Pacific Journal of Mathematics

THE NUMBER OF SOLUTIONS OF CERTAIN CUBIC CONGRUENCE

ECKFORD COHEN

Vol. 5, No. 6 1955

THE NUMBER OF SOLUTIONS OF CERTAIN CUBIC CONGRUENCES

ECKFORD COHEN

1. Introduction. In this paper we shall be concerned with cubic congruences of the form

$$n \equiv a_1 x_1^3 + \cdots + a_s x_s^3 \pmod{m}, \tag{1.1}$$

where n is arbitrary, $m > 1$, and the a_i are integers prime to m. The number of sets of solutions $(x_1, \cdots, x_s)$ of (1.1), distinct modulo m, will be denoted by $N_s(n, m)$. Our discussion of $N_s(n, m)$ is limited to the cases $s=2$ and $s=3$; however, we emphasize that the method involved can be extended to arbitrary s.

Suppose that m has the factorization $m = p_1^{\lambda_1}, \cdots, p_l^{\lambda_l}$ as a product of powers of distinct primes $p_1, \cdots, p_l$. Then it follows easily that

$$N_s(n, m) = N_s(n, p_1^{\lambda_1}) \cdots N_s(n, p_l^{\lambda_l}). \tag{1.2}$$

Thus the determination of $N_s(n, m)$ reduces to the problem of determining $N_s(n, p^\lambda)$ where p is a prime. We accordingly limit ourselves to the case of a prime-power modulus p^λ.

If we denote by t the largest integer $\leq \lambda$ such that $n \equiv 0 \pmod{p^t}$, then one may write

$$n = p^t \xi, \qquad (\xi, p) = 1, \qquad 0 \leq t \leq \lambda. \tag{1.3}$$

We observe, in case $\lambda > t$, that ξ is uniquely determined $(\mathrm{mod}\, p)$. Our main goal will be to obtain exact formulas for the number of solutions $N_2(n, p^\lambda, t) = N_2$ of

$$n \equiv ax^3 + by^3 \pmod{p^\lambda}, \tag{1.4}$$

and the number of solutions $N_3(n, p^\lambda, t) = N_3$ of

$$n \equiv ax^3 + by^3 + cz^3 \pmod{p^\lambda}, \tag{1.5}$$

where n is arbitrary of the form (1.3), and the following conditions are satisfied:

$$p \equiv 1 \pmod 3, \qquad abc \not\equiv 0 \pmod p. \tag{1.6}$$

The restriction $p \equiv 1 \pmod 3$ is natural, since other primes are special in the case of cubic congruences.

The method of the paper is based on elementary properties of

Received March 5, 1954. This paper is based on research completed when the author was a member of the Institute for Advanced Study.

finite exponential sums. These are listed for the cubic case as preliminary lemmas in § 2. The principal formula for N_2 is contained in Theorem 1 (§ 3) and the corresponding result for N_3 in Theorem 2 (§ 4). Both results involve the pair of integers (A, B), determined uniquely by the relations [7],

$$4p=A^2+27B^2, \qquad A\equiv 1 \pmod 3, \quad B>0. \tag{1.7}$$

However, in the special case $t\not\equiv 0 \pmod 3$, the value of N_2 is given explicity (§ 3, Corollary 2).

On the basis of these formulas, solvability criteria for (1.4) and (1.5) are developed in § 5. In fact, it is shown in Theorem 5 that (1.5) is *always* solvable ($N_3>0$). As for N_2, the following criterion is established: *If* $p\neq 7$, *then* (1.4) *is insolvable if and only if* $t\not\equiv 0 \pmod 3$, $t<\lambda$, *and* a *and* b *belong to different cubic character classes* (mod p). (For the exceptional case $p=7$, see the complete statement of the criterion in Theorem 6). Approximations to N_2 and N_3 are also given in § 5 (Theorems 3 and 4, respectively).

