Surveys in Mathematics and its Applications

ISSN 1842-6298 (electronic), 1843-7265 (print)
Volume 21 (2026), 157 – 176

POWER RESIDUES, DIGIT EXPANSIONS, AND RELATIVE CLASS NUMBERS

Kurt Girstmair

Abstract. This is a survey of a connection between the distribution of certain power residues modulo p, p a prime, and relative class numbers. The focus lies on quadratic residues and sixth power residues. Dirichlet's class number formula yields a number of results about the distribution of quadratic residues, for instance, the well-known fact that the interval $[0, p/2]$ contains more quadratic residues than nonresidues. This class number formula is also responsible for some properties of the digit expansions of numbers m/p, $p \nmid m$. In a certain sense the results based on Dirichlet's formula can be extended to sixth power residues, where geometry plays an important role.

1 Introduction

Let p be a prime $\equiv 3 \bmod 4$, $p > 3$. Let C denote the set of quadratic residues mod p in $\{1, 2, \ldots, p-1\}$ and N the set of quadratic nonresidues in this set. We have $|C| = |N| = (p-1)/2$. The following result is due to Dirichlet:

$$|C \cap [0, p/2]| - |N \cap [0, p/2]| > 0; \tag{1.1}$$

see [2, p. 373] Hence there are more quadratic residues in the interval $[0, p/2]$ than quadratic nonresidues. More precisely,

$$|C \cap [0, p/2]| - |N \cap [0, p/2]| = \begin{cases} h, & \text{if } p \equiv 7 \bmod 8; \\ 3h, & \text{if } p \equiv 3 \bmod 8, \end{cases} \tag{1.2}$$

where h is the class number of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-p})$. So this class number determines not only the sign of the difference $|C \cap [0, p/2]| - |N \cap [0, p/2]|$ but also its magnitude.

2020 Mathematics Subject Classification: 11A15; 11A63; 11R29.
Keywords: Power residues; digit expansions; relative class numbers; sign vectors.

From (1.2) one obtains the following result, which is shown in [1].

$$|C \cap [0, p/6]| - |N \cap [0, p/6]| = \begin{cases} -h, & \text{if } \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1, \\ h, & \text{otherwise.} \end{cases} \tag{1.3}$$

Here $\left(\frac{-}{p}\right)$ is the Legendre symbol. Accordingly, the class numbers determines the absolute value of this difference, whereas its sign depends on $\{2, 3\} \subseteq N$.

Moreover, the said class number formula implies the following result of [6]. For $p \equiv 3 \bmod 4$, $p > 3$, and $b \geq 2$ let

$$\frac{1}{p} = \sum_{k=1}^{\infty} a_k b^{-k} \tag{1.4}$$

be the *digit expansion* of $1/p$ with respect to the basis b, i.e., the digits a_k take only values in $\{0, 1, \ldots, b-1\}$. If, in addition, b is a primitive root mod p, then $(a_1, a_2, \ldots, a_{p-1})$ is a period of this expansion. Then

$$(a_2 + a_4 + \ldots + a_{p-1}) - (a_1 + a_3 + \ldots + a_{p-2}) = (b+1)h, \tag{1.5}$$

where h is as above. This means that the difference on the left-hand side of (1.5) is always positive. Therefore, the sum of the digits with even indices in the period exceeds the sum of the digits with odd indices. For example, 10 is a primitive root mod 7 and $1/7 = 0.\overline{142857}$, where the bar marks the period. Then $(4+8+7) - (1+2+5) = 11 = (10+1)h$, since $h = 1$ for $p = 7$.

A common viewpoint for the results (1.2), (1.3) and (1.5) was developed in [8]. Furthermore, the respective statements concerning the signs of the left-hand sides of these identities were generalized in a certain sense, in particular, to sixth power residues. However, the generality of this approach has the effect that the most interesting special cases get lost in some sense, in particular, since their description is scattered over several sections of a long paper.

In contrast to this situation, the present article is focused on the most relevant special cases, which become clearer in this way, as we hope. But it is not merely an epitome of the said paper. It also contains new developments like Theorems 3 and 5 on digit expansions, which considerably generalize known results and give rise to new examples. In the case of sixth power residues, the two diagrams are also novel and allow us new insights. Moreover, we illustrate the results by many examples. Finally, we point out what is possible for tenth power residues and hint on some more recent developments in the literature.

2 The b-deviation vector

In what follows let p be a prime and q an even divisor of $p-1$. The cyclic group $G = (\mathbb{Z}/p\mathbb{Z})^\times$ consists of the residue classes $\overline{1}, \overline{2}, \ldots, \overline{p-1}$. It has exactly one subgroup

of index q, namely $H = \{\overline{k}^q; k = 1, \dots, p-1\}$. We require $\overline{\overline{-1}} \notin H$, which means $p \equiv q+1 \bmod 2q$. The factor group G/H consists of the classes $\overline{\overline{k}}$, $k = 1, 2, \dots, p-1$. We identify each class $C \in G/H$ with $\{k; 1 \le k \le p-1, \overline{\overline{k}} = C\}$. If $q = 2$, then G/H consists of the classes H and $\{1, 2, \dots, p-1\} \setminus H$, which comprise the quadratic residues and nonresidues mod p, respectively. As a rule, we describe the classes $C \in G/H$ as follows. Let g be a primitive root p. Then

$$G/H = \{\overline{\overline{g}}^0, \overline{\overline{g}}^1, \dots, \overline{\overline{g}}^{q-1}\}.$$

For an integer k let $(k)_p$ be the representative of k mod p, i.e., the number $j \in \{0, 1, \dots, p-1\}$ fulfilling $j \equiv k$ mod p. Let $b \ge 2$ be a natural number, $p \nmid b$. We define the function

$$\theta_b : \mathbb{Z} \to \mathbb{Z} : k \mapsto \theta_b(k) = \frac{b(k)_p - (bk)_p}{p}. \tag{2.1}$$

It is easy to illustrate the effect of this function. Indeed, for $k \in \{1, \dots, p-1\}$,

$$\theta_3(k) = \begin{cases} 0 & \text{if } k < p/3; \\ 1 & \text{if } p/3 \le k < 2p/3; \\ 2 & \text{if } 2p/3 \le k. \end{cases}$$

We also need the property

$$\theta_b(k) + \theta_b(p-k) = b - 1 \text{ for } k \in \{1, 2, \dots, p-1\}, \tag{2.2}$$

which is easy to check. For a class $C \in G/H$ we define

$$S_C^{(b)} = \sum_{k \in C} \theta_b(k).$$

In the case $b = 2$, say, we count, thereby, the elements of C that are $> p/2$. Because of (2.2) we have

$$\sum_{C \in G/H} S_C^{(b)} = \sum_{1 \le k \le p-1} \theta_b(k) = \sum_{1 \le k < p/2} \theta_b(k) + \sum_{1 \le k < p/2} \theta_b(p-k) = \frac{(b-1)(p-1)}{2}.$$

