PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Homogeneous Additive Congruences

M. Dodson

Phil. Trans. R. Soc. Lond. A 1967 **261**, 163-210
doi: 10.1098/rsta.1967.0002

HOMOGENEOUS ADDITIVE CONGRUENCES

By M. DODSON

Department of Mathematics, University of York

(*Communicated by H. Davenport, F.R.S.—Received 22 June 1966*)

CONTENTS

An investigation of conditions under which the congruence

$$a_1 x_1^k + \ldots + a_s x^k \equiv 0 \pmod{p^n},$$

where $a_1, \ldots, a_s$ are any non-zero integers and p^n is any prime power, has a primitive solution.

1. Introduction

In this paper we consider when, for given positive integral exponent k, the additive homogeneous congruence

$$a_1 x_1^k + \ldots + a_s x_s^k \equiv 0 \pmod{p^n}, \tag{1·1}$$

where $a_1, \ldots, a_s$ are arbitrary non-zero integers, has a *primitive* solution, that is a solution with the variables $x_1, \ldots, x_s$ integral and not all divisible by p, for every prime power p^n.

[*Note added in proof*, 10 *November* 1966.] Since this paper was submitted I have received a copy of K. Norton, *On homogeneous diagonal congruences of odd degree*, Technical Report No. 16, University of Illinois, Urbana, Illinois, (1966), the results of which overlap a little with those of the present paper. In particular Norton shows that $\Gamma^*(k) \geqslant 2k+1$ for all $k \geqslant 2$, and for all odd $k \geqslant 3$, he improves the estimate (1·4) of Chowla & Shimura 1963, Theorem A) for $\Gamma^*(k)$.

Vol. 261. A. 1119. (Price 18*s.*: U.S. $2.70) 21 [Published 26 January 1967

This question was studied in a paper by Davenport & Lewis (1963) on additive homogeneous equations. In their investigation they were led to consider the self-contained, purely arithmetical problem of determining the least value, which they defined to be $\Gamma^*(k)$, of s, such that the congruence (1·1) has a primitive solution for every prime power p^n. In some respects the function $\Gamma^*(k)$ is similar to the function $\Gamma(k)$, introduced by Hardy & Littlewood (1928) in their study of Waring's problem. $\Gamma(k)$ can be shown to be the least value of s for which the congruence

$$x_1^k+\ldots+x_s^k \equiv N \pmod{p^n} \tag{1·2}$$

has a primitive solution for every prime power p^n and every integer N, and some of the techniques used in estimating $\Gamma(k)$ are readily adapted to estimating $\Gamma^*(k)$.

The main object of Davenport & Lewis's paper was to establish the following sharp upper bound for $\Gamma^*(k)$: for all k we have

$$\Gamma^*(k) \leqslant k^2+1, \tag{1·3}$$

and here there is equality whenever $k+1$ is a prime. They also deduced from this and other known results that

$$\Gamma^*(3) = 7, \quad \Gamma^*(4) = 17, \quad \Gamma^*(5) = 16, \quad \Gamma^*(6) = 37.$$

Using results established in the present paper I have been able to show that $\Gamma^*(7) = 22$ and $\Gamma^*(9) = 37$, but have not yet been able to determine the value of $\Gamma^*(8)$.

When k is odd, box arguments provide an effective means of estimating $\Gamma^*(k)$, and using these, Chowla & Shimura (1963) showed that for all odd $k > k_0(\epsilon)$

$$\Gamma^*(k) < (2/(\log 2)+\epsilon)\, k \log k, \tag{1·4}$$

where ϵ is any positive number. They also proved that for an infinity of odd k

$$\Gamma^*(k) > (k \log k)/(\log 2). \tag{1·5}$$

In this paper we are concerned with obtaining estimates for $\Gamma^*(k)$ when $k+1$ is not a prime. One of the main difficulties, which does not arise in the case of Hardy & Littlewood's $\Gamma(k)$, is the arbitrariness of the coefficients $a_1, \ldots, a_s$. This makes it very difficult to compute $\Gamma^*(k)$ for a particular value of k, even if k is fairly small, unless there is a general argument which happens to give the best possible upper bound for $\Gamma^*(k)$. Our first estimate is an improvement of (1·3) when $k+1$ is not a prime; we prove

THEOREM 5·2·1. *Suppose $k+1$ is composite. Then*

$$\Gamma^*(k) \leqslant \tfrac{49}{64}k^2+1. \tag{1·6}$$

The constant $\frac{49}{64}$ is probably capable of improvement, but to effect this we should have to know more about the value of $\Gamma^*(8)$. However, if we restrict the values of k slightly, we can obtain a sharp upper bound for $\Gamma^*(k)$ when $k+1$ is composite. We prove

THEOREM 5·2·2. *Suppose $k+1$ is composite and $k \neq 8$ and $k \neq 32$. Then*

$$\Gamma^*(k) \leqslant \tfrac{1}{2}k^2\left(1+\frac{2}{1+\sqrt{(1+4k)}}\right)+1, \tag{1·7}$$

and there is equality here when $k = p(p-1)$ for some prime p, in which case the inequality becomes

$$\Gamma^*(k) = \tfrac{1}{2}k^2(1+1/p)+1. \tag{1·8}$$

By further restricting k, we obtain more sharp estimates of this nature, but the results only hold when k is very large and are not of any practical use in evaluating $\Gamma^*(k)$ for numerical values of k. When k is odd, we have the effective estimate (1·4) for $\Gamma^*(k)$, and when k is even, we show that $\Gamma^*(k)$ is of lower order than k^2 infinitely often in

THEOREM 5·4·2. *There exists an infinity of even k for which*

$$\Gamma^*(k) < 12(\log k)^2 k^{\frac{15}{8}}. \tag{1·9}$$

As regards a lower bound for $\Gamma^*(k)$, we prove

THEOREM 5·3·1. *For all k*

$$\Gamma^*(k) \geqslant k+1. \tag{1·10}$$

This lower bound is probably not the best possible and we conjecture that

$$\lim_{k\to\infty} \frac{\Gamma^*(k)}{k} = \infty. \tag{1·11}$$

The problem of establishing a good lower bound seems a difficult one and may be related to the same problem for $\Gamma(k)$, about which little is known beyond $\Gamma(k) \geqslant 3$ for all $k > 1$.

The solubility of the congruence

$$a_1 x_1^k + \ldots + a_s x_s^k \equiv 0 \pmod{p^n}, \tag{1·12}$$

where p is a prime and $a_1, \ldots, a_s$ are arbitrary integers not divisible by p, for every positive integer n, plays an important part in determining the solubility of the more general congruence (1·1). In view of this, we introduce the function $\gamma^*(k, p^n)$, which we define to be the least value of s such that the congruence (1·12) has a primitive solution for the particular prime p, and for the positive integer n. Section 2 of this paper is devoted to estimating $\gamma^*(k, p)$ for all primes p and §3 to estimating $\gamma^*(k, p^n)$ in the case when $p-1$ does not divide k.

It is convenient in our discussion of $\Gamma^*(k)$ to introduce the auxiliary function $\Gamma^*(k, p)$, which is defined to be the least value of s for which the congruence

$$a_1 x_1^k + \ldots + a_s x_s^k \equiv 0 \pmod{p^n},$$

where $a_1, \ldots, a_s$ are arbitrary non-zero integers, has a primitive solution for every positive integer n, for the particular prime p. It follows from this definition that

$$\Gamma^*(k) = \underset{(\text{primes } p)}{\text{maximum}}\, \Gamma^*(k, p). \tag{1·13}$$

We investigate $\Gamma^*(k, p)$ in §4 and we use the results obtained there to establish our results for $\Gamma^*(k)$ in §5.

2. CONGRUENCES TO A PRIME MODULUS

2·1. *Introduction*

We have defined $\gamma^*(k, p)$ as the least positive integer s with the following property: if $a_1, \ldots, a_s$ are any integers prime to p, then the congruence

$$a_1 x_1^k + \ldots + a_s x_s^k \equiv 0 \pmod{p} \tag{2·1·1}$$

has a primitive solution, that is a solution with not all of the variables $x_1, \ldots, x_s$ divisible by p. The object of this section is to estimate, or evaluate if possible, the number $\gamma^*(k,p)$.

It is well known that the non-zero residue classes (mod p) form a cyclic group of order $p-1$. From this it follows that the values assumed by x^k, for given k and arbitrary x, are the same as the values assumed by x^d, where, as always, $d = (k, p-1)$. Hence

$$\gamma^*(k,p) = \gamma^*(d,p), \tag{2·1·2}$$

and it therefore suffices to investigate $\gamma^*(d,p)$ when $p-1$ is any multiple of d. The case $d = 1$ is trivial, and plainly

$$\gamma^*(1,p) = 2. \tag{2·1·3}$$

For the remainder of this section, we suppose that $p > 2$, since for $p = 2$ the only possibility is $d = 1$, covered by (2·1·3).

The case $d = p-1$, although not so trivial, is also somewhat special, since the only values (mod p) assumed by x^d are 0 and 1. We shall easily prove (in lemma 2·3·1) that

$$\gamma^*(p-1,p) = p. \tag{2·1·4}$$

We shall use several different methods of investigation. Some of them extend naturally to the investigation of $\gamma^*(k,p^n)$ when $n > 1$, and we may quote here from the work of § 3, where this question is discussed.

2·2. *The case when $\frac{1}{2}(p-1)$ is a multiple of d*

Here a simple box argument gives a good upper bound for $\gamma^*(d,p)$ which is best possible in some cases. We can generalize the argument to the modulus p^n, and accordingly this argument appears again in § 3, but is given there in a slightly different form which is capable of being generalized further. Nevertheless, as it is so short, we give it here too, in its simpler form.

Lemma 2·2·1. *If $\frac{1}{2}(p-1)$ is a multiple of d, then*

$$\gamma^*(d,p) \leqslant [(\log p)/(\log 2)] + 1. \tag{2·2·1}$$

Here there is equality if $d = \frac{1}{2}(p-1)$ and we have

$$\gamma^*(\tfrac{1}{2}(p-1),p) = [(\log p)/(\log 2)] + 1. \tag{2·2·2}$$

Proof. The condition that $\frac{1}{2}(p-1)$ is divisible by d is sufficient (and also necessary) for -1 to be a dth power residue (mod p); this follows from the fact that the index of -1 relative to any primitive root for the prime p is $\frac{1}{2}(p-1)$. Thus the congruence (2·1·1), with d in place of k, will be non-trivially soluble provided that the congruence

$$a_1 y_1 + \ldots + a_s y_s \equiv 0 \pmod{p}$$

is soluble non-trivially with each $y_i = 0$, 1 or -1. This will be the case if the values (mod p) assumed by $a_1 t_1 + \ldots + a_s t_s$, for each $t_i = 0$ or 1, are not all mutually distinct. The number of values is 2^s, and if $2^s > p$, then the values cannot be all distinct (mod p). Hence, for the congruence (2·1·1) to have a primitive solution, it is enough if $s > (\log p)/(\log 2)$, and this gives the result expressed in (2·2·1).

If $d = \frac{1}{2}(p-1)$, the only values assumed by x^d (mod p) are 0, 1, -1. Hence in this case it is not only sufficient but also necessary that two of the values assumed by $a_1 t_1 + \ldots + a_s t_s$

should be congruent (mod p). If we take $a_i = 2^{i-1}$, the values are the integers from 0 to 2^s-1 inclusive, and these are mutually incongruent (mod p) if $p < 2^s$. It follows that the congruence is not always soluble if $s = [(\log p)/(\log 2)]$, and this (together with the previous result) implies (2·2·2).

2·3. *The addition of residue classes*

A natural approach to congruences of an additive type is through general theorems on the addition of residue classes (mod p). The simplest such theorem was given by Cauchy in 1812, but was overlooked until it had been rediscovered by Davenport (1935, 1947). It states that if $a_1, \ldots, a_m$ are distinct (mod p) and if $b_1, \ldots, b_n$ are also distinct (mod p), then the number of distinct residue classes of the form $a_i + b_j$ is at least min $(m+n-1, p)$. Using this we prove:

LEMMA 2·3·1. *We have*

$$\gamma^*(d,p) \leqslant d+1 \tag{2·3·1}$$

and

$$\gamma^*(p-1,p) = p. \tag{2·3·2}$$

Proof. The number of distinct values (mod p) assumed by x^d for $x \not\equiv 0$ (mod p) is $(p-1)/d$, this being a consequence of the fact that the non-zero residues (mod p) form a cyclic group. Hence, for $a \not\equiv 0$ (mod p), the number of distinct residue classes representable as ax^d is $(p-1)/d+1$. By induction on r, using the Cauchy–Davenport theorem, the number of residue classes representable as $a_1 x_1^d + \ldots + a_r x_r^d$ is at least min $(r(p-1)/d+1, p)$. If we take $r = d$, we get every residue class representable in this way. Hence we can solve the congruence

$$a_1 x_1^d + \ldots + a_d x_d^d \equiv -a_{d+1} \pmod{p},$$

and this proves that $\gamma^*(d,p) \leqslant d+1$.

In particular, we have $\gamma^*(p-1,p) \leqslant p$, and since the congruence

$$x_1^{p-1} + \ldots + x_{p-1}^{p-1} \equiv 0 \pmod{p}$$

is obviously insoluble except trivially, the complementary inequality also holds, whence (2·3·2).

This result was proved by Davenport & Lewis (1963) in their lemma 1 and they noted that it had also been proved by Schwarz (1948). These proofs, however, depend on a property of polynomial identities (mod p).

Most of the work done recently on the addition of residue classes is aimed at greater generality rather than greater precision, and is therefore useless for the present purpose. There is, however, one important case in which the result has been improved upon, namely by Chowla, Mann & Straus (1959). They proved that if $d < \frac{1}{2}(p-1)$ and $n \geqslant \frac{1}{2}(d+1)$, then every residue class (mod p) is representable as

$$a_1 x_1^d + \ldots + a_n x_n^d,$$

assuming that all the coefficients are prime to p. This implies immediately, in the same way as in the proof of the preceding lemma:

LEMMA 2·3·2. *If* $d < \frac{1}{2}(p-1)$ *then*

$$\gamma^*(d,p) \leqslant [\tfrac{1}{2}(d+4)]. \tag{2·3·3}$$

The results (2·3·1) and (2·3·3) have the merit of being simple and of being effective in numerical instances. In the remainder of this chapter we shall obtain results which show that $\gamma^*(d,p) = o(d)$ for $d < p-1$; these results are also effective in the sense of being explicit, but they involve fairly large numerical constants and are therefore less useful in particular cases.

2·4. *Exponential sums*

The use of exponential sums provides, as is well known, a powerful method of attack upon problems of an additive nature. For given p and d, we define

$$S(b) = \sum_{x=0}^{p-1} e_p(bx^d), \tag{2·4·1}$$

where $e_p(y) = e^{2\pi iy/p}$. This sum can be expressed in terms of the Gaussian sums corresponding to the Dirichlet characters $\chi \pmod p$ which satisfy $\chi^d = \chi_0$, where χ_0 denotes the principal character. There are exactly d such characters, and if χ is one of them other than the principal character, the Gaussian sum $\tau(\chi)$ is defined by

$$\tau(\chi) = \sum_{y=1}^{p-1} \chi(y)\, e_p(y). \tag{2·4·2}$$

For such characters, we have that if y is a dth power residue $(\mathrm{mod}\, p)$, then $\chi(y) = 1$, whence the sum of these characters is $d-1$, while if y is not a dth power residue, the characters $\chi(y)$ form a geometric progression whose sum is -1. Thus the number of solutions of

$$x^d \equiv y \pmod p$$

can be expressed as

$$1 + \sum_{\chi} \chi(y),$$

where the summation is extended over the above mentioned $d-1$ characters, and we have

$$\begin{aligned} S(b) &= \sum_{y=0}^{p-1} \{1 + \sum_{\chi} \chi(y)\}\, e_p(by) \\ &= \sum_{\chi} \sum_{y=1}^{p-1} \chi(y)\, e_p(by) \\ &= \sum_{\chi} \overline{\chi}(b)\, \tau(\chi). \end{aligned} \tag{2·4·3}$$

It is well known (Landau 1947; Satz 308) that

$$|\tau(\chi)| = p^{\frac{1}{2}} \tag{2·4·4}$$

for any non-principal character χ.

Using these results we prove

LEMMA 2·4·1. *We have*

$$\gamma^*(d,p) \leqslant \begin{cases} 3 & \text{if } p > d^4, \quad (2·4·5) \\ [(2\log 2d)/(\log 2)] + 1 & \text{if } p > 2d^2. \quad (2·4·6) \end{cases}$$

Proof. The number of solutions of the congruence

$$a_1 x_1^d + \ldots + a_{s-1} x_{s-1}^d + a_s \equiv 0 \pmod p$$

with $0 \leqslant x_j < p$ $(j=1,\ldots,s-1)$ is

$$p^{-1}\sum_{t=0}^{p-1}\sum_{x_1=0}^{p-1}\ldots\sum_{x_{s-1}=0}^{p-1} e_p(t(a_1x_1^d+\ldots+a_{s-1}x_{s-1}^d+a_s)) = p^{s-2}+p^{-1}\sum_{t=1}^{p-1} S(ta_1)\ldots S(ta_{s-1})\,e_p(ta_s).$$

By (2·4·3), the second term is

$$p^{-1}\sum_{t=1}^{p-1}\sum_{\chi_1}\ldots\sum_{\chi_{s-1}} \bar{\chi}_1(ta_1)\ldots\bar{\chi}_{s-1}(ta_{s-1})\,e_p(ta_s)\,\tau(\chi_1)\ldots\tau(\chi_{s-1}),$$

where $\chi_1,\ldots,\chi_{s-1}$ run independently through the $d-1$ non-principal characters satisfying $\chi^d=\chi_0$. If $\chi_1\ldots\chi_{s-1}=\chi_0$, we have

$$\sum_{t=1}^{p-1}\bar{\chi}_1\ldots\bar{\chi}_{s-1}(t)\,e_p(ta_s) = \sum_{t=1}^{p-1} e_p(ta_s) = -1,$$

and if $\chi_1\ldots\chi_{s-1}\neq\chi_0$, we have

$$\sum_{t=1}^{p-1}\bar{\chi}_1\ldots\bar{\chi}_{s-1}(t)\,e_p(ta_s) = \chi_1\ldots\chi_{s-1}(a_s)\,\tau(\overline{\chi_1\ldots\chi_{s-1}}).$$

Using (2·4·4), we deduce that the absolute value of the second term is at most

$$p^{-1}(d-1)^{s-1}p^{\frac{1}{2}s}.$$

Hence the congruence is soluble provided

$$p^{-1}(d-1)^{s-1}p^{\frac{1}{2}s} < p^{s-2},$$

that is, provided

$$(d-1)^{s-1} < p^{\frac{1}{2}s-1}.$$

This condition is satisfied with $s=3$ if $p>d^4$, from which it follows that $\gamma^*(d,p)\leqslant 3$ if $p>d^4$. This result has already been proved by I. Chowla (1937, theorem 1).

