Journal of Number Theory 129 (2009) 2820–2830

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On digit sums of multiples of an integer

Cécile Dartyge [a], Florian Luca [b,*,1], Pantelimon Stănică [c]

[a] Institut Élie Cartan, Université Henri Poincaré-Nancy 1, BP 239, 54506 Vandoeuvre Cedex, France
[b] Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, Mexico
[c] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943-5216, USA

ARTICLE INFO

Article history:
Received 13 November 2008
Revised 8 March 2009
Available online 29 May 2009
Communicated by Carl Pomerance

MSC:
11N25
11N37

Keywords:
Sum of digits
Carmichael lambda function
Sturdy numbers

ABSTRACT

Let $g > 1$ be an integer and $s_g(m)$ be the sum of digits in base g of the positive integer m. In this paper, we study the positive integers n such that $s_g(n)$ and $s_g(kn)$ satisfy certain relations for a fixed, or arbitrary positive integer k. In the first part of the paper, we prove that if n is not a power of g, then there exists a nontrivial multiple of n say kn such that $s_g(n) = s_g(kn)$. In the second part of the paper, we show that for any $K > 0$ the set of the integers n satisfying $s_g(n) \leqslant K s_g(kn)$ for all $k \in \mathbb{N}$ is of asymptotic density 0. This gives an affirmative answer to a question of W.M. Schmidt.

© 2009 Elsevier Inc. All rights reserved.

1. Introduction

The distribution of various arithmetic functions on positive integers written in given base $g > 1$ is a classical area of investigation and a huge body of literature on this topic has been published. In this paper, we denote by $s_g(n)$ the sum of digits in base g of the positive integer n and study positive integers n such that there is some relation between $s_g(n)$ and $s_g(kn)$ for some small positive integer k which might be specified or not. For example, first we study the numbers n having a nontrivial multiple m (that is, m/n is not a power of g) such that $s_g(n) = s_g(m)$. More precisely, let

$$\mathcal{N}_g = \{n\colon\ s_g(n) = s_g(kn) \text{ for some integer } k \neq g^{\ell}\}.$$

* Corresponding author.
E-mail addresses: dartyge@iecn.u-nancy.fr (C. Dartyge), fluca@matmor.unam.mx (F. Luca), pstanica@nps.edu (P. Stănică).

[1] Work by the second author was done in the Spring of 2007 while he visited the Naval Postgraduate School. He would like to thank this institution for its hospitality. The third author was supported by a RIP grant from NPS.

0022-314X/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2009.04.003

Note that $\mathcal{N}_g$ misses some integers. For example, no power of g belongs to $\mathcal{N}_g$. Our first result is that $\mathcal{N}_g$ contains all positive integers except for the powers of g.

Theorem 1. *The set $\mathcal{N}_g$ consists of all positive integers which are not a power of g.*

Let $(a_g(n))_{n\geqslant 1}$ be the sequence defined by

$$a_g(n) = \min\{kn\colon\ k \neq g^\ell,\ s_g(n) = s_g(kn)\}, \quad \text{if } n \in \mathcal{N}_g,$$

and $a_g(n) = 0$, otherwise. Our Theorem 1 shows that $a_g(n) \neq 0$ for all $n \neq g^\ell$. In base 10, we have

$$(a_{10}(n))_{n\geqslant 1} = (0, 110, 12, 112, 140, 24, 133, 152, 18, 0, 1001, 300, 2002, \ldots).$$

This is sequence $A087303$ in [10].

It seems interesting to study the extremal orders of $a_g(n)$. Our next result gives some nontrivial estimates on $a_g(n)$.

Theorem 2. *The inequalities*

$$n\left(\frac{\log n}{\log\log n}\right)^{1/3} \ll a_g(n) \leqslant \exp\left(\frac{n}{(\log n)^{(1+o(1))\log\log\log n}}\right)$$

hold for almost all positive integers n.

Taking $n = g^m + 1$, we see easily that $a_g(n) = g^{3m} + 1$. In particular, $a_g(n) \asymp n^3$ holds for infinitely many n. Furthermore, taking $n = 1 + g + \cdots + g^{p-1}$ where p is a prime number and noting that $M = 1 + g^2 + \cdots + g^{p-1} + g^{p+1} = n - g + g^{p+1}$ is a nontrivial multiple of n with the same sum of digits, we get that in fact $a_g(n) \asymp n$ also holds for infinitely many n.

