(M_q may be taken positive since without loss of generality we may assume that none of the lines L_q or L_q^* lies in the y, z-plane.) It is easy to verify that the hypercubes $\mathscr{C}_n$ and $\mathscr{D}_n$ have the required properties if we let

$$R^{3/2} = \frac{2^5}{KK^*}, \qquad \bar{\varrho}_q = \frac{(KK^*)^{2^q} K_2^{1/2} M_q l_0}{(K+1)2^{5 \cdot 2^q + 1}}. \tag{5.12}$$

As we noted earlier, the Theorem now follows from the work in Section 3, for the avoidance of a tube around L_q^* by $\Lambda(a^*)$ is equivalent to the avoidance of a layer about P_q by $\Lambda(a)$.

References

[1] J. W. S. Cassels, *On a result of Marshall Hall*, Mathematika 3 (1956), pp. 109–110.

[2] — *An Introduction to Diophantine Approximation*, Cambridge 1957.

[3] — *An Introduction to the Geometry of Numbers*, Berlin 1959.

[4] H. Davenport, *A Note on Diophantine Approximation*, Studies in Mathematical Analysis and Related Topics, pp. 77–81, Stanford University Press, 1962.

Reçu par la Rédaction le 10. 8. 1968

ACTA ARITHMETICA
XVI (1969)

The average order of two arithmetical functions

by

M. M. Dodson (Auckland)

Let $F(k)$ be an arithmetical function of the positive integral variable k. If there is a simple function of k, $f(k)$ say, such that

$$\sum_{k \leqslant N} F(k) \sim \sum_{k \leqslant N} f(k),$$

then we say that $f(k)$ is the *average order* of $F(k)$. In this paper we establish an asymptotic expression for the sum $\sum\limits_{k \leqslant N} f(k)$ when $F(k)$ satisfies certain conditions. By considering two special cases we obtain the average order of two arithmetical functions. First we show that the average order of the function $\Gamma^*(k)$, introduced by Davenport and Lewis in their work on homogeneous additive equations [3], is $\dfrac{\pi^2 k^2}{6 \log k}$. Then we show that the average order of the function $\Gamma(k)$, introduced by Hardy and Littlewood in their work on Waring's Problem [5], is $\dfrac{5\pi^2 k}{12 \log k}$. We make use of a result in Sieve Theory on the distribution of primes and the underlying idea is that, with a permissible error, the values of k for which the function $F(k)$ is large have a simple distribution.

We begin with some notation and lemmas. Throughout this paper, k will denote a positive integer, N a sufficiently large positive integer and p a prime. We shall always write $r = [(\log N)^2]$, the integral part of $(\log N)^2$. Also we shall always write $d = (k, p-1)$, the highest common factor of k and $p-1$.

Now for any given prime p, we can express the positive integer k as

$$k = p^v dm = p^v \frac{p-1}{t} m, \tag{1}$$

where k is divisible by p^v but not by p^{v+1} and where $d = (k, p-1)$ and $t = \dfrac{p-1}{d}$. Thus in the representation (1) of an integer k, we have $(m, p) = 1$ and $(t, m) = \left(\dfrac{p-1}{d}, m\right) = 1$.

When $(m,t)=1$, we define the set $S(m,t)$ as follows:

$$S(m,t)=\left\{k\leqslant N;\ k=\frac{p-1}{t}m,\ (m,p)=1,\ \frac{p-1}{t}>1\right\}.$$

The number of elements in a set X will be denoted by $|X|$. Also, the symbol $\ll$ will denote an inequality with an unspecified positive constant factor.

We now obtain an estimate for the overlap between two different such sets. The proof relies on the following result from Sieve Theory ([9], p. 45, Satz 4.2):

THEOREM 1. *Let $a_1,\dots,a_s,b_1,\dots,b_s$ be integers and let*

$$a_i\neq 0,\quad (a_i,b_i)=1$$

for $i=1,\dots,s$ and suppose that the equations

$$a_i=\pm a_j,\quad b_i=\pm b_j,\quad i\neq j$$

do not hold simultaneously. Let $w(p)$ be the number of solutions, distinct $(\mathrm{mod}\,p)$, of the congruence

$$(a_1x+b_1)\dots(a_sx+b_s)\equiv 0\,(\mathrm{mod}\,p)$$

and suppose that $w(p)<p$ for all primes p. Finally let

$$E=\prod_{1\leqslant i\leqslant s}a_i\prod_{1\leqslant i\leqslant s}(a_ib_j-a_jb_i).$$

Then for all $N\geqslant 2$, the number of elements in the set

$$\{x\leqslant N;\ |a_ix+b_i|\ \textit{prime for}\ i=1,\dots,s\}$$

is

$$<c(s)\frac{N}{(\log N)^s}\prod_{p|E}\left(1-\frac{1}{p}\right)^{-(s-w(p))},$$

where $c(s)$ is a constant depending only on s and not on $a_1,\dots,a_s,b_1,\dots,b_s$ or N.

