ACTA ARITHMETICA
LXXXI.2 (1997)

On the arithmetic structure of the integers whose sum of digits is fixed

by

Christian Mauduit (Marseille) and
András Sárközy (Budapest)

1. Throughout this paper we use the following notations: We write $e(\alpha) = e^{2\pi i\alpha}$. We denote by $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{N}$ the sets of real numbers, integers, and positive integers. We write $l_1 = \log N$, $l_2 = \log\log N$, $l_3 = \log\log\log N$. If $F(N) = O(G(N))$, then we write $F(N) \ll G(N)$; if the implied constant depends on certain parameters $\alpha, \beta, \ldots$ (but on no other parameters), then we write $F(N) = O_{\alpha,\beta,\ldots}(G(N))$ and $F(N) \ll_{\alpha,\beta,\ldots} G(N)$. We denote by $\omega(n)$ the number of distinct prime factors of n and by $\Omega(n)$ the number of prime factors of n counted with multiplicity.

Let $g \in \mathbb{N}$ be fixed with

$$g \geq 2. \tag{1.1}$$

If $n \in \mathbb{N}$, then representing n in the number system to base g:

$$n = \sum_{j=0}^{\mu} a_j g^j, \qquad 0 \leq a_j \leq g-1,\ a_\mu \geq 1,$$

we write

$$S(n) = \sum_{j=0}^{\mu} a_j.$$

The sum of digits function S has been studied by several authors in different contexts (see [Mau] for a bibliography).

This function can be considered like a base g analogue of the usual "number of prime factors" function. Its main property is the following

1991 *Mathematics Subject Classification*: Primary 11A63.

Research of the second author was partially supported by Hungarian National Foundation for Scientific Research, Grant No. 1901 and CEE fund No. CIPA-CT92-4022. This paper was written when the second author was visiting the Laboratoire de Mathématiques Discrètes (UPR 9016 CNRS), Marseille.

"g-additive" property: for any integers k, a, b such that $b < g^k$,

$$S(g^k a + b) = S(a) + S(b).$$

The study of "g-additive" sequences will lead us to introduce complex polynomials as generating functions.

For $N \in \mathbb{N}$, $m \in \mathbb{N}$ and $r \in \mathbb{Z}$ we write $U_{(m,r)}(N) = \{n : n \le N, S(n) \equiv r \pmod m\}$.

The arithmetic structure of the sets $U_{m,r}(N)$ has been studied by Gelfond [Gel]. His main result which extends an earlier result of Fine [Fin] is the following: if $m \in \mathbb{N}$ is fixed with

$$(m, g-1) = 1, \tag{1.2}$$

then for all $r \in \mathbb{Z}$, the set $U_{(m,r)}(N)$ is well-distributed in the residue classes modulo q. More exactly, if $g \in \mathbb{N}$, $m \in \mathbb{N}$, $q \in \mathbb{N}$ are fixed with (1.1), (1.2), $m > 1$ and $q > 1$, and $r \in \mathbb{Z}$, $l \in \mathbb{Z}$, then for $N \to \infty$ we have

$$|\{n : n \in U_{(m,r)}(N),\ n \equiv l \pmod q\}| = \frac{N}{mq} + O(N^\lambda) \tag{1.3}$$

where $\lambda = \lambda(g, m) < 1$ (and λ is independent of N, q, r, l). As an application of this result, he showed that if $g \in \mathbb{N}$, $m \in \mathbb{N}$, $z \in \mathbb{N}$ are fixed with (1.1), (1.2), and $z > 1$, and $r \in \mathbb{Z}$, then for $N \to \infty$ we have

$$\begin{aligned}|\{n : n \in U_{(m,r)}(N),\ \text{there is no prime } p \text{ with } p^z \mid n\}| \\ = \frac{N}{m\zeta(z)} + O(N^{\lambda_1})\end{aligned} \tag{1.4}$$

where $\lambda_1 = (1 + (z-1)\lambda)/z$ with the number λ defined above. Moreover, he studied another application of similar type.

In [M-S] we continued the study of the arithmetic structure of the sets $U_{(m,r)}(N)$. First we showed that if $g \in \mathbb{N}$, $m \in \mathbb{N}$ are fixed with (1.1) and (1.2), and $r \in \mathbb{Z}$, $N \in \mathbb{N}$, $\mathcal{A}, \mathcal{B} \subset \{1, \ldots, N\}$, then

$$\begin{aligned}\left| |\{(a,b) : a \in \mathcal{A},\ b \in \mathcal{B},\ S(a+b) \equiv r \pmod m\}| - \frac{|\mathcal{A}| \cdot |\mathcal{B}|}{m} \right| \\ \le \gamma N^\lambda (|\mathcal{A}| \cdot |\mathcal{B}|)^{1/2}\end{aligned} \tag{1.5}$$

with $\gamma = \gamma(g, m)$, $\lambda = \lambda(g, m) < 1$. Next we showed that the elements of $U_{(m,r)}(N)$ satisfy an Erdős–Kac type theorem: if g, m, r are defined as above, then

$$\begin{aligned}\Bigg| \frac{1}{|U_{(m,r)}(N)|} |\{n : n \in U_{(m,r)}(N),\ \omega(n) - l_2 \le x l_2^{1/2}\}| \\ - (2\pi)^{-1/2} \int_{-\infty}^{x} e^{-u^2/2}\, du \Bigg| < c l_3 l_2^{-1/2}\end{aligned} \tag{1.6}$$

with some constant $c = c(g,m)$, uniformly in all real x and $N \in \mathbb{N}$, $N \geq 3$. Finally, we showed that defining g, m, r as above and writing

$$\Omega(g,n) = \sum_{\substack{p^\alpha \| n \\ (p,g)=1}} \alpha,$$

for $\varepsilon > 0$, $N > N_0(\varepsilon)$ we have

$$\max_{n \in U_{(m,r)}(N)} \omega(n) > \left(\frac{1}{2} - \varepsilon\right) \frac{\log N}{\log\log N} \tag{1.7}$$

and for $N > N_0(g,m)$ we have

$$\max_{n \in U_{(m,r)}(N)} \Omega(g,n) > c \log N \tag{1.8}$$

with $c = c(g,m) > 0$. (See [F-M1] and [F-M2] for a further related result.)

2. All the results above cover the set $U_{(m,r)}(N)$ whose cardinality is $(1 + o(1))(N/m)$ so that, roughly speaking, it is a set of positive density (recall that m is fixed). Since the integers characterized by a simple digit property have a very specific structure and they can be studied very effectively by the generating function principle, one expects that it can be proved that much "thinner" sets of this type still have a nice arithmetic structure. The most natural way to construct "thin" sets of this type is to consider the sets

$$V_k = V_k(N) = \{n : n \leq N,\ S(n) = k\}$$

where $k \in \mathbb{N}$, $0 \leq k \leq (g-1)\left(\frac{\log N}{\log g} + 1\right)$. Indeed, it could be deduced easily from Theorem 1 below that for every k we have

$$|V_k(N)| \ll_g N(\log N)^{-1/2},$$

and $|V_k(N)| \to \infty$ arbitrary slowly if $k \to \infty$ sufficiently slowly so that these sets are much thinner than the sets $U_{(m,r)}(N)$. In this paper our goal is to show that, in spite of the much smaller cardinality, the sets $V_k(N)$ possess the same "nice" arithmetic structure as the sets $U_{(m,r)}(N)$; in particular, $k \to \infty$ is sufficient to ensure that $V_k(N)$ is well-distributed in the residue classes of small moduli, moreover, we will show that if k is close to its mean value $\frac{g-1}{2} \cdot \frac{\log N}{\log g}$, then $V_k(N)$ satisfies an Erdős–Kac type theorem.

First we will need a lower bound, uniform in k, for $|V_k(N)|$ (Corollary 1 below). For our purpose, it will be sufficient to consider the somewhat simpler case when N is of the form $g^\nu - 1$. In other words, for $N \in \mathbb{N}$ define $\nu = \nu(N)$ by

$$g^\nu - 1 \leq N < g^{\nu+1} - 1 \tag{2.1}$$

and write

$$M = M(N) = g^{\nu} - 1. \tag{2.2}$$

For $0 < k < (g-1)\nu$, clearly $n \in V_k(M)$ holds if and only if $M - n \in V_{(g-1)\nu-k}(M)$ so that

$$|V_k(M)| = |V_{(g-1)\nu-k}(M)|. \tag{2.3}$$

Thus we may assume that k does not exceed the mean value of $S(n)$ (for $1 \le n \le N$):

$$k \le \frac{g-1}{2}\nu. \tag{2.4}$$

To estimate $|V_k(M)|$, we will use a variant of the saddle point method (see, e.g., [Ten]). First we have to introduce a parameter $r = r(N,k)$. Consider the generating function

$$P(x) = x^{-k}(1 + x + \ldots + x^{g-1})^{\nu} \qquad (x \in \mathbb{R}, x > 0)$$

whose constant term is, clearly, $|V_k(g^{\nu} - 1)| = |V_k(M)|$. To minimize the contribution of the other terms, we have to solve the equation

$$\begin{aligned} P'(x) &= x^{-k-1}(1 + x + \ldots + x^{g-1})^{\nu-1} \\ &\quad \times (-k(1 + x + \ldots + x^{g-1}) + \nu x(1 + 2x + \ldots + (g-1)x^{g-2})) = 0. \end{aligned}$$

For $x > 0$, this equation can be written in the equivalent form

$$\begin{aligned} Q(x) &= -k(1 + x + \ldots + x^{g-1}) + \nu x(1 + 2x + \ldots + (g-1)x^{g-2}) \\ &= (\nu(g-1) - k)x^{g-1} + (\nu(g-2) - k)x^{g-2} + \ldots + (\nu - k)x - k \\ &= 0. \end{aligned} \tag{2.5}$$

Then $Q(0) = -k < 0$ and, by (2.1),

$$Q(1) = \nu\frac{(g-1)g}{2} - gk = g\left(\frac{g-1}{2}\nu - k\right)\begin{cases} = 0 & \text{for } k = \frac{g-1}{2}\nu, \\ > 0 & \text{for } k < \frac{g-1}{2}\nu. \end{cases} \tag{2.6}$$