A problem closely related to the determination of the set $\mathcal{N}_g$ is to study the set of positive integers n such that the inequality $s_g(n) \leqslant s_g(kn)$ holds with some fixed integer $k \geqslant 2$ coprime with g. In 1980, Stolarsky [12] proved that the set of positive integers n satisfying the above inequality with $g = 2$ and $k = 3$ has density 1/2. He called such numbers 3-*sturdy* numbers. He also introduced the k-*sturdy* numbers as being the numbers n such that $s_2(n) \leqslant s_2(kn)$, as well as the *sturdy* numbers, as being the numbers n which are k-sturdy for all positive integers k.

Schmidt [9] proved that for every fixed odd integer $k \geqslant 3$, the set of k-sturdy numbers has density 1/2. He also showed that the sturdy numbers have density 0.

He asked (see p. 608 in [9]) for the following generalization of this problem.

Question 3. *Given $K > 0$, is it true that the set of numbers n with*

$$s_2(n) \leqslant K s_2(kn) \quad \textit{for all } k \geqslant 1,$$

forms a set of asymptotic density 0?

In this paper, we give an affirmative answer to Schmidt's question.

Theorem 4. *Let $g \geqslant 2$ and $K > 0$. For $x \geqslant 3$, the number of positive integers $n \leqslant x$ satisfying*

$$s_g(n) \leqslant K s_g(kn) \quad \textit{for all } k \geqslant 1,$$

is $O(x/(\log x)^{1/2})$. In particular, such numbers form a set of asymptotic density 0.

The above result is interesting only for $K \geqslant 1$, since for $K \in (0,1)$ it is a direct consequence of Theorem 1. With a bit more care, it is possible to replace the exponent 1/2 on the logarithm in Theorem 4 above by $1-\varepsilon$, where $\varepsilon > 0$ is arbitrarily small.

The rest of the paper is organized as follows. Section 2 contains the proof of Theorem 1, which is elementary. Section 3 consists of the proof of Theorem 2, which uses some results on the joint distribution of $s_g(n)$ and $s_g(hn)$ in arithmetic progressions with small prime moduli, due to the first author and G. Tenenbaum [4], as well as an upper bound for the Carmichael λ-function of n valid for almost all positive integers n, due to P. Erdős, C. Pomerance and E. Schmutz [5]. The last section is devoted to the proof of Theorem 4. The idea of this proof is to apply a recent result of Bourgain [2] on exponential sums. For this, we also need an estimate of Tenenbaum [14] on the number of positive integers $n \leqslant x$ with a large divisor having only small prime factors, a result of Banks, Garaev, and the second author [1] on the order of the subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ generated by the number g, and an upper bound on the counting function of the positive integers n such that $s_g(n)$ is abnormally small obtained by Mauduit, Pomerance and Sárközy [6].

Throughout this paper, we use the Landau symbols O and o and the Vinogradov symbols $\gg$, $\ll$ and $\asymp$ with their usual meanings. The constants implied by them depend on the number g. We denote by $P^+(n)$ (respectively by $P^-(n)$) the greatest (respectively the smallest) prime factor of the positive integer n with the conventions $P^+(1) = 1$, $P^-(1) = \infty$. We use p and q with or without subscripts for prime numbers.

2. The proof of Theorem 1

First suppose that n has at least two nonzero digits in base g:

$$n = c_1 g^{\ell_1} + \cdots + c_t g^{\ell_t},$$

with $t \geqslant 2$, $1 \leqslant c_1, \ldots, c_t \leqslant g-1$ and $0 \leqslant \ell_1 < \cdots < \ell_t$. Write $n = ab$, where all the primes dividing a divide also g and b is coprime to g. Clearly, there exists a natural number α such that $a \mid g^\alpha$. Since $(b,g) = 1$, it follows that $g^{\lambda(b)} \equiv 1 \pmod{b}$, where for a positive integer m we use $\lambda(m)$ for the Carmichael function of m, which is the maximal order of invertible elements modulo m. Thus, $g^{\ell_t+\alpha+\lambda(b)} \equiv g^{\ell_t+\alpha} \pmod{n}$. We now put

$$M = c_1 g^{\ell_1+\alpha} + \cdots + c_{t-1} g^{\ell_{t-1}+\alpha} + c_t g^{\ell_t+\lambda(b)+\alpha}.$$

We then have

$$M \equiv c_1 g^{\ell_1+\alpha} + \cdots + c_t g^{\ell_t+\alpha} \pmod{n} \equiv n g^\alpha \pmod{n} \equiv 0 \pmod{n}.$$

It is also obvious that $s_g(M) = s_g(n)$. Since $g^{\ell_1} \parallel n$ and $g^{\alpha+\ell_1} \parallel M$, the equality $M = g^k n$ can only be satisfied by the integer $k = \alpha$. But we easily check that $M - g^\alpha n = c_t g^{\ell_t+\alpha}(g^{\lambda(b)} - 1) \neq 0$. Thus, M/n is not a power of g.