Accordingly, each sum $S_C^{(b)}$ has the *expected value*

$$E^{(b)} = \frac{(b-1)(p-1)}{2q}. \tag{2.3}$$

The deviation of $S_C^{(b)}$, $C \in G/H$, from the expected value is measured by

$$T_C^{(b)} = S_C^{(b)} - E^{(b)}, \ \ C \in G/H.$$

It turns out, in this context, that we can dispense with half of the classes C. We write

$$-C = \overline{\overline{-1}}C = \{p - k; k \in C\}$$

and obtain

$$T^{(b)}_{-C} = -T^{(b)}_C, \ \ C \in G/H \tag{2.4}$$

from (2.2). Hence it suffices to select one class from each pair $C, -C$. The following choice is self-evident. As above, let g be a primitive root mod p. Then the classes $\overline{\overline{g}}^k$ with even exponents $k \in \{0, \dots, q-1\}$ turn into those with odd exponents by multiplication with $\overline{\overline{-1}}$. In the sequel put $n = q/2$ and

$$C_j = \overline{\overline{g}}^{2(j-1)}, j = 1, \dots, n.$$

All these classes C_j consist of quadratic residues mod p. Observe that the order of the classes in C_j, $j \geq 2$, depends on the choice of the primitive root g if $n \geq 3$.

Moreover, we write $S^{(b)}_j = S^{(b)}_{C_j}$ and $T^{(b)}_j = T^{(b)}_{C_j}$, $j = 1, \dots, n$. We call

$$T^{(b)} = (T^{(b)}_1, \dots, T^{(b)}_n)$$

the *b-deviation vector* of G/H.

By the interrelation between the b-deviation vector and relative class numbers, we will, in the main, obtain insight into two quantities connected with $T^{(b)}$: on the one hand, the Euclidean norm $\|T^{(b)}\|$, i.e., the *dispersion* of the numbers $S^{(b)}_j$, $j = 1, \dots, n$; on the other hand, the *signs* of the numbers $T^{(b)}_j$, which show whether the sums $S^{(b)}_j$ are greater or smaller than their expected value $E^{(b)}$. The assertions (1.1), (1.2), (1.3), and (1.5) emerge from these quantities in the case $q = 2$.

3 Characters and Bernoulli numbers

We consider the $\mathbb{C}$-vector space $\mathbb{C}^n$, $n = q/2$, with the standard scalar product defined by

$$\langle z, u \rangle = \sum_{j=1}^{n} z_j \overline{u_j},$$

where the bar denotes complex conjugation. A confusion with the bar used for residue classes is hardly possible.

We also consider the character group X of G/H, whose elements χ are understood as Dirichlet characters mod p. In particular, $\chi(k) = 1$ if $k \in H$. Since $\overline{\overline{-1}} \neq \overline{\overline{1}} \in G/H$, one half of X consists of odd characters, which are characterized by $\chi(-1) = -1$. Let X^- denote the set of odd characters in X. We interpret each

$\chi \in X^-$ as a vector in $\mathbb{C}^n$ on identifying χ with $(\chi(C_1)), \ldots, \chi(C_n))$. The well-known orthogonality relations between characters show, for $\chi, \chi' \in X^-$,

$$\langle \chi, \chi' \rangle = \begin{cases} 0 & \text{if } \chi \neq \chi', \\ n & \text{otherwise.} \end{cases}$$

Hence the characters $\chi \in X^-$ form an orthogonal basis of $\mathbb{C}^n$. Therefore,

$$z = \frac{1}{n} \sum_{\chi \in X^-} \langle z, \chi \rangle \chi \quad \text{and} \quad \|z\|^2 = \frac{1}{n} \sum_{\chi \in X^-} |\langle z, \chi \rangle|^2 \tag{3.1}$$

for all $z \in \mathbb{C}^n$.

For a character $\chi \in X^-$,

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

is the corresponding Bernoulli-number. Our first main result is as follows.

Theorem 1. *For the b-deviation vector $T^{(b)}$ and each character $\chi \in X^-$,*

$$\langle T^{(b)}, \chi \rangle = (b - \chi(b)) B_{\overline{\chi}}/2,$$

where $\overline{\chi}$ denotes the complex conjugate character of χ.

Proof. By (2.4), we have, since χ is odd,

$$2\langle T^{(b)}, \chi \rangle = \sum_{C \in G/H} T_C^{(b)} \overline{\chi(C)}.$$

This equals

$$\sum_{C \in G/H} S_C^{(b)} \overline{\chi}(C) - E^{(b)} \sum_{C \in G/H} \overline{\chi}(C).$$

Here the second sum vanishes since χ is a nontrivial character of G/H. Therefore, (2.1) gives

$$2\langle T^{(b)}, \chi \rangle = \frac{1}{p} \sum_{k=1}^{p-1} \theta_b(k) \overline{\chi}(k) = \frac{b}{p} \sum_{k=1}^{p-1} k \overline{\chi}(k) - \frac{1}{p} \sum_{k=1}^{p-1} (bk)_p \overline{\chi}(k).$$

Only the last of these sums requires some discussion. Since $p \nmid b$, the numbers $(bk)_p$ run through all $l \in \{1, \ldots, p-1\}$. However, if $l = (bk)_p$, then $\overline{k} = \overline{l} \cdot \overline{b}^{\,-1} \in G$. The assertion follows from $\overline{\chi}(\overline{b}^{\,-1}) = \chi(b)$. □

4 Quadratic residues

It is easy to prove the identities (1.2) and (1.3) with the above tools. We will also prove another result of this kind; see (4.7).

Let $q = 2$, in particular, $p \equiv 3 \bmod 4$. Furthermore, let $p > 3$. Here $n = 1$ and $C_1 = C = H$, the set of quadratic residues mod p of Section 1. The only odd character of G/H is the Legendre symbol $\left(\frac{-}{p}\right)$, for which we write χ_2 in the sequel. Moreover, $-B_{\chi_2}$ is the class number of $\mathbb{Q}(\sqrt{-p})$, which is also the relative class number of this imaginary quadratic number field and denoted by h_2^-; see [19, p. 38]. The b-deviation vector $T^{(b)}$ has the form

$$T^{(b)} = T_C^{(b)} = S_C^{(b)} - (b-1)(p-1)/4.$$

Because of (3.1) and Theorem 1, we have

$$T_C^{(b)} = -(b - \chi_2(b))h_2^-/2 \tag{4.1}$$

Accordingly,

$$S_C^{(b)} = (b-1)(p-1)/4 - (b - \chi_2(b))h_2^-/2. \tag{4.2}$$

In Section 2 we observed that, for $b = 2$,

$$S_C^{(2)} = |C \cap [p/2, p]|. \tag{4.3}$$

Since $|C| = (p-1)/2$, we obtain

$$|C \cap [0, p/2]| = (p-1)/2 - S_C^{(2)}. \tag{4.4}$$

Let $N = -C$ be as in Section 1. Then

$$|N \cap [0, p/2]| = (p-1)/2 - |C \cap [0, p/2]\}| = S_C^{(2)}.$$

Together with (4.2), this yields (1.2), provided that we observe that $\left(\frac{2}{p}\right) = 1$ only if $p \equiv 7 \bmod 8$.

