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

\[ |S(T') - S(T)| < B + \Delta \psi_1(T) < \Lambda \psi_1(T) = \psi(T). \]

На этом доказательство закончено.

**Литература**


Поступило 9. 9. 1974
по исправлению 2. 12. 1974

---

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

by

M. M. DODSON (York) and A. TIEŤĂVĂINEN (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 \( s \) \( k \)th power residues \( (mod \ p) \). In other words, if \( s \geq \gamma(k, p) \), the congruence

\[ a_1^k + \ldots + a_s^k = N \quad (mod \ p) \]

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

\[ \gamma(k, p) = \gamma(d, p) \]

and that

\[ \gamma(p - 1, p) = p - 1, \quad \gamma(\lfloor (p - 1)/2 \rfloor, p) = \lfloor (p - 1)/2 \rfloor, \]

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

\[ \gamma(k) = \max_{\gamma(k, p)} \gamma(k, p): d < \lfloor (p - 1)/2 \rfloor. \]

In 1943 I. Chowla [3] proved that

\[ \gamma(k) = O(k^{\alpha - \epsilon}) \]

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

\[ \gamma(k) < k^{1/6} \]

providing \( k \) is sufficiently large and in 1973 Tietāvāniņa [7] showed that

\[ \gamma(k) = O(k^{\alpha - \epsilon}). \]

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

\[ \gamma(k, p) \leq \Gamma(k, p) \leq \gamma(k, p) + 1 \]
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 \( \varepsilon \),
\[
\gamma(k) = O(k^{1/2 + \varepsilon})
\]
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 \( k \) in \( \frac{1}{2} \), i.e. if \( a < \frac{1}{2} \), then
\[
\gamma(k) = O(k^a).
\]
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 \( \mathbb{Q}_p \) by sums of \( k \)th 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 \( s \) \( k \)th 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 \( \gamma(k, p) = \gamma(\phi, p) \) we may suppose that \( k \) divides \( p - 1 \) and since we are concerned only with the case \( \phi < \frac{1}{2}(p - 1) \), we can suppose further that
\[
k \leq \frac{(p - 1)}{3}.
\]
If \( p > k^2 \) then it has been shown ([5], p. 151) that
\[
\gamma(k, p) \leq \max\{3, (32 \log k)^{1/2} + 1\},
\]
so that we can take \( p < k^2 \) from now on without loss of generality.

Let \( Q \) be the set of \( t \) nonzero \( k \)th power residues \( (\text{mod} \ p) \) so that \( Q \) is a subgroup of the multiplicative group \( \mathbb{F}^* = \mathbb{GF}(p) - \{0\} \) of nonzero residues \( (\text{mod} \ p) \). Let \( Q_n \) be the set of those residues \( (\text{mod} \ p) \) which can be represented as the sum of \( n \) \( k \)th power residues \( (\text{mod} \ p) \) and let \( q_n \) be the cardinality of \( Q_n \).

For any integer \( a \), we denote by \( \|a\| \) the absolute value of the residue of \( a \) \( (\text{mod} \ p) \) which has least absolute value. Also we define
\[
o(a) = e^{\text{int} a/p}.
\]

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 hypotheses and Lemma 1 (which is Lemma 2 of [7]) and Lemma 3 are needed in the proof of Lemma 4.

Lemma 1. If \( q_n \geq 2k \) then
\[
\gamma(k, p) \leq w(1 + [2 \log p \log 2])/w).
\]

Lemma 2. Suppose that every coset \( aQ \) of \( Q \) in \( \mathbb{F}^* \) contains at most \( t(1 - 1/\log p) \) elements \( b \) which satisfy \( |b| < p/3k^{12} \). Then
\[
\gamma(k, p) < 17(\log p)^2 k^{12} < 68(\log k)^2 k^{12}.
\]

Proof. Suppose \( |b| > p/3k^{12} \). Then for any positive integer \( u \),
\[
\left| \sum_{j=1}^u e(jb) \right| = \left| \frac{1 - e(ub)}{1 - e(b)} \right| < \frac{2}{|\min(\pi/4k^{12})|} < 4k^{12}.
\]
Write
\[
R_u = \{jq: 1 \leq j \leq u, q \in Q \},
\]
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 \( u \) \( k \)th powers (\( \text{mod} \ p \)) and the cardinality of the set is \( ut \). Take \( u = [8k^{12}] + 1 \). Then for any \( a \equiv 0 \ (\text{mod} \ p) \) we have
\[
\left| \sum_{v \in R_u} e(ay) \right| = \left| \sum_{v \in R_u} e(jaq) \right| = \left| \sum_{j=1}^u \sum_{a=1}^u e(jb) \right| < ut \left( 1 - \frac{1}{\log p} \right) + 4k^{12} \frac{t}{\log p} < ut \left( 1 - \frac{1}{2 \log p} \right)
\]
since \( 8k^{12} < u \).