Suppose next that n has only one nonzero digit in base g. If $n = g^\ell$, then it is clear that $n \notin \mathcal{N}_g$. Thus, assume now that $n = cg^\ell$, where $2 \leqslant c \leqslant g-1$. If c and g are coprime, we then take $M = g^\ell(c - 1 + g^{\lambda(c)})$ and it is clear that $n \mid M$ and that $M/n = 1 + (g^{\lambda(c)} - 1)/c$ is not a power of g. More generally, if $c = c_1 c_2$, where $c_1 \geqslant 2$ is coprime to g and all prime factors of c_2 divide g, we then take α to be such that $c_2 \mid g^\alpha$ and put $M = g^{\ell+\alpha}(c_1 c_2 - 1 + g^{\lambda(c_1)})$. The integer M has two nonzero digits and n only one, thus M/n is not a power of g.

Finally, if $n = cg^\ell$, where all prime factors of c divide g, we can then take $M = g^{\ell+\alpha}(c - 1 + g)$, where again α is sufficiently large such that $c \mid g^\alpha$.

3. The proof of Theorem 2

If we write $n = ab$, where all prime factors of a divide g and b is coprime to n, then for almost all positive integers n we have that $a < \log n$. Now the proof of Theorem 1 shows that the inequality

$$a_g(n) \leqslant g^{\alpha(n)+\lambda(n)} n \tag{1}$$

holds for all positive integers $n \in \mathcal{N}_g$, where we put $\alpha(n)$ for the smallest α such that $a \mid g^\alpha$. Since $a < \log n$ for almost n, it follows easily that $g^{\alpha(n)} \ll (\log n)^{\omega(g)}$, where $\omega(g)$ is the number of distinct prime factors of g. In particular, the inequality $g^{\alpha(n)} < n$ holds for all sufficiently large n in a set of asymptotic density 1.

Now Theorem 2 of [5] shows that the inequality

$$\lambda(n) \leqslant n \exp\bigl(-\bigl(1 + o(1)\bigr) \log\log n \log\log\log n\bigr)$$

holds as $n \to \infty$ in a set of asymptotic density 1. Thus, using inequality (1), one gets easily that

$$a_g(n) \leqslant \exp\biggl(\frac{n}{(\log n)^{(1+o(1))\log\log\log n}}\biggr)$$

holds as $n \to \infty$ in a set of asymptotic density 1, which is the upper bound of Theorem 2.

For the lower bound, let x be large and let H be some parameter depending on x and tending to infinity with x to be chosen later. We count the number of $n \leqslant x$ such that $s_g(n) = s_g(hn)$ holds with some positive integer $2 \leqslant h \leqslant H$ which is coprime to g. Let us fix the number H. Let $p > \max\{H(\log H)^{1/2}, g\}$ be some prime depending also on x to be fixed later. Corollary 2.10 in [4] shows that under these conditions, we have

$$\begin{aligned} \mathcal{A}_{h,p,a}(x) &= \#\bigl\{n \leqslant x\colon\ s_g(n) \equiv s_g(hn) \equiv a \ (\mathrm{mod}\ p)\bigr\} \\ &= \frac{x}{p^2} + O\bigl(x^{1-c_0/(p^2 H \log H)}\bigr), \end{aligned}$$

where c_0 is a positive constant depending on g. Assuming that

$$x^{c_0/(p^2 H \log H)} > p^3, \tag{2}$$

and that x is large, we then see that the inequality

$$\mathcal{A}_{h,p,a}(x) < \frac{2x}{p^2}$$

holds uniformly for $2 \leqslant h \leqslant H$ and $a \in \{0, 1, \dots, p-1\}$. Thus,

$$\begin{aligned} \mathcal{A}(x) &= \sum_{\substack{2 \leqslant h \leqslant H \\ g \nmid h}} \#\bigl\{n \leqslant x\colon\ s_g(n) = s_g(hn)\bigr\} \\ &\leqslant \sum_{\substack{2 \leqslant h \leqslant H \\ g \nmid h}} \#\bigl\{n \leqslant x\colon\ s_g(n) = s_g(hn) \ (\mathrm{mod}\ p)\bigr\} \end{aligned}$$

$$= \sum_{\substack{2\leqslant h\leqslant H\\ g\nmid h}} \sum_{0\leqslant a\leqslant p-1} \mathcal{A}_{h,p,a}(x)$$