Thus $Q(x)$ has at least one zero in the interval $(0,1]$. On the other hand, the sequence $\nu(g-1) - k$, $\nu(g-2) - k$, $\ldots$, $\nu - k$, $-k$ of the coefficients of $Q(x)$ has exactly one change of sign, thus by Descartes' rule of signs (see, e.g., [P-S], Vol. II, p. 41, Problem 36), $Q(x)$ has at most one positive zero. It follows that $Q(x)$ has exactly one zero in $(0,1]$. Denote this unique zero by $r = r(N,k)$ so that

$$r = 1 \text{ for } k = \frac{g-1}{2}\nu \quad \text{and} \quad 0 < r < 1 \text{ for } 0 < k < \frac{g-1}{2}\nu \tag{2.7}$$

and, by (2.5),

$$Q(r) = -k(1 + r + \ldots + r^{g-1}) + \nu r(1 + 2r + \ldots + (g-1)r^{g-2}) = 0 \tag{2.8}$$

whence

$$\frac{r+2r^2+\ldots+(g-1)r^{g-1}}{1+r+\ldots+r^{g-1}}=\frac{k}{\nu}. \tag{2.9}$$

Moreover, it follows easily from (2.8) that

$$r=\frac{k}{\nu-k}\quad \text{for } g=2$$

and

$$r=\frac{k}{\nu}-\left(\frac{k}{\nu}\right)^2+O\left(\left(\frac{k}{\nu}\right)^3\right)\qquad \text{for } g\ge 3,\ k=o(\nu), \tag{2.10}$$

while for $\Delta=\frac{g-1}{2}\nu-k=o(\nu)$, by (2.6) and

$$Q'(1)=-k\sum_{j=1}^{g-1}j+\nu\sum_{j=1}^{g-1}j^2=\frac{(g-1)g(\nu(2g-1)-3k)}{6}\qquad(\gg\nu),$$

we have

$$\begin{aligned} r&=1-\frac{Q(1)}{Q'(1)}+O_g\left(\left(\frac{Q(1)}{Q'(1)}\right)^2\right)\\ &=1-\Delta\left(\frac{(g-1)(\nu(2g-1)-3k)}{6}\right)^{-1}\\ &=1-\frac{12\Delta}{(g^2-1)\nu}+O_g(\Delta^2\nu^{-2}) \end{aligned} \tag{2.11}$$

for $\Delta=\frac{g-1}{2}\nu-k=o(\nu)$.

We will prove the following result:

Theorem 1. *Uniformly for $k\to\infty$, $k\le\frac{g-1}{2}\nu$ we have*

$$|V_k(M)|=r^{-k}(1+r+\ldots+r^{g-1})^{\nu}\pi^{1/2}(D\nu)^{-1/2}(1+O_g(D\nu)^{-1/2}) \tag{2.12}$$

where

$$D=2\pi^2(B-A^2) \tag{2.13}$$

with

$$A=\Big(\sum_{j=1}^{g-1}jr^j\Big)\Big(\sum_{j=0}^{g-1}r^j\Big)^{-1}=\frac{k}{\nu}\quad\textit{and}\quad B=\Big(\sum_{j=1}^{g-1}j^2r^j\Big)\Big(\sum_{j=0}^{g-1}r^j\Big)^{-1}.$$

Note that a simple computation gives

$$D=2\pi^2\frac{(r^{2g}-g^2r^{g+1}+2(g^2-1)r^g-g^2r^{g-1}+1)r}{(r-1)^2(r^g-1)^2}$$

however, in order to estimate D, it is better to use the definitions of A and B. Indeed, by $0 < r < 1$ and Cauchy's inequality we have

$$\begin{aligned}(2.14)\quad D &= 2\pi^2(B - A^2)\\ &= 2\pi^2\Big(\sum_{j=0}^{g-1} r^j\Big)^{-2}\Big(\sum_{j=1}^{g-1} j^2r^j \sum_{j=0}^{g-1} r^j - \Big(\sum_{j=1}^{g-1} jr^j\Big)^2\Big)\\ &= 2\pi^2\Big(\sum_{j=0}^{g-1} r^j\Big)^{-2}\Big(\sum_{j=1}^{g-1} j^2r^j + \Big(\sum_{j=1}^{g-1} j^2r^j \sum_{j=1}^{g-1} r^j - \Big(\sum_{j=1}^{g-1} jr^j\Big)^2\Big)\Big)\\ &\geq 2\pi^2 g^{-2} r\end{aligned}$$

and

$$(2.15)\qquad D \leq 2\pi^2 B < 2\pi^2 g^2 r.$$

By (2.7), (2.9) and (2.10) there are positive constants $c_1 = c_1(g)$ and $c_2 = c_2(g)$ such that uniformly for $k \to \infty$ we have

$$(2.16)\qquad c_1 \frac{k}{\nu} < r < c_2 \frac{k}{\nu}.$$

By (2.14)–(2.16), there are positive constants $c_3 = c_3(g)$ and $c_4 = c_4(g)$ such that the product $D\nu$ appearing in (2.11) satisfies

$$(2.17)\qquad c_3 k < D\nu < c_4 k.$$

Moreover, for fixed k, $|V_k(N)|$ is clearly an increasing function of N. Thus, using also (2.3), we obtain the following result which will play an important role later in the proof of Theorem 2:

Corollary 1. *There is a positive constant* $c_5 = c_5(g)$ *such that, writing*

$$(2.18)\qquad l = \min(k, (g-1)\nu - k),$$

uniformly for $l \to \infty$ *we have*

$$|V_k(N)| \geq |V_k(M)| = |V_l(M)| > c_5 r^{-l}(1 + r + \ldots + r^{g-1})^\nu l^{-1/2}.$$

In the important special case when k is near the mean value of $S(n)$, we will deduce from Theorem 1 that

Corollary 2. *For* $N \to \infty$ *and*

$$(2.19)\qquad \Delta = \frac{g-1}{2}\nu - k = o(\nu),$$

we have

$$\begin{aligned}(2.20)\quad |V_k(M)| &= 6^{1/2}\pi^{-1/2}(g^2-1)^{-1/2} M \nu^{-1/2}\\ &\quad\times \exp\Big(-\frac{6}{g^2-1}\cdot\frac{\Delta^2}{\nu} + O_g(\Delta^3\nu^{-2} + \nu^{-1/2})\Big).\end{aligned}$$

In the other extreme case when k is far from the mean value, it follows from Theorem 1 that

Corollary 3. *Defining* l *by* (2.18), *for* $g \ge 3$, $l \to \infty$, $l = o(\nu)$ *we have*

$$\begin{aligned} (2.21)\qquad |V_k(M)| &= |V_l(M)| \\ &= 2^{-1/2}\pi^{-1/2}\exp\biggl(-l\log\frac{l}{\nu}+l-\frac{1}{2}\log l-\frac{1}{2}\cdot\frac{l}{\nu} \\ &\qquad +\frac{l^2}{2\nu}+O(l^3\nu^{-2}+l^{-1/2})\biggr). \end{aligned}$$

Note that for $l = o(\nu^{1/2})$ this is $(1+o(1))\binom{\nu}{l}$ as expected. It could be shown that for $l \gg \nu^{1/2}$ it is not so anymore.

Next we will show that if

$$(2.22)\qquad 0 < k < (g-1)\nu, \qquad l = \min(k, (g-1)\nu - k) \to \infty$$

and

$$(2.23)\qquad m < \exp(c_6 l^{1/2}),$$

then V_k is well-distributed in the modulo m residue classes:

Theorem 2. *There exist positive constants* l_0, c_7, c_8 (*all depending on* g *only*) *such that if* n, k, $m \in \mathbb{N}$, $m \ge 2$, $((g-1)g, m) = 1$, $h \in \mathbb{Z}$,

$$(2.24)\qquad l > l_0$$

and (2.23) *holds*, *then*

$$\begin{aligned} (2.25)\qquad &\biggl|\,|\{n : n \in V_k(N),\ n \equiv h \pmod m\}| - \frac{1}{m}|V_k(N)|\biggr| \\ &\qquad < c_7\frac{1}{m}|V_k(N)|\exp\biggl(-c_8\frac{l}{\log m}\biggr). \end{aligned}$$

Note that a condition of type $((g-1)g, m) = 1$ is necessary. Indeed, it is easy to see that if, say, $m = p$ is a prime number with $p \mid (g-1)g$, and $l \to \infty$ sufficiently slowly, then $V_k(N)$ is not well-distributed in the modulo p residue classes.

One may apply Theorem 2 to prove the V_k analogue of Gelfond's result (1.4):

Theorem 3. *If* $g, z \in \mathbb{N}$, $g, z \ge 2$, *then there are constants* N_0, c_9, c_{10} (*each depending on* g *and* z *only*) *such that if* $N, k \in \mathbb{N}$, $N > N_0$,

$$\left|\frac{g-1}{2}\nu - k\right| < c_9(\log N)^{3/4},$$

then the number of those integers n with $n \in V_k(N)$ which are not divisible by the zth power of a prime p with $((g-1)g, p) = 1$ is

$$\Big(\zeta(z) \prod_{p \mid (g-1)g} \Big(1 - \frac{1}{p^z}\Big)\Big)^{-1} |V_k(N)|(1 + O(\exp(-c_{10}(\log N)^{1/2}))).$$

(Here $|V_k(N)|$ can be estimated by using Corollary 2.) Indeed, by using also Corollary 2, Theorem 3 can be derived from Theorem 2 in the same way as (1.4) from (1.3), thus we will not give the details here.