Now suppose only that $p>2d^2$. Then the condition is satisfied if

$$d^{s-1} < p^{\frac{1}{2}s-1},$$

that is, if

$$s \geqslant \frac{\log p-\log d}{\frac{1}{2}\log p-\log d}.$$

For fixed d and $p>d^2$, the right-hand side increases as p decreases. Hence it will suffice if

$$s \geqslant \frac{\log 2d^2-\log d}{\frac{1}{2}\log 2d^2-\log d} = \frac{2\log 2d}{\log 2}.$$

This proves (2·4·6).

2·5. *The case $d^2<p<2d^2$*

It will be seen that the result of the preceding section depends on p being appreciably greater than d^2, and that the method employed there rapidly loses its effectiveness if we allow p to approach d^2. The underlying reason for this is that expressing $S(b)$ as a sum of $d-1$ terms of the form $\chi(b)\,\tau(\chi)$, each of absolute value $p^{\frac{1}{2}}$, is no longer useful. We now modify the approach, using ideas suggested by the work of I. Chowla (1943) on Waring's problem, so as to deal with the range $d^2<p<2d^2$, for which we still get a satisfactory estimate for $\gamma^*(d,p)$. The condition $p<2d^2$ will not actually be used here.

The function $\gamma(d,p)$ was introduced by I. Chowla (1943) in his work on Waring's problem and is defined as the least positive integer r for which the congruence

$$x_1^d+\ldots+x_r^d \equiv N \pmod{p} \tag{2·5·1}$$

is soluble for all integers N.

We recall that the $p-1$ non-zero residue classes $(\mathrm{mod}\,p)$ fall into d disjoint equivalence classes, one such class consisting of the dth power residues and the others being the various classes of dth power non-residues. We denote by $\sum_b{}^*$ a summation in which b runs through a set of representatives, one from each of the d classes. Now we prove a series of results which enable us to estimate $\gamma^*(d,p)$ when $d^2<p<2d^2$.

Lemma 2·5·1.

$$\sum_b{}^*|S(b)|^2 = d(d-1)\,p. \tag{2·5·2}$$

Proof. We have

$$\sum_{t=0}^{p-1}|S(t)|^2 = \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e_p(t(x^d-y^d)) = pM,$$

where M denotes the number of solutions of the congruence $x^d \equiv y^d \pmod{p}$. For given x, there is one solution if $x \equiv 0 \pmod{p}$ and there are d solutions if $x \not\equiv 0 \pmod{p}$. Hence $M = 1+(p-1)\,d$. Since $S(0)=p$, we obtain

$$\sum_{t=1}^{p-1}|S(t)|^2 = p\{1+(p-1)\,d\}-p^2 = (d-1)\,p(p-1).$$

The lemma follows since $S(t)$ has the same value for each of the $(p-1)/d$ values of t which belong to the same one of the d classes.

Lemma 2·5·2. *Suppose that $x_1^d+\ldots+x_r^d$ does not represent every residue class $(\mathrm{mod}\,p)$. Then there exists some c, prime to p, such that*

$$|S(c)| > p(1-L), \tag{2·5·3}$$

where $L = (\log p)/r$, and this implies that

$$|S(mc)| > p(1-m^2L) \tag{2·5·4}$$

for every non-zero integer m.

Proof. Suppose $x_1^d+\ldots+x_r^d \not\equiv N \pmod{p}$. Then

$$p^{-1}\sum_{t=0}^{p-1} S(t)^r\, e_p(-tN) = 0.$$

Hence, separating out the term $t=0$, we get

$$\sum_{t=1}^{p-1} S(t)^r\, e_p(-tN) = -p^r.$$

It follows that there exists an integer c which is not divisible by p, such that

$$|S(c)|^r \geqslant \frac{p^r}{p-1} > p^{r-1},$$

whence

$$|S(c)| > p\exp\left(-\frac{\log p}{r}\right) > p\left(1-\frac{\log p}{r}\right),$$

which is (2·5·3).

Now suppose that c has this property. Then for some real θ,

$$\sum_{x=0}^{p-1} e_p(cx^d-\theta) = |S(c)| > p(1-L).$$

This implies that

$$\sum_{x=0}^{p-1} \cos(2\pi/p)(cx^d-\theta) > p(1-L),$$

whence

$$\sum_{x=0}^{p-1} \sin^2(\pi/p)(cx^d-\theta) < \tfrac{1}{2}pL.$$

Since $|\sin m\phi| \leqslant |m \sin\phi|$, we deduce that

$$\sum_{x=0}^{p-1} \sin^2(\pi m/p)(cx^d-\theta) < \tfrac{1}{2}m^2 pL,$$

whence

$$\sum_{x=0}^{p-1} \cos(2\pi m/p)(cx^d-\theta) > p(1-m^2L),$$

and this gives (2·5·4).

LEMMA 2·5·3. *Suppose that* 2 *is a d-th power residue* (mod p). *Then*

$$\gamma(d,p) < [(\log p)/(\log 2)]+1. \tag{2·5·5}$$

Proof. We have to prove that every integer N is congruent (mod p) to a sum of at most $[(\log p)/(\log 2)]+1$ dth powers. Without loss of generality we can suppose $0 \leqslant N < p$, and then we can express N as

$$N = a_0+2a_1+\ldots+2^h a_h,$$

where each a_i $(i=1,\ldots,h-1)$ is 0 or 1 and $a_h = 1$. Plainly $2^h < p$. Now each term is a dth power, and so N is congruent to a sum of at most $(h+1)$ dth powers, which gives the result.

LEMMA 2·5·4. *If* $d^2 < p < 2d^2$, *then*

$$\gamma(d,p) < [8\log p]+1. \tag{2·5·6}$$

Proof. It suffices to prove that the congruence (2·5·1) is soluble for $r = [8\log p]+1$. We suppose the contrary and obtain a contradiction. By lemma 2·5·2, there exists an integer c, prime to p, such that

$$|S(c)| > p(1-L), \quad |S(2c)| > p(1-4L),$$

where $L = (\log p)/r < \frac{1}{8}$.

If 2 is not a dth power residue (mod p), we can take c and $2c$ as representatives of two different classes in the sum of lemma 2·5·1. This gives

$$p^2(1-L)^2+p^2(1-4L)^2 \leqslant pd(d-1) < p^2,$$

whereas on the contrary, since $L < \frac{1}{8}$, we have

$$(1-L)^2+(1-4L)^2 > \tfrac{49}{64}+\tfrac{1}{4} > 1.$$

Hence 2 must be a dth power residue (mod p), and now Lemma 2·5·3 implies that the congruence (2·5·1) is soluble with r satisfying

$$r \leqslant [(\log p)/(\log 2)]+1.$$

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

This clearly contradicts the assumption that the congruence was insoluble for

$$r = [8 \log p] + 1,$$

and hence gives us the result.

LEMMA 2·5·5. *If* $d^2 < p < 2d^2$, *then*

$$\gamma^*(d,p) \leqslant [12 \log p] + 1. \tag{2·5·6a}$$

Proof. The total number of solutions of the congruence

$$a_1 x_1^d + \ldots + a_s x_s^d \equiv 0 \pmod{p}, \tag{2·5·7}$$

with $0 \leqslant x_j < p$ $(j = 1, \ldots, s)$ is

$$p^{-1} \sum_{t=0}^{p-1} S(ta_1) \ldots S(ta_s).$$

Suppose the congruence (2·5·7) has only the trivial solution for $s = [12 \log p] + 1$, so that the total number of solutions must be 1. It follows that we get, on separating out the term $t = 0$,

$$\sum_{t=1}^{p-1} S(ta_1) \ldots S(ta_s) = p - p^s.$$

Hence

$$\sum_{t=1}^{p-1} |S(ta_1) \ldots S(ta_s)| \geqslant p^s - p,$$

and it follows that there exists an integer c, prime to p, for which

$$|S(ta_1) \ldots S(ta_s)| \geqslant \frac{p^s - 1}{p - 1} > p^{s-1}.$$

Suppose, as we may, that $|S(ta_1)| \geqslant |S(ta_2)| \geqslant \ldots \geqslant |S(ta_s)|$.

Then

$$|S(ta_1)| > p^{1-1/s} > p\left(1 - \frac{\log p}{s}\right).$$

Further, since $|S(ta_1)| \leqslant p$, we have

$$|S(ta_2)| > p^{(s-2)/(s-1)} > p\left(1 - \frac{\log p}{s-1}\right),$$

and so on. Generally, provided $j \leqslant s$,

$$|S(ta_j)| > p\left(1 - \frac{\log p}{s-j+1}\right).$$

Suppose that we can choose r to satisfy

$$s - r + 1 > \tfrac{7}{2} \log p. \tag{2·5·8}$$

Then $|S(ta_j)| > \frac{5}{7}p$ for $j = 1, \ldots, r$. If $a_1, \ldots, a_r$ did not belong to the same equivalence class (mod p), we could take two of them as values of b in the sum of lemma 2·5·1, giving

$$(\tfrac{5}{7}p)^2 + (\tfrac{5}{7}p)^2 \leqslant pd(d-1) < p^2,$$

which is a contradiction.

Hence, provided r and s satisfy the above condition, $a_1, \ldots, a_r$ all belong to the same equivalence class and we can write the congruence (2·5·7) as

$$a_1(y_1^d + \ldots + y_r^d) + \ldots + a_s y_s^d \equiv 0 \pmod{p}.$$

We have supposed this congruence to have only the trivial solution for $s = [12\log p]+1$. Hence the congruence

$$a_1(y_1^d+\ldots+y_r^d)+a_s \equiv 0 \pmod p \qquad (2\cdot5\cdot9)$$

is *a fortiori* insoluble. But since $s = [12\log p]+1$ enables us to take $r = [8\log p]+1$ and still have r satisfying (2·5·8), the congruence (2·5·9) is soluble by lemma 2·5·4, and so we have a contradiction. This gives us the result.

2·6. *The case $p < d^2$*

We first develop a more elaborate version of the preceding argument and obtain an estimate for $\gamma^*(d,p)$ which is satisfactory if p is not much less than d^2. The following lemma is due to Davenport. The idea behind it is not new and is used in Landau (1947) in Satz 300, which is due to Hardy & Littlewood.

LEMMA 2·6·1. *Suppose that none of the integers $2, 3, \ldots, M$ (where $2 \leqslant M < p$) is a d-th power residue* (mod p). *Let the number of distinct equivalence classes to which $1, 2, \ldots, M$ belong be h. Then every integer up to and including M, is representable as a sum of h d-th powers* (mod p).

Proof. Let $C_1, C_2, \ldots, C_h$ be the h equivalence classes to which $1, 2, \ldots, M$ belong, and let b_i denote the greatest of these integers in the class C_i. We arrange $C_1, C_2, \ldots, C_h$ in increasing order of $b_1, b_2, \ldots, b_h$. Then, by hypothesis, C_1 contains 1 and no other integer up to M. Let $n(C)$ denote the number of dth powers needed to represent an element of the class C (it is obviously the same for all elements in the class).

If $b_i < M$, let b_i+1 belong to the class C_j. Then by the above definitions we have $j > i$. Since 1 is a dth power, it follows that $n(C_j) \leqslant n(C_i)+1$. Starting with $i = 1$ and $n(C_1) = 1$, we obtain in this way a sequence of integers

$$1 = i_1 < i_2 < i_3 < \ldots,$$

such that $n(C_{i_g}) \leqslant g$. Since there are at most h classes, the sequence must terminate after at most h terms, and it can only terminate at i_g when $b_{i_g} = M$. Then M belongs to C_{i_g} and $n(C_{i_g}) \leqslant g \leqslant h$, whence the result.

LEMMA 2·6·2. *If one of $2, 3, \ldots, M$ is a d-th power residue* (mod p), *then*

$$\gamma(d,p) < \max\left\{2\left(\frac{\log p}{\log 2}+1\right),\quad M\left(\frac{\log p}{\log M}+1\right)\right\}. \qquad (2\cdot6\cdot1)$$

Proof. Suppose $m \geqslant 2$ is a dth power residue (mod p). Reasoning as in lemma 2·5·3, but with m instead of 2 and therefore with $0 \leqslant a_i < m$, we see that every integer N is representable as a sum of $(m-1)(h+1)$ dth powers (mod p), where $m^h < p$. Now

$$(m-1)(h+1) < m\left(\frac{\log p}{\log m}+1\right),$$

and since the function $x/(\log x)$ increases with x for $x > e$, every integer N is representable as a sum of at most

$$\max\left\{2\left(\frac{\log p}{\log 2}+1\right),\quad M\left(\frac{\log p}{\log M}+1\right)\right\}$$

dth powers (mod p). This proves the lemma.

The next lemma is due to Davenport and replaces a less effective result of I. Chowla (1943, lemma 4 (ii)).

LEMMA 2·6·3. *If every positive integer up to and including M is representable as a sum of h d-th powers* (mod p), *where $M \geqslant 2$ and $h \geqslant 2$, then*

$$\gamma(d,p) < 2h^{1+[(\log p)/(\log M)]}. \tag{2·6·2}$$

Proof. We have to show that any integer N $(0 \leqslant N < p)$ is congruent (mod p) to a sum of at most

$$2h^{1+[(\log p)/(\log M)]}$$

dth powers. We again express N as

$$N = a_0 + a_1 M + \ldots + a_j M^j,$$

where $0 \leqslant a_i < M$ for $i = 1, \ldots, j-1$ and $0 < a_j < M$. Plainly $M^j < p$.

Now M and $a_i < M$ are representable as sums of at most h dth powers (mod p) by hypothesis. It is clear that M^i is therefore representable as a sum of h^i dth powers (mod p), and hence N is representable as a sum of at most

$$h + h^2 + \ldots + h^{1+j} < 2.h^{1+j}$$

dth powers (mod p). Since $j \leqslant [(\log p)/(\log M)]$, the lemma follows.

LEMMA 2·6·4. *Suppose $p < d^2$ and put $d^2/p = p^\kappa$ $(0 < \kappa < 1)$, and $(\log 2)/(\log p) = \delta$. Then*

$$\gamma(d,p) < 4(\log p)\,(p^J+1)^2+1, \tag{2·6·3}$$

where

$$J = \tfrac{1}{4}\{\kappa + \sqrt{(\kappa^2 + 8(\kappa+\delta))}\}. \tag{2·6·4}$$

Proof. We assume that

$$\gamma(d,p) \geqslant 4\,(\log p)\,(p^J+1)^2+1 \tag{2·6·5}$$

and obtain a contradiction. Let

$$r = [4M^2 \log p] + 1, \tag{2·6·6}$$

where

$$M = [p^J] + 1. \tag{2·6·7}$$

Then

$$r < 4(\log p)\,(p^J+1)^2+1 \leqslant \gamma(d,p)$$

by our assumption (2·6·5), whence, from the definition of $\gamma(d,p)$, the sum $x_1^d + \ldots + x_r^d$ does not represent every residue class (mod p). Hence by Lemma 2·5·2, there exists an integer c, prime to p, such that

$$|S(mc)| > p(1 - m^2(\log p)/r),$$

for all non-zero integers m.

Let m run through the values $1, 2, \ldots, M\,(=[p^J]+1)$. Then, by (2·6·6),

$$|S(mc)| > \tfrac{3}{4}p$$

for $m = 1, 2, \ldots, M$, and it follows from lemma 2·5·1 that h, the number of equivalence classes into which these m fall, satisfies

$$h(\tfrac{3}{4}p)^2 < pd(d-1) < pd^2,$$

whence

$$h < 2d^2/p = 2p^\kappa = p^{\kappa+\delta}.$$

If one of $2, 3, \ldots, M$ is a dth power residue (mod p), then lemma 2·6·2 implies

$$\gamma(d,p) < \max\left\{2\left(\frac{\log p}{\log 2}+1\right),\quad M\left(\frac{\log p}{\log M}+1\right)\right\}$$

$$< (p^J+1)\left(\frac{\log p}{\log 2}+1\right),$$

which contradicts (2·6·5) since

$$\frac{\log p}{\log 2}+1 < 8\log p \leqslant 4(\log p)\,(p^J+1).$$

If none of $2, 3, \ldots, M$ is a dth power residue (mod p), then lemma 2·6·1 applies and every integer up to and including M is a sum of h dth powers (mod p), where $h \geqslant 2$. In this case lemma 2·6·3 implies

$$\gamma(d,p) < 2h^{1+[(\log p)/(\log M)]} \leqslant 2h^{1+(1/J)} < 4p^{\kappa+(\kappa+\delta)/J} = 4p^{2J},$$

whence

$$\gamma(d,p) < 4(\log p)\,(p^J+1)^2,$$

which again contradicts (2·6·5), and the lemma follows.

LEMMA 2·6·5. *Suppose $p < d^2$. Then we have, in the notation of lemma* 2·6·4,

$$\gamma^*(d,p) \leqslant 12(d^2/p)\,(\log p)\,(p^J+1)^2. \tag{2·6·8}$$

Proof. Suppose the congruence

$$a_1 x_1^d + \ldots + a_s x_s^d \equiv 0 \pmod p$$

has only the trivial solution. Proceeding as in the proof of lemma 2·5·5, we can suppose that there is some c, prime to p, such that

$$|S(ca_j)| > p\left(1-\frac{\log p}{s+j-1}\right) \quad \text{for} \quad j = 1, \ldots, s.$$

Let r satisfy $s-r+1 > 4\log p$. Then $|S(ca_j)| > \frac{3}{4}p$ for $j = 1, \ldots, r$, and it follows from lemma 2·5·1, as in the proof of the preceding lemma, that h, the number of distinct equivalence classes to which $a_1, \ldots, a_r$ belong, satisfies $h < p^{\kappa+\delta}$. It follows from Dirichlet's box argument that there is some class which contains at least R of $a_1, \ldots, a_r$, where

$$R \geqslant r/p^{\kappa+\delta}.$$

Suppose, as we may, that $a_1, \ldots, a_R$ belong to this class. Then, since by hypothesis the congruence

$$a_1(x_1^d + \ldots + a_R^d) + a_s \equiv 0 \pmod p$$

is insoluble, it follows from lemma 2·6·4 that

$$R < 4\log p(p^J+1)^2+1.$$

Thus we have

$$r < 4\log p(p^J+1)^2 p^{\kappa+\delta} + p^{\kappa+\delta}.$$

Hence we can satisfy the condition $s-r+1 > 4\log p$, and so reach a contradiction, provided

$$s > 4\log p(p^J+1)^2 p^{\kappa+\delta} + p^{\kappa+\delta} + 4\log p - 1.$$

It follows from the definition of $\gamma^*(d,p)$ that

$$\gamma^*(d,p) \leqslant 4\log p(p^J+1)^2 p^{\kappa+\delta}(1+\tfrac{1}{2}),$$

whence (2·6·8), since $p^\delta = 2$ and $p^\kappa = d^2/p$.