$$\leqslant \frac{2Hx}{p} \ll \frac{x}{(\log H)^{1/2}} = o(x) \tag{3}$$

as $x \to \infty$. Inequality (2) tells us that we should choose p such that

$$c_0 \log x > 3p^2 H \log H \log p.$$

Choosing p to be the first prime $> H \log H$, we get that the above estimate implies that

$$c_0 \log x \geqslant \big(3 + o(1)\big)(H \log H)^3,$$

giving

$$H = \big(c_1 + o(1)\big)\left(\frac{\log x}{\log_2 x}\right)^{1/3} \quad \text{as } x \to \infty,$$

where $c_1 = (9c_0)^{1/3}$. Since, $a_g(n) \geqslant Hn$ holds for all $n \leqslant x$ with the exception of a set of positive integers n of cardinality $o(x)$ as $x \to \infty$ (see inequality (3)), the lower bound follows. The proof of Theorem 2 is complete.

Schmid [8] proved that if $k_1 \neq k_2$ are fixed odd integers and a is a fixed integer, then the asymptotic

$$\#\big\{n\colon\ 0 \leqslant n < x\colon\ s_2(k_1 n) - s_2(k_2 n) = a\big\} \sim \frac{x}{\sqrt{2\pi V(\log x/\log 2)}} e^{-\frac{a^2 \log 2}{2V \log x}}$$

holds as $x \to \infty$, where

$$V = \frac{1}{2}\left(1 - \frac{\gcd(k_1, k_2)^2}{k_1 k_2}\right).$$

Applying this asymptotic with $(k_1, k_2) = (1, 3)$ yields the lower bound

$$\#\big\{n \leqslant x\colon\ a_2(n) = 3n\big\} \gg \frac{x}{\sqrt{\log x}}.$$

It is perhaps possible to generalize the result of Schmid to other bases. Steiner [11] obtained a very general result on the global joint distribution of sequences $\{s_g(P_\ell(n))\}_{n\geqslant 1}$, $\ell = 1, \ldots, d$, where $P_1, \ldots, P_\ell$ are polynomials in $\mathbb{Z}[X]$. It would be very interesting to obtain a local result for the above joint distribution at least for the case of linear polynomials.

4. The proof of Theorem 4

For coprime positive integers g and n, let $t_g(n)$ denote the order of g modulo n. For $x \geqslant 2$, we define the following functions of x:

$$y_0 = \exp\big((\log x)^{1/2}\big), \qquad z_0 = \exp\big((\log x)^{3/4}\big),$$
$$y_1 = \exp\big((\log x)^{1/8}\big), \qquad z_1 = \exp\big((\log x)^{1/4}\big). \tag{4}$$

Every positive integer n has a decomposition of the form $n = a_n b_n$ with $P^+(a_n) \leqslant y_0 < P^-(b_n)$.

The idea of this proof is the following. Since a_n is small for almost integers n, its sum of digits is very small. The main ingredient of the proof then consists in finding for almost all positive integers n, a multiple of b_n, say kb_n, with very few and sparse nonzero digits, such that $a_n(kb_n) = kn$ has a small sum of digits.

Define the following sets of primes

$$\mathcal{P} = \{p\colon\ t_g(p) < p^{1/2}(\log p)^{-10}\}$$

and

$$\mathcal{Q}(x) = \{p \leqslant x\colon\ p \equiv 1 \pmod d \text{ for some } d > z_1 \text{ with } P^+(d) < y_1\}.$$

We denote by $\mathcal{P}(x)$ the set $\mathcal{P} \cap [1, x]$. The following lemma turns out to be quite useful.

Lemma 5. *The following estimates hold*:

$$\#\mathcal{P}(x) = O\left(\frac{x}{(\log x)^2}\right), \tag{5}$$

$$\#\mathcal{Q}(x) \ll x \exp\bigl(-c_0(\log x)^{1/8}(\log\log x)\bigr), \tag{6}$$

where $c_0 = 1/16$. *In particular,*

$$\sum_{\substack{p>y\\ p\in\mathcal{P}}} \frac{1}{p} \ll \frac{1}{\log y}, \tag{7}$$

and

$$\sum_{\substack{p>y\\ p\in\mathcal{Q}(x)}} \frac{1}{p} \ll \exp\bigl(-c_1(\log y)^{1/8}(\log\log y)\bigr), \tag{8}$$

where $c_1 = 1/17$.

