Journal of Number Theory **70**, 99–120 (1998)
Article No. NT982229

On Arithmetic Properties of Integers with Missing Digits I: Distribution in Residue Classes

Paul Erdős*

Mathematical Institute of the Hungarian Academy of Science, H-1053 Budapest, Reáltanoda u. 13–15, Hungary

Christian Mauduit

Institut de Mathématiques de Luminy, CNRS-UPR9016, 163 av. de Luminy, case 907, F-13288 Marseille Cedex 9, France

and

Department of Algebra and Number Theory, Eötvös Loránd University, H-1088 Budapest, Muzeum krt. 6–8, Hungary

Communicated by Alan C. Woods

Received July 18, 1996

Consider all the integers not exceeding x with the property that in the system number to base g all their digits belong to a given set $\mathscr{D} \subset \{0, 1, ..., g, -1\}$. The distribution of these integers in residue classes to "not very large" moduli is studied.

SECTION 1

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

* Research partially supported by Hungarian National Foundation for Scientific Research, Grant 1901 and CEE fund CIPA-CT92-4022. This paper was written when the first and the third authors were visiting the Laboratoire de Mathématiques Discrètes (UPR 9016 CNRS), Marseille.

0022-314X/98 $25.00

distinct prime factors of n and by $\Omega(n)$ the number of prime factors of n counted with multiplicity. The greatest prime factor of the integers n will be denoted by $P(n)$ and $\varphi(n)$ is Euler's function. If α is a real number, we write $e(\alpha) = e^{2i\pi\alpha}$ and $\|\alpha\| = d(\alpha, \mathbb{Z})$ the distance of α to the closest integer.

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

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

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

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

we write

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

For $N \in \mathbb{N}$, $m \in \mathbb{N}$, $r \in \mathbb{Z}$ we write

$$\mathcal{U}_{(m,r)}(N) = \{n : n \leqslant N,\ S(n) \equiv r \pmod{m}\}.$$

The arithmetic structure of the sets $\mathcal{U}_{m,r}(N)$ has been studied by Gelfond [GEL]. His main result which extends an earlier result of Fine [FIN] is the following:

RU 1. *If $m \in \mathbb{N}$ is fixed with*

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

then for all $r \in \mathbb{Z}$ and all "small" $q \in \mathbb{N}$. the set $\mathcal{U}_{(m,r)}(N)$ is well-distributed in the residue classes modulo q.

As an application of the result above, Gelfond estimated the number of "z-free" elements of $\mathcal{U}_{(m,r)}(N)$:

(RU 2) 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 $N \to +\infty$ Gelfond [GEL] gave an asymptotics for the member of elements of $\mathcal{U}_{(m,r)}(N)$ which are not divisible by the zth power of a prime.

In [MS1] we studied further arithmetic properties of the elements of the sets $\mathcal{U}_{(m,r)}(N)$. But one might think that these results are not very much surprising since the sets $\mathcal{U}_{(m,r)}(N)$ are of "positive density" and would like to study "thinner" sets characterized by digit properties and to see whether still the same conclusion holds.

Indeed, in [MS2] we introduced the sets $\mathcal{V}_k(N)$ defined in the following way: if $g \in \mathbb{N}$, $g \geqslant 2$, $N \in \mathbb{N}$, $k \in \mathbb{N}$, $0 \leqslant k \leqslant (g-1)(\log N/\log g + 1)$, then let

$$\mathcal{V}_k = \mathcal{V}_k(N) = \{n: n \leqslant N, S(n) = k\}$$

(where again, $S(n)$ denotes the sum of the digits in the number system to base g). We showed that for every k we have

$$|\mathcal{V}_k(N)| \ll_g N(\log N)^{-1/2}$$

so that, in fact, the sets $\mathcal{V}_k$ are much thinner than the sets $\mathcal{U}_{(m,r)}$. In [MS2] we proved analogs of the resuts (RU 1) and (RU 2) with the sets $\mathcal{V}_k$ in place of the sets $\mathcal{U}_{(m,r)}$:

RV 1. *If* $g \in \mathbb{N}$, $g \geqslant 2$, $k \in \mathbb{N}$, $0 < k < (g-1)(\log N/\log g + 1)$,

$$\min\left(k, (g-1)\frac{\log N}{\log k} - k\right) \to +\infty,$$

$m \in \mathbb{N}$ *and* m *is "small," then* $\mathcal{V}_k$ *is well-distributed in the residue classes modulo* m.

As an application of this result, (RV 2) a $\mathcal{V}$-analog of (RU 2) is given in [MS2].

Several other arithmetic properties of the sets $\mathcal{U}_{(m,r)}$ and $\mathcal{V}_k$ are given in [MS1], [MS2].

SECTION 2

In this paper, our goal is to study even thinner sets characterized by digit properties. Indeed, while $|\mathcal{U}_{(m,r)}(N)| \gg N$ and

$$\max_k |\mathcal{V}_k(N)| \geqslant N(\log N)^{-1/2},$$

here our goal is to study sets with cardinality $< N^{1-\varepsilon}$. The most natural way to construct such a set via digit properties is to consider integers with missing digits. In other words, let

$$g \in \mathbb{N}, \qquad g \geqslant 3, \qquad t \in \mathbb{N}, \qquad 2 \leqslant t \leqslant g-1, \tag{2.1}$$

$$\mathcal{D} \subset \{0, 1, ..., g-1\}, \qquad 0 \in \mathcal{D}, \qquad |\mathcal{D}| = t, \tag{2.2}$$

and let $\mathscr{W}_{\mathscr{D}}(N)$ denote the set of the integers n such that $0 \leqslant n \leqslant N$ and representing n in the number system to base g:

$$n = \sum_{j=0}^{\nu} a_j g^j, \qquad 0 \leqslant a_j \leqslant g-1, \tag{2.3}$$

where now

$$g^{\nu} \leqslant N < g^{\nu+1}, \tag{2.4}$$

we have

$$a_j \in \mathscr{D} \qquad \text{for} \quad j = 0, 1, ..., \nu.$$

(Note that the assumption $0 \in \mathscr{D}$ is not necessary, but it makes the discussion slightly simpler, besides the general case can be reduced to this one.) Sets of the type $\mathscr{W}_{\mathscr{D}}(N)$ have been studied in [COQ1], [COQ2], [COQ3], [FK], [MAU]. Here our goal is to prove analogs of the results (RU 1), (RU 2), (RV 1), (RV 2) for the sets $\mathscr{W}_{\mathscr{D}}$. The study of the analogs of the other arithmetic properties studied in [MS1], [MS2] with the sets $\mathscr{W}_{\mathscr{D}}$ in place of the sets $\mathscr{U}_{(m, r)}$ or $\mathscr{V}_k$ will appear in a further paper.

