ACTA ARITHMETICA
XXIX (1976)

A note on Waring's problem in p-adic fields

by

J. D. Bovey (Cardiff)

1. Introduction. Let p be any prime and k any positive integer. The number $\Gamma_p(k)$ is defined as the least positive integer s such that we can solve non-trivially the congruence

(1) $$x_1^k + \ldots + x_s^k \equiv N \pmod{p^n}$$

for all integers N and all positive integers n. It is well known that $\Gamma_p(k)$ is also the least s such that any p-adic integer can be represented non-trivially as the sum of s kth powers of p-adic integers.

The function $\Gamma_p(k)$ was introduced by Hardy and Littlewood in their work on Waring's problem [5] though with a different notation and they showed that for all p and k ([5], p. 186, Theorem 12)

(2) $$\Gamma_p(k) \leqslant 4k.$$

In 1943 I. Chowla [2] showed that if $\frac{1}{2}(p-1)$ does not divide k then for all positive ε

$$\Gamma_p(k) \ll k^{1-c+\varepsilon},$$

where $c = (103-3\sqrt{641})/220$ and $\ll$ as usual denotes inequality with a fixed positive constant. More recently Dodson [3] improved the exponent to $7/8$.

If p does not divide k then the solubility of the congruence (1) is equivalent to the solubility of the congruence

(3) $$x_1^k + \ldots + x_s^k \equiv N \pmod{p}.$$

If $\Gamma(k, p)$ is defined as the least s such that (3) is non-trivially soluble for all integers N then Dodson and Tietäväinen [4] have shown that if $\frac{1}{2}(p-1)$ does not divide k then for all $\varepsilon > 0$

(4) $$\Gamma(k, p) \ll k^{1/2+\varepsilon}.$$

In this paper we generalize Dodson and Tietäväinen's result to the general p-adic case and prove

THEOREM 3. *Given* $\varepsilon > 0$ *then*

$$\Gamma_p(k) \leqslant k^{1/2+\varepsilon}$$

for all positive integers k *and all primes* p *such that* $\frac{1}{2}(p-1)$ *does not divide* k.

Theorem 3 follows fairly easily from Theorems 1 and 2 which are effective when p is large and small respectively.

THEOREM 1. *Let* $k = p^\tau dm$, *where* p *is an odd prime,* $d = (k, p-1)$ *and* p *does not divide* m. *Then*

$$\Gamma_p(k) \leqslant \tfrac{3}{2}\Gamma(k, p)\big(3\Gamma(k, p)\big)^\tau.$$

THEOREM 2. *Let* k *be any positive integer and* p *any odd prime. Then for any* $\varepsilon > 0$ *we have*

$$\Gamma_p(k) < C(p, \varepsilon)\, k^{\frac{1}{\varphi(t)}+\varepsilon},$$

where $t = (p-1)/d$, $d = (k, p-1)$, φ *is Euler's* φ*-function and* $C(p, \varepsilon)$ *is a function of* p *and* ε *only.*

It seems likely that (4) is not the best possible (see [4] and [6]) and it is clear that any improvement in the exponent in (4) could be generalized at once to the p-adic case.

2. Notation and preliminary results. We shall always take k, d and t to be positive integers and p to be an odd prime with $p-1 = dt$. As is usual we will write

$$k = p^\tau dm, \tag{5}$$

where $d = (k, p-1)$ and p does not divide m. If $d = p-1$ or $\frac{1}{2}(p-1)$ then $\Gamma_p(k)$ is known and is not in general less than k (see [1] or [5]). This is certainly true if $p = 2$ and so we lose nothing by assuming $p \geqslant 3$.

The number $\Gamma(k, p^n, N)$ is defined as the least s such that the congruence (1) has a non-trivial solution for particular prime power p^n and integer N. Then

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

is clearly the least s such that (1) has a non-trivial solution for all integers N.

LEMMA 1. *If* k *is expressed as in* (5), *where* p *is an odd prime, then*

$$\Gamma_p(k) = \Gamma_p(p^\tau d) = \Gamma(p^\tau d, p^{\tau+1}).$$

Proof. This is very well known (see [1] for example).

Also we need some notation connected with the easier Waring problem. We denote by $\Delta(k, p^n, N)$ the least s such that the congruence

$$\varepsilon_1 x_1^k + \ldots + \varepsilon_s x_s^k \equiv N \pmod{p^n}, \tag{6}$$

where each coefficient ε_i, $i = 1, \ldots, s$, can assume the values $+1$ or -1, has a primitive solution for some choice of $\varepsilon_1, \ldots, \varepsilon_s$ and for the particular prime power p^n. It is plain that

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

is the least s such that the congruence (6) has a primitive solution for every integer N.

