

Article

Lower limit for the number of sets of solutions
of $x^e + y^e + z^e \dots 0 \pmod{p}$.

Dickson, L.E.

in: Journal für die reine und angewandte

Mathematik - 135 | Periodical

8 page(s) (181 - 188)

Nutzungsbedingungen

DigiZeitschriften e.V. gewährt ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht kommerziellen Gebrauch bestimmt. Das Copyright bleibt bei den Herausgebern oder sonstigen Rechteinhabern. Als Nutzer sind Sie nicht dazu berechtigt, eine Lizenz zu übertragen, zu transferieren oder an Dritte weiter zu geben.

Die Nutzung stellt keine Übertragung des Eigentumsrechts an diesem Dokument dar und gilt vorbehaltlich der folgenden Einschränkungen:

Sie müssen auf sämtlichen Kopien dieses Dokuments alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten; und Sie dürfen dieses Dokument nicht in irgend einer Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen; es sei denn, es liegt Ihnen eine schriftliche Genehmigung von DigiZeitschriften e.V. und vom Herausgeber oder sonstigen Rechteinhaber vor.

Mit dem Gebrauch von DigiZeitschriften e.V. und der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

Terms of use

DigiZeitschriften e.V. grants the non-exclusive, non-transferable, personal and restricted right of using this document. This document is intended for the personal, non-commercial use. The copyright belongs to the publisher or to other copyright holders. You do not have the right to transfer a licence or to give it to a third party.

Use does not represent a transfer of the copyright of this document, and the following restrictions apply:

You must abide by all notices of copyright or other legal protection for all copies taken from this document; and You may not change this document in any way, nor may you duplicate, exhibit, display, distribute or use this document for public or commercial reasons unless you have the written permission of DigiZeitschriften e.V. and the publisher or other copyright holders.

By using DigiZeitschriften e.V. and this document you agree to the conditions of use.

Kontakt / Contact

DigiZeitschriften e.V.

Papendiek 14

37073 Goettingen

Email: info@digizeitschriften.de

**Lower limit for the number
of sets of solutions of $x^e + y^e + z^e \equiv 0 \pmod{p}$.**

By Mr. *L. E. Dickson* at Chicago.

1. From the results established in the present paper it follows that, when e and p are odd primes, the congruence

$$(1.) \quad x^e + y^e + z^e \equiv 0 \pmod{p}$$

has integral solutions x, y, z , each prime to p , for every $p \geq E$, where

$$(2.) \quad E = (e-1)^2(e-2)^2 + 6e - 2.$$

When e is prime to $p-1$, every integer is a residue of an e^{th} power modulo p , so that the congruence (1.) has obvious solutions. Henceforth we assume that e and p are odd primes such that e divides $p-1$. We set $p-1 = ef$.

Let g be a primitive root of p . Then (1.) has solutions x, y, z , prime to p , if and only if the congruence

$$(3.) \quad 1 + g^{et} \equiv g^{e\tau} \pmod{p}$$

has integral solutions t, τ . The more general congruence

$$(4.) \quad 1 + g^{et+k} \equiv g^{e\tau+h} \pmod{p}$$

is employed in the theory of the division of the circle (Kreisteilung). For given integers k and h of the series $0, 1, \dots, e-1$, let (k, h) denote the number of integers t of the series $0, 1, \dots, f-1$ for which (4.) may be satisfied by choice of an integer τ of the latter series.

Our aim is to find a lower limit for the number $(0,0)$ of sets of solutions t, τ (each $< f$) of (2.), and finally (§ 5) a lower limit for the number of sets of solutions prime to p of (1.).

2. Let r be a primitive p^{th} root of unity. The e periods are

$$(5.) \quad \eta_k = \sum_{t=0}^{f-1} r^{g^{et+k}}. \quad (k=0, 1, \dots, e-1)$$

Let ω be a primitive $(p-1)^{\text{th}}$ root of unity. *Jacobis* function is

$$(6.) \quad [\omega^h, r] = \sum_{\lambda=0}^{p-2} \omega^{h\lambda} r^{g^\lambda},$$

the notation $[\]$ being used here to avoid confusion with the above symbol $(.)$. Let $\omega^f = \beta$, so that β is a primitive e^{th} root of unity. Note that, for $h = mf$, (6.) be given the form

$$(7.) \quad [\beta^m, r] = \sum_{\lambda=0}^{p-2} \beta^{m\lambda} r^{g^\lambda} = \sum_{k=0}^{e-1} \beta^{km} \eta_k,$$

as follows from (5.) upon setting $\lambda = e + k$. We here employ only the special *Jacobi*-functions (7.), which are linear functions of the periods. For $m+n$ not divisible by e , we have the relation*)

$$(8.) \quad \frac{[\beta^m, r] [\beta^n, r]}{[\beta^{m+n}, r]} = \sum_{\mu=1}^{p-2} \beta^{m \text{ ind } \mu - (m+n) \text{ ind } (1+\mu)},$$

the indices relating to the prime modulus p . The second member is in-

*) From (28.), p. 86, *Bachmann*, *Kreisteilung*, with $h = mf$, $k = nf$.

dependent of r . Taking $m = 1$, we set

$$(9.) \quad R_n(\beta) = \sum_{\mu=1}^{p-2} \beta^{\text{ind } \mu - (1+n) \text{ ind } (1+\mu)}. \quad (n=1, \dots, e-2)$$

For $m+n$ divisible by e , we have*), instead of (8.),

$$(10.) \quad [\beta^m, r] [\beta^{-m}, r] = p.$$

Hence we have the relation

$$(11.) \quad R_n(\beta) \cdot R_n(\beta^{-1}) = p.$$

3. Let K_n denote the sum of the terms in (9.) whose exponents are multiples of e . For the moment, set

$$1 + n \equiv \frac{1}{\varrho} \pmod{e}, \quad \mu = g^{d+ke}, \quad 1 + \mu = g^l. \quad (0 \leq d < e, 0 \leq k \leq f-1)$$

Then the exponent in (9.) is a multiple of e if and only if $l \equiv \varrho d \pmod{e}$. Hence there are as many exponents multiples of e as there are pairs of integers d, k for which

$$1 + g^{d+ke} \equiv g^{d\varrho} \pmod{p}.$$

It follows from the definition in § 1 that

$$(12.) \quad K_n = \sum_{d=0}^{e-1} (d, d\varrho). \quad \varrho(1+n) \equiv 0 \pmod{e}$$

In (9.), n may take, the values $1, \dots, e-2$. Then $\varrho \equiv (1+n)^{-1}$ takes the values $2, \dots, e-1 \pmod{e}$ in some order. Hence

*) Bachmann, p. 87, (29), with $h = mf$. Note that f is even for e odd.

$$\sum_{n=1}^{e-2} K_n = \sum_{d=0}^{e-1} \sum_{\rho=2}^{e-1} (d, d\rho) = (e-2)(0,0) + \sum_{d=1}^{e-1} L_d,$$

$$L_d = \sum_{\rho=2}^{e-1} (d, d\rho) = \sum_{\substack{j=1, \dots, e-1 \\ j \neq d}} (d, j),$$

since, for $d \neq 0$, $2d, \dots, (e-1)d$ are congruent, modulo e , to $1, \dots, d-1, d+1, \dots, e-1$, in some order. Now, for e odd, f even,

$$(13.) \quad \sum_{j=0}^{e-1} (0, j) = f-1, \quad \sum_{j=0}^{e-1} (d, j) = f. \quad (d=1, \dots, e-1)$$

Also, $(d, d) = (0, e-d)$. Hence

$$\sum_{d=1}^{e-1} L_d = \sum_{d=1}^{e-1} \{f - (d, 0) - (0, e-d)\} = (e-1)f - 2 \sum_{j=1}^{e-1} (0, j).$$

Applying also (13.), we obtain

$$(14.) \quad \sum_{n=1}^{e-2} K_n = e(0, 0) + (e-3)f + 2.$$

4. In (9.) we reduce the exponents by means of $\beta^e = 1$ and set

$$(15.) \quad R_n(\beta) = K_n + \sum_{k=1}^{e-1} C_{nk} \beta^k.$$

Since there are $p-2$ terms in (9.), we have

$$(16.) \quad K_n + \sum_{k=1}^{e-1} C_{nk} = p-2.$$

From (15.) we subtract

$$0 = K_n \left(1 + \sum_{k=1}^{e-1} \beta^k\right).$$

Let $a_{nk} = C_{nk} - K_n$. Then (15.) and (16.) give

$$(17.) \quad R_n(\beta) = \sum_{k=1}^{e-1} a_{nk} \beta^k, \quad \sum_{k=1}^{e-1} a_{nk} = p - 2 - eK_n.$$

From (11.) and (17.), we have

$$(18.) \quad p = \sum_{k=1}^{e-1} a_{nk} \beta^k \cdot \sum_{l=1}^{e-1} a_{nl} \beta^{-l} = \sum_{k=1}^{e-1} a_{nk}^2 + \sum_{s=1}^{\frac{1}{2}(e-1)} A_{ns} (\beta^s + \beta^{-s}),$$

where obviously

$$(19.) \quad \sum_{s=1}^{\frac{1}{2}(e-1)} A_{ns} = \sum a_{nk} a_{nl}, \quad (k, l=1, \dots, e-1; k < l)$$

Since $\sum_{k=0}^{e-1} \beta^k = 0$ is irreducible in the domain of rational members, equation (18.) requires that

$$(20.) \quad \sum_{k=1}^{e-1} a_{nk}^2 - p = A_{ns}. \quad (s=1, \dots, \frac{1}{2}(e-1))$$

Hence by (19.)

$$(21.) \quad p = \sum_{k=1}^{e-1} a_{nk}^2 - \frac{1}{\frac{1}{2}(e-1)} \sum a_{nk} a_{nl}, \quad (k, l=1, \dots, e-1; k < l)$$