First we will prove the $\mathscr{W}$-analog of the results (RU 1), (RV 1):

THEOREM 1. *If g and t satisfy* (2.1), *then there exist positive constants $c_1 = c_1(g, t)$, $c_2 = c_2(g, t)$, $c_3 = c_3(g, t)$ such that if also* (2.2) *holds, and writing $\mathscr{D} = \{d_1, d_2, ..., d_t\}$ where $d_1 = 0$, we have*

$$(d_2, ..., d_t) = 1, \tag{2.5}$$

moreover, $N \in \mathbb{N}$, $m \in \mathbb{N}$, $m \geqslant 2$, $((g-1)\, g, m) = 1$,

$$m < \exp(c_1 (\log N)^{1/2}) \tag{2.6}$$

and $h \in \mathbb{Z}$, then

$$\left| |\{n: n \in \mathscr{W}_{\mathscr{D}}(N), n \equiv h (\bmod m)\}| - \frac{1}{m} |\mathscr{W}_{\mathscr{D}}(N)| \right|$$
$$< c_2 \frac{1}{m} |\mathscr{W}_{\mathscr{D}}(N)| \exp\left(-c_3 \frac{\log N}{\log m}\right). \tag{2.7}$$

(Note that the condition (2.5) is necessary since $(d_2, ..., d_t)$ divides every element of $\mathscr{W}_{\mathscr{D}}(N)$.)

By Theorem 1, the set $\mathscr{W}_{\mathscr{D}}(N)$ is well-distributed in the modulo m residue classes if $m < \exp(c(g, t)(\log N)^{1/2})$. It follows that for such an m, $\mathscr{W}_{\mathscr{D}}(N)$ meets every residue class modulo m. One may ask the question that how large can m be with this property? We will prove the following theorem in this direction:

THEOREM 2. *If g, t satisfy (2.1), then there is an effectively computable number $N_0 = N_0(g, t)$ such that if $\mathscr{D} \subset \{0, 1, ..., g-1\}$, $|\mathscr{D}| = t$, $N > N_0$, then there is a prime p with the following properties: writing*

$$k = \left[2 \frac{\log g}{\log t} \right] + 1,$$

we have

$$p > N^{(\log t)/2(k \log g)},$$

and $\mathscr{W}_{\mathscr{D}}(N)$ meets every residue class modulo p.

From the opposite direction, one might like to show that there exist relatively small moduli m (small in terms of $|\mathscr{W}_{\mathscr{D}}(N)|$) such that $\mathscr{W}_{\mathscr{D}}(N)$ does not meet residue class modulo m. If $m > |\mathscr{W}_{\mathscr{D}}(N)|$ then this is clearly so. We will improve on this trivial bound considerably:

THEOREM 3. *Let $\varepsilon > 0$. Then there is a number $g_0 = g_0(\varepsilon)$ such that if $g \in \mathbb{N}$, $g > g_0$ and $\mathscr{D} = \{0, 1\}$, then for infinitely many $N \in \mathbb{N}$ there is an $m \in \mathbb{N}$ such that $gcd(m, g) = 1$,*

$$m < |\mathscr{W}_{\mathscr{D}}(N)|^{\varepsilon} \tag{2.8}$$

and $\mathscr{W}_{\mathscr{D}}(N)$ does not meet every residue class modulo m.

(Indeed, it will turn out that $\mathscr{W}_{\mathscr{D}}(N)$ meets only "few" residue classes modulo m.)

One can apply Theorem 1 to prove the $\mathscr{W}$-analog of (RU 2), (RV 2):

THEOREM 4. *If $g, t, \mathscr{D}$ are defined as in Theorem 1, and $z \in \mathbb{N}$,*

$$z > \frac{\log g}{\log t}, \tag{2.9}$$

then there are effectively computable constants N_0, c_4 (both depending on g, t and z only) such that if $N > N_0$, then the number $T_z(N)$ of those integers n with $n \in \mathscr{W}_{\mathscr{D}}(N)$ which are not divisible by the zth power of a prime p with $((g-1)g, p) = 1$ is

$$T_z(N)=\left(\xi(z)\prod_{p\mid(g-1)g}\left(1-\frac{1}{p^z}\right)\right)^{-1}|\mathcal{W}_{\mathcal{D}}(N)|$$
$$\times\left(1+O_{g,\,t,\,z}\left(\exp\left(-c_4(\log N)^{1/2}\left(\frac{\log t}{\log g}-\frac{1}{z}\right)\right)\right)\right) \quad (2.10)$$

Note that we have no asymptotics for $T_z(N)$ if (2.9) does not hold. Thus, e.g., we have not been able to settle the following problem:

Problem 1. Is it true that if $g\in\mathbb{N}$, $g\geqslant 6$ then there are infinitely many square-free integers such that every digit of them in the number system to base g is 0 or 1?

Note that for $g=3, 4$ and 5 this has been proved by Filaseta and Konyagin in [FK], and the $g=3$ special case also follows from Theorem 4 above.

By Theorem 4, if $\log t/\log g$ is "large" then there are many integers free of zth powers in $\mathcal{W}_{\mathcal{D}}(N)$. One might like to prove the opposite statement, i.e., that there are integers with large zth power part in $\mathcal{W}_{\mathcal{D}}(N)$. Indeed, if g, t, $\mathcal{D}$ are defined as in Theorem 1, $z\in\mathbb{N}$ and $z\geqslant 2$, then by Theorem 1, for large n $\mathcal{W}_{\mathcal{D}}(N)$ contains integers with zth power part greater than $\exp(c(\log N)^{1/2})$. We will show that if t is close enough to g and z is small enough in terms of t and g then $\mathcal{W}_{\mathcal{D}}(N)$ contains integers with zth power parts as large as N^c (with $c=c(g, t, z)$):

THEOREM 5. *If g, t, $\mathcal{D}$ satisfy* (2.1) *and* (2.2), *and $z\in\mathbb{N}$,*

$$z<\left(2\left(1-\frac{\log t}{\log g}\right)\right)^{-1}, \quad (2.11)$$

then there are effectively computable constants $N_0=N_0(g; t; z)$ and $c_5=c_5(g; t; z)$ such that if $N>N_0$ then there is a positive integer n and a prime p with

$$n\in\mathcal{W}_{\mathcal{D}}(N), \qquad p>c_5\left(\frac{N^{(\log t)/(2\log g)}}{\log N}\right)^{1/(2z-1)}$$

and

$$p^z\mid n.$$

Thus, e.g., if $\log t/\log g>\frac{3}{4}$ then there are integers with large prime square part in $\mathcal{W}_{\mathcal{D}}(N)$. On the other hand, we have not been able to settle the following question:

Problem 2. Is it true that if $g\in\mathbb{N}$, $g\geqslant 3$ then there is a constant $c=c(g)$ with the following property: there are infinitely many integers n such that every digit of them in the number system to base g is 0 or 1, and there is a prime with $p > n^c$, $p^2 | n$?