Remark 2. *From (4.2) we see that the deviation of $S_C^{(b)}$ from the expected value $E^{(b)}$ is small relative to $E^{(b)} = (b-1)(p-1)/4$ if b is fixed and p tends to infinity. Indeed, the inequality of Pólya-Vinogradov implies $h_2^- \ll \sqrt{p}\log p$; see [19, pp. 45, 214].*

Next we introduce the function $f = 1 + \theta_2 + \theta_3 - \theta_6$. It is easy to check that for $k \in \{1, \dots, p-1\}$

$$f(k) = \begin{cases} 1 & \text{if } k < p/6; \\ -1 & \text{if } k > 5p/6; \\ 0 & \text{otherwise.} \end{cases}$$

We form

$$S_C^f = \sum_{k\in C} f(k) = |C \cap [0, p/6]| - |C \cap [5p/6, p]|.$$

The expected value of this sum is

$$E^f = |C| + E^{(2)} + E^{(3)} - E^{(6)} = 0.$$

Hence we obtain

$$S_C^f = S_C^f - E^f = T_C^{(2)} + T_C^{(3)} - T_C^{(6)}. \tag{4.5}$$

For $\chi_2 = \left(\frac{=}{p}\right)$ we have, because of (4.1),

$$S_C^f = \langle S_C^f, \chi_2\rangle = \langle T_C^{(2)} + T_C^{(3)} - T_C^{(6)}, \chi_2\rangle = -\widetilde{c}_{\chi_2} h_2^-/2, \tag{4.6}$$

with $\widetilde{c}_{\chi_2} = -1 - \chi_2(2) - \chi_2(3) + \chi_2(6)$. But the number $\widetilde{c}_{\chi_2}$ takes the value 2 if $\chi_2(2) = \chi_2(3) = -1$, and -2, otherwise. Therefore, (4.5) and (4.6) yield the identity (1.3).

One can also find $|C \cap [p/6, p/3]| - |C \cap [2p/3, 5p/6]|$ if one uses the function $-\theta_2 - 2\theta_3 + \theta_6$ instead of f, and $|C \cap [p/3, p/2]| - |C \cap [p/2, 2p/3]|$ by means of the function $-2\theta_2 + \theta_3$; see [1].

Finally, let $b = p+1$. The definition (2.1) shows $\theta_{p+1}(k) = k$ for $k \in \{1, 2, \ldots, p-1\}$ and

$$S_C^{(p+1)} = \sum_{k\in C} k.$$

Hence we call $S_C^{(p+1)}$ the *class sum* of C. By (4.2), and since $\chi_2(p+1) = 1$,

$$\sum_{k\in C} k = p(p-1)/4 - ph_2^-/2.$$

This shows that the class sum of C is smaller than its expected value $p(p-1)/4$. As we remarked in the context of (1.2), the elements of C are accumulated in the lower half of the interval $[0, p]$. This convenes with the magnitude of the class sum. With $N = -C$ as in Section 1 we have

$$S_C^{(p+1)} - S_N^{(p+1)} = -ph_2^-. \tag{4.7}$$

As concerns the distribution of quadratic residues by means of Dirichlet's formula (1.3), see also [5]. Further results on the distribution of quadratic residues and higher power residues can be found in [15], [17], and [18].

5 Digit expansions

Let $p \equiv 3 \bmod 4$, $p > 3$ and $H = C_1 = C$ be as in the foregoing section.

We will show that (1.5) is a corollary to a more general theorem. To this end let b be a quadratic nonresidue mod p. Let d be the order of the subgroup $\langle \bar{b} \rangle$ of G (observe that d is even). Moreover, let g be a primitive root mod p and $b_j = (g^{2j})_p$, $j = 0, \ldots, (p-1)/d - 1$. By [7, Satz 1], b_j/p has the digit expansion

$$b_j/p = \sum_{k=1}^{\infty} a_k^{(j)} b^{-k} \quad \text{with} \quad a_k^{(j)} = \theta_b(b_j b^{k-1}), \tag{5.1}$$

and the period $(a_1^{(j)}, a_2^{(j)}, \ldots, a_d^{(j)})$.

Theorem 3. *In the above setting, let*

$$S_j = a_1^{(j)} + a_3^{(j)} + \ldots + a_{d-1}^{(j)}, \quad j = 0, \ldots, (p-1)/d - 1,$$

be the sum of the digits with odd indices in the respective period. Then

$$S_0 + S_1 + \ldots + S_{(p-1)/d-1} = (b-1)(p-1)/4 - (b+1)h_2^-/2. \tag{5.2}$$

Proof. The sum on the left-hand side of (5.2) consists of the summands $\theta_b(b_j b_p^{k-1})$, $j = 0, \ldots, (p-1)/d - 1$, $k = 1, 3, \ldots, d-1$. But the residue classes $\bar{b}^{k-1}$, $k = 1, 3, \ldots, d-1$ run through the group $H \cap \langle \bar{b} \rangle$ and the numbers b_j, $j = 0, \ldots, (p-1)/d - 1$, are a system of representatives of $H/H \cap \langle \bar{b} \rangle$. Accordingly, the numbers $(b_j b^{k-1})_p$ run through all elements of $H = C$. So this sum equals $S_C^{(b)}$. Since $\chi_2(b) = -1$, the assertion follows from (4.2). □

If b is a primitive root mod p, i.e., if $d = p - 1$, only $b_0 = 1$ occurs in Theorem 3. Then $b_0/p = 1/p$ has the period $(a_1, a_2, \ldots, a_{p-1})$. The theorem says

$$a_1 + a_3 + \ldots + a_{p-2} = (b-1)(p-1)/4 - (b+1)h_2^-/2. \tag{5.3}$$

From (2.2) we derive

$$a_k + a_{k+(p-1)/2} = b - 1, \quad k = 1, \ldots, p-1.$$

But $a_{k+(p-1)/2}$ runs through the digits $a_2, a_4, \ldots, a_{p-1}$, if k runs through $1, 3, \ldots, p-2$. Hence we have

$$(a_1 + a_3 + \ldots + a_{p-2}) + (a_2 + a_4 + \ldots + a_{p-1}) = (b-1)(p-1)/2.$$

Together with (5.3), this yields (1.5).

Example 4. *A simple example of Theorem 3 is* $p = 11$ *and* $b = 10$*; so* $d = 2$*. With* 2 *as a primitive root mod* p*, we obtain* $b_0 = 1$*,* $b_1 = 4$*,* $b_2 = 5$*,* $b_3 = 9$*,* $b_4 = 3$*. We have* $1/p = 0.\overline{09}$*,* $4/p = 0.\overline{36}$*,* $5/p = 0.\overline{45}$*,* $9/p = 0.\overline{81}$*, and* $3/p = 0.\overline{27}$*. Hence the sum on the left-hand side of (5.2) is* $0 + 3 + 4 + 8 + 2 = 17$*. On the other hand, the right hand side of (5.2) is* $9 \cdot 10/4 - 11 \cdot h_2^-/2 = 17$ *since* $h_2^- = 1$*.*

Next let b be a quadratic residue mod p. So $\langle \bar{b} \rangle$ is a subgroup of H. Let $|\langle \bar{b} \rangle| = d$. As above, let g be a primitive root mod p and define $b_j = (g^{2j})_p$, $j = 0, \ldots, (p-1)/(2d) - 1$. We have

$$b_j/p = \sum_{k=1}^{\infty} a_k^{(j)} b^{-k} \quad \text{with} \quad a_k^{(j)} = \theta_b(b_j b^{k-1}),$$

and the period $(a_1^{(j)}, a_2^{(j)}, \ldots, a_d^{(j)})$.