For any integer \( A \), let \( N(A) \) be the number of solutions of the congruence
\[
y_1 + \ldots + y_r = A \ (\text{mod} \ p), \quad y_j \in R_u.
\]
Then
\[
g_N(A) = \sum_{y_1 \in R_u} \ldots \sum_{y_r \in R_u} \sum_{a=0}^{p-1} e(a(y_1 + \ldots + y_r - A)) = \sum_{a=0}^{p-1} e(-aA) \prod_{j=1}^r \sum_{y \in R_u} e(a y_j)
\]
\[
> (ut)^r \left( 1 - (p - 1) \left( 1 - \frac{1}{2 \log p} \right) \right) > 0
\]
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 \( k \geq 20 \). The estimate \( \gamma(k, p) \leq [\frac{1}{2} (k+4)] \) due to Chowla, Mann and Straus [4] implies that \( \gamma(k) \leq 11 \) for \( k \leq 19 \) and the lemma is proved.

**Lemma 3.** Let \( k > 100 \). Suppose that some coset \( aQ \) of \( Q \in \mathbb{F}^n \) 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

\[
|b_1| < \sqrt[4]{2k} < p/8k^{1/2}.
\]

**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 \( |b| > 2k^{1/2} \) and so for some \( b_1 \) in \( aQ \) we have

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

Now

\[
b_1 q = (b_1 q)^2 \pmod{p}
\]

and

\[
|b_1^2 b_1 q^3 - |b_1^2 q^3| |b_1| (|b_1| - 1) \leq 2k p.
\]

whence

\[
|b_1| |b_1^2 q^3| \leq 2k^2 < p
\]

i.e. there exist coprime positive integers \( c_1 \) and \( c_4 \) such that

\[
\frac{|b_1^2 q^3|}{|b_1^2 q^3|} = \frac{|b_1 q^3|}{|b_1 q^3|} = \frac{c_4}{c_1}.
\]

Moreover \( c_1 \neq c_4 \) since \( t > 2 \) implies \( |b_1 q^3| \neq |b_1 q^3| \).

If we replace \( b_1 \) by \( b_1 q \) and repeat the argument we get

\[
\frac{|b_1^2 q^3|}{|b_1^2 q^3|} = \frac{|b_1 q^3|}{|b_1 q^3|} = \frac{c_4}{c_1}.
\]

and repeated application with \( b_1 q \) replaced by \( b_1 q^3 \) and so on gives

\[
\frac{|b_1^2 q^3|}{|b_1^2 q^3|} = \cdots = \frac{|b_1 q^3|}{|b_1 q^3|} = \frac{c_4}{c_1}.
\]

Hence

\[
|b_1| = (c_1/c_4)^{\lfloor \log p \rfloor - 1} |b_1^2 q^3|^{\lfloor \log p \rfloor - 1}.
\]

and so there exists a positive integer \( c_5 \) such that

\[
|b_1| = c_5 |b_1^2 q^3|^{-1} \quad \text{and} \quad |b_1^2 q^3|^{11} = c_5^{11} q^{11}.\]
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 \( i = 1, \ldots, n, b_i \in Q, \) there exist \( n \) \( k \)th power residues (mod p), \( q_1, \ldots, q_n, \) say such that

\[ b_i = aq_i \text{ (mod p)} \]

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

\[ m_1q_1 + \ldots + m_nq_n, \quad 0 \leq m_i < t_i, \]

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

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

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

\[ \gamma(k) < 6k(\log k)^2 k^{1/2}. \]

Hence given any positive \( \epsilon, \)

\[ \gamma(k) = O(k^{1/2+\epsilon}). \]

**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

\[ \gamma(k) > \frac{1}{2}(\sqrt{3}k - 1). \]

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

\[ \gamma(k, 1 + 3k) > \frac{1}{2}(\sqrt{3}k - 1). \]

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

\[ Q_w = \{ x + ya + s(-1 - a); \quad 0 \leq s + y + s \leq w \} = \{ x + s + (y - a); \quad 0 \leq x + y + z \leq w \} \subset \{ u + va; \quad -w \leq u, v \leq w \}. \]

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

\[ Q_w \neq \text{GF(p)} \quad \text{if} \quad w < \frac{1}{2}(\sqrt{3}k - 1) < \frac{1}{2}(p^{1/2} - 1) \]

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 e,

\[
\max_p \{ I_p(k) : d < \frac{1}{2}(p - 1) \} = O(k^{1+\epsilon}).
\]

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

\[
\max_p \{ I_p(k) : d < \frac{1}{2}(p - 1) \} > \frac{1}{3}(\sqrt{3k} - 1).
\]

**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

\[a_1^s + \ldots + a_r^s, \text{ where } s < \frac{1}{3}(\sqrt{3k} - 1),\]

is therefore congruent to the expression

\[u + va + w(-1-a) \text{ (mod } p^{m+1})\],

where \(0 \leq u + v + w \leq s\),

i.e. to

\[(u-w)+(v-w)a \text{ (mod } p^{m+1})\],

where \(-s \leq u-w, v-w \leq s\).

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

References


[2] — *On the congruence \( a_1x_1^s + \ldots + a_rx_r^s = N \) (mod p)*, Acta Arith. 23 (1973), pp. 257-268.