If the estimate of this lemma is expressed as a power of d, the exponent for large d is

$$\frac{3\kappa+\sqrt{\{\kappa^2+8(\kappa+\delta)\}}}{1+\kappa}.$$

Here $\delta(=(\log 2)/(\log p))$ is small when p is large and hence the exponent is small if κ is small, that is, if p is not much less than d^2. Unfortunately the exponent increases rapidly with κ, and (if we ignore δ) becomes 1 when $\kappa = 2-\frac{1}{3}\sqrt{33} = 0{\cdot}085\ldots$, corresponding to d being about $p^{0{\cdot}542}$. However, there is a result, which we prove in a more general context in the next section, which holds in the case $p < d^2$ and which becomes more effective as p decreases. We quote from lemma 3·3·3 with $\tau = 0$:

LEMMA 2·6·6. *Suppose that* $1 < d < p-1$ *and write* $t = (p-1)/d$. *Let*

$$r = [(\log pt)/(\log 4)]+2. \tag{2·6·9}$$

Then

$$\gamma^*(d,p) \leqslant r^2t+r. \tag{2·6·10}$$

This result is plainly of no use unless $t < d$, that is unless $p < d^2$. Thus it is to be compared with (2·6·8). For large p, the exponents of p arising in the two results are equal if, ignoring δ, $\frac{3}{2}\kappa+\frac{1}{2}\sqrt{(\kappa^2+8\kappa)} = \frac{1}{2}(1-\kappa)$, that is if $\kappa = \frac{1}{15}$, corresponding to $d = p^{\frac{1}{2}(1+\kappa)} = p^{\frac{8}{15}}$. For small d, (2·6·8) is the better of these two estimates, while for large d, (2·6·10) is more effective. For all d $(<p-1)$, we get

$$\gamma^*(d,p) = O(d^{\frac{7}{8}+\epsilon})$$

for any positive ϵ. We obtain this result more precisely in

LEMMA 2·6·7. *If* $1 < d < p-1$, *then*

$$\gamma^*(d,p) < 12(\log d)^2 d^{\frac{7}{8}}. \tag{2·6·11}$$

Proof. We need only to consider the case $p < d^2$, since otherwise the results of lemmas 2·4·1 and 2·5·5 are available and are much more effective. Also, we can suppose $d > 2^{24}$, since otherwise the estimate $[\frac{1}{2}(d+4)]$ (lemma 2·3·2) is sharper.

By lemma 2·6·5, we have

$$\gamma^*(d,p) \leqslant 12(\log p)\,(d^2/p)\,(p^J+1)^2,$$

where $$\frac{d^2}{p} = p^\kappa, \quad \delta = \frac{\log 2}{\log p} \quad \text{and} \quad J = \tfrac{1}{4}(\kappa^2+\sqrt{\{\kappa^2+8(\kappa+\delta)\}}),$$

and by Lemma 2·6·6 we have $$\gamma^*(d,p) \leqslant r^2t+r,$$

where $$t = \frac{p-1}{d} > 1 \quad \text{and} \quad r = [(\log pt)/(\log 4)]+2.$$

Case 1. *Suppose* $\kappa \leqslant \frac{1}{15}$. Then
$$\begin{aligned} 4J &= \kappa+\sqrt{\{\kappa^2+8(\kappa+\delta)\}} \\ &\leqslant \tfrac{1}{15}+\sqrt{(\tfrac{121}{225}+8\delta)} \\ &< \tfrac{4}{5}+\tfrac{60}{11}\delta. \end{aligned}$$

Also we have, from lemma 2·6·5 and since $p = d^{2/(1+\kappa)}$,

$$\begin{aligned} \gamma^*(d,p) &\leqslant 12(\log p)\,(p^J+1)^2\,d^2/p \\ &\leqslant 12(\log p)\,(p^{\frac{1}{5}+\frac{15}{11}\delta}+1)^2\,d^{2\kappa/(1+\kappa)}, \\ &< 12\,(\log p)\,(1+p^{-\frac{1}{5}})^2\,p^{\frac{2}{5}+\frac{30}{11}\delta}\,d^{2\kappa/(1+\kappa)} \\ &< 12(1+p^{-\frac{1}{5}})^2\,2(\log d)\,p^{\frac{30}{11}\delta}\,d^{\frac{1}{5}(4+10\kappa)/(1+\kappa)} \end{aligned}$$

since $p < d^2$. Further, since we can take $d > 2^{24}$ and since $d < p-1$ and d divides $p-1$, we can take $p > 2^{25}$ and $\log d > 16$, from which it follows that

$$\begin{aligned}\gamma^*(d,p) &\leqslant 12(1+2^{-5})^2\, 2^{-\frac{3}{11}}\, (\log d)^2\, d^{\frac{1}{5}(4+10\kappa)/(1+\kappa)} \\ &< 12(\log d)^2\, d^{\frac{1}{5}(4+10\kappa)/(1+\kappa)} \\ &\leqslant 12(\log d)^2\, d^{\frac{7}{8}},\end{aligned}$$

since $\frac{1}{5}(4+10\kappa)/(1+\kappa)$ is an increasing function of κ for all $\kappa > -1$.

Case 2. *Suppose* $\kappa > \frac{1}{15}$. Then we have

$$t = \frac{p-1}{d} < \frac{p}{d} = d^{(1-\kappa)/(1+\kappa)} < d^{\frac{7}{8}} \quad \text{and} \quad pt < d^3,$$

whence $\log pt < 3 \log d$, which gives

$$r \leqslant (\log pt)/(\log 4) + 2 < (2.17) \log d + 2.$$

Hence using the inequality $\log d > 16$, we obtain

$$r^2 t + r < 12(\log d)^2\, d^{\frac{7}{8}}.$$

This completes the proof, since by lemma 2·6·6

$$\gamma^*(d,p) \leqslant r^2 t + r.$$

It will be seen that to improve the present estimate for $\gamma^*(d,p)$ the crucial results are the estimate for $\gamma(d,p)$ in lemma 2·6·4 and the estimate for $\gamma^*(d,p)$ in lemma 2·6·6. Any estimate which is sharper than these will immediately give a better estimate for $\gamma^*(d,p)$. Now I. Chowla's work (1943, theorem 7, with $\frac{2}{3} \leqslant \rho \leqslant \frac{3}{2}$) tells us that if $d^{\frac{5}{8}} < p < d^{\frac{5}{3}}$, then

$$\gamma(d,p) < d^{\frac{2}{3}+O(1/\log\log d)},$$

for all sufficiently large d ($< p-1$). If we use this bound instead of (2·6·3), we can save roughly $\frac{1}{6}$ instead of $\frac{1}{8}$ in the exponent of d in the estimate for $\gamma^*(d,p)$ for large d, and we get

$$\gamma^*(d,p) < d^{\frac{5}{6}+O(1/\log\log d)}.$$

However, this result is not easily made explicit and for this reason we do not take advantage of it.

When $t(=(p-1)/d)$ is composite, there is quite a good estimate for $\gamma^*(d,p)$ which saves a $\frac{1}{2}$ in the exponent of d. This case is considered more generally at the end of the next section and we quote the result (3·3·5) obtained there with $\tau = 0$: if t is composite, then

$$\gamma^*(d,p)\ (=\gamma^*(k,p)) \leqslant r^2 t^{\frac{1}{2}} + r,$$

where $t = (p-1)/d$ and $r = [(\log pt)/(\log 4)] + 2$.

Now we can take $d > p^{\frac{1}{2}}$, since otherwise, from lemmas 2·4·1 and 2·5·5, we get

$$\gamma^*(d,p) = O(\log d).$$

Hence we can take $t < p^{\frac{1}{2}} < d$, from which it follows that

$$\gamma^*(d,p) = O((\log d)^2\, d^{\frac{1}{2}}) < d^{\frac{1}{2}+\epsilon}.$$

Also, when $t = 2$, $d = \frac{1}{2}(p-1)$ and lemma 2·2·1 implies that $\gamma^*(d,p) = O(\log d)$. Therefore, to improve the estimate for $\gamma^*(d,p)$ given in lemma 2·6·7, it suffices to consider only the case when t is an odd prime greater than $d^{\frac{1}{2}}$.

Let $\Gamma(d,p)$ be the least number of dth powers whose sum represents non-trivially every residue class (mod p). Then it is clear that $\gamma(d,p) \leqslant \Gamma(d,p)$. Heilbronn (1964, p. 5) has conjectured that given $\epsilon > 0$, $\Gamma(d,p) = O(d^{\epsilon})$ for t sufficiently large, or at least, if $t > 2$, then $\Gamma(d,p) = O(d^{\frac{1}{2}})$. If the stronger conjecture could be established, it is possible to show, by replacing t in lemma 2·6·6 by $\Gamma(d,p)$, which we may, that $\gamma^*(d,p) = O(d^{\epsilon})$ for d sufficiently large, while if the second could be established, we can get, in the same way, that

$$\gamma^*(d,p) = O(d^{\frac{1}{2}+\epsilon}).$$

S. Chowla (1963, p. 62) has made the weaker conjecture that, for d sufficiently large, $\theta(d) < d^{\frac{1}{2}+\epsilon}$, where ϵ is any positive number and where $\theta(d)$ is defined to be the least r such that the congruence

$$x_1^d + \ldots + x_r^d \equiv 0 \pmod{p} \qquad (2\cdot6\cdot12)$$

has a non-trivial solution. If this conjecture could be proved, we could replace t by $\theta(d)$ in § 3·3 and lemma 2·6·6 would then give

$$\gamma^*(d,p) \leqslant r^2\theta(d) + r = O(d^{\frac{1}{2}+\epsilon}).$$

When $d < p^{\frac{1}{2}}$, it follows from lemma 2·4·1 (with $a_1 = \ldots = a_s = 1$) and lemma 2·5·4 that $\theta(d) = O(\log d)$. Also, if t is composite, then in a similar way to the discussion of $\gamma^*(k, p^{\tau+1})$ in § 3·3 below, the congruence (2·6·12) has a non-trivial solution with $r \leqslant t^{\frac{1}{2}}$. Thus, if t is composite, $\theta(d) \leqslant t^{\frac{1}{2}}$, and further if $d > p^{\frac{1}{2}}$, we have $\theta(d) \leqslant d^{\frac{1}{2}}$. Also, when $t = 2$, $d = \frac{1}{2}(p-1)$ and plainly $\theta(d) = 2$. Hence, when t is not an odd prime greater than $d^{\frac{1}{2}}$, S. Chowla's conjecture holds, and it follows that to effect an improvement on our present estimate for $\gamma^*(d,p)$, this conjecture needs only to be proved when t is a large prime.

3. Congruences to an odd prime power modulus

3·1. *Introduction*

In this section we investigate when the more general congruence

$$a_1 x_1^k + \ldots + a_s x_s^k \equiv 0 \pmod{p^n}, \qquad (3\cdot1\cdot1)$$

where p is an odd prime and $a_1, \ldots, a_s$ are arbitrary integers not divisible by p, has a primitive solution for every positive integer n. We define $\gamma^*(k, p^n)$ as the least positive integer s such that if $a_1, \ldots, a_s$ are any integers prime to p, then the congruence (3·1·1) has a primitive solution for the particular prime power p^n. This is equivalent to asserting that if $s \geqslant \gamma^*(k, p^n)$ for all $n \geqslant 1$, then the equation $a_1 x_1^k + \ldots + a_s x_s^k = 0$ has a non-trivial solution in the field of p-adic numbers, but we make no real use of this interpretation.

It is appropriate to express the positive integer k, for any given prime p, as

$$k = p^{\tau} d k_0, \qquad (3\cdot1\cdot2)$$

where p^{τ} ($\tau \geqslant 0$) is the exact power of p which divides k and where $d = (k, p-1)$, as always. Thus we have $(k_0, p) = 1$ and $(k_0, (p-1)/d) = 1$. As usual in work on Waring's problem we define γ as follows:

$$\gamma = \begin{cases} \tau+1 & \text{if} \quad p > 2, \\ \tau+2 & \text{if} \quad p = 2. \end{cases}$$

It is well known (see, for example, Vinogradov (1953), chapter 2, lemma 8) that if the congruence $x^k \equiv a \pmod{p^\gamma}$ is soluble with x prime to p, then so is the congruence

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

for every $n \geqslant 1$. It follows that in order to estimate $\gamma^*(k, p^n)$ for every n, it suffices to estimate $\gamma^*(k, p^\gamma)$, which is the least s such that the congruence

$$a_1 x_1^k + \ldots + a_s x_s^k \equiv 0 \pmod{p^\gamma} \tag{3·1·3}$$

has a primitive solution.

The result (2·1·2) extends easily to odd prime power moduli and takes the form

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

Thus it would be possible to replace k by $p^\tau d$, just as k was replaced by d in § 2 in the case $\tau = 0$. But when $\tau > 0$ there is no appreciable gain from doing so, and hence we retain k in this section. Also, from henceforth in this section we shall take p to be an odd prime such that $p-1$ does not divide k (i.e. $d < p-1$) and in fact the results of this section do not hold in the excluded cases.

3·2. *The case when $\frac{1}{2}(p-1)$ is a multiple of d*

In this case there is a simple box argument which is very effective, and which we have already used in lemma 2·2·1, in a version specialized to congruences to the modulus p. The estimate for $\gamma^*(k, p^{\tau+1})$ can be obtained using this argument, in an identical way to lemma 2·2·1, except that the congruences considered here are to the modulus $p^{\tau+1}$. However, we shall give a slightly different approach which is capable of being generalized in a useful way.

LEMMA 3·2·1. *If $\frac{1}{2}(p-1)$ is a multiple of d, then*

$$\gamma^*(k, p^{\tau+1}) \leqslant \left[\frac{(\tau+1)\log p}{\log 2}\right] + 1. \tag{3·2·1}$$

Moreover, there is equality here when $d = \frac{1}{2}(p-1)$ and we then have

$$\gamma^*(k, p^{\tau+1}) = \left[\frac{(\tau+1)\log p}{\log 2}\right] + 1. \tag{3·2·2}$$

Proof. The condition that $\frac{1}{2}(p-1)$ is a multiple of d is equivalent to -1 being a kth power residue $(\mathrm{mod}\, p^{\tau+1})$; this is a consequence of the fact that the index of -1 relative to any primitive root $(\mathrm{mod}\, p^{\tau+1})$ is $\frac{1}{2}(p-1)p^\tau$.

Now consider all the 2^s possible sums of coefficients (with distinct suffices):

$$0, a_i, a_i + a_j, \ldots, a_1 + \ldots + a_s,$$

where $a_1, \ldots, a_s$ are all prime to p. If we take $s > (\tau+1)(\log p)/(\log 2)$, so that $2^s > p^{\tau+1}$, there must be two sums which are mutually congruent $(\mathrm{mod}\, p^{\tau+1})$. On removing any common elements, we obtain two disjoint sets of coefficients, $a_1, \ldots, a_r$ and $a_{r+1}, \ldots, a_n$ say, whose sums are congruent $(\mathrm{mod}\, p^{\tau+1})$. On taking $x_i \equiv 1 \pmod{p^{\tau+1}}$ for $i = 1, \ldots, r$ and $x_i^k \equiv -1 \pmod{p^{\tau+1}}$ for $i = r+1, \ldots, n$ and $x_i = 0$ for $i > n$, we get a primitive solution of the congruence (3·1·3) and the estimate (3·2·1) follows from the definition of $\gamma^*(k, p^{\tau+1})$.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

If $d = \frac{1}{2}(p-1)$, the only values assumed by $x^k \pmod{p^{\tau+1}}$ are 0, 1 and -1. Also the only values assumed by the form

$$x_1^k + 2x_2^k + \ldots + 2^{s-1}x_{s-1}^k$$

with not all of the variables $x_1, \ldots, x_s$ divisible by p, are the integers $\pm 1, \pm 2, \ldots, \pm 2^s$. Thus if $2^s < p^{\tau+1}$, the congruence (3·1·3) does not have a primitive solution when the coefficients are $a_i = 2^{i-1}$ $(i = 1, \ldots, s)$. Hence, by the definition of $\gamma^*(k, p^{\tau+1})$, we have

$$\gamma^*(k, p^{\tau+1}) > \frac{(\tau+1)\log p}{\log 2},$$

and this result together with (3·2·1) implies (3·2·2).

We note that if k is odd, then d necessarily divides $\frac{1}{2}(p-1)$ and lemma 3·2·1 holds for all odd primes p.

3·3. *A more general combinatorial method*

The preceding argument was based on -1 being a kth power residue $(\mathrm{mod}\, p^{\tau+1})$ and only holds under the hypothesis that d divides $\frac{1}{2}(p-1)$. The argument of the present subsection (the possibility of which was suggested to me by Dr Erdös, through Professor Davenport) applies without that hypothesis and is based on the existence of a set of values of x^k whose sum is congruent to 0 $(\mathrm{mod}\, p^{\tau+1})$. In fact the set of distinct values $y_1, \ldots, y_t$, where $t = (p-1)/d$, of $x^k \pmod{p^{\tau+1}}$ form such a set, provided that $t > 1$, for they are given by the roots of the congruence

$$y^t - 1 \equiv 0 \pmod{p^{\tau+1}}, \tag{3·3·1}$$

and the sum of the roots of this congruence is congruent to 0 $(\mathrm{mod}\, p^{\tau+1})$, i.e.

$$y_1 + \ldots + y_t \equiv 0 \pmod{p^{\tau+1}}$$

when $t > 1$. Since throughout this section we have taken p to be an odd prime such that $p-1$ does not divide k, we necessarily have $t > 1$. The results we obtain will be most effective when t is small.

Suppose we can find t disjoint sets of coefficients, say

$$a_1, \ldots, a_{r_1}; \quad a_{r_1+1}, \ldots, a_{r_2}; \quad \ldots; \quad a_{r_{t-1}+1}, \ldots, a_{r_t},$$

such that their sums are all mutually congruent $(\mathrm{mod}\, p^{\tau+1})$. Then we can solve the congruence (3·1·3) by taking

$$x_i^k \equiv y_j \pmod{p^{\tau+1}} \quad \text{for} \quad r_{j-1} < i \leqslant r_j \quad (j = 1, \ldots, t)$$

(where $r_0 = 0$) and

$$x_i = 0 \quad \text{for} \quad i > r_t.$$

The possibility of finding t such sets of coefficients is provided by a purely combinatorial theorem of Erdös & Rado (1960, theorem III). We state this first in a self-contained form.

