то, из (75), в силу (81), (86), получается

$$|S(\overset{*}{t}'')-S(\overset{*}{t}')| < B+A\psi_1(T) < A\psi_1(T) = \psi(T). \tag{87}$$

На этом доказательство закончено.

Литература

[1] Ян Мозер, *О некоторых арифметических средних в теории дзета-функции Римана*, Acta Arith. 28 (1976), стр. 363–377.

[2] A. Selberg, *On the zeros of Riemann's zeta-function*, Skr. Norske vid. Akad. Oslo, 10 (1942), стр. 1–59.

[3] — *Contributions to the theory of the Riemann zeta-function*, Arch. for. Math. og Naturv. B, 48 (1946), No. 5.

[4] Е. К. Титчмарш, *Теория дзета-функции Римана*, Москва 1953.

Поступило 9. 9. 1974
по исправлению 2. 12. 1974 (617)

ACTA ARITHMETICA
XXX (1976)

A note on Waring's problem in GF(p)

by

M. M. Dodson (York) and A. Tietäväinen (Turku)

1. Introduction. Let p be a prime, k a positive integer, $d = (k, p-1)$ the greatest common divisor of k and $p-1$, and $t = (p-1)/d$. Let $\gamma(k, p)$ denote the least positive integer s such that every residue (mod p) can be represented as a sum of s kth power residues (mod p). In other words, if $s \geqslant \gamma(k, p)$, the congruence

$$x_1^k+\ldots+x_s^k \equiv N \pmod p \tag{1}$$

has a solution for all integers N. It is well known that

$$\gamma(k, p) = \gamma(d, p)$$

and that

$$\gamma(p-1, p) = p-1, \quad \gamma\big(\tfrac{1}{2}(p-1), p\big) = \tfrac{1}{2}(p-1),$$

p being odd in the last equation. In this paper we shall be concerned with the case when $d < \frac{1}{2}(p-1)$ and for convenience we define

$$\gamma(k) = \max_p \{\gamma(k, p):\ d < \tfrac{1}{2}(p-1)\}.$$

In 1943 I. Chowla [3] proved that

$$\gamma(k) = O(k^{1-c+\varepsilon})$$

where $c = (103-3\sqrt{641})/220$ and where ε is, as always in this paper, a positive number. In 1971 Dodson [5] improved this estimate to the simpler result

$$\gamma(k) < k^{7/8}$$

providing k is sufficiently large and in 1973 Tietäväinen [7] showed that

$$\gamma(k) = O(k^{3/5+\varepsilon}).$$

Actually the first two results above were obtained for $\Gamma(k, p)$, the least s such that the congruence (1) has primitive or nontrivial solutions for all integers N. However in view of the immediate inequalities

$$\gamma(k, p) \leqslant \Gamma(k, p) \leqslant \gamma(k, p)+1$$

it is plain that the estimates given above are equivalent to the original ones.

In Theorem 1 of this paper we prove that for any positive number ε,

$$\gamma(k) = O(k^{1/2+\varepsilon})$$

or equivalently that if $\frac{1}{2}(p-1)$ does not divide k, then

$$\max_p \Gamma(k,p) = O(k^{1/2+\varepsilon}).$$

This result is almost best possible for in Theorem 2 we show that the lower bound for the exponent of k is $\frac{1}{2}$, i.e. if $\alpha < \frac{1}{2}$, then

$$\gamma(k) \neq O(k^{\alpha}).$$

Heilbronn [6] has conjectured that

$$\gamma(k) = O(k^{1/2})$$

and it is probable that this conjecture is true although we have been unable to prove it.

A related question is the representation of every integer in the p-adic field Q_p by sums of kth powers of p-adic integers. Denote by $\Gamma_p(k)$ the least s such that every p-adic integer is represented nontrivially by a sum of s kth powers. Then it follows from a recent paper by J. Bovey [1] that the estimates for $\Gamma(k,p)$ can be extended to $\Gamma_p(k)$.

2. Preliminary results and notation. Since $\gamma(k,p) = \gamma(d,p)$ we may suppose that k divides $p-1$ and since we are concerned only with the case $d < \frac{1}{2}(p-1)$, we can suppose further that

$$k \leqslant (p-1)/3.$$

If $p > k^2$ then it has been shown ([5], p. 151) that

$$\gamma(k,p) \leqslant \max\{3, [32\log k]+1\},$$

so that we can take $p < k^2$ from now on without loss of generality.