Proof. Estimate (5) appears in Lemma 4 in [1], and estimates (7) and (8) follow from estimates (5) and (6) by Abel's summation formula. Thus, it remains to prove estimate (6). For $x \geqslant 1$, $y \geqslant 1$, $z \geqslant 1$, we define the function $\Theta(x, y, z)$ by

$$\Theta(x, y, z) = \#\Bigl\{n \leqslant x\colon\ \prod_{\substack{p^\nu \| n\\ p\leqslant y}} p^\nu > z\Bigr\}. \tag{9}$$

Let $u = \log x/\log y$, $v = \log z/\log y$ and ϱ be the Dickman–de Bruijn function. Tenenbaum [14, Eq. (1.5)] showed that for all $\varepsilon > 0$ the asymptotic

$$\Theta(x, y, z) \sim \mathrm{e}^{-\gamma} x \int_v^\infty \varrho(t)\,\mathrm{d}t$$

holds for

$$y \geqslant 2, \qquad 1 \leqslant z \leqslant \exp\exp\{(\log y)^{3/5-\varepsilon}\}, \qquad z \leqslant x^{1-\varepsilon},$$

provided that both u and y tend to infinity. More precise asymptotic formulas for $\Theta(x, y, z)$ appear in [13] and [14] (see also [3] for a less precise asymptotic which is valid in a larger range for z versus y).

We now have

$$\mathcal{Q}(x) \subset \Bigl\{p \leqslant x\colon \prod_{\substack{q^\nu \| p-1 \\ q \leqslant y_1}} q^\nu > z_1\Bigr\}.$$

Since the function ϱ satisfies $\varrho(t) = t^{-t+o(t)}$ for $t \to \infty$, we have

$$\#\mathcal{Q}(x) \leqslant \Theta(x, y_1, z_1) \ll x\mathrm{e}^{-v(\log v)/2} \ll x\exp\bigl(-c_0(\log x)^{1/8}(\log\log x)\bigr), \tag{10}$$

which is what we wanted. □

Before continuing, we point out that the cardinality of the set $\mathcal{Q}(x)$ with a somewhat larger value of y_1 was also studied in Theorem 2 in [7].

Lemma 6. *Let $x \geqslant 2$. The following properties are satisfied by almost all integers $n \leqslant x$ with at most $O(x/(\log x)^{1/2})$ exceptions*:

(i) $a_n \leqslant z_0$;
(ii) b_n *is squarefree*;
(iii) *If $p \mid b_n$, then $p \notin \mathcal{P} \cup \mathcal{Q}(x)$, where these sets of primes are defined in the beginning of this section*;
(iv) *If $d \mid b_n$, then $t_g(d) > d^{2/5}$.*

Proof. We assume that $n > x/(\log x)^{1/2}$, since there are at most $x/(\log x)^{1/2}$ positive integers n failing this condition.

We begin with (i). By the definition of Θ given in (9), the number of positive integers $n \leqslant x$ not satisfying (i) is exactly $\Theta(x, y_0, z_0)$. As in estimate (10), we have

$$\Theta(x, y_0, z_0) \ll x\mathrm{e}^{-v(\log v)/2} \ll x\exp\bigl(-c_2(\log x)^{1/4}(\log\log x)\bigr),$$

where $c_2 = 1/8$. Thus, there are at most $O(x/(\log x)^{1/2})$ positive integers $n \leqslant x$ failing (i).

If $n \leqslant x$ fails (ii), then there exists a prime $p > y_0$ such that $p^2 \mid n$. Given p, the number $n \leqslant x$ which are multiples of p^2 is $\leqslant x/p^2$. Thus, the number of $n \leqslant x$ failing (ii) is at most

$$\leqslant \sum_{y_0 \leqslant p \leqslant x^{1/2}} \frac{x}{p^2} \ll \frac{x}{y_0} = \frac{x}{(\log x)^{1/2}}. \tag{11}$$

If $n \leqslant x$ fails (iii), then there exists $p \in \mathcal{P} \cup \mathcal{Q}(x)$ such that $p \mid n$ and $p > y_0$. The number of such positive integers $n \leqslant x$ is at most

$$\sum_{\substack{p \in \mathcal{P} \\ p > y_0}} \frac{x}{p} + \sum_{\substack{p \in \mathcal{Q}(x) \\ p > y_0}} \frac{x}{p} \ll \frac{x}{\log y_0} = \frac{x}{(\log x)^{1/2}}.$$