LEMMA 3·3·1. *Let a and b be positive integers and let*

$$c = b!\, a^{b+1}\left(1 - \frac{1}{2!\, a} - \frac{2}{3!\, a^2} - \ldots - \frac{b-1}{b!\, a^{b-1}}\right). \tag{3·3·2}$$

Let $X_1, \ldots, X_{c'}$, where $c' > c$, be sets of at most b elements (the sets not necessarily being distinct). Then there exist sets $Y_1, \ldots, Y_{a'}$, where $a' > a$, such that

(i) *each of the sets Y_i is one of the sets X_j, and the number of values of i for which Y_i is the same set does not exceed the number of values of j for which X_j is this set;*

(ii) *for* $1 \leqslant i < j \leqslant a'$, *the common part of* Y_i *and* Y_j *is a set* Z *which is the same for all* i *and* j.

In our application the sets $X_1, \ldots, X_{c'}$ will in fact be distinct, so that (i) will simply say that the sets $Y_1, \ldots, Y_{a'}$ are a selection from them, while (ii) states that there exist more than a of the sets such that any two of them have the same common part (possibly null).

Let r be a positive integer less than s. Consider the $\binom{s}{r}$ sets of r of the coefficients $a_1, \ldots, a_s$, the coefficients in each set having distinct suffices. These sets are, of course, distinct, though not generally disjoint. Of these sets there must be at least $p^{-\tau-1}\binom{s}{r}$ which have the same sum $(\mathrm{mod}\, p^{\tau+1})$. We take these sets to be the sets $X_1, \ldots, X_{c'}$, where

$$c' \geqslant p^{-\tau-1}\binom{s}{r}.$$

We also take $b = r$, the number of coefficients in each set, and we take $a = t-1$.

Provided the equation of the lemma is satisfied, which will obviously be so if

$$c' > b!\, a^{b+1}\left(1 - \frac{1}{2!\, a} - \ldots - \frac{b-1}{b!\, a^{b-1}}\right),$$

the lemma asserts that there exist t of the above sets such that the common part of any two of these sets is the same. On removing this common part, we obtain t disjoint sets of coefficients, the sums of the coefficients in all the sets being mutually congruent $(\mathrm{mod}\, p^{\tau+1})$.

We have therefore proved

LEMMA 3·3·2. *Suppose* p *is an odd prime and* $p-1$ *does not divide* k. *Let* $(k, p-1) = d$ *and* $t = (p-1)/d$. *Suppose that* $1 < r < s$ *and that*

$$p^{-\tau-1}\binom{s}{r} \geqslant r!(t-1)^{r+1}. \tag{3·3·3}$$

Then the congruence $\quad a_1 x_1^k + \ldots + a_s x_s^k \equiv 0 \pmod{p^{\tau+1}},$

where $a_1, \ldots, a_s$ *are integers prime to* p, *has a primitive solution.*

The inequality assumed in the enunciation is plainly sufficient for that required in the previous lemma.

We can now deduce an estimate for $\gamma^*(k, p^{\tau+1})$.

LEMMA 3·3·3. *If* p *is an odd prime and* p^τ $(\tau \geqslant 0)$ *exactly divides* k, *and if* $t = (p-1)/d > 1$, *where* $d = (k, p-1)$, *then*

$$\gamma^*(k, p^{\tau+1}) \leqslant r^2 t + r, \tag{3·3·4}$$

where

$$r = \left[\frac{\log p^{\tau+1} t}{\log 4}\right] + 2.$$

Proof. The condition on s in the preceding lemma is satisfied if

$$(s-r+1)^r \geqslant p^{\tau+1}(r!)^2 t^{r+1},$$

and is therefore satisfied if $\quad s-r+1 \geqslant t r^2 4^{-1+(1/r)}(p^{\tau+1}t)^{1/r},$

since

$$r! \leqslant \frac{r^r}{2^{r-1}}.$$

We take $r = \left[\frac{\log p^{\tau+1}t}{\log 4}\right]+2$, so that

$$(4p^{\tau+1}t)^{1/r} < 4.$$

Hence the condition is satisfied if $s \geqslant r^2t+r$,
whence the result.

We note that if t is composite and $t = t_1 t_2, t_1 > 1$ and $t_2 > 1$, then the kth power residues $(\mathrm{mod}\, p^{\tau+1})$ satisfy

$$y^{t_1 t_2}-1 \equiv 0 \pmod{p^{\tau+1}},$$

so that there exist t_1 kth power residues $z_1, \ldots, z_{t_1}$ say, which satisfy

$$z^{t_1}-1 \equiv 0 \pmod{p^{\tau+1}}$$

and hence which satisfy $z_1+\ldots+z_{t_1} \equiv 0 \pmod{p^{\tau+1}}$.

It is clear we can replace t in § 2·3 by t_1 and that we can choose $t_1 \leqslant t^{\frac{1}{2}}$. Hence we get

$$\gamma^*(k, p^{\tau+1}) \leqslant r^2t_1+r \leqslant r^2t^{\frac{1}{2}}+r, \tag{3·3·5}$$

where $r = \left[\frac{\log p^{\tau+1}t_1}{\log 4}\right]+2.$

When $\tau > 0$, p divides k and so $t = (p-1)/d < p \leqslant k$, whence, provided t is composite,

$$\gamma^*(k, p^{\tau+1}) = O((\log k)^2 k^{\frac{1}{2}}).$$

4. The number $\Gamma^*(k, p)$

4·1. *Introduction*

We recall the definition of $\Gamma^*(k,p)$ as the least positive integer s with the following property: for any non-zero integers $a_1, \ldots, a_s$ and any positive integer n, the congruence

$$a_1 x_1^k+\ldots+a_s x_s^k \equiv 0 \pmod{p^n} \tag{4·1·1}$$

has a primitive solution, that is a solution with not all of $x_1, \ldots, x_s$ divisible by the prime p. This is equivalent to asserting that the equation

$$a_1 x_1^k+\ldots+a_s x_s^k = 0$$

has a non-trivial solution in the field of p-adic integers, but as before we shall make no real use of this concept.

The coefficients $a_1, \ldots, a_s$ are no longer restricted to being prime to p and so may contain powers of p. By grouping them accordingly and introducing powers of p into the variables if necessary, we can obtain from (4·1·1) an equivalent congruence of the form

$$F^{(0)}+pF^{(1)}+\ldots+p^{k-1}F^{(k-1)} \equiv 0 \pmod{p^n}, \tag{4·1·2}$$

where each $F^{(j)}$ is an additive form in v_j variables, with coefficients not divisible by p, and where the variables in the different $F^{(j)}$ are disjoint, so that $v_0+v_1+\ldots+v_{k-1} = s$. The equivalence is such that the primitive solubility of (4·1·1) for all n, implies that of (4·1·2) and vice versa.

An operation which still remains available is that of permuting the forms $F^{(0)}, \ldots, F^{(k-1)}$ cyclically. Using this, Davenport & Lewis (1963, lemma 3) showed that it is possible to ensure that in the equivalent congruence (4·1·2), the numbers of variables in $F^{(0)}, \ldots, F^{(k-1)}$ satisfy

$$v_0 \geqslant s/k, \quad v_0+v_1 \geqslant 2s/k, \ldots, v_0+\ldots+v_{k-1} = s. \tag{4·1·3}$$

They then proceed to ensure that after this normalization, the congruence (4·1·2) has a solution with not all of the v_0 variables in $F^{(0)}$ divisible by p. Any value of s for which this solubility is proved always to hold, gives an upper bound for $\Gamma^*(k,p)$, though it may possibly fail to give the full truth.

In the same way as in § 3·1, in order to estimate $\Gamma^*(k,p)$ it suffices to prove that for a certain value of s, the congruence

$$F^{(0)}+pF^{(1)}+\ldots+p^{k-1}F^{(k-1)} \equiv 0 \pmod{p^\gamma} \tag{4·1·4}$$

is always soluble with at least one of the variables in $F^{(0)}$ not divisible by p. For this value of s we have $\Gamma^*(k,p) \leqslant s$. The normalization procedure enables us to estimate $\Gamma^*(k,p)$ in terms of the auxiliary functions $\gamma^*(d,p)$ and $\gamma^*(k,p^\gamma)$, which were discussed in the preceding sections.

We note as a matter of interest that γ is generally less than k. In this case some of the original variables cease to play any part in (4·1·4) and this may be an imperfection of the method.

4·2. *The connexion between* $\Gamma^*(k,p)$ *and* $\gamma^*(k,p^\gamma)$

We give first a simple estimate for $\Gamma^*(k,p)$ in terms of $\gamma^*(k,p^\gamma)$. In the case when $\tau = 0$ and $d = p-1$ we are able to determine $\Gamma^*(k,p)$ exactly.

LEMMA 4·2·1. *We have* $$\Gamma^*(k,p) \leqslant k\{\gamma^*(k,p^\gamma)-1\}+1. \tag{4·2·1}$$

Proof. Suppose the number of variables in (4·1·4) satisfies

$$s \geqslant k\{\gamma^*(k,p^\gamma)-1\}+1.$$

Then by the normalization conditions (4·1·3), we have $v_0 \geqslant s/k$, whence $v_0 \geqslant \gamma^*(k,p^\gamma)$. Hence, by the definition of $\gamma^*(k,p^\gamma)$, we can solve the congruence

$$F^{(0)} \equiv 0 \pmod{p^\gamma}$$

with not all the v_0 variables in $F^{(0)}$ divisible by p. This provides a solution of (4·1·4) with not all the variables in $F^{(0)}$ divisible by p, by taking all the other variables to be 0, whence the result.

We note as a special case of this lemma that when the prime p does not divide k (i.e. when $\tau = 0$),

$$\Gamma^*(k,p) \leqslant k\{\gamma^*(d,p)-1\}+1. \tag{4·2·2}$$

We now treat another special case.

LEMMA 4·2·2. *If* $d = p-1$ *and* $\tau = 0$, *so that* $k = (p-1)\,k_0$, *then*

$$\Gamma^*(k,p) = k(p-1)+1 = 1+k^2/k_0. \tag{4·2·3}$$

Proof. We consider the cases $p > 2$ and $p = 2$ separately. First, the case $p > 2$. By (2·1·2) and (2·1·4) we have

$$\gamma^*(k,p) = \gamma^*(p-1,p) = p.$$

Hence, by the preceding lemma,

$$\Gamma^*(k,p) \leqslant k(p-1)+1 = 1+k^2/k_0.$$

To prove the complementary inequality we must refer to the definition of $\Gamma^*(k,p)$. It suffices to exhibit a form in $k(p-1)$ variables such that the congruence (4·1·1) has only the trivial solution for some n. Such a form is provided by

$$\Sigma^{(0)}+p\Sigma^{(1)}+\ldots+p^{k-1}\Sigma^{(k-1)},$$

where $\Sigma^{(j)}$ $(j=0,\ldots,k-1)$ is a sum of $p-1$ kth powers (with coefficients unity). Such a sum is not congruent to 0 (mod p) unless each variable is divisible by p, so that if $n > k-1$, the congruence (mod p^n) has only the trivial solution.

Now we consider the case when $p = 2$. Since we are given $\tau = 0$, we have $\gamma = \tau+2 = 2$, and hence that $\gamma^*(k,p^\gamma) = \gamma^*(k,4)$, and we also have that k must be odd. Therefore we can solve non-trivially the congruence

$$a_1 x_1^k + a_2 x_2^k \equiv 0 \pmod 4,$$

where a_1 and a_2 are arbitrary odd integers. For plainly if $a_1 \equiv a_2 \pmod 4$, then $x_1 = 1$ and $x_2 = -1$ is a solution, while if $a_1 \not\equiv a_2 \pmod 4$, then $a_1+a_2 \equiv 0 \pmod 4$ and $x_1 = x_2 = 1$ is a solution. Hence by definition, $\gamma^*(k,4) \leqslant 2$ and since clearly $\gamma^*(k,4) > 1$, we have

$$\gamma^*(k,4) = 2.$$

Thus the preceding lemma gives

$$\Gamma^*(k,2) \leqslant k+1 = 1+k^2/k_0,$$

since in this case $k = 2^0.1.k_0 = k_0$.

To prove the complementary inequality for $\Gamma^*(k,2)$, we again exhibit a form in k variables such that the congruence (4·1·1) has, for some n, only the trivial solution. Such a form is given by

$$x_0^k+2x_1^k+\ldots+2^{k-1}x_{k-1}^k,$$

since $x^k \equiv 1 \pmod 2$ if x is odd and $x^k \equiv 0 \pmod 2$ if x is even, so that if $n > k-1$, the congruence (mod 2^n) has only the trivial solution. This completes the lemma.

4·3. *The connexion between* $\Gamma^*(k,p)$ *and* $\gamma^*(d,p)$

Now we turn our attention to those finitely many primes p which divide k (i.e. primes for which $\tau > 0$).

Throughout this section we write

$$\nu = \gamma^*(d,p)\ (=\gamma^*(k,p)), \tag{4·3·1}$$

where $1 \leqslant d = (k,p-1) \leqslant p-1$, so that the congruence

$$a_1 x_1^k+\ldots+a_\nu x_\nu^k \equiv 0 \pmod p,$$

where $a_1,\ldots,a_\nu$ are arbitrary integers prime to p, always has a primitive solution, that is a solution with say $x_1 \not\equiv 0 \pmod p$. Also, we suppose that the prime p divides k, so that we always suppose here that $\tau > 0$, since we have dealt with the case when p does not divide

k in the previous subsection. The prime p is not restricted to being odd here, but we remark that a better estimate for $\Gamma^*(k,p)$ in the case $p=2$, when $\nu = d+1 = 2$, is obtained in the next subsection.

The argument is inductive and is a slightly stronger form of a result of Davenport & Lewis (1963, lemma 5). We start with a normalized form, F say, and we recall that

$$F = F^{(0)} + pF^{(1)} + \ldots + p^{k-1}F^{(k-1)}, \tag{4·3·2}$$

where the $F^{(j)}$ are disjoint additive forms in v_j variables with coefficients prime to p and where the numbers of variables in the $F^{(j)}$ satisfy

$$v_0 \geqslant s/k, \quad v_0+v_1 \geqslant 2s/k, \quad \ldots, \quad v_0+\ldots+v_{k-1} = s.$$

Following Davenport & Lewis, we define an operation of *contraction* which has the effect of replacing a sum of ν terms in the normalized form F by a single term, and here we make use of the auxiliary function $\gamma^*(d,p)$ $(=\nu)$. The process of contraction will be used to replace a set of ν terms in some $F^{(i)}$ by a single term in some $F^{(j)}$, where $j > i$. Consider a sum

$$a_1 y_1^k + \ldots + a_\nu y_\nu^k. \tag{4·3·3}$$

In what follows, one of the variables $y_1, \ldots, y_\nu$ is to be distinguished from the others and we take this distinguished variable to be y_1. By the definition of ν, we can solve

$$a_1 y_1'^k + \ldots + a_\nu y_\nu'^k \equiv 0 \pmod{p}$$

with y_1' prime to p. By choosing the solution suitably we can suppose the integer on the left is not zero, and then we can write

$$a_1 y_1'^k + \ldots + a_\nu y_\nu'^k = p^g e,$$

where e is prime to p and $g \geqslant 1$. The substitution $y_i = y_i' z$ gives us

$$a_1 y_1^k + \ldots + a_\nu y_\nu^k = p^g e z^k. \tag{4·3·4}$$

The operation of contraction consists of replacing the terms (4·3·3) by the single term $p^g e z^k$. We note that $z \not\equiv 0 \pmod{p}$ implies that $y_1 \not\equiv 0 \pmod{p}$.

Contractions are first applied to groups of ν terms in $F^{(0)}$ and here any one of the variables can be chosen to be distinguished. Any remaining variables not in the groups are put equal to zero. There results a form

$$pG^{(1)} + p^2 G^{(2)} + \ldots, \tag{4·3·5}$$

where $G^{(j)}$ contains the original v_j terms plus possibly additional terms arising from the contractions. These additional variables are called *derived* variables. We repeat this process, ensuring at each stage that at least one of the variables in a group is derived either directly or indirectly from a variable in $F^{(0)}$. Suppose that after any number of permissible contractions we reach a form H such that the congruence $H \equiv 0 \pmod{p^\gamma}$ is soluble with at least one of the derived variables in H prime to p. This implies a solution of $F \equiv 0 \pmod{p^\gamma}$ and on tracing back the derived variables to their ancestors in $F^{(0)}$, we see that the solution has at least one of the variables in $F^{(0)}$ prime to p. In particular, this will be the case if we reach a form

$$H_m = p^m H^{(m)} + p^{m+1} H^{(m+1)} + \ldots \tag{4·3·6}$$

in which any one of the forms $H^{(\gamma)}$, $H^{(\gamma+1)}$, ... contains a derived variable; for then we can take the derived variable to be 1 and the rest zero, and have the congruence $H_m \equiv 0 \pmod{p^\gamma}$ soluble in the required way. We call this the *soluble* case.

We go on to prove a slightly strengthened form of lemma 5 in the paper of Davenport & Lewis (1963).

LEMMA 4·3·1. *For $m = 1, \ldots$, we can obtain from a normalized form F as given in (4·3·2) by repeated contractions, a form H_m of the type (4·3·6), where $H^{(m)}, H^{(m+1)}, \ldots$ are disjoint additive forms with coefficients prime to p. For $j \leqslant k-1$, $H^{(j)}$ contains the v_j terms of $F^{(j)}$ possibly together with additional derived variables; for $j \geqslant k$, $H^{(j)}$ can contain only derived variables. Further, if S_m denotes the total number of derived variables in H_m, then*

$$S_m \geqslant \min\left(\frac{v_0}{\nu^{m-1}}, \frac{v_0}{\nu^m} + \ldots + \frac{v_{m-1}}{\nu}\right) - 1 + \frac{1}{\nu^m}, \tag{4·3·7}$$

where $\nu = \gamma^*(d, p)$.

Proof. This is similar to Davenport & Lewis's lemma 5 (1963), except that we show that their induction goes through with the additional term $1/\nu^m$.

Suppose first $m = 1$. We divide the v_0 terms in $F^{(0)}$ into sets of ν terms and equate surplus terms in $F^{(0)}$ to zero. On contraction, each set gives a single term of the type (4·3·4), i.e. of the type $p^g e z^k$, where e is prime to p and $g \geqslant 1$. If $g \leqslant k-1$, we add each such term to the corresponding part $p^g F^{(g)}$ of F and denote the sum by $p^g H^{(g)}$. Thus we obtain a form of the type (4·3·6) with $m = 1$, and the total number of derived variables, S_1, satisfies

$$S_1 = \left[\frac{v_0}{\nu}\right] \geqslant \frac{v_0}{\nu} - \frac{\nu-1}{\nu} = \frac{v_0}{\nu} - 1 + \frac{1}{\nu},$$

and hence (4·3·7) holds when $m = 1$, the minimum being attained by the second expression.