When t is small the number $\Delta(k, p^n)$ can provide a good bound for $\Gamma(k, p^n)$. Let τ be any non-negative integer and let x be any integer such that $x^{p^\tau d} \not\equiv 1 \pmod{p}$. Then, by Euler's theorem, we have

$$(x^{p^\tau d})^t \equiv 1 \pmod{p^{\tau+1}}$$

and so

$$1 + x^{p^\tau d} + \ldots + (x^{t-1})^{p^\tau d} \equiv 0 \pmod{p^{\tau+1}},$$

i.e.

$$x^{p^\tau d} + \ldots + (x^{t-1})^{p^\tau d} \equiv -1 \pmod{p^{\tau+1}}.$$

It clearly follows that

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

Finally we introduce two new functions which simplify considerably the analysis of the problem. For any non-negative integer τ define $g(p^\tau, d)$ as the least s such that we can solve

$$x_1^{p^\tau d} + \ldots + x_s^{p^\tau d} \equiv ap^\tau \pmod{p^{\tau+1}}$$

for some a prime to p. Similarly define $f(p^\tau, d)$ to be the least s such that we can solve

$$\varepsilon_1 x_1^{p^\tau d} + \ldots + \varepsilon_s x_s^{p^\tau d} \equiv ap^\tau \pmod{p^{\tau+1}}$$

for some a prime to p and some $\varepsilon_1, \ldots, \varepsilon_s$ taking the values $+1$ and -1. The following straightforward inequalities are crucial in establishing the final estimates for $\Gamma_p(k)$.

LEMMA 2. *If* a, b, α *and* β *are integers with* $\alpha, \beta \geqslant 0$ *then*

(i) $\Gamma(p^{\alpha+\beta}d, p^{\alpha+\beta+1}, abp^{\alpha+\beta}) \leqslant \Gamma(p^\alpha d, p^{\alpha+1}, ap^\alpha)\,\Gamma(p^\beta d, p^{\beta+1}, bp^\beta)$,

(ii) $\Delta(p^{\alpha+\beta}d, p^{\alpha+\beta+1}, abp^{\alpha+\beta}) \leqslant \Delta(p^\alpha d, p^{\alpha+1}, ap^\alpha)\,\Delta(p^\beta d, p^{\beta+1}, bp^\beta)$.

Proof. We prove only (i) as the proof of (ii) is essentially identical. First we make the well known observation that for $u \geqslant v$ and for any x prime to p

$$x^{p^u} \equiv x^{p^v} \pmod{p^{v+1}}.$$

Therefore we know that for some A and B we can solve

(8) $$x_1^{p^{\alpha+\beta}d}+\ldots+x_r^{p^{\alpha+\beta}d} = ap^\alpha + Ap^{\alpha+1},$$

(9) $$y_1^{p^{\alpha+\beta}d}+\ldots+y_s^{p^{\alpha+\beta}d} = bp^\beta + Bp^{\beta+1},$$

with

$$r = \Gamma(p^\alpha d, p^{\alpha+1}, ap^\alpha), \quad s = \Gamma(p^\beta d, p^{\beta+1}, bp^\beta).$$

Multiplying (9) and (8) we get

$$\sum_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant s}} (x_i y_j)^{p^{\alpha+\beta}d} \equiv abp^{\alpha+\beta} (\operatorname{mod} p^{\alpha+\beta+1})$$

and the result follows.

LEMMA 3. *Let p be any odd prime, d divide $p-1$ and τ be any non-negative integer. Then*

(i) $$\Gamma(p^\tau d, p^{\tau+1}) \leqslant \Gamma(d, p)\sum_{\sigma=0}^{\tau} g(p^\sigma, d),$$

(ii) $$\Delta(p^\tau d, p^{\tau+1}) \leqslant \Delta(d, p)\sum_{\sigma=0}^{\tau} f(p^\sigma, d).$$

Proof. Again we only prove (i). The proof is by induction on τ. Clearly it is true for $\tau = 0$ and so it is sufficient to show that for all $\tau \geqslant 1$

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

Let N be any integer. Since $x^{p^\tau d} \equiv x^{p^{\tau-1}d} (\operatorname{mod} p^\tau)$, we can solve

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

for $s = \Gamma(p^{\tau-1}d, p^\tau)$. So for some h we have

(10) $$x_1^{p^\tau d}+\ldots+x_s^{p^\tau d} + hp^\tau \equiv N (\operatorname{mod} p^{\tau+1}).$$

