If $a \geqslant 2$, *then as* $x \to \infty$,

$$N\big(n \leqslant x\colon\ 2^a \nmid \sigma_\nu(n, \chi)\big) \sim B_2 x (\log\log x)^{a-2} (\log x)^{-1},$$

where $B_2 > 0$.

From Theorem 1 of [10], it follows that in fact

$$B_2 = \frac{\pi^2}{2^{a+1}(a-2)!} \prod_{p|Q} \frac{p+1}{p},$$

where Q is defined by (37) with $d = 2^a$, and furthermore that

$$N\big(n \leqslant x\colon\ 2 \nmid \sigma_\nu(n, \chi)\big) \sim \prod_{p|2Q} (1+p^{-1/2}) x^{1/2}.$$

References

[1] E. Cohen, *Arithmetical functions associated with the unitary divisors of an integer*, Math. Zeitschr. 74 (1960), pp. 66–80.

[2] H. Delange, *Sur la distribution des entiers ayant certaines propriétés*, Ann. Sci. École Norm. Sup. (3) 73 (1956), pp. 15–74.

[3] P. Erdös und G. Szekeres, *Über die Anzahl der abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem*, Acta Scientiarum Mathematicarum, Szeged, 7 (1934), pp. 95–102.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 3rd ed., Oxford 1954.

[5] W. Narkiewicz, *Divisibility properties of a class of multiplicative functions*, Colloq. Math. 18 (1967), pp. 219–232.

[6] — *Divisibility properties of some multiplicative functions*, Colloquia Mathematica Societatis János Bolyai, 2. Number Theory, edited by P. Turán, Debrecen (Hungary) 1968, pp. 147–159.

[7] R. A. Rankin, *The divisibility of divisor function*, Proc. Glasgow Math. Assoc. 5 (1961), pp. 35–40.

[8] L. G. Sathe, *On a congruence property of the divisor functions*, Amer. J. Math. 67 (1945), pp. 397–406.

[9] E. J. Scourfield, *On the divisibility of* $\sigma_\nu(n)$, Acta Arith. 10 (1964), pp. 245–285.

[10] — *On the divisibility of a modified divisor function*, Proc. London Math. Soc. (3) 21 (1970), pp. 145–159.

[11] G. N. Watson, *Über Ramanujansche Kongruenzeigenschaften der Zerfällungsanzahlen (I)*, Math. Zeitschr. 39 (1935), pp. 712–731.

WESTFIELD COLLEGE
London NW3 7ST

Received on 13. 11. 1971 (238)

ACTA ARITHMETICA
XXII (1973)

On Waring's Problem in p-adic fields

by

M. M. Dodson (Heslington)

In this paper, which is a sequel to [5], we show that for a large enough exponent k, any p-adic integer can be represented non-trivially as a sum of less than $k^{7/8}$ kth powers of integers in any p-adic field Q_p with $(k, p-1) < \frac{1}{2}(p-1)$. As is well known the problem of representing any p-adic integer by a sum of s kth powers of p-adic integers is equivalent to finding a primitive solution of the congruence

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

for any rational integer N, where $\gamma = \tau+1$ and where τ is the exact power of the prime p which divides $2k$. In fact, as is also well known, a primitive solution of (1) implies that the congruence

$$x_1^k + \ldots + x_s^k \equiv N \pmod{p^n} \tag{2}$$

has a primitive solution for every integer $n \geqslant 1$. The number $\Gamma(k, p^n)$ is defined to be the least s such that the congruence (2) has a primitive solution for any integer N so that $\Gamma(k, p^n) \leqslant \Gamma(k, p^\gamma)$ for every $n \geqslant 1$, i.e.

$$\Gamma(k, p^\gamma) = \operatorname*{Max}_{n} \Gamma(k, p^n),$$

where the maximum is taken over all positive integers. Also plainly if $s \geqslant \Gamma(k, p^\gamma)$ then every p-adic integer can be represented as a non-trivial sum of s kth powers of p-adic integers.

The number $\Gamma(k, p^\gamma)$ was introduced by Hardy and Littlewood in their work on Waring's Problem ([7]) though from a different point of view and with a different notation, namely γ_p, and they proved ([8], p. 533, Theorem 4) that if $d < \frac{1}{2}(p-1)$ then $\Gamma(k, p^\gamma) \leqslant k$, where as always $d = (k, p-1)$, the highest common factor of k and $p-1$. I. Chowla ([3], p. 197, Theorem 4) showed that if k is sufficiently large, then for all primes p with $d < \frac{1}{2}(p-1)$ we have for all sufficiently large k,

$$\Gamma(k, p^\gamma) < k^{1-c+\varepsilon},$$

i.e. for all integers $n \geqslant 1$,

$$\Gamma(k, p^n) < k^{1-c+\varepsilon},$$

where ε is any positive number and $c = (103 - 3\sqrt{641})/220$, a result which for large k is much stronger than Hardy and Littlewood's.