SECTION 3

Three Lemmas. To prove Theorem 1 we shall need three lemmas.

LEMMA 1. *If g, t and $\mathcal{D}$ are defined as in Theorem* 1 *and $\alpha \in \mathbb{R}$, then there is an integer j such that $2 \leqslant j \leqslant t$ and*

$$\|d_j \alpha\| \geqslant \frac{1}{2(g-1)^2} \|\alpha\|. \tag{3.1}$$

Proof of Lemma 1. We have to distinguish two cases.

Case 1. Assume that

$$\|\alpha\| \leqslant \frac{1}{2(g-1)},$$

i.e., α can be written in the form

$$\alpha = k + \theta_1$$

with $k \in \mathbb{Z}$ and

$$|\theta_1| = \|\alpha\| \leqslant \frac{1}{2(g-1)}. \tag{3.2}$$

Then we have

$$d_2 \alpha = d_2 k + d_2 \theta_1 = d_2 k + \theta_2 \tag{3.3}$$

where, in view of (3.2),

$$|\theta_2| = |d_2 \theta_1| = d_2 \, |\theta_1| \leqslant (g-1) \frac{1}{2(g-1)} = \frac{1}{2}. \tag{3.4}$$

It follows from (3.3) and (3.4) that

$$\|d_2 \alpha\| = |\theta_2| = |d_2 \theta_1|$$

so that

$$\|d_2 \alpha\| = d_2 \, |\theta_1| \geqslant |\theta_1| = \|\alpha\|$$

which implies (3.1) with 2 in place of j.

Case 2. Assume now that

$$\|\alpha\| > \frac{1}{2(g-1)}. \tag{3.5}$$

If

$$\|d_2\alpha\| \geqslant \frac{1}{2(g-1)^2},$$

then (3.1) holds with $j=2$; thus we may assume that

$$\|d_2\alpha\| < \frac{1}{2(g-1)},$$

i.e., $d_2\alpha$ can be written in the form

$$d_2\alpha = l + \theta_3 \tag{3.6}$$

with $l \in \mathbb{Z}$ and

$$|\theta_3| < \frac{1}{2(g-1)^2}. \tag{3.7}$$

Dividing (3.6) by d_2 we obtain

$$\alpha = \frac{l}{d_2} + \frac{\theta_3}{d_2}. \tag{3.8}$$

If $d_2 \mid l$ then this implies

$$\|\alpha\| \leqslant \frac{|\theta_3|}{d_2} \leqslant |\theta_3| < \frac{1}{2(g-1)^2}$$

which contradicts (3.5). It follows that $d_2 \nmid l$ so that writing l/d_2 in the form

$$\frac{l}{d_2} = \frac{u}{v}, \qquad u \in \mathbb{Z}, \quad v \in \mathbb{N}, \quad (u, v) = 1, \tag{3.9}$$

here we have

$$v > 1 \tag{3.10}$$

and

$$v \leqslant d_2 \leqslant g-1. \tag{3.11}$$

Then by (2.5) and (3.10) there is a j such that $j \in \{2, 3, ..., t\}$ and $v \nmid d_j$ whence, by (3.8), (3.9), (3.10) and (3.11),

$$\|d_j \alpha\| = \left\| d_j \left(\frac{u}{v} + \frac{\theta_3}{d_2} \right) \right\| \geqslant \left\| \frac{d_j u}{v} \right\| - \frac{d_j}{d_2} |\theta_3|$$

$$\geqslant \frac{1}{v} - (g-1) \frac{1}{2(g-1)^2} \geqslant \frac{1}{g-1} - \frac{1}{2(g-1)}$$

$$= \frac{1}{2(g-1)}$$

so that (3.1) holds and this completes the proof of Lemma 1.

Write

$$u(\alpha) = u_{\mathscr{D}}(\alpha) = \sum_{k=1}^{t} e(d_k \alpha)$$

and

$$\mathscr{U}(\alpha) = \mathscr{U}_{\mathscr{D}}(\alpha) = \frac{u_{\mathscr{D}}(\alpha)}{t}.$$

LEMMA 2. *If* $g, t, \mathscr{D}, \alpha$ *are defined as in Lemma* 1 *then we have*

$$|\mathscr{U}(\alpha)| \leqslant 1 - \frac{1}{(g-1)^5} \|\alpha\|^2.$$

Proof of Lemma 2. By Lemma 1 there is a j satisfying $2 \leqslant j \leqslant t$ and (3.1). Then we have

$$|\mathscr{U}(\alpha)| = \frac{1}{t} \left| \sum_{k=1}^{t} e(d_k \alpha) \right| \leqslant \frac{1}{t} \left(|e(d_1 \alpha) + e(d_1 \alpha)| + \left| \sum_{\substack{2 \leqslant k \leqslant t \\ k \neq j}} e(d_k \alpha) \right| \right)$$

$$\leqslant \frac{1}{t} (|1 + e(d_j \alpha)| + (t-2)) \tag{3.12}$$

For all $\beta \in \mathbb{R}$ we have

$$|1 + e(\beta)|^2 = 2 + 2 \cos 2\pi\beta = 4(1 - \sin^2 \pi\beta)$$

$$\leqslant 4(1 - (2 \|\beta\|)^2) = 4(1 - 4 \|\beta\|^2)$$

whence

$$|1+e(\beta)| \leqslant 2(1-4\ \|\beta\|^2)^{1/2} \leqslant 2(1-2\ \|\beta\|^2).$$

Thus it follows from (3.1) and (3.12) that

$$|\mathscr{U}(\alpha)| \leqslant \frac{1}{t}\,(2(1-2\ \|d_j\alpha\|^2)+(t-2)) = 1-\frac{4}{t}\ \|d_j\alpha\|^2$$

$$\leqslant 1-\frac{4}{g-1}\left(\frac{1}{2(g-1)^2}\ \|\alpha\|\right)^2 = 1-\frac{1}{(g-1)^5}\ \|\alpha\|^2$$

which completes the proof of Lemma 2.

