ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

554

NOTE ON WARING'S PROBLEM (mod p)

BY

AIMO TIETÄVÄINEN

HELSINKI 1973
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1973.554

ISBN 951-41-0131-6

Communicated 14 May 1973 by K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1973

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 $(\operatorname{mod} p)$ is representable as a sum of s kth power residues $(\operatorname{mod} p)$. It is well known [6] that

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

and

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

Put

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

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

$$\gamma(k) \leqq [\tfrac{1}{2}(k+4)].$$

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

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

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

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

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

$$\gamma(k) = O(k^{3/5+\varepsilon}). \tag{2}$$

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

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

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

Therefore we may suppose that

$$p \leqq d^2 . \tag{3}$$

Let Q_w be the set of those distinct residues $(\bmod\, p)$ which can be represented as the sum of w kth power residues $(\bmod\, p)$, and let q_w be the number of the elements in Q_w. Put

$$e(x) = e^{2\pi i x/p}\ ,\ S_w(u) = \sum_y{}^{*} e(uy)\ ,\ M_w = \max\{|S_w(u)| : u \not\equiv 0 \ (\bmod\, p)\}$$

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

$$M_w < (q_w d)^{1/2} .$$

3. The main lemmas.

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

$$\alpha_i + \beta_j \quad (1 \leqq i \leqq m\ ,\ 1 \leqq j \leqq n) .$$

Then $h \geqq \min\{p\ ,\ m + n - 1\}$.

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

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

$$y_1 + \ldots + y_r \equiv a \quad (\bmod\, p)\ ,\ y_i \in Q_w .$$

Then

$$\begin{aligned} pN &= \sum_{y_1}{}^{*} \ldots \sum_{y_r}{}^{*} \sum_{u=0}^{p-1} e(u(y_1 + \ldots + y_r - a)) \\ &= \sum_{u=0}^{p-1} (S_w(u))^r e(-ua) \\ &= q_w^r + \sum_{u=1}^{p-1} (S_w(u))^r e(-ua) \\ &\geqq q_w^r - (p-1) M_w^r . \end{aligned}$$

Hence, by the inequalities $M_w < (q_w d)^{\frac{1}{2}}$, $q_w/d \geqq 2$ and $r/2 > \log p/\log 2$, we get

$$
\begin{aligned}
N &> p^{-1}(q_w d)^{r/2}((q_w/d)^{r/2} - p + 1) \\
&\geqq p^{-1}(q_w d)^{r/2}(2^{r/2} - p + 1) > 0 .
\end{aligned}
$$

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

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

Let R be a nonzero kth power residue which is not congruent to $\pm 1 \pmod p$. It is known ([5], p. 151; [1]) that then there exist integers x and y satisfying

$$R \equiv xy^{-1} \pmod p , \quad 1 \leqq y < |x| < p^{\frac{1}{2}} , \quad (x , y) \leqq 1 .$$

Consider now three separate cases:

(i) $$d^{2/5} \leqq |x| < p^{1/2}$$

(ii) $$d^{1/5} \leqq |x| < d^{2/5}$$

(iii) $$1 < |x| < d^{1/5} .$$

As in Dodson's paper [5] we may see that in case (i) the numbers of the form

$$m + nR \quad (0 \leqq m , n < \tfrac{1}{2}d^{2/5})$$

generate at least $d^{4/5}/4$ integers which are incongruent $\pmod p$. Moreover each of these numbers is a sum of at most $d^{2/5}$ kth powers $\pmod p$. Hence, by Lemma 1, the expression

$$m_1 + n_1R + \ldots + m_r + n_rR \quad (0 \leqq m , n < \tfrac{1}{2}d^{2/5})$$

which is a sum of at most $rd^{2/5}$ kth powers $\pmod p$ represents at least $\min\{p , rd^{4/5}/4 - r + 1\}$ residues $\pmod p$. Setting $r = [100d^{1/5}]$ we get the lemma.

In case (ii) we may show, as Dodson in [5], that the numbers

$$h + mR + nR^2 \quad (0 \leqq h , m , n < d^{1/5}/3)$$

are incongruent $\pmod p$. Hence, by Lemma 1, the expression

$$h_1 + m_1R + n_1R^2 + \ldots + h_r + m_rR + n_rR^2 \quad (0 \leqq h_i , m_i , n_i < d^{1/5}/3)$$

which is a sum of at most $rd^{1/5}$ kth powers $\pmod p$ represents at least $\min\{p , rd^{3/5}/27 - r + 1\}$ residues $\pmod p$. Putting $r = [100d^{2/5}]$ we get the desired result.

Also in case (iii) we adopt the method of [5] and choose an integer f such that

$$d^{2/5} \leqq |x|^f < d^{3/5} .$$

Thus

$$R^f \equiv x^f y^{-f} \pmod{p}$$

where $(x^f , y^f) = 1$, $1 \leqq y^f < |x|^f$ and $R^f \not\equiv \pm 1 \pmod{p}$. Moreover (cf. [5], pp. 153—154) the numbers

$$m + nR^f \quad (0 \leqq m , n < \tfrac{1}{2}d^{2/5})$$

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

4. Proof of (2). Lemma 3 implies that $q_w \geqq 2d$ if $w \geqq 100d^{3/5}$. It follows from this and Lemma 2 that

$$\gamma(k , p) < (1 + 100d^{3/5})(1 + 2 \log p/\log 2) . \tag{4}$$

Since we assumed in (3) that $p \leqq d^2$, the inequality (4) implies

$$\gamma(k , p) < (1 + 100d^{3/5})(1 + 4 \log d/\log 2) = O(k^{3/5+\varepsilon}) .$$

University of Turku
Turku, Finland

References

[1] CHOWLA, I.: On Waring's Problem (mod p). - Proc. Indian Nat. Acad. Sci. A 13 (1943), 195–220.

[2] CHOWLA, S. — MANN, H. B. — STRAUS, E. G.: Some Applications of the Cauchy-Davenport Theorem. - Norske Vid. Selsk. Forh. (Trondheim) 32 (1959), 74–80.

[3] DAVENPORT, H.: On the Addition of Residue Classes. - J. London Math. Soc. 10 (1935), 30–32.

[4] —»— A Historical Note. - J. London Math. Soc. 22 (1947), 100–107.

[5] DODSON, M.: On Waring's Problem in $GF(p)$. - Acta Arithmetica XIX (1971), 147–173.

[6] HARDY, G. H. — LITTLEWOOD, J. E.: Some Problems of 'Partitio Numerorum': VIII. The Number $\Gamma(k)$ in Waring's Problem. - Proc. London Math. Soc. 28 (1927), 518–542.

[7] HEILBRONN, H.: Lecture Notes on Additive Number Theory mod p . California Institute of Technology, 1964.

[8] TIETÄVÄINEN, A.: Proof of a Conjecture of S. Chowla. - J. Number Theory (to appear).

Printed September 1973