ACTA ARITHMETICA
XXIII (1973)

# On the congruence $a_1x_1^k+\ldots+a_sx_s^k \equiv N(\mathrm{mod}\,p^n)$

by

J. D. Bovey (Heslington)

**§ 1. Introduction.** Let $p^n$ be any prime power and $k$ any positive integer. We define $\Gamma(k, p^n)$ as the least positive integer $s$ such that

$$(1)\qquad x_1^k+\ldots+x_s^k \equiv N(\mathrm{mod}\,p^n)$$

has a primitive solution for all integers $N$ (a primitive solution is one in which not all the variables are divisible by $p$). Dodson [3] has shown that for sufficiently large $k$ and for any prime $p$ such that $\frac{1}{2}(p-1)$ does not divide $k$

$$\Gamma(k, p^n) < k^{\frac{7}{8}-\eta} \quad \text{for all } n$$

where $\eta$ is a small positive absolute constant.

The object of this paper is to extend this estimate to the more general congruence

$$(2)\qquad c_1x_1^k+\ldots+c_sx_s^k \equiv N(\mathrm{mod}\,p^n)$$

where $c_1, \ldots, c_s$ are prime to $p$.

We define $\Gamma^\dagger(k, p^n)$ as the least $s$ such that (2) has a primitive solution for all integers $c_1, \ldots, c_s$ prime to $p$ and for all integers $N$.

We also define

$$\Gamma_p(k) = \sup_n \Gamma(k, p^n)$$

and

$$\Gamma_p^\dagger(k) = \sup_n \Gamma^\dagger(k, p^n).$$

Plainly $\Gamma_p(k) \leqslant \Gamma_p^\dagger(k)$ (indeed $\Gamma(k, p^n) \leqslant \Gamma^\dagger(k, p^n)$ for all $n$) and in the other direction we prove

THEOREM 1. *For all positive integers $k$ and all primes $p$ we have*

$$\Gamma_p^\dagger(k) \ll (\log k)^7\,\Gamma_p(k),$$

*where $\ll$ as usual denotes inequality with a fixed positive constant.*

From this and the result of Dodson it clearly follows that

THEOREM 2. *For all sufficiently large $k$ and all primes $p$ such that $\frac{1}{2}(p-1)$ does not divide $k$ we have*

$$\Gamma_p^\dagger(k) < k^{7/8}.$$

We remark that $\Gamma_p^\dagger(k)$ is the least $s$ such that we can solve the equation

$$c_1x_1^k+\ldots+c_sx_s^k = N$$

non-trivially in the ring of $p$-adic integers, for all $p$-adic units $c_1, \ldots, c_s$ and all $p$-adic integers $N$.

In § 2 we prove some special cases and then in § 3 we prove the main results.

**§ 2.** We define $\gamma(k, p^n)$ as the least $s$ such that we can solve (1) for all integers $N$. Similarly we define $\gamma^\dagger(k, p^n)$ as the least $s$ such that we can solve (2) for all integers $c_1, \ldots, c_s$ prime to $p$ and all integers $N$. The difference between $\Gamma$, $\Gamma^\dagger$ and $\gamma$, $\gamma^\dagger$ is that in the latter case we allow non-primitive solutions.

Clearly

$$\gamma(k, p^n) \leqslant \Gamma(k, p^n) \leqslant \gamma(k, p^n)+1 \tag{3}$$

and

$$\gamma^\dagger(k, p^n) \leqslant \Gamma^\dagger(k, p^n) \leqslant \gamma^\dagger(k, p^n)+1 \tag{4}$$

for all $k$ and $p^n$.