Next, one would like to prove the V_k analogue of our result (1.5). Unfortunately, we have not been able to prove such a theorem (Theorem 2 is not strong enough for this purpose). Thus, in particular, we have not been able to prove the following conjecture:

Conjecture 1. *If $\varepsilon > 0$, $N > N_0(\varepsilon)$, $\mathcal{A}, \mathcal{B} \subset \{1, \ldots, N\}$ and $|\mathcal{A}|, |\mathcal{B}| > \varepsilon N$, then there are integers a, b such that $a \in \mathcal{A}$, $b \in \mathcal{B}$ and*

$$S(a+b) = [(g-1)\nu/2].$$

The V_k analogue of (1.6) provides the most interesting problem. Indeed, we will prove the following theorem:

Theorem 4. *For every positive number K there are effectively computable constants $\nu_0 = \nu_0(g, K)$ and $c_{11} = c_{11}(g, K)$ with the following properties*: *Let*

$$\nu \in \mathbb{N}, \quad \nu > \nu_0, \quad \nu > 2, \tag{2.26}$$

$$N = g^\nu - 1 \quad (= M(N)), \tag{2.27}$$

$k \in \mathbb{N}$ and, *writing $\Delta = \frac{g-1}{2}\nu - k$*,

$$|\Delta| < K(\log N)^{1/2}. \tag{2.28}$$

Let $F_N(z)$ denote the frequency of those elements n of $V_k(N)$, amongst all the elements of $V_k(N)$, for which $\omega(n) - \log\log N \le z\sqrt{\log\log N}$. Then

$$\Big|F_N(z) - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-u^2/2}\,du\Big| < c_{11}\frac{\log\log\log N}{\sqrt{\log\log N}} \tag{2.29}$$

uniformly in all real z (*and ν, k satisfying* (2.26) *and* (2.28)).

Besides Theorem 2, this is our other main result. Namely, the proof is much more difficult than the proof of (1.6) and, in particular, a non-trivial application of the large sieve will be needed.

Note that the result could be extended easily to general integers N instead of considering integers N of the special form (2.27); however, although the same argument goes through this extension would make the formulas involved much more complicated and thus we decided to restrict ourselves to the simpler special case (2.27).

Note, moreover, that the upper bound on the right hand side of (2.28) could be replaced by a slightly greater one, but to replace it by, say, $(\log N)^{1-\varepsilon}$ further ideas would be needed.

Finally, looking for the V_k analogue of (1.7), we can prove the following slightly weaker result:

THEOREM 5. *There are positive constants N_0, c_{12}, c_{13} such that if N, $k \in \mathbb{N}$, $N > N_0$ and $\left|k - \frac{g-1}{2}\nu\right| < c_{12}\nu$, then*

$$\max_{n\in V_k(N)} \omega(n) > c_{13}\frac{\log N}{\log\log N}.$$

Indeed, this can be proved by the same method as the one used in the proof of (1.7), except that while the proof of (1.7) used an argument from [Er-P-S-S], here we have to replace this argument by the one used in the proof of Theorem 1 in [S-S].

On the other hand, we have not been able to give any reasonable lower bound for $\max_{n\in V_k(N)} \Omega(g,n)$ so that, for example, we have not been able to settle the following conjecture:

CONJECTURE 2. *For $N \in \mathbb{N}$, $N > N_0$ there is an integer n such that $1 \le n \le N$, $S(n) = [(g-1)\nu/2]$ and*

$$\Omega(g,n) > c_{14}\log N$$

with some positive constant $c_{14} = c_{14}(g)$.

3. Proof of Theorem 1. As we saw in Section 2, $|V_k(M)|$ is the coefficient of z^k in the generating function

$$f(z) = (\varphi(z))^\nu \quad (z \in \mathbb{C})$$

where

$$\varphi(z) = 1 + z + \ldots + z^{g-1}.$$

Thus we have

$$|V_k(M)| = r^{-k}\int_0^1 f(re(\alpha))e(-k\alpha)\,d\alpha = r^{-k}(1 + r + \ldots + r^{g-1})^\nu J \tag{3.1}$$

where $r = r(M)$ is defined in Section 2 and

$$J = \int_0^1 (U(\alpha))^\nu e(-k\alpha)\,d\alpha = \int_{|\alpha|\le\delta} + \int_{\delta<|\alpha|\le 1/2} = J_1 + J_2 \tag{3.2}$$

with

$$U(\alpha) = \frac{1 + re(\alpha) + \ldots + r^{g-1}e((g-1)\alpha)}{1 + r + \ldots + r^{g-1}} \tag{3.3}$$

and $\delta = k^{-1/2}\log k$. Uniformly for $|\alpha| \le 1/2$ we have

$$U(\alpha) = U(0) + U'(0)\alpha + \frac{1}{2}U''(0)\alpha^2 + O_g(r\alpha^3)$$

where

$$U(0) = 1,$$
$$U'(0) = 2\pi i\Big(\sum_{j=1}^{g-1} jr^j\Big)\Big(\sum_{j=1}^{g-1} r^j\Big)^{-1} = 2\pi i A$$

where by (2.9),

$$A = k/\nu, \tag{3.4}$$

and $U''(0) = -4\pi^2 B$ so that

$$U(\alpha) = 1 + 2\pi i A\alpha - 2\pi^2 B\alpha^2 + O_g(r\alpha^3).$$

Clearly, $A = O_g(r)$ and $B = O_g(r)$. Thus by (3.4), it follows that for $|\alpha| < \alpha_0 = \alpha_0(g)$,

$$U(\alpha) = \exp\left(2\pi i\frac{k}{\nu}\alpha - D\alpha^2 + O_g(r\alpha^3)\right)$$

where $D = 2\pi^2(B - A^2)$ (so that D satisfies (2.13)).

Thus the integral J_1 in (3.2) can be rewritten as

$$\begin{aligned} J_1 &= \int\limits_{|\alpha|\le\delta} \exp(2\pi i k\alpha - D\nu\alpha^2 + O_g(r\nu\alpha^3))e(-k\alpha)\,d\alpha \\ &= \int\limits_{|\alpha|\le\delta} \exp(-D\nu\alpha^2 + O_g(r\nu\alpha^3))\,d\alpha. \end{aligned}$$

By (2.16) we have $r\nu = O_g(k)$ so that by the definition of δ, for $|\alpha| \le \delta$ we have

$$\begin{aligned} J_1 &= \int\limits_{|\alpha|\le\delta} \exp(-D\nu\alpha^2)\,d\alpha + O_g\Big(r\nu \int\limits_{|\alpha|\le\delta} |\alpha|^3 \exp(-D\nu\alpha^2)\,d\alpha\Big) \\ &= \int\limits_{-\infty}^{\infty} \exp(-D\nu\alpha^2)\,d\alpha + O\Big(\int\limits_{\delta}^{\infty} \exp(-D\nu\alpha^2)\,d\alpha\Big) \\ &\quad + O_g\Big(r\nu\int\limits_0^{\delta}\alpha^3\exp(-D\nu\alpha^2)\,d\alpha\Big). \end{aligned} \tag{3.5}$$

Substituting $\alpha = (2D\nu)^{-1/2}x$ we get

$$\begin{aligned} \int\limits_{-\infty}^{\infty} \exp(-D\nu\alpha^2)\,d\alpha &= (2D\nu)^{-1/2}\int\limits_{-\infty}^{\infty}\exp(-x^2/2)\,dx \\ &= \pi^{1/2}(D\nu)^{-1/2} \end{aligned} \tag{3.6}$$

(since it is well known from probability theory that the last integral is equal to $(2\pi)^{1/2}$), and the substitution $\alpha = (D\nu)^{-1/2}x^{1/2}$ gives

$$(3.7)\qquad \int\limits_{\delta}^{\infty} \exp(-D\nu\alpha^2)\,d\alpha = \frac{1}{2}(D\nu)^{-1/2}\int\limits_{D\nu\delta^2}^{\infty} x^{-1/2}\exp(-x)\,dx$$
$$< \frac{1}{2}(D\nu)^{-1/2}(D\nu\delta^2)^{-1/2}\int\limits_{D\nu\delta^2}^{\infty}\exp(-x)\,dx$$
$$= \frac{1}{2}(D\nu\delta)^{-1}\exp(-D\nu\delta^2).$$

Moreover, substituting $\alpha = (D\nu)^{-1/2}x$ we get

$$(3.8)\qquad r\nu\int\limits_{0}^{\delta}\alpha^3\exp(-D\nu\alpha^2)\,d\alpha = rD^{-2}\nu^{-1}\int\limits_{0}^{(D\nu)^{1/2}\delta} x^3\exp(-x^2)\,dx$$
$$< rD^{-2}\nu^{-1}\int\limits_{0}^{\infty} x^3\exp(-x^2)\,dx$$
$$= O(rD^{-2}\nu^{-1}).$$

Finally, in order to estimate J_2, we need the following lemma:

LEMMA 1. *For $0 < r \le 1$ and all $\alpha \in \mathbb{R}$ we have*

$$|U(\alpha)| \le 1 - \frac{2r}{g}\|\alpha\|^2.$$

Proof. Clearly,

$$\left|\frac{1+re(\alpha)}{1+r}\right|^2 = \frac{(1+r)^2 - 2r(1-\cos 2\pi\alpha)}{(1+r)^2}$$
$$= 1 - \frac{2r}{(1+r)^2}2\sin^2\pi\alpha \le 1 - r(2\|\alpha\|)^2 = 1 - 4r\|\alpha\|^2$$

whence $|1+re(\alpha)| \le (1+r)(1-4r\|\alpha\|^2)^{1/2} \le (1+r)(1-2r\|\alpha\|^2)$.

By $0 < r \le 1$, it follows that

$$|U(\alpha)| = \frac{|1+re(\alpha)+r^2e(2\alpha)+\ldots+r^{g-1}e((g-1)\alpha)|}{1+r+\ldots+r^{g-1}}$$
$$\le \frac{|1+re(\alpha)|+r^2+\ldots+r^{g-1}}{1+r+\ldots+r^{g-1}}$$
$$\le \frac{(1+r)(1-2r\|\alpha\|^2)+r^2+\ldots+r^{g-1}}{1+r+\ldots+r^{g-1}}$$
$$= 1 - \frac{2(1+r)r\|\alpha\|^2}{1+r+\ldots+r^{g-1}} \le 1 - \frac{2r\|\alpha\|^2}{g}$$

which completes the proof of the lemma.