We complete the proof by induction on m. We assume the lemma to be true for m $(1 \leqslant m < \gamma)$: we have to prove the lemma holds with $m+1$ replacing m. Let w denote the number of derived variables in $H^{(m)}$; then the total number of derived variables in $H^{(m+1)}, H^{(m+2)}, \ldots$ is $S_m - w$. We divide the $v_m + w$ terms in $H^{(m)}$ into the maximum number of sets of ν such that each set contains at least one of the w derived variables. The number of such sets that can be formed is

$$\begin{cases} w & \text{if} \quad v_m \geqslant (\nu-1)\, w, \\ \left[\dfrac{v_m + w}{\nu}\right] & \text{if} \quad v_m < (\nu-1)\, w. \end{cases}$$

Any variables remaining in $H^{(m)}$ are put equal to zero. Each set of ν terms can be contracted into a single term, which will be of the form $p^g e z^k$, where $g \geqslant m+1$ and e is prime to p. Adding each such term to the corresponding form $H^{(g)}$, we obtain a form of the type

$$p^{m+1} I^{(m+1)} + p^{m+2} I^{(m+2)} + \ldots,$$

where each $I^{(j)}$ contains the original v_j variables from $F^{(j)}$ for $j \leqslant k-1$, plus possibly derived variables already in $H^{(j)}$ and new derived variables. The total number of derived variables in $I^{(m+1)}, I^{(m+2)}, \ldots$ is S_{m+1} and equals

$$(S_m - w) + \begin{cases} w & \text{if} \quad v_m \geqslant (\nu-1)\, w, \\ \left[\dfrac{v_m + w}{\nu}\right] & \text{if} \quad v_m < (\nu-1)\, w. \end{cases}$$

Case I. Suppose $v_m \geqslant (\nu-1)\,w$. Then $S_{m+1} = S_m - w + w = S_m$. If the minimum is attained for the first expression in (4·3·7), then immediately

$$S_{m+1} = S_m \geqslant \frac{v_0}{\nu^{m-1}} - 1 + \frac{1}{\nu^m} > \frac{v_0}{\nu^m} - 1 + \frac{1}{\nu^{m+1}}$$

and S_{m+1} satisfies the corresponding inequality with $m+1$ replacing m. If the minimum is attained by the second expression, we get

$$S_{m+1} = S_m \geqslant \frac{v_0}{\nu^m} + \ldots + \frac{v_{m-1}}{\nu} - 1 + \frac{1}{\nu^m}$$

$$> \frac{v_0}{\nu^m} - 1 + \frac{1}{\nu^{m+1}}$$

and again S_{m+1} satisfies the required inequality.

Case II. Suppose $v_m < (\nu-1)\,w$. Then

$$S_{m+1} = S_m - w + \left[\frac{w+v_m}{\nu}\right] \geqslant S_m - w + \frac{w}{\nu} + \frac{v_m}{\nu} - 1 + \frac{1}{\nu}$$

and since $S_m \geqslant w$, we get $$S_{m+1} \geqslant \frac{S_m + v_m}{\nu} - 1 + \frac{1}{\nu}.$$

If the minimum is attained by the first expression in (4·3·7), then

$$S_{m+1} \geqslant \frac{v_0}{\nu^m} - \frac{1}{\nu} + \frac{1}{\nu^{m+1}} + \frac{v_m}{\nu} - 1 + \frac{1}{\nu},$$

whence $$S_{m+1} \geqslant \frac{v_0}{\nu^m} - 1 + \frac{1}{\nu^{m+1}}$$

and S_{m+1} satisfies (4·3·7) with $m+1$ replacing m.

Finally, if the minimum is attained by the second expression, then

$$S_{m+1} \geqslant \frac{v_0}{\nu^{m+1}} + \ldots + \frac{v_{m-1}}{\nu^2} - \frac{1}{\nu} + \frac{1}{\nu^{m+1}} + \frac{v_m}{\nu} - 1 + \frac{1}{\nu},$$

and clearly (4·3·7) is again satisfied with $m+1$ replacing m. This completes the lemma.

As a consequence of this result we have

LEMMA 4·3·2. *For all primes* p, $\Gamma^*(k,p)$ *satisfies*

$$\Gamma^*(k,p) \leqslant \left[\frac{k(\nu^\gamma - 1)}{\min(\nu,\gamma)}\right] + 1, \tag{4·3·8}$$

where $\nu = \gamma^*(d,p)$.

Proof. Suppose the number of variables, s, in the congruence (4·1·4) satisfies

$$s \geqslant \left[\frac{k(\nu^\gamma - 1)}{\min(\nu,\gamma)}\right] + 1. \tag{4·3·9}$$

Then by the normalization conditions (4·1·3), we have $v_0 \geqslant s/k$ and

$$\frac{v_0}{\nu^\gamma} + \ldots + \frac{v_{\gamma-1}}{\nu} \geqslant \frac{v_0 + \ldots + v_{\gamma-1}}{\nu^\gamma} \geqslant \frac{\gamma s}{\nu^\gamma k}.$$

Hence
$$\min\left(\frac{v_0}{\nu^{\gamma-1}}, \frac{v_0}{\nu^{\gamma}}+\ldots+\frac{v_{\gamma-1}}{\nu}\right) \geqslant \min\left(\frac{s}{\nu^{\gamma-1}k}, \frac{\gamma s}{\nu^{\gamma}k}\right)$$
$$> 1-\frac{1}{\nu^{\gamma}},$$

from (4·3·9), and it follows that $S_\gamma > 0$. It follows from the definition of S_m that the soluble case occurs if $S_\gamma > 0$, whence the lemma, from the definition of $\Gamma^*(k,p)$.

4·4. *Two estimates for $\Gamma^*(k,p)$ when $p-1$ does not divide k*

We apply this and previous results established for $\gamma^*(d,p)$ to obtain estimates for $\Gamma^*(k,p)$. In our first application, using only lemma 2·3·2 which asserts that $\nu = \gamma^*(d,p) \leqslant [\frac{1}{2}(d+4)]$ if $d < \frac{1}{2}(p-1)$ and lemma 2·2·1 which asserts that $\gamma^*(d,p) = [(\log p)/(\log 2)]+1$ when $d = \frac{1}{2}(p-1)$, we can deduce from the last lemma a simple and general estimate for $\Gamma^*(k,p)$, provided $d < p-1$. We note here that p is necessarily an odd prime.

Lemma 4·4·1. *If $d < p-1$ and $k \geqslant 7$, we have*
$$\Gamma^*(k,p) \leqslant \tfrac{1}{2}k^2+k+1. \qquad (4\cdot4\cdot1)$$

Proof. We consider various cases.

(i) $\tau = 0$, $1 \leqslant d \leqslant 3$. Here, by lemma 2·3·1, we have
$$\gamma^*(k,p) = \gamma^*(d,p) \leqslant d+1 \leqslant 4,$$
so that by lemmas 4·2·1 or 4·3·2, we have
$$\Gamma^*(k,p) \leqslant 3k+1 \leqslant \tfrac{1}{2}k^2+k+1,$$
since we are given $k \geqslant 7$.

(ii) $\tau = 0$, $1 \leqslant d < \frac{1}{2}(p-1)$. Here, by lemma 2·3·2, we have
$$\gamma^*(d,p) \leqslant [\tfrac{1}{2}(d+4)],$$
so that, by either lemmas 4·2·1 or 4·3·2,
$$\Gamma^*(k,p) \leqslant \tfrac{1}{2}(d+2)\,k+1 \leqslant \tfrac{1}{2}k^2+k+1,$$
since d divides k.

(iii) $\tau = 0$, $d = \frac{1}{2}(p-1)$, $d \geqslant 4$. In this case lemma 2·2·1 applies and we have
$$\gamma^*(d,p) = \left[\frac{\log p}{\log 2}\right]+1 = \left[\frac{\log(2d+1)}{\log 2}\right]+1 < \tfrac{1}{2}(d+4),$$
since $d \geqslant 4$. Thus it follows as in (ii) that
$$\Gamma^*(k,p) \leqslant \tfrac{1}{2}k^2+k+1.$$

This covers all the possible cases when p does not divide k. We now obtain an estimate for $\Gamma^*(k,p)$ when p divides k.

(iv) $\tau > 0$, $d = 1$. Here $\gamma^*(k,p) = 2$, whence by lemma 4·3·2,
$$\Gamma^*(k,p) \leqslant \tfrac{1}{2}k(2^{\tau+1}-1)+1 = k2^{\tau}-\tfrac{1}{2}k+1.$$

Since $k \geqslant p^\tau \geqslant 3^\tau$, this implies that

$$\Gamma^*(k,p) \leqslant k^{1+(\log 2)/(\log 3)}+1 < \tfrac{1}{2}k^2+1,$$

since $k^{(\log 2)/(\log 3)} < \frac{1}{2}k$ for $k \geqslant 7$.

(v) $\tau > 0$, $d = 2$ *or* 3 *and* $d < \frac{1}{2}(p-1)$. By lemma 2·3·2 we have $\gamma^*(d,p) \leqslant 3$, whence

$$\Gamma^*(k,p) \leqslant \begin{cases} 4k+1 & \text{if} \quad \tau = 1, \\ \frac{1}{3}k(3^{\tau+1}-1)+1 & \text{if} \quad \tau \geqslant 2. \end{cases}$$

Now $4k+1 < \frac{1}{2}k^2+k+1$ when $k \geqslant 7$, while in the remaining case, we have, since

$$k \geqslant dp^\tau \geqslant 2.3^\tau,$$

$$\Gamma^*(k,p) < 3^\tau k+1 \leqslant \tfrac{1}{2}k^2+1.$$

(vi) $\tau > 0$, $4 \leqslant d < \frac{1}{2}(p-1)$. Again by lemma 2·3·2 we have

$$\gamma^*(d,p) \leqslant [\tfrac{1}{2}(d+4)],$$

whence by lemma 4·3·2, $\quad \Gamma^*(k,p) \leqslant \frac{1}{2}k\{\frac{1}{2}(d+4)\}^{\tau+1}+1.$

Now, since $d \geqslant 4$, plainly $\frac{1}{2}(d+4) \leqslant d$. Also, since $d = (k, p-1)$, the inequality $d < \frac{1}{2}(p-1)$ implies that $d \leqslant \frac{1}{3}(p-1)$, so that

$$\tfrac{1}{2}(d+4) \leqslant \tfrac{1}{6}(p+11) < p,$$

since $p \geqslant 3$. It follows that, since $k \geqslant p^\tau d$, we have

$$\Gamma^*(k,p) \leqslant \tfrac{1}{2}kp^\tau d+1 \leqslant \tfrac{1}{2}k^2+1.$$

(vii) $\tau > 0$, $d = \frac{1}{2}(p-1)$. In this case lemma 3·2·1 applies and gives us

$$\gamma^*(k,p^{\tau+1}) \leqslant \left[\frac{(\tau+1)\log p}{\log 2}\right]+1 = \left[\frac{\log p^\tau(2d+1)}{\log 2}\right]+1 \leqslant \left[\frac{\log 3k}{\log 2}\right]+1,$$

whence by lemma 4·2·1,

$$\Gamma^*(k,p) \leqslant k\left[\frac{\log 3k}{\log 2}\right]+1 < \tfrac{1}{2}k^2+k+1,$$

since $k \geqslant 7$.

Except for the case $d = p-1$, which is excluded by hypothesis, we have covered all the possible values that d and τ can assume. We see that the greatest upper bound for $\Gamma^*(k,p)$ is $\frac{1}{2}k^2+k+1$, which gives us the lemma.

In our second application we use the deeper but more complicated results of § 2 to obtain an estimate for $\Gamma^*(k,p)$ when $d < p-1$, which is more effective when k is large.

LEMMA 4·4·2. *If* $d < p-1$ *and* $k \geqslant 7$, *then*

$$\Gamma^*(k,p) < 12\,(\log k)^2 k^{\frac{15}{8}}. \tag{4·4·2}$$

Proof. If $\tau = 0$, so that $\gamma = 1$, it follows from lemmas 4·2·1 and 2·6·7 that

$$\Gamma^*(k,p) < k\{12(\log d)^2 d^{\frac{7}{8}}-1\}+1$$
$$< 12(\log k)^2 k^{\frac{15}{8}}.$$

We have tacitly assumed $d > 1$ here, but if $d = 1$, then $\gamma^*(k,p) = \gamma^*(1,p) = 2$ and lemma 4.2.1 gives

$$\Gamma^*(k,p) \leqslant k+1,$$

which plainly implies the result.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

If $\tau = 1$ and $p > 2d^2$, it follows from lemma 2·4·1 that

$$\gamma^*(k,p) \leqslant \left[\frac{2\log 2d}{\log 2}\right]+1 \leqslant \left[\frac{2\log k}{\log 2}\right]+3 \leqslant 6\log k.$$

Hence by lemma 4·3·2, with $\nu \leqslant 6\log k$,

$$\Gamma^*(k,p) \leqslant \tfrac{1}{2}k(6\log k)^2 < 12(\log k)^2 k^{\frac{15}{8}},$$

since $k \geqslant 7$.

If $\tau = 1$ and $p < 2d^2$, we appeal first to lemma 3·3·3, which gives

$$\gamma^*(k,p^2) \leqslant r^2 t + r,$$

where $r = [(\log p^2 t)/(\log 4)]+2$ and where $t = (p-1)/d$. We note that $p < 2d^2$ implies that $d > (\frac{1}{2}p)^{\frac{1}{2}} > 1$. Since $t < p/d < 2d \leqslant d^2$ and $k \geqslant pd$, we have

$$r \leqslant (2\log k)/(\log 4)+2 < \tfrac{3}{2}\log k + 2 < 3\log k.$$

Also, since $d > (\frac{1}{2}p)^{\frac{1}{2}}$ and $k \geqslant pd \geqslant 2p$, we have

$$t < p/d < (2p)^{\frac{1}{2}} \leqslant k^{\frac{1}{2}}.$$

Hence
$$\gamma^*(k,p^2) < 9(\log k)^2 k^{\frac{1}{2}} + 3\log k < 12(\log k)^2 k^{\frac{1}{2}},$$

since $k \geqslant 7$. It follows from lemma 4·2·1 that

$$\begin{aligned}\Gamma^*(k,p) &\leqslant k\{\gamma^*(k,p^2)-1\}+1 < 12(\log k)^2 k^{\frac{3}{2}} \\ &< 12(\log k)^2 k^{\frac{15}{8}}.\end{aligned}$$

If $\tau \geqslant 2$, we repeat in essence the last argument, but now p^2 divides k, so that we always have

$$t < p \leqslant k^{\frac{1}{2}}. \tag{4·4·3}$$

Again we have by lemma 3·3·3 that

$$\gamma^*(k,p^{\tau+1}) \leqslant r^2 t + r,$$

where now
$$r = \left[\frac{\log p^{\tau+1}t}{\log 4}\right]+2.$$

It follows from (4·4·3) and from the inequality $k \geqslant p^\tau$ that $p^{\tau+1}t < k^2$ and hence that

$$r \leqslant (2\log k)/(\log 4)+2 < 3\log k.$$

Since $t < k^{\frac{1}{2}}$, we get the same conclusion as before, namely

$$\Gamma^*(k,p) \leqslant k\{\gamma^*(k,p^{\tau+1})-1\}+1 < 12(\log k)^2 k^{\frac{3}{2}},$$

and this completes the lemma.

4·5. *Another inductive argument*

In lemmas 4·4·1 and 4·4·2 we have obtained estimates for $\Gamma^*(k,p)$ when

$$d = (k, p-1) < p-1,$$

and we have also dealt with the case when $d = p-1$ and $\tau = 0$ in lemma 4·2·2. It remains to consider the case $d = p-1$ when $\tau > 0$, and here we note that the case $p = 2$ is not excluded. By (2·3·2) we have, when $d = p-1$,

$$\gamma^*(d,p) = \gamma^*(p-1,p) = p.$$

Thus lemma 4·3·2 gives in this case

$$\Gamma^*(k,p) \leqslant \left[\frac{k(p^\gamma-1)}{\min(p,\gamma)}\right]+1.$$

We now develop a more elaborate inductive argument to show in effect that if $p \leqslant \gamma$, the term p in the minimum above can still be omitted. This more elaborate argument is based on that of Davenport & Lewis's lemma 7 (1963), which was concerned with the case $p = 2$ (when $d = p-1$ and $p \leqslant \gamma = \tau+2$ necessarily).

For those primes p satisfying $p \leqslant \gamma$, we employ two processes of contraction analogous to the ones used by Davenport & Lewis. We continue to use the type of contraction already defined, in which one of the variables is distinguished and the choice of this variable is restricted to being one of the variables in $F^{(0)}$, or to having one of the variables in $F^{(0)}$ among its ancestors. The new variables arising from such contractions, previously called derived variables, will now be called *primary derived variables*, or more simply, *primary variables*, since we need to differentiate them from variables which result from a second type of contraction.

This second type of contraction depends on whether the prime p is odd or even. First, when p is odd, it is as follows: suppose we have the expression

$$c_1 x_1^k+\ldots+c_p x_p^k, \tag{4·5·1}$$

where $c_1, \ldots, c_p$ are all in the same non-zero residue class (mod p). Then we put

$$x_1 = \ldots = x_p = z$$

and obtain the single term

$$pez^k, \tag{4·5·2}$$

where e and z are prime to p. This replacement of the expression (4·5·1) by (4·5·2) forms the second type of contraction for odd primes and the source of the variables $x_1, \ldots, x_p$ is immaterial. Secondly, when $p = 2$, the second type of contraction is as follows: suppose we have the expression

$$c_1 x_1^k+c_2 x_2^k, \tag{4·5·3}$$

where c_1 and c_2 are odd and $c_1 \equiv c_2 \pmod 4$. Then we put $x_1 = x_2 = z$ and obtained the single term

$$2ez^k, \tag{4·5·4}$$

where e and z are odd. This replacement of the expression (4·5·3) by (4·5·4) forms the second type of contraction when $p = 2$, and is applied regardless of the sources of the variables x_1 and x_2. In both cases the resulting variables are called *secondary derived variables*, or more simply, *secondary variables*, and they will not necessarily have ancestors among the variables in $F^{(0)}$ nor will they be available for use as primary derived variables.