Regarding previous research on cubic congruences, we note the work of Gauss who evaluated N_2 in the case of a prime modulus p [4]. More recently, Dickson determined N_3 for a prime modulus, with $a=b=c=1$ [3, p. 167]. In addition, Skolem [9] and Selmer [8] have considered such congruences in their treatment of cubic Diophantine equations. Some of these results were deduced by the author in an earlier note anticipating the present paper [2].

2. Notation and preliminary lemmas. The cubic Gauss sum $G(n, m)$ is defined by

$$G(n, m)=\sum_{\mu \pmod m} \varepsilon(n^3, m)\,, \tag{2.1}$$

where the summation is over a complete residue system (mod m), and ε is defined for integral α, by

$$\varepsilon(\alpha, m)=e^{2\pi i\alpha/m}. \tag{2.2}$$

Expansion of $N_s(n, m)$ into a Fourier sum [1, § 5] reveals immediately the relation between $N_s(n, m)$ and the Gauss sum (2.1):

LEMMA 1. *The number of solutions of* (1.1) *is given by*

$$N_s(n,m)=\frac{1}{m}\sum_{\mu \pmod m} \varepsilon(n, m) \prod_{i=1}^{s} G(-a_i\mu, m)\,. \tag{2.3}$$

We next note two reduction formulas for G [6].

LEMMA 2.

$$G(nm', mn') = m' G(n, m). \tag{2.4}$$

LEMMA 3. *If* $(\nu, p)=1$, *then*

$$G(\nu, p^k) = \begin{cases} p^{2j} & (k=3j), \\ p^{2j} G(\nu, p) & (k=3j+1), \\ p^{2j+1} & (k=3j+2). \end{cases} \tag{2.5}$$

Closely related to $G(n, p^k)$ are the two Gauss-Kummer sums defined by

$$\tau_i^{(k)}(n) = \sum_{\substack{\nu \pmod{p^k} \\ (\nu, p)=1}} \chi^i(\nu) \varepsilon(n, p^k), \qquad (i=1, 2), \tag{2.6}$$

where $\chi(\nu)$ and $\chi^2(\nu)$ denote the two non-principal cubic characters $(\mathrm{mod}\ p)$, the summation being over a reduced residue system $(\mathrm{mod}\ p^k)$. In order to differentiate between the two non-principal characters, we write

$$\theta_1 = \frac{1}{2}(A+3B\sqrt{-3}), \quad \theta_2 = \bar{\theta}_1, \qquad (\theta_1\theta_2 = p), \tag{2.7}$$

where A and B are defined by (1.7). Then one may define $\chi(\alpha)$, for integers α prime to p, to be that cube root of unity satisfying

$$\chi(\alpha) \equiv \alpha^{(p-1)/3} \pmod{\theta_1}. \tag{2.8}$$

The relation (2.8) is the cubic extension of the Euler criterion [5, p. 455]. In our discussion, the primitive cube roots of unity will be denoted by ω and ω^2, with $\omega = \frac{1}{2}(-1+\sqrt{-3})$.

We place further,

$$\tau_i(n) = \tau_i^{(1)}(n), \quad \tau_i = \tau_i(1), \qquad (i=1, 2).$$

With this notation, we state the following reduction formula for $\tau_i^{(k)}(n)$.

LEMMA 4. *If* $k \geq 1$ *and* $i=1$ *or* 2, *then*

$$\tau_i^{(k)}(n) = \begin{cases} p^{k-1}\tau_i(\xi) & (n=p^{k-1}\xi, \ (\xi, p)=1), \\ 0 & (\text{otherwise}) \end{cases} \tag{2.9}$$

The important relation connecting $G(\nu, p)$, $\tau_1(\nu)$, and $\tau_2(\nu)$ is contained in the following lemma.

