NOTE ON WARING'S PROBLEM (mod p)

BY

AIMO TIEÄVÄINEN

HELSINKI 1973
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1973.554
Communicated 14 May 1973 by K. Inkere
Note on Waring’s Problem (mod p)

1. Introduction. Let \( p \) be a prime, \( k \) a positive integer and \( d \) the highest common factor of \( k \) and \( p - 1 \). Let \( \gamma(k, p) \) denote the least positive integer \( s \) such that every residue (mod \( p \)) is representable as a sum of \( s k \)th power residues (mod \( p \)). It is well known [6] that

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

and

\[
\gamma(p - 1, p) = p - 1, \quad \gamma(\frac{1}{2}(p - 1), p) = \frac{1}{2}(p - 1).
\]

Put

\[
\gamma(k) = \max \{ \gamma(k, p) : d < \frac{1}{2}(p - 1) \}.
\]

S. Chowla, Mann and Straus [2] showed in 1959 that

\[
\gamma(k) \leq \left[ \frac{1}{4}(k + 4) \right].
\]

Much earlier, in 1943, I. Chowla [1] had proved the result

(1) \[
\gamma(k) = O(k^{1-\epsilon+\epsilon'})
\]

where \( \epsilon = (103 - 3\sqrt{641})/220 \) and, as always in this paper, \( \epsilon \) is a positive number. Recently Dodson [5] improved (1) to the simpler result

\[
\gamma(k) < k^{7.6},
\]

provided \( k \) is sufficiently large. The purpose of this note is to show that

(2) \[
\gamma(k) = O(k^{3.5+\epsilon}).
\]

It is very probable that (2) is not best possible, and it would be desirable to reduce the exponent to \( \epsilon \) or, at least, to \( \frac{1}{2} + \epsilon \) (cf. [7] and [5]).

2. Preliminary results. Dodson ([5], p. 151) has shown that if \( p > d^2 \) then

\[
\gamma(k, p) \leq \max \{ 3, \lfloor 32 \log d \rfloor + 1 \}.
\]

Therefore we may suppose that
(3) \[ p \leq d^2. \]

Let \( Q_w \) be the set of those distinct residues \((\text{mod } p)\) which can be represented as the sum of \( w \) \( k \)-th power residues \((\text{mod } p)\), and let \( q_w \) be the number of the elements in \( Q_w \). Put

\[ e(x) = e^{2\pi ix/p}, \quad S_w(u) = \sum_{\gamma} e(u\gamma), \quad M_w = \max \{|S_w(u)| : u \equiv 0 \pmod{p}\} \]

where the sum \( \sum^* \) is over all the elements of \( Q_w \). Then ([8], Lemma 1)

\[ M_w < (qwd)^{1/2}. \]

3. The main lemmas.

**Lemma 1** (Cauchy-Davenport Theorem; see [3] and [4]). Let \( \alpha_1, \ldots, \alpha_m \) be \( m \) different residue classes \((\text{mod } p)\); let \( \beta_1, \ldots, \beta_n \) be \( n \) different residue classes \((\text{mod } p)\). Let \( \gamma_1, \ldots, \gamma_n \) be all those different residue classes which are representable as

\[ \alpha_i + \beta_j \quad (1 \leq i \leq m, 1 \leq j \leq n). \]

Then \( h \geq \min \{p, m + n - 1\} \).

**Lemma 2** (cf. [8], Lemma 2). If \( q_w \geq 2d \) then \( \gamma(k, p) \leq w(1 + [2 \log p/\log 2]) \).

**Proof.** Put \( r = 1 + [2 \log p/\log 2] \). Let \( a \) be any integer, and let \( N = N(a) \) be the number of solutions of

\[ y_1 + \ldots + y_r \equiv a \pmod{p}, \quad y_i \in Q_w. \]

Then

\[ pN = \sum_{\gamma_1} \ldots \sum_{\gamma_r} \sum_{u=0}^{p-1} e(u(y_1 + \ldots + y_r - a)) \]

\[ = \sum_{u=0}^{p-1} (S_w(u))^r e(-ua) \]

\[ = q_w^r + \sum_{u=1}^{p-1} (S_w(u))^r e(-ua) \]

\[ \geq q_w^r - (p - 1)M_w. \]