Theorem 5. *In the above setting, let*

$$S_j = a_1^{(j)} + a_2^{(j)} + \ldots + a_d^{(j)}$$

be the sum of the digits of the period of b_j/p*,* $j = 0, \ldots, (p-1)/(2d) - 1$*. Then*

$$S_0 + S_1 + \ldots + S_{(p-1)/(2d)-1} = (b-1)(p-1)/4 - (b-1)h_2^-/2. \tag{5.4}$$

The *proof* is quite analogous to the proof of Theorem 3 and, therefore, omitted.

In the case $\langle \bar{b} \rangle = H$, i.e., $d = (p-1)/2$ we have only the digit sum S_0 of the period of $1/p$ on the left-hand side of (5.4). This special case of Theorem 5 was shown in [7]; see also [13].

Example 6. *Let* $p = 79$ *and* $b = 10$*, a quadratic residue mod* p*. We have* $|\langle \overline{10} \rangle| = 13$ *and* $(p-1)/(2d) = 3$*. We take* $g = 3$ *and obtain* $b_0 = 1$*,* $b_1 = 9$*,* $b_2 = 2$*. Now*

$$1/79 = 0.\overline{0126582278481},\ 9/79 = 0.\overline{1139240506329},\ 2/79 = 0.\overline{0253164556962},$$

and the digit sums of the respective periods are 54*,* 45*,* 54*. Their sum is* 153*. On the other hand, the right-hand side of (5.4) is* $9 \cdot 78/4 - 9 \cdot h_2^-/2 = 153$ *since* $h_2^- = 5$*.*

Theorem 7. *Let* $p \equiv 3$ *mod* 4*,* $p > 3$*, and* $b \geq 2$*,* $p \nmid b$*. In addition, let* b *be even and of the order* $(p-1)/2$ *mod* p*. Then we have, for the period* $(a_1, \ldots, a_{(p-1)/2})$ *of* $1/p$ *,*

$$|\{k; a_k \leq b/2 - 1\}| - |\{k; a_k \geq b/2\}| = (2 - \chi_2(2))h_2^-. \tag{5.5}$$

Remark 8. *Whereas* b *appears on the left-hand side of (5.5), it does not appear on the right hand side. Accordingly, the difference on the left-hand side is the same for all* b *in question.*

Proof of Theorem 7. The digits of the period have the form $\theta_b(j)$, $j \in C$. One shows, for each $j \in C$, the equivalence of two assertions, namely,

$$\theta_b(j) \le b/2 - 1 \ \text{ and } \ j \le p/2.$$

For this purpose one uses the estimates

$$\frac{bj-1}{p} \ge \frac{bj-(bj)_p}{p} \ge \frac{bj+1-p}{p}.$$

Then the theorem follows from (4.2), (4.3) and (4.4). □

Remark 9. *The adaption of Theorem 7 to the setting of Theorem 5 is left to the reader.*

The connection between digit expansions and class numbers is also investigated in [4], [10], [12], and [14]. As an example of an analytical result on the digit expansion of m/p, $(m,p)=1$, we mention [3, Cor. 8].

6 Sixth power residues

In the case $q=2$, $n=1$, the b-deviation vector $T^{(b)} = T_C^{(b)}$ satisfies the equation (4.1), whose right-hand side is always negative since $\chi_2(b) \in \{\pm 1\}$. Accordingly, the sum $S_C^{(b)}$ is always smaller than its expected value. In the context of (1.5), the sum of the digits with odd indices is smaller than the sum of the digits with even indices — which is a consequence of the same fact. Therefore, we think that it is desirable to know the signs of the numbers $T_j^{(b)}$, $j=1,\dots,n$, for greater values of $q=2n$. We will see that, under certain conditions, this is possible for $q=6$.

For the time being, we assume $q=2n$, where n is odd. Recall the setting of Sections 2, 3. In particular, $p \equiv q+1 \bmod 2q$, $p > q+1$. For a primitive root g mod p we have $C_j = \overline{g}^{2(j-1)}$, $j=1,\dots,n$. For $b \ge 2$, we consider $S_j^{(b)} = S_{C_j}^{(b)}$ and $T_j^{(b)} = T_{C_j}^{(b)}$, $j=1,\dots,n$. The b-deviation vector is $T^{(b)} = (T_1^{(b)},\dots,T_n^{(b)})$.

The set X^- of odd characters of G/H satisfies $|X^-| = n$. Since n is odd, we have $p \equiv 3 \bmod 4$. Therefore, $\chi_2 = \left(\frac{-}{p}\right) \in X^-$. In the sequel we use the abbreviation

$$c_\chi = b - \chi(b), \ \ \chi \in X^-.$$

Then the assertion of Theorem 1 takes the form

$$\langle T^{(b)}, \chi \rangle = c_\chi B_{\overline{\chi}}/2. \tag{6.1}$$

Because of (4.1) and $\chi_2(C_j)=1$, $j=1,\dots,n$, the vector $T^{(b)}$ lies in the hyperplane

$$P = \{(z_1,\dots,z_n) \in \mathbb{R}^n; z_1+\dots+z_n = -c_{\chi_2} h_2^-/2\} \ (\subseteq \mathbb{R}^n). \tag{6.2}$$

Let the sign of a real number x be defined in the usual way, namely,

$$\operatorname{sign}(x) = \begin{cases} 1 & \text{if } x > 0; \\ 0 & \text{if } x = 0; \\ -1 & \text{if } x < 0. \end{cases}$$

For $z = (z_1, \ldots, z_n) \in \mathbb{R}^n$ we define the *sign vector*

$$\operatorname{sign}(z) = (\operatorname{sign}(z_1), \ldots, \operatorname{sign}(z_n)).$$

The point of P with the smallest (Euclidean) norm has the form

$$z^{(0)} = -c_{\chi_2} h_2^-(1, 1, \ldots, 1)/n.$$

Its sign vector is $(-1, \ldots, -1)$, which we call the *main type*. The following idea is plausible: Namely, the closer $T^{(b)}$ is to $z^{(0)}$, the more $\operatorname{sign}(T^{(b)})$ resembles the main type. We have the following theorem.

Theorem 10. *Let $n > 1$ be odd.*
(a) *The vector $\operatorname{sign}(T^{(b)})$ agrees with the main type in at least one position.*
(b) *If*

$$\|T^{(b)}\|^2 \geq c_{\chi_2}^2 \frac{(h_2^-)^2}{4},$$

then $\operatorname{sign}(T^{(b)})$ differs from the main type.
(c) *Let $k \in \{1, 2, \ldots, n-1\}$. If*

$$\|T^{(b)}\|^2 < c_{\chi_2}^2 \frac{(h_2^-)^2}{4k},$$

then $\operatorname{sign}(T^{(b)})$ agrees with the main type in at least $k+1$ positions.

The theorem is an immediate consequence of the following.

Lemma 11. *Let $n > 1$ and $x_1, \ldots, x_n \in \mathbb{R}$ such that $x_1 + \ldots + x_n = 1$.*
(a) *There is a $j \in \{1, \ldots, n\}$ such that $x_j > 0$.*
(b) *If $x_1^2 + \ldots + x_n^2 \geq 1$, then there is a j with $x_j \leq 0$.*
(c) *Let $k \in \{1, \ldots, n-1\}$. If $x_1^2 + \ldots + x_n^2 < 1/k$, there are at least $k+1$ indices j with $x_j > 0$.*

Proof. Assertion (a) is obvious.
Ad (b): If all $x_j > 0$, then $n > 1$ implies $0 < x_j < 1$ for all j. Thus, $x_1^2 + \ldots + x_n^2 < x_1 + \ldots + x_n = 1$.
Ad (c): We write $x = (x_1, \ldots, x_n)$ and use the standard scalar product and the corresponding Euclidean norm in $\mathbb{R}^n$. Suppose $|\{j; x_j > 0\}| \leq k$. Then we may assume, without loss of generality, $x_{k+1}, \ldots, x_n \leq 0$. Let $(1, 1, \ldots, 1, 0, 0, \ldots, 0) \in \mathbb{R}^n$ be the vector with exactly k entries equal to 1. We have $1 \leq x_1 + \ldots + x_k = \langle x, (1, 1, \ldots, 1, 0, 0, \ldots, 0) \rangle$. Cauchy's inequality shows $1 \leq \|x\| \sqrt{k}$. □

Remark 12. *The Lemma is sharp, inasmuch one does not receive stronger statements from its premises. In the case $n = 3$, which is the most relevant for us, we will get a graphic demonstration that no stronger result is possible.*

Now to the case $q = 6$, i.e., $n = 3$. Here $X^- = \{\chi_2, \chi_6, \overline{\chi_6}\}$, where χ_6 is a character of order 6 and, as above, $\overline{\chi_6} = \chi_6^{-1}$ its complex conjugate character. Because of (3.1) and (6.1),

$$\|T^{(b)}\|^2 = \frac{1}{3}(|\langle T^{(b)}, \chi_2\rangle|^2 + 2|\langle T^{(b)}, \chi_6\rangle|^2) = \frac{1}{3}(c_{\chi_2}^2 \frac{B_{\chi_2}^2}{4} + 2|c_{\chi_6}|^2 \frac{|B_{\chi_6}|^2}{4}). \tag{6.3}$$

The Bernoulli numbers in this formula are connected with relative class numbers. To this end let $\mathbb{Q}^{(p)}$ be the pth cyclotomic field. We identify its Galois group over $\mathbb{Q}$ in the usual way with the cyclic group $G = (\mathbb{Z}/p\mathbb{Z})^\times$. Since $p \equiv 7 \bmod 12$, the field $\mathbb{Q}^{(p)}$ has exactly one subfield K_6 of degree $[K_6 : \mathbb{Q}] = 6$. The field K_6 is the fixed field of the subgroup $H \subseteq G$ of index 6; because $\overline{-1} \notin H$, K_6 is imaginary. Let h_6^- be its relative class number. By [19, Th. 4.17] and [9, Satz 23], we have $h_6^- = |B_{\chi_2} B_{\chi_6}^2|/4$ (observe $p > 7$). Moreover, K_6 contains a unique subfield K_2 of degree $[K_2 : \mathbb{Q}] = 2$, the fixed field of $H' = \{\overline{k}^2; \overline{k} \in G\}$. Because $p \equiv 3 \bmod 4$, $\overline{-1} \notin H'$ and, thus, K_2 is also imaginary. In addition, $K_2 \subseteq K_6$. The relative class number h_2^- of K_2 is given by $|B_{\chi_2}| = h_2^-$. With this notation, (6.3) yields the following.

Theorem 13. *Let $p \equiv 7$ mod 12, $p > 7$. Let $q = 6$ and $b \geq 2$, $p \nmid b$. The b-deviation vector $T^{(b)}$ satisfies*

$$\|T^{(b)}\|^2 = \frac{1}{3}(c_{\chi_2}^2 \frac{(h_2^-)^2}{4} + 2|c_{\chi_6}|^2 \frac{h_6^-}{h_2^-}). \tag{6.4}$$

So the theorem expresses the *variance* of the sums S_j, $j = 1, 2, 3$, by relative class numbers. Combined with Theorem 10 and some computation, formula (6.4) gives the following corollary.

Corollary 14. *In the setting of Theorem 13, the following assertions hold.*
(a) *The sign vector sign$(T^{(b)})$ agrees with the main type $(-1, -1, -1)$ in at least one position.*
(b) *If*

$$|c_{\chi_6}|^2 h_6^- \geq c_{\chi_2}^2 \frac{(h_2^-)^3}{4},$$

then sign$(T^{(b)})$ differs from the main type.
(c1) *If*

$$|c_{\chi_6}|^2 h_6^- < c_{\chi_2}^2 \frac{(h_2^-)^3}{4},$$

then sign$(T^{(b)})$ agrees with the main type in at least two positions.
(c2) *If*

$$|c_{\chi_6}|^2 h_6^- < c_{\chi_2}^2 \frac{(h_2^-)^3}{16},$$

then sign$(T^{(b)})$ *is the main type.*

In the case $q = 6$, the group H consists of the sixth powers in G and equals the class C_1. Moreover, C_2 and C_3 are the cosets of H in the group H' of the squares in G. These cosets have the form $\overline{\overline{g}}^2$ and $\overline{\overline{g}}^4$, respectively; their order depends on the choice of the primitive root g mod p.

Example 15. *We compare the cases* $b = 2$ *and* $b = p + 1$. *In the case* $b = 2$,

$$T_j^{(b)} = |C_j \cap [p/2, p]| - (p-1)/12,$$

in the case $b = p + 1$, *however,*

$$T_j^{(b)} = \sum_{k \in C_j} k - p(p-1)/12,$$

$j = 1, 2, 3$; *see (2.3).*

For the primes $p \equiv 7 \bmod 12$, $7 < p < 500$, the situation is as follows. For 13 of 23 primes in question the criterion (b) of Corollary 14 applies both for $b = 2$ and $b = p + 1$. For the remaining ten primes the respective information is given in Table 1.

p	g	c_6	c_2	h_6^-	h_2^-	$b = 2$	sign	$b = p + 1$	sign
79	3	7	1	5	5	(b)	$-1, -1, 1$	(c2)	main type
103	5	7	1	5	5	(b)	$1, -1, -1$	(c2)	main type
139	2	3	9	9	3	(c1)	main type	(b)	$1, -1, -1$
151	6	7	1	7	7	(c1)	$1, -1, -1$	(c2)	main type
199	3	7	1	27	9	(b)	$1, -1, -1$	(c2)	main type
271	6	7	1	11	11	(c2)	main type	(c2)	main type
367	6	7	1	27	9	(b)	$-1, -1, 1$	(c2)	main type
439	15	1	1	405	15	(c1)	$-1, -1, 1$	(c1)	$-1, -1, 1$
463	3	7	1	49	7	(b)	$1, -1, -1$	(c1)	$1, -1, -1$
487	3	7	1	49	7	(b)	$-1, -1, 1$	(c1)	$-1, -1, 1$