LEMMA 5. *If* $(\nu, p)=1$, *then*

$$G(\nu, p) = \tau_1(\nu, p) + \tau_2(\nu, p). \tag{2.10}$$

The sums $\tau_1(\nu)$, $\tau_2(\nu)$ have the following fundamental properties [5],

$$\tau_1(\nu)=\chi^2(\nu)\tau_1\,,\quad \tau_2(\nu)=\chi(\nu)\tau_2\,,\qquad (\nu,\ p)=1\,, \tag{2.11}$$

$$\tau_1\tau_2=p\,, \tag{2.12}$$

$$\tau_1^3=p\theta_1\,,\qquad \tau_2^3=p\theta_2\,, \tag{2.13}$$

θ_1 and θ_2 being defined by (2.7).

Corresponding to the principal character (mod p), we have the familiar (Ramanujan) sum,

$$C(n,p^k)=\sum_{\substack{\nu(\mathrm{mod}\ p^k)\\(\nu,\ p)=1}}\varepsilon(n\nu,\ p^k)\,, \tag{2.14}$$

which has the evaluation ($k>0$),

$$C(n,\ p^k)=\begin{cases} p^{k-1}(p-1) & (p^k\mid n\,,\\ -p^{k-1} & (p^{k-1}\mid n,\ p^k\nmid n)\,,\\ 0 & (p^{k-1}\nmid n)\,.\end{cases} \tag{2.15}$$

Also of importance in this paper are the functions,

$$T(\alpha)=\frac{1}{p}\,(\chi^2(\alpha)\tau_1^3+\chi(\alpha)\tau_2^3)\,, \tag{2.16}$$

$$J(\alpha)=\begin{cases} A & (\chi(\alpha)=1)\,,\\ \tfrac{1}{2}(9h(\alpha)B-A) & (\chi(\alpha)\neq 1)\,,\end{cases} \tag{2.17}$$

where $h(\alpha)$ is defined for cubic non-residues α (mod p) by

$$h(\alpha)=1\quad\text{or}\quad -1\,, \tag{2.18}$$

according as $\chi(\alpha)=\omega$ or ω^2.

Application of (2.13) gives

LEMMA 6.

$$T(\alpha)=J(\alpha)\,. \tag{2.19}$$

The following notation will be needed.

$$q=\left[\frac{t-1}{3}\right],\qquad r=\left[\frac{t}{3}\right],\qquad s=\left[\frac{t-2}{3}\right], \tag{2.20}$$

$$Q=\left[\frac{\lambda-1}{3}\right],\qquad R=\left[\frac{\lambda}{3}\right],\qquad S=\left[\frac{\lambda-2}{3}\right], \tag{2.21}$$

where $[\beta]$ indicates the largest integer $\leq\beta$; and for $i=0,\ 1,\ 2$,

$$L_i(t)=\begin{cases} 1 & (t\equiv i\ (\mathrm{mod}\ 3),\quad t<\lambda)\,,\\ 0 & (\text{otherwise})\,.\end{cases} \tag{2.22}$$

3. The number of solutions of (1.4). In this section we use the notation,

$$\zeta = ab\xi , \tag{3.1}$$

where ξ is defined by (1.3), and

$$\eta = \chi(a)\chi^2(b)+\chi(b)\chi^2(a) = 2 \quad \text{or} \quad -1 , \tag{3.2}$$

according as $\chi(a)=\chi(b)$ or $\chi(a)\neq\chi(b)$.

The main result on (1.4) is contained in

THEOREM 1. *The number of solutions of* (1.4) *is given by*

$$\begin{aligned} N_2(n, p^\lambda, t) = p^{\lambda-1}\{&p^r J(\zeta)L_0(t)+p^{q+1}\eta(1-L_0(t)) \\ &+p^{r+1}(1-L_2(t))+p^{s+1}(1-L_1(t))-(\eta+1)\} , \end{aligned} \tag{3.3}$$

where t is defined by (1.3), *J by* (2.17), *q, r, s by* (2.20), *the $L_i(t)$ by* (2.22), *and ζ, η by* (3.1) *and* (3.2) *respectively.*