Let Q be the set of t nonzero kth power residues (mod p) so that Q is a subgroup of the multiplicative group $F^* = \mathrm{GF}(p)-\{0\}$ of nonzero residues (mod p). Let Q_w be the set of those residues (mod p) which can be represented as the sum of w kth power residues (mod p) and let q_w be the cardinality of Q_w.

For any integer a, we denote by $\|a\|$ the absolute value of the residue of a (mod p) which has least absolute value. Also we define

$$e(a) = e^{2\pi i a/p}.$$

3. The main theorem. The proof of the main theorem (Theorem 1) depends on a number of lemmas. Lemma 2 and Lemma 4 give estimates for $\gamma(k,p)$ under various hypothesis and Lemma 1 (which is Lemma 2 of [7]) and Lemma 3 are needed in the proof of Lemma 4.

LEMMA 1. *If $q_w \geqslant 2k$ then*

$$\gamma(k,p) \leqslant w(1+[2\log p/\log 2]).$$

LEMMA 2. *Suppose that every coset aQ of Q in F^* contains at most $t(1-1/\log p)$ elements b which satisfy $\|b\| < p/8k^{1/2}$. Then*

$$\gamma(k,p) < 17(\log p)^2 k^{1/2} < 68(\log k)^2 k^{1/2}.$$

Proof. Suppose $\|b\| \geqslant p/8k^{1/2}$. Then for any positive integer u,

$$\Big|\sum_{j=1}^{u} e(jb)\Big| = \Big|\frac{1-e(ub)}{1-e(b)}\Big| < \frac{2}{|\sin(\pi/4k^{1/2})|} < 4k^{1/2}.$$

Write

$$R_u = \{jq\colon 1 \leqslant j \leqslant u,\ q \in Q\},$$

where each element is included as often as it can be represented in the form jq. Thus each element in R_u is a sum of at most u kth powers (mod p) and the cardinality of the set is ut. Take $u = [8k^{1/2}]+1$. Then for any $a \not\equiv 0 \pmod p$ we have

$$\Big|\sum_{y\in R_u} e(ay)\Big| = \Big|\sum_{q\in Q}\sum_{j=1}^{u} e(jaq)\Big| \leqslant \sum_{b\in aQ}\Big|\sum_{j=1}^{u} e(jb)\Big|$$
$$< ut\Big(1-\frac{1}{\log p}\Big) + 4k^{1/2}\frac{t}{\log p} < ut\Big(1-\frac{1}{2\log p}\Big)$$

since $8k^{1/2} < u$.

For any integer A, let $N(A)$ be the number of solutions of the congruence

$$y_1+\ldots+y_r \equiv A \pmod p, \qquad y_j \in R_u.$$

Then

$$pN(A) = \sum_{y_1\in R_u}\ldots\sum_{y_r\in R_u}\sum_{a=0}^{p-1} e\big(a(y_1+\ldots+y_r-A)\big)$$
$$= \sum_{a=0}^{p-1} e(-aA)\prod_{j=1}^{r}\sum_{y_j\in R_u} e(ay_j) \geqslant (ut)^r - \sum_{a=1}^{p-1}\prod_{j=1}^{r}\Big|\sum_{y_j\in R_u} e(ay_j)\Big|$$
$$> (ut)^r\Big(1-(p-1)\Big(1-\frac{1}{2\log p}\Big)^r\Big) > 0$$

when $r > 2(\log p)^2$. Hence

$$\gamma(k,p) < 17(\log p)^2 k^{1/2} < 68(\log k)^2 k^{1/2}$$

if $k \geqslant 20$. The estimate $\gamma(k,p) \leqslant [\frac{1}{2}(k+4)]$ due to Chowla, Mann and Straus [4] implies that $\gamma(k) \leqslant 11$ for $k \leqslant 19$ and the lemma is proved.

LEMMA 3. *Let $k > 100$. Suppose that some coset aQ of Q in F^* contains at least $t(1-1/\log p)$ elements b with $\|b\| < p/8k^{1/2}$. Then aQ contains an element b_1 such that*

$$k^{1/2} < \|b_1\| < p/8k^{1/2}.$$

Proof. Let q be a generator of the cyclic group Q and let $\{b_1, \ldots, b_n\}$, where $n > t(1-1/\log p)$, be the subset of elements of aQ for which $\|b\| < p/8k^{1/2}$.