The application of Lemma 1 gives

$$|J_2| = \Big| \int\limits_{\delta<\alpha\le 1/2} (U(\alpha))^\nu e(-k\alpha)\,d\alpha \Big| \le 2 \int\limits_{\delta}^{1/2} |U(\alpha)|^\nu\,d\alpha$$
$$\le 2 \int\limits_{\delta}^{1/2} \left(1 - \frac{2r\|\alpha\|^2}{g}\right)^\nu d\alpha < \left(1 - \frac{2r\delta^2}{g}\right)^\nu.$$

For $0 < x < 1$ we have $1 - x < \exp(-x)$, thus it follows that

$$|J_2| < \exp\left(\frac{-2r\nu}{g}\delta^2\right). \tag{3.9}$$

Combining (3.2) and (3.5)–(3.9), by (2.16) and (2.17) we get

$$\begin{aligned} J &= J_1 + J_2 \\ &= \pi^{1/2}(D\nu)^{-1/2} \\ &\quad + O_g\bigg((D\nu\delta)^{-1}\exp(-D\nu\delta^2) + rD^{-2}\nu^{-1} + \exp\Big(-\frac{2r\nu}{g}\delta^2\Big)\bigg) \\ &= \pi^{1/2}(D\nu)^{-1/2} + O_g\Big(\frac{1}{D\nu}\Big). \end{aligned} \tag{3.10}$$

(2.12) follows from (3.1) and (3.10), and this completes the proof of Theorem 1.

Proof of Corollary 2. By (2.3), we may assume that $k \le (g-1)\nu/2$. It follows from (2.11) and (2.19) by an easy computation that

$$A = \frac{k}{\nu} = \frac{g-1}{2} + O(\varDelta\nu^{-1})$$

and

$$B = \frac{(g-1)(2g-1)}{6} + O_g(\varDelta\nu^{-1})$$

whence

$$D = 2\pi^2(B - A^2) = \frac{\pi^2}{6}(g^2-1) + O(\varDelta\nu^{-1}). \tag{3.11}$$

Moreover, writing $\eta = 1 - r$ so that, by (2.11),

$$\eta = \frac{12\varDelta}{(g^2-1)\nu} + O_g(\varDelta^2\nu^{-2}), \tag{3.12}$$

we have

$$\begin{aligned} r^{-k} &= \exp(-k\log(1-\eta)) = \exp\big(k\eta + \tfrac{1}{2}k\eta^2 + O(k\eta^3)\big) \\ &= \exp\bigg(\Big(\frac{g-1}{2}\nu - \varDelta\Big)\eta + \frac{g-1}{4}\nu\eta^2 + O_g(\varDelta^3\nu^{-2})\bigg). \end{aligned} \tag{3.13}$$

Next, writing $h(x)=1+x+\ldots+x^{g-1}$, we have

$$\begin{aligned}h&=1+r+\ldots+r^{g-1}=h(1-\eta)=h(1)-h'(1)\eta+\tfrac{1}{2}h''(1)\eta^2+O_g(\eta^3)\\&=g-\frac{(g-1)g}{2}\eta+\frac{(g-2)(g-1)g}{6}\eta^2+O_g(\eta^3)\end{aligned}$$

so that

$$\begin{aligned}(3.14)\quad &(1+r+\ldots+r^{g-1})^\nu=(h(r))^\nu\\&=g^\nu\biggl(1-\frac{g-1}{2}\eta+\frac{(g-2)(g-1)}{6}\eta^2+O_g(\eta^3)\biggr)^\nu\\&=(1+O(M^{-1}))\\&\quad\times M\exp\biggl(\nu\log\biggl(1-\biggl(\frac{g-1}{2}\eta-\frac{(g-2)(g-1)}{6}\eta^2+O_g(\eta^3)\biggr)\biggr)\biggr)\\&=(1+O(M^{-1}))\exp\biggl(-\frac{g-1}{2}\nu\eta+\frac{(g-1)(g-5)}{24}\nu\eta^2+O_g(\varDelta^3\nu^{-2})\biggr).\end{aligned}$$

Combining (3.13) and (3.14), and using (3.12), we get

$$\begin{aligned}(3.15)\quad &r^{-k}(1+r+\ldots+r^{g-1})^\nu\\&=(1+O(M^{-1}))M\exp\biggl(-\varDelta\eta+\frac{g^2-1}{24}\nu\eta^2+O_g(\varDelta^3\eta^{-2})\biggr)\\&=(1+O(M^{-1}))M\exp\biggl(-\frac{6}{g^2-1}\cdot\frac{\varDelta^2}{\nu}+O_g(\varDelta^3\nu^{-2})\biggr).\end{aligned}$$

(2.20) follows from (2.12), (3.11) and (3.15), and this completes the proof of Corollary 2.

Proof of Corollary 3. By (2.3), we may assume that $k\le\frac{g-1}{2}\nu$. By $g\ge3$, it follows from (2.8) and (2.10) that

$$B=\frac{r+4r^2+O(r^3)}{1+r+O(r^2)}=r+3r^2+O(r^3)=\frac{k}{\nu}+2\biggl(\frac{k}{\nu}\biggr)^2+O\biggl(\biggl(\frac{k}{\nu}\biggr)^3\biggr)$$

so that, by (2.13),

$$D=2\pi^2(B-A^2)=2\pi^2\biggl(\frac{k}{\nu}+\biggl(\frac{k}{\nu}\biggr)^2+O\biggl(\biggl(\frac{k}{\nu}\biggr)^3\biggr)\biggr).$$

It follows that the factor $\pi^{1/2}(D\nu)^{-1/2}$ appearing in (2.12) is

$$\begin{aligned}(3.16)\quad \pi^{1/2}(D\nu)^{-1/2}&=2^{-1/2}\pi^{-1/2}(k+k^2\nu^{-1}+O(k^3\nu^{-2}))^{-1/2}\\&=2^{-1/2}\pi^{-1/2}k^{-1/2}\biggl(1-\frac{1}{2}\cdot\frac{k}{\nu}+O(k^2\nu^{-2})\biggr).\end{aligned}$$

Moreover, by $g \geq 3$ and (2.10) we have

$$
\begin{aligned}
(3.17)\quad & r^{-k}(1+r+\ldots+r^{g-1})^{\nu}\\
&= \exp(-k\log r+\nu\log(1+r+r^2+O(r^3)))\\
&= \exp\Big(-k\log\frac{k}{\nu}\Big(1-\frac{k}{\nu}+O\Big(\Big(\frac{k}{\nu}\Big)^2\Big)\Big)+\nu\Big(r+\frac{r^2}{2}\Big)+O(\nu r^3)\Big)\\
&= \exp\Big(-k\log\frac{k}{\nu}+k+\frac{k^2}{2\nu}+O(k^3\nu^{-2})\Big).
\end{aligned}
$$

Since now $l = k$, (2.21) follows from (3.16) and (3.17) and this completes the proof of Corollary 3.

4. Proof of Theorem 2. Assume first that $k \leq (g-1)\nu/2$. Consider the generating function

$$
G(z,\gamma) = \sum_{n=1}^{N} z^{S(n)} e(n\gamma) \tag{4.1}
$$

(where $z \in \mathbb{C}$, $\gamma \in \mathbb{R}$) so that

$$
\frac{1}{m}\sum_{j=1}^{m} e\Big(-\frac{hj}{m}\Big)G\Big(z,\frac{j}{m}\Big) = \sum_{\substack{1\leq n\leq N\\ n\equiv h \,(\mathrm{mod}\, m)}} z^{S(n)}.
$$

Thus taking $z = re(\beta)$ where $r = r(N,k)$ is defined in Section 2, we have

$$
\begin{aligned}
(4.2)\quad & |\{n : n \in V_k(N),\ n \equiv h \pmod m\}|\\
&= r^{-k}\int_0^1 e(-k\beta) \sum_{\substack{1\leq n\leq N\\ n\equiv h \,(\mathrm{mod}\, m)}} (re(\beta))^{S(n)}\, d\beta\\
&= \frac{1}{m} r^{-k} \sum_{j=1}^{m}\int_0^1 e\Big(-k\beta-\frac{hj}{m}\Big)G\Big(re(\beta),\frac{j}{m}\Big)\,d\beta.
\end{aligned}
$$

Here the term with $j = m$ is

$$
\begin{aligned}
&\frac{1}{m} r^{-k}\int_0^1 e(-k\beta)G(re(\beta),0)\,d\beta\\
&\qquad = \frac{1}{m} r^{-k}\int_0^1 e(-k\beta)\Big(\sum_{n=1}^{N} r^{S(n)}e(S(n)\beta)\Big)\,d\beta = \frac{1}{m}|V_k(N)|.
\end{aligned}
$$

Thus it follows from (4.2) that

$$(4.3)\qquad \left||\{n : n \in V_k(N),\ n \equiv h \pmod{m}\}| - \frac{1}{m}|V_k(N)|\right| \le \frac{1}{m} r^{-k} \sum_{j=1}^{m-1} \int_0^1 \left|G\left(re(\beta), \frac{j}{m}\right)\right| d\beta.$$

Write N in the form

$$N = \sum_{j=1}^{t} b_j g^{\nu_j}, \qquad \nu_1 > \ldots > \nu_t,\ b_j \in \{1, \ldots, g-1\} \text{ for } j = 1, \ldots, t,$$

so that, defining $\nu = \nu(N)$ as in Section 2, we have $\nu_1 = \nu$ if $N \ge g^\nu$ and $\nu_1 = \nu - 1$ if $N = g^\nu - 1$. Moreover, for $l = 1, \ldots, t$, let $\mathcal{A}_l$ denote the set of the integers n that can be represented in the form

$$(4.4)\qquad n = \sum_{i=1}^{l-1} b_i g^{\nu_i} + x g^{\nu_l} + \sum_{u=0}^{\nu_l - 1} y_u g^u$$

where $x \in \{0, 1, \ldots, b_l - 1\}$, $y_u \in \{0, 1, \ldots, j-1\}$ for $u = 0, 1, \ldots, \nu_l - 1$, and let $\mathcal{A}_{t+1} = \{N\}$. Then clearly we have

$$\bigcup_{l=1}^{t+1} \mathcal{A}_l = \{0, 1, \ldots, N\} \quad \text{and} \quad \mathcal{A}_j \cap \mathcal{A}_l = \emptyset \quad \text{for } 1 \le j < l \le t+1$$

so that, writing $S(0) = 0$ and using (4.1) and (4.4), for all β, $\gamma \in \mathbb{R}$ we have

$$\begin{aligned} 1 + G(re(\beta), \gamma) &= 1 + \sum_{n=1}^{N} (re(\beta))^{S(n)} e(n\gamma) \\ &= \sum_{l=1}^{t+1} \sum_{n \in \mathcal{A}_l} r^{S(n)} e(S(n)\beta + n\gamma) \\ &= \sum_{l=1}^{t+1} \sum_{n \in \mathcal{A}_l} (re(\beta))^{S(n)} e(n\gamma) \\ &= \sum_{l=1}^{t} \sum_{x} \sum_{y_0} \cdots \sum_{y_{\nu_l - 1}} (re(\beta))^{b_1 + \ldots + b_{l-1} + x + y_0 + \ldots + y_{\nu_l - 1}} \\ &\quad \times e((b_1 g^{\nu_1} + \ldots + b_{l_1} g^{\nu_l - 1} + x g^{\nu_l} + y_0 g^0 + \ldots \\ &\quad + y_{\nu_l - 1} g^{\nu_l - 1})\gamma) + (re(\beta))^{S(N)} e(N\gamma) \end{aligned}$$

whence, by $0 < r < 1$,

$$(4.5)\quad |G(re(\beta),\gamma)| \le 2+\sum_{l=1}^{t} r^{b_1+\ldots+b_l}\Big|\sum_{x=0}^{b_l-1}(re(\beta+g^{\nu_l}\gamma))^x\Big|\prod_{u=0}^{\nu_l-1}\Big|\sum_{y_u=0}^{g-1}(re(\beta+g^u\gamma))^{y_u}\Big|.$$