If $k$ is a positive integer and $p$ a prime we can then write $k = p^\tau dm$ where $d = (k, p-1)$ and $p$ does not divide $m$. We write

$$\nu = \begin{cases} \tau+1, & p \text{ odd}, \\ \tau+2, & p = 2. \end{cases}$$

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

$$\gamma(k, p^\nu) = \gamma(p^\tau d, p^\nu) \leqslant \Gamma_p(k) = \Gamma_p(p^\tau d) \leqslant \gamma(p^\tau d, p^\nu)+1,$$
$$\gamma^\dagger(k, p^\nu) = \gamma^\dagger(p^\tau d, p^\nu) \leqslant \Gamma_p^\dagger(k) = \Gamma_p^\dagger(p^\tau d) \leqslant \gamma^\dagger(p^\tau d, p^\nu)+1.$$

Proof. It is well known (see [2], page 36 for instance) that if, for an integer $a$, we can solve

$$x^k \equiv a \pmod{p^\nu}$$

with $p$ not dividing $x$, then we can solve

$$x^k \equiv a \pmod{p^n} \quad \text{for all } n.$$



It follows at once from this that

$$\sup_n \gamma(k, p^n) = \gamma(k, p^\nu), \qquad \sup_n \gamma^\dagger(k, p^n) = \gamma^\dagger(k, p^\nu)$$

and the result follows from this and (3) and (4).

LEMMA 2. *Let $M$ be any integer, and let $a_1, \ldots, a_n$ be incongruent* (mod $M$) *and $b_1, \ldots, b_m$ incongruent* (mod $M$) *and such that $b_1 = 0$ and $(b_i, M) = 1$ for $i = 2, \ldots, m$.*

*Then $a_i+b_j$ represents at least* $\min(m+n-1, M)$ *different residue classes* (mod $M$).

Proof. This is due to I. Chowla [1] but a more convenient reference is [6], p. 49, Theorem 15.

PROPOSITION 1. *If $k = 2^\tau m$ where $m$ is odd, $t > 0$ and $k > 2$ then*

$$\Gamma_2^\dagger(k) = \Gamma_2(k) = 2^{\tau+2}.$$

Proof. It can easily be seen that $x^k$ can represent just 1 and 0 (mod $^{\tau+2}$). Hence for any fixed $c_i \not\equiv 0 \pmod 2$ $c_ix^k$ represents 2 different residue classes $(\bmod 2^{\tau+2})$ with one of them $\equiv 0$ and the other coprime to $2^{\tau+2}$. Thus, using Lemma 2 inductively

$$c_1x_1^k+\ldots+c_sx_s^k$$

represents at least $\min(s+1, 2^{\tau+2})$ different residue classes $(\bmod 2^{\tau+2})$. Putting $s = 2^{\tau+2}-1$ we see that

$$\gamma^\dagger(k, 2^{\tau+2}) \leqslant 2^{\tau+2}-1$$

and hence by Lemma 1

$$\Gamma_2^\dagger(k) \leqslant 2^{\tau+2}.$$

On the other hand

$$x_1^k+\ldots+x_s^k \equiv 2^{\tau+2} \pmod{2^{\tau+2}}$$

has a primitive solution only if $s \geqslant 2^{\tau+2}$ and so we have

$$2^{\tau+2} \leqslant \Gamma_2(k) \leqslant \Gamma_2^\dagger(k) \leqslant 2^{\tau+2}$$

and the result follows.

In Proposition 2 we determine $\Gamma_p^\dagger(k)$ when $\frac{1}{2}(p-1)\,|\,k$. These results are not needed in the rest of the paper but are included here for completeness.

For the proof of the next proposition we make use of the number $\gamma^*(k, p^n)$ which is defined as the least $s$ such that

$$c_1x_1^k+\ldots+c_sx_s^k \equiv 0 \pmod{p^n}$$

has a primitive solution for all $c_1, \ldots, c_s$ prime to $p$.