We assume that the conclusion of the lemma is false. It follows from this assumption that at most $t/\log p$ elements b in aQ satisfy $\|b\| > k^{1/2}$ and so for some b_1 in aQ we have

$$\|b_1 q^j\| \leqslant k^{1/2} \quad \text{for} \quad j = 0, 1, \ldots, [\log p]-1.$$

Now

$$b_1 \cdot b_1 q^2 \equiv (b_1 q)^2 \pmod p$$

and

$$\big|\|b_1\|\,\|b_1 q^2\| - \|b_1 q\|^2\big| \leqslant \|b_1\|\,\|b_1 q^2\| + \|b_1 q\|^2 \leqslant 2k < p$$

whence

$$\|b_1\|\,\|b_1 q^2\| = \|b_1 q\|^2,$$

i.e. there exist coprime positive integers c_1 and c_2 such that

$$\frac{\|b_1 q^2\|}{\|b_1 q\|} = \frac{\|b_1 q\|}{\|b_1\|} = \frac{c_2}{c_1}.$$

Moreover $c_1 \neq c_2$ since $t > 2$ implies $\|b_1 q\| \neq \|b_1\|$.

If we replace b_1 by $b_1 q$ and repeat the argument we get

$$\frac{\|b_1 q^3\|}{\|b_1 q^2\|} = \frac{\|b_1 q^2\|}{\|b_1 q\|} = \frac{c_2}{c_1},$$

and repeated application with $b_1 q$ replaced by $b_1 q^2$ and so on gives

$$\frac{\|b_1 q^{[\log p]-1}\|}{\|b_1 q^{[\log p]-2}\|} = \ldots = \frac{\|b_1 q^2\|}{\|b_1 q\|} = \frac{\|b_1 q\|}{\|b_1\|} = \frac{c_2}{c_1}.$$

Hence

$$\|b_1\| = (c_1/c_2)^{[\log p]-1}\,\|b_1 q^{[\log p]-1}\|$$

and so there exists a positive integer c_3 such that

$$\|b_1\| = c_3 c_1^{[\log p]-1} \quad \text{and} \quad \|b_1 q^{[\log p]-1}\| = c_3 c_2^{[\log p]-1}.$$

It follows that

$$\max\{\|b_1\|, \|b_1 q^{[\log p]-1}\|\} = c_3(\max\{c_1, c_2\})^{[\log p]-1} \geqslant 2^{[\log p]-1} > 2^{\log(3k)-2} > k^{1/2},$$

which is the desired contradiction.

LEMMA 4. *Suppose that some coset aQ of Q in F^* contains at least $t(1-1/\log p)$ elements b such that $\|b\| < p/8k^{1/2}$. Then*

$$\gamma(k,p) < 10(\log p)k^{1/2} < 20(\log k)k^{1/2}.$$

Proof. Because of the Chowla–Mann–Straus estimate [4] we may suppose that $k > 100$ and hence $p > 300$. Therefore $t(1-1/\log p) > 2$.

Let $b_1, \ldots, b_n$, where $n > t(1-1/\log p) > 2$, be those elements in aQ for which

$$|b_j| = \|b_j\| < p/8k^{1/2}.$$

We can assume without loss of generality that the greatest common divisor $(b_1, \ldots, b_n)$ of $b_1, \ldots, b_n$ is 1 and also that $|b_1| > k^{1/2}$ by the preceding lemma.

Consider the numbers of the form

$$m_1 b_1 + \ldots + m_n b_n \quad (0 \leqslant m_i < t_i), \tag{2}$$

where

$$t_n = \min\{k^{1/2}, (b_1, \ldots, b_{n-1})\}, \tag{3}$$

and where for each $i = n-1, \ldots, 2$,

$$t_i = \min\left\{\frac{k^{1/2}}{t_n \ldots t_{i+1}}, \frac{(b_1, \ldots, b_{i-1})}{(b_1, \ldots, b_i)}\right\}, \tag{4}$$

and

$$t_1 = 2k^{1/2}.$$

It is easily seen that $t_i \geqslant 1$ for all i and that t_i is integral except for at most one value of i, $n \geqslant i \geqslant 2$. For suppose that the greatest value of the suffix i for which t_i is not integral is j $(n \geqslant j \geqslant 2)$. Then

$$t_j = \frac{k^{1/2}}{t_n \ldots t_{j+1}}$$

and so

$$t_{j-1} = \min\left\{\frac{k^{1/2}}{t_n \ldots t_{j+1} t_j}, \frac{(b_1, \ldots, b_{j-1})}{(b_1, \ldots, b_j)}\right\} = 1.$$

It follows from (4) that $t_{j-2} = t_{j-3} = \ldots = t_2 = 1$.