Thus using $0<r<1$ and defining $U(\alpha)$ by (3.3), we obtain

$$|G(re(\beta),\gamma)|\le 2+\sum_{l=1}^{t} r^{l-1}g(1+r+\ldots+r^{g-1})^{\nu_l}\prod_{u=0}^{\nu_l-1}|U(\beta+g^u\gamma)|.$$

It follows that defining the positive integer g by $\nu_q \ge \nu/2 > \nu_{q+1}$ (if $\nu_t \ge \nu/2$ then we put $q=t$), by $|U(\alpha)|\le 1$ (for all $\alpha\in\mathbb{R}$) for $j=1,\ldots,m-1$ we have

$$(4.6)\qquad |G(re(\beta),j/m)|\le 2+g\Big(\sum\nolimits_1+\sum\nolimits_2\Big)$$

where

$$(4.7)\quad \sum\nolimits_1=\sum_{l=1}^{q} r^{l-1}(1+r+\ldots+r^{g-1})^{\nu_l}\prod_{u=0}^{(\nu/2)-1}\Big|U\Big(\beta+g^u\frac{j}{m}\Big)\Big|,$$

$$\sum\nolimits_2=\sum_{l=q+1}^{t} r^{l-1}(1+r+\ldots+r^{g-1})^{\nu_l}.$$

Clearly, $\nu_l\le\nu_1-(l-1)\le\nu-(l-1)$ for all j. Thus by $0<r<1$, the first factor in $\sum_1$ can be estimated in the following way:

$$(4.8)\quad \sum_{l=1}^{q} r^{l-1}(1+r+\ldots+r^{g-1})^{\nu_l}$$
$$\le(1+r+\ldots+r^{g-1})^{\nu}\sum_{j=0}^{\infty}\Big(\frac{r}{1+r+\ldots+r^{g-1}}\Big)^j$$
$$\le(1+r+\ldots+r^{g-1})^{\nu}\sum_{j=0}^{\infty}\Big(\frac{r}{1+r}\Big)^j$$
$$=(1+r+\ldots+r^{g-1})^{\nu}(1+r)<2(1+r+\ldots+r^{g-1})^{\nu}.$$

To estimate the second factor, first we use Lemma 1:

$$(4.9)\quad \prod_{u=0}^{(\nu/2)-1}\Big|U\Big(\beta+g^u\frac{j}{m}\Big)\Big|\le\prod_{u=0}^{(\nu/2)-1}\Big(1-\frac{2r}{g}\Big\|\beta+g^u\frac{j}{m}\Big\|^2\Big)$$
$$\le\exp\Big(-\frac{2r}{g}\sum_{u=0}^{(\nu/2)-1}\Big\|\beta+g^u\frac{j}{m}\Big\|^2\Big)$$

since $1-x\le e^{-x}$ for $x\ge 0$.

Next, we need the following lemma:

Lemma 2. *If* $g, m, \varrho \in \mathbb{N}$, $g \ge 2$, $((g-1)g, m) = 1$, $m \ge 2$, $1 \le j \le m-1$,

$$\varrho \ge 2\frac{\log m}{\log g} + 8 \tag{4.10}$$

and $\beta \in \mathbb{R}$, *then*

$$\sum_{u=0}^{\varrho-1} \left\| \beta + g^u \frac{j}{m} \right\|^2 \ge \frac{(g-1)^2}{128 g^4} \cdot \frac{\varrho}{\log m}.$$

This lemma will be proved in the next section, first we will complete the proof of Theorem 2.

It follows from (2.23) that (4.10) holds with $[\nu/2]$ in place of ϱ so that Lemma 2 can be applied to estimate the sum in the exponent in (4.9). In view of (2.16), we obtain

$$\begin{aligned} \prod_{u=0}^{[\nu/2]-1} \left| U\left(\beta + g^u \frac{j}{m}\right) \right| & \\ \le \exp\left(- \frac{r(g-1)^2}{64 g^5} \cdot \frac{[\nu/2]}{\log m}\right) &< \exp\left(- c_{15} \frac{k}{\log m}\right). \end{aligned} \tag{4.11}$$

To estimate $\sum_2$, for $q+1 \le l \le t$ define i by $l = q+i$ so that $l \ge 1+i$ whence $l-1 \ge i$. Moreover, we have

$$\nu_l = \nu_{q+i} \le \nu_{q+1} - (i-1) < \nu/2 - (i-1)$$

so that, by $0 < r \le 1$ and using (2.16),

$$\begin{aligned} \sum\nolimits_2 &\le \sum_{i=1}^{t-q} r^i (1 + r + \ldots + r^{g-1})^{(\nu/2)-(i-1)} \\ &\le (1 + r + \ldots + r^{g-1})^{\nu/2} \sum_{j=0}^{\infty} \left(\frac{r}{1+r} \right)^j \\ &\le 2(1 + r + \ldots + r^{g-1})^{\nu} (1 + r + \ldots + r^{g-1})^{-\nu/2} \\ &\le 2(1 + r + \ldots + r^{g-1})^{\nu} (1 + r)^{-\nu/2} \\ &< 2(1 + r + \ldots + r^{g-1})^{\nu} \left(1 + c_1 \frac{k}{\nu}\right)^{-\nu/2} \\ &< (1 + r + \ldots + r^{g-1})^{\nu} \exp(-c_{16} k). \end{aligned} \tag{4.12}$$

It follows from (4.3), (4.6)–(4.8), (4.11) and (4.12) that

$$(4.13)\quad \left| |\{n : n \in V_k(N),\ n \equiv h \pmod{m}\}| - \frac{1}{m}|V_k(N)| \right|$$
$$\le \frac{1}{m} r^{-k} \sum_{j=1}^{m-1} \int_0^1 \Big| 2 + g(1 + r + \ldots + r^{g-1})^{\nu}$$
$$\times \left(2 \exp\left(-c_{15} \frac{k}{\log m} \right) + \exp(-c_{16} k) \right) \Big| \, d\beta$$
$$\le r^{-k}(1 + r + \ldots + r^{g-1})^{\nu} \exp\left(-c_{17} \frac{k}{\log m} \right).$$

(2.25) follows from Corollary 1, (2.23) and (4.13), and this completes the proof in the case $k \le (g-1)\nu/2$.

Finally, if $(g-1)\nu/2 < k < (g-1)\nu$ (by (2.22) $k < (g-1)\nu$ holds), then we replace the generating function $G(z, \gamma)$ in (4.1) by

$$G^{\star}(z, \gamma) = \sum_{n=1}^{N} z^{(g-1)\nu - S(n)} e(n\gamma),$$

and we set $z = re(\beta)$ where $r = r(N, l) = r(N, (g-1)\nu - k)$ is defined in Section 2. The rest of the proof is similar to the case $k \le (g-1)\nu/2$.

5. Proof of Lemma 2. We will prove slightly more: we will prove the lemma replacing the condition $((g-1)g, m) = 1$ by $(g, m) = 1$ and

$$(5.1)\qquad \frac{j}{m} \in \bigcup_{t=0}^{g-2} \left] \frac{t}{g-1}, \frac{t+1}{g-1} \right[.$$

(Clearly, (5.1) follows from $(g-1, m) = 1$ and $1 \le j \le m-1$.)

We will proceed in five steps.

First step: We show that if $0 < j/m \le 1/g$ and $(m, g) = 1$ then there exists n, $0 \le n \le \log m / \log g$, such that

$$\left\| g^{n+1} \frac{j}{m} - g^n \frac{j}{m} \right\| \ge \frac{g-1}{2g^2}.$$

- If $1/(2g) \le j/m \le 1/g$ then $1/2 \le gj/m \le 1$ and

$$\frac{gj}{m} - \frac{j}{m} = \frac{(g-1)j}{m} \ge \frac{g-1}{2g}.$$

- If $0 < j/m \le 1/(2g)$, let n be the smallest integer such that

$$g^n \frac{j}{m} \le \frac{1}{2g} \le g^{n+1} \frac{j}{m} \le \frac{1}{2}.$$

Then $n \le \log m/\log g$ and

$$g^{n+1}\frac{j}{m} - g^n\frac{j}{m} = (g-1)g^n\frac{j}{m} \ge \frac{g-1}{2g^2}.$$

Second step: We show that if $0 < j/m < 1/(g-1)$ and $(m,g) = 1$ then there exists n, $0 \le n \le 1 + \log m/\log g$, such that

$$\left\| g^{n+1}\frac{j}{m} - g^n\frac{j}{m} \right\| \ge \frac{g-1}{2g^2}.$$

It follows clearly from the first step that if $(g-1)/g \le j/m < 1$ then, for n as before,

$$\left\| g^{n+1}\frac{j}{m} - g^n\frac{j}{m} \right\| = \left\| g^{n+1}\left(1-\frac{j}{m}\right) - g^n\left(1-\frac{j}{m}\right) \right\| \ge \frac{g-1}{2g^2}$$

because $0 < (m-j)/m \le 1/g$.