Now in [5] where we considered the solubility of the congruence (2) with $n = 1$, we proved(¹) that if k were sufficiently large and $d < \frac{1}{2}(p-1)$ then

$$\Gamma(k, p) < k^{7/8-\eta} < k^{7/8}$$

where η is, as always in this paper, a sufficiently small positive number. Here we prove under the same hypotheses that

$$\Gamma(k, p^{\gamma}) < k^{7/8}, \quad \text{i.e.} \quad \Gamma(k, p^{n}) < k^{7/8}$$

for all positive integers n.

Of course if the odd prime p does not divide k then $\gamma = 1$ and $\Gamma(k, p^n) \leqslant \Gamma(k, p)$ for all positive integers n, so that here we are really only concerned with those primes which divide k. The arguments and results we use are in the main due to I. Chowla [3] and we simply verify that the improvement obtained in [5] can be maintained in the p-adic case when the prime p divides k. However as we have pointed out in [5], I. Chowla's paper is not easily obtainable and contains numerous misprints and obscurities and for these reasons and to keep this paper reasonably self-contained we repeat his work in some detail.

From now on we shall take k to be a sufficiently large positive integer and p to be a prime dividing k (so that $\tau \geqslant 1$) and such that $d = (k, p-1) < \frac{1}{2}(p-1)$ so that p is necessarily at least 5 and p^{τ} exactly divides k. The cases $d = p-1$ and $d = \frac{1}{2}(p-1)$ are exceptional in that $\Gamma(k, p^{\gamma}) = \Gamma(k, p^{\tau+1})$ can be determined in these cases and that in general the results of this paper cannot hold ([8], p. 524, Lemma 7). For example when $k = p^{\tau}(p-1)$, $p > 2$, then

$$\Gamma(k, p^{\tau+1}) = p^{\tau+1} = \frac{p}{p-1}\cdot k$$

and if $k = p^{\tau}\left(\frac{p-1}{2}\right), p > 3$, then

$$\Gamma(k, p^{\tau+1}) = \tfrac{1}{2}(p^{\tau+1}-1) = \frac{1-p^{-(\tau+1)}}{1-p^{-1}}\cdot k.$$

We need to make some of the earlier notation more explicit: we denote by

$$\Gamma(k, p^n, N)$$

(¹) Note added in proof. Recently A. Tietavainen has shown that the exponent 7/8 can be reduced to $3/5+\varepsilon$ (private communication 14. 9. 72).

the least s such that the congruence (2) has a primitive solution for the particular prime power modulus p^n and the particular integer N. Then plainly

$$\Gamma(k, p^n) = \max_{0 \leqslant N < p^n} \Gamma(k, p^n, N).$$

We also need some notation connected with the easier Waring Problem: we denote by

$$\Delta(k, p^n, N)$$

the least s such that the congruence

$$\varepsilon_1 x_1^k + \ldots + \varepsilon_s x_s^k \equiv N \pmod{p^n}, \tag{3}$$

where each coefficient ε_i, $i = 1, \ldots, s$, can assume the values $+1$ or -1, has a primitive solution. It is plain that

$$\Delta(k, p^n) = \max_{0 \leqslant N < p^n} \Delta(k, p^n, N)$$

is the least s such that the congruence (3) has a primitive solution for every integer N.

We shall always take $t = \dfrac{p-1}{d}$, so that t necessarily divides $p-1$ and the restriction $d < \frac{1}{2}(p-1)$ implies that $t > 2$.

Now it is well known that the reduced residue classes (mod p^n) form a cyclic group of order $\varphi(p^n) = p^{n-1}(p-1)$. As is appropriate for work on Waring's Problem, we write k in the form

$$k = p^{\tau} dm$$

where here p^{τ} exactly divides k, so that $(m, p) = 1 = (m, t)$. It follows that the values assumed by x^k, for given k and arbitrary x, are the same as those assumed by $x^{p^{\tau}d} \pmod{p^{\tau+1}}$. Thus

$$\Gamma(k, p^{\tau+1}, N) = \Gamma(p^{\tau} d, p^{\tau+1}, N) \tag{4}$$

and

$$\Delta(k, p^{\tau+1}, N) = \Delta(p^{\tau} d, p^{\tau+1}, N), \tag{5}$$

whence if $k = p^{\tau} dm$, we can take $m = 1$ without loss of generality.