LEMMA 3. *If* $g, m, j, \rho \in \mathbb{N}$, $g \geqslant 2$, $((g-1)g, m)=1$, $m \geqslant 2$, $1 \leqslant j \leqslant m-1$,

$$\rho \geqslant 2\,\frac{\log m}{\log g}+8 \tag{3.13}$$

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

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

Proof of Lemma 3. This is Lemma 2 in [MS2].

SECTION 4

Proof of Theorem 1. Consider the generating function

$$G(\alpha)=\sum_{n \in \mathscr{W}_{\mathscr{D}}(N)} e(n\alpha)$$

so that

$$G(0)=|\mathscr{W}_{\mathscr{D}}(N)| \tag{4.1}$$

and for all $h \in \mathbb{Z}$, $m \in \mathbb{N}$ we have

$$|\{n\colon n \in \mathscr{W}_{\mathscr{D}}(N),\ n \equiv h(\operatorname{mod} m)\}| = \frac{1}{m}\sum_{j=0}^{m-1} e\left(-\frac{hj}{m}\right) G\left(\frac{j}{m}\right). \tag{4.2}$$

It follows from (4.1) and (4.2) that

$$\left| |\{n\colon n \in \mathscr{W}_{\mathscr{D}}(N), n \equiv h (\text{mod } m)\}| - \frac{1}{m} |\mathscr{W}_{\mathscr{D}}(N)| \right|$$

$$= \left| |\{n\colon n \in \mathscr{W}_{\mathscr{D}}(N), n \equiv h (\text{mod } m)\}| - \frac{1}{m} G(0) \right|$$

$$\leqslant \frac{1}{m} \sum_{j=1}^{m-1} \left| G\left(\frac{j}{m}\right) \right| \tag{4.3}$$

so that it remains to estimate $|G(j/m)|$ for

$$j \in \{1, 2, ..., m-1\}. \tag{4.4}$$

As in [MS2], write N in the form

$$N = \sum_{j=1}^{s} b_j g^{\nu_j},$$

$$\nu_1 > \nu_2 > \cdots > \nu_s, \qquad b_j \in \{1, 2, ..., g-1\} \qquad \text{for} \quad j = 1, 2, ..., s$$

so that

$$g^{\nu_1} \leqslant N < g^{\nu_1 + 1}$$

whence

$$\nu_1 = \left[\frac{\log N}{\log g}\right].$$

Moreover, for $l = 1, 2, ..., s$, let $\mathscr{A}_l$ denote the set of the integers n that can be represented in the form

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

where

$$x \in \mathscr{D} \cap \{0, 1, ..., b_l - 1\}, \qquad y_u \in \mathscr{D} \qquad \text{for} \quad u = 0, 1, ..., \nu_l - 1,$$

and let

$$\mathscr{A}_{s+1} = \begin{cases} \{N\} & \text{if} \quad N \in \mathscr{W}_{\mathscr{D}}(N) \\ \varnothing & \text{if} \quad N \notin \mathscr{W}_{\mathscr{D}}(N). \end{cases}$$

Then clearly we have

$$\mathscr{W}_{\mathscr{D}}(N)=\bigcup_{i=1}^{s+1}\mathscr{A}_l$$

and

$$\mathscr{A}_1\cap\mathscr{A}_l=\varnothing \qquad \text{for} \quad 1\leqslant j<l\leqslant s+1$$

so that for all $\alpha\in\mathbb{R}$,

$$G_l(\alpha)=\sum_{n\in\mathscr{W}_{\mathscr{D}}(N)}e(n\alpha)=\sum_{l=1}^{s+1}\sum_{n\in\mathscr{A}_l}e(n\alpha)=\sum_{l=1}^{s+1}G_l(\alpha). \tag{4.5}$$

Here for $1\leqslant l\leqslant s$ we have

$$\begin{aligned}G_l(\alpha)=&\sum_{x}\sum_{y_0}\cdots\sum_{y_{v_l-1}}e((b_1g^{v_1}+\cdots+b_{l-1}g^{v_{l-1}}+xg_l^v+y_0g^0\\&+\cdots+y_{v_l-1}g^{v_l+1})\alpha)\\&=e(b_1g^{v_1}+\cdots+b_{l-1}g^{v_{l-1}}\Bigg(\sum_{x\in\mathscr{D}\cap\{0,1,...,b_{l-1}\}}e(xg^{v_l})\Bigg)\\&\times\prod_{u=0}^{v_l-1}\Bigg(\sum_{y_u\in\mathscr{D}}e(y_ug^u\alpha)\Bigg)\\&=e(b_1g^{v_1}+\cdots+b_{l-1}g^{v_{l-1}})\Bigg(\sum_{x\in\mathscr{D}\cap\{0,1,...,b_{l-1}\}}e(xg^{v_l})\Bigg)\prod_{u=0}^{v_l-1}u_{\mathscr{D}}(g^u\alpha)\end{aligned}$$

whence

$$|G_l(\alpha)|\leqslant|\mathscr{D}|\prod_{u=0}^{v_l-1}|u_{\mathscr{D}}(g^u\alpha)|\leqslant gt^{v_l}\prod_{u=0}^{v_l-1}|\mathscr{U}_{\mathscr{D}}(g^u\alpha)|. \tag{4.6}$$