Suppose now that

$$\frac{g-2}{g-1} < \frac{j}{m} \le \frac{g-2}{g-1} + \frac{1}{g},$$

so that

$$\frac{j}{m} - \frac{g-2}{g-1} = \frac{j(g-1) - m(g-2)}{m(g-1)} \in \left]0, \frac{1}{g}\right]$$

and we can apply the result from the first step (note that $(m(g-1), g) = 1$): there exists n,

$$0 \le n \le \frac{\log(m(g-1))}{\log g} \le 1 + \frac{\log m}{\log g},$$

such that

$$\left\| g^{n+1}\left(\frac{j}{m} - \frac{g-2}{g-1}\right) - g^n\left(\frac{j}{m} - \frac{g-2}{g-1}\right) \right\| \ge \frac{g-1}{2g^2}.$$

Since for every integer $n \ge 0$,

$$g^n\frac{g-2}{g-1} = -\frac{1}{g-1} \pmod 1,$$

we have proved that

$$\left\| g^{n+1}\frac{j}{m} - g^n\frac{j}{m} \right\| \ge \frac{g-1}{2g^2}.$$

But

$$\frac{g-2}{g-1} + \frac{1}{g} \ge \frac{g-1}{g}$$

so that we have shown that if $(g-2)/(g-1) < j/m < 1$ then there exists n, $0 \le n \le 1 + \log m/\log g$ such that

$$\left\| g^{n+1}\frac{j}{m} - g^n\frac{j}{m} \right\| \ge \frac{g-1}{2g^2}.$$

The second step follows by the same argument as before (we remark that if $0 < j/m < 1/(g-1)$, then $(g-2)/(g-1) < (m-j)/m < 1$).

Third step: We show that if

$$\frac{j}{m} \in \bigcup_{t=0}^{g-2} \left] \frac{t}{g-1}, \frac{t+1}{g-1} \right[$$

and $(m, g) = 1$ then there exists n, $0 \le n \le 2 + \log m / \log g$, such that

$$\left\| g^{n+1} \frac{j}{m} - g^n \frac{j}{m} \right\| \ge \frac{g-1}{2g^2}.$$

Let $k \in \{0, \dots, g-2\}$ be fixed and consider for any

$$\frac{j}{m} \in \left] \frac{t}{g-1}, \frac{t+1}{g-1} \right[$$

the rational number

$$\frac{j}{m} - \frac{t}{g-1} = \frac{j(g-1) - tm}{m(g-1)} \in \left] 0, \frac{1}{g-1} \right[.$$

Since $(m(g-1), g) = 1$, it follows from the second step that there exists n,

$$0 \le n \le 1 + \frac{\log m(g-1)}{\log g} \le 2 + \frac{\log m}{\log g}$$

such that

$$\left\| g^{n+1} \left(\frac{j}{m} - \frac{t}{g-1} \right) - g^n \left(\frac{j}{m} - \frac{t}{g-1} \right) \right\| \ge \frac{g-1}{2g^2}.$$

As for any integer $n \ge 0$,

$$g^n \frac{t}{g-1} \equiv \frac{t}{g-1} \pmod 1,$$

we have completed the third step.

Fourth step: If $(g, m) = 1$ and

$$\frac{j}{m} \in \bigcup_{t=0}^{g-2} \left] \frac{t}{g-1}, \frac{t+1}{g-1} \right[$$

then for any $\beta \in \mathbb{R}$ we have

$$\sum_{n \le [\log m / \log g] + 3} \left\| \beta + g^n \frac{j}{m} \right\|^2 \ge \frac{(g-1)^2}{8g^4}.$$

This step follows easily from the inequality

$$\left\| \beta + g^{n+1} \frac{j}{m} \right\|^2 + \left\| \beta + g^n \frac{j}{m} \right\|^2 \ge \frac{1}{2} \left\| g^{n+1} \frac{j}{m} - g^n \frac{j}{m} \right\|^2.$$

Fifth step: If $(g,m)=1$,

$$\frac{j}{m}\in\bigcup_{t=0}^{g-2}\left]\frac{t}{g-1},\frac{t+1}{g-1}\right[,\qquad b=\left[\frac{\log m}{\log g}\right]+4$$

and $\varrho=bq+r$ (with $0\le r<b$) then for any $\beta\in\mathbb{R}$ we have

$$\sum_{u<\varrho}\left\|\beta+g^u\frac{j}{m}\right\|^2\ge q\frac{(g-1)^2}{8g^4}.$$

We have

$$\sum_{u<\nu}\left\|\beta+g^u\frac{j}{m}\right\|^2\ge\sum_{u<bq}\left\|\beta+g^u\frac{j}{m}\right\|^2=\sum_{i<q}\sum_{bi\le u<b(i+1)}\left\|\beta+g^u\frac{j}{m}\right\|^2$$
$$=\sum_{i<q}\sum_{u<b}\left\|\beta+g^u\frac{g^{bi}j}{m}\right\|^2.$$

Thus to get the result, it is enough to prove that for any integer $n\ge0$ we have

$$\left\{\frac{g^nj}{m}\right\}\in\bigcup_{t=0}^{g-2}\left]\frac{t}{g-1},\frac{t+1}{g-1}\right[.$$

Suppose that there exist $n\ge0$, $t\in\{0,\dots,g-2\}$ and $v\in\mathbb{Z}$ such that $g^nj/m=t/(g-1)+v$. Then $j(g-1)g^n=tm+vm(g-1)$ so that m would divide $j(g-1)$ (because $(m,g)=1$), which would contradict our hypothesis $j/m\in\bigcup_{t=0}^{g-2}\,]\,t/(g-1),(t+1)/(g-1)[$. To prove Lemma 2, it is now enough to remark that as $bq\le\varrho<b(q+1)$ we have

$$q>\frac{\varrho}{b}-1=\frac{\varrho}{\left[\frac{\log m}{\log g}\right]+4}-1\ge\frac{\varrho}{\frac{\log m}{\log g}+4}-1.$$

But for $\varrho\ge2\log m/\log g+8$ we have

$$\frac{\varrho}{\frac{\log m}{\log g}+4}-1\ge\frac{\varrho}{2\left(\frac{\log m}{\log g}+4\right)}\ge\frac{1}{16}\cdot\frac{\varrho}{\log m}$$

because

$$\frac{\log m+4\log g}{\log m}\le1+\frac{4\log g}{\log 2}\le8\log g.$$

6. Proof of Theorem 4. We may assume that $k\le\frac{g-1}{2}\nu$ since the case $k>\frac{g-1}{2}\nu$ can be handled similarly (see the remark at the end of Section 4).

We will apply the general Kubilius model described in Elliott's book [Ell] (Chapter 3, pp. 129–132). Let $G(z)$ be the frequency corresponding to $F_N(z)$ when $\omega(n)$ is replaced by $\omega_1(n)$, the function which counts the number of distinct prime divisors p of n with $l_1^d < p \le \exp(l_1/l_3)$, where d will be fixed later independently of N. The role of the a_j in that model is here played by the elements of $V_k(N)$. We set $q = \exp(l_1/l_3)$, $X = |V_k(N)|$, $\eta(v) = v^{-1}$. Then the function S appearing there will be

$$\sum_{l_1^d < p \le q} \frac{\log p}{p-1},$$

which is $\le \log q + O(1)$. If now W_p, $l_1^d < p \le q$, are independent random variables, distributed according to

$$W_p = \begin{cases} 1 & \text{with probability } 1/p, \\ 0 & \text{with probability } 1 - 1/p, \end{cases}$$

then

$$\begin{aligned} &\Big|G(z) - P\Big(\sum_{l_1^d < p \le q} W_p \le z\sqrt{l_2} + l_2\Big)\Big| \\ &\le 10 \exp\left(-\frac{\log w}{8 \log q} \log\left(\frac{\log w}{S}\right)\right) + \frac{12}{|V_k(N)|} \sum_{m \le w^4}{}' 4^{\omega(m)} |R(m)| \\ &= E_1 + E_2 \end{aligned} \tag{6.1}$$

where $'$ indicates that m is squarefree and composed of primes in the interval $(l_1^d, q]$. The remainder $R(m)$ is given by

$$R(m) = |\{n : n \in V_k(N),\ n \equiv 0 \pmod{m}\}| - \frac{1}{m}|V_k(N)| \tag{6.2}$$

and the estimate (6.1) is valid for all $q \ge 2$, $8\max(\log q, S) \le \log w$.

If we set $w = N^{1/24}$, the first error term E_1 in (6.1) is clearly

$$E_1 = O(l_2^{-j}) \tag{6.3}$$

for each fixed $j > 0$.

The estimate of the second error term E_2 in (6.1) will be based on the large sieve inequality [Mon]:

Lemma 3. *If $U \in \mathbb{Z}$, $V \in \mathbb{Z}$, $a_{U+1}, a_{U+2}, \dots, a_{U+V}$ are complex numbers, X is a set of real numbers for which $\|x - x'\| \ge \delta > 0$ whenever x and x' are distinct members of X, and we write*

$$S(x) = \sum_{n=U+1}^{U+V} a_n e(nx),$$

then

$$\sum_{x \in X} |S(x)|^2 \le (\delta^{-1} + V) \sum_{n=U+1}^{U+V} |a_n|^2.$$

Moreover, observe that by (4.3) and (6.2), and as in (4.4) and (4.5) (indeed, now $1+G(z,\gamma)=\prod_{u=0}^{\nu-1}\varphi(ze(g^u\gamma))$), we have

$$(6.4)\qquad |R(m)| \le \frac{1}{m}r^{-k}\sum_{j=1}^{m-1}\int_0^1 \left|G\Big(re(\beta),\frac{j}{m}\Big)\right| d\beta$$
$$\le \frac{1}{m}r^{-k}\sum_{j=0}^{m-1}\int_0^1 \Big(1+\Big|\prod_{u=0}^{\nu-1}\varphi\Big(re\Big(\beta+g^u\frac{j}{m}\Big)\Big)\Big|\Big) d\beta$$

(where r, $U(\alpha)$, $\varphi(z)$, $G(z,\gamma)$ are defined as in Sections 2–4).