Plainly if -1 is a kth power residue (mod $p^{\tau+1}$), i.e. if d divides $\frac{1}{2}(p-1)$, then $\Gamma(k, p^{\tau+1}) = \Delta(k, p^{\tau+1})$, and it is clear that more generally we have

$$\Gamma(k, p^{\tau+1}) \leqslant \Gamma(k, p^{\tau+1}, -1)\cdot \Delta(k, p^{\tau+1}). \tag{6}$$

Moreover

$$\Gamma(k, p^{\tau+1}, -1) \leqslant t-1,$$

for by Euler's theorem

$$x^{\varphi(p^{\tau+1})}-1 = x^{p^{\tau}(p-1)}-1 \equiv 0 \ (\mathrm{mod}\ p^{\tau+1}),$$

i.e.

$$(x^{p^{\tau}d})^{t}-1 \equiv 0 \ (\mathrm{mod}\ p^{\tau+1})$$

and so the sum of the t distinct values of $x^{p^{\tau}d}$ (mod $p^{\tau+1}$) which are prime to p, $x_1^{p^{\tau}d}, \ldots, x_t^{p^{\tau}d}$, say, is congruent to 0 (mod $p^{\tau+1}$). Hence

$$-1 \equiv (x_1^{-1}x_2)^{p^{\tau}d}+ \ldots +(x_1^{-1}x_t)^{p^{\tau}d} \ (\mathrm{mod}\ p^{\tau+1}),$$

i.e.

$$\Gamma(p^{\tau}d, p^{\tau+1}, -1) \leqslant t-1,$$

and the assertion follows from (6), and we deduce that

$$\Gamma(k, p^{\tau+1}) \leqslant (t-1)\,\Delta(k, p^{\tau+1}). \tag{7}$$

(This estimate can also be established using sums of primitive roots.)

Thus when t is small we can work with the more tractable number $\Delta(k, p^{\tau+1})$ and plainly if t is less than some absolute constant, then (7) supplies us with a simple and effective estimate for $\Gamma(k, p^{\tau+1})$ in terms of $\Delta(k, p^{\tau+1})$. In particular if the prime p is less than an absolute constant, then certainly so is $t \leqslant p-1$, and we shall make use of this observation subsequently. If, on the other hand, t is large, then d is small and we exploit that this implies that $\Gamma(k, p)$ is small.

We now proceed to obtain an estimate for $\Delta(k, p^{\tau+1})$. The first result has some similarities with Lemma 2 of [5].

Lemma 1. *Let $p \geqslant 5$ and $k = p^{\tau}dm$. Then there is an integer l divisible by p but not by $p^{\tau+1}$ such that*

$$\Delta(k, p^{\tau+1}, l) \leqslant 2[p^{1/2}],$$

where $[p^{1/2}]$ is the integer part of $p^{1/2}$.

Proof. First we show that we can find a kth power residue (mod $p^{\tau+1}$), R say, prime to p and not congruent to ± 1 (mod $p^{\tau+1}$) such that

$$R \equiv xy^{-1} \ (\mathrm{mod}\ p^{\tau+1}), \tag{8}$$

where $(x, y) = 1$, $1 \leqslant y < p$, $p^{1/2} < |x| \leqslant p^{\tau}$ and $|x| > y$. Since $t > 2$ we can certainly find a kth power residue (mod $p^{\tau+1}$), R_1 say, which is prime to p and not congruent to ± 1 (mod $p^{\tau+1}$). Now the least positive residues (mod $p^{\tau+1}$) of the $p-1$ numbers

$$R_1, 2R_1, \ldots, (p-1)R_1,$$

say

$$u_1, u_2, \ldots, u_{p-1},$$

together with 0 and $p^{\tau+1}$ define $p+1$ distinct points distributed amongst the p half-open intervals

$$r(p^{\tau}+1) \leqslant \xi < (r+1)(p^{\tau}+1), \quad r = 0, 1, \ldots, p-1,$$

each of length $p^{\tau}+1$. At least one interval contains two such points and so there exist integers x_1 and y_1 say, satisfying

$$1 \leqslant y_1 \leqslant p-1, \quad 1 \leqslant |x_1| \leqslant p^{\tau}$$

with

$$y_1 R_1 \equiv x_1 \ (\mathrm{mod}\ p^{\tau+1}).$$

Moreover we can assume without loss of generality that $|x_1| > y_1$ since otherwise we can simply replace R_1 by R_1^{-1} in the above. Also p cannot divide y_1 and x_1 and so we can take x_1 and y_1 to be coprime.

Thus if $|x_1| > p^{1/2}$, the integers R_1, x_1 and y_1 fulfill the conditions required for the congruence (8). On the other hand, if $|x_1| < p^{1/2}$ we can find a positive integer f such that

$$p^{1/2} < |x_1|^{f} < p$$

and it is easily verified that R_1^{f}, x_1^{f} and y_1^{f} satisfy the conditions required for (8).