As before, we start with a normalized form

$$F = F^{(0)}+pF^{(1)}+\ldots+p^{k-1}F^{(k-1)}$$

and prove that by repeated contractions of these two types, we must reach the soluble case, i.e. reach a form of the type (4·3·6), namely

$$H_m = p^m H^{(m)}+p^{m+1}H^{(m+1)}+\ldots,$$

in which there is at least one primary variable in some $H^{(j)}$ with $j \geqslant \gamma$. This implies, as before, the existence of a solution of $F \equiv 0 \pmod{p^\gamma}$ with at least one of the variables in $F^{(0)}$ not divisible by p.

LEMMA 4·5·1. *Suppose p is any prime such that p and $p-1$ divide k, and that $p \leqslant \gamma$. Suppose also that*

$$\frac{s}{k} > \frac{p^\gamma - 1}{\gamma}. \tag{4·5·5}$$

Then for $m = 1, \ldots, \gamma$, we can obtain from the normalized form F, by repeated contractions of both kinds, a form H_m of the type (4·3·6), where $H^{(m)}$, $H^{(m+1)}$, ... are additive forms in disjoint variables with coefficients prime to p. For $j \leqslant k-1$, $H^{(j)}$ contains the v_j terms of $F^{(j)}$ and possibly additional terms containing derived variables of both kinds; for $j \geqslant k$, the form $H^{(j)}$ can contain only derived variables. Further, if S_m denotes the number of primary variables in H_m, then

$$S_m \geqslant \min\left(\frac{v_0}{p}, \frac{v_0}{p^2}+\frac{v_1}{p}, \ldots, \frac{v_0}{p^m}+\ldots+\frac{v_{m-1}}{p}\right) - 1 + \frac{1}{p^m}, \tag{4·5·6}$$

and if V_m denotes the number of original and secondary variables in H_m, then

$$S_m + V_m \geqslant \frac{v_0}{p^m}+\ldots+\frac{v_{m-1}}{p}+v_m-1+\frac{1}{p^m}. \tag{4·5·7}$$

Proof. Here, by lemma 2·3·1, $\nu = \gamma^*(k,p) = p$, since by hypothesis $d = p-1$. The proof of the lemma is by induction.

For $m = 1$ we proceed as in lemma 4·3·1, grouping the v_0 terms in $F^{(0)}$ into $[v_0/p]$ sums of p terms and applying to each sum a contraction of the first type. The new variables are all primary variables and their number is

$$S_1 = \left[\frac{v_0}{p}\right] \geqslant \frac{v_0}{p} - \frac{p-1}{p} = \frac{v_0}{p} - 1 + \frac{1}{p},$$

so that (4·5·6) holds for $m = 1$. Also, by definition, $V_1 = v_1$, so that

$$S_1 + V_1 \geqslant \frac{v_0}{p} - 1 + \frac{1}{p} + v_1,$$

whence (4·5·7) holds for $m = 1$ too.

We assume inductively that the statement of the lemma is true for m $(1 \leqslant m < \gamma)$ and we show it is true for $m+1$, and this will prove the lemma.

Let w denote the number of primary variables in $H^{(m)}$; then the total number of primary variables in $H^{(m+1)}$, $H^{(m+2)}$, ... is $S_m - w$.

Case I. Suppose $V_m \leqslant (p-1)\,w$. We can thus form $[(w+V_m)/p]$ sets of p terms from $H^{(m)}$, each containing at least one primary variable and to each set we apply a contraction of the first kind, obtaining $[(w+V_m)/p]$ new primary variables. Hence

$$S_{m+1} = S_m - w + \left[\frac{w+V_m}{p}\right] \quad \text{and} \quad V_{m+1} = v_{m+1},$$

there being no secondary variables formed. Hence

$$S_{m+1} \geqslant S_m - \frac{(p-1)\,w}{p} + \frac{V_m}{p} - \frac{p-1}{p}$$

and since $S_m \geqslant w$ by definition, $\quad S_{m+1} \geqslant \dfrac{S_m+V_m}{p}-1+\dfrac{1}{p}$

and so by the inductive hypothesis (4·5·7), we have

$$S_{m+1} \geqslant \frac{v_0}{p^{m+1}}+\ldots+\frac{v_{m-1}}{p^2}+\frac{v_m}{p}-\frac{1}{p}+\frac{1}{p^{m+1}}-1+\frac{1}{p}.$$

Thus (4·5·6) is satisfied for $m+1$. Also we have $V_{m+1} = v_{m+1}$, whence

$$S_{m+1}+V_{m+1} \geqslant \frac{v_0}{p^{m+1}}+\ldots+\frac{v_m}{p}+v_{m+1}-1+\frac{1}{p^{m+1}}$$

and therefore (4·5·7) is also satisfied with m replaced by $m+1$.

Case II. Suppose $V_m > (p-1)\,w$, $p > 2$. Let X_i $(i=1,\ldots,p-1)$ denote the number of coefficients of the V_m original and secondary variables in $H^{(m)}$ which are congruent to $i \pmod p$. Then

$$V_m = X_1+\ldots+X_{p-1}.$$

We can select sets of p terms from these groups of coefficients in the same residue class $\pmod p$ to make up any desired number of sets of secondary variables which does not exceed

$$\left[\frac{X_1}{p}\right]+\ldots+\left[\frac{X_{p-1}}{p}\right].$$

Suppose first that that $w \geqslant p-1$. Then we can form $[\{V_m-(p-1)\,w\}/p]$ such sets, for

$$\left[\frac{X_1}{p}\right]+\ldots+\left[\frac{X_{p-1}}{p}\right] \geqslant \frac{X_1}{p}+\ldots+\frac{X_{p-1}}{p}-\frac{(p-1)^2}{p} \geqslant \frac{V_m-(p-1)\,w}{p}.$$

To each set we apply a contraction of the second type and obtain $[\{V_m-(p-1)\,w\}/p]$ new secondary variables. Hence

$$V_{m+1} = v_{m+1}+\left[\frac{V_m-(p-1)\,w}{p}\right].$$

There remain $\quad V_m-p\left[\dfrac{V_m-(p-1)\,w}{p}\right] \geqslant w(p-1)$

terms in $H^{(m)}$. We combine $(p-1)\,w$ of these with the w primary variables in $H^{(m)}$, getting w new primary variables in H_{m+1}, so that we have

$$S_{m+1} = S_m-w+w = S_m.$$

Hence (4·5·6) is satisfied with m replaced by $m+1$, since the right-hand side of (4·5·6) decreases with increasing m. Also

$$\begin{aligned} S_{m+1}+V_{m+1} &\geqslant S_m+\left[\frac{V_m-(p-1)\,w}{p}\right]+v_{m+1} \\ &\geqslant \frac{S_m+V_m}{p}+v_{m+1}-1+\frac{1}{p} \\ &\geqslant \frac{v_0}{p^{m+1}}+\ldots+\frac{v_{m-1}}{p^2}+\frac{v_m}{p}-\frac{1}{p}+\frac{1}{p^{m+1}}+v_{m+1}-1+\frac{1}{p}, \end{aligned}$$

by the inductive hypothesis (4·5·7) applied to S_m+V_m, and so (4·5·7) holds for $m+1$.

Next, suppose $w < p-1$ and $V_m \geqslant (p-1)^2$. Then

$$\left[\frac{X_1}{p}\right]+\ldots+\left[\frac{X_{p-1}}{p}\right] \geqslant \frac{X_1}{p}+\ldots+\frac{X_{p-1}}{p}-\frac{(p-1)^2}{p} = \frac{V_m}{p}-\frac{(p-1)^2}{p} \geqslant 0.$$

Therefore we are able to select $[\{V_m-(p-1)^2\}/p]$ groups of secondary and original variables which can sustain contractions of the second kind, giving $[\{V_m-(p-1)^2\}/p]$ new secondary variables. The number of original and secondary variables remaining in $H^{(m)}$ after applying these operations is

$$V_m-p\left[\frac{V_m-(p-1)^2}{p}\right] \geqslant (p-1)^2 > (p-1)\,w.$$

Combining these $(p-1)\,w$ original and secondary variables with the w primary variables in $H^{(m)}$, we obtain on applying contractions of the first type, w new primary derived variables. As a result we have

$$S_{m+1} = S_m-w+w = S_m;$$

$$V_{m+1} = v_{m+1}+\left[\frac{V_m-(p-1)^2}{p}\right].$$

Now suppose $w < p-1$, as before, and $(p-1)\,w < V_m < (p-1)^2$. Then we can form w sets of p variables with each set containing one primary variable and $p-1$ original and secondary variables. We apply contractions of the first kind to these w sets, thus getting w new primary variables, so that we have $S_{m+1} = S_m-w+w = S_m$. We make no contractions of the second type, so that $V_{m+1} = v_{m+1}$. Since $V_m < (p-1)^2$ by supposition, it is immediate that

$$V_{m+1} = v_{m+1} \geqslant v_{m+1}+\left[\frac{V_m-(p-1)^2}{p}\right].$$

Hence if $w < p-1$ and $V_m > (p-1)\,w$,

$$S_{m+1} = S_m \quad \text{and} \quad V_{m+1} \geqslant v_{m+1}+\left[\frac{V_m-(p-1)^2}{p}\right].$$

It follows as before that the equation $S_{m+1} = S_m$ implies that (4·5·6) holds with $m+1$ in place of m. It remains to show that (4·5·7) is satisfied for $m+1$ in place of m, and here we must use the conditions that $p \leqslant \gamma = \tau+1$ and $s/k > (p^\gamma-1)/\gamma$. We have

$$\begin{aligned} S_{m+1}+V_{m+1} &\geqslant S_m+\left[\frac{V_m-(p-1)^2}{p}\right]+v_{m+1} \\ &\geqslant S_m+\frac{V_m}{p}-\frac{(p-1)^2}{p}-1+\frac{1}{p}+v_{m+1} \\ &\geqslant \frac{S_m+V_m}{p}-1+\frac{1}{p}+v_{m+1} \end{aligned}$$

provided $S_m \geqslant (S_m/p)+(p-1)^2/p$, i.e. provided $S_m \geqslant p-1$, for $m = 1, \ldots, \gamma-1$. Hence, provided $S_m \geqslant p-1$, we have by the inductive hypothesis (4·5·7) that

$$S_{m+1}+V_{m+1} \geqslant \frac{v_0}{p^{m+1}}+\ldots+\frac{v_m}{p}+v_{m+1}-1+\frac{1}{p^{m+1}},$$

and we see that (4·5·7) also holds with m replaced by $m+1$.

Now we show that $S_m \geqslant p-1$ for $m = 1, \ldots, \gamma-1$. By the inductive hypothesis (4·5·6) we have for $m = 1, \ldots, \gamma-1$,

$$S_m \geqslant \min\left(\frac{v_0}{p}, \frac{v_0}{p^2}+\frac{v_1}{p}, \ldots, \frac{v_0}{p^m}+\ldots+\frac{v_{m-1}}{p}\right)-1+\frac{1}{p^m}.$$

Suppose the minimum is attained by the expression

$$\frac{v_0}{p^r}+\ldots+\frac{v_{r-1}}{p},$$

where $1 \leqslant r \leqslant m$. Then it suffices if

$$\frac{v_0}{p^r}+\ldots+\frac{v_{r-1}}{p}-1+\frac{1}{p^m} > p-2.$$

Now the left-hand side of this inequality is

$$\geqslant \frac{v_0+\ldots+v_{r-1}}{p^r}-1+\frac{1}{p^m}$$

$$\geqslant \frac{r(s/k)}{p^r}-1+\frac{1}{p^m} \quad \text{by (4·1·3)},$$

$$\geqslant \frac{m(s/k)}{p^m}-1+\frac{1}{p^m} \quad \text{since } p > 2,$$

$$\geqslant \frac{(\gamma-1)\,s/k+1}{p^{\gamma-1}}-1 \quad \text{since } m \leqslant \gamma-1.$$

Hence it suffices to prove $$\frac{(\gamma-1)\,s/k+1}{p^{\gamma-1}} > p-1.$$

Now by hypothesis, $s/k > (p^\gamma-1)/\gamma$, so that it suffices to show

$$\frac{\gamma-1}{\gamma}(p^\gamma-1)+1 > p^{\gamma-1}(p-1).$$

Thus it is enough to show that $$\gamma p^{\gamma-1}+1 > p^\gamma$$

and since $p \leqslant \gamma$ by hypothesis, this inequality holds and hence the analogues of (4·5·6) and (4·5·7) with $m+1$ instead of m, hold when $p > 2$.

Case III. Suppose $V_m > w$, $p = 2$. Let X_1 denote the number of coefficients of the V_m original and secondary variables in $H^{(m)}$ which are congruent to 1 (mod 4), and let X_2 denote the number congruent to 3 (mod 4). Then $V_m = X_1+X_2$. We can select pairs of terms from these two groups of coefficients in the same residue class (mod 4) to construct at least $[\frac{1}{2}X_1]+[\frac{1}{2}X_2]$ secondary variables.

First, suppose $w > 0$. Then we can select $[\frac{1}{2}(V_m-w)]$ such pairs, for

$$[\tfrac{1}{2}(V_m-w)] = [\tfrac{1}{2}(X_1+X_2-w)] \leqslant [\tfrac{1}{2}X_1]+[\tfrac{1}{2}X_2],$$

and by applying contractions of the second kind to them, obtain $[\frac{1}{2}(V_m-w)]$ new secondary variables. Hence

$$V_{m+1} = v_{m+1}+[\tfrac{1}{2}(V_m-w)].$$

There remain $$V_m - 2[\tfrac{1}{2}(V_m - w)] \geqslant w$$

original and secondary variables in $H^{(m)}$. We combine w of these with the w primary variables in $H^{(m)}$, and thus get w new primary variables in H_{m+1}, so that plainly

$$S_{m+1} = S_m - w + w = S_m.$$

As before this implies that (4·5·6) is satisfied when m is replaced by $m+1$. We also have

$$\begin{aligned} S_{m+1} + V_{m+1} &= S_m + [\tfrac{1}{2}(V_m - w)] + v_{m+1} \\ &\geqslant \tfrac{1}{2}(S_m + V_m) + v_{m+1} - 1 + \tfrac{1}{2}, \end{aligned}$$

since $S_m \geqslant w$. Because the inductive hypothesis (4·5·7) holds for $S_m + V_m$, it follows exactly as in the case $p > 2$ that (4·5·7) also holds when m is replaced by $m+1$.

Next suppose $w = 0$ and $V_m \geqslant 2$. Then immediately

$$S_{m+1} = S_m.$$

Also we have $$[\tfrac{1}{2}X_1] + [\tfrac{1}{2}X_2] \geqslant \tfrac{1}{2}X_1 + \tfrac{1}{2}X_2 - 1 = \tfrac{1}{2}(V_m - 2) \geqslant 0.$$

Hence we are able to select at least $\frac{1}{2}(V_m - 2)$ pairs of secondary and original variables from $H^{(m)}$ which can sustain contractions of the second type, giving us at least $\frac{1}{2}(V_m - 2)$ new secondary variables in $H^{(m+1)}$, from which it follows that

$$V_{m+1} \geqslant v_{m+1} + \tfrac{1}{2}(V_m - 2).$$

Finally, suppose that $w = 0$ and $V_m = 1$. Then it is again immediate that

$$S_{m+1} = S_m,$$

and since we make no contractions of the second kind, plainly

$$V_{m+1} = v_{m+1} \geqslant v_{m+1} + \tfrac{1}{2}(V_m - 2).$$

It follows as previously that the equation $S_{m+1} = S_m$ implies that (4·5·6) is satisfied for $m+1$ in place of m. It remains to show that (4·5·7) also holds when m is replaced by $m+1$. We have

$$\begin{aligned} S_{m+1} + V_{m+1} &\geqslant S_m + \tfrac{1}{2}V_m - 1 + v_{m+1} \\ &\geqslant \tfrac{1}{2}(S_m + V_m) + v_{m+1} - 1 + \tfrac{1}{2}, \end{aligned}$$

provided $S_m \geqslant 1$, in which case we have, as before, that (4·5·7) holds with m replaced by $m+1$.

In order to show $S_m \geqslant 1$ for $m = 1, \ldots, \gamma - 1$, we must use the conditions $2 \leqslant \gamma$ and $s/k > (2^\gamma - 1)/\gamma$. By the inductive hypothesis (4·5·6), it suffices to prove

$$\frac{v_0}{2^r} + \ldots + \frac{v_{r-1}}{2} - 1 + \frac{1}{2^m} > 0$$

for $r = 1, \ldots, m$. In the same way as in the case $p > 2$, the conditions $2 \leqslant \gamma$ and $s/k > (2^\gamma - 1)/\gamma$ imply this inequality, and the proof is now complete.

4·6. *Upper and lower bounds for* $\Gamma^*(k,p)$ *when* $p-1$ *divides* k

As a consequence of the preceding lemma, we have

LEMMA 4·6·1. *If* p *is any prime and* $p-1$ *divides* k, *then*

$$\Gamma^*(k,p) \leqslant \left[\frac{k(p^\gamma-1)}{\gamma}\right]+1. \tag{4·6·1}$$

Proof. Since we are given that $p-1$ divides k, we have $d=(k,p-1)=p-1$, whence $\gamma^*(k,p)=p$ by (2·3·2). We note that the case $p=2$ is automatically included here.

If $p \geqslant \gamma$, the result follows from lemma 4·3·2 (with $\nu=p$), so that we can suppose $p<\gamma$. Moreover, if p is prime to k, then by lemma 4·2·2, the statement of the lemma holds with equality. Thus, without loss of generality, we assume that $p<\gamma$ and p divides k.

We have to prove that for these primes p, the congruence (4·1·1) has a primitive solution if

$$s > \frac{k(p^\gamma-1)}{\gamma},$$

and for this it suffices if, in the notation of lemma 4·5·1, $S_\gamma > 0$. Now by lemma 4·5·1, we have by (4·5·6) with $m=\gamma$,

$$S_\gamma \geqslant \min\left(\frac{v_0}{p}, \frac{v_0}{p^2}+\frac{v_1}{p}, \ldots, \frac{v_0}{p^\gamma}+\ldots+\frac{v_{\gamma-1}}{p}\right)-1+\frac{1}{p^\gamma}.$$

Suppose the minimum is attained for

$$\frac{v_0}{p^r}+\ldots+\frac{v_{r-1}}{p},$$

where $1 \leqslant r \leqslant \gamma$. The last expression is at least

$$\frac{v_0+\ldots+v_{r-1}}{p^r} > \frac{rs/k}{p^r} \geqslant \frac{r(p^\gamma-1)}{p^r\gamma} \geqslant \frac{p^\gamma-1}{p^\gamma},$$

since r/p^r does not increase for increasing integer values of $r \geqslant 1$ when $p \geqslant 2$. It follows that $S_\gamma > 0$, whence the lemma.