PROPOSITION 2. *Suppose $k$ is of the form $k = p^\tau dm$ where $d = (k, p-1)$, $p$ does not divide $m$ and $p$ is an odd prime. Then*

$$\gamma^\dagger(k, p^{\tau+1}) \leqslant \frac{p^{\tau+1}-1}{t} \tag{5}$$

*where $t = (p-1)/d$.*

*Further*

(i) *if $d = p-1$*

$$\Gamma_p^\dagger(k) = p^{\tau+1} = \Gamma_p(k);$$

(ii) *if $d = \frac{1}{2}(p-1)$ and either $p > 5$ or $\tau > 0$ then*

$$\Gamma_p^\dagger(k) = \tfrac{1}{2}(p^{\tau+1}-1) = \Gamma_p(k);$$

(iii) *if $d = 2$, $p = 5$, $\tau = 0$ then*

$$\Gamma_5^\dagger(k) = 3 = \Gamma_5(k)+1;$$

(iv) *if $d = 1$, $p = 3$, $\tau = 0$ then*

$$\Gamma_3^\dagger(k) = 2 = \Gamma_3(k).$$

Proof. The results for $\Gamma_p(k)$ are well known (see [7]) but we prove them here.

For any fixed $c_i \not\equiv 0 \pmod p$ $c_i x_i^k$ (for $n_i = 0$ or $p \nmid n_i$) represents $t+1$ different residue classes $(\bmod p^{\tau+1})$ with one of them $= 0$ and the rest coprime to $p^{\tau+1}$. Hence by induction using Lemma 2

$$c_1 x_1^k + \ldots + c_s x_s^k$$

represents at least $\min(st+1, p^{\tau+1})$ different residue classes $(\bmod p^{\tau+1})$. Putting $s = (p^{\tau+1}-1)/t$ gives the inequality.

In (i) $d = p-1$, so that $t = 1$ and (5) together with Lemma 1 gives

$$\Gamma_p^\dagger(k) \leqslant p^{\tau+1}-1+1 = p^{\tau+1}.$$

On the other hand $x^k \equiv 1$ or $0 \pmod{p^{\tau+1}}$ and so we can only solve

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

non-trivially if $s \geqslant p^{\tau+1}$. Hence we have

$$p^{\tau+1} \leqslant \Gamma_p(k) \leqslant \Gamma_p^\dagger(k) \leqslant p^{\tau+1},$$

which gives the required result for (i).

It is easy to see, using the same method as in Lemma 1 that

$$\sup_n \gamma^*(k, p^n) = \gamma^*(k, p^\nu) = \gamma^*(k, p^{\tau+1})$$

for $p$ odd.



Therefore we have (since $\gamma^\dagger(k, p^{\tau+1})$ allows the possibility of a non primitive representation of 0)

$$\Gamma_p^\dagger(k) \leqslant \max\big(\gamma^\dagger(k, p^{\tau+1}), \gamma^*(k, p^{\tau+1})\big).$$

In the case $d = \frac{1}{2}(p-1)$ Dodson ([4], p. 179) has shown that

$$\gamma^*(k, p^{\tau+1}) = \left[\frac{(\tau+1)\log p}{\log 2}\right]+1$$

and so in this case we have

$$\Gamma_p^\dagger(k) \leqslant \max\left(\frac{p^{\tau+1}-1}{2}, \left[\frac{(\tau+1)\log p}{\log 2}\right]+1\right).$$

The first term is larger if $p^{\tau+1} > 5$ and so in (ii) we have

$$\Gamma_p^\dagger(k) \leqslant \frac{p^{\tau+1}-1}{2}$$

but $x^k$ represents just $1$, $-1$ and $0 \pmod{p^{\tau+1}}$ and so clearly we cannot solve

$$x_1^k + \ldots + x_s^k \equiv \tfrac{1}{2}(p^{\tau+1}-1) \pmod{p^{\tau+1}}$$

unless $s \geqslant \frac{1}{2}(p^{\tau+1}-1)$, thus we have

$$\Gamma_p(k) \geqslant \tfrac{1}{2}(p^{\tau+1}-1)$$

and (ii) follows. If $p = 5$ and $\tau = 0$ the second term equals 3. Clearly we cannot solve $2x^2+y^2 \equiv 0 \pmod 5$ non-trivially and so (iii) follows. Part (iv) is trivial.

When $d^2 < p$, exponential sum techniques give good estimates for $\gamma^\dagger(d, p)$.