In order to apply this result we replace the set given by the intersection of the two distinct sets $S(m,t)$ and $S(m',t')$ by a more tractable set, and we prove

LEMMA 1. *Let $[m,m']$ be the lowest common multiple of m and m' and let m_0 and m_0' be defined by*

$$mm_0=m'm_0'=[m,m'].$$

Suppose $(m,t)=(m',t')=1$ and suppose the equations

$$m=m',\quad t=t'$$

do not hold simultaneously. Then

$$|S(m,t)\cap S(m',t')|\leqslant|T(m,m';t,t')|$$

where

$$T(m,m';t,t')=\left\{n\leqslant\frac{N}{[m,m']};\ tm_0n+1,\ t'm_0'n+1\ \textit{distinct primes}\right\}.$$

Proof. Let k be a member of the set $S(m,t)\cap S(m',t')$, so that

$$k=\frac{p-1}{t}m=\frac{p'-1}{t'}m',$$

where $(m,p)=(m',p')=1$, p and p' are primes, $(m,t)=(m',t')=1$ and $\frac{p-1}{t}>1$, $\frac{p'-1}{t'}>1$. We note first that p and p' are distinct: for otherwise we would have $mt'=m't$, which, since $(m,t)=(m',t')=1$, implies that $m=m'$ and $t=t'$, contrary to the hypothesis of the lemma.

Now since m and m' both divide k, their lowest common multiple, $[m,m']$, divides k and we can write k as

$$k=[m,m']\cdot n,$$

for some $n\leqslant\frac{N}{[m,m']}$. Hence we can write the prime p in the form

$$p=\frac{tk}{m}+1=tm_0\frac{k}{[m,m']}+1=tm_0n+1$$

and the prime p' in the form

$$p'=\frac{t'k}{m'}+1=t'm_0'\frac{k}{[m,m']}+1=t'm_0'n+1,$$

and it follows that $\frac{k}{[m,m']}$ belongs to the set $T(m,m';t,t')$. Thus each element in the set $S(m,t)\cap S(m',t')$ corresponds to just one element in the set $T(m,m';t,t')$, whence

$$|S(m,t)\cap S(m',t')|\leqslant|T(m,m';t,t')|.$$

Next we obtain an estimate for $|T(m,m';t,t')|$, the number of elements in the set $T(m,m';t,t')$, and hence, in view of the above lemma, for $|S(m,t)\cap S(m',t')|$.

LEMMA 2. *Suppose $1\leqslant m,m'\ll r=[(\log N)^2]$ and $1\leqslant t,t'\leqslant T$, T a fixed positive integer. Suppose also that $(m,t)=(m',t')=1$ and that the equations $m=m'$, $t=t'$ do not hold simultaneously. Then for N sufficiently large*

$$|T(m,m';t,t')|\ll\frac{N(\log\log r)^2}{[m,m'](\log N)^2}.$$

Proof. Let m_0 and m_0' be defined by $mm_0 = m'm_0' = [m, m']$, the lowest common multiple of m and m'. Then $tm_0 \neq t'm_0'$, since otherwise we would have $m't = mt'$, which is excluded. Next it is plain that the congruence

$$(tm_0x+1)(t'm_0'x+1) \equiv 0 \pmod{p}$$

has at most two solutions distinct (mod p) and that when $p = 2$, it has at most one. Lastly, since $r = [(\log N)^2]$, we can choose N large enough to ensure that

$$\frac{N}{[m, m']} \geqslant \frac{N}{r^2} \geqslant 2.$$

Taking $s = 2$, $a_1 = tm_0$, $a_2 = t'm_0'$ and noting that we have $w(p) < p$ for all primes p, we see that providing N is sufficiently large, Theorem 1 can be applied to the set $T(m, m'; t, t')$ and we deduce that

$$|T(m, m'; t, t')| \ll \frac{N}{[m, m']\left(\log \dfrac{N}{[m, m']}\right)^2} \prod_{p|E} \left(1 - \frac{1}{p}\right)^{-(2-w(p))}$$

where $E = tm_0t'm_0'(tm_0 - t'm_0')$.