As a complement to the preceding result, we now establish a lower bound for $\Gamma^*(k,p)$. We consider the cases p odd and $p=2$ separately.

LEMMA 4·6·2. *If* p *is an odd prime such that* $p-1$ *divides* k, *then*

$$\Gamma^*(k,p) \geqslant [k/\gamma]\,(p^\gamma-1)+1. \tag{4·6·2}$$

Proof. First if p does not divide k, then $\tau=0$ and $\gamma=1$ and lemma 4·2·2 applies, giving us

$$\Gamma^*(k,p) = k(p-1)+1,$$

which plainly implies the result. It remains to prove the lemma when p divides k and it suffices, by the definition of $\Gamma^*(k,p)$, to construct a form in $[k/\gamma]\,(p^\gamma-1)$ variables such that the congruence (4·1·1) has only the trivial solution for some n. Consider the form

$$\Sigma = \Sigma^{(0)}+p^\gamma\Sigma^{(1)}+p^{2\gamma}\Sigma^{(2)}+\ldots+p^{([k/\gamma]-1)\gamma}\Sigma^{([k/\gamma]-1)},$$

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

where each $\Sigma^{(j)}$ $(j=1,\ldots,[k/\gamma]-1)$ is a sum of $p^\gamma-1$ kth powers. Now for odd primes p, we have $\gamma=\tau+1<p^\tau\leqslant k$, whence if $x\equiv 0 \pmod p$,

$$x^k\equiv 0 \pmod{p^\gamma}.$$

If $x\not\equiv 0 \pmod p$, then by Euler's theorem,

$$x^k=x^{p^\tau(p-1)k_0}\equiv 1 \pmod{p^{\tau+1}},$$

since by hypothesis, k is expressible as $k=p^\tau(p-1)k_0$, where k_0 is prime to p.

It follows that no sum $\Sigma^{(j)}$ is congruent to 0 $(\mathrm{mod}\, p^\gamma)$ unless each variable is divisible by p, so that if $n>([k/\gamma]-1)\gamma$ the congruence

$$\Sigma\equiv 0 \pmod{p^n}$$

has only the trivial solution. This concludes the lemma.

We now consider the case $p=2$.

Lemma 4·6·3. *Suppose k is greater than 2. Then*

$$\Gamma^*(k,2)\begin{cases}\geqslant [k/\gamma]\,(2^\gamma-1)+1 & \text{if } k \text{ is even,}\\ =k+1 & \text{if } k \text{ is odd.}\end{cases} \tag{4·6·3}$$

Proof. If k is odd, the result is simply lemma 4·2·2 with $p=2$. If k is even, then $k>2$ by hypothesis, whence if x is even and $k=2^\tau k_0$, where k_0 is odd,

$$x^k=x^{2^\tau k_0}\equiv 0 \pmod{2^\gamma},$$

since $\gamma=\tau+2$. On the other hand if x is odd,

$$x^2\equiv 1 \pmod 8,$$

and it follows that

$$x^{2^\tau}\equiv 1 \pmod{2^{3+\tau-1}},$$

whence

$$x^k=x^{2^\tau k_0}\equiv 1 \pmod{2^\gamma}.$$

Consider the form Σ in $[k/\gamma]\,(2^\gamma-1)$ variables given by

$$\Sigma=\Sigma^{(0)}+2^\gamma\Sigma^{(1)}+\ldots+2^{([k/\gamma]-1)\gamma}\Sigma^{([k/\gamma]-1)},$$

where each $\Sigma^{(j)}$ $(j=1,\ldots,[k/\gamma]-1)$ is a sum of $2^\gamma-1$ kth powers. Since x^k assumes only the values 1 (for odd k) and 0 (for even k), no sum $\Sigma^{(j)}$ is congruent to 0 $(\mathrm{mod}\, 2^\gamma)$ unless each variable is even. Hence if $n>([k/\gamma]-1)\gamma$, the congruence

$$\Sigma\equiv 0 \pmod{p^n}$$

has only the trivial solution, whence the lemma, by the definition of $\Gamma^*(k,2)$.

We observe that if, in addition, γ divides k, then the upper and lower bounds for $\Gamma^*(k,p)$ just given coincide and we have

Lemma 4·6·4. *Suppose p is any prime and suppose $p-1$ and γ divide k. Then*

$$\Gamma^*(k,p)=\frac{k(p^\gamma-1)}{\gamma}+1. \tag{4·6·4}$$

Proof. If p is odd, the result plainly follows from lemmas 4·6·1 and 4·6·2. If $p = 2$ and k is even then it follows from lemmas 4·6·1 and 4·6·3. If $p = 2$ and k is odd, then $\gamma = 2$ and hence cannot divide k, and the lemma is proved.

Some of the results established for $\Gamma^*(k, p)$ are set out in table 1.

TABLE 1

k	$\Gamma^*(k, p)$
$p-1$	k^2+1
$p(p-1)$	$\frac{1}{2}k^2(1+1/p)+1$
$2(p-1)$	$\frac{1}{2}k^2+1$

It will be seen that $\Gamma^*(k, p)$ decreases as a function of k as we go down the table. At present, however the table cannot be continued, since when k is expressible as $k = p^2(p-1)$ for some odd prime p, $\Gamma^*(k, p)$ cannot in general be evaluated exactly, and we know only that

$$[\tfrac{1}{3}k]\,(p^3-1)+1 \leqslant \Gamma^*(k,p) \leqslant [\tfrac{1}{3}k(p^3-1)]+1 = [\tfrac{1}{3}k^2(1+p^{-1}+p^{-2})]+1,$$

by lemmas 4·6·1 and 4·6·2. To have equality here, we require k to be divisible by 3.

It is possible to obtain a sharper result than that of lemma 4·6·2 when γ does not divide k: if p and $p-1$ divide k and γ does not divide k, then

$$\Gamma^*(k,p) \geqslant [k/\gamma]\,(p^\gamma-1)+p^{k-[k/\gamma]\gamma}.$$

This is obtained by introducing $p^{k-[k/\gamma]\gamma}-1$ more variables into the form Σ in lemma 4·6·2 as follows. Consider the form

$$\Sigma_1 = \Sigma^{(0)}+p^\gamma\Sigma^{(1)}+\ldots+p^{([k/\gamma]-1)\gamma}\Sigma^{([k/\gamma]-1)}+p^{[k/\gamma]\gamma}\Sigma',$$

where Σ' is a sum of $p^{k-[k/\gamma]\gamma}-1$ kth powers and the $\Sigma^{(j)}$ are sums of $p^\gamma-1$ kth powers as before. Since Σ' assumes only the values $0, 1, \ldots, p^{k-[k/\gamma]\gamma}-1$, the congruence

$$\Sigma_1 \equiv 0 \pmod{p^n}$$

has only the trivial solution for $n > k-1$.

This result is not used here but we note that when γ does divide k, we get lemma 4·6·2.

5. The number $\Gamma^*(k)$

5·1. *Introduction*

We are now in a position to establish our results for $\Gamma^*(k)$. We recall the definition of $\Gamma^*(k)$ as the least positive integer s with the following property: for any non-zero integers $a_1, \ldots, a_s$, the congruence

$$a_1 x_1^k+\ldots+a_s x_s^k \equiv 0 \pmod{p^n} \qquad (5\cdot1\cdot1)$$

has a primitive solution for every prime power p^n. In §4 we investigated the solubility of this congruence for any given prime p by means of the function $\Gamma^*(k, p)$, which was defined to be the least positive integer s such that for any non-zero integers $a_1, \ldots, a_s$ and every positive integer n, the congruence (5·1·1) has a primitive solution for the particular prime p. As we saw in §1, it is immediate that

$$\Gamma^*(k) = \underset{\text{(primes } p)}{\text{maximum}}\ \Gamma^*(k,p). \qquad (5\cdot1\cdot2)$$

We use this formula to obtain our results for $\Gamma^*(k)$.

5·2. *Some arithmetical results for* $\Gamma^*(k)$

We recall that Davenport & Lewis (1963, theorem 1) have shown that for all k,

$$\Gamma^*(k) \leqslant k^2+1 \tag{5·2·1}$$

and that there is equality here whenever $k+1$ is a prime. Also, Chowla & Shimura (1963, theorem A) have proved that for all odd $k > k_1(\epsilon)$,

$$\Gamma^*(k) < (2/\log 2+\epsilon)\, k \log k,$$

where ϵ is an arbitrary positive number. Here we obtain estimates for $\Gamma^*(k)$ when k is even and $k+1$ is not a prime, and we prove the result of Chowla & Shimura in a more explicit form (without the ϵ as above), which is applicable for numerical values of k.

Our first result provides a simple upper bound for all k for which $k+1$ is not a prime.

THEOREM 5·2·1. *Suppose $k+1$ is composite. Then*

$$\Gamma^*(k) \leqslant \tfrac{49}{64}k^2+1. \tag{5·2·2}$$

Proof. The theorem is true for $k \leqslant 6$ when $k+1$ is composite, since $\Gamma^*(3) = 7$ and $\Gamma^*(5) = 16$. For $k \geqslant 7$, by virtue of (5·1·2) it suffices to show that if $k+1$ is composite, then

$$\Gamma^*(k,p) \leqslant \tfrac{49}{64}k^2+1$$

for every prime p. We consider the various cases with $k \geqslant 7$.

Case I. $d = (k, p-1) < p-1$. In this case lemma 4·4·1 applies and we have

$$\Gamma^*(k,p) \leqslant \tfrac{1}{2}k^2+k+1 < \tfrac{49}{64}k^2+1,$$

since $k \geqslant 7$.

Case II. $d = p-1$. Here we consider primes p such that $p-1$ divides k, so that k is expressible as

$$k = p^\tau(p-1)\, k_0, \quad (k_0, p) = 1 \quad (\tau \geqslant 0). \tag{5·2·3}$$

We note that the case $p = 2$ is necessarily included.

(i) $\tau = 0$. Here the conditions of lemma 4·2·2 are satisfied and we have

$$\Gamma^*(k,p) = k(p-1)+1 = 1+k^2/k_0.$$

Plainly, $\Gamma^*(k,2) = k+1$, and when p is odd, we must have $k_0 \geqslant 2$, since otherwise $k+1$ would be a prime. Hence in this case

$$\Gamma^*(k,p) \leqslant \tfrac{1}{2}k^2+1 < \tfrac{49}{64}k^2+1.$$

(ii) $\tau = 1, p > 2$. Here k can be expressed in the form

$$k = p(p-1)\, k_0, \quad (k_0, p) = 1,$$

and it follows from lemma 4·6·1 that

$$\Gamma^*(k,p) \leqslant \tfrac{1}{2}k(p^2-1)+1 = \frac{k^2}{2k_0}\left(1+\frac{1}{p}\right)+1 \leqslant \tfrac{3}{5}k^2+1,$$

for the least integer k of the form $p(p-1)\, k_0$ such that $k+1$ is composite is 20 ($p = 5$).

(iii) $\tau \geqslant 2, p > 2$. In this case k is expressible in the form (5·2·3) except that now $\tau \geqslant 2$, so that $\gamma \geqslant 3$, and $p \geqslant 3$. It follows that

$$\frac{p^\gamma - 1}{\gamma} \leqslant \frac{1}{2}\cdot\frac{2}{3}\cdot\frac{p^{\tau+1}-1}{p-1}(p-1) < \tfrac{1}{2}p^\tau(p-1) \leqslant \tfrac{1}{2}k.$$

Applying lemma 4·6·1 again, we get

$$\Gamma^*(k,p) \leqslant \frac{k(p^\gamma-1)}{\gamma} + 1 < \tfrac{1}{2}k^2 + 1 < \tfrac{49}{64}k^2 + 1.$$

It remains to consider the case $p = 2$ when k is even.

(iv) $\tau > 0, p = 2$. Once more lemma 4·6·1 gives

$$\Gamma^*(k,2) \leqslant \left[\frac{k(2^{\tau+2}-1)}{\tau+2}\right] + 1, \tag{5·2·4}$$

since $\gamma = \tau+2$ now. Also k is of the form

$$k = 2^\tau k_0, \quad k_0 \text{ odd}, \quad \tau > 0.$$

First suppose $k_0 > 1$. Then since $\tau \geqslant 1$ and $k_0 > 2$, we have

$$\Gamma^*(k,2) \leqslant \frac{k}{3}\left(\frac{4k}{3} - 1\right) + 1 < \tfrac{49}{64}k^2 + 1.$$

Next suppose $k_0 = 1$, i.e. $k = 2^\tau$, where $\tau \geqslant 3$ by the hypothesis that $k+1$ is composite. If $\tau > 3$, it follows from (5·2·4) that

$$\Gamma^*(k,2) \leqslant \frac{k}{\tau+2}(4k-1) + 1 \leqslant \tfrac{1}{6}k(4k-1) + 1 < \tfrac{2}{3}k^2 + 1 < \tfrac{49}{64}k^2 + 1;$$

and when $\tau = 3$, we have $\Gamma^*(8,2) \leqslant \left[\frac{8\times 31}{5}\right] + 1 = \tfrac{49}{64}k^2 + 1.$

We have now covered all the possible cases and thus have shown that if $k+1$ is composite, then

$$\Gamma^*(k,p) \leqslant \tfrac{49}{64}k^2 + 1$$

for all primes p. This establishes theorem 5·2·1.

We remark that we need to know more about $\Gamma^*(8)$ in order either to establish that the constant $\frac{49}{64}$ is best possible or to improve on it. However, by excluding two particular values of k, we get a sharp upper bound for $\Gamma^*(k)$ in

THEOREM 5·2·2. *Suppose $k+1$ is composite and $k \geqslant 7$. Then if the cases $k = 8$ and $k = 32$ are excluded,*

$$\Gamma^*(k) \leqslant \tfrac{1}{2}k^2\left(1 + \frac{2}{1+\sqrt{(1+4k)}}\right) + 1, \tag{5·2·4a}$$

and there is equality here when $k = p(p-1)$ for some odd prime p, in which case the inequality becomes

$$\Gamma^*(k) = \Gamma^*(p(p-1)) = \tfrac{1}{2}k^2(1+1/p) + 1. \tag{5·2·5}$$

Proof. We observe that in the preceding proof, with the exception of the case $p = 2$, $k_0 = 1$, $\tau > 0$ and the case $p > 2$, $d = p-1$, $\tau = 1$, we have

$$\begin{aligned}\Gamma^*(k,p) &\leqslant \tfrac{1}{2}k^2+k+1\\ &< \tfrac{1}{2}k^2\left(1+\frac{2}{1+\sqrt{(1+4k)}}\right)+1\end{aligned}$$

for $k \geqslant 7$.

First, we consider the case $p = 2$, $k_0 = 1$, $\tau > 0$, i.e. the case when k is a power of 2. By lemma 4·6·1 we have

$$\begin{aligned}\Gamma^*(k,2) &\leqslant \frac{k}{\tau+2}(2^{\tau+2}-1)+1\\ &\leqslant \tfrac{1}{8}k(4k-1)+1,\end{aligned}$$

for by the hypotheses of the theorem we have excluded the cases $k = 2, 4, 8, 16$ and 32. It follows that

$$\Gamma^*(k,2) < \tfrac{1}{2}k^2+1.$$

Now we deal with the case $p > 2$, $d = p-1$, $\tau = 1$. Here k is expressible in the form

$$k = p(p-1)\,k_0, \quad (k_0,p) = 1. \tag{5·2·6}$$

Since $p-1$ divides k, k is even and so $\gamma\ (=2)$ divides k, whence lemma 4·6·4 gives

$$\begin{aligned}\Gamma^*(k,p) &= \tfrac{1}{2}k(p^2-1)+1\\ &= \frac{k^2}{2k_0}(1+1/p)+1,\end{aligned}$$

using the representation for k given in (5·2·6). Hence, when $k_0 \geqslant 2$,

$$\Gamma^*(k,p) \leqslant \tfrac{1}{4}k^2(1+1/p)+1 \leqslant \tfrac{1}{3}k^2+1,$$

since $p \geqslant 3$. Lastly, when $k_0 = 1$, i.e. when $k = p(p-1)$, we have

$$\begin{aligned}\Gamma^*(k,p) &= \tfrac{1}{2}k^2(1+1/p)+1\\ &= \tfrac{1}{2}k^2\left(1+\frac{2}{1+\sqrt{(1+4k)}}\right)+1.\end{aligned}$$

In view of (5·1·2), this gives the theorem.

This theorem enables us to evaluate $\Gamma^*(k)$ exactly when $k+1$ is composite and k is expressible in the form $k = p(p-1)$ for some odd prime p. Thus we deduce that

$$\Gamma^*(20) = 241, \quad \Gamma^*(110) = 6\,601, \quad \Gamma^*(272) = 39\,169.$$

When k is odd, we have good estimates for $\Gamma^*(k,p)$ for all primes p and this immediately leads to a good estimate for $\Gamma^*(k)$ in this case. We prove

THEOREM 5·2·3. *If k is odd and $k \geqslant 7$,* then

$$\Gamma^*(k) \leqslant k\left[\frac{2\log 2k}{\log 2}\right]+1. \tag{5·2·7}$$

Proof. By (5·1·2) it suffices to prove that for odd k,

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

for every prime p.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

First, suppose $p = 2$. Then since k is odd, we have by lemma 4·2·2 that

$$\Gamma^*(k, 2) = k+1.$$

Next suppose p is an odd prime. Then $d = (k, p-1)$ divides $\frac{1}{2}(p-1)$. Suppose further that p divides k. Then by lemma 3·2·1,

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

since $\gamma = \tau+1$ and $\tau \geqslant 1$. Therefore lemma 4·2·1 gives

$$\Gamma^*(k, p) \leqslant k\left[\frac{2 \log k}{\log 2}\right]+1.$$

Finally, suppose p is prime to k. Then from lemma 2·2·1 we have

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

Thus if $p < 2d^2$, $$\gamma^*(k, p) \leqslant \left[\frac{\log (2d)^2}{\log 2}\right]+1 = \left[\frac{2 \log 2d}{\log 2}\right]+1,$$

while if $p > 2d^2$, then by lemma 2·4·1 we have

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

whence, since d divides k, we have that when p does not divide k,

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

Therefore by comparison with the estimates obtained above for $\Gamma^*(k, p)$ for other primes p, we get

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

for all primes p, whence the theorem, by virtue of (5·1·2).

5·3. *A lower bound for* $\Gamma^*(k)$

When k is odd, we have by lemma 4·2·2 that

$$\Gamma^*(k, 2) = k+1,$$

whence, by (5·1·2), $$\Gamma^*(k) \geqslant k+1$$

for all odd k.

