ACTA ARITHMETICA
LXVII.4 (1994)

The digits of $1/p$ in connection with class number factors

by

Kurt Girstmair (Innsbruck)

1. Introduction. Let p be a prime and g a natural number, $g \geq 2$. Like any other real number, the quotient $1/p$ has a digit expansion with respect to the basis g. This means that

$$\frac{1}{p} = \sum_{k=1}^{\infty} x_k g^{-k}$$

with $x_k \in \{0, 1, \ldots, g-1\}$. The numbers x_k, $k \in \mathbb{N}$, are uniquely determined and called the *digits* of $1/p$ with respect to g. In what follows we always assume that g is a primitive root modulo p. For this reason the digits $x_1, \ldots, x_{p-1}$ form a period of shortest possible length in the above expansion. Our concern are some remarkable properties of this period, which seem to be unknown even in the simplest cases. For example, if $p \equiv 3 \bmod 4$, $p \geq 7$,

$$(1) \qquad (x_2 + x_4 + \ldots + x_{p-1}) - (x_1 + x_3 + \ldots + x_{p-2}) = (g+1)h_2^-,$$

h_2^- denoting the class number of the quadratic field $\mathbb{Q}(\sqrt{-p})$. This identity slightly resembles the Hirzebruch–Zagier formula (cf. [5]), which expresses h_2^- in terms of the period of the continued fraction of $\sqrt{p}$, provided that $\mathbb{Q}(\sqrt{p})$ has class number one.

The half-periods $x_1, \ldots, x_{(p-1)/2}$ and $x_{(p+1)/2}, \ldots, x_{p-1}$ are connected by the formula

$$(2) \qquad x_k + x_{k+(p-1)/2} = g - 1,$$

$k \geq 1$, which was already known at the beginning of the 19th century (cf. [1], p. 161; a short proof is given below). By (2), the sum of the digits $x_1, \ldots, x_{p-1}$ is $(g-1)(p-1)/2$, so the mean value of these digits is $(g-1)/2$. Now let q be a divisor of the period length $p-1$. It seems natural to group the digits $x_1, \ldots, x_{p-1}$ in classes

$$\mathcal{C}_j = \{x_k \,;\, 1 \leq k \leq p-1,\ k \equiv j \bmod q\}, \qquad j = 1, \ldots, q,$$

and to investigate the mean value of each such class. Of course this is the

same as investigating the sums

$$S_j = \sum_{x \in \mathcal{C}_j} x = \sum \{x_k \,;\, 1 \le k \le p-1,\ k \equiv j \bmod q\}, \qquad j = 1, \ldots, q.$$

The expected value of each sum S_j is

$$S = \frac{(g-1)(p-1)}{2q},$$

since $S_1 + \ldots + S_q = x_1 + \ldots + x_{p-1} = (g-1)(p-1)/2$. We first consider the *trivial* case, i.e., when $S_j = S$ for all $j \in \{1, \ldots, q\}$. Here the mean value of the digits in the class $\mathcal{C}_j$ does not differ from the "general" mean value $(g-1)/2$ of above. The trivial case occurs whenever q divides $(p-1)/2$. Indeed, if $(p-1)/2 \equiv 0 \bmod q$,

$$S_j = \sum \{x_k + x_{k+(p-1)/2} \,;\, 1 \le k \le (p-1)/2,\ k \equiv j \bmod q\}, \qquad j = 1, \ldots, q.$$

Therefore (2) gives $S_j = (g-1)(p-1)/(2q) = S$ for all j.

In the sequel we *exclude* $(p-1)/2 \equiv 0 \bmod q$. In other words, we always require: q even, $p \equiv q+1 \bmod 2q$. On putting

$$T_j = S_j - S, \qquad j = 1, \ldots, q, \tag{3}$$

we bring the sums S_j into a "balanced" form with respect to their expected value S. Throughout this paper let

$$n = q/2.$$

Then it suffices to investigate the first half $T_1, \ldots, T_n$ of the sequence $T_1, \ldots, \ldots, T_q$. In fact,

$$S_j + S_{j+n} = \sum \{x_k \,;\, 1 \le k \le p-1,\ k \equiv j \bmod n\} = 2S, \tag{4}$$

since the modulus $n = q/2$ belongs to the trivial case. This identity and (3) imply

$$T_{j+n} = -T_j, \qquad j = 1, \ldots, n. \tag{5}$$

We call $T = (T_1, \ldots, T_n) \in \mathbb{Q}^n$ the *q-digit eccentricity of $1/p$ with respect to g*.

The subject of this paper is the connection of T with class number factors. Let $\mathbb{Q}^{(m)}$ denote the mth cyclotomic field. The field $\mathbb{Q}^{(p)}$ contains a (unique) subfield K_q with $[K_q : \mathbb{Q}] = q$. Since q is even and $p \equiv q+1 \bmod 2q$, K_q is imaginary. Let h_q^- denote the *minus part of the class number of K_q* (also called the relative class number of K_q). In Theorem 1 the number h_q^- is expressed in terms of T and qth roots of unity. The case $q = 2$ yields

$$T = T_1 = -\frac{g+1}{2} h_2^-,$$

which is equivalent to (1) via (5). In order to obtain simple rational formulas (cf. example below) we use Hasse's representation of h_q^- as a product of canonical factors h_r^*, r running through certain divisors of q (cf. [3]). For each r there is a *norm form* N_r such that $N_r(T_1, \dots, T_n) = c_r h_r^*$, with an explicit factor c_r (Theorem 2).

