOF. From [1, Table 2] we have

$$162(2,5)_9 = 2p+2-L+27N+6d_0+18d_1+18d_2-36d_3-36d_4-36d_5$$

and

$$162(2,6)_9 = 2p+2-L-27N+6d_0+18d_1+18d_2+18d_3-36d_4-36d_5$$

so that

$$54N = 54d_3+162\{(2,5)_9-(2,6)_9\} ,$$

that is

$$N \equiv d_3 \pmod 3) .$$

3. The diophantine system.

Using Lemma 1 and Dickson's Theorem 3 in [2] we obtain

LEMMA 3. *The triple of diophantine equations*

$$p = w_0^2+9(w_1^2+w_2^2+w_3^2+w_4^2+w_5^2)-3w_0w_3-9w_1w_4-9w_2w_5 , \tag{3.1}$$

$$w_0w_1+3w_1w_2+3w_2w_3+3w_3w_4+3w_4w_5-w_0w_4-3w_1w_5-w_0w_5 = 0, \tag{3.2}$$

$$w_0w_2+3w_1w_3+3w_2w_4+3w_3w_5-w_0w_4-3w_1w_5-w_0w_5 = 0 , \tag{3.3}$$

has exactly six solutions

$$(w_0,w_1,w_2,w_3,w_4,w_5) \neq (\tfrac{1}{2}(L\pm 9N),0,0,\pm 3N,0,0)$$

satisfying $w_0 \equiv -1$ (mod 3). *If* $(w_0,w_1,w_2,w_3,w_4,w_5)$ *is one of these six solutions the other five are given by*

$$\left\{\begin{array}{l}(w_0-3w_3,w_5,w_1-w_4,-w_3,w_2,-w_4) ,\\ (w_0,-w_4,w_5-w_2,w_3,w_1-w_4,-w_2) ,\\ (w_0-3w_3,-w_2,-w_1,-w_3,w_5-w_2,w_4-w_1) ,\\ (w_0,w_4-w_1,-w_5,w_3,-w_1,w_2-w_5) ,\\ (w_0-3w_3,w_2-w_5,w_4,-w_3,-w_5,w_1) .\end{array}\right. \tag{3.4}$$

Moreover $(d_0,d_1,d_2,d_3,d_4,d_5)$ *is one of these six solutions.*

Diagonalizing equation (3.1) by an appropriate linear transformation we obtain the following diophantine system in terms of which the necessary and sufficient condition for 3 to be a ninth power (mod p) will be given, namely

$$8p = 2x_1^2+18x_2^2+18x_3^2+27x_4^2+27x_5^2+54x_6^2 , \tag{3.5}$$

$$9x_4^2-9x_5^2+4x_1x_3-6x_1x_4+2x_1x_5+12x_2x_3+6x_2x_4+6x_2x_5+ \\ +24x_2x_6-6x_3x_4+6x_3x_5+12x_3x_6+18x_4x_6+18x_5x_6 = 0 , \tag{3.6}$$

$$(3.7)\quad 2x_1x_2-3x_1x_4-x_1x_5+6x_2x_4+6x_2x_5+6x_2x_6-6x_3x_4+6x_3x_5+ \\ +12x_3x_6+9x_4x_6-9x_5x_6 = 0\ .$$

Before giving the transformation between the system (3.1)–(3.3) and the system (3.5)–(3.7) we prove some simple congruences for the solutions of the system (3.5)–(3.7) which we will need in order to show that the transformation is a bijection.