The $([p^{1/2}]+1)^2$ integers of the form

$$m+nR, \quad 0 \leqslant m, n < p^{1/2} \tag{9}$$

where R satisfies (8), are incongruent (mod $p^{\tau+1}$), for if

$$m_1+n_1R \equiv m_2+n_2R \ (\mathrm{mod}\ p^{\tau+1})$$

then

$$x(n_1-n_2) \equiv y(m_2-m_1) (\mathrm{mod}\ p^{\tau+1}),$$

i.e. since $|x(n_1-n_2)+y(m_1-m_2)| < p^{\tau}\cdot p^{1/2}+(p-1)p^{1/2} < p^{\tau+1}$, we have

$$x(n_1-n_2) = y(m_2-m_1).$$

But $(x, y) = 1$ so x must divide m_1-m_2 which because $|m_2-m_1| < p^{1/2} < |x|$, implies $m_1 = m_2$ and consequently that $n_1 = n_2$. Now since $([p^{1/2}]+1)^2 > p$, it follows that there are two such integers congruent (mod p) and hence their difference l say which is representable as $m-m'+(n-n')R$ (mod $p^{\tau+1}$) is divisible by p but not by $p^{\tau+1}$, and

$$\Delta(k, p^{\tau+1}, l) \leqslant 2[p^{1/2}],$$

as required.

This result is used to prove

Lemma 2. *Let $k = p^{\tau}dm$ where $d < \frac{1}{2}(p-1)$ and suppose that p satisfies*

$$1+2[p^{1/2}] \leqslant p^{\delta}$$

where $\delta > \frac{1}{2}$. *Then*

$$\Delta(k, p^{\tau+1}) \leqslant p^{\delta\tau}\Gamma(k, p).$$

Proof. By (5) it suffices to prove the result for $\Delta(p^{\tau}d, p^{\tau+1})$. Now the inequality is clearly true for $\tau = 0$, and we assume inductively that for every natural number $\sigma < \tau$

$$\Delta(p^{\sigma}d, p^{\sigma+1}) \leqslant p^{\delta\sigma}\Gamma(d, p).$$

By the preceding lemma we can find an integer $l = hp^{a}$ say where p does not divide h and $1 \leqslant a \leqslant \tau$ such that

$$\Delta(p^{\tau}d, p^{\tau+1}, hp^{a}) \leqslant 2[p^{1/2}].$$

Further it follows from the observation that

$$x^{p^{\tau}} \equiv x^{p^{\nu}} (\operatorname{mod} p^{\nu+1}) \tag{10}$$

for any $\nu \leqslant \tau$, that we can solve non-trivially the congruence

$$\varepsilon_1 x_1^{p^{\tau}d} + \ldots + \varepsilon_s x_s^{p^{\tau}d} \equiv h^{-1}n \, (\operatorname{mod} p^{\tau-a+1}),$$

where as always the coefficients $\varepsilon_1, \ldots, \varepsilon_s$ can take the values $+1$ or -1, for any integer n, providing $s \geqslant \Delta(p^{\tau-a}d, p^{\tau-a+1})$. Hence for all integers n,

$$\Delta(p^{\tau}d, p^{\tau+1}, np^{a}) \leqslant \Delta(p^{\tau}d, p^{\tau+1}, hp^{a}) \cdot \Delta(p^{\tau-a}d, p^{\tau-a+1}). \tag{11}$$

Also it follows from (10) that for $s \geqslant \Delta(p^{\tau-1}d, p^{\tau})$, the congruence

$$\varepsilon_1 x_1^{p^{\tau}d} + \ldots + \varepsilon_s x_s^{p^{\tau}d} \equiv N \, (\operatorname{mod} p^{\tau})$$

has a non-trivial solution for every integer N, i.e.

$$\varepsilon_1 x_1^{p^{\tau}d} + \ldots + \varepsilon_s x_s^{p^{\tau}d} \equiv N + N'p^{\tau} \, (\operatorname{mod} p^{\tau+1}) \tag{12}$$

where without loss of generality p does not divide N', has a non-trivial solution. We use (11) to get rid of the term $N'p^{\tau}$: indeed putting $n = N'p^{\tau-a}$ we see that (11) implies we can solve

$$\varepsilon_1' y_1^{p^{\tau}d} + \ldots + \varepsilon_s' y_s^{p^{\tau}d} \equiv N'p^{\tau} \, (\operatorname{mod} p^{\tau+1})$$

if

$$s \geqslant \Delta(p^{\tau}d, p^{\tau+1}, hp^{a}) \cdot \Delta(p^{\tau-a}d, p^{\tau-a+1}).$$

Now from (12) and by the inductive hypothesis, we have

$$\begin{aligned}
\Delta(k, p^{\tau+1}) = \Delta(p^{\tau}d, p^{\tau+1}) &\leqslant \Delta(p^{\tau-1}d, p^{\tau}) + \Delta(p^{\tau}d, p^{\tau+1}, N'p^{\tau}) \\
&\leqslant p^{\delta(\tau-1)}\Gamma(d, p) + 2[p^{1/2}] \cdot p^{\delta(\tau-a)} \cdot \Gamma(d, p) \\
&\leqslant p^{(\tau-1)\delta}(1 + 2[p^{1/2}])\Gamma(d, p) \\
&\leqslant p^{\tau\delta}\Gamma(d, p),
\end{aligned}$$

providing $p^{\delta} \geqslant 1 + 2[p^{1/2}]$, and the lemma is proved.