Thus by $t\geqslant 2$ we have

$$\begin{aligned}\sum_{l:\,v_l\leqslant 1/2\log N/\log g}|G_l(\alpha)|&\leqslant\sum_{l:\,v_l\leqslant 1/2\log N/\log g}gt^{v_l}\prod_{u=0}^{v_l-1}1<g\sum_{j=0}^{+\infty}t^{(\log N)/(2\log g)-j}\\&\leqslant 2gt^{(\log N)/(2\log g)-j}<2g(t^{v_1+1})^{1/2}<2g^2(t^{v_1})^{1/2}\\&\leqslant 2g^2\,|\mathscr{W}_{\mathscr{D}}(N)|^{1/2} \qquad (\text{for }\alpha\in\mathbb{R})\end{aligned} \tag{4.7}$$

since clearly

$$|\mathscr{W}_{\mathscr{D}}(N)|\geqslant t^{v_1}. \tag{4.8}$$

If $v_l > \frac{1}{2} \log N/\log g$, then by (2.6),

$$v_l > \frac{1}{2}\frac{\log N}{\log g} > 2\frac{\log m}{\log g} + 8$$

so that (3.13) holds with v_l in place of ρ. Thus using Lemma 2 and 3, by (4.6) and $1 - x \leqslant e^{-x}$ (for $x \geqslant 0$) for $l \leqslant s$, $v_l > \frac{1}{2} \log N/\log g$, $1 \leqslant j \leqslant m-1$ we have

$$\begin{aligned}\left|G_l\left(\frac{j}{m}\right)\right| &\leqslant g t^{v_l} \prod_{u=0}^{v_l-1}\left(1 - \frac{1}{(g-1)^5}\left\|g^u \frac{j}{m}\right\|^2\right)\\ &\leqslant g t^{v_l} \exp\left(-\frac{1}{(g-1)^5}\sum_{u=0}^{v_l-1}\left\|g^u \frac{j}{m}\right\|^2\right)\\ &\leqslant g t^{v_l} \exp\left(-\frac{1}{128 g^4 (g-1)^3}\frac{v_l}{\log m}\right)\\ &\leqslant g t^{v_l} \exp\left(-\frac{1}{256 g^4 (g-1)^3 \log g}\frac{\log N}{\log m}\right)\end{aligned}$$

whence, by (2.1), (2.6) and (4.8),

$$\begin{aligned}\sum_{\substack{l \leqslant s\\ v_l > 1/2 \log N/\log g}} \left|G_l\left(\frac{j}{m}\right)\right| &\leqslant g \exp\left(-\frac{\log N}{c_{10} \log m}\right)\sum_{j=0}^{+\infty} t^{v_1 - j}\\ &\leqslant t^{v_1} \exp\left(-\frac{\log N}{c_{11} \log m}\right)\\ &\leqslant |\mathscr{W}_{\mathscr{D}}(N)| \exp\left(-\frac{\log N}{c_{11} \log m}\right)\\ &\qquad \text{for} \quad j \in \{1, 2, ..., m-1\} \qquad (4.9)\end{aligned}$$

(where c_{10}, c_{11} depend on g and t). Finally, clearly we have

$$|G_{s+1}(\alpha)| = \left|\sum_{n \in \mathscr{A}_{s+1}} e(n\alpha)\right| \leqslant \sum_{n \in \mathscr{A}_{s+1}} 1 = |\mathscr{A}_{s+1}| \leqslant 1 \qquad (\text{for } \alpha \in \mathbb{R}). \qquad (4.10)$$

It follows from (4.5, (4.7), (4.9) and (4.10) that for j satisfying (4.4) we have

$$\left|G\left(\frac{j}{m}\right)\right| \leqslant 2g^2 \, |\mathscr{W}_{\mathscr{D}}(N)|^{1/2} + |\mathscr{W}_{\mathscr{D}}(N)| \exp\left(-\frac{\log N}{c_{11} \log m}\right) + 1$$

$$= \frac{1}{m} \, |\mathscr{W}_{\mathscr{D}}(N)| \, (2mg^2) \, |\mathscr{W}_{\mathscr{D}}(N)|^{-1/2}$$

$$+ m \exp\left(-\frac{\log N}{c_{11} \log_m}\right) + m \, |\mathscr{W}_{\mathscr{D}}(N)|^{-1}) \tag{4.11}$$

By $t \geqslant 2$ and (4.8), there are positive constants $c_{12} = c_{12}(g)$ and $c_{13} = c_{13}(g)$ such that

$$|\mathscr{W}_{\mathscr{D}}(N)| \geqslant t^{\nu_1} \geqslant 2^{[(\log N)/\log g)]} > c_{12} N^{c_{13}}. \tag{4.12}$$

If c_1 in (2.6) is chosen small enough, then (2.7) follows from (2.6), (4.3), (4.11) and (4.12), and this completes the proof of Theorem 1.

SECTION 5

Proof of Theorem 2. The proof will be based on the Cauchy–Davenport lemma and Gallagher's "larger sieve:"

LEMMA 4 ([DAV1], [DAV2]). *Let p be a prime number and let $\mathscr{A}$ and $\mathscr{B}$ sets of distinct modulo p residue classes: $\mathscr{A}$ and $\mathscr{B} \in \mathbb{Z}_p$. Then*

$$|\mathscr{A} + \mathscr{B}| \geqslant \min(|\mathscr{A}| + |\mathscr{B}| - 1, \, p)$$

(*where* $\mathscr{A} + \mathscr{B} = \{a + b\colon a \in \mathscr{A}, \, b \in \mathscr{B}\}$).

If $\mathscr{A} \subset \mathbb{Z}$, $m \in \mathbb{N}$ then let $\nu(\mathscr{A}, m)$ denote the number of residue classes modulo $m$that contain at least one element of $\mathscr{A}$.

LEMMA 5 ([GAL]). *Let $M \in \mathbb{R}$, $N \in \mathbb{N}$ and let $\mathscr{A}$ be a set of integers in the interval $[M+1, M+N]$. Then for any finite set of primes S we have*

$$|\mathscr{A}| \leqslant \frac{\sum_{p \in S} \log p - \log N}{\sum_{p \in S} (\log p / \nu(\mathscr{A}, p)) - \log p}$$

provided that the denominator is positive.

Write

$$\delta = \frac{\log t}{2 \log g} - \frac{1}{k}$$

so that

$$\delta > 0 \tag{5.1}$$

by the definition of k, and set

$$x = \left[\frac{\log N}{k \log g} \right]$$

so that

$$g^x \leqslant N^{1/k} < g^{x+1}. \tag{5.2}$$

Finally, write

$$y = N^{(\log t)/(2k \log g)}. \tag{5.3}$$

We start out the indirect assumption that there is no p with $y < p \leqslant y^2$ such that $\mathscr{W}_{\mathscr{D}}(N)$ meets every residue class modulo p:

$$\nu(\mathscr{W}_{\mathscr{D}}(N), p) < p \qquad \text{for all} \quad y < p \leqslant y^2. \tag{5.4}$$

For $j = 1, 2, ..., k$, write

$$\mathscr{A}_j = \{(g^x)^{j-1} n \colon n \in \mathscr{W}_{\mathscr{D}}(g^x - 1)\}$$

so that, in view of (5.2),

$$\sum_{j=1}^{k} \mathscr{A}_j \subset \mathscr{W}_{\mathscr{D}}(N), \tag{5.5}$$

and clearly,

$$\nu(\mathscr{A}_j, p) = \nu(\mathscr{W}_{\mathscr{D}}(g^x - 1), p) \tag{5.6}$$

for $j \in \{1, 2, ..., k\}$ and all $p > g$.