It remains to deal with the positive integers $n \leqslant x$ failing (iv). We may assume that such n satisfies (i), (ii) and (iii), and let d be a divisor of b_n. Then d is also squarefree, and we have

$$t_g(d) = \big[t_g(p), p \mid d\big],$$

where $[t_g(p), p \mid d]$ denotes the least common multiple of all the numbers $t_g(p)$ taken over all the prime factors p of d. Since $t_g(p) \mid p-1$ holds for all p, it follows that if $q \mid \gcd(t_g(p), t_g(p'))$ for two distinct prime factors p and p' of d, then $q \mid \gcd(p-1, p'-1)$. The number of positive integers $n \leqslant x$ for which there exists $q > y_1$ such that $q \mid \gcd(t_g(p), t_g(p'))$ for two distinct primes factors p, p' of b_n is at most

$$\sum_{\substack{y_1 < q \leqslant \sqrt{x} \\ p, p' \equiv 1 \pmod q}} \frac{x}{pp'} \leqslant x \sum_{q > y_1} \Bigg(\sum_{\substack{m \leqslant x \\ m \equiv 1 \pmod q}} \frac{1}{m} \Bigg)^2 \ll x (\log x)^2 \sum_{q > y_1} \frac{1}{q^2} \ll \frac{x (\log x)^2}{y_1}.$$

For the remaining n, we have

$$\big[t_g(p), p \mid d\big] \geqslant \prod_{p \mid d} \frac{t_g(p)}{\prod_{p \mid d} \prod_{\substack{q^\nu \| p-1 \\ q \leqslant y_1}} q^\nu}.$$

We now use the fact that, by (iii), the prime factors of d do not belong to $\mathcal{P} \cup \mathcal{Q}(x)$. Thus,

$$\big[t_g(p), p \mid d\big] \geqslant \frac{\sqrt{d}}{(z_1 (\log d)^{10})^{\omega(d)}},$$

where $\omega(d)$ stands for the number of distinct prime factors of n. By the well-known Hardy–Ramanujan bounds, $\omega(n)$ is very close to $\log\log n$ for almost all n. More precisely,

$$\begin{aligned} \#\big\{n \leqslant x \colon \omega(n) > 10 \log\log x\big\} &\leqslant \sum_{n \leqslant x} 3^{\omega(n) - 10 \log\log x} \\ &\ll x (\log x)^{-10 \log 3} \prod_{p \leqslant x} (1 + 3/p) \\ &\ll x (\log x)^{3 - 10 \log 3} \ll x (\log x)^{-7}. \end{aligned}$$

Thus, for all positive integers $n \leqslant x$ with at most $O(x/(\log x)^{1/2})$ exceptions, we have

$$\big[t_g(p), p \mid d\big] \geqslant \frac{\sqrt{d}}{(z_1 (\log d)^{10})^{10 \log\log x}}.$$

We now recall that $P^-(d) > y_0$. Thus, for x large enough we have

$$z_1^{10 \log\log x} = \exp\big(10 (\log x)^{1/4} \log\log x\big) \leqslant y_0^{1/20} \leqslant d^{1/20}$$

and

$$(\log d)^{100 \log\log x} \leqslant \exp\big(100 (\log\log x)^2\big) \leqslant d^{1/20}.$$

Thus, (iv) is also satisfied for all positive integers $n \leqslant x$ with at most $O(x/(\log x)^{1/2})$ exceptions. $\square$

We prove the following lemma.

Lemma 7. *Let n be an integer satisfying Lemma 6. There exists an absolute constant $\ell_0 \in \mathbb{N}$ such that for $\ell \geqslant \ell_0$ and $x \geqslant x_0(\ell_0)$ large enough, the congruence*

$$g^{j_1} + \cdots + g^{j_\ell} \equiv 0 \pmod{b_n} \tag{12}$$

has a solution $(j_1, \ldots, j_\ell) \in \{0, \ldots, t_g(b_n) - 1\}^\ell$.

Proof. For $t \in \mathbb{R}$, we use the notation $\mathbf{e}(t) = \exp(2i\pi t)$. Let S_ℓ denotes the number of solutions in $\{0, \ldots, t_g(b_n) - 1\}^\ell$ to the congruence (12). We have

$$\begin{aligned} S_\ell &= \frac{1}{b_n} \sum_{h=1}^{b_n} \left(\sum_{j=0}^{t_g(b_n)-1} \mathbf{e}\left(\frac{hg^j}{b_n}\right)\right)^\ell \\ &= \frac{(t_g(b_n))^\ell}{b_n} + \frac{1}{b_n} \sum_{h=1}^{b_n-1} \left(\sum_{j=0}^{t_g(b_n)-1} \mathbf{e}\left(\frac{hg^j}{b_n}\right)\right)^\ell \\ &= \frac{(t_g(b_n))^\ell}{b_n} + R_\ell, \end{aligned} \tag{13}$$

say. We will prove that for ℓ large enough the term R_ℓ is sufficiently small. The main tool for this proof is the following lemma of Bourgain [2].