Starting with a kth power residue $(\operatorname{mod} p^{\tau+1})$, R say, satisfying (8), we use the addition of residue classes to obtain in a way similar to Lemma 2 of [5], but modified to deal with congruences to a prime power modulus, an estimate for $\Gamma(k, p^2)$ which is effective when d is large. However we cannot use the Cauchy–Davenport Theorem to deal with addition of residue classes modulo a prime power and the following modified version is used:

Lemma 3. *Let n be a positive integer and let $a_1, \ldots, a_l$ be l distinct residue classes* $(\operatorname{mod} n)$. *Let $b_1, \ldots, b_m$ be m distinct residue classes* $(\operatorname{mod} n)$, *one of which is* 0 *and the remainder prime to n. Then the number of distinct residue classes representable as*

$$a_i + b_j, \quad 1 \leqslant i \leqslant l, 1 \leqslant j \leqslant m,$$

is at least

$$\min(l+m-1, n).$$

This is due to I. Chowla ([1]) but a more convenient reference is Halberstam and Roth ([6], p. 49, Theorem 15).

Lemma 4. *Let $k = pdm$, i.e. let $\tau = 1$. Then for $p > 31$,*

$$\operatorname*{Max}_{n} \Gamma(k, p^n) = \Gamma(k, p^2) < 54\, p^{6/5}.$$

Proof. By the first part of Lemma 1 we know that there exists a kth power residue $(\operatorname{mod} p^2)$, R say, such that R is prime to p and not congruent to $\pm 1 \, (\operatorname{mod} p^2)$ and such that

$$R \equiv xy^{-1} \, (\operatorname{mod} p^2)$$

where $1 \leqslant y < p$, $y < |x| < p$, $(x, y) = 1$.

We consider three separate cases:

$$\text{(i)}\ p^{4/5} < |x| < p, \quad \text{(ii)}\ p^{2/5} < |x| < p^{4/5}, \quad \text{(iii)}\ 1 < |x| < p^{2/5}.$$

It is straightforwardly verified along the lines of the preceding lemma or as in the case 1 of [5], Lemma 2, p. 150, that in case (i), the numbers of the form

$$m + nR, \quad 0 \leqslant m,\ n < \tfrac{1}{2}p^{4/5}$$

generate at least $\frac{1}{4}p^{8/5}$ integers which are incongruent $(\operatorname{mod} p^2)$. Moreover each of these numbers is a sum of at most $p^{4/5}$ kth powers $(\operatorname{mod} p^2)$ of which at least $\frac{1}{4}p^{8/5} - p$ are prime to p. Hence by Lemma 3 the expression

$$m_1 + n_1 R + \ldots + m_r + n_r R, \quad 0 \leqslant m_i, n_i < \tfrac{1}{2}p^{4/5} \ (1 \leqslant i \leqslant r),$$

of at most $r \cdot p^{4/5}$ kth powers $(\operatorname{mod} p^2)$ represents at least

$$\min\left(\tfrac{1}{4}rp^{8/5} - (r-1)p,\ p^2\right)$$

distinct residue classes $(\operatorname{mod} p^2)$. Therefore, provided $p > 31$,

$$\Gamma(k, p^2) < 8p^{2/5}p^{4/5} = 8p^{6/5}.$$

In case (ii) we consider, as in case 2 of [5], Lemma 2, p. 150, numbers of the form

$$l+mR+nR^2, \quad 0 \leqslant l, m, n < \tfrac{1}{3}p^{2/5},$$

and it is straightforward to verify these generate at least $\frac{1}{27}p^{6/5}$ numbers which are incongruent (mod p^2). Each number is a sum of at most $p^{2/5}$ kth powers (mod p^2) of which at least $\frac{1}{27}p^{6/5}-p$ are prime to p. Then as in case (i), repeated application of Lemma 3 gives us that in this case

$$\Gamma(k, p^2) < 54p^{6/5}$$

for $p > 31$.

In the remaining case where $1 < |x| < p^{2/5}$ we adopt a device similar to that employed in case 3 of Lemma 2 in [5], and we choose an integer f such that

$$p^{4/5} < |x|^f < p^{6/5}$$

and observe that R^f is a kth power (mod p^2) and that

$$R^f \equiv x^f y^{-f} \pmod{p^2}$$

where $1 < y^f < |x|^f < p$ and $(x^f, y^f) = 1$. Then it is readily checked that the numbers

$$m+nR^f, \quad 0 \leqslant m, n < \tfrac{1}{2}p^{4/5},$$

generate at least $\frac{1}{4}p^{8/5}$ distinct residues (mod p^2), each of which is a sum of less than $p^{4/5}$ kth powers (mod p^2). Also at least $\frac{1}{4}p^{8/5}-p$ of these numbers are prime to p. Thus, as in case (i), repeated application of Lemma 3 leads us to the conclusion that

$$\Gamma(k, p^2) < 8p^{6/5}$$

for $p > 31$ and the lemma is proved.