We write

$$e_p(b) = e^{\frac{2\pi i b}{p}},$$

$$S(b) = \sum_{x=0}^{p-1} e_p(bx^d),$$

$$\tau(\chi) = \sum_{x=1}^{p-1} \chi(x) e_p(x),$$

where $\chi$ is any Dirichlet character $(\bmod p)$ and $\chi_0$ is the principal character. It is easily shown that [8]

$$S(b) = \sum_{\chi} \bar\chi(b)\tau(\chi),$$

where the sum is over the $d-1$ non principal characters $\chi$ satisfying $\chi^d = \chi_0$; and that for non principal characters $\chi$,

$$|\tau(\chi)| = p^{1/2}.$$

LEMMA 3. *Suppose $d^3 < p$ and $d \mid p-1$. Then*

$$\gamma^\dagger(d, p) < 6.$$

Proof. Suppose that for some $c_1, \ldots, c_s$, $N$ we cannot solve

$$c_1x_1^d + \ldots + c_sx_s^d \equiv N(\bmod p).$$

We show that this implies $s < 6$.

We have that

$$\sum_{y=0}^{p-1}\sum_{x_1=0}^{p-1}\ldots\sum_{x_s=0}^{p-1} e_p\big(y(c_1x_1^d+\ldots+c_sx_s^d-N)\big) = 0,$$

i.e. that

$$p^s + \sum_{y=1}^{p-1} S(yc_1)\ldots S(yc_s)e_p(-yN) = 0$$

on rearranging

$$\sum_{y=1}^{p-1}\sum_{\chi_1}\ldots\sum_{\chi_s}\bar\chi_1(yc_1)\ldots\bar\chi_s(yc_s)\tau(\chi_1)\ldots\tau(\chi_s)e_p(-yN) = -p^s$$

where $\chi_1, \ldots, \chi_s$ are again summed over all the $d-1$ non principal characters satisfying $\chi^d = \chi_0$.

Taking the moduli we get

$$\sum_{y=1}^{p-1}\sum_{x_1}\ldots\sum_{x_s} p^{s/2} \geqslant p^s$$

and hence certainly

$$(p-1)(d-1)^s p^{s/2} \geqslant p^s, \qquad d^s > p^{s/2-1}.$$

But by hypothesis $d^3 < p$ and so $s/3 > s/2-1$ which implies $s < 6$ as required.

**§ 3.** Let $c_1, \ldots, c_s$ be a finite sequence of integers. We say a set of $r$ terms in the sequence is an $(r, a, N)$ set if the sum of the terms is congruent to $a(\bmod N)$. Let $k = p^\tau dm$ as usual and consider the congruence

$$c_1x_1^k + \ldots + c_sx_s^k \equiv N(\bmod p^{\tau+1}). \tag{6}$$

Suppose we can find $\gamma(k, p^{\tau+1})$ disjoint $(r, a, p^{\tau+1})$ sets of the $c_1, \ldots, c_s$ for some $a$ not divisible by $p$ and for some $r \geqslant 1$. Then by putting $x_i = x_j$



if $c_i$ and $c_j$ are in the same set and $x_j = 0$ if $c_j$ is in non of the sets, we find that we can solve (6) if we can solve

$$a(x_1^k+\ldots+x_\gamma^k) \equiv N(\bmod p^{\tau+1}) \quad \text{where} \quad \gamma = \gamma(k, p^{\tau+1}),$$

which we clearly can by the definition of $\gamma(k, p^{\tau+1})$. The following two combinatorial lemmas give sufficient conditions to make this possible.

LEMMA 4. *Let $p$ be an odd prime and let $c_1, \ldots, c_s$ be a finite sequence of integers prime to $p$. Let $\gamma$ be any positive integer and suppose*

$$s \geqslant 36([\log p]+1)^4\gamma.$$

*Then for some $a$ prime to $p$ and for some $r$ we can find $\gamma$ disjoint $(r, a, p)$ sets.*

Proof. Suppose $c_1, \ldots, c_s$ is such that for all $r$ and for all $a$ prime to $p$ we cannot find $\gamma$ disjoint $(r, a, p)$ sets. We shall show that this implies $s < 36([\log p]+1)^4\gamma$. We can assume $\gamma \leqslant s$.