Lemma 8. *Let $q \in \mathbb{N}$ and $H \subset (\mathbb{Z}/q\mathbb{Z})^*$ be a multiplicative subgroup such that $|H| > q^\delta$, $\delta > 0$ arbitrary. Then one has the exponential sum estimate*

$$\max_{a \in \mathbb{Z}_q^*} \left| \sum_{x \in H} \mathbf{e}_q(ax) \right| < c_3 q^{-\varepsilon} |H| \quad \textit{for some } c_3 > 0 \textit{ and } \varepsilon = \varepsilon(\delta) > 0.$$

To apply the above lemma, we must work with irreducible fractions h/d. We write

$$R_\ell = \frac{1}{b_n} \sum_{\substack{d \mid b_n \\ d \neq 1}} \sum_{\substack{1 \leqslant h \leqslant d \\ \gcd(h, b_n) = 1}} \left(\sum_{j=0}^{t_g(b_n)-1} \mathbf{e}\left(\frac{hg^j}{d}\right)\right)^\ell.$$

If we write $j = u + \lambda t_g(d)$ with $0 \leqslant u < t_g(d)$ and $0 \leqslant \lambda < t_g(b_n)/t_g(d)$, we then have

$$g^j \equiv g^u \pmod{d}.$$

Thus, we also have

$$|R_\ell| \leqslant \frac{1}{b_n} \sum_{\substack{d \mid b_n \\ d \neq 1}} \sum_{\substack{1 \leqslant h \leqslant d \\ \gcd(h, b_n) = 1}} \left(\frac{t_g(b_n)}{t_g(d)}\right)^\ell \left| \sum_{j=0}^{t_g(d)-1} \mathbf{e}\left(\frac{hg^j}{d}\right)\right|^\ell.$$

By Lemma 6, we have that $t_g(d) > d^{2/5}$ holds for all $d \mid b_n$ with $d > 1$. Thus, for each d we may apply Lemma 8 with $H = \langle g\rangle$, which is the subgroup of $(\mathbb{Z}/d\mathbb{Z})^*$ generated by g, and with $\delta = 2/5$. We obtain the following estimate for R_ℓ:

$$|R_\ell| \leqslant \frac{(c_3 t_g(b_n))^\ell}{b_n} \sum_{\substack{d \mid b_n \\ d \neq 1}} \varphi(d) d^{-\ell\varepsilon} \leqslant \frac{(c_3 t_g(b_n))^\ell}{b_n} \frac{\pi^2}{6} y_0^{3-\ell\varepsilon}. \tag{14}$$

Here, ε and c_3 are the positive constants given by Lemma 8. In the last upper bound above, we used the fact that the inequality $\varphi(d) d^{-\varepsilon\ell} \leqslant d^{-2} y_0^{3-\ell\varepsilon}$ holds for all $d > y_0$ when $3 - \ell\varepsilon < 0$. Finally, combining estimates (13) with the bound (14) on R_ℓ, we have

$$S_\ell \geqslant \frac{t_g(b_n)^\ell}{b_n}\left(1 - \frac{\pi^2}{6} c_3^\ell y_0^{3-\ell\varepsilon}\right) > 0,$$

provided that $\ell > 3\varepsilon^{-1}$ and that x is large enough, which completes the proof of Lemma 7. □

We are now ready to prove Theorem 4.

Let $K > 0$. Let x be large enough. Let $\mathcal{M}(x)$ be the set of positive integers $n \leqslant x$ satisfying the conditions of Lemma 6 such that

$$\left| s_g(n) - \frac{(g-1)}{2}\left\lfloor \frac{\log x}{\log g} \right\rfloor \right| \leqslant \frac{(g-1)}{4}\left\lfloor \frac{\log x}{\log g} \right\rfloor. \tag{15}$$

Lemma 4 in [6] shows that the number of positive integers $n \leqslant x$ not satisfying estimate (15) is

$$\ll x^{1 - c_4/\log\log x}, \tag{16}$$

where c_4 is a positive constant depending on g. Thus, we certainly have

$$\#\mathcal{M}(x) = x + O\big(x(\log x)^{-1/2}\big).$$

Let $n \in \mathcal{M}(x)$. We will show that there exists a multiple kn of it such that $s_g(kn) \leqslant K s_g(n)$.