LEMMA 4. *Any solution* $(x_1,x_2,x_3,x_4,x_5,x_6)$ *of* (3.5)–(3.7) *satisfies*

$$x_1+x_6 \equiv x_4+x_5 \equiv x_2+x_3+x_5 \equiv 0 \pmod 2\ ,$$

$$2x_3+x_4+x_5 \equiv 0 \pmod 4\ .$$

PROOF. Reducing (3.5) modulo 2 we obtain

$$x_4+x_5 \equiv 0 \pmod 2\ .$$

Thus we may define an integer t by

$$(3.8)\qquad x_4 = x_5+2t\ .$$

Reducing (3.5) modulo 4 we obtain

$$(3.9)\qquad 0 \equiv 2x_1^2+2x_2^2+2x_3^2+3x_4^2+3x_5^2+2x_6^2 \pmod 4\ .$$

From (3.8) we have $x_4^2 \equiv x_5^2 \pmod 4$. Using this in (3.9) gives

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

that is

$$(3.10)\qquad x_1+x_2+x_3+x_4+x_6 \equiv 0 \pmod 2\ .$$

Next taking (3.6) modulo 8 we obtain

$$(3.11)\quad x_4^2-x_5^2+4x_1x_3+2x_1x_4+2x_1x_5+4x_2x_3-2x_2x_4-2x_2x_5+ \\ +2x_3x_4-2x_3x_5+4x_3x_6+2x_4x_6+2x_5x_6 \equiv 0 \pmod 8\ .$$

Using (3.8) in (3.11) we obtain

$$t(x_1+x_2+x_3+x_5+x_6)+t^2+(x_1+x_2+x_6)(x_3+x_5) \equiv 0 \pmod 2\ ,$$

which in view of (3.10) gives

$$(3.12)\qquad t \equiv x_3+x_5 \pmod 2$$

that is

$$(3.13)\qquad \tfrac{1}{2}(x_4-x_5) \equiv x_3+x_5 \pmod 2,\qquad 2x_3+x_4+x_5 \equiv 0 \pmod 4\ .$$

Finally reducing (3.7) modulo 4 we obtain, using $x_4 \equiv x_5 \pmod 2$,

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

that is, by (3.13),

$$(x_1+x_6)(x_2+x_3+x_5) \equiv 0 \pmod 2) . \tag{3.14}$$

By (3.10) and (3.14) we have

$$x_1+x_6 \equiv x_2+x_3+x_5 \equiv 0 \pmod 2) .$$

We are now in a position to relate the two systems (3.1)–(3.3) and (3.5)–(3.7). We prove

Lemma 5. *The diophantine system* (3.5)–(3.7) *has exactly six solutions*

$$(x_1,x_2,x_3,x_4,x_5,x_6) \neq (L,0,0,0,0,\pm 3N)$$

with $x_1 \equiv 1 \pmod 3$. *If one of these is* $(x_1,x_2,x_3,x_4,x_5,x_6)$ *the other five are*

$$\begin{aligned}
&\left(x_1, x_3, \tfrac{1}{4}(-2x_2+3x_4-3x_5), \tfrac{1}{4}(2x_2-x_4-3x_5), \tfrac{1}{4}(2x_2+3x_4+x_5), -x_6\right) ,\\
&\left(x_1, \tfrac{1}{4}(-2x_2+3x_4-3x_5), -\tfrac{1}{4}(2x_3+3x_4+3x_5) ,\right.\\
&\qquad\qquad\qquad \left.\tfrac{1}{2}(-x_2+x_3-x_4), \tfrac{1}{2}(x_2+x_3-x_5), x_6\right) ,\\
&\left(x_1, -\tfrac{1}{4}(2x_3+3x_4+3x_5), -\tfrac{1}{4}(2x_2+3x_4-3x_5) ,\right.\\
&\qquad\qquad\qquad \left.-\tfrac{1}{2}(x_2+x_3-x_4), -\tfrac{1}{2}(x_2-x_3+x_5), -x_6\right) ,\\
&\left(x_1, -\tfrac{1}{4}(2x_2+3x_4-3x_5), \tfrac{1}{4}(-2x_3+3x_4+3x_5) ,\right.\\
&\qquad\qquad\qquad \left.\tfrac{1}{2}(x_2-x_3-x_4), -\tfrac{1}{2}(x_2+x_3+x_5), x_6\right) ,\\
&\left(x_1, \tfrac{1}{4}(-2x_3+3x_4+3x_5), x_2, \tfrac{1}{4}(2x_3-x_4+3x_5) ,\right.\\
&\qquad\qquad\qquad \left.-\tfrac{1}{4}(2x_3+3x_4-x_5), -x_6\right) .
\end{aligned} \tag{3.15}$$