Proof. By Lemma 1 it follows immediately that

$$N_2 = \frac{1}{p^\lambda} \sum_{\mu \pmod{p^\lambda}} \varepsilon(n\mu, p^\lambda)G(-a\mu, p^\lambda)G(-b\mu, p^\lambda) . \tag{3.4}$$

The residue system $\mu \pmod{p^\lambda}$ may be assumed to be the set $\mu = \nu p^{\lambda-k}$ where k ranges over the values $0 \leq k \leq \lambda$, and for each k, ν ranges over a reduced residue system $(\text{mod } p^k)$. Thus (3.4) becomes, using (2.4),

$$N_2 = p^\lambda \sum_{k=0}^{\lambda} \frac{1}{p^{2k}} \sum_{\substack{\nu \pmod{p^k} \\ (\nu, p)=1}} \varepsilon(\nu n, p^k)G(-a\nu, p^k)G(-b\nu, p^k) . \tag{3.5}$$

We now break up the k summation according as $k \equiv 1$, 0, or 2 (mod 3), and apply Lemma 3 to obtain

$$N_2 = U_1 + U_2 + U_3 , \tag{3.6}$$

where

$$U_1 = p^{\lambda-2} \sum_{j=0}^{Q} \frac{1}{p^{2j}} \sum_{\substack{\nu \pmod{p^{3j+1}} \\ (\nu, p)=1}} \varepsilon(\nu n, p^{3j+1})G(-a\nu, p)G(-b\nu, p) , \tag{3.7}$$

$$U_2 = p^\lambda \sum_{j=0}^{R} \frac{1}{p^{2j}} C(n, p^{3j}) , \qquad U_3 = p^{\lambda-2} \sum_{j=0}^{S} \frac{1}{p^{2j}} C(n, p^{3j+2}) . \tag{3.8}$$

Applying Lemma 5 and (2.11) to (3.7), and expanding, U_1 may be written

(3.9) $$U_1=U_{11}+U_{12}+U_{13},$$

where

$$U_{11}=p^{\lambda-2}\chi^2(ab)\tau_1^2\sum_{j=0}^{Q}\frac{1}{p^{2j}}\tau_1^{(3j+1)}(n),$$

$$U_{12}=p^{\lambda-2}\chi(ab)\tau_2^2\sum_{j=0}^{Q}\frac{1}{p^{2j}}\tau_2^{(3j+1)}(n),$$

$$U_{13}=p^{\lambda-2}\tau_1\tau_2\eta\sum_{j=0}^{Q}\frac{1}{p^{2j}}C(n,\ p^{3j+1}).$$

Application of (2.11) and Lemmas 4 and 6 to U_{11} and U_{12} gives

(3.10) $$U_{11}+U_{12}=p^{\lambda-1+r}J(\zeta)L_0(t),$$

while U_{13} becomes, on the basis of (2.12) and (2.15),

(3.11) $$U_{13}=p^{\lambda-1}\eta\{p^{q+1}(1-L_0(t))-1\}.$$

Also, using (2.15) and summing, we get

(3.12) $$U_2=p^{\lambda+r}(1-L_2(t)),\qquad U_3=p^{\lambda-1}\{p^{s+1}(1-L_1(t))-1\}.$$

The theorem follows on combining (3.6), (3.9), (3.10), (3.11), and (3.12).

Three main cases of Theorem 1 are distinguished according as, (i) $\lambda>t$, $t\equiv 0 \pmod 3$, (ii) $\lambda>t$, $t\not\equiv 0 \pmod 3$, or (iii) $\lambda=t$ $(n=0)$. Corresponding to these cases, one may deduce the following corollaries from (3.3).

COROLLARY 1. *If* $\lambda>t=3e$, *then*

(3.13) $$N_2(n,\ p^\lambda,\ 3e)=p^{\lambda-1}\{p^e(J(\zeta)+p+1)-\eta-1\}.$$

COROLLARY 2. *If* $\lambda>t\not\equiv 0 \pmod 3$, *then*

(3.14) $$N_2(n,\ p^\lambda,\ t)=p^{\lambda-1}(p^{e+1}-1)(\eta+1),$$

where $t=3e+1$ *or* $3e+2$, *according as* $t\equiv 1$ *or* $2 \pmod 3$.