From the definition of $g(p^\tau, d)$ we have, for some a prime to p,

$$\Gamma(p^\tau d, p^{\tau+1}, ap^\tau) = g(p^\tau, d).$$

Now applying Lemma 2 with $\alpha = \tau$ and $\beta = 0$ we see that

$$\Gamma(p^\tau d, p^{\tau+1}, hp^\tau) \leqslant \Gamma(p^\tau d, p^{\tau+1}, ap^\tau)\Gamma(d, p, h\bar{a})$$

if $a\bar{a} \equiv 1 (\operatorname{mod} p)$.

Combined with (10) this gives the required result.

Thus we see that if we can get suitable bounds for $g(p^\tau, d)$ and $f(p^\tau, d)$ we will get bounds for Γ and Δ.

Let α and β continue to be non-negative integers. Then it is an immediate consequence of Lemma 2 that

(11) $$g(p^{\alpha+\beta}, d) \leqslant g(p^\alpha, d)g(p^\beta, d)$$

and

(12) $$f(p^{\alpha+\beta}, d) \leqslant f(p^\alpha, d)f(p^\beta, d).$$

In particular, for any $\tau > 0$

(13) $$g(p^\tau, d) \leqslant g(p, d)^\tau$$

and

(14) $$f(p^\tau, d) \leqslant f(p, d)^\tau.$$

Also it is immediate that $g(p^\alpha, d) \geqslant 2$ and $f(p^\alpha, d) \geqslant 2$.

3. Large p. The bound for $\Gamma_p(k)$ found in this section is valid for all primes $p \geqslant 3$ but is really only effective for large p.

LEMMA 4. *We have that*

$$g(p, d) \leqslant 3\Gamma(d, p).$$

Proof. The proof is by contradiction. We write $s = \Gamma(d, p)$ and we suppose that if for some $x_1, \ldots, x_{3s}$ we have

$$x_1^{pd}+\ldots+x_{3s}^{pd} \equiv 0 (\operatorname{mod} p)$$

then we must have

$$x_1^{pd}+\ldots+x_{3s}^{pd} \equiv 0 (\operatorname{mod} p^2).$$

Now for each $i = 1, \ldots, p-1$ we can solve

$$x_1^{pd}+\ldots+x_s^{pd} \equiv i + h_i p (\operatorname{mod} p^2),$$

where $0 \leqslant h_i \leqslant p-1$ for each i. Then by our assumption, if $i+j+k = p$ we have

$$h_i + h_j + h_k \equiv p-1 (\operatorname{mod} p)$$

and if $i+j = p$ we have

(15) $$h_i + h_j \equiv p-1 (\operatorname{mod} p).$$

So in particular, for each $i = 2, \ldots, p-1$ we have

$$h_{i-1} + h_1 + h_{p-i} \equiv p-1 (\operatorname{mod} p)$$

and

$$h_i + h_{p-i} \equiv p-1 (\operatorname{mod} p).$$

Subtracting, we get $h_i \equiv h_{i-1} + h_1 (\operatorname{mod} p)$ which gives inductively

$$h_i \equiv ih_1 (\operatorname{mod} p) \quad \text{for} \quad i = 1, \ldots, p-1$$

and in particular

$$h_{p-1} \equiv (p-1)h_1 (\operatorname{mod} p).$$

Hence we have $h_{p-1}+h_1 = ph_1 \equiv 0 \pmod{p}$ which contradicts (15) and the result is proved.

THEOREM 1. *Let $k = p^\tau dm$ where p is a prime $\geqslant 3$, $d = (k, p-1)$ and p does not divide m. Then*

$$\Gamma_p(k) \leqslant \tfrac{3}{2}\Gamma(d, p)\big(3\Gamma(d, p)\big)^\tau.$$

Proof. By Lemma 1, Lemma 3 and (13) we have

$$\Gamma_p(k) = \Gamma(p^\tau d, p^{\tau+1}) \leqslant \Gamma(d, p)\sum_{\sigma=0}^{\tau} g(p, d)^\tau = \Gamma(d, p)\frac{g(p, d)^{\tau+1}-1}{g(p, d)-1}$$

$$\leqslant \Gamma(d, p)\frac{\big(3\Gamma(d, p)\big)^{\tau+1}-1}{3\Gamma(d, p)-1} < \Gamma(d, p)\frac{\big(3\Gamma(d, p)\big)^{\tau+1}}{2\Gamma(d, p)} \quad (\text{since } \Gamma(d, p) \geqslant 2)$$

$$= \tfrac{3}{2}\Gamma(d, p)\big(3\Gamma(d, p)\big)^\tau.$$

4. p bounded. Now we obtain an estimate which is highly effective when p is bounded.