When k is even, k is of the form $k = 2^\tau k_0$, where k_0 is odd and $\tau > 0$, and we have, by lemma 4·6·3,

$$\Gamma^*(k, 2) \geqslant \left[\frac{k}{\tau+2}\right](2^{\tau+2}-1)+1 \geqslant \left(\frac{k-\tau-1}{\tau+2}\right)(2^{\tau+2}-1)+1.$$

Now
$$\begin{aligned}(k-\tau-1)(2^{\tau+2}-1)-k2^{\tau} &= (3.2^{\tau}-1)k-(\tau+1)2^{\tau+2}+\tau+1\\ &\geqslant (3.2^{\tau}-1)2^{\tau}-(\tau+1)2^{\tau+2}+\tau+1\\ &> 0\end{aligned}$$

for $k \geqslant 6$, whence
$$\begin{aligned}\Gamma^*(k,2) &\geqslant \frac{k2^{\tau}}{\tau+2}+1,\\ &\geqslant k+1\end{aligned}$$

providing $\tau \geqslant 2$. When $\tau = 1$, lemma 4·6·3 again gives
$$\begin{aligned}\Gamma^*(k,2) &\geqslant \tfrac{1}{3}(k-2)7+1\\ &\geqslant k+1\end{aligned}$$

for $k \geqslant 4$. Thus if k is even, $\Gamma^*(k) \geqslant k+1$, since it is well known that $\Gamma^*(2) = 5$. Hence we have proved†

THEOREM 5·3·1. *For all* k
$$\Gamma^*(k) \geqslant k+1.$$

This lower bound may be capable of substantial improvement for all sufficiently large k and in fact we conjecture that
$$\lim_{k\to\infty}\frac{\Gamma^*(k)}{k} = \infty.$$

However this seems a difficult problem and may be connected with the problem of a lower bound for $\Gamma(k)$, about which little is known beyond $\Gamma(k) \geqslant 3$ for all $k > 1$.

5·4. *Some order results for* $\Gamma^*(k)$

It is an immediate consequence of (5·2·1) that
$$\Gamma^*(k) \ll k^2,$$

where $\ll$ and $\gg$ denote inequalities with unspecified positive constants. We now show that for certain k,
$$\Gamma^*(k) \gg k^2,$$

that is
$$\Gamma^*(k) > ck^2,$$

for some positive constant $c < 1$.

THEOREM 5·4·1. *Suppose* k *is expressible in the form*
$$k = p^{\tau}(p-1)k_0,$$

where p *is an odd prime,* k_0 *is not divisible by* p *and* $\tau \geqslant 0$. *Suppose further that* $\tau \ll 1$ *and* $k_0 \ll 1$. *Then*
$$k^2 \ll \Gamma^*(k) \ll k^2. \qquad (5\cdot4\cdot1)$$

Proof. By (5·2·1), $\Gamma^*(k) \ll k^2$ for all k. To prove $\Gamma^*(k) \gg k^2$ whenever k is of the type given, it is enough to show, by (5·1·2), that for the particular prime p,
$$\Gamma^*(k,p) \gg k^2.$$

Now we can suppose $\tau > 0$ without loss of generality, since otherwise, by lemma 4·2·2,
$$\begin{aligned}\Gamma^*(k,p) &= k(p-1)+1\\ &= 1+k^2/k_0\\ &\gg k^2.\end{aligned}$$

† This result can also be deduced from the fact that if p is a prime not dividing k, the congruence $x_1^k+px_2^k+\ldots+p^{k-1}x_k^k \equiv 0 \pmod{p}$ does not have a primitive solution.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Since $p \geqslant 3$ and $\tau \geqslant 1$, we have the inequality

$$(k-\tau)(p^{\tau+1}-1)-kp^{\tau}(p-1) \geqslant p^{\tau}(p-1)(p^{\tau}-1)-\tau(p^{\tau+1}-1)$$
$$> p^{2\tau+1}(1-1/p-(\tau+1)/p^{\tau+1}) \geqslant 0,$$

and since by lemma 4·6·2

$$\Gamma^*(k,p) \geqslant \left[\frac{k}{\tau+1}\right](p^{\tau+1}-1)+1 \geqslant \left(\frac{k-\tau}{\tau+1}\right)(p^{\tau+1}-1)+1,$$

it follows that

$$\Gamma^*(k,p) \geqslant \frac{k^2}{(\tau+1)k_0}+1.$$

Therefore by the hypothesis on k_0 and τ we have

$$\Gamma^*(k,p) \gg k^2,$$

and this proves the theorem.

We note that we could replace the conditions on τ and k_0 in the enunciation of the theorem by the single condition $(\tau+1)k_0 \ll 1$, but since $\tau \geqslant 0$ and $k_0 \geqslant 1$, it is clear that they are equivalent.

We have shown in Theorem 5·2·3 that for odd k, $\Gamma^*(k) = O(k \log k)$. Now we show that there are infinitely many even k for which $\Gamma^*(k)$ is of lower order than k^2. More precisely, we prove

THEOREM 5·4·2. *There exists an infinity of even k such that*

$$\Gamma^*(k) < 12(\log k)^2 k^{\frac{15}{8}}.$$

Proof. Suppose p is a prime congruent to 1 (mod 3), and suppose q is any prime greater than 3. Then $q-1$ does not divide $2p$; for suppose the contrary. Then we can write $2p$ as

$$2p = (q-1)m,$$

where, since p is a prime, the only possible values for m are 1, 2, p or $2p$. We consider these four possibilities separately:

(i) $m = 1$. Since $p \equiv 1 \pmod 3$, there exists an integer a such that $p = 3a+1$, whence

$$q = 2p+1 = 2(3a+1)+1 = 3(2a+1).$$

It follows that 3 must divide q which contradicts the choice of q.

(ii) $m = 2$. In this case $p = q-1$, which is impossible since p and q are both primes > 3.

(iii) $m = p$. Here q must be 3, which is a contradiction.

(iv) $m = 2p$. This case implies $q = 2$ which again is a contradiction.

We take $k = 2p$, where p is a prime congruent to 1 (mod 3). Then, if q is any prime > 3, we have by lemma 4·4·2 that

$$\Gamma^*(k,q) < 12(\log k)^2 k^{\frac{15}{8}},$$

since, by our choice of k, $q-1$ does not divide k.

Next we consider $\Gamma^*(k,3)$. In this case

$$d = (k, 3-1) = (2p, 2) = 2 \quad \text{and} \quad \tau = 0.$$

Hence, by lemma 4·2·2,

$$\Gamma^*(k,3) = 2k+1.$$

Finally, we consider $\Gamma^*(k, 2)$. Here $\tau = 1$ and $\gamma = 3$, and lemma 4·6·1 gives us that

$$\Gamma^*(k, 2) \leqslant \tfrac{1}{3}k(2^3-1)+1 < 3k.$$

It follows from (5·1·2) that when $k = 2p$, where $p \equiv 1 \pmod 3$ is a prime,

$$\Gamma^*(k) < 12(\log k)^2 k^{\frac{15}{8}}.$$

Since by Dirichlet's theorem on primes in arithmetic progression there are infinitely many primes $p \equiv 1 \pmod 3$, the theorem is proved.

5·5. *Estimates for $\Gamma^*(k)$ when k is large*

It is possible to improve the estimate for $\Gamma^*(k)$ given in theorem 5·2·2 at the cost of further restricting k, and in fact we need in addition to $k+1$ being composite, to have k not expressible in the form $k = p(p-1)$, where p is an odd prime, and to have k sufficiently large as well. The necessity for the last condition arises from the arithmetical estimate for $\Gamma^*(k, p)$ when $p-1$ does not divide k, given in lemma 4·4·1, no longer being strong enough and this forces us to use the estimate of lemma 4·4·2.

THEOREM 5·5·1. *If k is sufficiently large, then*

$$\Gamma^*(k) \leqslant \tfrac{1}{2}k^2+1, \tag{5·5·1}$$

unless k belongs to either of the following special disjoint classes:

(I) $k = p-1$, *p an odd prime, in which case*

$$\Gamma^*(k) = k^2+1;$$

(II) $k = p(p-1)$, *p an odd prime and k is not a member of the class (I), in which case*

$$\Gamma^*(k) = \tfrac{1}{2}k^2(1+1/p)+1.$$

Moreover, when k is sufficiently large and expressible in the form

$$k = 2(p-1)$$

for some odd prime p, then we have equality in (5·5·1) and

$$\Gamma^*(k) = \tfrac{1}{2}k^2+1. \tag{5·5·2}$$

Proof. If k is in either class (I) or class (II), then the theorem follows immediately by (5·2·1) and theorem 5·2·2 respectively.

Suppose k does not belong to either of the classes (I) or (II). Now if $d = (k, p-1) < p-1$, then by Lemma 4·4·2 we have

$$\Gamma^*(k, p) < 12(\log k)^2 k^{\frac{15}{8}} \leqslant \tfrac{1}{2}k^2+1$$

for k sufficiently large. Thus in view of (5·1·2), we need only consider $\Gamma^*(k, p)$ when $p-1$ divides k.

First, when $p = 2$, we express k in the form

$$k = 2^\tau k_0, \quad k_0 \text{ odd}, \quad \tau \geqslant 0,$$

and we have, by lemma 4·6·1, that

$$\Gamma^*(k,2) \leqslant \left[\frac{k}{\tau+2}(2^{\tau+2}-1)\right]+1$$
$$< \frac{4k^2}{(\tau+2)k_0}+1$$
$$\leqslant \tfrac{1}{2}k^2+1$$

for $k > 32$.

When p is odd and $p-1$ divides k, we express k in the form

$$k = p^\tau(p-1)k_0, \quad (k_0,p)=1, \quad \tau \geqslant 0.$$

In this case lemma 4·6·1 gives

$$\Gamma^*(k,p) \leqslant \left[\frac{k(p^{\tau+1}-1)}{\tau+1}\right]+1.$$

Now when k does not belong to either of the classes (I) or (II), $\tau = 0$ or 1 implies $k_0 \geqslant 2$, and in the first of these two cases we have by lemma 4·2·2, that

$$\Gamma^*(k,p) = k(p-1)+1 = 1+k^2/k_0 \leqslant \tfrac{1}{2}k^2+1,$$

and we note that there is equality here when $k_0 = 2$. In the second case, lemma 4·6·4 holds and we have

$$\Gamma^*(k,p) = \tfrac{1}{2}k(p^2-1)+1 = \frac{k^2}{2k_0}\left(1+\frac{1}{p}\right)+1 \leqslant \tfrac{1}{3}k^2+1.$$

If $\tau \geqslant 2$, then lemma 4·6·1 gives

$$\Gamma^*(k,p) \leqslant \frac{k(p^{\tau+1}-1)}{\tau+1}+1 < \frac{kp^\tau(p-1)}{\tau+1}\,\frac{p}{p-1}+1 \leqslant \tfrac{1}{2}k^2+1.$$

Hence, when k is not a member of either of the classes (I) or (II), we have by (5·1·2) that

$$\Gamma^*(k) \leqslant \tfrac{1}{2}k^2+1,$$

and as we noted above, there is equality here when $k = 2(p-1)$ for some odd prime p, by lemma 4·2·2. This completes the theorem.

It is evident that this theorem does not provide a practical method for evaluating $\Gamma^*(k)$, since k must be very large indeed ($> 10^{13}$) before lemma 4·4·2 becomes effective. If we could improve either lemma 2·3·2 or lemma 2·6·7 sufficiently, we could prove this result for numerical values of k. We conjecture that this theorem is true for all k, so that for instance we conjecture that

$$\Gamma^*(24) = 289.$$

It seems difficult to obtain any substantial improvement in the classification of those k for which

$$\Gamma^*(k) > ck^2+1,$$

where c is a constant less than $\frac{1}{2}$. The reason for this is that at present, $\Gamma^*(k,p)$, unlike the analogous function $\Gamma(k,p)$ (Hardy & Littlewood 1928, lemma 7), cannot always be evaluated exactly when $p-1$ divides k. However we can extend theorem 5·5·1 in the following way:

THEOREM 5·5·2. *Let N be a positive integer. Suppose k is not expressible in the form*

$$k = (p-1)\,k_0, \quad (k_0, p) = 1,$$

with $k_0 < N$, nor in the form

$$k = p^\tau (p-1)\,k_0, \quad (k_0, p) = 1, \quad \tau > 0,$$

with

$$(\tau+1)\,k_0 < \tfrac{3}{2}N.$$

Then there exists a number $k_1(N)$ such that $k > k_1(N)$ implies

$$\Gamma^*(k) \leqslant 1 + k^2/N \tag{5·5·3}$$

and there is equality here when k is expressible in the form

$$k = (p-1)\,N,$$

where p is a prime not dividing N.

Proof. This follows the same lines as for the preceding theorem. As before, providing $k > k_1'(N)$, we can disregard $\Gamma^*(k,p)$ when $p-1$ does not divide k, and hence we need only consider those primes p such that $p-1$ divides k.

First, consider $\Gamma^*(k,2)$. Then, writing k in the form $k = 2^\tau k_0$, where k_0 is odd, we have from lemma 5·6·1 that

$$\Gamma^*(k,2) \leqslant \left[\frac{k}{\tau+2}(2^{\tau+2}-1)\right] + 1 < \frac{4k^2}{(\tau+2)\,k_0} + 1.$$

Now plainly $(\tau+2)\,k_0 \geqslant 4N$ if $k_0 \geqslant 2N$, and if $k_0 < 2N$ then

$$k = 2^\tau k_0 < 2^{\tau+1}N,$$

whence

$$(\tau+2)\,k_0 > \tau+1 > \frac{\log(k/N)}{\log 2} \geqslant 4N,$$

providing k is sufficiently large. Hence there exists a number $k_1''(N)$ such that $k > k_1''(N)$ implies

$$\Gamma^*(k,2) < 1 + k^2/N.$$

When p is an odd prime and $p-1$ divides k, we can express k as

$$k = p^\tau (p-1)\,k_0, \quad (k_0, p) = 1,$$

and in this case we have by lemma 4·6·1,

$$\Gamma^*(k,p) \leqslant \left[\frac{k(p^{\tau+1}-1)}{\tau+1}\right] + 1.$$

By hypothesis if $\tau = 0$ then $k_0 \geqslant N$, whence, in this case, lemma 4·2·2 gives

$$\Gamma^*(k,p) = 1 + k^2/k_0 \leqslant 1 + k^2/N,$$

and it is plain that if k is expressible in the form

$$k = (p-1)\,N,$$

where p is prime to N, there is equality here. If $\tau > 0$, then

$$\begin{aligned}\Gamma^*(k,p) &\leqslant \frac{kp^\tau(p-1)}{\tau+1}\,\frac{1-p^{-\tau-1}}{1-p^{-1}}+1\\ &\leqslant \frac{k^2}{(\tau+1)\,k_0}\,\frac{3}{2}+1\\ &\leqslant 1+k^2/N,\end{aligned}$$

since we are given that $(\tau+1)\,k_0 \geqslant \frac{3}{2}N$. The theorem follows on taking

$$k_1(N) = \max\{k_1'(N), k_1''(N)\},$$

and using (5·1·2).

We can extend this theorem further to other types of k.

THEOREM 5·5·3. *Suppose k is not expressible in the form*

$$k = p^\tau(p-1)\,k_0, \quad \tau \geqslant 0,$$

where p is an odd prime not dividing k_0, with

$$\frac{p^{\tau+1}-1}{\tau+1} \leqslant A.$$

Then there exists a positive number $k_1(A)$ such that $k > k_1(A)$ implies

$$\Gamma^*(k) \leqslant Ak+1,$$

and there is equality here if k can be expressed in the form

$$k = q^\tau(q-1)\,k_0, \quad (k_0, q) = 1, \quad \tau \geqslant 0,$$

where $\tau+1$ divides k, and

$$A = \frac{q^{\tau+1}-1}{q-1}.$$

The proof is similar to that of the preceding theorems: we verify that for k sufficiently large

$$\Gamma^*(k,p) \leqslant Ak+1,$$

and if k is of the form given in the enunciation, then by lemma 4·6·4,

$$\Gamma^*(k,q) = Ak+1.$$

As an example, suppose k is sufficiently large and expressible as $q(q-1)\,2$ for an odd prime q. Suppose further that k is not representable as $p-1$, $p(p-1)$, $p^2(p-1)$, $(p-1)\,2$ or $(p-1)\,3$ for any odd prime p. Then we deduce that

$$\Gamma^*(k) = \tfrac{1}{4}k(q^2-1)+1 = \tfrac{1}{4}k^2(1+1/q)+1.$$

We note that we have already dealt with the case when k is representable as $k = p(p-1)$, without the restriction that k must be sufficiently large, in theorem 5·2·2, and we conjecture that theorems 5·5·2 and 5·5·3 are also true without this restriction.

However, the question of the value of $\Gamma^*(k)$ when k is not of one of the types discussed above is not settled by this method.

This paper formed part of a dissertation submitted for the Ph.D. degree at the University of Cambridge, and I am deeply grateful to my supervisor Professor Davenport for suggesting this problem and for his considerable help and advice.

References

Chowla, I. 1937 On the number of solutions of some congruences in two variables. *Proc. Indian Nat. Acad. Sci.* A **5**, 40–44.

Chowla, I. 1943 On Waring's problem (mod p). *Proc. Nat. Acad. Sci. India* A **13**, 195–220.

Chowla, S. 1963 *Proceedings of the 1963 Number Theory Conference*. University of Colorado, Boulder, Colorado.

Chowla, S., Mann, H. B. & Straus, E. G. 1959 Some applications of the Cauchy–Davenport Theorem. *K. norske vidensk. Selsk. Forh.* **32**, Nr 13, 74–80.

Chowla, S. & Shimura, G. 1963 On the representation of zero by a linear combination of kth powers. *K. norske vidensk. Selsk. Forh.* **36**, Nr 37, 169–176.

Davenport, H. 1935 On the addition of residue classes. *J. Lond. Math. Soc.* **10**, 30–32.

Davenport, H. 1947 A historical note. *J. Lond. Math. Soc.* **22**, 100–101.

Davenport, H. & Lewis, D. J. 1963 Homogeneous additive equations. *Proc. Roy. Soc.* A **274**, 443–460.

Erdös, P. & Rado, R. 1960 Intersection theorems for systems of sets. *J. Lond. Math. Soc.* **35**, 85–90.

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

Heilbronn, H. 1964 *Lecture notes on additive number theory mod p*. California Institute of Technology.

Landau, E. 1947 *Vorlesungen über Zahlentheorie*. I. New York: Chelsea.

Schwarz, S. 1948 On Waring's problem for finite fields. *Quart. J. Math.* **19**, 160–163.

Vinogradov, I. M. 1953 *The method of trigonometrical sums in the theory of numbers* (trans. Roth and Davenport). London: Interscience.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES