JOURNAL OF NUMBER THEORY 33, 132–151 (1989)

On the Joint Distribution of Digital Sums

JEROME A. SOLINAS

Department of Defense, Ft. Meade, Maryland 20755

Communicated by P. T. Bateman

Received July 9, 1987; revised January 7, 1989

Let $s(n)$ be the sum of the digits of n written to the base b. We determine the joint distribution (modulo m) of the sequences $s(k_1 n), ..., s(k_\ell n)$. In the case where m and $b-1$ are relatively prime, we find that their values are equally distributed among ℓ-tuples of residue classes (modulo m). © 1989 Academic Press, Inc.

1. INTRODUCTION

Given an integer $b \geqslant 2$, denote by $s(n)$ the sum of the digits of the non-negative integer n expressed to the base b. A. O. Gelfond [2] proved that, if $k \geqslant 1$, $m \geqslant 2$, and $(m, b-1) = 1$, then the numbers $s(kn)$, $n = 0, 1, 2, ...$ are distributed equally among residue classes (mod m). In this paper we consider the joint distribution (mod m) of the sequences $s(k_1 n), ..., s(k_\ell n)$ in the general case.

Throughout this paper, all variables are positive integers unless stated otherwise. We will assume that $\ell \geqslant 1$, $m \geqslant 2$, $b \geqslant 2$, and that $k_1, ..., k_\ell$ are distinct. Since $s(bn) = s(n)$ for all n, we lose no generality in assuming that $b \nmid k_j$ for $j = 1, ..., \ell$.

For arbitrary $r_1, ..., r_\ell$, form the system of congruences

$$s(k_j n) \equiv r_j \pmod{m}, \; j = 1, ..., \ell. \tag{$*$}$$

We will prove the existence of, and evaluate, the rational number

$$L = \lim_{N \to \infty} \frac{1}{N} \operatorname{card}\{0 \leqslant n < N : n \text{ satisfies } (*)\}.$$

We begin with a simple argument giving a necessary condition for $(*)$ to have a solution. We will let $g = (m, b-1)$ throughout this paper.

PROPOSITION 1. *If $(*)$ has a solution, then so does the system*

$$k_j n \equiv r_j \pmod{g}, \; j = 1, ..., \ell. \tag{$**$}$$

0022-314X/89 $3.00

Proof. Since

$$s(k_j n) \equiv k_j n \qquad (\text{mod } b-1)$$

for every j, it follows that

$$s(k_j n) \equiv k_j n \qquad (\text{mod } g)$$

for every j. Thus every solution of (*) also satisfies (**). ∎

It follows from the elementary theory of congruences that, if (**) has a solution, it has precisely $(d_1, \ldots, d_\ell)$ solutions, where

$$d_j = (k_j, g), \qquad j = 1, \ldots, \ell.$$

Thus if the sequences $(s(k_j n))$ are statistically independent $(\text{mod } m)$, we expect the following theorem.

THEOREM 1. *If (**) has a solution, then*

$$L = \left(\frac{g}{m}\right)^\ell \frac{(d_1, \ldots, d_\ell)}{g}.$$

As special cases, we have the following generalizations of Gelfond's theorem.

COROLLARY 1. *If $(m, b-1) = 1$, and (**) has a solution, then $L = 1/m^\ell$.*

COROLLARY 2. *Let $\ell = 1$. If $(m, b-1, k_1) \mid r_1$ in (**), then $L = (m, b-1, k_1)/m$.*

2. TYPE ℓ SUMS

To prove Theorem 1, we investigate the sum

$$\sum_{0 \leqslant n < N} e\left(\frac{1}{m} \sum_{j=1}^{\ell} a_j s(k_j n)\right), \tag{1}$$

where $e(x) = \exp(2\pi i x)$ and $0 \leqslant a_j < m$ for $j = 1, \ldots, \ell$. In an extension of common usage we call (1) a *Type ℓ sum.*

LEMMA 1. *If $n = n'b^r + n''$, where $0 \leqslant n'' < b^r$, then*

$$s(n) = s(n') + s(n'').$$

Proof. If $n=\sum_i \varepsilon_i b^i$, then $n'=\sum_{i\geqslant r}\varepsilon_i b^{i-r}$ and $n''=\sum_{i<r}\varepsilon_i b^i$. The result follows since $\sum_i \varepsilon_i=\sum_{i\geqslant r}\varepsilon_i+\sum_{i<r}\varepsilon_i$. ∎

LEMMA 2. $s(k(n+wb^r))=s([kn/b^r]+kw)+s(kn)-s([kn/b^r])$.

Proof. By Lemma 1,

$$s(kn+kwb^r))=s\left(\left[\frac{kn}{b^r}\right]+kw\right)+s\left(kn-\left[\frac{kn}{b^r}\right]b^r\right)$$

and

$$s\left(kn-\left[\frac{kn}{b^r}\right]b^r\right)=s(kn)-s\left(\left[\frac{kn}{b^r}\right]\right). \quad ∎$$

Let $K=[k_1, ..., k_\ell]$. For $0\leqslant h<K$, we define

$$\begin{aligned} T(r, v, h) &= \sum_{(v+h/k)b^r\leqslant n<(v+(h+1)/k)b^r} e\left(\frac{1}{m}\sum_{j=1}^{\ell} a_j s(k_j n)\right),\\ T(r, v) &= \sum_{0\leqslant h<K} T(r, v, h)=\sum_{vb^r\leqslant n<(v+1)b^r} e\left(\frac{1}{m}\sum_{j=1}^{\ell} a_j s(k_j n)\right). \end{aligned} \tag{2}$$

LEMMA 3. *For* $0\leqslant u<b$, *let*

$$\xi_j=\left[\frac{bh+u}{K/k_j}\right], \qquad \lambda=\left[\frac{bh+u}{K}\right].$$

Let $\zeta(h, u, v)$ *be the complex number*

$$e\left(\frac{1}{m}\sum_{j=1}^{\ell} a_j(s(k_j bv+\xi_j)-s(\xi_j-k_j\lambda))\right). \tag{3}$$

Then

$$T(r+1, v, h)=\sum_{0\leqslant u<b} \zeta(h, u, v)\, T(r, 0, bh+u-K\lambda).$$

Proof. Write

$$T(r+1, v, h)=\sum_{0\leqslant u<b}\ \sum_{(bv+(bh+u)/K)b^r\leqslant n<(bv+(bh+u+1)/K)b^r} e\left(\frac{1}{m}\sum_{j=1}^{\ell} a_j s(k_j n)\right),$$

and in each inner sum replace n by $n+(bv+\lambda)b^r$. The inner sums become

$$\sum_{((bh+u)/K-\lambda)b^r\leqslant n<((bh+u+1)/K-\lambda)b^r} e\left(\frac{1}{m}\sum_{j=1}^{\ell} a_j s(k_j(n+(bv+\lambda)b^r))\right).$$

By Lemma 2 with $k = k_j$ and $w = bv + \lambda$, the summand equals

$$e\left(\frac{1}{m}\sum_{j=1}^{\ell} a_j\left(s\left(\left[\frac{k_j n}{b^r}\right] + k_j(bv+\lambda)\right) + s(k_j n) - s\left(\left[\frac{k_j n}{b^r}\right]\right)\right)\right).$$

The result now follows from the observation that

$$\left[\frac{k_j n}{b^r}\right] = \xi_j - k_j \lambda$$

in each inner sum. ∎

LEMMA 4. *Let $A(v)$ be the K-by-K matrix whose (h, i)th entry is*

$$A_{v,1}(h, i) = \sum_{\substack{0 \leqslant u < b \\ bh + u \equiv i \pmod K}} \zeta(h, u, v). \tag{4}$$

Then

$$\begin{bmatrix} T(r+1, v, 0) \\ \vdots \\ T(r+1, v, K-1) \end{bmatrix} = A(v) \begin{bmatrix} T(r, 0, 0) \\ \vdots \\ T(r, 0, K-1) \end{bmatrix}.$$

Proof. The result follows at once from Lemma 3 by matrix multiplication. ∎

The following is an immediate corollary of Lemma 4.

PROPOSITION 2. *If $r \geqslant 1$, then*

$$\begin{bmatrix} T(r, v, 0) \\ T(r, v, 1) \\ \vdots \\ T(r, v, K-1) \end{bmatrix} = A(v)\, A(0)^{r-1} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{5}$$

3. TYPE ℓ MATRICES

We call the matrices $A(v)$ *Type ℓ matrices.* We assume throughout this section that $v = 0$. It is clear from (3) that

$$\zeta(h, u, 0) = 1$$

for $0 \leqslant bh + u < K$.

Denote by $A_{v,r}(h, i)$ the (h, i)th entry of $A(v)^r$. By (4),

$$T(r, 0, h) = A_{0,r}(h, 0). \tag{6}$$

We now derive a formula for $A_{0,r}(h, i)$.

For $\lambda \geqslant 0$ and $0 \leqslant i < K$, we make the (invertible) change of variables

$$K\lambda + i = bh + u, \tag{7}$$

where $h \geqslant 0$, $0 \leqslant u < b$. We now define the function $a(\lambda, i)$ as follows: for $0 \leqslant \lambda < b$,

$$a(\lambda, i) = \zeta(h, u, 0).$$

For

$$\begin{gathered} \lambda = \mu b^r + v, \qquad 0 \leqslant \mu < b,\ 0 \leqslant v < b^r, \\ a(\lambda, i) = a(v, i)\, a\left(\mu, \left[\frac{Kv + i}{b^r}\right]\right). \end{gathered} \tag{8}$$

We note that

$$a(0, i) = 1 \qquad \text{for} \quad 0 \leqslant i < K. \tag{9}$$

LEMMA 5. *For all* r, $0 \leqslant h < K$, $0 \leqslant i < K$,

$$A_{0,r}(h, i) = \sum_{\substack{\lambda \\ hb^r \leqslant K\lambda + i < (h+1)b^r}} a(\lambda, i). \tag{10}$$

Thus

$$|A_{0,r}(h, i)| \leqslant \sum_{\substack{\lambda \\ hb^r \leqslant K\lambda + i < (h+1)b^r}} 1. \tag{11}$$

Proof. The result is easily verified for $r = 0$, and the case $r = 1$ follows at once from (4) and (7). Assume that (10) holds for r; we prove it for $r + 1$. By matrix multiplication,

$$A_{0,r+1}(h, i) = \sum_{0 \leqslant \gamma < K} A_{0,1}(h, \gamma)\, A_{0,r}(\gamma, i).$$

By the induction hypothesis, this is

$$\sum_{0 \leqslant \gamma < K} \sum_{\substack{\mu \\ hb \leqslant K\mu + \gamma < (h+1)b}} a(\mu, \gamma) \sum_{\substack{v \\ \gamma b^r \leqslant Kv + i < (\gamma+1)b^r}} a(v, i).$$

Let $\psi = K\mu + \gamma$. We may regard μ and γ as functions of ψ, namely, $\mu = [\psi/K]$ and $\gamma = \psi - K[\psi/K]$. Thus we can rewrite the sum over γ and μ as a sum over ψ; i.e.,

$$A_{0,r+1}(h, i) = \sum_{\substack{\psi \\ hb \leqslant \psi < (h+1)b}} a(\mu, \gamma) \sum_{\substack{v \\ \gamma b^r \leqslant Kv + i < (\gamma+1)b^r}} a(v, i).$$

We now make the substitution (8) in the inner sum; then

$$a(\lambda, i) = a(v, i)\, a(\mu, \gamma).$$

Thus

$$A_{0,r+1}(h, i) = \sum_{\substack{\psi \\ hb \leqslant \psi < (h+1)b}} \sum_{\substack{\lambda \\ (K\mu+\gamma)b^r \leqslant K\lambda + i < (K\mu+\gamma+1)b^r}} a(\lambda, i).$$

Since $\psi = K\mu + \gamma$, this becomes

$$= \sum_{\substack{\lambda \\ hb^{r+1} \leqslant K\lambda + i < (h+1)b^{r+1}}} a(\lambda, i),$$

which completes the induction. ∎

We say that the Type ℓ matrix $A(0)$ is *trivial* if $a(\lambda, i) = 1$ for $0 \leqslant \lambda < b$, $0 \leqslant i < K$. If $A(0)$ is trivial, it follows from (8) that

$$a(\lambda, i) = 1 \qquad \text{for all} \quad \lambda \geqslant 0, \quad 0 \leqslant i < K. \tag{12}$$

LEMMA 6. *If the matrix associated with the Type ℓ sum $T(r, 0)$ is trivial, then $T(r, 0) = b^r$.*

Proof. By (2) and (6),

$$T(r, 0) = \sum_{0 \leqslant h < K} A_{0,r}(h, 0).$$

By Lemma 5, this is

$$\sum_{0 \leqslant h < T} \sum_{\substack{\lambda \\ hb^r \leqslant K\lambda < (h+1)b^r}} a(\lambda, 0).$$

The result now follows from (12). ∎

PROPOSITION 3. *If the matrix associated with the sum $T(r, 0)$ is trivial, then for all $n \geqslant 0$,*

$$e\left(\frac{1}{m} \sum_{j=1}^{\ell} a_j s(k_j n)\right) = 1.$$

Thus

$$\sum_{j=1}^{\ell} a_j s(k_j n) \equiv 0 \pmod{m}.$$

Proof. Given $n \geqslant 0$, choose r so that $b^r > n$. By Lemma 6, $T(r, 0)$ is a sum of b^r unimodular complex numbers adding to b^r. Thus each term of $T(r, 0)$ equals 1. ∎

We now investigate nontrivial matrices. If $A(0)$ is nontrivial, then $a(\lambda_0, i_0) \neq 1$ for some $0 \leqslant \lambda_0 < b$, $0 \leqslant i_0 < K$. By (9), $\lambda_0 \neq 0$.

Choose $r' > 1 + \log_b K$, so that $b^{r'} > Kb$. It is easily seen that the sum (10) for each entry of $A^{r'}$ is nonempty.

LEMMA 7. *If A is nontrivial, then*

$$|A_{0,r'}(0, i_0)| < \sum_{\substack{\lambda \\ 0 \leqslant K\lambda + i_0 < b^{r'}}} 1.$$

Proof. By (10),

$$A_{0,r'}(0, i_0) = \sum_{\substack{\lambda \\ 0 \leqslant K\lambda + i_0 < b^{r'}}} a(\lambda, i_0).$$

This sum contains both $a(0, i_0) = 1$ and $a(\lambda_0, i_0) \neq 1$. The result follows since (10) is a sum of unimodular terms not all equal. ∎

LEMMA 8. *If A is nontrivial, then for $0 \leqslant i < K$,*

$$|A_{0,2r'}(0, i)| < \sum_{\substack{\lambda \\ 0 \leqslant K\lambda + i < b^{2r'}}} 1.$$

Proof. From the identity $A^{2r'} = A^{r'} A^{r'}$ and matrix multiplication,

$$A_{0,2r'}(0, i) = \sum_{0 \leqslant \gamma < K} A_{0,r'}(0, \gamma)\, A_{0,r'}(\gamma, i). \tag{13}$$

For $r=r'$, the sum in (10) is nonempty for each (h, i). Thus it follows from (11) and Lemma 7 that

$$|A_{0,r'}(0, i_0)\,A_{0,r'}(i_0, i)| \leqslant \Bigg(\sum_{\substack{\lambda \\ 0 \leqslant K\lambda + i_0 < b^{r'}}} 1\Bigg)\Bigg(\sum_{\substack{\mu \\ i_0 b^{r'} \leqslant K\mu + i < (i_0+1)b^{r'}}} 1\Bigg).$$

Combining this with (11) and (13) yields

$$|A_{0,2r'}(0, i)| < \sum_{0 \leqslant \gamma < K} \sum_{\substack{\lambda \\ 0 \leqslant K\lambda + \gamma < b^{r'}}} \sum_{\substack{\mu \\ \gamma b^{r'} \leqslant K\mu + i < (\gamma+1)b^{r'}}} 1.$$

The result follows upon rearranging this triple sum. ∎

LEMMA 9. *If A is nontrivial, then for $0 \leqslant i < K$,*

$$\sum_{0 \leqslant h < K} |A_{0,2r'}(h, i)| < b^{2r'}.$$

Proof. By (11) and Lemma 8,

$$\sum_{0 \leqslant h < K} |A_{0,2r'}(h, i)| < \sum_{0 \leqslant h < K} \sum_{\substack{\lambda \\ hb^{2r'} \leqslant K\lambda + i < (h+1)b^{2r'}}} 1,$$

from which the result follows. ∎

In a similar way we can prove

LEMMA 10. *For all $v \geqslant 0$, $0 \leqslant i < K$,*

$$\sum_{0 \leqslant h < K} |A_{v,1}(h, i)| \leqslant b.$$

4. APPLICATION TO TYPE ℓ SUMS

PROPOSITION 4. *If the associated Type ℓ matrix is trivial, then*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{0 \leqslant n < N} e\left(\frac{1}{m} \sum_{j=1}^{\ell} a_j s(k_j n)\right) = 1.$$

Proof. This follows at once from Proposition 3. ∎

We begin our investigation of the nontrivial case with the following lemma, whose proof follows easily by matrix multiplication.

LEMMA 11. *Let $A = [a_{h,i}]$ be a K-by-K matrix and let*

$$\mathbf{v} = \begin{bmatrix} v(0) \\ \vdots \\ v(K-1) \end{bmatrix}.$$

Define $N(\mathbf{v}) = \sum_{0 \leqslant i < K} |v(i)|$, and suppose that $\sum_{0 \leqslant h < K} |a_{hi}| \leqslant M$ for $0 \leqslant i < K$. Then $N(A\mathbf{v}) \leqslant MN(\mathbf{v})$.

LEMMA 12. *If the matrix A corresponding to the sum $T(r, 0)$ is non-trivial, then for $a \geqslant 0$, $v \geqslant 0$,*

$$|T(2ar'+1, v)| \leqslant b^{2(1-\delta)ar'+1}$$

for some real $\delta > 0$ which is independent of v.

Proof. For all $r \geqslant 0$,

$$|T(r, v)| \leqslant \sum_{0 \leqslant h < K} |T(r, v, h)| = N\left(\begin{bmatrix} T(r, v, 0) \\ \vdots \\ T(r, v, K-1) \end{bmatrix}\right).$$

Thus, by Proposition 2,

$$|T(2ar'+1, v)| \leqslant N\left(A(v)\, A(0)^{2ar'} \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}\right).$$

It now follows from Lemmas 9, 10, and 11 that

$$|T(2ar'+1, v)| \leqslant bc^a N\left(\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}\right),$$

where $c = \sum_{0 \leqslant h < K} |A_{0,2r'}(h, i)|$. Since $c < b^{2r'}$, then $c = b^{2r'(1-\delta)}$ for some $\delta > 0$. Since

$$N\left(\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}\right) = 1,$$

the result is established. ∎

The next lemma is an easy corollary of Lemma 12.

LEMMA 13. *If the matrix A corresponding to the sum $T(r, 0)$ is nontrivial, then for some $\delta > 0$,*

$$T(r, v) \ll b^{(1-\delta)r}$$

uniformly for $r \geqslant 0$, $v \geqslant 0$.

PROPOSITION 5. *If the matrix A corresponding to the sum $T(r, 0)$ is nontrivial, then for some $\delta > 0$,*

$$\sum_{0 \leqslant n < N} e\left(\frac{1}{m} \sum_{j=1}^{\ell} a_j s(k_j n)\right) \ll N^{1-\delta}$$

as $N \to \infty$.

Proof. We partition the interval $0 \leqslant n < N$ into subintervals of the form $v_i b^{r_i} \leqslant n < (v_i + 1) b^{r_i}$, where $0 \leqslant r_i \leqslant \log_b N$ for all i, and where each value of r_i appears in at most $b-1$ subintervals. The sum in question is bounded by $\sum_i |T(r_i, v_i)|$, which by Lemma 13 is

$$\ll \sum_i b^{(1-\delta) r_i}$$

$$\ll (b-1) \sum_{0 \leqslant i \leqslant \log_b N} b^{(1-\delta) i}.$$

The result follows upon summing this geometric series. ∎

PROPOSITION 6. *If the matrix associated with $T(r, 0)$ is nontrivial, then for some $n \geqslant 0$,*

$$\sum_{j=1}^{\ell} a_j s(k_j n) \not\equiv 0 \pmod{m}.$$

Proof. Were this not the case, we would have

$$T(r, 0) = b^r$$

for all $r \geqslant 0$, in contradiction to Lemma 13. ∎

5. DETERMINATION OF TRIVIAL AND NONTRIVIAL SUMS

By Propositions 3 and 6, the matrix $A(0)$ associated with the sum $T(r, 0)$ is nontrivial if and only if

$$\sum_{j=1}^{\ell} a_j s(k_j n) \not\equiv 0 \pmod{m}$$

for some $n \geq 0$. We now determine precisely when this happens. We consider two cases.

PROPOSITION 7. *Suppose that* $m \mid a_j(b-1)$ *for* $j = 1, ..., \ell$. *Then*

$$\sum_{j=1}^{\ell} a_j s(k_j n) \equiv 0 \pmod{m} \tag{14}$$

for all n if and only if

$$\sum_{j=1}^{\ell} a_j k_j \equiv 0 \pmod{m}. \tag{15}$$

Proof. We have

$$s(k_j n) \equiv k_j n \pmod{b-1}$$

for all n. Thus for all n,

$$a_j s(k_j n) \equiv a_j k_j n \pmod{a_j(b-1)},$$

so that

$$a_j s(k_j n) \equiv a_j k_j n \pmod{m}.$$

It is clear from this that if (15) holds, then (14) holds for all $n \geq 0$, and that if (15) fails, then (14) fails for $n = 1$. ∎

PROPOSITION 8. *Suppose that* $m \nmid a_j(b-1)$ *for some j. Then for some n,*

$$\sum_{j=1}^{\ell} a_j s(k_j n) \not\equiv 0 \pmod{m}. \tag{16}$$

Before giving the proof, we establish some lemmas.

Let k be the largest k_j for which $m \nmid a_j(b-1)$, and let a be the coefficient a_j corresponding to k. We further put $h = (k, b)$. Note that $h < b$ since we are assuming that $b \nmid k$.

LEMMA 14. *There exists* $f > 0$ *such that*

(i) $b \nmid (fk/h + 1)v$ *for* $1 \leq v < h$

(ii) $b \mid fk + h$

(iii) $b^2 \nmid fk + h$.

Proof. Let w be the largest divisor of b which is relatively prime to b/h.

Then

$$w \mid h, \qquad \left(w, \frac{h}{w}\right) = 1.$$

Choose u relatively prime to h/w. Then the congruence system

$$\begin{aligned} t &\equiv u \qquad \left(\mathrm{mod}\ \frac{h}{w}\right) \\ \frac{b}{h}\, t &\equiv 1 \qquad (\mathrm{mod}\ w) \end{aligned} \tag{17}$$

has a solution $t > 0$, and $(t, h) = 1$. Since $h = (b, k)$, we can define f_0 by

$$0 < f_0 \leqslant \frac{b}{h}, \qquad f_0 k \equiv -h \qquad (\mathrm{mod}\ b).$$

Let $\lambda = f_0 k/h$; then

$$h\lambda \equiv -h \qquad (\mathrm{mod}\ b).$$

Thus $(\lambda, b/h) = 1$, and therefore

$$\left((\lambda, b), \frac{b}{h}\right) = 1.$$

Since also $(\lambda, b) \mid b$, then by the maximality of w,

$$(\lambda, b) \mid w. \tag{18}$$

Let $\mu = tb/h - 1$; then $w \mid \mu$ by (17), and

$$h\mu \equiv -h \qquad (\mathrm{mod}\ b). \tag{19}$$

Since $w \mid \mu$, then $(\lambda, b) \mid \mu$ by (18), and so the congruence

$$f_1 \lambda \equiv \mu \qquad (\mathrm{mod}\ b) \tag{20}$$

has a solution $f_1 > 0$. Let $f = f_0 f_1$; then by (20),

$$\frac{fk}{h} + 1 \equiv \frac{tb}{h} \qquad (\mathrm{mod}\ b).$$

Since $(t, h) = 1$, conditions (i) and (ii) follow. Condition (iii) follows from (i) since $bh \nmid fk + h$. ∎

From the inequality

$$\frac{h}{k+1} < \frac{h}{k} < \min\left(\frac{h+1}{k}, \frac{h}{k-1}\right)$$

we see that, for sufficiently large γ, we can choose positive integers α and β such that

$$\frac{h}{k+1}\,b^{\gamma} < \alpha < \frac{h}{k}\,b^{\gamma} < \beta < \min\left(\frac{h+1}{k}, \frac{h}{k-1}\right) b^{\gamma}.$$

We may rewrite these inequalities as

$$\begin{aligned} k\alpha &< hb^{\gamma} < (k+1)\alpha, \\ (k-1)\beta &< hb^{\gamma} < k\beta < (h+1)b^{\gamma}. \end{aligned} \tag{21}$$

We define

$$\begin{aligned} \tau_1 &= fb^{\gamma} + \alpha \\ \tau_2 &= fb^{\gamma+1} + \alpha \\ \tau_3 &= fb^{\gamma} + \beta \\ \tau_4 &= fb^{\gamma+1} + \beta, \end{aligned} \tag{22}$$

where f is as defined in Lemma 14. For $i = 1, 2, 3, 4$, let

$$S_i = \sum_{j=1}^{\ell} a_j s(k_j \tau_i).$$

Finally, we partition the set $\{1, 2, ..., \ell\}$ into the following classes:

$$\begin{aligned} T &= \left\{ j\colon k_j = \frac{v}{h} k \text{ for some } v \leqslant h \right\} \\ J &= \{ j \notin T\colon m \nmid a_j(b-1) \} \\ I &= \{ j \notin T\colon m \mid a_j(b-1) \}. \end{aligned}$$

LEMMA 15. *For* $i = 1, 2$,

$$\sum_{j \in I} a_j s(k_j \tau_{2i-1}) \equiv \sum_{j \in I} a_j s(k_j \tau_{2i}) \qquad (\text{mod } m).$$

Proof. Since $\tau_{2i-1} \equiv \tau_{2i} \pmod{b-1}$, then

$$s(k_j \tau_{2i-1}) \equiv s(k_j \tau_{2i}) \qquad (\text{mod } b-1)$$

for all $j \in I$. The result follows since $m \mid a_j(b-1)$ for all $j \in I$. ▮

The following lemma is an immediate corollary.

LEMMA 16. *$S_1 - S_2 - S_3 + S_4 \equiv S'_1 - S'_2 - S'_3 + S'_4 \pmod{m}$, where*

$$S'_i = \sum_{j \in T \cup J} a_j s(k_j \tau_i).$$

We now restrict our attention to $j \in T \cup J$. For such j, $k_j \leqslant k$. We write

$$\begin{aligned} fk_j &= bu_j + u'_j, & 0 &\leqslant u'_j < b \\ \alpha k_j &= b^\gamma v_j + v'_j, & 0 &\leqslant v'_j < b^\gamma \\ \beta k_j &= b^\gamma w_j + w'_j, & 0 &\leqslant w'_j < b^\gamma. \end{aligned} \tag{23}$$

LEMMA 17. *If $j \in J$, then $v_j = w_j$.*

Proof. Since $\alpha \leqslant \beta$ by (21), then $v_j \leqslant w_j$. Suppose that $v_j < w_j$; then by (23),

$$\alpha k_j < w_j b^\gamma < \beta k_j. \tag{24}$$

Now $k_j < k$ since $j \in J$; thus $k_j \beta < hb^\gamma$ by (21). We conclude that $1 \leqslant w_j < h$. It follows from (21) that

$$\frac{w_j}{h} k\alpha < w_j b^\gamma < \left(\frac{w_j}{h} k + 1\right) \alpha,$$

$$\left(\frac{w_j}{h} k - 1\right) \beta < w_j b^\gamma < \frac{w_j}{h} k\beta.$$

By (24), this implies that $k_j = (w_j/h)k$, contrary to the hypothesis that $j \in J$. This contradiction establishes the result. ▮

LEMMA 18. *$S_1 - S_2 - S_3 + S_4 \equiv S''_1 - S''_2 - S''_3 + S''_4 \pmod{m}$, where*

$$S''_i = \sum_{j \in T} a_j s(k_j \tau_i).$$

Proof. By (22) and (23),

$$
\begin{aligned}
k_j\tau_1 &= u_j b^{\gamma+1} + (u_j' + v_j) b^\gamma + v_j' \\
k_j\tau_2 &= u_j b^{\gamma+2} + u_j' b^{\gamma+1} + v_j b^\gamma + v_j' \\
k_j\tau_3 &= u_j b^{\gamma+1} + (u_j' + w_j) b^\gamma + w_j' \\
k_j\tau_4 &= u_j b^{\gamma+2} + u_j' b^{\gamma+1} + w_j b^\gamma + w_j'.
\end{aligned} \tag{25}
$$

By Lemma 17,

$$s(k_j\tau_1) - s(k_j\tau_2) - s(k_j\tau_3) + s(k_j\tau_4) = 0$$

for $j \in J$. The result now follows from Lemma 16. ▮

LEMMA 19. *If* $k_j = vk/h$, $1 \leqslant v \leqslant h$, *then* $u_j' = b - v$ *if and only if* $v = h$.

Proof. By Lemma 14,

$$\left(\frac{fk}{h} + 1\right) v \equiv 0 \qquad (\text{mod } b)$$

if and only if $v = h$. Thus

$$fk_j \equiv -v \qquad (\text{mod } b)$$

if and only if $v = h$. ▮

LEMMA 20. *If* $k_j = vk/h$, $1 \leqslant v \leqslant h$, *then* $v_j = v - 1$ *and* $w_j = v$.

Proof. Since $h \leqslant k$, then

$$\left(\frac{v-1}{h} k + 1\right) \alpha \leqslant \frac{v}{h} k\alpha.$$

But

$$(v-1) b^\gamma \leqslant \left(\frac{v-1}{h} k + 1\right) \alpha$$

by (21), so that

$$(n-1) b^\gamma \leqslant \frac{v}{h} k\alpha.$$

Since also

$$\frac{v}{h} k\alpha < v b^\gamma$$

by (21), we conclude by (23) that $v_j = v - 1$. A similar argument establishes that $w_j = v$ for $1 \leqslant v < h$, and this follows for $v = h$ from (21). ▮

LEMMA 21. $S_1 - S_2 - S_3 + S_4 \equiv a(s(k\tau_1) - s(k\tau_2) - s(k\tau_3) + s(k\tau_4))$ (mod m).

Proof. Let $j \in T$, $k_j \neq k$. Then $k_j = (v/h)k$ where $1 \leqslant v < h$. By the two preceding lemmas, we have

$$u'_j \neq b - v, \qquad v_j = v - 1, \qquad w_j = v.$$

Thus

$$s(bu_j + u'_j + v_j) = s(bu_j + u'_j + w_j) - 1.$$

Therefore, by (25),

$$s(k_j\tau_1) - s(k_j\tau_2) - s(k_j\tau_3) + s(k_j\tau_4) = 0.$$

The result now follows from Lemma 18. ▮

LEMMA 22. $a(s(k\tau_1) - s(k\tau_2) - s(k\tau_3) + s(k\tau_4)) \not\equiv 0$ (mod m).

Proof. Let $k = k_j$. By Lemmas 19 and 20,

$$u'_j = b - h, \qquad v_j = h - 1, \qquad w_j = h.$$

Thus by (25),

$$s(k\tau_1) - s(k\tau_2) - s(k\tau_3) + s(k\tau_4) = s(u_j) - s(u_j + 1) + b. \tag{26}$$

Now

$$fk + h = (u_j + 1)b$$

by (23) and Lemma 19. Thus $b \nmid u_j + 1$ by Lemma 14. It follows that $s(u_j + 1) = s(u_j) + 1$. By (26) we conclude that

$$s(k\tau_1) - s(k\tau_2) - s(k\tau_3) + s(k\tau_4) = b - 1.$$

Since k and a were chosen so that $m \nmid a(b-1)$, the result follows. ▮

Proof of Proposition 8. By Lemmas 21 and 22,

$$S_1 - S_2 - S_3 + S_4 \not\equiv 0 \qquad (\text{mod } m),$$

so that

$$S_i \not\equiv 0 \qquad (\text{mod } m)$$

for some i. Thus (16) is satisfied with $n = \tau_i$. ▮

6. Proof of Theorem 1

We begin the proof by writing

$$C_N = \text{card}\{0 \leqslant n < N\colon s(k_j n) \equiv r_j \pmod m \text{ for } j = 1, ..., \ell\}$$
$$= \sum_{0 \leqslant n < N} \prod_{j=1}^{\ell} \frac{1}{m} \sum_{0 \leqslant a < m} e\left(\frac{a}{m}(s(k_j n) - r_j)\right).$$

Multiplying out the sums and rearranging, we obtain

$$C_N = \frac{1}{m^\ell} \sum_{0 \leqslant a_1 < m} \cdots \sum_{0 \leqslant a_\ell < m} e\left(-\frac{1}{m}\sum_j a_j r_j\right) \sum_{0 \leqslant n < N} e\left(\frac{1}{m}\sum_j a_j s(k_j n)\right).$$

By Propositions 4 and 5, the (rational) limit

$$L = \lim_{N \to \infty} \frac{C_N}{N}$$

exists, and

$$L = \frac{1}{m^\ell} \sum_{\substack{0 \leqslant a_1 < m \\ (a_1, ..., a_\ell) \in R}} \cdots \sum_{0 \leqslant a_\ell < m} e\left(-\frac{1}{m}\sum_j a_j r_j\right),$$

where R is the set of ℓ-tuples $(a_1, ..., a_\ell)$ for which the corresponding Type ℓ sum is trivial.

By Propositions 3 and 6, R is the set of ℓ-tuples $(a_1, ..., a_\ell)$ for which

$$\sum_{j=1}^{\ell} a_j s(k_j n)) \equiv 0 \pmod m$$

for all $n \geqslant 0$. By Propositions 7 and 8, this implies that

$$L = \frac{1}{m^\ell} \sum_{\substack{0 \leqslant a_1 < m \\ m \mid a_1(b-1) \\ m \mid \sum_j a_j k_j}} \cdots \sum_{\substack{0 \leqslant a_\ell < m \\ m \mid a_\ell(b-1)}} e\left(-\frac{1}{m}\sum_j a_j r_j\right).$$

Therefore

$$L = \frac{1}{m^{2\ell+1}} \sum_{0 \leqslant a_1 < m} \cdots \sum_{0 \leqslant a_\ell < m} e\left(-\frac{1}{m}\sum_j a_j r_j\right) \sum_{0 \leqslant u < m} e\left(\frac{u}{m}\sum_j a_j k_j\right)$$
$$\cdot \sum_{0 \leqslant v_1 < m} e\left(\frac{a_1 v_1 (b-1)}{m}\right) \cdots \sum_{0 \leqslant v_\ell < m} e\left(\frac{a_\ell v_\ell (b-1)}{m}\right).$$