LEMMA 5. *Let p be any prime $\geqslant 3$, and let $p-1 = dt$ with $t \geqslant 2$. Then there exist arbitrarily large integers σ' such that*

$$f(p^{\sigma'}, d) \leqslant \varphi(t)p^{\frac{\sigma'}{\varphi(t)}}$$

where φ is Euler's φ-function.

Proof. Let g be a primitive root $(\bmod p)$. For $i = 1, 2, \ldots$ we define

$$R_i = g^{dp^{i-1}}.$$

Then we note that in the p-adic field the sequence $\{R_i\}$ converges to R say, where R is a primitive tth root of 1, and that for $i \leqslant j$

(16) $$R_j \equiv R_i \pmod{p^i}.$$

Let w be any integer > 0 and write $r = \varphi(t)$. We will find $\sigma' \geqslant rw$. Consider the $(p^w+1)^r$ integers

$$n_0 + n_1 R_{rw} + \ldots + n_{r-1}R_{rw}^{r-1}, \quad 0 \leqslant n_0, \ldots, n_{r-1} < p^w.$$

It is clear that two of them must be congruent $(\bmod p^{rw})$ and so it follows that there exist integers $m_0, m_1, \ldots, m_{r-1}$, not all zero such that

$$m_0 + m_1 R_{rw} + \ldots + m_{r-1}R_{rw}^{r-1} \equiv 0 \pmod{p^{rw}}, \quad 0 \leqslant |m_0|, \ldots, |m_{r-1}| \leqslant p^w,$$

or

$$F(R_{rw}) \equiv 0 \pmod{p^{rw}},$$

where $F(x)$ is the polynomial $m_0 + m_1 x + \ldots + m_{r-1}x^{r-1}$ of degree at most $r-1$ with rational integer coefficients.

Now suppose $F(R_i) \equiv 0 \pmod{p^i}$ for all $i \geqslant rw$. Then $F(R) = 0$ in the field of p-adic numbers, but F is a non-zero polynomial with rational coefficients and degree less than $\varphi(t)$ while R has degree $\varphi(t)$ over the rational numbers. Hence we have a contradiction and there exists $i > rw$ with $F(R_i) \not\equiv 0 \pmod{p^i}$. We thus have

$$F(R_i) \equiv 0 \pmod{p^{rw}} \quad \text{by (16)}$$

and

$$F(R_i) \not\equiv 0 \pmod{p^i}.$$

Let σ' be the largest integer such that

$$F(R_i) \equiv 0 \pmod{p^{\sigma'}}.$$

Clearly $\sigma' \geqslant rw$, and we have by (16)

$$F(R_{\sigma'+1}) \equiv ap^{\sigma'} \pmod{p^{\sigma'+1}}$$

for some a prime to p. Further $\sum_{j=0}^{r-1}|m_j| \leqslant rp^w \leqslant rp^{\sigma'/r}$ as required.

THEOREM 2. *Let k be any positive integer, and p any prime $\geqslant 3$. Then for any $\varepsilon > 0$ we have*

$$\Gamma_p(k) < C(p, \varepsilon)k^{\frac{1}{\varphi(t)}+\varepsilon},$$

where $t = (p-1)/d$, $d = (k, p-1)$, φ is Euler's φ-function and $C(p, \varepsilon)$ is a function of p and ε only.

Proof. If $t = 1$ the result follows from (2) and so we can assume $t \geqslant 2$. By Lemma 1 and the estimate (7), where it was observed that

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

it is sufficient to show that

$$\Delta(p^\tau d, p^{\tau+1}) < C(p, \varepsilon)k^{\frac{1}{\varphi(t)}+\varepsilon}.$$

Let σ and σ' be any positive integers. We can write $\sigma = \left[\frac{\sigma}{\sigma'}\right]\sigma' + r$, where $0 \leqslant r \leqslant \sigma'-1$, and so by (12) we get

$$f(p^\sigma, d) \leqslant f(p^{\sigma'}, d)^{[\sigma/\sigma']}f(p, d)^r \leqslant f(p^{\sigma'}, d)^{\sigma/\sigma'}f(p, d)^{\sigma'}.$$

Now by Lemma 3

(17) $$\Delta(p^\tau d, p^{\tau+1}) \leqslant \Delta(d, p)\sum_{\sigma=0}^{\tau} f(p^\sigma, d) \leqslant \Delta(d, p)f(p, d)^{\sigma'}\sum_{\sigma=0}^{\tau} f(p^{\sigma'}, d)^{\sigma/\sigma'}$$

$$< \Delta(d, p)f(p, d)^{\sigma'}f(p^{\sigma'}, d)^{(\tau+1)/\sigma'}$$

since $f(p^{\sigma'}, d) > 1$.