We let $f(r, a)$ be the number of $(r, a, p)$ sets and let

$$f(r) = \max_{a\not\equiv 0(p)} f(r, a).$$

We find an upper bound for $f(r)$. Suppose $p$ does not divide $a$ and $2 \leqslant r \leqslant s$, let $X_1, \ldots, X_\alpha$ be a maximal set of disjoint $(r, a, p)$ sets in $c_1, \ldots, c_s$. Then our assumption above implies $\alpha < \gamma$.

$X = \bigcup_{i=1}^{\alpha} X_i$ contains $\alpha r$ terms and any $(r, a, p)$ set in $c_1, \ldots, c_r$ must contain at least one term in $X$. Moreover if say $c_1, \ldots, c_r$ is an $(r, a, p)$ set then $a-c_1 \equiv c_2+\ldots+c_r(\bmod p)$ and so $c_2, \ldots, c_r$ is an $(r-1, a-c_1, p)$ set. Thus since every $(r, a, p)$ set has at least one element $c$ say in $X$, the number of $(r, a, p)$ sets

$$f(r, a) \leqslant \sum_{c\in X} f(r-1, a-c).$$

By hypothesis less than $\gamma$ of the $c$ can be congruent to $a$ and so we can write

$$f(r, a) < \gamma r f(r-1) + \gamma f(r-1, 0).$$

And thus

$$f(r) < \gamma r f(r-1) + \gamma f(r-1, 0). \tag{7}$$

Next we estimate $f(r-1, 0)$. For any $r$ the number of $r$-tuples $(c_{i_1}, \ldots, c_{i_r})$ with $c_{i_1}+\ldots+c_{i_r} \equiv a(\bmod p)$ is equal to $r!f(r, a)$. For each $c_{i_1}$, $i_1 = 1, \ldots, s$, the number of $r$-tuples $(c_{i_1}, \ldots, c_{i_r})$ satisfying

$$c_{i_1}+\ldots+c_{i_r} \equiv 0(\bmod p)$$

is equal to $(r-1)!f(r-1, -c_{i_1})$, and so we have

$$r!f(r, 0) = \sum_{i=1}^{s} (r-1)!f(r-1, -c_i),$$

which gives

(8) $$f(r, 0) \leqslant \frac{s}{r} f(r-1).$$

Substituting (8) in (7) gives, for $3 \leqslant r \leqslant s$

(9) $$f(r) < \gamma r f(r-1) + \frac{\gamma s}{r-1} f(r-2),$$

and as $f(1) < \gamma$ and $f(1, 0) = 0$, (7) implies that

(10) $$f(2) < 2\gamma^2.$$

Now if we let

$$f(r) = \gamma^r r! \left(\frac{s}{\gamma}\right)^{(r-1)/2} g(r)$$

and substitute this in (9) we get

$$\gamma^r r! \left(\frac{s}{\gamma}\right)^{(r-1)/2} g(r) < \gamma^r r! \left(\frac{s}{\gamma}\right)^{(r-2)/2} g(r-1) + \gamma^{r-1} \frac{(r-2)!}{r-1} s \left(\frac{s}{\gamma}\right)^{(r-3)/2} g(r-2)$$

which on simplifying gives

$$g(r) < \left(\frac{\gamma}{s}\right)^{1/2} g(r-1) + \frac{1}{r(r-1)^2} g(r-2) \quad \text{for} \quad r \geqslant 3.$$

Also by (10), $g(1)$ and $g(2)$ are $< 1$. We can assume w.l.o.g.

$$\left(\frac{\gamma}{s}\right)^{1/2} < \frac{1}{2} \quad \text{and} \quad \frac{1}{r(r-1)^2} < \frac{1}{2} \quad \text{if } r \geqslant 3$$

and so by induction $g(r) < 1$ for all $r$, $1 \leqslant r \leqslant s$. We get therefore

