Exact exponent in the remainder term of Gelfond’s digit theorem in the binary case

by

VLADIMIR SHEVELEV (Beer-Sheva)

1. Introduction. For integers $m > 1$ and $a \in [0, m - 1]$, define

\begin{equation}
T_{m,a}^{(j)}(x) = \sum_{0 \leq n < x, n \equiv a \mod m, s(n) \equiv j \mod 2} 1, \quad j = 1, 2,
\end{equation}

where $s(n)$ is the number of 1’s in the binary expansion of $n$. Gelfond [7] proved that

\begin{equation}
T_{m,a}^{(j)}(x) = \frac{x}{2m} + O(x^{\lambda}), \quad j = 0, 1,
\end{equation}

where

\begin{equation}
\lambda = \frac{\ln 3}{\ln 4} = 0.79248125 \ldots.
\end{equation}

This is the binary case of Gelfond’s main digit theorem about the distribution of digit sums of arbitrary base in different residue classes. Gelfond’s theorem initiated a whole line of research (see Notes on Chapter 3 in [1], as well as [10], [3], [9]). A related circle of works, dealing with the so-called Newman-like phenomena, started with the unexpected results of D. J. Newman [11] (see also [2], [5], [15]; again, an extensive bibliography may be found in [1]). In this paper, we shall be concerned only with the binary case of Gelfond’s digit theorem. Recently, the author proved [13] that the exponent $\lambda$ in the remainder term in (2) is the best possible when $m$ is a multiple of 3 and is not the best possible otherwise. In this paper we give a simple formula for the exact exponent in the remainder term of (2) for an arbitrary $m$. Our method is based on constructing a recursion relation for the Newman-like sum corresponding to (1),

\begin{equation}
S_{m,a}(x) = \sum_{0 \leq n < x, n \equiv a \mod m} (-1)^{s(n)}.
\end{equation}

2000 Mathematics Subject Classification: Primary 11A63.
Key words and phrases: cyclotomic cosets of 2 modulo $m$, order of 2 modulo $m$, difference equation, trigonometric sums.

DOI: 10.4064/aa136-1-7
It is sufficient for our purposes to deal with odd numbers \( m \). Indeed, it is easy to see that, if \( m \) is even, then

\[
S_{m,a}(2x) = (-1)^a S_{m/2,\lfloor a/2 \rfloor}(x).
\]

For \( m > 1 \) odd, consider the number \( r = r(m) \) of distinct cyclotomic cosets of 2 modulo \( m \) [8, pp. 104–105]. E.g., \( r(15) = 4 \), since for \( m = 15 \) we have the following four cyclotomic cosets of 2: \( \{1, 2, 4, 8\} \), \( \{3, 6, 12, 9\} \), \( \{5, 10\} \), \( \{7, 14, 13, 11\} \).

Note that, if \( C_1, \ldots, C_r \) are all different cyclotomic cosets of 2 modulo \( m \), then

\[
\bigcup_{j=1}^r C_j = \{1, \ldots, m-1\}, \quad C_{j_1} \cap C_{j_2} = \emptyset, \quad j_1 \neq j_2.
\]

Let \( h \) be the least common multiple of \( |C_1|, \ldots, |C_r| \),

\[
h = \lcm(|C_1|, \ldots, |C_r|).
\]

Note that \( h \) is of order 2 modulo \( m \) (this follows easily, e.g., from Exercise 3, p. 104 in [12]).

**Definition 1.** The exact exponent in the remainder term in (2) is \( \alpha = \alpha(m) \) if

\[
T_{m,a}^j(x) = \frac{x}{2m} + O(x^{\alpha+\varepsilon}), \quad T_{m,a}^j(x) = \frac{x}{2m} + \Omega(x^{\alpha-\varepsilon}), \quad \forall \varepsilon > 0.
\]

Our main result is the following.

**Theorem 1.** If \( m \geq 3 \) is odd, then the exact exponent in the remainder term in (2) is

\[
\alpha = \max_{1 \leq l \leq m-1} \left( 1 + \frac{1}{h \ln 2} \sum_{k=0}^{h-1} \ln \left| \sin \frac{\pi l 2^k}{m} \right| \right).
\]

Note that, if \( 2 \) is a primitive root of an odd prime \( p \), then \( r = 1, \ h = p-1 \). As a corollary of Theorem 1 we obtain the following result.

**Theorem 2.** If \( p \) is an odd prime for which \( 2 \) is a primitive root, then the exact exponent in the remainder term in (2) is

\[
\alpha = \frac{\ln p}{(p-1) \ln 2}.
\]

Theorem 2 generalizes the well-known result for \( p = 3 \) ([11], [2], [1]). Furthermore, we say that \( 2 \) is a semiprimitive root modulo \( p \) if \( 2 \) is of order \( (p-1)/2 \) modulo \( p \) and the congruence \( 2^x \equiv -1 \mod p \) is not solvable. E.g., \( 2 \) is of order 8 modulo 17, but the congruence \( 2^x \equiv -1 \mod 17 \) has the solution \( x = 4 \). Therefore, 2 is not a semiprimitive root of 17. The first
primes for which 2 is a semiprimitive root are (see [14, A 139035])

\[7, 23, 47, 71, 79, 103, 167, 191, 199, 239, 263, \ldots\]

For these primes we have \( r = 2 \) and \( h = (p - 1)/2 \). As a second corollary of Theorem 1 we obtain the following result.

**Theorem 3.** If \( p \) is an odd prime for which 2 is a semiprimitive root, then the exact exponent \( \alpha \) in the remainder term in (2) is also given by (9).

We also prove the following lower estimate for \( \alpha(m) \).

**Theorem 4.** For \( m \) odd,

\[ \alpha(m) \geq \frac{\ln m}{rh \ln 2}. \]

In particular, if \( m = p \) is prime, then \( rh = p - 1 \) and

\[ \alpha(p) \geq \frac{\ln p}{(p - 1) \ln 2}. \]

Note that, if Artin’s conjecture of the infinity of primes for which 2 is a primitive root is true, then by Theorem 2,

\[ \liminf_{p \to \infty} \alpha(p) = 0. \]

In Section 2 we provide an explicit formula for \( S_{m,a}(x) \), while in Sections 3–4 we prove Theorems 1–4.

**2. Explicit formula for** \( S_{m,a}(x) \). Let \( \lfloor x \rfloor = N \). We have

\[ S_{m,a}(N) = \sum_{n=0}^{N-1} (-1)^{s(n)} \frac{1}{m} \sum_{t=0}^{m-1} \sum_{n=0}^{N-1} (-1)^{s(n)} e^{2\pi i (n-a) t/m} \]

\[ = \frac{1}{m} \sum_{t=0}^{m-1} \sum_{n=0}^{N-1} e^{2\pi i \left( \frac{t}{m}(n-a) + \frac{1}{2}s(n) \right)}. \]

Note that the interior sum is of the form

\[ \Phi_{a,\beta}(N) = \sum_{n=0}^{N-1} e^{2\pi i (\beta(n-a)+\frac{1}{2}s(n))}, \quad 0 \leq \beta < 1. \]

Putting

\[ F_{\beta}(N) = e^{2\pi i \beta a} \Phi_{a,\beta}(N), \]

we note that \( F_{\beta}(N) \) does not depend on \( a \).

**Lemma 1.** If \( N = 2^{\nu_0} + 2^{\nu_1} + \cdots + 2^{\nu_{\sigma}} \) with \( \nu_0 > \nu_1 > \cdots > \nu_{\sigma} \geq 0 \), then

\[ F_{\beta}(N) = \sum_{g=0}^{\sigma} e^{2\pi i (\beta \sum_{j=0}^{g-1} 2^{\nu_j} + g/2)} \prod_{k=0}^{\nu_g-1} (1 + e^{2\pi i (\beta 2^k + 1/2)}). \]
Proof. Let $\sigma = 0$. Then by (12) and (13),

$$F_\beta(N) = \sum_{n=0}^{N-1} (-1)^{s(n)} e^{2\pi i \beta n}$$

$$= 1 - \sum_{j=0}^{\nu_0-1} e^{2\pi i \beta 2^j} + \sum_{0 \leq j_1 < j_2 \leq \nu_0-1} e^{2\pi i \beta (2j_1 + 2j_2)} - \ldots$$

$$= \prod_{k=0}^{\nu_0-1} (1 - e^{2\pi i \beta 2^k}),$$

which corresponds to (14) for $\sigma = 0$.

Assuming that (14) is valid for every $N$ with $s(N) = \sigma + 1$, let us consider $N_1 = 2^{\nu_\sigma} b + 2^{\nu_\sigma+1}$ where $b$ is odd, $s(b) = \sigma + 1$ and $\nu_{\sigma+1} < \nu_\sigma$. Let

$$N = 2^{\nu_\sigma} b = 2^{\nu_0} + \ldots + 2^{\nu_\sigma},$$

$$N_1 = 2^{\nu_0} + \ldots + 2^{\nu_\sigma} + 2^{\nu_{\sigma+1}}.$$ 

Notice that for $n \in [0, 2^{\nu_{\sigma+1}})$ we have

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

Therefore,

$$F_\beta(N_1) = F_\beta(N) + \sum_{n=N}^{N_1-1} e^{2\pi i (\beta n + \frac{1}{2} s(n))}$$

$$= F_\beta(N) + \sum_{n=0}^{2^{\nu_{\sigma+1}-1}} e^{2\pi i (\beta n + \beta N + \frac{1}{2} (s(N)+s(n)))}$$

$$= F_\beta(N) + e^{2\pi i (\beta N + \frac{1}{2} s(N))} \sum_{n=0}^{2^{\nu_{\sigma+1}-1}} e^{2\pi i (\beta n + \frac{1}{2} s(n))}.$$

Thus, by (14) and (15),

$$F_\beta(N_1) = \sum_{g=0}^{\sigma} e^{2\pi i (\beta \sum_{j=0}^{g-1} 2^{\nu_j} + g/2)} \prod_{k=0}^{\nu_g-1} (1 + e^{2\pi i (\beta 2^k + 1/2)})$$

$$+ e^{2\pi i (\beta \sum_{j=0}^{\sigma} 2^{\nu_j} + (\sigma+1)/2)} \prod_{k=0}^{\nu_{\sigma+1}-1} (1 + e^{2\pi i (\beta 2^k + 1/2)})$$

$$= \sum_{g=0}^{\sigma+1} e^{2\pi i (\beta \sum_{j=0}^{g-1} 2^{\nu_j} + g/2)} \prod_{k=0}^{\nu_g-1} (1 + e^{2\pi i (\beta 2^k + 1/2)}).$$
Formulas (11)–(14) give an explicit expression for $S_m(N)$ as a linear combination of products of the form

$$\prod_{k=0}^{\nu_g-1} (1 + e^{2\pi i (\beta 2^k + 1/2)}), \quad \beta = t/m, \ 0 \leq t \leq m - 1. \quad (16)$$

**Remark 1.** One may derive (14) from a very complicated general formula of Gelfond [7]. However, we preferred to give an independent proof.

In particular, if $N = 2^\nu$, then from (11)–(13) and (15) for

$$\beta = t/m, \quad t = 0, 1, \ldots, m - 1, \quad (17)$$

we obtain the known formula (cf. [4]):

$$S_{m,a}(2^\nu) = \frac{1}{m} \sum_{t=1}^{m-1} e^{-2\pi i t a/m} \prod_{k=0}^{\nu-1} (1 - e^{2\pi i t 2^k/m}). \quad (18)$$

### 3. Proof of Theorem 1.

Consider the equation of order $r$

$$z^r + c_1 z^{r-1} + \cdots + c_r = 0 \quad (19)$$

with the roots

$$z_j = \prod_{t \in C_j} (1 - e^{2\pi it/m}), \quad j = 1, \ldots, r. \quad (20)$$

Notice that for $t \in C_j$ we have

$$\prod_{k=n+1}^{n+h} (1 - e^{2\pi i t 2^k/m}) = \left( \prod_{t \in C_j} (1 - e^{2\pi it/m}) \right)^{h/h_j} = z_j^{h/h_j}, \quad (21)$$

where $h$ is defined by (7). Therefore, for every $t \in \{1, \ldots, m - 1\}$, according to (19) we have

$$\prod_{k=n+1}^{n+r h} (1 - e^{2\pi i t 2^k/m}) + c_1 \prod_{k=n+1}^{n+(r-1)h} (1 - e^{2\pi i t 2^k/m}) + \cdots + c_{r-1} \prod_{k=n+1}^{n+h} (1 - e^{2\pi i t 2^k/m}) + c_r = 0. \quad (22)$$

After multiplication by $e^{-2\pi i t a/m} \prod_{k=0}^{n} (1 - e^{2\pi i t 2^k/m})$ and summing over $t = 1, \ldots, m - 1$, by (18) we find

$$S_{m,a}(2^{n+r h+1}) + c_1 S_{m,a}(2^{n+(r-1)h+1}) + \cdots + c_{r-1} S_{m,a}(2^{n+h+1}) + c_r S_{m,a}(2^{n+1}) = 0. \quad (23)$$
Moreover, using the general formulas (11)–(14) for a positive integer \( u \), we obtain the equality
\[
S_{m,a}(2^{rh+1}u) + c_1 S_{m,a}(2^{(r-1)h+1}u) + \cdots + c_{r-1} S_{m,a}(2^h u) + c_r S_{m,a}(2u) = 0.
\]
Putting here
\[
S_{m,a}(2^u) = f_{m,a}(u),
\]
we have
\[
f_{m,a}(y + rh + 1) + c_1 f_{m,a}(y + (r - 1)h + 1) + \cdots + c_{r-1} f_{m,a}(y + h + 1) + c_r f_{m,a}(y + 1) = 0,
\]
where
\[
y = \log_2 u.
\]
The characteristic equation of (26) is
\[
v^{rh} + c_1 v^{(r-1)h} + \cdots + c_{r-1} v^h + c_r = 0.
\]
A comparison of (28) and (20)–(21) shows that the roots of (28) are
\[
v_{j,w} = e^{2\pi i w/h} \prod_{t \in C_j} (1 - e^{2\pi it/m})^{1/h}, \quad w = 0, \ldots, h - 1, \ j = 1, \ldots, r.
\]
Thus,
\[
v = \max |v_{j,l}| = 2 \max_{1 \leq l \leq m-1} \left( \prod_{k=0}^{h-1} \sin \frac{\pi l 2^k}{m} \right)^{1/h}.
\]
Generally speaking, some numbers in (20) could be equal. In view of (29), the \( v_{j,w} \)'s have the same multiplicities. If \( \eta \) is the maximal multiplicity, then according to (25) and (27),
\[
S_{m,a}(u) = f_{m,a}(\log_2 u) = O((\log_2 u)^{\eta-1} u^{\ln v/\ln 2}).
\]
Nevertheless, at least
\[
S_{m,a}(u) = \Omega(u^{\ln v/\ln 2}).
\]
Indeed, let, say, \( v = |v_{1,w}| \) and suppose that in the solution of (26) with some natural initial conditions, all coefficients of \( y^j v_{1,w}^w, \ j_1 \leq \eta - 1, \ w = 0, \ldots, h - 1 \), are 0. Then \( f_{m,a}(y) \) satisfies a difference equation with the characteristic equation not having roots \( v_{1,w} \), and the corresponding relation for \( S_{m,a}(2^u) \) (see (23)) has the characteristic equation (19) without the root \( z_1 \). This is impossible since by (18) and (21) we have
\[
S_{m,a}(2^{h+1}) = \frac{1}{m} \sum_{j=1}^{r} \sum_{t \in C_j} e^{-2\pi i \frac{t}{m} \frac{1}{a}} \prod_{k=1}^{h} (1 - e^{2\pi i \frac{t}{m} 2^k}) = \frac{1}{m} \sum_{j=1}^{r} \sum_{t \in C_j} e^{-2\pi i \frac{t}{m} a_{j}^{h/j}}.
\]
Therefore, the coefficients considered do not all vanish, and (32) follows. Now from (30)–(32) we obtain (8). ■

**Remark 2.** In (8) it is sufficient to let $l$ run over a system of distinct representatives of the cyclotomic cosets $C_1, \ldots, C_r$ of 2 modulo $m$.