Now

$$\prod_{p|E} \left(1 - \frac{1}{p}\right)^{-(2-w(p))} \leqslant \prod_{p|E} \left(1 - \frac{1}{p}\right)^{-2} = \left(\frac{E}{\varphi(E)}\right)^2 \ll (\log\log r)^2,$$

since $\varphi(E) \gg E/\log\log E$ ([6], p. 267, Theorem 328) and since $E \leqslant r^3T^3 \ll r^3$. Also, providing N is sufficiently large, we have that

$$\log\left(\frac{N}{[m, m']}\right) \geqslant \log(Nr^{-2}T^{-2}) \gg \log N,$$

and the lemma follows.

Lemma 3. *Suppose* $1 \leqslant m, m' \leqslant r = [(\log N)^2]$ *and* $1 \leqslant t, t' \leqslant T$, *a fixed integer. Suppose further that* $(m, t) = (m', t') = 1$ *and that the equations* $m = m'$, $t = t'$ *are not simultaneously satisfied. Then*

$$\sum_{t,t',m,m'} \sum_{k} 1 \ll \frac{N}{(\log N)^{3/2}},$$

where the inner sum is extended over all $k \in S(m, t) \cap S(m', t')$.

Proof. We have just proved that the inner sum

$$\sum_{k} 1 = |S(m, t) \cap S(m', t')| \leqslant |T(m, m'; t, t')| \ll \frac{N(\log\log r)^2}{[m, m'](\log N)^2}.$$

Also,

$$\sum_{1 \leqslant m, m' \leqslant r} \frac{1}{[m, m']} = \sum_{1 \leqslant m, m' \leqslant r} \frac{(m, m')}{mm'} = \sum_{1 \leqslant m \leqslant r} \frac{1}{m} \sum_{1 \leqslant m' \leqslant r} \frac{(m, m')}{m'}$$
$$= \sum_{1 \leqslant c \leqslant r} \frac{1}{c} \cdot \sum_{1 \leqslant m_1 \leqslant r/c} \frac{1}{m_1} \cdot \sum_{\substack{1 \leqslant m' \leqslant r/c \\ (m_1, m_1') = 1}} \frac{1}{m_1'},$$

where $c = (m, m')$ and $m = cm_1$, $m' = cm_1'$. Hence

$$\sum_{1 \leqslant m, m' \leqslant r} \frac{1}{[m, m']} \ll (\log r)^3$$

and so, combining this estimate with the one obtained for the inner sum, we get that

$$\sum_{t,t',m,m'} \sum_{k} 1 \ll T^2 \frac{N(\log\log r)^2(\log r)^3}{(\log N)^2} \ll \frac{N}{(\log N)^{3/2}},$$

for N sufficiently large, since T is a constant and $r = [(\log N)^2]$.

Lemma 4. *Let S be the union of the finite sets $S_1, \ldots, S_n$ and let f be a real, non-negative function defined on S. Then*

$$(2) \qquad \sum_{1 \leqslant i \leqslant n} \sum_{x \in S_i} f(x) - \sum_{1 \leqslant i < j \leqslant n} \sum_{x \in S_i \cap S_j} f(x) \leqslant \sum_{x \in S} f(x) \leqslant \sum_{1 \leqslant i \leqslant n} \sum_{x \in S_i} f(x).$$

For suppose an element of S, x say, belongs to exactly m of the sets $S_1, \ldots, S_n$. Then $f(x)$ is counted $m - \frac{1}{2}m(m-1) \leqslant 1$ times on the left hand side of (2), while the other inequality is obvious.

We now prove

Theorem 2. *Let k be a positive integer with the representation*

$$k = p^v \frac{p-1}{t} m$$

for each prime p, where p^v exactly divides k, $t = \dfrac{p-1}{(k, p-1)}$ and $(m, p) = 1$. Let $c > 0$, let T be a fixed positive integer and $r = [(\log N)^2]$, where N is sufficiently large positive integer. Let $F(k)$ be an arithmetical function of k defined by

$$(3) \qquad F(k) = \underset{p}{\operatorname{maximum}}\, F(k, p),$$

where the maximum is taken over all primes p and where $F(k, p)$ satisfies the following conditions:

(i) *when* $k = \frac{p-1}{t}m$, $1 \leqslant t \leqslant T$, $p \geqslant 2t+1$, *then*

$$F(k, p) = F\left(k, \frac{kt}{m}+1\right) = F\left(\frac{p-1}{t}m, p\right)$$

satisfies

$$F(k, p) = G(k, m, t) = H(p, m, t) = O(k^c/m),$$

(ii) *when* $k = p^v \frac{p-1}{t} m$, $1 \leqslant t \leqslant T$, $p \geqslant 2t+1$, $v \geqslant 1$, *then* $F(k, p)$ *satisfies*

$$F(k, p) = O(k^c/vm),$$

(iii) *when* $k = p^v m, v \geqslant 0, p = t+1, 1 \leqslant t \leqslant T$, *then* $F(k, p)$ *satisfies*

$$F(k, p) = O(k^c/m),$$

and

(iv) *otherwise* $F(k, p)$ *satisfies*

$$F(k, p) = O(k^{c-b}), \quad b > 0.$$

Then

$$\sum_{k \leqslant N} F(k) = \sum_{\substack{1 \leqslant t \leqslant T \\ 1 \leqslant m \ll r}} \sum_{l|t} \sum_{p \leqslant Nt/lm} \mu(l) H(p, lm, t) + O\left(\frac{N^{c+1}}{(\log N)^{3/2}}\right). \tag{4}$$

Proof. We shall write $S = \bigcup_{m,t} S(m, t)$ where the union is taken over all coprime m and t with $1 \leqslant m \ll r$ and $1 \leqslant t \leqslant T$. Suppose the integer k has no representations of the kinds given by (i), (ii) or (iii). Then we can neglect the contribution of such k to the sum $\sum_{k \leqslant N} F(k)$ with an error of at most $N^{c-b+1} \ll N^{c+1}/r$ for N sufficiently large. Moreover we have that

$$\sum_{k \leqslant N} F(k) = \sum_{\substack{k \leqslant N \\ F(k) > N^c/r}} F(k) + O(N^{c+1}/r).$$

But if $F(k) > N^c/r$, then k must have at least one representation of at least one of the following kinds: (i) or (iii), subject to $1 \leqslant m \ll r$ or (ii) subject to $1 \leqslant vm \ll r$.

Suppose then that $\underset{p}{\text{maximum}}\, F(k, p)$ is attained for a representation of type (ii) with $1 \leqslant vm \ll r$, i.e. for some prime $q \geqslant t+1$, we have

$$k = q^v \frac{q-1}{t} m, \quad (m, t) = (m, q) = 1, \quad v \geqslant 1, \quad 1 \leqslant t \leqslant T, \quad 1 \leqslant vm \ll r$$

and

$$F(k) = F(k, q).$$

Then the contribution of such k to the sum $\sum_{k \leqslant N} F(k)$ is at most

$$\sum_{\substack{k = q^v \frac{q-1}{t} m \leqslant N \\ 1 \leqslant vm \ll r \\ 1 \leqslant t \leqslant T}} F(k) \ll N^c \sum_{\substack{q^{v+1} \leqslant Nt/m \\ 1 \leqslant vm \ll r \\ 1 \leqslant t \leqslant T}} 1 \ll N^c \sum_{\substack{1 \leqslant vm \ll r \\ 1 \leqslant t \leqslant T}} \pi\left(\left\{\frac{Nt}{m}\right\}^{1/(v+1)}\right),$$

where $\pi(x)$ is the number of primes up to x. Thus we get that the contribution is

$$\ll N^c \sum_{\substack{1 \leqslant vm \ll r \\ 1 \leqslant t \leqslant T}} N^{1/2} t^{1/2} \ll N^{c+1/2} T^{3/2} r^2 \ll N^{c+1}/r.$$

Next suppose that maximum $F(k, p)$ is attained by a representation of type (iii) with $1 \leqslant m \ll r$, so that there exists a prime $q = t+1$ such that

$$k = q^v m, \quad v \geqslant 0, \quad q = t+1, \quad (m, t) = (m, q) = 1, \quad 1 \leqslant t \leqslant T$$

and

$$F(k) = F(k, q).$$

Then the contribution of such numbers to the sum $\sum_{k \leqslant N} F(k)$ is at most

$$\sum_{\substack{k = q^v m \leqslant N \\ q-1 \leqslant T \\ q \text{ prime} \\ 1 \leqslant m \ll r}} F(k) \ll N^c \sum_{\substack{v \leqslant \log N \\ 1 \leqslant m \ll r \\ 1 \leqslant t \leqslant T}} 1 \ll N^c \cdot T \cdot r \log N \ll N^{c+1}/r.$$