Rearranging this sum, we obtain

$$L=\frac{1}{m}\sum_{0\leqslant u<m}\prod_{j=1}^{\ell}\frac{1}{m}\sum_{0\leqslant v_j<m}\frac{1}{m}\sum_{0\leqslant a_j<m}e\left(\frac{a_j}{m}(k_ju+(b-1)v_j-r_j)\right).$$

Therefore

$$L=\frac{1}{m}\sum_{0\leqslant u<m}\prod_{j=1}^{\ell}\frac{1}{m}\operatorname{card}\{0\leqslant v_j<m: m\mid k_ju+(b-1)v_j-r_j\}.$$

We recall that $g=(b-1, m)$. The congruence

$$(b-1)v\equiv r-ku \qquad (\operatorname{mod} m)$$

has g solutions v if $g\mid r-ku$, and none if $g\nmid r-ku$. Thus

$$L=\frac{1}{m}\sum_{\substack{0\leqslant u<m\\ g\mid r_j-k_ju\\ \text{for } j=1,\ldots,\ell}}\prod_{j=1}^{\ell}\frac{g}{m}.$$

Therefore

$$L=\left(\frac{g}{m}\right)^{\ell}\frac{1}{m}\operatorname{card}\{0\leqslant u<m: k_ju\equiv r_j\ (\operatorname{mod} g), j=1,\ldots,\ell\}.$$

By the elementary theory of congruences, this implies that

$$L=\left(\frac{g}{m}\right)^{\ell}\frac{1}{g}\operatorname{card}\{0\leqslant u<g: k_ju\equiv r_j\ (\operatorname{mod} g), j=1,\ldots,\ell\}. \tag{27}$$

The congruence system appearing in (27) is just the system (**). The theorem now follows from our earlier remark that if (**) has a solution, then it has precisely $(d_1, \ldots, d_\ell)$ solutions.

7. Further Remarks

By taking more care in the above arguments, it is possible to give an explicit error bound for the remainder term

$$R(N)=\frac{C_N}{N}-L.$$

Indeed, it is shown in [3] that

$$|R(N)|\leqslant \tfrac{12}{11}b^5T^2N^{-\sigma}, \tag{28}$$

where

$$\sigma = \frac{4\sin^2(\pi/2m)}{b^4T^2\log(b^4T^2)}.$$

This bound is far from best possible.

The results of this paper are easily generalized to deal with the system

$$s(k_jn+h_j) \equiv r_j \qquad (\mathrm{mod}\ m),\ j=1, ..., \ell \tag{***}$$

in the case where

$$h_j = \left[\frac{k_j\rho}{K}\right] \tag{29}$$

for some ρ with $0 \leqslant \rho < K$. Lemma 3 is easily generalized to this case, and the generalization of Theorem 1 follows at once. (See [3].)

For a system (***) where (29) does not hold, it can still be possible to obtain an analog of Lemma 4 using a matrix of a slightly different form. (See [3] for an example of this.) We conjecture that the techniques of this paper can be extended to generalize Theorem 1 to the case (***).

Gelfond's proof [2] of his theorem used generating functions rather than Type ℓ sums. Thus the proof of Theorem 1 provides a new proof of Gelfond's result. It is unlikely that generating functions can be used to obtain nontrivial bounds for Type ℓ sums with $\ell > 1$.

Finally, we mention another application of Type 2 sums. Gelfond [2] conjectured that, if $(m, b-1) = 1$, then the numbers $s(p)$ (p prime) are equally distributed among residue classes (mod m). This conjecture would be true if, for $a = 1, ..., m-1$,

$$\sum_{p \leqslant N} e\left(\frac{a}{m}s(p)\right) = o(\pi(N)) \tag{30}$$

as $N \to \infty$. By using Vaughan's version of Vinogradov's method of exponential sums [1], it is easily seen that (30) follows from the following conjecture.

CONJECTURE. *For all sufficiently large N there exist U and V such that $U \geqslant 2$, $V \geqslant 2$, $UV \leqslant N$, and such that for all M with $U \leqslant M \leqslant N/V$, we have*

$$\sum_{V<j\leqslant N/M}\ \sum_{V<k\leqslant N/M}\left(\sum_{\substack{M<n\leqslant 2M\\ n\leqslant N/j\\ n\leqslant N/k}} e\left(\frac{a}{m}(s(jn)-s(kn))\right)\right)^2 = o(N^2\log^{-12}N)\Bigg)$$

as $N \to \infty$.

The bounds (28) are far too weak to prove this conjecture.

Acknowledgment

The author expresses his gratitude to Professor Hugh L. Montgomery, who directed the doctoral thesis [3] of which this paper is a revision and expansion.

References

1. H. Davenport, "Multiplicative Number Theory," 2nd ed., Springer-Verlag, New York, 1980.
2. A. O. Gelfond, Sur les nombres qui ont des propriétés additives et multiplicatives données, *Acta Arithm.* **13** (1968), 259–265.
3. J. Solinas, "A Theorem of Metric Diophantine Approximation and Estimates for Sums Involving Binary Digits," Thesis, University of Michigan, August 1985.