$t_1t_2\ldots t_n = 2k$ whence there are at least $2k$ numbers of the form (2). These numbers are all incongruent (mod p), for if two were congruent (mod p), i.e. if

$$m_1b_1+\ldots+m_nb_n \equiv m_1'b_1+\ldots+m_n'b_n \pmod p,$$

then

$$(m_1-m_1')b_1+\ldots+(m_n-m_n')b_n \equiv 0 \pmod p.$$

But

$$|(m_1-m_1')b_1+\ldots+(m_n-m_n')b_n| \leqslant |m_1-m_1'|\,|b_1| + \max_{2\leqslant j\leqslant n}|b_j| \sum_{i=2}^{n} |m_i-m_i'|$$

$$< 2k^{1/2}\cdot\frac{p}{8k^{1/2}} + \frac{p}{8k^{1/2}}\Big(1+\sum_{i=2}^{n}(t_i-1)\Big),$$

since $|m_i-m_i'|\leqslant t_i-1$ except for at most one value of i. Hence

$$|(m_1-m_1')b_1+\ldots+(m_n-m_n')b_n| < \frac{p}{4}+\frac{p}{8k^{1/2}}+\frac{p}{8k^{1/2}}\prod_{i=2}^{n} t_i < p,$$

which implies that

$$(m_1-m_1')b_1+\ldots+(m_n-m_n')b_n = 0,$$

i.e.

(5) $$(m_1-m_1')b_1+\ldots+(m_{n-1}-m_{n-1}')b_{n-1} = (m_n'-m_n)b_n.$$

Now $(b_1, \ldots, b_{n-1})$ divides the left hand side and hence the right hand side of (5) and since $\big((b_1, \ldots, b_{n-1}), b_n\big) = (b_1, b_2, \ldots, b_n) = 1$, $(b_1, \ldots, b_{n-1})$ divides $m_n'-m_n$. But

$$|m_n'-m_n| < t_n = \min\{k^{1/2}, (b_1, \ldots, b_{n-1})\} \leqslant (b_1, \ldots, b_{n-1}),$$

whence $m_n = m_n'$ and

$$(m_1-m_1')b_1+\ldots+(m_{n-1}-m_{n-1}')b_{n-1} = 0.$$

We now proceed inductively and assume

(6) $$(m_1-m_1')b_1+\ldots+(m_{i-1}-m_{i-1}')b_{i-1}+(m_i-m_i')b_i = 0,$$

where $n-2\geqslant i\geqslant 2$. Then we get

(7) $$(m_1-m_1')b_1'+\ldots+(m_{i-1}-m_{i-1}')b_{i-1}' = (m_i'-m_i)b_i',$$

where for each $j = 1, \ldots, i$, $b_j = b_j'(b_1, \ldots, b_i)$. Plainly

$$\big((b_1', \ldots, b_{i-1}'), b_i'\big) = (b_1', \ldots, b_{i-1}', b_i') = 1$$

and so $(b_1', \ldots, b_{i-1}') = (b_1, \ldots, b_{i-1})/(b_1, \ldots, b_i)$ divides $|m_i-m_i'|$. But $|m_i-m_i'| < t_i \leqslant (b_1, \ldots, b_{i-1})/(b_1, \ldots, b_i)$, whence $m_i = m_i'$ and

$$(m_1-m_1')b_1+\ldots+(m_{i-1}-m_{i-1}')b_{i-1} = 0.$$

Thus it follows that for $i = n, \ldots, 1$, $m_i = m_i'$, which implies that the numbers (2) are all incongruent (mod p) and so indeed represent at least $2k$ distinct residues (mod p).

Since for each $i = 1, \ldots, n$, $b_i \in aQ$, there exist n kth power residues (mod p), $q_1, \ldots, q_n$, say such that

$$b_i \equiv aq_i \pmod p$$

for $i = 1, \ldots, n$. Consequently the expression

$$m_1q_1+\ldots+m_nq_n, \quad 0\leqslant m_i < t_i,$$

which is a sum of at most $3k^{1/2}$ kth power residues (mod p), represents at least $2k$ distinct residues (mod p). Hence by Lemma 1,

$$\gamma(k, p) \leqslant 3k^{1/2}(1+[2\log p/\log 2]) < 10k^{1/2}\log p < 20k^{1/2}\log k,$$

and so Lemma 4 is proved.