2. The main result. Let the above notations hold. For an integer $k \geq 0$ let $g_k \in \{1, \dots, p-1\}$ be defined by

$$g_k \equiv g^k \bmod p. \tag{6}$$

A central tool of this paper is the simple formula

$$x_k = \frac{g g_{k-1} - g_k}{p}, \tag{7}$$

which holds for all $k \in \mathbb{N}$ and is proved as follows: Let y_k be the right side of (7). Then (6) shows that y_k is an integer. Since both g_{k-1}, g_k are less than p, one obtains $-1 < y_k < g$. Therefore y_k is in $\{0, 1, \dots, g-1\}$. By (7),

$$\sum_{k=1}^{\infty} y_k g^k = \frac{1}{p}\Big(\sum_{k=1}^{\infty} g_{k-1}/g^{k-1} - \sum_{k=1}^{\infty} g_k/g^k\Big) = \frac{1}{p}.$$

The uniqueness of the digit expansion of $1/p$ yields $y_k = x_k$ for all $k \geq 1$.

From (7) formula (2) follows immediately: Since $g^{(p-1)/2} \equiv -1 \bmod p$, we get $g_{k+(p-1)/2} = p - g_k$, $k \geq 1$. By (7),

$$x_{k+(p-1)/2} = (g(p - g_{k-1}) - (p - g_k))/p = g - 1 - x_k,$$

which is (2).

Now we turn to the connection with class number factors. Let X_q^- be the set of all odd Dirichlet characters $\chi \bmod p$ belonging to K_q. Put

$$E_q^- = \{\eta \in \mathbb{C}\,;\eta^n = -1\}$$

(this is one half of the set of qth roots of unity). X_q^- and E_q^- are in one-to-one correspondence by $\chi \mapsto \chi(g)$. Let

$$B_\chi = \frac{1}{p}\sum_{k=1}^{p-1} k\chi(k)$$

be the first Bernoulli number attached to $\chi \in X_q^-$. Consider the polynomial

$$P = \frac{1}{p}\sum_{k=1}^{p-1} g_k Z^k$$

with rational coefficients. For $\chi \in X_q^-$ and $\zeta = \chi(g)$, we have $B_\chi = P(\zeta)$. On account of (7) it is easy to connect the digits $x_1, \dots, x_{p-1}$ with B_χ.

Indeed, let

$$Q = \sum_{k=1}^{p-1} x_k Z^k.$$

Then

$$Q(\zeta) = (g\zeta - 1)P(\zeta) = (g\chi(g) - 1)B_\chi. \tag{8}$$

Moreover, $\zeta^q = 1$, hence $Q(\zeta) = \sum_{j=1}^{q} S_j \zeta^j$. In view of (4) and $\zeta^{j+n} = -\zeta^j$, we obtain $Q(\zeta) = 2\sum_{j=1}^{n} T_j \zeta^j$, and from (8),

$$\sum_{j=1}^{n} T_j \zeta^j = (g\zeta - 1)B_\chi/2, \tag{9}$$

with $\zeta = \chi(g)$. The connection of (9) with the number h_q^- is clear. Put

$$\gamma_q = \begin{cases} p & \text{if } p = q+1, \\ 1 & \text{otherwise.} \end{cases} \tag{10}$$

The analytic class number formula yields (cf. [4])

$$\prod_{\chi \in X_q^-} \frac{B_\chi}{2} = \frac{(-1)^n h_q^-}{2\gamma_q}. \tag{11}$$

On using

$$\prod_{\zeta \in E_q^-} (g\zeta - 1) = (-1)^n (g^n + 1)$$

we obtain from (9) and (11)

THEOREM 1. *Let q be even, $p \equiv q+1 \bmod 2q$ and $T = (T_1, \dots, T_n)$ the q-digit eccentricity of $1/p$ with respect to g. Then*

$$\prod_{\zeta \in E_q^-} \sum_{j=1}^{n} T_j \zeta^j = \frac{g^n + 1}{2\gamma_q} h_q^-. \tag{12}$$

In particular, $T \neq (0, \dots, 0)$.