In order to obtain a good upper bound via large sieve, first we have to replace the trigonometric polynomial $\prod_{u=0}^{\nu-1}U(\beta+g^u\alpha)$ of degree N in α by polynomials of lower degree. Indeed, write

$$\mu_1=[\nu/2],\qquad \mu_2=\nu-[\nu/2],$$

$$(6.5)\qquad G_1(\beta,\gamma)=\prod_{u=0}^{\mu_1-1}\varphi(re(\beta+g^u\gamma)),$$

$$(6.6)\qquad G_2(\beta,\gamma)=\prod_{u=\mu_1}^{\mu_1+\mu_2-1}\varphi(re(\beta+g^u\gamma)),$$

$$(6.7)\qquad H_1(\beta,\gamma)=G_1(\beta,\gamma),$$

$$(6.8)\qquad H_2(\beta,\gamma)=G_2(\beta,g^{-\mu_1}\gamma)=\prod_{v=0}^{\mu_2-1}\varphi(re(\beta+g^v\gamma)),$$

so that

$$(6.9)\qquad \max(\mu_1,\mu_2)\le[\nu/2]+1\le(\nu/2)+1,$$

$$(6.10)\qquad G_1(\beta,\gamma)G_2(\beta,\gamma)=H_1(\beta,\gamma)H_2(\beta,g^{\mu_1}\gamma)=\prod_{u=0}^{\nu-1}\varphi(re(\beta+g^u\gamma)),$$

$H_1(\beta,\gamma)$, $H_2(\beta,\gamma)$ are of the form

$$H_i(\beta,\gamma)=\sum_{n=0}^{g^{\mu_i}-1}a_n^{(i)}(\beta)e(n\gamma)\qquad\text{for } i=1,2,$$

and, by (6.9), for fixed β the degree of the trigonometric polynomials $H_i(\beta,\gamma)$ (in γ) is

$$(6.11)\qquad \deg H_i(\beta,\gamma)=g^{\mu_i}-1\le g^{(\nu/2)+1}$$
$$< g^2g^{(\nu-1)/2}< g^2N^{1/2}\qquad\text{for } i=1,2.$$

Since every m in the sum in E_2 is composed of primes greater than l_1^d, we have $(g,m)=1$. Thus by (6.4)–(6.8), (6.10) and by the inequality

$|ab| \le \frac{1}{2}(|a|^2+|b|^2)$, it follows that for such m we have

$$\begin{aligned}|R(m)| &\le r^{-k}\int_0^1 \biggl(1+\frac{1}{m}\sum_{j=1}^{m-1}\Bigl|G_1\Bigl(\beta,\frac{j}{m}\Bigr)G_2\Bigl(\beta,\frac{j}{m}\Bigr)\Bigr|\biggr)\,d\beta\\ &\le r^{-k}\int_0^1 \biggl(1+\frac{1}{m}\biggl(\sum_{j=1}^{m-1}\Bigl|G_1\Bigl(\beta,\frac{j}{m}\Bigr)\Bigr|^2+\sum_{j=1}^{m-1}\Bigl|G_2\Bigl(\beta,\frac{j}{m}\Bigr)\Bigr|^2\biggr)\biggr)\,d\beta\\ &= r^{-k}\int_0^1 \biggl(1+\frac{1}{m}\biggl(\sum_{j=1}^{m-1}\Bigl|H_1\Bigl(\beta,\frac{j}{m}\Bigr)\Bigr|^2+\sum_{j=1}^{m-1}\Bigl|H_2\Bigl(\beta,g^{\mu_1}\frac{j}{m}\Bigr)\Bigr|^2\biggr)\biggr)\,d\beta\\ &= r^{-k}\int_0^1 \biggl(1+\frac{1}{m}\sum_{i=1}^{2}\sum_{j=1}^{m-1}\Bigl|H_i\Bigl(\beta,\frac{j}{m}\Bigr)\Bigr|^2\biggr)\,d\beta.\end{aligned}$$

It follows that

$$\begin{aligned}E_2 &\ll r^{-k}|V_k(N)|^{-1}\int_0^1 {\sum_{m\le w^4}}' 4^{\omega(m)}\biggl(1+\frac{1}{m}\sum_{i=1}^{2}\sum_{j=1}^{m-1}\Bigl|H_i\Bigl(\beta,\frac{j}{m}\Bigr)\Bigr|^2\biggr)\,d\beta\\ &\ll r^{-k}|V_k(N)|^{-1}\max_\beta\biggl({\sum_{m\le w^4}}' 4^{\omega(m)}\biggl(1+\frac{1}{m}\sum_{i=1}^{2}\sum_{j=1}^{m-1}\Bigl|H_i\Bigl(\beta,\frac{j}{m}\Bigr)\Bigr|^2\biggr)\biggr)\end{aligned}$$

whence, using $\omega(m)=o(\log m)$,

$$(6.12)\qquad \begin{aligned}E_2 &\ll r^{-k}|V_k(N)|^{-1}\\ &\times\biggl(N^{5/24}+\max_\beta\sum_{i=1}^{2}{\sum_{m\le w^4}}'\frac{4^{\omega(m)}}{m}\sum_{j=1}^{m-1}\Bigl|H_i\Bigl(\beta,\frac{j}{m}\Bigr)\Bigr|^2\biggr).\end{aligned}$$

Here the fractions j/m, $1\le j\le m-1$, may be collected according to the value m/δ of (j,m). For a fixed divisor δ of m, the reduced fractions t/δ, $1\le t\le \delta-1$, $(t,\delta)=1$ will occur just once. Thus, for $i=1,2$ and every real β we have

$$(6.13)\qquad \begin{aligned}&{\sum_{m\le w^4}}'\frac{4^{\omega(m)}}{m}\sum_{j=1}^{m-1}\Bigl|H_i\Bigl(re(\beta),\frac{j}{m}\Bigr)\Bigr|^2\\ &\le {\sum_{1<\delta\le w^4}}'\frac{4^{\omega(\delta)}}{\delta}\sum_{\substack{1\le t\le\delta-1\\(t,\delta)=1}}\Bigl|H_i\Bigl(re(\beta),\frac{t}{\delta}\Bigr)\Bigr|^2{\sum_{h\le w^4/\delta}}'\frac{4^{\omega(h)}}{h}.\end{aligned}$$

Here the innermost sum is

$$\le \prod_{p\le q}\Bigl(1+\frac{4}{p}\Bigr)\ll(\log q)^4\ll l_1^4.$$

We split the δ's into two classes, according to whether $\omega(\delta) > K \log\log N$ or not, where K is a large positive number to be fixed later; denote these two classes by D_1 (the one with $\omega(\delta) > K \log\log N$) and D_2.

Clearly, the coefficient $a_n^{(i)}(\beta)$ of $H_i(\beta,\gamma)$ is maximal in β if $\beta = 0$:

$$|a_n^{(i)}(\beta)| \le a_n^{(i)}(0), \tag{6.14}$$

and we have

$$H_i(0,\gamma) = \sum_{n=0}^{g^{\mu_i}-1} a_n^{(i)}(0) e(n\gamma) = \prod_{u=0}^{\mu_i-1} \varphi(re(g^u\gamma)) = 1 + \sum_{n=1}^{g^{\mu_i}-1} r^{S(n)} e(n\gamma)$$

so that, by (6.9),

$$\begin{aligned} \sum_{n=0}^{g^{\mu_i}-1} (a_n^{(i)}(0))^2 &= 1 + \sum_{n=0}^{g^{\mu_i}-1} r^{2S(n)} = \prod_{u=0}^{\mu_i-1} \varphi(r^2) \\ &= (1 + r^2 + \ldots + r^{2(g-1)})^{\mu_i} \\ &\le (1 + r^2 + \ldots + r^{2(g-1)})^{(\nu/2)+1} \le g\left(\frac{1-r^{2g}}{1-r^2}\right)^{\nu/2}. \end{aligned} \tag{6.15}$$

Thus by using the large sieve (Lemma 3), in view of (6.11) we deduce for $\delta \in D_1$ that

$$\begin{aligned} \sum_{\substack{1\le t\le \delta-1\\(t,\delta)=1}} \left|H_i\left(re(\beta), \frac{t}{\delta}\right)\right|^2 &\le \sum_{t=1}^{\delta} \left|H_i\left(re(\beta), \frac{t}{\delta}\right)\right|^2 \\ &\le (g^2N^{1/2} + \delta) \sum_{n=0}^{g^{\mu_i}-1} |a_n^{(i)}(\beta)|^2 \\ &\le (g^2N^{1/2} + w^4) \sum_{n=0}^{g^{\mu_i}-1} (a_n^{(i)}(0))^2 \\ &< 2g^3N^{1/2}\left(\frac{1-r^{2g}}{1-r^2}\right)^{\nu/2}. \end{aligned}$$

Thus for all β, the contribution of the δ's with $\delta \in D_1$ to the upper bound in (6.13) is

$$\begin{aligned} &\ll_g l_1^4 N^{1/2}\left(\frac{1-r^{2g}}{1-r^2}\right)^{\nu/2} \sum_{\delta\in D_1} \frac{2^{3\omega(\delta)-Kl_2}}{\delta} \\ &\ll_g l_1^{12-K\log 2} N^{1/2}\left(\frac{1-r^{2g}}{1-r^2}\right)^{\nu/2} \end{aligned}$$

(uniformly in β).