(11) $$f(r) < \gamma^r r! \left(\frac{s}{\gamma}\right)^{(r-1)/2}.$$

Now

$$f(r, 0) \leqslant \frac{s}{r} f(r-1) < \frac{s}{r} \gamma^{r-1} (r-1)! \left(\frac{s}{\gamma}\right)^{(r-2)/2} < \gamma^r r! \left(\frac{s}{\gamma}\right)^{r/2}$$

and so we get that for all $a$ and for all $r$

(12) $$f(r, a) < r!(\gamma s)^{r/2}.$$



Now for any $r$ we have that $\sum_{a=0}^{p-1} f(r, a)$ is the number of all possible sets of $r$ terms chosen from the $s$ coefficients and so we have

$$\sum_{a=0}^{p-1} f(r, a) = \binom{s}{r}$$

and so

$$pr!\,(\gamma s)^{r/2} > \frac{s!}{(s-r)!\,r!},$$

whence

$$pr^{2r} (\gamma s)^{r/2} > (s-r)^r.$$

Extracting $r$th roots we get

$$s < p^{1/r} r^2 \gamma^{1/2} s^{1/2} + r < 2p^{1/r} r^2 \gamma^{1/2} s^{1/2}$$

and putting $r = [\log p]+1$ we get

$$s < 6([\log p]+1)^2 \gamma^{1/2} s^{1/2},$$

i.e.

$$s < 36([\log p]+1)^4 \gamma$$

as required.

LEMMA 5. *Let $b_1, \ldots, b_s$ be a finite sequence of integers, let $\beta$ be any positive integer and suppose*

$$s \geqslant 15([\log p^\tau]+1)^3 \beta$$

*where $p$ is an odd prime. Then for some $a$ and for some $r$ prime to $p$ we can find $\beta$ disjoint $(r, a, p^\tau)$ sets.*

Proof. Suppose that $b_1, \ldots, b_s$ is such that for all $a$, and for all $r$ prime to $p$, we cannot find $\beta$ disjoint $(r, a, p^\tau)$ sets. We will show that this implies $s < 15([\log p^\tau]+1)^3 \beta$. We let $f(r, a)$ be the number of $(r, a, p^\tau)$ sets and we show by induction on $r$ that

$$f(r, a) < \beta^r r! \left(\frac{s}{\beta}\right)^{[r/p]} \quad \text{for all } r, a.$$

Clearly it is true for $r = 1$. Suppose that for some $r$ and for all $a$

$$f(r-1, a) < \beta^{r-1} (r-1)! \left(\frac{s}{\beta}\right)^{[(r-1)/p]}.$$

We consider 2 cases:

(i) $p$ does not divide $r$. Let $a$ be any integer and let $X_1, \ldots, X_\alpha$ be a maximal disjoint set of $(r, a, p^\tau)$ sets. Then $\alpha < \beta$ and $X = \bigcup_{i=1}^{\alpha} X_i$

contains $ar$ terms. Any $(r, a, p^\tau)$ set must contain some term in $X$ and so

$$f(r, a) \leqslant \sum_{b\in X} f(r-1, a-b) \leqslant ar\beta^{r-1}(r-1)!\left(\frac{s}{\beta}\right)^{[(r-1)/p]} < \beta^r r!\left(\frac{s}{\beta}\right)^{[r/p]}$$

as required.

(ii) $p\mid r$. For each $i = 1, \ldots, s$ the number of $(r, a, p^\tau)$ sets containing $b_i$ is less than or equal to $f(r-1, a-b_i)$ and so we get

$$f(r, a) \leqslant \sum_{i=1}^{s} f(r-1, a-b_i) < s\beta^{r-1}(r-1)!\left(\frac{s}{\beta}\right)^{[(r-1)/p]}$$
$$< \beta^r r!\left(\frac{s}{\beta}\right)\left(\frac{s}{\beta}\right)^{[(r-1)/p]} = \beta^r r!\left(\frac{s}{\beta}\right)^{[r/p]} \quad \text{as } p\mid r$$

and this again is what is required.