**Remark 3.** It is easy to see that there exists $l \geq 1$ such that $|C_l| = 2$ if and only if $m$ is a multiple of 3. Moreover, for $l$ we can take $m/3$. Now from (8), choosing $l = m/3$, we obtain $\alpha = \lambda = \ln 3 / \ln 4$. This result was obtained in [13] together with estimates of the constants in $S_{m,0}(x) = O(x^\lambda)$ and $S_{m,0}(x) = \Omega(x^\lambda)$ which are based on the formula, proved in [13],

$$S_{m,0}(x) = \frac{3}{m} S_{3,0}(x) + O(x^{\lambda_1})$$

for $\lambda_1 = \lambda_1(m) < \lambda$ and Coquet’s theorem [2].

**Example 1.** Let $m = 17$, $a = 0$. Then $r = 2$, $h = 8$,

$$C_1 = \{1, 2, 4, 8, 16, 15, 13, 9\}, \quad C_2 = \{3, 6, 12, 7, 14, 11, 5, 10\}.$$

The calculation of

$$\alpha_l = 1 + \frac{1}{8 \ln 2} \sum_{k=0}^{17} \left( \ln \left| \sin \frac{\pi l 2^k}{17} \right| \right)$$

for $l = 1$ and $l = 3$ gives

$$\alpha_1 = -0.12228749 \ldots, \quad \alpha_3 = 0.63322035 \ldots.$$

Therefore by Theorem 1, $\alpha = 0.63322035 \ldots$. Moreover, we will prove that

$$\alpha = \frac{\ln(17 + 4\sqrt{17})}{\ln 256}.$$

Indeed, according to (23), for $n = 0$ and $n = 1$ we obtain the system ($S_{17,0} = S_{17}$):

$$\begin{aligned}
S_{17}(1) &= 0, \\
S_{17}(2^1) &= 1, \\
S_{17}(2^2) &= 1, \\
S_{17}(2^3) &= 21, \\
S_{17}(2^4) &= 29, \\
S_{17}(2^5) &= 697, \\
S_{17}(2^6) &= 969.
\end{aligned}$$

By direct calculations we find

$$c_1 S_{17}(2^1) + c_2 S_{17}(2^2) = -S_{17}(2^{17}),$$

(33) $$c_1 S_{17}(2^4) + c_2 S_{17}(2^2) = -S_{17}(2^{18}).$$

Solving (33) we obtain

$$c_1 = -34, \quad c_2 = 17.$$

Thus, by (23) and (24),

$$S_{17}(2^{n+1}) = 34S_{17}(2^{n+9}) - 17S_{17}(2^{n+1}), \quad n \geq 0,$$

(34) $$S_{17}(2^{17}x) = 34S_{17}(2^9x) - 17S_{17}(2x), \quad x \in \mathbb{N}.$$
Putting furthermore
(36) \[ S_{17}(2^x) = f(x), \]
we have
\[ f(y + 17) = 34f(y + 9) - 17(y + 1), \]
where \( y = \log_2 x \). Hence,
\[ f(x) = O((17 + 4\sqrt{17})^{x/8}), \]
that is
(37) \[ S_{17}(x) = O((17 + 4\sqrt{17})^{\frac{1}{8}\log_2 x}) = O(x^\alpha), \]
where
\[ \alpha = \frac{\ln(17 + 4\sqrt{17})}{\ln 256} = 0.633220353\ldots. \]

4. Proofs of Theorems 2–4

Proof of Theorem 2. By the assumptions of Theorem 2 we have \( r = 1 \) and \( h = p - 1 \). Using (8) we have
\[ \alpha = 1 + \frac{1}{(p - 1)\ln 2} \ln \left| \prod_{k=0}^{p-2} \sin \frac{\pi 2^k}{p} \right| \]
\[ = 1 + \frac{1}{(p - 1)\ln 2} \ln \left| \prod_{l=1}^{p - 1} \sin \frac{\pi l}{p} \right|. \]