Thus, with a permissible error, we need only consider those integers k which have a representation of type (i) with $1 \leqslant m \ll r$, and such k comprise, by definition, the set S. Hence we have

$$\begin{aligned} \sum_{k \leqslant N} F(k) &= \sum_{k \epsilon S} F(k) + O(N^{c+1}/r) \\ &= \sum_{\substack{1 \leqslant m \ll r \\ 1 \leqslant t \leqslant T \\ (m,t)=1}} \sum_{k \epsilon S(m,t)} F(k) + O\Big(\sum_{m,m',t,t'} \sum_{k} F(k)\Big) + O(N^{c+1}/r), \end{aligned}$$

by Lemma 4, where the inner sum in the second term is extended over all $k \epsilon S(m, t) \frown S(m', t')$ and where the outer sum is extended over all m, m', t, t' with $1 \leqslant m, m' \ll r, 1 \leqslant t, t' \leqslant T, (m, t) = (m', t') = 1$ and with the equations $m = m', t = t'$ not soluble simultaneously. It follows from Lemma 3 that

$$\sum_{k \leqslant N} F(k) = \sum_{\substack{1 \leqslant m \ll r \\ 1 \leqslant t \leqslant T \\ (m,t)=1}} \sum_{k \epsilon S(m,t)} F(k) + O\left(\frac{N^{c+1}}{(\log N)^{3/2}}\right).$$

Finally, suppose that $k \epsilon S(m, t)$ and that $G(k, m, t) < F(k)$. Then k must have another representation of type (i), with $1 \leqslant m \ll r$, or a representation of type (ii) with $1 \leqslant vm \ll r$, or one of type (iii) with $1 \leqslant m \ll r$. It follows that the error introduced in replacing $F(k)$ by $G(k, m, t)$ when $F(k) > G(k, m, t)$ in the sum $\sum_{k \leqslant N} F(k)$ is at most $O(N^{c+1}/r)$. Hence we have

$$\sum_{k \leqslant N} F(k) = \sum_{\substack{1 \leqslant m \ll r \\ 1 \leqslant t \leqslant T \\ (m,t)=1}} \sum_{k \epsilon S(m,t)} G(k, m, t) + O\left(\frac{N^{c+1}}{(\log N)^{3/2}}\right)$$

$$= \sum_{\substack{1 \leqslant m \ll r \\ 1 \leqslant t \leqslant T \\ (m,t)=1}} \sum_{\substack{p \leqslant \frac{Nt}{m}+1 \\ (m,p)=1}} H(p, m, t) + O\left(\frac{N^{c+1}}{(\log N)^{3/2}}\right),$$

since if $k \epsilon S(m, t)$, we can express k in the form $k = \frac{p-1}{t} m \leqslant N$, for some prime p, where $(m, p) = 1$. Also

$$\sum_{\substack{p \leqslant \frac{Nt}{m}+1 \\ p|m}} H(p, m, t) \leqslant \sum_{p^2 \leqslant 2Nt} H(p, m, t) \ll N^c \cdot N^{1/2} T^{1/2}$$

whence

$$\sum_{k \leqslant N} F(k) = \sum_{\substack{1 \leqslant m \ll r \\ 1 \leqslant t \leqslant T \\ (m,t)=1}} \sum_{p \leqslant \frac{Nt}{m}+1} H(p, m, t) + O(r \cdot T^{3/2} \cdot N^{c+1/2}) + O\left(\frac{N^{c+1}}{(\log N)^{3/2}}\right)$$

$$= \sum_{\substack{1 \leqslant m \ll r \\ 1 \leqslant t \leqslant T \\ (m,t)=1}} \sum_{p \leqslant \frac{Nt}{m}} H(p, m, t) + O\left(\frac{N^{c+1}}{(\log N)^{3/2}}\right)$$

$$= \sum_{1 \leqslant t \leqslant T} \sum_{l|t} \sum_{1 \leqslant m' \ll \frac{r}{l}} \sum_{p \leqslant \frac{Nt}{lm'}} \mu(l) H(p, lm', t) + O\left(\frac{N^{c+1}}{(\log N)^{3/2}}\right),$$

putting $m = lm'$ and where $\mu(l)$ is the Möbius function. Since $l \leqslant T \ll 1$, on omitting the dashes, we have

$$\sum_{k \leqslant N} F(k) = \sum_{1 \leqslant t \leqslant T} \sum_{l|t} \sum_{1 \leqslant m \ll r} \sum_{p \leqslant \frac{Nt}{lm}} \mu(l) H(p, lm, t) + O\left(\frac{N^{c+1}}{(\log N)^{3/2}}\right),$$

which gives the required result.

