ACTA ARITHMETICA
XXXVII (1980)

On the difference of cubes (mod p)

by

S. Chowla (Princeton, N. J.), M. Cowles and
J. Cowles (Charlottesville, Va.)

Dedicated to the memory of Paul Turán

For a prime $p \equiv 1 \pmod 3$, let N_c symbolize the number of solutions of

$$x^3 - y^3 \equiv c \pmod p. \tag{1}$$

In 1830 or thereabouts, G. Libri showed by use of Gauss's derivation [2] of the cubic equation of periods that

$$N_1 = p \pm a - 2, \tag{2}$$

where $4p = a^2 + 27b^2$. By 1837 V. A. Lebesgue discovered that the proper sign in (2) is uniquely determined by

$$4p = a^2 + 27b^2 \quad \text{and} \quad a \equiv 1 \pmod 3. \tag{3}$$

A modern exposition of this work of Libri and Lebesgue can be found in the last chapter of [1]. Lebesgue also gave a formula for N_c for any c but it contained an ambiguity of sign. T. Stieltjes, in an 1883 paper on cubic and biquadratic residues using methods derived from Gauss's first memoir on biquadratic residues found results which can be used to remove the ambiguity. A modern discussion of Stieltjes' work can be found in [3]. Formulae for the number of solutions of $a_1 x_1^k + \ldots + a_s x_s^k \equiv 0 \pmod p$ in terms of Gaussian sums have been studied by numerous authors including L. Dickson, G. Hardy, J. Littlewood, H. Vandiver and L. Hua, A. Weil, S. Chowla and G. Shimura. The Gaussian sums involved are linear combinations of the sums $\tau(\chi) = \sum_{n=1}^{p} \chi(n) \exp(2\pi i/p)$ where χ is a character $(\bmod p)$. It is known that $|\tau(\chi)| = \sqrt{p}$ but it appears that additional information on $\tau(\chi)$ is necessary to make, for example, the proper choice of sign in (2).

For a prime $p \equiv 1 \pmod 3$, let G be the multiplicative group of non-zero residues (mod p) and let H be the subgroup of non-zero cubic residues (mod p). Let M_c symbolize the number of solutions of

$$x^3+y^3+cz^3 \equiv 0 \pmod{p}. \tag{4}$$

Of course M_c and N_c are closely related.

Proposition. *For a prime $p \equiv 1 \pmod 3$ and $c \in G$, $M_c = (p-1)N_c+ +3p-2$.*

Proof. When $y = 0 = z$, (4) has only one solution. Since $p \equiv 1 \pmod 3$, for $z = 0$ and for each $y \in G$, (4) has three solutions. Since there are $p-1$ choices for y, this case gives a total of $3(p-1)$ solutions. For $z \in G$, (4) can be written as $\left(\frac{x}{z}\right)^3 - \left(\frac{y}{z}\right)^3 \equiv c \pmod{p}$. Then each solution of $u^3-v^3 \equiv c \pmod{p}$ determines a solution of (4) by letting $u = x/z$ and $v = y/z$. Since there are $p-1$ choices for z, this last case gives a total of $(p-1)N_c$ solutions. Thus the number of solutions of (4) is $1+3(p-1)+(p-1)N_c$.

Thus a simple calculation using the results of Libri and Lebesgue shows that

$$M_1 = p^2+a(p-1), \tag{5}$$

where a is uniquely determined by (3).

Using methods essentially included in Gauss's work [2] on the cubic equation of periods, it is shown below that if $2 \in G-H$ then for $c = 2$ or 4

$$M_c = p^2+\tfrac{1}{2}(p-1)(9b-a). \tag{6}$$

Here a and b are given by (3) together with

$$a \equiv b \pmod 4 \text{ for } c = 2 \quad \text{and} \quad a \not\equiv b \pmod 4 \text{ for } c = 4. \tag{7}$$

This result is also derived from the results of Stieltjes. These results are also used to prove that if $3 \in G-H$, then for $c = 3$ or $c = 9$, M_c is given by (6) where a and b are determined by (3) together with

$$b \equiv 2 \pmod 3 \text{ if } c = 3 \quad \text{and} \quad b \equiv 1 \pmod 3 \text{ if } c = 9. \tag{8}$$

In general, M_c is given by (6) where the criterion for a and b is more complicated, namely: Condition (3) plus

$$a-3b\left(c^{\frac{2}{3}(p-1)}-c^{\frac{1}{3}(p-1)}\right) \equiv 0 \pmod{p}, \tag{9}$$

where again $c \in G-H$.