Table 1

In the first line of the table we find $c_6 = |c_{\chi_6}|^2$ and $c_2 = c_{\chi_2}^2$ for the case $b = 2$. In the case $b = p + 1$, we have $|c_{\chi_6}|^2 = p^2 = c_{\chi_2}^2$, hence these constants play no role in the application of the criteria of Corollary 14. In the columns headed "$b = 2$" and "$b = p + 1$" one finds the criterion that may be applied; here "(c1)" says that the

criterion (c2) cannot be applied. In the columns labeled "sign" we omit the brackets of the sign vectors; for instance, $-1,-1,1$ stands for $(-1,-1,1)$. In one case, namely $p=139$, $b=2$, we have the main type although only (c1) is applicable.

Among the 13 primes $p\equiv 7 \bmod 12$, $7<p<500$, not rendered in the table we find sign vectors with two entries 1, such as $p=163$, $g=2$, with $(1,1,-1)$ in the case $b=p+1$.

Observe that Corollary 14 can be applied to

$$|C_j\cap[0,p/6]|-|C_j\cap[5p/6,p]=T_j^{(2)}+T_j^{(3)}-T_j^{(6)},\ \ j=1,2,3,$$

where the constant c_{χ_6} has to be replaced by $\widetilde{c}_{\chi_6}=-1-\chi_6(2)-\chi_6(3)+\chi_6(6)$ and c_{χ_2} by $\widetilde{c}_{\chi_2}=-1-\chi_2(2)-\chi_2(3)+\chi_2(6)$. Since $\widetilde{c}_{\chi_2}=\pm 2$, the main type takes two possible forms, namely $(-1,-1,-1)$ and $(1,1,1)$, in the respective cases; see (4.6).

Corollary 14 can also be applied to *digit expansions*. As an example, we assume that b has the order $(p-1)/2 \bmod p$, a case considered in connection with Theorem 5. Then $1/p$ has the period $(a_1,\dots,a_{(p-1)/2})$. As above, we have three classes $C_j=\overline{b}^{j-1}$, $j=1,2,3$. In this situation, the sums $S_j^{(b)}$ satisfy

$$S_j^{(b)}=\sum_{k=0}^{(p-1)/6-1}a_{j+3k}\ \text{ and }\ T_j^{(b)}=S_j^{(b)}-(b-1)(p-1)/12,\ \ j=1,2,3.$$

In the case $b=10$, we have $|c_{\chi_6}|^2=111$ and $c_{\chi_2}^2=81$. There are 15 primes $p\equiv 7 \bmod 12$, $7<p<1000$, such that 10 has the order $(p-1)/2 \bmod p$. For 10 of these primes the criterion (b) of Corollary 14 applies. Table 2 describes the situation for the remaining five primes. It is organized like Table 1.

p	h_6^-	h_2^-	$b=10$	sign
151	7	7	(c2)	main type
199	27	9	(c2)	main type
439	405	15	(c1)	$-1,1,-1$
631	325	13	(c1)	$-1,1,-1$
991	119	17	(c2)	main type

Table 2

Next we elucidate the geometric meaning of Lemma 1 in the case $n=3$. We write $x=(x_1,x_2,x_3)$ for a vector in $\mathbb{R}^3$. Then

$$P=\{x\in\mathbb{R}^3; x_1+x_2+x_3=1\}$$

is the plane spanned by the standard basis vectors $e_1=(1,0,0)$, $e_2=(0,1,0)$ and $e_3=(0,0,1)$. This plane is rendered in Diagram 1.

Here the points e_j are the corners of the equilateral triangle in the middle, whose sides have the length $\sqrt{2}$. The three straight lines through these points divide P into seven zones. The diagram shows the value of $\operatorname{sign}(x)$ for each zone. Whereas we have $(1,1,1)$ (as the main type) for the points in the interior of the triangle, we have one or two negative signs in the interior of the other zones. The circle through e_1, e_2, e_3 consists of the points $x \in P$ with $\|x\|^2 = 1$. It is the circumcircle of the triangle. On this circle and outside it we have the situation of criterion (b) of the lemma. Indeed, the diagram shows that the main type does not occur there. Criterion (c) of the lemma with $k = 1$ (which corresponds to criterion (c1) of Corollary 14) applies to the points x in the interior of this circle. For these points $\operatorname{sign}(x)$ has at least two entries equal to 1.

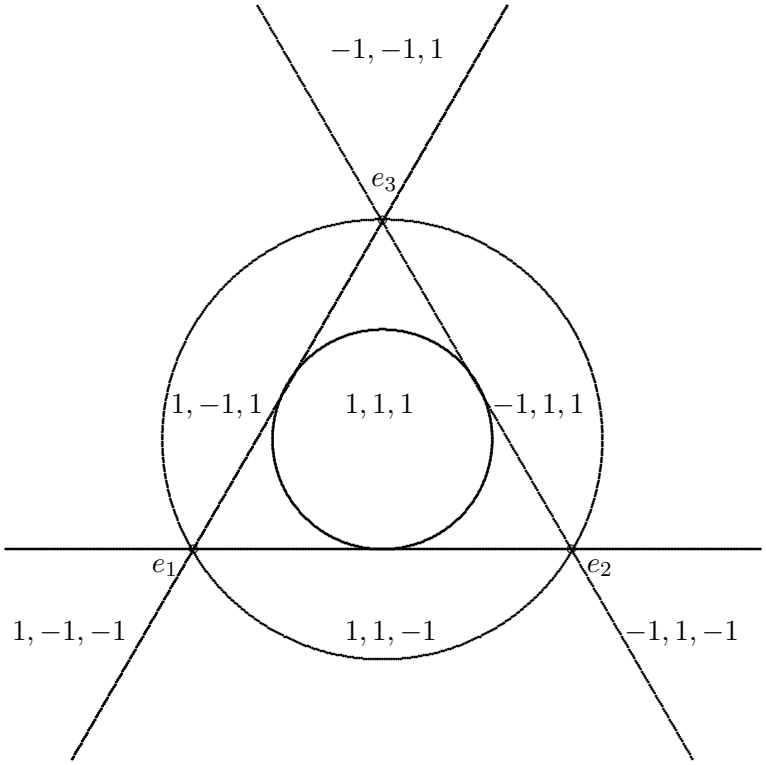

Diagram 1

The circle through the points $(e_1 + e_2)/2$, $(e_1 + e_3)/2$, $(e_2 + e_3)/2$ consists of all points $x \in P$ with $\|x\|^2 = 1/2$ and is the incircle of the triangle. In the interior of the incircle we have $\operatorname{sign}(x) = (1,1,1)$, which corresponds to criterion (c2) of Corollary 14. The diagram also shows that a better criterion for $\operatorname{sign}(x)$ based only on $\|x\|$ does not exist, since all other circles concentric with these two circles are inferior. In

particular, no such criterion for the occurrence of two signs -1 in $\operatorname{sign}(x)$ is possible.