We now choose σ' to satisfy Lemma 5 and such that

$$\varphi(t)^{1/\sigma'} < p^{\varepsilon},$$

and (17) then gives

$$\begin{aligned} \Delta(p^{\tau}d, p^{\tau+1}) &< \Delta(d, p)f(p, d)^{\sigma'}\left(\varphi(t)p^{\frac{\sigma'}{\varphi(t)}}\right)^{\frac{\tau+1}{\sigma'}} \\ &= \Delta(d, p)f(p, d)^{\sigma'}\left(\varphi(t)^{\frac{1}{\sigma'}}p^{\frac{1}{\varphi(t)}}\right)^{\tau+1} \\ &< \Delta(d, p)f(p, d)^{\sigma'}p^{\left(\frac{1}{\varphi(t)}+\varepsilon\right)(\tau+1)} \\ &\leqslant \Delta(d, p)f(p, d)^{\sigma'}p^{\frac{1}{\varphi(t)}+\varepsilon}k^{\frac{1}{\varphi(t)}+\varepsilon}, \end{aligned}$$

as required.

5. The main result. First we note that if $d^3 < p$ then $\Gamma(d, p) \leqslant 6$ ([1], Lemma 3).

THEOREM 3. *Given* $\varepsilon > 0$ *then*

$$\Gamma_p(k) \leqslant k^{1/2+\varepsilon}$$

for all integers $k > 0$ *and all primes* p *such that* $\frac{1}{2}(p-1)$ *does not divide* k.

Proof. As usual we write $k = p^{\tau}dm$ where p does not divide m and $d = (k, p-1)$. Let $\varepsilon > 0$ be given. By (4) we can find an integer D such that for $d \geqslant D$, $\Gamma(d, p) < d^{1/2+\varepsilon/2}$. We can then find an integer P such that $P > D^3$, $P^{\varepsilon/2} > 3$ and $P^{1/2} > 18$.

We consider three cases

(i) $p > P$ and $d > p^{1/3}$. Then $d > D$ and by Theorem 1

$$\begin{aligned} \Gamma_p(k) &< \tfrac{3}{2}d^{1/2+\varepsilon/2}(3d^{1/2+\varepsilon/2})^{\tau} \\ &< \tfrac{3}{2}d^{1/2+\varepsilon/2}(3p^{1/2+\varepsilon/2})^{\tau} < \tfrac{3}{2}d^{1/2+\varepsilon}p^{1/2+\varepsilon} \leqslant \tfrac{3}{2}k^{1/2+\varepsilon}. \end{aligned}$$

(ii) $p > P$ and $d < p^{1/3}$. Then $\Gamma(d, p) \leqslant 6$ and by Theorem 1

$$\Gamma_p(k) < \tfrac{3}{2} \times 6 \times 18^{\tau} < 9p^{\tau/2} \leqslant 9k^{1/2}.$$

(iii) $p < P$. The assumption $\frac{1}{2}(p-1)$ does not divide k implies $t > 2$ and so $\varphi(t) \geqslant 2$. Hence by Theorem 2

$$\Gamma_p(k) \ll k^{\frac{1}{\varphi(t)}+\varepsilon} \leqslant k^{\frac{1}{2}+\varepsilon}$$

and the proof of the theorem is complete.

References

[1] J. D. Bovey, *On the congruence* $a_1x_1^k + \ldots + a_sx_s^k \equiv N \pmod{p^n}$, Acta Arith. 23 (1973), pp. 257–269.

[2] I. Chowla, *On Waring's problem* (mod$p$), Proc. Nat. Acad. Sci. India, A, 12 (1943), pp. 195–220.

[3] M. M. Dodson, *On Waring's problem in p-adic fields*, Acta Arith. 22 (1973), pp. 315–327.

[4] M. M. Dodson and A. Tietäväinen, *A note on Waring's problem in* GF$[p]$, Acta Arith., to appear.

[5] 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.

[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. Ser. AI 554 (1973).

Received on 5. 4. 1974

and in revised form on 15. 11. 1974 (555)