LEMMA 5. *If $p \geqslant 7$ and $d < \frac{1}{2}(p-1)$, then for k sufficiently large*

$$\Delta(k, p^{\tau+1}) < k^{\frac{7}{8}-\eta}$$

where η is a small enough positive number.

Proof. Since $7^7 > 5^8$ and $3^8 \cdot 11^3 > 7^8$, and since for $p \geqslant 11$,

$$p^{3/8} \geqslant 11^{3/8} > \tfrac{7}{3} = 2+\tfrac{1}{3} > 2+\frac{1}{p^{1/2}},$$

we have

$$p^{\frac{7}{8}-\eta} > 1+2\,[p^{1/2}]$$

for all $p \geqslant 7$, provided $\eta > 0$ is small enough.

Now it is straightforward to verify from [5], Theorems 1 and 2, that for $d \geqslant d_0$, where d_0 is some constant depending only on η, that

$$\Gamma(d, p) < d^{\frac{7}{8}-\eta}.$$

Therefore choosing $\delta = \frac{7}{8}-\eta$ in Lemma 2, we have that

$$\Delta(k, p^{\tau+1}) \leqslant p^{\left(\frac{7}{8}-\eta\right)\tau} d^{\frac{7}{8}-\eta} = k^{\frac{7}{8}-\eta}$$

providing $d \geqslant d_0$. Otherwise when $d < d_0$, we know that $d < \frac{1}{2}(p-1)$ implies $\Gamma(d, p) \leqslant d$ ([8], p. 533, Theorem 4), whence

$$\Delta(k, p^{\tau+1}) \leqslant p^{\left(\frac{7}{8}-\eta\right)\tau} d < p^{\left(\frac{7}{8}-\eta\right)\tau} d_0 < k^{\left(\frac{7}{8}-\frac{\eta}{2}\right)}$$

for k sufficiently large, which completes the proof.

The following lemma is needed because the previous one fails to deal with $p = 5$.

LEMMA 6. *If k is odd and 5^τ exactly divides k, then*

$$\Gamma(k, 5^{\tau+1}) < 50k^{1/2}.$$

Proof. The hypothesis that k is odd ensures that $d = (k, 5-1) = 1 < \dfrac{5-1}{2}$, so that $\Gamma(k, 5) = 2$. Thus without loss of generality, we can take $\tau = \gamma - 1 \geqslant 1$. Let g be a primitive root (mod $5^{\tau+1}$) and write

$$R = g^k$$

so that R is a kth power (mod $5^{\tau+1}$) which is not congruent to $+1$ or -1 or divisible by 5. Also

$$R^2 = g^{2k} \equiv -1 \pmod{5^{\tau+1}}$$

since $4 \cdot 5^\tau$ divides $4k$. The numbers

$$m+nR, \quad 0 \leqslant m, n < \tfrac{1}{2}\,5^{(\tau+1)/2} \tag{13}$$

generate $([\frac{1}{2}\,5^{(\tau+1)/2}]+1)^2 > \frac{1}{4}\,5^{\tau+1}$ integers which are all incongruent (mod $5^{\tau+1}$). For if $m+nR \equiv m'+n'R \pmod{5^{\tau+1}}$ then we would have

$$(m-m')^2+(n-n')^2 \equiv 0 \pmod{5^{\tau+1}},$$

whence, because the left hand side of the last congruence is at most $\frac{1}{2}\,5^{\tau+1}$, $m = m'$ and $n = n'$.

Moreover each of the numbers (13) is a sum of at most $5^{(\tau+1)/2}$ kth powers (mod $5^{\tau+1}$) and at least $\frac{1}{4}\,5^{\tau+1}-5 = \frac{1}{4}\,5^\tau$ of them are prime to 5. It follows from repeated application of Lemma 3 that

$$\Gamma(k, 5^{\tau+1}) < 20 \cdot 5^{(\tau+1)/2} < 50 \cdot 5^{\tau/2} \leqslant 50 \cdot k^{1/2},$$

as desired.

LEMMA 7. *Let $k = p^\tau dm$ where $d < p^{2/5}$. Then*

$$\Gamma(k, p^{\tau+1}) \leqslant \operatorname{Max}\left(10\cdot 12^\tau, 10\,\Delta(k, p^{\tau+1})\right).$$

Proof. It can be verified readily by using standard exponential sum techniques (see for example [4], § 2.4) that if $d < p^{2/5}$ then $\Gamma(k, p) \leqslant 10$, whence in particular $\Gamma(k, p, -1) \leqslant 10$, or equivalently

$$-1 = y_1^k + \ldots + y_{10}^k + p^g\cdot e \tag{14}$$

where $g \geqslant 1$, p does not divide e and not all of the integers $y_1, \ldots, y_{10}$ are divisible by p.