Now we make two applications of this result and obtain the average order of the two arithmetical functions $\Gamma^*(k)$ and $\Gamma(k)$.

THE AVERAGE ORDER OF $\Gamma^*(k)$. The number $\Gamma^*(k)$ is defined as the least positive integer s with the following property: for any non-zero integers $a_1, \ldots, a_s$, the congruence

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

has a solution, with not all the variables $x_1, \ldots, x_s$ divisible by p, for every prime power p^n. Such solutions will be called *primitive*.

The number $\Gamma^*(k)$ was introduced by Davenport and Lewis in their investigation of homogeneous additive equations [3]. Their main object was to show that $\Gamma^*(k) \leqslant k^2+1$ and that there is equality here whenever $k+1$ is prime. When k is odd, $\Gamma^*(k)$ can be estimated quite effectively and Chowla and Shimura have proved ([2], Theorem A) that

$$\Gamma^*(k) < \left(\frac{2}{\log 2} + \varepsilon\right) k \log k \quad \text{for all odd } k > k_0(\varepsilon),$$

where ε is any positive number and they also proved that

$$\Gamma^*(k) > \frac{k \log k}{\log 2} \quad \text{for infinitely many odd } k.$$

K. Norton ([8], Theorem 6.70) has improved the upper estimate for $\Gamma^*(k)$ for odd $k \geqslant 3$ to

$$\Gamma^*(k) < \frac{k}{2\log 2}(3\log k + 5\log\log k + 6),$$

so that for all $k > k_0(\varepsilon)$,

$$\Gamma^*(k) < \left(\frac{3}{2\log 2} + \varepsilon\right) k \log k.$$

The number $\Gamma^*(k)$ can be determined exactly for another class of integers ([4], p. 201, Theorem 5.2.2) but otherwise, except for a few small values of k, little is known.

Let us define the function $\Gamma^*(k, p)$ to be the least integer s with the following property: for any non-zero integers $a_1, \ldots, a_s$ and every positive integer n, the congruence (5) has a primitive solution for the particular prime p. It follows that

$$(6) \qquad \Gamma^*(k) = \operatorname*{maximum}_{p} \Gamma^*(k, p).$$

Now it has been shown ([4], p. 183, Lemma 4.2.2) that if $p-1$ divides k and p does not divide k, then

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

where $k=(p-1)m$, $(m,p)=1$. Further, if $p-1$ divides k and p^v exactly divides k, $v\geqslant 1$, then ([4], p. 197, Lemma 4.6.1)

$$\Gamma^*(k,p)\leqslant\begin{cases}\dfrac{k(p^{v+1}-1)}{v+1}+1 & \text{when} \quad p \text{ is odd},\\[2ex] \dfrac{k(p^{v+2}-1)}{v+2}+1 & \text{when} \quad p=2.\end{cases}$$

Since

$$p^{v+1}-1\leqslant 2p^v(p-1) = 2k/m \quad \text{when} \quad p>2$$

and

$$2^{v+2}-1\leqslant 2^{v+2} = 4k/m \quad \text{when} \quad p=2,$$

it follows that in this case

$$\Gamma^*(k,p) = O(k^2/vm).$$

Also, if for some prime $p>2$, $p-1$ does not divide k, then a straightforward modification of Lemma 4.4.2 ([4], p. 189) gives

$$\Gamma^*(k,p)\ll(\log k)^2k^{15/8}\ll k^{2-1/9}.$$

Thus we see that the conditions of Theorem 2 are fulfilled with $T=1$, $c=2$, $b=\frac{1}{9}$ and with

$$G(k,m,l) = \frac{k^2}{m}+1$$

and

$$H(p,m,l) = m(p-1)^2+1.$$

Hence we have

$$\sum_{k\leqslant N}\Gamma^*(k) = \sum_{1\leqslant m\leqslant r}\;\sum_{p\leqslant N/m} mp^2+O\left(\frac{N^3}{(\log N)^{3/2}}\right),$$

since it is plain that we can replace the term $m(p-1)^2+1$ by mp^2 in the sum on the right hand side, with a permissible error.

