MATH. SCAND. 60 (1987), 148-150

A REMARK ON THE CRITERIA FOR 3 TO BE A NINTH POWER (MOD p)

KEN-ICHI SATO

1. Introduction.

For a prime $p \equiv 1 \pmod 3$, it is well-known that 3 is a cube $\pmod p$ if and only if $M \equiv 0 \pmod 3$, where M is one of the exactly two solutions $(L, \pm M)$ of

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

In [2], K. S. Williams proved the following

Theorem 1. *If* $p \equiv 1 \pmod 9$ *is a prime such that* 3 *is a cube* $\pmod p$, 3 *is a ninth power* $\pmod p$ *if and only if* $x_2 - x_3 + x_6 \equiv 0 \pmod 3$, *where* $(x_1, x_2, x_3, x_4, x_5, x_6) \neq (L, 0, 0, 0, 0, \pm M)$ *is one of the exactly six-type integral solutions with* $x_1 \equiv 1 \pmod 3$ *of the diophantine system of quadratic equations*

$$8p = 2x_1^2 + 18x_2^2 + 18x_3^2 + 27x_4^2 + 27x_5^2 + 54x_6^2, \tag{1.1}$$

$$\begin{aligned} 9x_4^2 - 9x_5^2 + 4x_1x_3 - 6x_1x_4 + 2x_1x_5 + 12x_2x_3 + 6x_2x_4 + 6x_2x_5 + \\ + 24x_2x_6 - 6x_3x_4 + 6x_3x_5 + 12x_3x_6 + 18x_4x_6 + 18x_5x_6 = 0, \end{aligned} \tag{1.2}$$

$$\begin{aligned} 2x_1x_2 - 3x_1x_4 - x_1x_5 + 6x_2x_4 + 6x_2x_5 + 6x_2x_6 - 6x_3x_4 + 6x_3x_5 + \\ + 12x_3x_6 + 9x_4x_6 - 9x_5x_6 = 0. \end{aligned} \tag{1.3}$$

In this note, we give another four criterions which 3 is a ninth power $(\mathrm{mod}\, p)$. We note if $p \not\equiv 1 \pmod 9$, 3 is always a ninth power $(\mathrm{mod}\, p)$ (used Euler's criterion).

2. The main result.

Lemma 1. $x_1 \equiv -2 \pmod 9$.

Received June 24, 1985; in revised form September 3, 1985.

PROOF. By reducing (1.1) (mod 9) and $x_1 \equiv 1 \pmod 3$, we get $x_1 \equiv -2 \pmod 9$.

Now let g be a fixed primitive root of p. Let $p-1 = 9f$. Then

$$x^2+x+1 \equiv (x-g^{3f})(x-g^{6f}) \pmod p.$$

Taking $x = 1$ in the above equation we obtain

$$3 \equiv (1-g^{3f})(1-g^{6f}) \pmod p. \tag{2.1}$$

By the same method used in [2] we obtain

$$\operatorname{ind}_g 3 \equiv \sum_{w=1}^{8} w\{(w,3)_9+(w,6)_9\} \equiv \tag{2.2}$$

$$\equiv 1-N+d_0+d_3 \pmod 9, \quad \text{where } M = 3N.$$

THEOREM 2. *3 is a ninth power* (mod p) *if and only if* $N \equiv 2x_6 \pmod 9$ *or* $N \equiv -2x_6 \pmod 9$.

PROOF. 3 is a ninth power (mod p) if and only if

$$2\operatorname{ind}_g 3 \equiv 2-2N+2d_0+2d_3 \equiv 0 \pmod 9. \tag{2.3}$$

By (3.4) in [2] we know that $d_0 = w_0$, $d_3 = w_3$ or $d_0 = w_0-3w_3$, $d_3 = -w_3$. Substituting $d_0 = w_0$, $d_3 = w_3$ in (2.3) and $2w_0 = x_1+3x_6$, $w_3 = x_6$ (see (3.17) in [2]),

$$1+5x_1-2x_6 \equiv N \pmod 9.$$

Since $x_1 \equiv -2 \pmod 9$, we obtain $N \equiv -2x_6 \pmod 9$.

Next substituting $d_0 = w_0-3w_3$, $d_3 = -w_3$, similarly we obtain

$$N \equiv 2x_6 \pmod 9.$$

This proves Theorem 2.

By using the following Lemma 2, we get three criterions which are a slight modification of Williams's criterion.

LEMMA 2. $$x_2+x_3 \equiv 0 \pmod 3.$$

PROOF. Reducing (1.3) and (3.2), (3.3) in [2] (mod 3) and $w_0 \equiv -1 \pmod 3$ we get

$$w_1 \equiv w_2 \pmod 3. \tag{2.4}$$

Reducing (1.3) mod 3 we obtain $x_5 \equiv 2x_2 \pmod 3$ and substituting (3.17) of [2] in (2.4), it holds

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

Here it is obvious that $x_2 + x_3 \equiv 0 \pmod 3$ does not depend on the choice of the solutions of (1.1)–(1.3). This completes the proof of Lemma 2. Therefore as the criterion which 3 to be a ninth power $\pmod p$, instead of Williams's criterion; $x_2 - x_3 + x_6 \equiv 0 \pmod 3$, we can take any one of $x_2 \equiv x_6 \pmod 3$, $x_3 + x_6 \equiv 0 \pmod 3$, or $x_5 + x_6 \equiv 0 \pmod 3$.

REFERENCES

1. L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp. 21 (1976), 204–219.
2. K. S. Williams, *3 as a ninth power* $\pmod p$, Math. Scand. 35 (1974), 309–317.

COLLEGE OF ENGINEERING
NIHON UNIVERSITY
KORIYAMA, FUKUSHIMA-KEN
JAPAN