In view of the case $n = 3$, it is not difficult to visualize the case $n = 4$. Here the equilateral triangle is replaced by a regular tetrahedron whose corners are the standard basis vectors $e_1, \ldots, e_4$ of $\mathbb{R}^4$. The planes containing its sides give rise to 15 zones in the hyperplane P, which is a three-dimensional space. Each zone is connected with a certain sign pattern. Instead of the two circles we have three spheres, namely, through the corners of the tetrahedron (the circumsphere), through the midpoints of its edges, and through the midpoints of its sides (the insphere of the tetrahedron). Here criterion (b) of Lemma 11 is the same as saying that the point $(x_1, \ldots, x_4)$ lies on the circumsphere or outside it. Criterion (c) for $k = 1$ says that this point lies inside the circumsphere. In the case $k = 2$ this criterion says that the point lies inside the sphere through the six midpoints of the edges — such a midpoint is $(e_1 + e_2)/2$, for instance. The case $k = 3$ means that the point lies inside the insphere of the tetrahedron.

In higher dimensions the situation is quite analogous, a regular $(n-1)$-simplex playing the role of the tetrahedron. Here $n-1$ different spheres occur, corresponding to the cases of criterion (c) of the lemma.

Suppose that $\operatorname{sign}(T^{(b)})$ is the main type in the case $n = 3$. Then criterion (c1) of Corollary 14 applies and says that $\operatorname{sign}(T)$ differs from the main type in at most one position. The proportion of the area of the incircle to the area of the triangle in Diagram 1 suggests a chance of about 60 % for the applicability of criterion (c2). However, this is only true if the main type is uniformly distributed in the triangle. But it seems that this does not hold, see Diagram 2 and its explanations.

The $(p+1)$-deviation vector $T^{(p+1)}$ describes the difference between the *class sums*

$$S_j^{(p+1)} = \sum_{k \in C_j} k, \quad j = 1, 2, 3,$$

and their expected value $p(p-1)/12$. Diagram 2 shows the distribution of 4754 vectors $T^{(p+1)}$ for $7 < p < 3 \cdot 10^5$, where g is the smallest primitive root mod p. These vectors have been *normalized*, i.e., divided by $-ph_2^-/2$, with the effect that the sum of the three components equals 1; see (6.2). For this reason we can adopt the scheme of Diagram 1 for our visualization. The main type corresponds to the sign vector $(1, 1, 1)$. Only those vectors (1748 in number) whose image points fall outside our display window have been omitted. The main type seems to occur with a frequency of about 25 % of all primes $p \equiv 7 \bmod 12$. Computations suggest a chance of about 70 % for the applicability of the criterion (c2) provided that the sign vector is the main type. This relatively high percentage comes from the higher density of image points in the interior of the incircle of the triangle. But there are no image points near the midpoint of this circle.

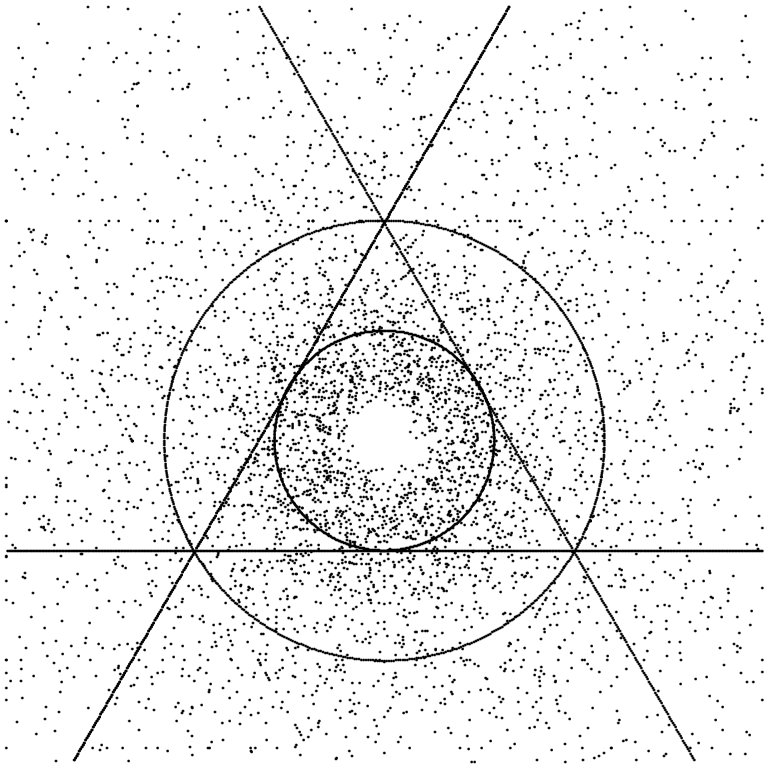

Diagram 2

This empty space can be explained as follows. Due to Theorem 13, the normalized $(p+1)$-deviation vector has the number $(1+8h_6^-/(h_2^-)^3)/3$ as the square of its norm. But the minimum of the numbers $h_6^-/(h_2^-)^3$ for primes in the range in question is about 0.0039. This means that the said vector keeps some distance to the midpoint $(1,1,1)/3$ of the incircle. Of course, this distance could become smaller if larger primes p are included.

The Brauer-Siegel theorem implies

$$\log(h_6^-)/\log((h_2^-)^3) \to 1$$

for $p \to \infty$; see [19, pp. 42–45]. This says that h_6^- and $(h_2^-)^3$ have the same order of magnitude, but only very roughly.

The application of the criteria of Corollary 14 in the case just considered requires only the relative class numbers h_6^- and h_2^- (since $c_{\chi_2}^2 = |c_{\chi_6}^2| = p^2$). There are effective methods for the computation of these numbers; see [11]. Thereby, one could find larger primes (say $p > 10^{12}$) belonging to the main type.

It should be mentioned that for other values of b, in particular, for $b = 2$, one obtains pictures of normalized b-deviation vectors that are fairly different from Diagram

2.

For sixth power residues see also [16].