Now we have

$$\sum_{a=0}^{p^\tau-1} f(r, a) = \binom{s}{r}.$$

Whence

$$p^\tau \beta^r r!\left(\frac{s}{\beta}\right)^{[r/p]} > \frac{s!}{(s-r)!\,r!}$$

and as we can assume $s \geqslant \beta$

$$p^\tau\left(\beta r^2\left(\frac{s}{\beta}\right)^{1/p}\right)^r > (s-r)^r.$$

Extracting $r$th roots and taking $r = [\log p^\tau]+1$ we get that

$$6\beta r^2\left(\frac{s}{\beta}\right)^{1/p} > s$$

and so

$$6\beta^{(p-1)/p} r^2 > s^{(p-1)/p},$$

i.e.

$$6^{p/(p-1)}\beta r^{2p/(p-1)} > s.$$

But $p \geqslant 3$ and so

$$s < 6^{3/2}\beta r^3$$

or

$$s < 15([\log p^\tau]+1)^3\beta$$

as required.

THEOREM 1. *For every positive integer $k$ and every prime $p$ we have*

$$\Gamma_p^\dagger(k) \ll (\log k)^7\,\Gamma_p(k).$$



Proof. As usual we write $k = p^\tau dm$ with $d = (p-1, k)$, $p$ does not divide $m$. We can assume that $p$ is odd because if $p = 2$ the result follows from Proposition 1.

Suppose that $\tau = 0$ and we have $c_1, \ldots, c_s$ prime to $p$ with

$$s \geqslant 36([\log p]+1)^4\gamma(d, p),$$

then, by Lemma 4, we can find $\gamma(d, p)$ disjoint $(r, a, p)$ sets of the $c_i$ for some $r$ and for some $a$ prime to $p$. Hence we can solve

$$c_1x_1^k+\ldots+c_sx_s^k \equiv N \pmod p$$

for all integers $N$ and we have

$$\gamma^\dagger(d, p) \leqslant 36([\log p]+1)^4\gamma(d, p)$$

and thus by Lemma 1

$$\Gamma_p^\dagger(k) \leqslant \gamma^\dagger(d, p)+1 \ll (\log p)^4\gamma(d, p) \leqslant (\log p)^4\Gamma_p(k).$$

But by Lemma 3 we can assume $d^3 > p$ and so

$$\Gamma_p^\dagger(k) \ll (3\log d)^4\Gamma_p(k) \ll (\log k)^4\Gamma_p(k)$$

as required.

Now suppose $\tau \geqslant 1$ and we have $c_1, \ldots, c_s$ prime to $p$ with

$$s \geqslant 15([\log p^\tau]+1)^3 36([\log p]+1)^4\gamma(k, p^{\tau+1}).$$

By Lemma 4 we can find $15([\log p^\tau]+1)^3\gamma(k, p^{\tau+1}) = \gamma_1$ say disjoint $(r, a, p)$ sets $X_1, \ldots, X_{\gamma_1}$ for some $r$ and some $a$ prime to $p$. Suppose

$$\sum_{c\in X_j} c = a+pb_j, \quad j = 1, \ldots, \gamma_1.$$

By Lemma 5 we can find $\gamma(k, p^{\tau+1}) = \gamma$ say disjoint $(r', b, p^\tau)$ sets of the $b_j$, $Y_1, \ldots, Y_\gamma$ say for some $b$ and for some $r'$ prime to $p$. If we let

$$Z_i = \bigcup_{b_j\in Y_i} X_j, \quad i = 1, \ldots, \gamma,$$

then the $Z_i$ form $\gamma(k, p^{\tau+1})$ disjoint $(rr', r'a+pb, p^{\tau+1})$ sets of the $c_i$ and $p$ does not divide $r'a$.