Since the hypothesis of either Lemma 2 or Lemma 4 must hold, we obtain

THEOREM 1. *For all k we have*

$$\gamma(k) < 68(\log k)^2 k^{1/2}.$$

Hence given any positive ε,

$$\gamma(k) = O(k^{1/2+\varepsilon}).$$

4. Other theorems. As we have remarked Theorem 1 is almost best possible and we have

THEOREM 2. *There are infinitely many k for which*

$$\gamma(k) \geqslant \tfrac{1}{2}(\sqrt{3k}-1).$$

Proof. Since there is an infinity of primes of the form $1+3k$, it suffices to show that

$$\gamma(k, 1+3k) \geqslant \tfrac{1}{2}(\sqrt{3k}-1).$$

Let $p = 1+3k$. The number of kth power residues (mod p) is $t = (p-1)/k = 3$ and since their sum is congruent to $0 \pmod p$, we can take $Q = \{1, a, -1-a\}$. Then

$$Q_w = \{x+ya+z(-1-a)\colon\ 0\leqslant x+y+z\leqslant w\}$$
$$= \{x-z+(y-z)a\colon\ 0\leqslant x+y+z\leqslant w\}$$
$$\subset \{u+va\colon\ -w\leqslant u, v\leqslant w\}.$$

The cardinality of the latter set is $\leqslant (2w+1)^2$, whence

$$Q_w \neq \mathrm{GF}(p) \quad \text{if} \quad w < \tfrac{1}{2}(\sqrt{3k}-1) < \tfrac{1}{2}(p^{1/2}-1)$$

and the theorem follows.

In conclusion we remark that Theorems 1 and 2 can be extended to the p-adic case. We have

THEOREM 3. *Given any positive* ε,

$$\max_p\{\Gamma_p(k):\ d<\tfrac{1}{2}(p-1)\}=O(k^{1/2+\varepsilon}).$$

This theorem follows immediately by combining our Theorem 1 with Theorems 1 and 2 in Bovey's paper [1].

As in the (mod p) case, this result is close to best possible as the following theorem, which is similar to Theorem 2, shows

THEOREM 4. *There are infinitely many* k *for which*

$$\max_p\{\Gamma_p(k):\ d<\tfrac{1}{2}(p-1)\}\geqslant\tfrac{1}{2}(\sqrt{3k}-1).$$

Proof. Let p be a prime and congruent to 1 (mod 3). Then there are infinitely many integers k of the form $p^m(p-1)/3$. Also there are just 3 nonzero kth power residues (mod p^{m+1}), including 1, and their sum is congruent to 0 (mod p^{m+1}), so that we can write them 1, a and $-1-a$ (mod p^{m+1}). The form

$$x_1^k+\ldots+x_s^k,\quad \text{where}\quad s<\tfrac{1}{2}(\sqrt{3k}-1),$$

is therefore congruent to the expression

$$u+va+w(-1-a)\ (\text{mod}\ p^{m+1}),\quad \text{where}\quad 0\leqslant u+v+w\leqslant s,$$

i.e. to

$$(u-w)+(v-w)a\ (\text{mod}\ p^{m+1}),\quad \text{where}\quad -s\leqslant u-w,\ v-w\leqslant s.$$

Since $(2s+1)^2<3k<p^{m+1}$, the form cannot represent every residue (mod p^{m+1}), whence $\Gamma_p(k)\geqslant\frac{1}{2}(\sqrt{3k}-1)$.

References

[1] J. D. Bovey, *A note on Waring's problem in p-adic fields*, Acta Arith. 29 (1976), pp. 343–351.

[2] — *On the congruence* $a_1x_1^k+\ldots+a_sx_s^k\equiv N\,(\text{mod}\,p^n)$, Acta Arith. 23 (1973), pp. 257–269.

[3] I. Chowla, *On Waring's problem* (mod p), Proc. Indian Nat. Acad. Sci. A 13 (1943), pp. 195–220.

[4] S. Chowla, H. B. Mann and E. G. Straus, *Some applications of the Cauchy–Davenport theorem*, Norske Vid. Selsk. Forh. (Trondheim) 32 (1959), pp. 74–80.

[5] M. M. Dodson, *On Waring's problem in* GF[p], Acta Arith. 19 (1971), pp. 147–173.

[6] H. Heilbronn, *Lecture notes on additive number theory* mod p, California Institute of Technology, 1964.

[7] A. Tietäväinen, *Note on Waring's problem* (mod p), Ann. Acad. Sci. Fenn. A I 554 (1973).

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF YORK
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TURKU

Received on 23. 9. 1974 (622)