Now if $g \geqslant \tau+1$ it follows by very definition that

$$\Gamma(k, p^{\tau+1}, -1) \leqslant 10$$

so (6) implies

$$\Gamma(k, p^{\tau+1}) \leqslant 10\cdot \Delta(k, p^{\tau+1})$$

as required.

So suppose $1 \leqslant g \leqslant \tau$. We use an inductive argument similar to that of Lemma 2, and we assume inductively that for each non-negative $\sigma < \tau$

$$\Gamma(k, p^{\sigma+1}) \leqslant 12^\sigma \Gamma(k, p) \leqslant 12^\sigma\cdot 10, \tag{15}$$

an assumption which certainly holds for $\sigma = 0$. A trivial rearrangement of (14) gives us that

$$y_1^k + \ldots + y_{11}^k = e\cdot p^g$$

where $1 \leqslant g \leqslant \tau$, p does not divide e and not all the variables $y_1, \ldots, y_{11}$ are divisible by p. By definition the congruence

$$z_1^k + \ldots + z_\nu^k \equiv e^{-1} n \pmod{p^{\tau-g+1}}$$

has a primitive solution for every integer n, where $\nu = \Gamma(k, p^{\tau-g+1})$. Thus on multiplying by ep^g it follows that for every integer n

$$\Gamma(k, p^{\tau+1}, np^g) \leqslant 11\cdot\Gamma(k, p^{\tau-g+1}),$$

whence, as in Lemma 2 and by the inductive hypothesis (15),

$$\begin{aligned}\Gamma(k, p^{\tau+1}) &\leqslant \Gamma(k, p^\tau) + \operatorname*{Max}_n \Gamma(k, p^{\tau+1}, np^g)\\ &\leqslant \Gamma(k, p^\tau) + 11\cdot\Gamma(k, p^{\tau-g+1})\\ &\leqslant 12^{\tau-1}\Gamma(k, p) + 11\cdot 12^{\tau-g}\Gamma(k, p)\\ &\leqslant 12^\tau\Gamma(k, p) \leqslant 12^\tau\cdot 10,\end{aligned}$$

and the induction is established.

The lemma follows on combining the two estimates for $\Gamma(k, p^{\tau+1})$.

We now use these lemmas to obtain the

THEOREM. *Let $d = (k, p-1) < \frac{1}{2}(p-1)$. Then provided k is large enough,*

$$\Gamma(k, p^n) < k^{7/8}$$

for all $n \geqslant 1$.

Proof. It suffices to establish the inequality for $n = \gamma = \tau+1$ where p^τ exactly divides k and in view of [5], p. 166, Theorem 2, we need only consider the case $\tau \geqslant 1$. Also by Lemma 6, we can take $p \geqslant 7$. We consider various cases and begin by taking d large.

First suppose $\tau = 1$, $p > 31$ and $d > p^{2/5}$ so that $t < 2p^{3/5}$. Then by Lemma 4,

$$\Gamma(k, p^2) < 54\, p^{6/5} < 54\,\left(p^{\frac{2}{5}+1}\right)^{\left(\frac{7}{8}-\eta\right)}$$

providing η is small enough, and hence

$$\Gamma(k, p^2) < 54\,(pd)^{\frac{7}{8}-\eta} < k^{7/8}$$

for k sufficiently large.

Next suppose $\tau = 1$, $d > p^{2/5}$ and $7 \leqslant p \leqslant 31$. Then $t < 2p^{3/5} < 16$ and so by (7) and Lemma 5,

$$\Gamma(k, p^2) < 15\cdot\Delta(k, p^2) < 15\cdot k^{\frac{7}{8}-\eta} < k^{7/8}$$

for k sufficiently large.

We continue to take $d > p^{2/5}$ but now suppose that $\tau \geqslant 2$. Then (providing $\eta < \frac{1}{40}$) $\frac{3}{5}+\frac{11}{20}\tau < (\frac{7}{8}-\eta)\tau$, and it is readily verified that if $p > 2^{21}$ we have

$$p^{11/20} > 1 + 2\,[p^{1/2}].$$

It follows from Lemma 2 with $\delta = 11/20$ that

$$\Delta(k, p^{\tau+1}) \leqslant p^{(11/20)\tau}\Gamma(k, p)$$

and combining this inequality with (7) we get that

$$\Gamma(k, p^{\tau+1}) < 2p^{3/5}\cdot p^{(11/20)\tau}\cdot\Gamma(k, p) < 2\,(p^\tau d)^{\frac{7}{8}-\eta} < k^{7/8}$$

for k sufficiently large. As above the result when $p < 2^{21}$ is an immediate consequence of (7) and Lemma 5: if $7 \leqslant p \leqslant 2^{21}$, then

$$\Gamma(k, p^{\tau+1}) < 2^{21}\cdot k^{\frac{7}{8}-\eta} < k^{7/8}$$

for k large enough.