Proof. For any solution $(w_0,w_1,w_2,w_3,w_4,w_5)$ with $w_0 \equiv -1 \pmod 3$ of (3.1)–(3.3) we obtain a solution $(x_1,x_2,x_3,x_4,x_5,x_6)$ of (3.5)–(3.7) by setting

$$\begin{cases} x_1 = 2w_0-3w_3, & x_2 = 2w_2-w_5, \quad x_3 = 2w_1-w_4 ,\\ x_4 = w_4+w_5, & x_5 = w_4-w_5, \quad x_6 = w_3 , \end{cases} \tag{3.16}$$

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 (3.5)–(3.7) with $x_1 \equiv 1 \pmod 3$ we may define, by Lemma 4, a solution $(w_0,w_1,w_2,w_3,w_4,w_5)$ of (3.5)–(3.7) by setting

$$(3.17)\qquad \begin{cases} 2w_0 = x_1+3x_6, \quad 4w_1 = 2x_3+x_4+x_5\,, \\ 4w_2 = 2x_2+x_4-x_5, \quad w_3 = x_6\,, \\ 2w_4 = x_4+x_5, \quad 2w_5 = x_4-x_5\,, \end{cases}$$

which satisfies

$$w_0 \equiv -1 \pmod 3)\,.$$

Finally it is easy to check that the excluded solutions correspond to one another and that (3.4) gives rise to (3.15).

For example when $p=73$ the six solutions of (3.5)–(3.7), with $x_1 \equiv 1 \pmod 3$, different from $(7,0,0,0,0,\pm 3)$, are

$$(-2,-2,2,2,2,2), \quad (-2,2,1,-3,1,-2), \quad (-2,1,-4,1,-1,2)$$
$$(-2,-4,1,1,1,-2), \quad (-2,1,2,-3,-1,2), \quad (-2,2,-2,2,-2,-2)\,.$$

4. Index of 3 modulo 9.

In this section we assume only that $p \equiv 1 \pmod 9$. The cyclotomic polynomial of degree $\varphi(9)=6$ modulo p is

$$f(x) = \prod_{\substack{v=1\\(v,3)=1}}^{9} (x-g^{vf})\,,$$

where $f=\frac{1}{9}(p-1)$ is even. It is well-known that $F(1)\equiv 3 \pmod p$ so that

$$(4.1)\qquad 3 \equiv \prod_{\substack{v=1\\(v,3)=1}}^{9} (1-g^{vf}) \pmod p\,.$$

The congruence

$$x^f - g^{vf} \equiv 0 \pmod p$$

has the f roots $x \equiv g^{9i+v} \pmod p$ $(1 \leqq i \leqq f)$ so that

$$(4.2)\qquad x^f - g^{vf} \equiv \prod_{i=1}^{f} (x-g^{9i+v}) \pmod p\,.$$

Taking $x=+1$ in (4.2) we obtain

$$(4.3)\qquad 1-g^{vf} \equiv \prod_{i=1}^{f} (1-g^{9i+v}) \pmod p\,.$$

Putting (4.1) and (4.3) together we obtain

$$3 \equiv \prod_{\substack{v=1\\(v,3)=1}}^{9} \prod_{i=1}^{f} (1-g^{9i+v}) \pmod p$$

so that

$$(4.4)\qquad \operatorname{ind}(3) \equiv \sum_{\substack{v=1\\(v,3)=1}}^{9} \sum_{i=1}^{f} \operatorname{ind}(1-g^{9i+v}) \pmod 9\,.$$

Collecting together terms in (4.4) for which

$$1-g^{9i+v} \equiv -g^{9j+w} \pmod p$$

we obtain, as $\operatorname{ind}(-1)=9f/2\equiv 0 \pmod 9$ (recall f even), LEMMA 6.

$$\operatorname{ind}(3) \equiv \sum_{\substack{v=1\\(v,3)=1}}^{9} \sum_{w=0}^{8} w(w,v)_9 \pmod 9 .$$

We remark that the right-hand side of the expression in Lemma 6 can be further simplified but this is unnecessary for our purposes.