7 Tenth power residues

In the case $q = 10$, let $p \equiv 11 \bmod 20$ and $p > 11$. We restrict ourselves to $b = p+1$, i.e., $S_j^{(b)} = \sum_{k \in C_j} k$ is the class sum of $C_j = \overline{\overline{g}}^{2(j-1)}$, $j = 1, \ldots, 5$, and $E^{(b)}$ equals $p(p-1)/20$. We have $X^- = \{\chi_2\} \cup \{\chi_{10}, \overline{\chi_{10}}, \chi_{10}^3, \overline{\chi_{10}}^3\}$, where $\chi_2 = \left(\frac{-}{p}\right)$ and χ_{10} is a character of order 10. Since $b = p+1$, $c_\chi = p$ for all $\chi \in X^-$. Therefore, the analogue of (6.3) has the form

$$\|T^{(b)}\|^2 = \frac{p^2}{5}(B_{\chi_2}^2/4 + |B_{\chi_{10}}|^2/2 + |B_{\chi_{10}^3}|^2/2). \tag{7.1}$$

The main difference between this case and the case $q = 6$ consists in the fact that $|B_{\chi_{10}}|^2$ and $|B_{\chi_{10}^3}|^2$ cannot be expressed by rational class number factors. Indeed, we only have

$$|B_{\chi_{10}}|^2 |B_{\chi_{10}^3}|^2 = 16\, h_{10}^-/h_2^-,$$

where h_{10}^- and h_2^- are the relative class numbers of the subfields of $\mathbb{Q}^{(p)}$ of the degrees 10 and 2, respectively. The arithmetic-geometric inequality, applied to the last two summands on the right-hand side of (7.1), gives

$$\|T^{(b)}\|^2 \geq \frac{p^2}{5}((h_2^-)^2/4 + 4\sqrt{h_{10}^-/h_2^-}). \tag{7.2}$$

Therefore, criterion (b) of Theorem 10 can be applied in the strict sense, however, no other one. Indeed, the right-hand side of (7.2) is $\geq p^2(h_2^-)^2/4$, if, and only if,

$$h_{10}^- \geq (h_2^-)^5/16.$$

In this case $\operatorname{sign}(T^{(b)})$ differs from the main type.

Nevertheless, computations for $11 < p < 2 \cdot 10^6$ show that $\|T^{(b)}\|^2$ is quite close to the right-hand side of (7.2) in most cases. Therefore, we may try to take (7.2) as an equality. This allows us to apply the criteria (c) of Theorem 10 in a *probabilistic* sense. In the case $k = 4$ we obtain the following. If

$$h_{10}^- < (h_2^-)^5/4096,$$

then $\operatorname{sign}(T^{(b)})$ is (probably) the main type. This procedure gives only two false predictions for $p < 10^5$; see [8, Sect. 3.3], where further details can be found.

References

[1] B. C. Berndt, *Classical theorems on quadratic residues*, Enseign. Math. (2) **22** (1976), 261–304. MR0441835. Zbl 0337.10031.

[2] S. I. Borewicz, I. R. Šafarevič, *Zahlentheorie*, Basel, 1966. MR195802. Zbl 0134.27303.

[3] J. Bourgain, S. V. Konyagin, I. E. Shparlinski, *Product sets of rationals, multiplicative translates of soubgroups in residue rings, and fixed points of the discrete logarithm*, Int. Math. Res. Not. 2008, Art. ID rnn 090, 29 pp. MR2439546. Zbl 1232.11003. DOI: https://doi.org/10.1093/imrn/rnn090.

[4] K. Chakraborty, K. Krishnamoorthy, *On some symmetries of the base n expansion of $1/m$: the class number connection*, Pacific J. Math. **319** (2022), 39–53. MR4475673. Zbl 1503.11138. DOI: https://doi.org/10.2140/pjm.2022.319.39

[5] J. Chattopadhyay, B. Roy, S. Sarkan, R. Thangadurai, *Distribution of residues modulo p using Dirichlet's class number formula*, in: Class Groups of Number Fields and Related Topics, Singapore, 2020, 97–107. MR4292547. Zbl 1444.11008. DOI: https://doi.org/10.1007/978-981-15-1514-9_9

[6] K. Girstmair, *The digits of $1/p$ in connection with class number factors*, Acta Arith. **67** (1994) 381–386. MR1301825. ZBl 0827.11004. DOI: https//doi.org/10.4064/aa-67-4-381-386.

[7] K. Girstmair, *Periodische Dezimalbrüche – was nicht jeder darüber weiß*, Jahrbuch Überblicke Mathematik 1995, Braunschweig, 1995, 163–179. MR1342348. Zbl 0832.11004.

[8] K. Girstmair, *Class number factors and distribution of residues*, Abh. Math. Sem. Univ. Hamburg **67** (1997), 65–104. MR1481527. Zbl 0889.11032. DOI: https://doi.org/10.1007/BF02940820.

[9] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin, 1952. MR842666. Zbl 0046.26003.

[10] M. Hirabayashi, *Generalizations of Girstmair's formula*, Abh. Math. Sem. Univ. Hamburg **75** (2005), 83–95. MR2187580. Zbl 1185.11066. DOI: https://doi.org/10.1007/BF02942037.

[11] S. Louboutin, *Computation of class numbers of quadratic number fields*, Math. Comp. **71** (2002), 1735–1743. MR1933052. Zbl 1030.11079. DOI: https://doi.org/10.1090/S0025-5718-01-01367-9.

[12] Y. Mizuno, *A certain character twisted average value of the digits of rational numbers and the class numbers of imaginary quadratic fields*, Acta Arith. **208** (2023), 215–233. MR4631980. Zbl 1535.11013. DOI: https://doi.org/10.4064/aa220114-28-5.

[13] M. R. Murty, R. Thangadurai, *The class number of* $\mathbb{Q}(\sqrt{-p})$ *and digits of* $1/p$, Proc. Amer. Math. Soc. **139** (2011), 1277–1289. MR2748421. Zbl 1228.11012. DOI: https://doi.org/10.1090/S0002-9939-2010-10560-9.

[14] S. Pujahari, N. Saikia, *l-adic digits and class numbers of imaginary quadratic fields*, Internat. J. Math. **35** (2024), Paper No. 2450041, 16 pp. MR4801989. Zbl 1558.11008. DOI: https://doi.org/10.1142/S0129167X24500411.

[15] I. E. Shparlinski, *On small gaps between the elements of multiplicative subgroups in finite fields*, Des. Codes Cryptogr. **80** (2016), 63–71. MR3507574. Zbl 1367.11040. DOI: https://doi.org/10.1007/s10623-015-0063-9.

[16] J. Su, J. Zhang, *On the sixth residues and some new properties of their distribution*, J. Math. 2021, Art. ID 6652045, 8 pp. MR4238822. Zbl 1477.11009. DOI: https://doi.org/10.1155/2021/6652045.

[17] X. Wang, H. Fang, *The distribution properties of consecutive quadratic residue sequences*, J. Math. 2023, Art. ID 5253261, 15 pp. MR4653843. DOI: https://doi.org/10.1155/2021/6652045.

[18] J. Wang, Zh. Xu, *Double and triple character sums and gaps between the elements of subgroups of finite fields*, Int. J. Number Th. **20** (2024), 1725–1737. MR4776663. Zbl 1548.11151. DOI: https://doi.org/10.1142/S1793042124500842.

[19] L. C. Washington, *Introduction to Cyclotomic fields*, New York, 1982. MR718674. Zbl 0484.12001.

Kurt Girstmair, ORCID: https://orcid.org/0000-0003-3105-5111
Institut für Mathematik, Universität Innsbruck,
Technikerstr. 13/7, A-6020 Innsbruck, Austria.
e-mail: kurt.girstmair@uibk.ac.at

License

Received: September 29, 2025; Accepted: April 22, 2026
Published electronically: April 23, 2026