COROLLARY 3. $(n=0)$. *If* $\lambda=t=3e+j$, $(j=0,\ 1,\ 2)$, *then*

(3.15) $$N_2(n,\ p^\lambda,\ \lambda)=p^{\lambda-1}\{(\eta+1)(p^{e+\gamma}-1)+p^{e+j+1-2\gamma}\},$$

where $\gamma=0$ *or* 1 *according as* $t\equiv 0$ *or* $t\not\equiv 0 \pmod 3$.

4. The number of solutions of (1.5). The elements of the set $(a,\ b,\ c,\ \xi)=H$ may be distributed among the three cubic character classes (mod p) in essentially four different ways. These four distributions, denoted by H_1, H_2, H_3, and H_4, are defined as follows: (H_1)

Every class contains at least one element of H; (H_2) One class contains two elements of H and a second class contains the other two; (H_3) One class contains three elements of H but not all four; (H_4) All four elements lie in the same class.

Using this notation we define the function,

$$\delta(H)=0,\ 3,\ -3,\ \text{or}\ 6, \tag{4.1}$$

according as the elements of H have a distribution of type H_1, H_2, H_3, or H_4.

We will also make use of the following notation:

$$\theta=abc;\quad \eta_1=\eta_1(a,b,c)=\chi(a)\chi^2(bc)+\chi(b)\chi^2(ac)+\chi(c)\chi^2(ab),\quad \eta_2=\bar{\eta}_1, \tag{4.2}$$

$\bar{\eta}_1$ denoting the complex conjugate of η_1:

$$\Delta(H)=\eta_1\chi(\xi)+\eta_2\chi^2(\xi). \tag{4.3}$$

On the basis of the above notation, one may deduce

LEMMA 7.

$$\Delta(H)=\delta(H). \tag{4.4}$$

We now state the main theorem for $N_3(n, p^\lambda, t)$.

THEOREM 2. *The number solutions of* (1.5) *is given by*

$$\begin{aligned} N_3(n,p^\lambda,t)=p^{2\lambda-2}\{&[(p-1)(q+1)-L_0(t)]J(\theta)+p\delta(H)L_0(t)\\ &-L_1(t)-pL_2(t)+(p-1)(pr+s+1)+p^2\}, \end{aligned} \tag{4.5}$$

where $\delta(H)$ *is defined by* (4.1), θ *by* (4.2), *and the rest of the notation has the same meaning as in Theorem* 1.

Proof. As in the proof of Theorem 1, we may express N_3 as a Fourier sum and apply Lemmas 2 and 3 to obtain

$$N_3=V_1+V_2+V_3, \tag{4.6}$$

where

$$V_1=p^{2\lambda-3}\sum_{j=0}^{Q}\frac{1}{p^{3j}}\sum_{\substack{\nu \pmod{p^{3j+1}}\\(\nu,p)=1}}\varepsilon(\nu n,p^{3j+1})G(-a\nu,p)G(-b\nu,p)G(-c\nu,p), \tag{4.7}$$

$$V_2=p^{2\lambda}\sum_{j=0}^{R}\frac{1}{p^{3j}}C(n,p^{3j}),\qquad V_3=p^{2\lambda-3}\sum_{j=0}^{S}\frac{1}{p^{3j}}C(n,p^{3j+2}). \tag{4.8}$$

Application of Lemma 5 and (2.11) to (4.7) yields

$$V_1=V_{11}+V_{12}+V_{13}, \tag{4.9}$$

where

$$V_{11}=p^{2\lambda-2}T(\theta)\sum_{j=0}^{Q}\frac{1}{p^{3j}}C(n,\ p^{3j+1}),$$

$$V_{12}=p^{2\lambda-3}\tau_1^2\tau_2\eta_1\sum_{j=0}^{Q}\frac{1}{p^{3j}}\tau_2^{(3j+1)}(n),$$

$$V_{13}=p^{2\lambda-3}\tau_1\tau_2^2\eta_2\sum_{j=0}^{Q}\frac{1}{p^{3j}}\tau_1^{(3j+1)}(n).$$