5. Statement and proof of main result.

We prove

THEOREM. *Let p be a prime* $\equiv 1 \pmod 9$ *such that* 3 *is a cube* $(\operatorname{mod} p)$. *Then* 3 *is a ninth power* $(\operatorname{mod} p)$ *if and only if*

$$x_2 - x_3 + x_6 \equiv 0 \pmod 3 , \tag{5.1}$$

where $(x_1, x_2, x_3, x_4, x_5, x_6) \neq (L, 0, 0, 0, 0, \pm 3N)$ *is a solution with* $x_1 \equiv 1 \pmod 3$ *of* (3.5)–(3.7).

Note that in view of (3.15) condition (5.1) does not depend upon which of the six solutions of (3.5)–(3.7) is chosen.

PROOF. By Lemma 6, 3 is a ninth power $(\operatorname{mod} p)$ if and only if

$$\sum_{\substack{v=1\\(v,3)=1}}^{9} \sum_{w=0}^{8} w(w,v)_9 \equiv 0 \pmod 9 .$$

Using Dickson's formulae for the cyclotomic numbers of order nine, when $\operatorname{ind} 3 \equiv 0 \pmod 3$, see Baumert and Fredricksen [1] (Tables 1 and 2), this condition becomes

$$d_1 - d_2 + d_4 - d_5 + N \equiv 0 \pmod 3 .$$

Appealing to Lemma 2, Lemma 3 and (3.17) this simplifies to

$$x_2 - x_3 + x_6 \equiv 0 \pmod 3 .$$

6. Application of theorem to primes $p<1000$.

From tables for the values of L, M in the representation $4p = L^2 + 27M^2$ we see that the only primes $p \equiv 1 \pmod 9$, $p < 1000$, for which 3 is a cube $(\operatorname{mod} p)$ are

$$p = 73, 307, 523, 577, 613, 757, 919, 991 .$$

For these primes Mr. Barry Lowe used Carleton University's $\Sigma 9$ computer to calculate a non-trivial solution of the diophantine system (3.5)–(3.7). The results are listed in table 1.

Table 1

p	x_1	x_2	x_3	x_4	x_5	x_6	$x_2 - x_3 + x_6 \pmod 3$
73	-2	-2	2	2	2	2	$+1$
307	7	2	-2	8	4	-1	0
523	-20	4	-7	1	-7	4	0
577	-20	8	10	-4	4	0	$+1$
613	-2	-2	-1	-11	-7	2	$+1$
757	16	-8	-7	9	-7	0	-1
919	-11	-14	-10	0	-4	5	$+1$
991	-20	6	9	-7	-3	8	-1

Thus, by the theorem, of these primes, only $p = 307$ and 523 have 3 as a ninth power $\pmod p$. Indeed it is easy to check directly that

$$3 \equiv 298^9 \pmod{307}, \quad 3 \equiv 65^9 \pmod{523}.$$

7. Conclusion.

Baumert and Fredricksen [1] (equation (3.6)) have noted that for primes $p \equiv 1 \pmod 9$

$$\text{ind}(3) \equiv -M \pmod 3, \tag{7.1}$$

and it would be straight-forward to extend the ideas of this paper to obtain a corresponding congruence for ind(3) (mod 9).

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.

CARLETON UNIVERSITY
OTTAWA, ONTARIO
CANADA