Now

$$\sum_{p\leqslant N/m}p^2 = \frac{(N/m)^3}{3\log(N/m)}+O\left(\frac{(N/m)^3}{(\log(N/m))^2}\right)$$

and

$$\sum_{1\leqslant m\leqslant r}\frac{1}{m^2\log(N/m)} = \frac{1}{\log N}\sum_{1\leqslant m\leqslant r}\frac{1}{m^2}\left(1+O\left(\frac{\log m}{\log N}\right)\right)$$

$$= \frac{1}{\log N}\left\{\sum_{m=1}^{\infty}\frac{1}{m^2}+O\left(\frac{1}{r}\right)\right\}+O\left(\frac{\log r}{(\log N)^2}\right)$$

$$= \frac{\zeta(2)}{\log N}+O\left(\frac{1}{(\log N)^{3/2}}\right).$$

Hence

$$\sum_{1\leqslant m\leqslant r}\;\sum_{p\leqslant N/m}mp^2 = \frac{\zeta(2)N^3}{3\log N}+O\left(\frac{N^3}{(\log N)^{3/2}}\right).$$

Thus, since $\zeta(2) = \pi^2/6$ and since

$$\sum_{k\leqslant N}\frac{k^2}{\log k}\sim\frac{N^3}{3\log N},$$

we have proved

THEOREM 3. *The average order of $\Gamma^*(k)$ is $\pi^2k^2/6\log k$, or more precisely,*

$$\sum_{k\leqslant N}\Gamma^*(k) = \frac{\pi^2N^3}{18\log N}+O\left(\frac{N^3}{(\log N)^{3/2}}\right).$$

THE AVERAGE ORDER OF $\Gamma(k)$. The number $\Gamma(k)$ is defined to be the least value of s for which the congruence

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

where N is any integer, has a primitive solution for every prime power p^n.

As in the preceding discussion, we introduce the function $\Gamma(k,p)$, which is defined to be the least s for which the congruence (7) has a primitive solution for every integer N and every positive integer n, for the particular prime p. Plainly

$$\Gamma(k) = \operatorname*{maximum}_{p}\Gamma(k,p).$$

The functions $\Gamma(k)$ and $\Gamma(k,p)$ were introduced by Hardy and Littlewood in [5], though in a different way and with a different notation for $\Gamma(k,p)$, namely γ_p. They showed that for all k, $\Gamma(k)\leqslant 4k$ ([5], p. 186, Theorem 12). They continued their investigation of $\Gamma(k)$ and $\Gamma(k,p)$

in more detail in [6] and proved there (p. 533, Theorem 4) that $\Gamma(k) \leqslant k$ unless k belongs to certain special classes, and evaluated $\Gamma(k)$ for many values of k. Nevertheless, the behaviour of $\Gamma(k)$ for large k is still to a considerable extent unknown. In the course of their work, they determined $\Gamma(k, p)$ when $p-1$ or $\frac{1}{2}(p-1)$ divides k ([6], p. 524, Lemma 7), and they showed that if

(i) $p = 2, v = 0$, i.e. k is odd, then

$$\Gamma(k, 2) = 2;$$

(ii) $p = 2, v > 0$, i.e. $k = 2^v m, m$ odd, then

$$\Gamma(k, 2) = 2^{v+2} = \frac{4k}{m};$$

(iii) $p > 2$, $d = p-1$, i.e. $k = p^v(p-1)m$, $(m, p) = 1$, then

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

(iv) $p > 2$, $d = \frac{1}{2}(p-1)$, i.e. $k = p^v\cdot\frac{1}{2}(p-1)m$, $(m, p) = 1$, then

$$\Gamma(k, p) = \tfrac{1}{2}(p^{v+1}-1) = \frac{1-(1/p^{v+1})}{1-(1/p)}\cdot\frac{k}{m};$$

except in the case $p = 3$, $v = 0$, when $\Gamma(k, 3) = 2$.

On the other hand, if $d = (k, p-1) < \frac{1}{2}(p-1)$, i.e. if $\frac{1}{2}(p-1)$ does not divide k, then I. Chowla has shown ([1], p. 197, Theorem 4) that for k sufficiently large,

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

where $\varepsilon > 0$ and $a = (103-3\sqrt{641})/220 > 1/9$.