The method of Gaussian sums. For a fixed prime $p \equiv 1 \pmod 3$ and for any integer j, let

$$S(j) = \sum_{k=0}^{p-1} \exp(2\pi ijk^3/p).$$

Let g be a generator of the multiplicative group G of non-zero residues (mod p). Then $S(1)$, $S(g)$, and $S(g^2)$ are the zeros of Gauss' cubic period equation

$$x^3-3px-pa = 0$$

where a is fixed by (3). Manipulating the known relationships between the zeros and coefficients of a cubic polynomial leads to

$$\begin{aligned} S^2(1)S(g)+S^2(g)S(g^2)+S^2(g^2)S(1) &= \tfrac{1}{2}\left(-3pa \pm \sqrt{-(27p^2a^2-108p^3)}\right) \\ &= \tfrac{1}{2}\left(-3pa \pm p\sqrt{27(4p-a^2)}\right) \\ &= \tfrac{1}{2}\left(-3pa \pm p\sqrt{27^2b^2}\right) = \tfrac{3}{2}(-d \pm 9b)p. \end{aligned}$$

The above equation leads without too much work to

$$\sum_{j=1}^{p-1} S^2(j)S(jg) = \tfrac{1}{2}p(p-1)(-a \pm 9b). \tag{10}$$

But interchanging the order of summation on the left side of (10) gives

$$\sum_{j=1}^{p-1} S^2(j)S(jg) = pM_g-p^3. \tag{11}$$

Together (10) and (11) show that M_g is one of the values

$$p^2+\tfrac{1}{2}(p-1)(-a \pm 9b). \tag{12}$$

Now it is not difficult to see that $M_1+M_g+M_{g^2} = 3p^2$. Together with (5) this shows that $M_g \neq M_{g^2}$ and M_{g^2} is also one of the values given by (12).

Observe that if $c \in G-H$, then c is in the coset gH if and only if $c^2 \in g^2H$, and for $1 \leqslant i \leqslant 2$, if $c \in g^iH$, then $M_c = M_{g^i}$.

Let A_c be the number of times c occurs as the difference between non-zero cubic residues (mod$p$). If $c \in G-H$, then $N_c = 9A_c$ and $M_c = 9(p-1)A_c+3p-2$. If $c \in H$, then $N_c = 9A_c+6$ and $M_c = 9(p-1)A_c+ +9p-8$.

Lemma. *If $2 \in G-H$, then A_2 is odd, while A_4 and A_c, for $c \in H$, are even.*

Proof. Let $x = u$ and $y = v$ be solutions from H of $x-y = c$. So long as $u \neq -v$, then $x = -v$ and $y = -u$ is a different solution. But $u = -v$ if and only if $2u = c$. Thus A_c is odd if and only if there is an odd number of $u \in H$ such that $2u = c$. If $c = 2$, then u can only be 1; so A_2 is odd. If $c = 4$, then u can only be 2, but $2 \notin H$; so A_4 is even. If $c \notin H$, then $2 = \frac{c}{u} \in H$, but $2 \notin H$; so A_c is even.

Theorem. *For a prime $p \equiv 1 \pmod 3$ with $2 \notin H$, if $c \notin G-H$, then*

$M_c = p^2+\frac{1}{2}(p-1)(9b-a)$ *where* a *and* b *are uniquely determined by* (3), $b\equiv a \pmod 4$ *for* $c\equiv 2 \pmod H$ *and* $b\not\equiv a \pmod 4$ *for* $c\equiv 4 \pmod H$.

Proof. It is not difficult to see for $c\equiv 2 \pmod H$ that $M_c = M_2$.

$$M_2 = p^2+\frac{1}{2}(p-1)(9b-a) = 9(p-1)A_2+3p-2$$

where a is determined and b is determined except for sign by $4p = a^2+27b^2$ and $a\equiv 1 \pmod 3$. Thus $9A_2 = p-2+\frac{1}{2}(9b-a)$. Studying the parity of both sides: $1\equiv 1+\frac{1}{2}(b-a) \pmod 2$ so that $b-a\equiv 0 \pmod 4$. Similarly the case when $c\equiv 4 \pmod H$ leads to $9A_4 = p-2+\frac{1}{2}(9b-a)$ and $0\equiv 1+\frac{1}{2}(b-a) \pmod 2$, so $\frac{1}{2}(b-a)$ must be odd and $b\not\equiv a \pmod 4$.

THEOREM. *If* $2\in H$, *then* $A_1\equiv 3 \pmod 4$.

Proof. From (2) and $N_1 = 9A_1+6$ it follows that $A_1 = (p+a-8)/9$. Gauss proved that if $2\in H$, then there are integers u and v such that $p = u^2+27v^2$. If u is odd, then v is even and $p\equiv 1 \pmod 4$. Then $4p = (2u)^2+27\cdot(2v)^2 = a^2+27b^2$. Since the representation of $4p$ by the form x^2+27y^2 is unique up to the signs of x and y, then $\pm a = 2u$ so $a\equiv 2 \pmod 4$. Hence in this case $A_1\equiv 3 \pmod 4$. If u is even, then v is odd and $p\equiv 3 \pmod 4$ and as before $\pm a = 2u$, so $a\equiv 0 \pmod 4$. Thus in this case $A\equiv 3 \pmod 4$.

The derivation of the formulae for M_c from the results of Stieltjes. In view of the proposition and the equality $N_c = 9A_c$ it is enough to show that under conditions (7), (8) or (9)

$$9A_c = p-2+\frac{1}{2}(9b-a). \tag{13}$$

In the notation of Chapter III § 4 of [3] we have $a = L$, $b = \pm M$ and since N_c equals the number of solutions of $x^3-cy^3\equiv 1 \pmod p$, $y\not\equiv 0$

$$A_c = \begin{cases} j & \text{if} \quad c^{(p-1)/3}\equiv f \pmod p, \\ h & \text{if} \quad c^{(p-1)/3}\equiv f^2 \pmod p, \end{cases}$$

where f is a root of the congruence $f^2+f+1\equiv 0 \pmod p$ and the sign of M is determined by the condition

$$L+3M(f^2-f)\equiv 0 \pmod p. \tag{14}$$

Using the formulae for j and h given on p. 92 of [3] we get

$$A_c = \frac{2p-4-\varepsilon M-L}{18} \quad \text{if} \quad c^{(p-1)/3}\equiv f^{\varepsilon} \pmod p, \quad \varepsilon = \pm 1. \tag{15}$$

Define now ε by the equation $\varepsilon M = -b$. Then (13) follows from (15) provided $c^{(p-1)/3}\equiv f^{\varepsilon} \pmod p$. To deduce the latter congruence from (7) or (8) we use the following two statements italicized on p. 93 of [3] and here reformulated in order to avoid a confusion in notation:

$$2^{(p-1)/3}\equiv f^{\varepsilon} \pmod p \quad \text{if} \quad \tfrac{1}{2}(3\varepsilon M-L)\equiv 0 \pmod 2,$$
$$3^{(p-1)/3}\equiv f^{\varepsilon} \pmod p \quad \text{if} \quad M\equiv \varepsilon \pmod 3.$$

Finally if (9) holds we have by (14)

$$L+3\varepsilon M(c^{2(p-1)/3}-c^{(p-1)/3})\equiv 0\equiv L+3M(f^2-f) \pmod p$$

hence again

$$c^{(p-1)/3}\equiv f^{\varepsilon} \pmod p.$$

Using the cubic reciprocity law one can derive for any c conditions similar to (7) and (8).

References

[1] S. Chowla, *The Riemann Hypothesis and Hilbert's tenth problem*, Gordon and Breach, New York 1965.

[2] C. F. Gauss, *Disquisitiones Arithmeticae*, translated by A. A. Clarke, Yale University Press, New Haven and London 1966.

[3] B. A. Venkov, *Elementary number theory*, translated by Helen Alderson, Wolters-Nordhoff Publishing Co, Groningen 1970.

Received on 1. 4. 1977
and in revised form on 17. 12. 1977 (932)