ACTA ARITHMETICA
LXIV.2 (1993)

On the l-divisibility of the relative class number of certain cyclic number fields

by

Kurt Girstmair (Innsbruck)

Introduction. Let q be a natural number and p a prime with $2q\,|\,p-1$. Let $\xi_p = e^{2\pi i/p}$ and $\mathbb{Q}_p = \mathbb{Q}(\xi_p)$, i.e., the pth cyclotomic field. Moreover, consider $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ and the multiplicative group $G_p = \mathbb{F}_p^\times$ of this field. There is a canonical group isomorphism

$$G_p \to \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q}) \ : \ k \mapsto \sigma_k\,,$$

σ_k being defined by $\sigma_k(\xi_p) = \xi_p^k$. The field $\mathbb{Q}_p$ contains a uniquely determined subfield $K_{2q} = K_{2q,p}$ of degree $[K_{2q} : \mathbb{Q}] = 2q$, viz., the fixed field of the group $\{\sigma_k\ ;\ \overline{k} \in G_p^{2q}\}$. Here G_p^m means $\{\overline{k}^m\ ;\ \overline{k} \in G_p\}$, $m \in \mathbb{N}$. K_{2q} is *imaginary* if and only if $-1 \notin G_p^{2q}$, i.e., $p \equiv 2q+1 \bmod 4q$. We shall assume this throughout the present paper.

In the sequel let $g = g_p \in G_p$ be chosen such that

$$G_p/G_p^{2q} = \{\overline{1}, \overline{g}, \ldots, \overline{g}^{q-1}, -\overline{1}, -\overline{g}, \ldots, -\overline{g}^{q-1}\}\,. \tag{1}$$

This holds, e.g., if one of the following assumptions is fulfilled:

Assumption A. $\langle\overline{g}\rangle = G_p/G_p^{2q}$.

Assumption B. q is odd and $\langle\overline{g}\rangle = G_p^2/G_p^{2q}$.

The reader may verify (1) in both cases. Now let $t \in G_p/G_p^{2q}$. Thus t is a set of elements of G_p, and we define the *excess* Φ_t of this set by

$$\Phi_t = |\{k\ ;\ 1 \le k < p/2,\ \overline{k} \in t\}| - |\{k\ ;\ p/2 < k \le p-1,\ \overline{k} \in t\}|\,.$$

If $g = g_p$ is as above and $j \in \mathbb{Z}$, we put, in particular,

$$\Phi_j = \Phi_j(g) = \Phi_{\overline{g}^j} = |\{k < p/2\ ;\ \overline{k} \in \overline{g}^j\}| - |\{k > p/2\ ;\ \overline{k} \in \overline{g}^j\}|\,.$$

Then

$$\Phi = \Phi(g) = (\Phi_0, \ldots, \Phi_{q-1}) \in \mathbb{Z}^q$$

is called the *excess vector* belonging to $g = g_p$. Because of (1) and the relation $\Phi_{-t} = -\Phi_t$, the vector Φ describes *all* excesses Φ_t, $t \in G_p/G_p^{2q}$.

In the subsequent Section 1 we express the relative class number $h_{2q}^- = h_{2q}^-(p)$ of the field K_{2q} in terms of the excesses Φ_j, $j = 0, \ldots, q-1$ (formulas (2), (4A), (4B)). Thereby we generalize formulas given in [4].

In Section 2 we investigate the divisibility of h_{2q}^- by an odd prime number l. The assertion $l \mid h_{2q}^-$ can be rephrased in systems of linear congruences mod l for the excesses $\Phi_0, \ldots, \Phi_{q-1}$ (Theorems 1, 2). More precisely, the following holds: Suppose that for all primes $p \equiv 2q + 1 \bmod 4q$ the element $g = g_p$ is chosen such that Assumption A is satisfied. Then there exists, for almost all primes l, a linear manifold $M_l \subseteq \mathbb{F}_l^q$, i.e., a union of finitely many linear subspaces of $\mathbb{F}_l^q$, with the following property: l divides $h_{2q}^-(p)$ if and only if $\overline{\Phi}(g) = (\overline{\Phi}_0, \ldots, \overline{\Phi}_{q-1})$ $(\in \mathbb{F}_l^q)$ is in M_l (Theorem 3). The corresponding result is also valid under Assumption B.

In Section 3 we consider special cases in which the congruences describing M_l can be rendered in a completely explicit shape. Some of these results have been found previously, but from a less general viewpoint (cf. [4]).

Section 4 is based on the following plausible (yet unproved) hypothesis: In the situation of Theorem 3 we suppose that the excess vectors $\overline{\Phi}(g)$ are *equally distributed* in the space $\mathbb{F}_l^q$ when p runs through all primes $\equiv 2q + 1 \bmod 4q$. Then

$$m_l = |M_l|/l^q$$

is the probability that an arbitrary vector $\overline{\Phi}(g)$ is in M_l. By Theorem 3, this is the probability that l divides $h_{2q}^-(p)$. For $1 \le q \le 6$ and $3 \le l < 100$ we compare m_l with the number

$$n_l = \frac{|\{p < 500000\ ;\ p \equiv 2q+1 \bmod 4q, l \mid h_{2q}^-(p)\}|}{|\{p < 500000\ ;\ p \equiv 2q+1 \bmod 4q\}|}\,.$$

The result is given in Table 1, and it shows a high degree of conformity between m_l and n_l in most cases.

At the end of this paper we give a table of the numbers $h_{12}^-(p)$, $p < 10000$. The corresponding tables for $h_{2q}^-(p)$, $1 \le q \le 5$, can be found in [2], [6], and [3].