By the Cauchy–Davenport lemma (Lemma 4) it follows from (5.4), (5.5) and (5.6) that

$$\begin{aligned} p > \nu(\mathscr{W}_{\mathscr{D}}(N), p) &\geqslant \nu\left(\sum_{j=1}^{k} \mathscr{A}_j, p \right) \geqslant \sum_{j=1}^{k} \nu(\mathscr{A}_j, p) - (k-1) \\ &= k\nu(\mathscr{W}_{\mathscr{D}}(g^x - 1), p) - (k-1) \end{aligned}$$

whence

$$\nu(\mathcal{W}_{\mathcal{D}}(g^x-1), p)<\frac{p}{k}+1 \qquad (\text{for all } y<p\leqslant y^2).$$

Thus by using Gallagher's "larger sieve" (Lemma 5) with -1, g^x, $\mathcal{W}_{\mathcal{D}}(g^x-1)$ and $\{p\colon p\text{prime},\ y<p\leqslant y^2\}$ in place of M, N, $\mathcal{A}$ and S, respectively, by the prime number theorem and since

$$\sum_{p\leqslant u}\frac{\log p}{p}=\log u+O(1),$$

in view of (5.2) and (5.3) we obtain for $N\to+\infty$ that

$$\begin{aligned}|\mathcal{W}_{\mathcal{D}}(g^x-1)|&\leqslant\frac{\sum_{y<p\leqslant y^2}\log p-\log g^x}{\sum_{y<p\leqslant y^2}(\log p/(p/k)+1)-\log g^x}\\&=\frac{1+o(1))\ y^2-(\log N)/k+O(1)}{(1+o(1))k\log y-(\log N)/k+O(1)}\\&=\frac{(1+o(1))\ N^{(\log t)/(k\log g)}}{(1+o(1))\ \delta\log N+O(1)}\end{aligned}$$

where, by (5.1), indeed the denominator is positive for large N. By (5.2), it follows that

$$|\mathcal{W}_{\mathcal{D}}(g^x-1)|=O_{g,t}\left(\frac{(g^x)^{(\log t)/(\log g)}}{\log N}\right)=O_{g,t}\left(\frac{t^x}{\log N}\right) \tag{5.7}$$

On the other hand, clearly we have

$$|\mathcal{W}_{\mathcal{D}}(g^x-1)|=t^x$$

which contradicts (5.7), and this contradiction completes the proof of the theorem.

SECTION 6

Proof of Theorem 3. Let g be a (fixed) positive integer large enough in terms of ε and let $k\in\mathbb{N}$. Write $N=g^{(g-2)k}-1$ and $m=g^k-1$ so that

$$|\mathcal{W}_{\mathcal{D}}(N)|=2^{(g-2)k}$$

(with $\mathscr{D}=\{0, 1\}$) whence, for $k \to +\infty$,

$$m = g^k - 1 = (1+o(1))|\mathscr{W}_{\mathscr{D}}(N)|^{(\log g)/((g-1)(\log 2))}.$$

If $g > g_0(\varepsilon)$ then, indeed,

$$\frac{\log g}{(g-2)(\log 2)} < \varepsilon$$

so that (2.8) holds for every large k.

To show that $\mathscr{W}_{\mathscr{D}}(N)$ does not meet every residue class modulo m, observe that every $n \in \mathscr{W}_{\mathscr{D}}(N)$ is of the form

$$n = \sum_{i=0}^{(g-2)k-1} \varepsilon_i g^i$$

where $\varepsilon_i = 0$ or 1 for all i. It follows that

$$n = \sum_{l=0}^{g-3} \sum_{j=0}^{k-1} \varepsilon_{lk+j} (g^k)^l g^j \equiv \sum_{j=0}^{k-1} \left(\sum_{l=0}^{g-3} \varepsilon_{lk+j} \right) g^j \pmod{m}.$$

Here the coefficient of g^j satisfies

$$\sum_{l=0}^{g-3} \varepsilon_{lk+j} \in \{0, 1, ..., g-2\}$$

so that it may assume $g-1$ incongruent values modulo m. Thus this last sum may assume at most

$$(g-1)^k = (1+o(1))\, m^{(\log(g-1))/\log g)}$$

incongruent values, so that at most so many residue classes modulo m may meet $\mathscr{W}_{\mathscr{D}}(N)$ which completes the proof of the theorem.

SECTION 7

Proof of Theorem 4. First we will prove

LEMMA 6. *If* g, t *satisfy* (2.1) *and* $\mathscr{D} \in \{0, 1, ..., g-1\}$, $|\mathscr{D}| = t$, *then for* $n \in \mathbb{N}$, $m \in \mathbb{N}$,

$$m \leqslant N, \tag{7.1}$$

$h \in \mathbb{Z}$ we have

$$|\{n: n \in \mathcal{W}_{\mathcal{D}}(N), n \equiv h(\bmod m)\}| < 2g\, |\mathcal{W}_{\mathcal{D}}(N)|\, m^{-(\log t)/(\log g)}.$$

Proof of Lemma 6. For $m \in \mathbb{N}$, define r by $r \in \mathbb{N}$

$$g^r \leqslant m < g^{r+1}, \tag{7.2}$$

and for all $n \in \mathbb{N}$, define $x = x(n)$ and $y = y(n)$ by $n = xg^r + y$, $x, y \in \mathbb{Z}$, $0 \leqslant y < g^r$. If $x_0 \in \mathbb{Z}$ is such that there is at least one n with $n \in \mathcal{W}_{\mathcal{D}}(N)$, $x_n = x_0$, then clearly

$$|\{n: n \in \mathcal{W}_{\mathcal{D}}(N), x(n) = x_0\}| \begin{cases} = |\mathcal{W}_{\mathcal{D}}(g^r - 1)| = t^r & \text{for} \quad x_0 < [N/g^r] \\ \leqslant |\mathcal{W}_{\mathcal{D}}(g^r - 1)| = t^r & \text{for} \quad x_0 = [N/g^r]. \end{cases}$$

It follows that

$$|\{x_0: \text{there is } n \text{ with } n \in \mathcal{W}_{\mathcal{D}}(N), x(n) = x_0\}|\, t^r \leqslant |\mathcal{W}_{\mathcal{D}}(N)| + t^r$$

whence, by (7.1) and (7.2),

$$\begin{aligned} &|\{x_0: \text{there is } n \text{ with } n \in \mathcal{W}_{\mathcal{D}}(N), x(n) = x_0\}| \\ &\quad \leqslant |\mathcal{W}_{\mathcal{D}}(N)|t^{-r} + 1 = |\mathcal{W}_{\mathcal{D}}(N)|\, (g^r)^{-(\log t)/(\log g)} + 1 \\ &< |\mathcal{W}_{\mathcal{D}}(N)|\, (m/g)^{-(\log t)/(\log g)} + 1 < g\, |\mathcal{W}_{\mathcal{D}}(N)|\, m^{-(\log t)/(\log g)} + 1 \end{aligned}$$

By (7.1) and (7.2),

$$m^{-(\log t)/(\log g)} < t^{r+1} \leqslant g\, |\mathcal{W}_{\mathcal{D}}(m)| \leqslant g\, |\mathcal{W}_{\mathcal{D}}(N)|$$

so that

$$|\{x_0: \text{there is } n \text{ with } n \in \mathcal{W}_{\mathcal{D}}(N), x(n) = x_0\}| < 2g\, |\mathcal{W}_{\mathcal{D}}(N)|\, m^{-(\log t)/(\log g)}. \tag{7.3}$$

By (7.2), for all $x_0 \in \mathbb{Z}$ clearly we have

$$|\{n: n \in \mathcal{W}_{\mathcal{D}}(N), x(n) = x_0, n \equiv h(\bmod m)\}| \leqslant 1. \tag{7.4}$$

It follows from (7.3) and (7.4) that

$$\begin{aligned} &|\{n: n \in \mathcal{W}_{\mathcal{D}}(N), n \equiv h(\bmod m)\}| \\ &\quad = \sum_{x_0} |\{n: n \in \mathcal{W}_{\mathcal{D}}(N), x(n) = x_0, n \equiv h(\bmod m)\}| \\ &\quad \leqslant \sum_{x_0} 1 < 2g\, |\mathcal{W}_{\mathcal{D}}(N)|\, m^{-(\log t)/(\log g)} \end{aligned}$$

(where in $\sum_{x_0}$, x_0 runs over the integers such that there is n with $n \in \mathscr{W}_{\mathscr{D}}(N)$, $x(n) = x_0$), which completes the proof of Lemma 6.

In order to prove (2.10), observe that clearly we have

$$T_z(N) = \sum_{n \in \mathscr{W}_{\mathscr{D}}(N)} \sum_{\substack{d^z \mid n \\ (d,\,(g-1)g)=1}} \mu(d) = \sum_{(d,\,(g-1)g)=1} \mu(d)\, |\{n: n \in \mathscr{W}_{\mathscr{D}}(N),\, d^z \mid n\}|$$

$$= \sum_1 + \sum_2 + \sum_3 \tag{7.5}$$

with

$$\sum_1 = \sum_{\substack{d < \exp(c_1(\log N)^{1/2}/z) \\ (d,\,(g-1)g)=1}} \mu(d) \frac{\mathscr{W}_{\mathscr{D}}(N)|}{d^z},$$

$$\sum_2 = \sum_{\substack{d < \exp(c_1(\log N)^{1/2}/z) \\ (d,\,(g-1)g)=1}} \mu(d) \left(|\{n: n \in \mathscr{W}_{\mathscr{D}}(N),\, d^z \mid n\}| - \frac{|\mathscr{W}_{\mathscr{D}}(N)|}{d^z} \right)$$

and

$$\sum_3 = \sum_{\substack{d \geqslant \exp(c_1(\log N)^{1/2}/z) \\ (d,\,(g-1)g)=1}} \mu(d)\ |\{n: n \in \mathscr{W}_{\mathscr{D}}(N),\, d^z \mid n\}|.$$

Clearly we have

$$\sum_1 = |\mathscr{W}_{\mathscr{D}}(N)| \left(\sum_{(d,\,(g-1)g)=1} \frac{\mu(d)}{d^z} + O\left(\sum_{d \geqslant \exp(c_1(\log N)^{1/2}/z)} \frac{1}{d^z} \right) \right)$$

$$= \left(\left(\zeta(z) \prod_{p \mid (g-1)g} \left(1 - \frac{1}{p^z}\right) \right)^{-1} + O_z\left(\exp\left(-c_1 \left(1 - \frac{1}{z}\right) (\log N)^{1/2} \right) \right) \right) |\mathscr{W}_{\mathscr{D}}(N)| \tag{7.6}$$

Moreover, it follows from Theorem 1 that

$$\sum_2 = O\left(|\mathscr{W}_{\mathscr{D}}(N)| \sum_{d < \exp(c_1(\log N)^{1/2}/z)} d^{-z} \exp(-c_{14}(\log N)^{1/2}) \right)$$

$$= O_z(|\mathscr{W}_{\mathscr{D}}(N)| \exp(-c_{15}(\log N)^{1/2})). \tag{7.7}$$

Finally, in view of (2.9), by Lemma 6 we have

$$\sum_3 \leqslant \sum_{\exp(c_1(\log N)^{1/2}/z) \leqslant d} 2g\, |\mathscr{W}_{\mathscr{D}}(N)|\, d^{-z(\log t)/(\log g)}$$
$$= O_{g,t,z}\left(|\mathscr{W}_{\mathscr{D}}(N)| \exp\left(c_1(\log N)^{1/2}\left(\frac{1}{z}-\frac{\log t}{\log g}\right)\right)\right), \tag{7.8}$$

(2.10) follows from (7.5), (7.6), (7.7) and (7.8), and this completes the proof of Theorem 4.

SECTION 8

Proof of Theorem 5. The proof will be based on the following prime power moduli version of the large sieve (see, e.g., [SAR]):

LEMMA 7. *If* $K \in \mathbb{Z}$, $M \in \mathbb{N}$, $\mathscr{A} \subset \{K+1, K+2, ..., K+M\}$, $z \in \mathbb{N}$ *and* $v \in \mathbb{R}$, *then, writing*

$$Z = |\mathscr{A}| \qquad \text{and} \qquad Z(q, h) = |\{a\colon a \in \mathscr{A}, a \equiv h (\operatorname{mod} q)\}|,$$

we have

$$\sum_{p \leqslant v} p^z \sum_{h=0}^{p^z-1} \left(Z(p^z, h) - \frac{Z}{p^z}\right)^2 \leqslant (v^{2z} + M) Z.$$

Indeed, this is a straightforward consequence of the analytic form of the large sieve.