If we let $x_i = x_j$ if $c_i$ and $c_j$ are in the same one of these sets and if we let $x_i = 0$ if $c_i$ is in none of these sets; then we can see that we can solve

$$c_1x_1^k+\ldots+c_sx_s^k \equiv N \pmod{p^{\tau+1}}$$

if we can solve

$$(r'a+pb)(x_1^k+\ldots+x_\gamma^k) \equiv N \pmod{p^{\tau+1}}.$$

But we can always solve this by definition of $\gamma = \gamma(k, p^{\tau+1})$ and because $r'a+pb$ is prime to $p$. Hence we have

$$\gamma^{\dagger}(k, p^{\tau+1}) \leqslant 15([\log p^{\tau}]+1)^3 36([\log p]+1)^4 \gamma(k, p^{\tau+1}) \ll (\log k)^7 \gamma(k, p^{\tau+1})$$

and this, with Lemma 1, gives the result. We deduce

THEOREM 2. *If $k$ is sufficiently large and $\frac{1}{2}(p-1)$ does not divide $k$ then*

$$\Gamma_p^{\dagger}(k) < k^{7/8}.$$

Proof. Dodson [3] proved that if $\frac{1}{2}(p-1)$ does not divide $k$ then

$$\Gamma_p(k) \ll k^{7/8-\eta}$$

where $\eta$ is a small absolute positive constant. The result follows at once from this and from Theorem 1.

If $k$ is a positive integer we define $\Gamma^{\dagger}(k)$ as the least $s$ such that

$$c_1 x_1^k + \ldots + c_s x_s^k \equiv N (\operatorname{mod} p^n)$$

has a primitive solution for all integers $N$, all prime powers $p^n$ and all integers $c_1, \ldots, c_s$ with $(c_i, c_j) = 1$ if $i \neq j$. We note that if $s \geqslant \Gamma^{\dagger}(k)$ and $c_1, \ldots, c_s$ are coprime rational integers then $c_1 x_1^k + \ldots + c_s x_s^k$ represents every integer in every $p$-adic ring non-trivially. Clearly we have

$$\Gamma^{\dagger}(k) \leqslant \sup_p \Gamma_p^{\dagger}(k) + 1.$$

In conclusion we prove

THEOREM 3. *There are an infinite number of positive integers $k$ with*

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

Proof. By Theorem 2 and Propositions 1 and 2 it is sufficient to show that there are an infinite number of odd positive integers $k$ which are not divisible by 3 or by $\frac{1}{2}(p-1)$ for any prime $p \geqslant 5$. By Dirichlet's Theorem there are an infinite number of primes congruent to $1 (\operatorname{mod} 3)$. Suppose $k$ is prime and $k \equiv 1 (\operatorname{mod} 3)$ with $\frac{1}{2}(p-1) \mid k$ for some prime $p \geqslant 5$. Then

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

i.e.

$$p = 2k+1 \equiv 0 (\operatorname{mod} 3)$$

which is a contradiction.

Also it is not difficult to show that by virtue of Proposition 2 and Theorem 2 together with Theorem 2 in [5] that the average order of $\Gamma^{\dagger}$ is the same as that of $\Gamma$. In fact we have

$$\sum_{k \leqslant N} \Gamma^{\dagger}(k) = \frac{5\pi^2 N^2}{24 \log N} + O\left(\frac{N^2}{(\log N)^{3/2}}\right).$$



Acknowledgements. I am very grateful to Dr. Maurice Dodson for suggesting the problem and for his advice and encouragement. Also I would like to thank the Science Research Council for the Maintenance Grant on which the research for this paper was done.

**References**


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

[2] H. Davenport, *Analytic Methods for Diophantine Equations and Diophantine Inequalities*, Michigan 1962.

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

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

[5] — *The average order of two arithmetic functions*, Acta. Arith. 16 (1969), pp. 71–84.

[6] H. Halberstam and K. Roth, *Sequences*, Vol. 1, Oxford 1966.

[7] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum*, (VIII): *The number $\Gamma(k)$ in Waring's problem*, Proc. London Math. Soc. 28 (1928), pp. 518–542.

[8] I. M. Vinogradov, *The Method of Trigonometric Sums in the Theory of Numbers*, London 1953.


DEPARTMENT OF MATHEMATICS
UNIVERSITY OF YORK
Heslington, York

*Received on 15. 2. 1972* (258