Using (2.15) and Lemma 6 in case of V_{11}, one obtains

$$V_{11}=p^{2\lambda-2}J(\theta)\{(p-1)(q+1)-L_0(t)\}. \tag{4.10}$$

V_{12} and V_{13} may be transformed by (2.11), (2.12), and Lemmas 4 and 7, to give

$$V_{12}+V_{13}=p^{2\lambda-1}\delta(H)L_0(t). \tag{4.11}$$

As for V_2 and V_3, application of (2.15) gives

$$V_2=p^{2\lambda-2}\{p^2+pr(p-1)-pL_2(t)\}, \tag{4.12}$$

$$V_3=p^{2\lambda-2}\{(p-1)(s+1)-L_1(t)\}. \tag{4.13}$$

Combination of the results in (4.6) and formulas (4.10) through (4.13) leads to the theorem.

Corresponding to the corollaries of Theorem 1, we may deduce the following results as special cases of Theorem 2.

COROLLARY 1. *If* $\lambda>t=3e$, *then*

$$N_3(n,\ p^\lambda,\ 3e)=p^{2\lambda-2}\{(pe-e-1)J(\theta)+e(p^2-1)+p^2+p\delta(H)\}. \tag{4.14}$$

COROLLARY 2. *If* $\lambda>t\not\equiv 0 \pmod 3$, *then*

$$N_3(n,\ p^\lambda,\ t)=p^{2\lambda-2}(p-1)(e+1)(J(\theta)+p+1), \tag{4.15}$$

where $t=3e+1$ *or* $3e+2$.

COROLLARY 3 ($n=0$). *If* $\lambda=t$, *then*

$$N_3(n,\ p^\lambda,\ \lambda)=p^{2\lambda-2}\{(p-1)[J(\theta)(e+\mu_1)+e(p+1)+\mu_2]+p^2\}, \tag{4.16}$$

where $\mu_1=\mu_2=0$ *if* $t=3e>0$; $\mu_1=1$, $\mu_2=0$ *if* $t=3e+1$, *and* $\mu_1=\mu_2=1$ *if* $t=3e+2$.

5. Solvability criteria. First we establish some bounds for N_2 and N_3. To do this, note by Definition (1.7) that $|A|<2\sqrt{p}$, and by a simple process of maximalization, that $|9h(\alpha)B-A|<4\sqrt{p}$, $(h(\alpha)=\pm 1)$. Thus we have

LEMMA 8.

$$|J(\alpha)|<2\sqrt{p}\ . \tag{5.1}$$

By means of this Lemma and Corollary 1 of § 3, we get the following estimate for $N_2(n, p^\lambda, 3e)$.

THEOREM 3. *If* $\lambda>t=3e$, *then*

$$p^e(p+1-2\sqrt{p})-\eta-1<\frac{N_2}{p^{\lambda-1}}<p^e(p+1+2\sqrt{p})-\eta-1\,. \tag{5.2}$$

Similarly, we may deduce bounds for N_3 on the basis of Corollaries 1 and 2 of § 4.

THEOREM 4. *If* $\lambda>t$, *then in case* $t=3e$,

$$\begin{aligned} p^2+e(p^2-1)-2(pe-e-1)\sqrt{p}+p\delta(H)<p^{2(1-\lambda)}N_3 \\ <p^2+e(p^2-1)+2(pe-e-1)\sqrt{p}+p\delta(H)\,, \end{aligned} \tag{5.3}$$

and in case $t=3e+1$ *or* $3e+2$,

$$p+1-2\sqrt{p}<\frac{p^{2(1-\lambda)}N_3}{(p-1)(e+1)}<p+1+2\sqrt{p}\ . \tag{5.4}$$

We are now in a position to establish precise criteria for the solvability of (1.4) and (1.5).