Furthermore, using the identity
(38) \[ \prod_{l=1}^{p - 1} \sin \frac{l\pi}{p} = \frac{p}{2^{p-1}} \]
([6, p. 378] for example), we find
\[ \alpha = 1 + \frac{1}{(p - 1)\ln 2} (\ln p - (p - 1)\ln 2) = \frac{\ln p}{(p - 1)\ln 2}. \]

Remark 4. In this case, (24) has the simple form
\[ S_{p,a}(2^p u) + c_1 S_{p,a}(2u) = 0. \]

Since in the case of \( a = 0 \) or \( 1 \) we have
\[ S_{p,a}(2) = (-1)^{s(a)}, \]
while in the case of \( a \geq 2, \)
\[ S_{p,a}(2a) = (-1)^{s(a)}, \]
putting
\[ u = \begin{cases} 1, & a = 0, 1, \\ a, & a \geq 2, \end{cases} \]

\[ \frac{\ln p}{(p - 1)\ln 2}. \]
we find
\[ c_1 = (-1)^{s(a)+1} \left\{ \begin{array}{ll} S_{p,a}(2^p), & a = 0, 1, \\ S_{p,a}(a 2^p), & a \geq 2. \end{array} \right. \]
In particular, if \( p = 3 \) and \( a = 2 \) we have \( c_1 = S_{3,2}(16) = -3 \) and
\[ S_{3,2}(8u) = 3 S_{3,2}(2u). \]

**Proof of Theorem 3.** By the assumptions of Theorem 3 we have \( r = 2 \) and \( h = (p - 1)/2 \), so that cyclotomic cosets of 2 modulo \( p \) satisfy
\[ C_1 = -C_2. \]
Therefore, in (8) we obtain the same values for \( l_1 = 1 \) and \( l_2 = p - 1 \). Thus,
\[ \alpha = 1 + \frac{2}{(p - 1) \ln 2} \ln \left( \prod_{l=1}^{p-1} \sin \frac{\pi l}{p} \right)^{1/2} = \frac{\ln p}{(p - 1) \ln 2}. \]

**Proof of Theorem 4.** According to (19)–(20),
\[ c_r = (-1)^r \prod_{j=1}^{r} \prod_{t \in C_j} (1 - e^{2\pi it/m}) = (-1)^r \prod_{t=1}^{m-1} (1 - e^{2\pi it/m}). \]
Thus, using (38) we have
\[ |c_r| = 2^m \prod_{t=1}^{m-1} \sin \frac{\pi t}{m} = m. \]
Consequently, by (29),
\[ \prod_{j=1}^{r} |v_{j,w}| = m^{1/h}, \quad w = 0, 1, \ldots, h - 1. \]
Therefore,
\[ v = \max |v_{j,w}| \geq m^{1/rh} \]
and Theorem 4 follows.

Using Theorems 1–3, in particular, we find
\[ \alpha(3) = 0.7924 \ldots, \quad \alpha(5) = 0.5804 \ldots, \quad \alpha(7) = 0.4678 \ldots, \]
\[ \alpha(11) = 0.3459 \ldots, \quad \alpha(13) = 0.3083 \ldots, \quad \alpha(17) = 0.6332 \ldots, \]
\[ \alpha(19) = 0.2359 \ldots, \quad \alpha(23) = 0.2056 \ldots, \quad \alpha(29) = 0.1734 \ldots, \]
\[ \alpha(31) = 0.6358 \ldots, \quad \alpha(37) = 0.1447 \ldots, \quad \alpha(41) = 0.4339 \ldots, \]
\[ \alpha(43) = 0.6337 \ldots, \quad \alpha(47) = 0.1207 \ldots. \]

**Acknowledgments.** The author is grateful to Professor Daniel Berend (Department of Mathematics and of Computer Science, Ben-Gurion University) for his significant influence on the final version of this paper.
The article is partly supported by a grant of the Kamea Foundation of Israeli Ministry of Absorption.

References


Department of Mathematics
Ben-Gurion University of the Negev
Beer-Sheva 84105, Israel
E-mail: shevelev@bgu.ac.il

Received on 10.6.2008
and in revised form on 1.8.2008 (5734)