Hence, by the inequalities \( M_w < (qwd)^{1/2}, \quad q_w/d \geq 2 \) and \( r/2 > \log p/\log 2 \), we get
\[ N > p^{-1}(q_u d)^{r/2}(q_u d d d - p + 1) \]
\[ \geq p^{-1}(q_u d)^{r/2}(2^{2^2} - p + 1) > 0. \]

**Lemma 3.** If \( d < \frac{1}{2}(p - 1) \) and \( w \geq 100d^{3/5} \) then \( q_u \geq 2d \).

**Proof** (which is very similar to that of Lemma 2 of [5]). Clearly \( q_u > 2w \). Hence in case \( d \leq 100000 \) the assumption \( w \geq 100d^{3/5} \) implies \( q_u \geq 2d \). Consequently we may suppose that \( d > 100000 \).

Let \( R \) be a nonzero \( k \)th power residue which is not congruent to \( \pm 1 \) (mod \( p \)). It is known ([5], p. 151; [1]) that then there exist integers \( x \) and \( y \) satisfying
\[ R \equiv xy^{-1} \text{ (mod } p) , 1 \leq y < |x| < p^{1/2} , (x , y) \leq 1 . \]

Consider now three separate cases:

(i) \[ d^{2/5} \leq |x| < p^{1/2} \]

(ii) \[ d^{1/5} \leq |x| < d^{2/5} \]

(iii) \[ 1 < |x| < d^{1/5} . \]

As in Dodson’s paper [5] we may see that in case (i) the numbers of the form
\[ m + nR \ (0 \leq m , n < \frac{1}{2}d^{2/5}) \]
generate at least \( d^{3/5}/4 \) integers which are incongruent (mod \( p \)). Moreover each of these numbers is a sum of at most \( d^{2/5} \) \( k \)th powers (mod \( p \)). Hence, by Lemma 1, the expression
\[ m_1 + n_1 R + \ldots + m_r + n_r R \ (0 \leq m , n < \frac{1}{2}d^{2/5}) \]
which is a sum of at most \( rd^{2/5} \) \( k \)th powers (mod \( p \)) represents at least \( \min \{ p , rd^{2/5}/4 - r + 1 \} \) residues (mod \( p \)). Setting \( r = \lfloor 100d^{1/5} \rfloor \) we get the lemma.

In case (ii) we may show, as Dodson in [5], that the numbers
\[ h + mR + nR^2 \ (0 \leq h , m , n < d^{1/5}/3) \]
are incongruent (mod \( p \)). Hence, by Lemma 1, the expression
\[ h_1 + m_1 R + n_1 R^2 + \ldots + h_r + m_r R + n_r R^2 \ (0 \leq h_i , m_i , n_i < d^{1/5}/3) \]
which is a sum of at most \( rd^{1/5} \) \( k \)th powers (mod \( p \)) represents at least \( \min \{ p , rd^{1/5}/27 - r + 1 \} \) residues (mod \( p \)). Putting \( r = \lfloor 100d^{2/5} \rfloor \) we get the desired result.
Also in case (iii) we adopt the method of [5] and choose an integer $f$ such that
\[ d^{2/5} \leq |x|^f < d^{3/5}. \]

Thus
\[ R^f = x^f y^{-f} \pmod{p} \]

where \((x^f, y^f) = 1, 1 \leq y^f < |x|^f \) and \( R^f \equiv \pm 1 \pmod{p} \). Moreover (cf. [5], pp. 153–154) the numbers
\[ m + nR^f (0 \leq m, n < \frac{1}{2}d^{2/5}) \]

form at least \( d^{4/5}/4 \) distinct residues \( \pmod{p} \), each number being the sum of at most \( d^{2/5} \) \( k \)th powers \( \pmod{p} \). The result now follows as in case (i).

4. Proof of (2). Lemma 3 implies that \( q_w \geq 2d \) if \( w \geq 100d^{3/5} \). It follows from this and Lemma 2 that
\[ \gamma(k, p) < (1 + 100d^{3/5})(1 + 2 \log p/\log 2). \]

Since we assumed in (3) that \( p \leq d^2 \), the inequality (4) implies
\[ \gamma(k, p) < (1 + 100d^{3/5})(1 + 4 \log d/\log 2) = O(k^{3/5 + \epsilon}). \]

University of Turku
Turku, Finland
References


Printed September 1973