We will prove Theorem 3 by contradiction. Write

$$y = c_{16}(N^{(\log t)/(2\log g)}/\log N)^{1/(2z-1)},$$

and assume that

$$y < p \leqslant 2y, \qquad n \in \mathscr{W}_{\mathscr{D}}(N) \qquad \text{imply} \quad p^z \nmid n; \tag{8.1}$$

it suffices to show that if c_{16} is small enough in terms of g, t and z, then this assumption leads to a contradiction.

Define the integer k by

$$g^{2k} \leqslant N < g^{2k+2} \tag{8.2}$$

so that $k = [\log N/2 \log g]$. Then clearly $u, v \in \mathscr{W}_{\mathscr{D}}(g^k - 1)$ implies that $u + g^k v \in \mathscr{W}_{\mathscr{D}}(N)$. Assume that p is a prime greater than g, and $\mathscr{W}_{\mathscr{D}}(g^k - 1)$ meets more than $p^z/2$ residue classes modulo p^z. Then by $p > g$, the set

$\{-g^k v \colon v \in \mathcal{W}_{\mathcal{D}}(g^k-1)\}$ meets the same number of residue classes module p^z. Thus by the pigeon hole principle, there are $u, v \in \mathcal{W}_{\mathcal{D}}(g^k-1)$ with

$$u \equiv -g^k v \qquad (\bmod p^z)$$

so that $p^z \mid (u+g^k v) \in \mathcal{W}_{\mathcal{D}}(N)$. Thus by our indirect assumption (8.1),

$$\begin{aligned} &|\{h\colon 0 \leqslant h < p^z, \text{ there is } n \in \mathcal{W}_{\mathcal{D}}(g^k-1) \text{ with} \\ &\quad n \equiv h (\bmod p^z)\}| \leqslant \frac{p^z}{2} \qquad \text{for all} \quad y < p \leqslant 2y \end{aligned} \tag{8.3}$$

(note that $p > y$ implies $p > g$).

Now we apply Lemma 7 with -1, g^k, $\mathcal{W}_{\mathcal{D}}(g^k-1)$ and $2y$ in place of K, M, $\mathcal{A}$ and v, respectively. By (8.2) we obtain

$$\sum_{p \leqslant 2y} p^z \sum_{h=0}^{p^z-1} \left(Z(p^z, h) - \frac{Z}{p^z}\right)^2 \leqslant ((2y)^{2z} + g^k) Z \leqslant ((2y)^{2z} + N^{1/2}) Z. \tag{8.4}$$

On the other hand, by (8.3) and the prime number theorem for large N we have

$$\begin{aligned} &\sum_{p \leqslant 2y} p^z \sum_{h=0}^{p^z-1} \left(Z(p^z, h) - \frac{Z}{p^z}\right)^2 \\ &\quad \geqslant \sum_{y < p \leqslant 2y} p^z \sum_{\substack{0 \leqslant h < p^z - 1 \\ Z(p^2, h) = 0}} \frac{Z^2}{p^{2z}} \\ &\quad = Z^2 \sum_{y < p \leqslant 2y} p^{-z} |\{h\colon 0 \leqslant h < p^z - 1, Z(p^z, h) = 0\}| \\ &\quad \geqslant Z^2 \sum_{y < p \leqslant 2y} p^{-z} \frac{p^z - 1}{2} > \frac{1}{3} Z^2 \sum_{y < p \leqslant 2y} 1 \\ &\quad = \frac{1}{3} Z^2 (1 + o(1)) \frac{y}{\log y} > \frac{1}{4} Z^2 \frac{y}{\log y}. \end{aligned} \tag{8.5}$$

It follows from (8 4) and (8.5) that

$$Z < 4 \frac{\log y}{y} ((2y)^{2z} + N^{1/2}) < 4 \frac{\log N}{y} ((2y)^{2z} + N^{1/2}). \tag{8.6}$$

On the other hand, by (8.2) clearly we have

$$Z = |\mathcal{W}_{\mathcal{D}}(g^k-1)| = t^k = (g^{2k})^{(\log t)/(2 \log g)} > g^{-2} N^{(\log t)/(2 \log g)}. \tag{8.7}$$

It follows from (8.6) and (8.7) that

$$N^{(\log t)/(2 \log g)} < 4g^2 \frac{\log N}{y}((y)^{2z} + N^{1/2}).$$

However, in view of (2.11), an easy computation shows that if c_{16} in the definition of y is small enough then this inequality cannot hold, and this completes the proof of the theorem.

REFERENCES

[COQ1] J. Coquet, On the uniform distribution modulo one of some subsequences of polynomial sequences, *J. Number Theory* **10** (1978), 291–296.

[COQ2] J. Coquet, On the uniform distribution modulo one of some subsequences of polynomial sequences II, *J. Number Theory* **12** (1980), 244–250.

[COQ3] J. Coquet, Graphes connexes, représentation des entiers et équirépartition, *J. Number Theory* **16** (1983), 363–375.

[DAV1] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935), 30–32.

[DAV2] H. Davenport, A historical note, *J. London Math. Soc.* **22** (1947), 100–101.

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

[FK] M. Filaseta and S. Konyagin, Squarefree values of polynomials whose coefficients are 0 and 1, *Acta Arith.* **74** (1996), 191–205.

[GAL] P. X. Gallagher, A larger sieve, *Acta Arith.* **18** (1971), 77–81.

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

[MAU] C. Mauduit, Automates finis et ensembles normaux, *Ann. Inst. Fourier* **36** (1986), 1–25.

[MS1] C. Mauduit and A. Sárközy, On the arithmetic structure of sets characterized by sum of digits properties, *J. Number Theory* **61** (1996), 25–38.

[MS2] C. Mauduit and A. Sárközy, On the arithmetic structure of the integers whose sum of digits is fixed, *Acta Arithmetica* **81** (1997), 145–173.

[SAR] A. Sárközy, A note on the arithmetic form of the large sieve, *Studia Sci. Math. Hung.* **27** (1992), 83–95.