THEOREM 5. *The congruence* (1.5) *has a solution for every integer* n.

Proof. To prove this theorem it suffices to show that the lower bounds in (5.3) and (5.4) are positive. This follows immediately in the case of (5.4). Rewriting the lower bound in (5.3) in the form,

$$ep^{3/2}(\sqrt{p}-2)+e(2\sqrt{p}-1)+p(p+2p^{-1/2}+\delta)\,,$$

and remembering that the minimal values of p, $\delta(H)$, and e are $p=7$, $\delta=-3$, and $e=0$, we see that $N_3>0$ also in the case $\lambda>t\equiv 0 \pmod 3$.

THEOREM 6. *The congruence* (1.4) *has no solution if and only if either* $t\not\equiv 0 \pmod 3$, $t<\lambda$, *and* $\chi(a)\neq\chi(b)$, *or if* $p=7$, $t=0$, $\chi(a)=\chi(b)$ *and* $\zeta=ab\xi\equiv\pm 3 \pmod 7$.

Proof. If $\lambda>t\not\equiv 0 \pmod 3$, it follows directly from Corollary 2 of § 3, that $N_2=0$ if and only if $\eta=-1(\chi(a)\neq\chi(b))$. In the remainder of the proof we suppose, therefore, that $\lambda>t\equiv 0 \pmod 3$. Now the

lower bound in (5.2) is positive in case $\eta=-1$ and also in case $\eta=2$, $e>0$. In the remaining case ($\eta=2$, $e=0$), the lower bound is $p-2-2\sqrt{p}$, which is positive if $p>7$. But if $p=7$, $e=0$, $\eta=2$, then substitution in (3.13) shows that $N_2=0$ if and only if $\chi(\zeta)=\omega^2$, which implies that $\zeta\equiv\pm 3 \pmod 7$.

As a corollary of Theorem 6, we have the following result [8], [9]:

COROLLARY (Skolem-Selmer). *If $p\nmid abc$, then the congruence*

$$ax^3+by^3+cz^3\equiv 0 \pmod{p^\lambda} \tag{5.5}$$

always has a non-trivial solution (x, y, z not all $\equiv 0 \pmod p$).

Proof. With $z=1$, $c=-n$, Theorem 6 shows that (5.5) has a non-trivial solution $(X, Y, 1)$ unless $p=7$, $\chi(a)=\chi(b)$. In the latter case, however, there exists a solution $(X, 1, 0)$, because an integer α is a cubic residue (mod p^λ) if and only if it is a residue (mod p).

REFERENCES

1. Eckford Cohen, *Rings of arithmetic functions*, Duke Math. J., **19** (1952), 115–129.
2. ———, *Representations by cubic congruences*, Proc. Nat. Acad. Sci., **39** (1953), 119–121.
3. L.E. Dickson, *Congruences involving only e-th powers*, Acta Arithmetica, **1** (1935), 162–167.
4. C.F. Gauss, *Werke, I*, 445–449.
5. Helmut Hasse, *Vorlesungen über Zahlentheorie*, Berlin, 1950, 453–455.
6. Edmund Landau, *Vorlesungen über Zahlentheorie, I*, Leipzig, 1927, 280–302.
7. G.B. Mathews, *Theory of Numbers*, Part I, reprinted New York, 1927, p. 222.
8. Ernst Selmer, *The Diophantine equation $ax^3+by^3+cz^3=0$*, Acta Math., **85** (1951), 215–223.
9. Th. Skolem, *Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist*, Avh. Norske Vid. Akad. Oslo, I. **4** (1942), 6–14.

THE UNIVERSITY OF SOUTH CAROLINA

../../../FrontMatter/paper.pdf

Pacific Journal of Mathematics
Vol. 5, No. 6 , 1955