We see that the hypotheses of Theorem 2 are satisfied with $T = 2$, $c = 1$, $b = \frac{1}{9}$ and with

$$G(k, m, t) = \frac{k}{m} + 2 - t$$

and

$$H(p, m, t) = \frac{p-t+1}{t}.$$

Hence we have

$$\sum_{k\leqslant N}\Gamma(k) = \sum_{t=1}^{2}\sum_{l|t}\sum_{1\leqslant m\leqslant r}\sum_{p\leqslant Nt/ml}\mu(l)\frac{p}{t} + O\left(\frac{N^2}{(\log N)^{3/2}}\right),$$

since it is plain that we can replace $H(p, m, t)$ by p/t in this sum with a permissible error.

Now

$$\sum_{p\leqslant Nt/ml} p = \frac{N^2t^2}{2(ml)^2\log(Nt/ml)} + O\left(\frac{N^2}{m^2(\log N)^2}\right),$$

and

$$\sum_{1\leqslant m\leqslant r}\frac{1}{m^2\log(Nt/m)} = \frac{1}{\log N}\sum_{1\leqslant m\leqslant r}\frac{1}{m^2}\left[1+O\left(\frac{\log m}{\log N}\right)\right]$$

$$= \frac{1}{\log N}\left[\zeta(2)+O\left(\frac{1}{r}\right)\right] + O\left(\frac{1}{(\log N)^2}\right) = \frac{\pi^2}{6\log N} + O\left(\frac{1}{(\log N)^2}\right).$$

It follows that

$$\sum_{k\leqslant N}\Gamma(k) = \sum_{t=1}^{2}\sum_{l|t}\mu(l)\frac{\pi^2N^2t}{12l^2\log N} + O\left(\frac{N^2}{(\log N)^{3/2}}\right)$$

$$= \frac{\pi^2N^2}{12\log N} + \frac{\pi^2N^2 2}{12\log N} - \frac{\pi^2N^2 2}{48\log N} + O\left(\frac{N^2}{(\log N)^{3/2}}\right)$$

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

Since

$$\sum_{k\leqslant N}\frac{k}{\log k} \sim \frac{N^2}{2\log N},$$

we have proved

THEOREM 4. *The average order of $\Gamma(k)$ is*

$$\frac{5\pi^2 k}{12\log k}.$$

More precisely,

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

References

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

[2] S. Chowla and G. Shimura, *On the representation of zero by a linear combination of k-th powers*, Norske Vid. Selsk. Forh., Trondheim, 36 (37) (1963), pp. 169–176.

[3] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc., A, 274 (1963), pp. 443–460.

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

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

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

[7] — and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press 1960.

[8] K. Norton, *On homogeneous congruences of odd degree*, Ph. D. Thesis, University of Illinois, Urbana, Illinois.

[9] K. Prachar, *Primzahlverteilung*, Berlin 1957.

UNIVERSITY OF AUCKLAND
Auckland, New Zealand
UNIVERSITY OF YORK
York, England

Reçu par la Rédaction le 5. 10. 1968

ACTA ARITHMETICA
XVI (1969)

A note on the least prime quadratic residue (mod$p$)

by

D. Wolke (Marburg/Lahn)

Let p be an odd prime. By $r_2(p)$ we denote the least prime quadratic residue (mod$p$) and by $L(s,\chi)$ the L-function formed with the real character $\left(\frac{n}{p}\right)$.

Elliott [2] recently showed: If for an integer $k \geqslant 0$ and a real $c_1 > 0$

$$L(1,\chi) > \frac{c(\log\log p)^k}{\log p}$$

then we have, for every $\varepsilon > 0$,

$$r_2(p) \leqslant c(\varepsilon)p^{\frac{1}{4}(1+\varepsilon)(k+2)^{-1}}.$$

In this note we will sharpen Elliott's result to

Theorem. *Let $t(p)$ be a positive function with*

$$L(1,\chi) > \frac{t(p)}{\log p}. \tag{H}$$

Then, for absolute $c_2, c_3 > 0$

$$r_2(p) \leqslant c_2 p^{c_3(t(p))^{-1/2}} \tag{1}$$

holds.

For the proof we need two lemmas.

Lemma 1. *For every $\varepsilon > 0$, $p \geqslant p_0(\varepsilon)$ and $x = p^{\frac{1}{4}+\varepsilon}$ we have the inequality*

$$\sum_{n<x}\left(1-\frac{n}{x}\right)\sum_{d|n}\mu^2(d)\left(\frac{d}{p}\right) > \frac{x}{6}L(1,\chi). \tag{2}$$

For the proof see Elliott [2], (2). The proof rests upon Burgess' estimation for character sums [1], Siegel's theorem (s. [4], IV, § 8) and a method of Linnik–Vinogradov [3].