By Lemma 6, $a_n \leqslant z_0$. Thus, $s_g(a_n) \leqslant g \log z_0 / \log g = g(\log x)^{3/4}/\log g$ and $a_n < g^T$, where $T = 1 + \lfloor \log z_0 / \log g \rfloor$. Next, we choose a fixed integer $\ell \geqslant \ell_0$, where ℓ_0 is defined by Lemma 7. By this lemma, there exists $(j_1, \dots, j_\ell) \in \{0, \dots, t_g(b_n) - 1\}^\ell$ such that

$$\sum_{m=1}^{\ell} g^{j_m} \equiv 0 \pmod{b_n}.$$

Since $g^{t_g(b_n)} \equiv 1 \pmod{b_n}$, we also have

$$U = \sum_{m=1}^{\ell} g^{j_m + mTt_g(b_n)} \equiv 0 \pmod{b_n},$$

and the exponents of the nonzero digits of U are distinct. Furthermore, $a_n U$ is a multiple of n such that

$$s_g(a_n U) = s_g(a_n)\ell \ll (\log x)^{3/4} < K^{-1} s_g(n)$$

for x large enough.

Indeed writing $a_n = \sum_{i=0}^{T-1} c_i g^i$ with $0 \leqslant c_i \leqslant g-1$, we have

$$a_n U = \sum_{\substack{0 \leqslant i \leqslant T-1 \\ 1 \leqslant m \leqslant \ell}} c_i g^{i + j_m + mTt_g(b_n)} \tag{17}$$

and

$$i + j_m + mTt_g(b_n) = i' + j_{m'} + m'Tt_g(b_n) \quad \Rightarrow \quad m = m' \quad \text{and so} \quad i = i'.$$

Hence, the exponents in (17) are distinct. This completes the proof of Theorem 4.

As we have already mentioned, it is possible to replace the upper bound $x(\log x)^{-1/2}$ on the cardinality of the set of exceptional positive integers $n \leqslant x$ by $x(\log x)^{-\alpha_0}$ for any $\alpha_0 \in (0, 1)$ by taking

$$y_0 = \exp\bigl((\log x)^{\alpha_0}\bigr), \qquad z_0 = \exp\bigl((\log x)^{\beta_0}\bigr),$$
$$y_1 = \exp\bigl((\log x)^{\alpha_1}\bigr), \qquad z_1 = \exp\bigl((\log x)^{\beta_1}\bigr),$$

with $0 < \alpha_1 < \beta_1 < \alpha_0 < \beta_0 < 1$. We do not enter into such details.

Acknowledgments

We thank the anonymous referee and Professor Carl Pomerance for useful suggestions which improved the quality of our manuscript.

References

[1] W.D. Banks, M.Z. Garaev, F. Luca, I.E. Shparlinski, Uniform distribution of fractional parts related to pseudoprimes, Canad. J. Math., in press.
[2] J. Bourgain, Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary, J. Anal. Math. 97 (2005) 317–355.
[3] E.R. Canfield, P. Erdős, C. Pomerance, On a problem of Oppenheim concerning 'Factorisatio Numerorum', J. Number Theory 17 (1983) 1–28.
[4] C. Dartyge, G. Tenenbaum, Sommes des chiffres de multiples d'entiers, Ann. Inst. Fourier 7 (2005) 2423–2474.
[5] P. Erdős, C. Pomerance, E. Schmutz, Carmichael's lambda function, Acta Arith. 58 (1991) 363–385.
[6] C. Mauduit, C. Pomerance, A. Sárközy, On the distribution in residue classes of integers with a fixed digit sum, Ramanujan J. 9 (2005) 45–62.
[7] C. Pomerance, I.E. Shparlinski, Smooth orders and cryptographic applications, in: Proc. ANTS-V, Sydney, Australia, in: Lecture Notes in Comput. Sci., vol. 2369, Springer, 2002, pp. 338–348.
[8] J. Schmid, The joint distribution of the binary digits of integer multiples, Acta Arith. 43 (1984) 391–415.
[9] W.M. Schmidt, The joint distribution of the digits of certain integer s-tuples, Stud. Pure Math., Birkhäuser, Basel, 1983.
[10] N.J.A. Sloane, The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/.
[11] W. Steiner, On the joint distribution of q-additive functions on polynomial sequences, in: Proceedings of the Conference Dedicated to the 90th Anniversary of Boris Vladimirovich Gnedenko, Kyiv, 2002, Theory Stoch. Process. 8 (2002) 336–357.
[12] K.B. Stolarsky, Integers whose multiples have anomalous digital frequencies, Acta Arith. 38 (1980) 117–128.
[13] G. Tenenbaum, Crible d'Ératosthène et modèle de Kubilius, in: K. Győry, H. Iwaniec, J. Urbanowicz (Eds.), Number Theory in Progress, Proceedings of the Conference in Honor of Andrzej Schinzel, Zakopane, Poland, 1997, Walter de Gruyter, Berlin, 1999, pp. 1099–1129.
[14] G. Tenenbaum, Integers with a large friable component, Acta Arith. 124 (2006) 287–291.