There remains the case $\tau \geqslant 1$ and $d < p^{2/5}$, when Lemma 7 applies and so, providing $p > 12^{8/7}$,

$$\Gamma(k, p^{\tau+1}) \leqslant \operatorname{Max}\left(10\cdot p^{\left(\frac{7}{8}-\eta\right)\tau}, 10\cdot\Delta(k, p^\gamma)\right) < k^{7/8}$$

since k is sufficiently large.

Clearly as before, the inequality also holds for $p < 12^{8/7}$. All the various possibilities have now been exhausted and so the proof is complete.

It is evident that any improvement in the estimate for $\Gamma(k, p)$ would lead to a corresponding improvement in $\Gamma(k, p^{\tau+1})$, and in fact the exponent can be reduced slightly ([5], p. 166, Theorem 2) but we retain $\frac{7}{8}$ for simplicity as we are probably far from the final answer.

In conclusion, we define the familiar number $\Gamma(k)$ by

$$\Gamma(k) = \operatorname*{Max}_{p} \Gamma(k, p^{\gamma})$$

where the maximum is taken over all primes p, so that $\Gamma(k)$ is, as is well known, the least s such that the congruence (2) has a primitive solution for all integers N and all prime powers p^n. Hardy and Littlewood have shown that $\Gamma(k) \leqslant 4k$ for all k ([7], p. 186, Theorem 12) and further that $\Gamma(k) \leqslant k$ unless k belongs to certain special classes ([8], p. 533, Theorem 4), while I. Chowla ([2], p. 97, Theorem 1) proved that $\Gamma(q) \leqslant 2\,[q/3]+2$ for an infinity of primes q. Our results above enable us to show that $\Gamma(q) < q^{7/8}$ for an infinity of primes q by exhibiting infinitely many primes q which are not of the form $\frac{1}{2}(p-1)$ for any prime $p > 3$.

Indeed suppose the prime q is of the form $q = 1+3l$ where $l \geqslant 2$, and suppose also that

$$q = \frac{p-1}{2}$$

for some prime $p > 3$. Then $p = 2q+1 \equiv 0 \pmod 3$ contradicting the choice of p as a prime. Now in view of the trivial estimates $\Gamma(k, 2) \leqslant 2$ and $\Gamma(k, 3) \leqslant 3$ and of the above theorem, we have for q sufficiently large and for every positive integer n, that

$$\Gamma(q, p^n) < q^{7/8}$$

for all primes p, whence by definition

$$\Gamma(q) = \operatorname*{Max}_{\text{primes } p} \Gamma(q, p^{\gamma}) < q^{7/8}.$$

But by Dirichlet's Theorem on primes in arithmetic progression, we know that there are infinitely many primes $p \equiv 1 \pmod 3$, and so the assertion is established.

It can be proved in a similar fashion that

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

for an infinity of even k. Here we take q to be a prime congruent to $1 \pmod{15}$ and $k = 2q$ and suppose that for some prime $p > 5$,

$$k = 2q = \frac{p-1}{2} n,$$

so that $q = (p-1)/2$ or $2q = (p-1)/2$, i.e. $p = 2q+1$ or $p = 4q+1$. Hence either $p \equiv 0 \pmod 3$ or $p \equiv 0 \pmod 5$ respectively contradicting the choice of p as a prime and it follows that k is not divisible by $\frac{1}{2}(p-1)$ for any prime $p > 5$. The trivial estimate $\Gamma(k, 5) \leqslant 5$ together with the theorem above and the definition of $\Gamma(k)$ gives us as before that for q sufficiently large,

$$\Gamma(2q) < (2q)^{7/8}$$

where q is a prime congruent to $1 \pmod{15}$. Since there are infinitely many such primes we conclude that $\Gamma(k) < k^{7/8}$ for an infinity of even k.

References

[1] I. Chowla, *A theorem in the addition of residue classes*, Proc. Nat. Acad. Sci. India, 2 (1935), pp. 242–243.

[2] — *A new evaluation of the number $\Gamma(k)$ in Waring's problem*, Proc. Ind. Acad. Sci. (VI) No. 1, (1937), pp. 97–103.

[3] — *On Waring's problem* (mod$p$), Proc. Nat. Acad. Sci. India, A, 12 (1943), pp. 242–243.

[4] M. M. Dodson, *Homogeneous additive congruences*, Philos. Trans. Roy. Soc. London, A, 261 (1967), pp. 163–210.

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

[6] H. Halberstam and K. Roth, *Sequences I*, Oxford 1966.

[7] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum' (IV): The singular series in Waring's problem and the value of the number $G(k)$*, Math. Zeitschr. 12 (1922), pp. 161–188.

[8] — — *Some problems of 'Partitio Numerorum' (VIII): The number $\Gamma(k)$ in Waring's problem*, Proc. London Math. Soc. 28 (1928), pp. 518–542.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF YORK
Heslington, York

Received on 14. 11. 1971 (237)