The discriminant of the quadratic form

$$mp - (\sum a_{nk})^2,$$

with the value (21.) of p inserted, is seen to vanish only for $m=0$ or $m=(e-1)^2$. For the latter value, we have

$$(22.) \quad (e-1)^2 p - \left(\sum_{k=1}^{e-1} a_{nk}\right)^2 = eM_n, \quad M_n = (e-2) \sum_{k=1}^{e-1} a_{nk}^2 - 2 \sum a_{nk} a_{nl}$$

Since M_n may be given the form

$$(23.) \quad M_n = \sum (a_{nk} - a_{nl})^2 \quad (k, l, \dots, e-1; k < l)$$

we have $M_n > 0$; indeed, if the a 's were all equal, p would reduce to a^2 , and not be prime. Hence, by (22.),

$$(24.) \quad (e-1)\sqrt{p} > \sum_{k=1}^{e-1} a_{nk}.$$

Thus, by (17.), we have

$$(25.) \quad (e-1)\sqrt{p} > p-2-eK_n.$$

This result, like all others in §§ 3, 4 holds true for each $n=1, \dots, e-2$. Hence, applying (14.), we get

$$(e-2)(e-1)\sqrt{p} > (e-2)(p-2) - e^2(0,0) - (e-3)ef - 2e.$$

Since $ef=p-1$, we get

$$(26.) \quad e^2(0,0) > p+1-3e-(e-2)(e-1)\sqrt{p}.$$

5. By (26.), a sufficient condition for $(0,0) > 0$ is

$$p+1-3e \geq (e-2)(e-1)\sqrt{p}.$$

Squaring this and employing the abbreviation (2.), we get

$$(27.) \quad p^2 - pE + (3e-1)^2 \geq 0.$$

This condition is satisfied*) if $p \geq E$, and hence if

$$ef+1=p > E-1, \quad ef > e^4 - 6e^3 + 13e^2 - 6e.$$

Theorem. *If e and $p=ef+1$ are odd primes such that*

$$(28.) \quad f > e^3 - 6e^2 + 13e - 6,$$

congruence (1.) has a set of solutions prime to p . Formula (26.) gives a lower limit for the number $e^2(0,0)$ of sets of solutions prime to p of

$$(29.) \quad 1 + u^e \equiv v^e \pmod{p}.$$

For the number $N=(p-1)e^2(0,0)$ of sets of solutions prime to p of (1.), we have

$$(30.) \quad N > (p-1) \{p+1-3e-(e-1)(e-2)\sqrt{p}\}.$$

6. When f is a multiple of 3, there exists an integral root ϵ of

$$(\epsilon^{3e}-1)/(\epsilon^e-1) \equiv 0 \pmod{p=ef+1}.$$

Then (1.) has the set of solutions $x \equiv 1, y \equiv \epsilon, z \equiv \epsilon^2$. Hence in discussing the limit $p < E$ obtained in § 5 as a necessary condition for $(0,0)=0$, we need only test the primes $p=ef+1$ in which f is not divisible by 3.

For $e=3$, $E=20$, and the remaining primes are 7, 13. For each of these, $(0,0)=0$, so that the limit may be said to be exact.

*) We may take $p \geq P$, where P is the greater root of the equality (27.). But, for $e \geq 7$, $E-P < 1$, and there is no reduction for the integer p . For $e=5$, $P=170.85$ and we may replace the limit $E=172$ by 171, a trivial reduction since 171 is not prime. For $e=3$, we may replace the limit $E=20$ by $P=16$; the only intermediate prime of the form $3f+1$ is 19, which falls under the case in § 6.

For $e=5$, $E=172$, and the remaining primes are 11, 41, 71, 101, 131. For the first four, $(0,0)=0$; for 131, $(0,0)=6$.

For $e=7$, $E=940$, there remain 14 primes. Of these the first three (29, 71, 113) and the eighth (491) alone have $(0,0)=0$.

7. The method may be modified to apply to composite values of e . For $e=4$, let

$$p = 4f + 1 = A^2 + 4B^2.$$

For f even, set $(0,0)=\alpha$, $(1,2)=(1,3)=(2,3)=\varepsilon$. Then*

$$\alpha = 3\varepsilon - \frac{1}{2}f - 1, \quad 8\varepsilon - 2f - 1 = \pm A.$$

Hence $\alpha=0$ requires that

$$\mp 3A = 2f - 5, \quad p > A^2, \quad 0 > f^2 - 14f + 4, \quad f < 14, \quad p = 17.$$

For f odd, we have

$$\pm A = 2f - 3 - 8(0,0).$$

Then $(0,0)=0$ requires that

$$p > A^2, \quad 0 > f^2 - 4f + 2, \quad f \leq 3, \quad p = 5 \text{ or } 13.$$

Hence $x^4 + y^4 \equiv z^4 \pmod{p}$ has solutions prime to p for every prime $p = 4f + 1$ exceeding 17.

*) *Carey, Quarterly Journ. Math. vol. 26 (1893), p. 349—352.*