If $\delta \in D_2$, then by $\delta > 1$ and since the prime factors of δ are greater than l_1^d, we have $\delta > l_1^d$. Thus using again the large sieve (Lemma 3), in view of (6.11), (6.14) and (6.15) we see that the contribution of the δ's with $\delta \in D_2$ to the upper bound in (6.13) is

$$\begin{aligned}
&\ll l_1^4 \sideset{}{'}\sum_{1<\delta\le w^4} \frac{4^{Kl_2}}{l_1^d} \sum_{\substack{1\le t\le \delta-1\\(t,\delta)=1}} \left|H_i\left(re(\beta), \frac{t}{\delta}\right)\right|^2\\
&\le l_1^{4+K\log 4-d} \sum_{\delta\le w^4} \sum_{\substack{1\le t\le \delta-1\\(t,\delta)=1}} \left|H_i\left(re(\beta), \frac{t}{\delta}\right)\right|^2\\
&\le l_1^{4+K\log 4-d}(g^2N^{1/2}+w^8)\sum_{n=0}^{g^{\mu_i}-1} |a_n^{(i)}(\beta)|^2\\
&\ll_g l_1^{4+K\log 4-d}N^{1/2}\left(\frac{1-r^{2g}}{1-r^2}\right)^{\nu/2}
\end{aligned}$$

(again, uniformly in β). Thus we find from (6.12) and (6.13) that

$$\begin{aligned}
(6.16)\qquad E_2 &\ll_g r^{-k}|V_k(N)|^{-1}\\
&\times\left(N^{5/24}+(l_1^{12-K\log 2}+l_1^{4+K\log 4-d})N^{1/2}\left(\frac{1-r^{2g}}{1-r^2}\right)^{\nu/2}\right).
\end{aligned}$$

By (2.12), (2.14), (2.15), (2.28) and (3.14) we have

$$\begin{aligned}
(6.17)\qquad & r^{-k}|V_k(N)|^{-1}\\
&= (1+r+\ldots+r^{g-1})^{-\nu}\pi^{-1/2}(D\nu)^{1/2}(1+O_g(D\nu)^{-1/2})\\
&\ll_g N^{-1}\nu^{1/2}\exp\left(\frac{g-1}{2}\nu\eta+\frac{(g-1)(g-5)}{24}\nu\eta^2+O_g(\varDelta^3\nu^{-2})\right)
\end{aligned}$$

so that, by (2.28) and (3.12),

$$(6.18)\qquad r^{-k}|V_k(N)|^{-1} \ll_g N^{-1}l^{1/2}\exp(O_g(\varDelta)).$$

It follows from (3.12) and (6.18) that for N large enough,

$$(6.19)\qquad r^{-k}|V_k(N)|^{-1}N^{5/24} < N^{-1/2}.$$

Moreover, by $r = 1-\eta$ we have

$$\begin{aligned}
(6.20)\qquad \left(\frac{1-r^{2g}}{1-r^2}\right)^{\nu/2} &= \left(\frac{1-(1-\eta)^{2g}}{1-(1-\eta)^2}\right)^{\nu/2}\\
&= \left(g\left(1-(g-1)\eta+\frac{4g^2-9g+5}{6}\eta^2+O(\eta^3)\right)\right)^{\nu/2}
\end{aligned}$$

$$= g^{\nu/2}\biggl(\exp\biggl(-(g-1)\eta + \frac{g^2-3g+2}{6}\eta^2 + O(\eta^3)\biggr)\biggr)^{\nu/2}$$
$$\ll N^{1/2}\exp\biggl(-\frac{g-1}{2}\nu\eta + \frac{g^2-3g+2}{12}\nu\eta^2 + O(\nu\eta^3)\biggr).$$

It follows from (3.12), (6.18) and (6.20) that

$$(6.21)\qquad r^{-k}|V_k(N)|^{-1}N^{1/2}\biggl(\frac{1-r^{2g}}{1-r^2}\biggr)^{\nu/2}$$
$$\ll_g l_1^{1/2}\exp\biggl(\biggl(\frac{(g-1)(g-5)}{24} + \frac{g^2-3g+2}{12}\biggr)\nu\eta^2 + O_g(\Delta^3\nu^{-2} + \nu\eta^3)\biggr)$$
$$= l_1^{1/2}\exp\biggl(\frac{g^2-4g+3}{8}\nu\eta^2 + O_g(\Delta^3\nu^{-2})\biggr)$$
$$= l_1^{1/2}\exp\biggl(\frac{18(g-3)}{(g-1)(g+1)^2}\cdot\frac{\Delta^2}{\nu} + O_g(\Delta^3\nu^{-2})\biggr) \ll_{g,K} l^{1/2}.$$

Choosing first K and then d sufficiently large, we deduce from (6.16), (6.19) and (6.21) that

$$(6.22)\qquad E_2 \ll_{g,K} N^{-1/2} + (l_1^{12-K\log 2} + l_1^{4+K\log 4-d})l_1^{1/2} < l_1^{-1}$$

if N is large enough in terms of g and K.

It follows from (6.1), (6.3) and (6.22) that choosing d sufficiently large we have

$$\biggl|G(z) - P\biggl(\sum_{l_1^d<p\le q} W_p \le z\sqrt{l_2} + l_2\biggr)\biggr| \ll_{g,K} l_2^{-1}.$$

Next, using the Berry–Esseen inequality [Ess], in the same way as in [Ell-S] we compare $P(\sum_{l_1^d<p\le q} W_p \le z\sqrt{l_2} + l_2)$ with $\psi(z)$, the normal distribution with mean 0 and variance 1. As in [Ell-S], we obtain

$$(6.23)\qquad |G(z) - \psi(z)| \ll_{g,K} l_3 l_2^{-1/2}.$$

To complete the proof of the theorem it suffices to show that

$$(6.24)\qquad |F_N(z) - G(z)| \ll_{g,K} l_3 l_2^{-1/2}.$$

If $n \le N$, then n may have at most $\log n/\log q \le l_3$ distinct prime divisors p with $p > q$. Thus, by the uniformity of the estimate (6.23), removing the restriction $p \le q$ in the definition of $\omega_1(n)$ changes $G(z)$ by an amount which is $\ll_{g,K} l_3 l_2^{-1/2}$.

Finally, let $\omega_2(n)$ denote the number of distinct prime divisors of n which do not exceed l_1^d. Let L be a large positive number to be fixed later, and write $D = [Ll_3]$. As above, removing the restriction $p > l_1^d$ in the definition of $\omega_1(n)$ for those integers $n \in V_k(N)$ for which $\omega_2(n) \le D$ changes $G(z)$

by an amount which is $\ll_L l_3 l_2^{-1/2}$. Thus it suffices to show that, for L large enough, the frequency of the integers n with $\omega_2(n) > D$ amongst the elements of $V_k(N)$ is $\ll l_3 l_2^{-1}$:

$$|\{n : \omega_2(n) > D,\ n \in V_k(N)\}| \ll_{g,K} l_3 l_2^{-1} |V_k(N)|. \tag{6.25}$$

Set $S = \{n : \omega_2(n) > D, n \in V_k(N)\}$, and let $\mathcal{E}$ denote the set of the integers e which are composed of D distinct prime factors not exceeding l_1^d:

$$e = p_1 \ldots p_D, \qquad p_1 < \ldots < p_D \le l_1^d.$$

Clearly, $n \in S$ implies that there is an $e \in \mathcal{E}$ with e/n so that

$$|S| \le \sum_{e \in \mathcal{E}} |\{n : n \in V_k(N),\ n \equiv 0 \pmod e\}|. \tag{6.26}$$

If $e \in \mathcal{E}$ then for fixed L and $N \to \infty$,

$$e \le (l_1^d)^D \le \exp(Ldl_2l_3) = \exp(o(l^{1/2})) = \exp(o(k^{1/2}))$$

so that by Theorem 2 we have

$$\begin{aligned} &|\{n : n \in V_k(N),\ n \equiv 0 \pmod e\}| \\ &\qquad < \frac{1}{e}|V_k(N)|\left(1 + c_7 \exp\left(-c_8 \frac{k}{\log e}\right)\right) \\ &\qquad = (1 + o(1))\frac{1}{e}|V_k(N)| < \frac{2}{e}|V_k(N)|. \end{aligned} \tag{6.27}$$

It follows from (6.26) and (6.27) that

$$\begin{aligned} |S| &< 2|V_k(N)| \sum_{e \in \mathcal{E}} \frac{1}{e} \\ &= 2|V_k(N)| \sum_{p_1 < \ldots < P_D \le l_1^d} \frac{1}{p_1 \ldots p_D} \\ &\le 2|V_k(N)| \frac{1}{D!}\left(\sum_{p \le l_1^d} \frac{1}{p}\right)^D < 2|V_k(N)|\left(\frac{e(l_3 + O(1))}{D}\right)^D \\ &= 2|V_k(N)| \exp((1 + l_4 + o(1) - \log D)D) \\ &= |V_K(N)| \exp((1 - \log L + o(1))Ll_3). \end{aligned}$$

Choosing $L = 10$, for large N we obtain

$$|S| < l_2^{-10} |V_k(N)|,$$

which proves (6.25) and completes the proof of Theorem 4.

References

[Ell] P. D. T. A. Elliott, *Probabilistic Number Theory*, *I*, *Mean-Value Theorems*, Grundlehren Math. Wiss. 239, Springer, 1979.

[Ell-S] P. D. T. A. Elliott and A. Sárközy, *The distribution of the number of prime divisors of sums* $a+b$, J. Number Theory 29 (1988), 94–99.

[Er-P-S-S] P. Erdős, C. Pomerance, A. Sárközy and C. L. Stewart, *On elements of sumsets with many prime factors*, ibid. 44 (1993), 93–104.

[Ess] C. G. Esseen, *Fourier analysis of distribution functions. A mathematical study of Laplace–Gaussian law*, Acta Math. 77 (1945), 1–125.

[Fin] M. N. J. Fine, *The distribution of the sum of digits* (*mod* p), Bull. Amer. Math. Soc. 71 (1965), 2651–2652.

[F-M1] E. Fouvry et C. Mauduit, *Somme des chiffres et nombres presque premiers*, Math. Ann. 305 (1996), 571–599.

[F-M2] —, —, *Crible asymptotique de Bombieri et somme des chiffres*, preprint.

[Gel] A. O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. 13 (1968), 259–265.

[Mau] C. Mauduit, *Substitutions et ensembles normaux*, Habilitation Dir. Rech., Université Aix-Marseille II, 1989.

[M-S] C. Mauduit and A. Sárközy, *On the arithmetic structure of sets characterized by sum of digits properties*, J. Number Theory 61 (1996), 25–38.

[Mon] H. L. Montgomery, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. 84 (1978), 547–567.

[P-S] G. Pólya and G. Szegő, *Problems and Theorems in Analysis*, *II*, Grundlehren Math. Wiss. 216, Springer, 1976.

[S-S] A. Sárközy and C. L. Stewart, *On divisors of sums of integers*, V, Pacific J. Math. 166 (1994), 373–384.

[Ten] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Publ. Inst. Elie Cartan, 13, 1990.

Laboratoire de Mathématiques Discrètes
CNRS - UPR 9016
163, Avenue de Luminy
F13288 Marseille Cedex 9, France
E-mail: mauduit@lmd.univ-mrs.fr

Department of Algebra and Number Theory
Eötvös Loránd University
H-1088 Budapest, Múzeum krt. 6-8, Hungary
E-mail: sarkozy@cs.elte.hu

Received on 15.1.1996 (2914)