Following Hasse [3] we now decompose (12) into canonical factors. For an even number $r \geq 2$ let

$$E_r^* = \{\zeta \in E_r^- \,; \operatorname{ord}(\zeta) = r\}$$

be the set of roots of unity of (exact) order r. The notation $r \| q$ means that r divides q and q/r is odd. Then

$$E_q^- = \dot{\bigcup_{r \| q}} E_r^*.$$

The left side of (12) splits into the factors

$$N_r(T) = \prod_{\zeta \in E_r^*} \sum_{j=1}^{n} T_j \zeta^j, \qquad r \| d, \tag{13}$$

each of them being a $\mathbb{Q}^{(r)}/\mathbb{Q}$-norm. Moreover, we put

$$\delta_r = \begin{cases} 2 & \text{if } r \text{ is a power of 2,} \\ 1 & \text{otherwise.} \end{cases}$$

Let Φ_r denote the rth cyclotomic polynomial, μ the Möbius function, and ϕ the Euler function.

THEOREM 2. *For each r with $r \| q$, the q-digit eccentricity T of $1/p$ satisfies*

$$N_r(T) = \frac{\Phi_r(g) h_r^*}{\gamma_r \delta_r}. \tag{14}$$

All entries on the right side of (14) *are natural numbers*; γ_r *is defined by* (10) *and* h_r^* *by*

$$h_r^* = \prod_{s \| r} (h_s^-)^{\mu(r/s)}.$$

Furthermore, h_r^* *is prime to* $\gamma_r \delta_r$ *and divides* h_q^-.

P r o o f. Hasse ([3], p. 93, Satz 32) proved that

$$\prod \{B_\chi/2 \,;\, \mathrm{ord}(\chi) = r\} = \frac{\widetilde{h}_r}{\gamma_r \delta_r}$$

with an integer $\widetilde{h}_r$ prime to $\gamma_r \delta_r$. In view of (13) we get

$$N_r(T) = \frac{\Phi_r(g) \varepsilon_r \widetilde{h}_r}{\gamma_r \delta_r},$$

where ε_r is the $\mathbb{Q}^{(r)}/\mathbb{Q}$-norm of a number $\zeta \in E_r^*$. Now (12) shows

$$\prod_{r \| q} \varepsilon_r h_r^* = h_q^-, \tag{15}$$

and (multiplicative) Möbius inversion of (15) yields $h_r^* = \varepsilon_r \widetilde{h}_r$. But $\varepsilon_r \widetilde{h}_r$ is in $\mathbb{Z}$ and $h_r^* > 0$ by its definition, so h_r^* is a natural number. It divides h_q^- because of (15). Möbius inversion, applied to $\prod_{r \| q} \Phi_r(g) = g^n + 1$, also shows that $\Phi_r(g)$ is positive. ∎

We note that $N_r(T)$ is a *norm form* in $T_1, \ldots, T_n$; in particular, it is a homogeneous polynomial in $T_1, \ldots, T_n$ of degree $|E_r^*| = \phi(r)$ with coefficients in $\mathbb{Z}$.

It is not hard to compute these polynomials for small values of q, r.

In the case $q = r = 12$, e.g., we obtain

$$\tfrac{3}{4}(T_1^2 - T_2^2 + T_4^2 - T_5^2 + 2T_1T_3 - 2T_3T_5 + 2T_2T_6 + 2T_6T_4)^2$$
$$+ \tfrac{1}{4}(T_1^2 + T_2^2 - 2T_3^2 + T_4^2 + T_5^2 - 2T_6^2 - 2T_1T_3 - 2T_3T_5$$
$$- 4T_5T_1 + 2T_2T_6 - 2T_6T_4 + 4T_4T_2)^2 = (g^4 - g^2 + 1)h_{12}^-/h_4^-.$$

Remark. For $r \| q$ let b_r denote the right side of (14). Formulas (13) and (14), together with the arithmetic-geometric inequality, yield a lower bound for the euclidean norm $\|T\|$ of the digit eccentricity, namely

$$\|T\|^2 \geq \frac{1}{n} \sum_{r \| q} \phi(r) b_r^{2/\phi(r)}. \tag{16}$$

In the cases $q \leq 6$ equality holds in (16). Thus the 6-eccentricity satisfies

$$\|T\|^2 = \frac{(g+1)^2(h_2^-)^3 + 8(g^2 - g + 1)h_6^-}{12h_2^-}$$

for all $p \equiv 7 \bmod 12$, $p > 7$. It can be shown, however, that (14) does not supply an upper bound for $\|T\|$ if $q \geq 8$. But the lower bound (16) seems to be quite good.

Acknowledgments. The author would like to thank L. Skula, K. Dilcher, H. Herdlinger, and M. Schgraffer for their support in preparing this paper.

References

[1] L. E. Dickson, *History of the Theory of Numbers*, Vol. I (reprint), Chelsea, New York, 1952.
[2] K. Girstmair, *On the l-divisibility of the relative class number of certain cyclic number fields*, Acta Arith. 64 (1993), 189–204.
[3] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper* (Nachdruck der ersten Auflage), Springer, Berlin, 1985.
[4] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.
[5] D. Zagier, *Nombres de classes et fractions continues*, Astérisque 24 (1975), 81–97.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT INNSBRUCK
TECHNIKERSTR. 25/7
A-6020 INNSBRUCK, AUSTRIA
E-mail: KURT.GIRSTMAIR@UIBK.AC.AT

Received on 26.10.1993
and in revised form on 24.1.1994 (2507)