1. Formulas for h_{2q}^-. Let the above notations hold. By X_{2q} we denote the character group of G_p/G_p^{2q}; as usual, we consider X_{2q} as a subgroup of the character group of G_p, viz.,

$$X_{2q} = \{\chi\ ;\ \mathrm{Ker}\,\chi \supseteq G_p\}\,.$$

Let X_{2q}^- be the set of odd characters in X_{2q}. Then $|X_{2q}^-| = q$. Suppose that g satisfies (1). For a vector $a = (a_0, \ldots, a_{q-1}) \in \mathbb{C}^q$ we define the *Fourier transform*

$$Fa = ((Fa)_\chi\ ;\ \chi \in X_{2q}^-) \in \mathbb{C}^{X_{2q}^-}$$

by its components

$$(Fa)_\chi = \sum_{j=0}^{q-1} \chi(g^j) a_j \, .$$

For the special vector $a = \Phi = \Phi(g)$ the transform $F\Phi$ is independent of the choice of g. Indeed,

$$(F\Phi)_\chi = \sum (\chi(\overline{k}) \; ; \; 1 \le k < p/2)$$

(cf. [4], Lemma 1). As in [4] one obtains

$$\prod ((F\Phi)_\chi \; ; \; \chi \in X_{2q}^-) = \prod ((\chi(\overline{2}) - 2) B_\chi \; ; \; \chi \in X_{2q}^-) \, ,$$

B_χ being the first Bernoulli number attached to χ. In order to evaluate the product on the right side, one needs the order f_q (f_{2q}, resp.) of the element $\overline{\overline{2}}$ in the group G_p/G_p^q (G_p/G_p^{2q}, resp.). For each prime $p \equiv 2q + 1 \bmod 4q$, $p > 2q + 1$, the fundamental formula

$$\prod ((F\Phi)_\chi \; ; \; \chi \in X_{2q}^-) = 2^{q-1} C_{2q} h_{2q}^- \tag{2}$$

holds, with

$$C_{2q} = C_{2q}(p) = (2^{f_q} + (-1)^{f_{2q}/f_q})^{q/f_q} \tag{3}$$

(cf. [4], Theorem 1 and formula (9)).

As to the actual computation of the relative class number, it is useful to write the left side of (2) as a determinant in terms of the excesses Φ_j. First suppose that Assumption A of the Introduction holds. Let the character $\psi \in X_{2q}^-$ be arbitrarily chosen. Then

$$\det(\psi(g^{j-k}) \Phi_{j-k} \; ; \; j, k = 0, \ldots, q-1) = 2^{q-1} C_{2q} h_{2q}^- \, . \tag{4A}$$

In the case of Assumption B one has the simpler formula

$$\det(\Phi_{j-k} \; ; \; j, k = 0, \ldots, q-1) = 2^{q-1} C_{2q} h_{2q}^- \, . \tag{4B}$$

Indeed, the determinants in question are group determinants for the group G_p/G_p^q. Their evaluation is well-known (cf. [5], p. 23) and, together with (2), yields (4A) and (4B). These formulas have been used for the numerical computations displayed in Section 4.

2. Divisibility of h_{2q}^- and congruences for the excesses. In what follows let q be a natural number, p a prime, $p \equiv 2q+1 \bmod 4q$, $p > 2q+1$. In addition, let l be an odd prime not dividing q. The values of each character $\chi \in X_{2q}^-$ are in the field $\mathbb{Q}_{2q} = \mathbb{Q}(\xi_{2q})$, $\xi_{2q} = e^{\pi i/q}$. We consider the automorphism $\tau_l \in \mathrm{Gal}(\mathbb{Q}_{2q}/\mathbb{Q})$ defined by

$$\tau_l(\xi_{2q}) = \xi_{2q}^l \, .$$

For each $\chi \in X_{2q}^-$ the map $\tau_l \circ \chi : G_p \to \mathbb{C}^\times : \overline{k} \mapsto \tau_l(\chi(\overline{k}))$ is in X_{2q}^- again. Hence the group $\langle\tau_l\rangle$ acts on the set X_{2q}^-. The orbits under this action will play an important role.

The group $\langle\tau_l\rangle$ is the *decomposition group* of l in $\mathbb{Q}_{2q}$, and $L = L_l$ ($\subseteq \mathbb{Q}_{2q}$) denotes its fixed field. Let $\mathfrak{L}$ be a prime ideal of $\mathbb{Q}_{2q}$ with $\mathfrak{L} \,|\, l$ and put $\mathfrak{l} = \mathfrak{L} \cap L$. Since l splits completely in L, $\mathfrak{l}$ is a prime ideal of degree 1 over $\mathbb{Q}$. We denote by $\mathcal{O}_{2q}$ ($\mathcal{O}_L$, resp.) the ring of integers of $\mathbb{Q}_{2q}$ (of L, resp.). The canonical maps

$$\begin{array}{ll} \mathbb{F}_l \to \mathcal{O}_L/\mathfrak{l}\,, & \mathcal{O}_L/\mathfrak{l} \to \mathcal{O}_{2q}/\mathfrak{L} \\ \overline{k} \mapsto \overline{k} & \overline{x} \mapsto \overline{x} \end{array}$$

allow us to identify $\mathcal{O}_L/\mathfrak{l}$ with $\mathbb{F}_l$ and to consider $\mathbb{F}_l$ as a subset of $\mathcal{O}_{2q}/\mathfrak{L}$.

THEOREM 1. *In the above situation*, *the following assertions are equivalent*:

(i) $C_{2q}h_{2q}^- \equiv 0 \bmod l$.

(ii) *There is a prime divisor* $\mathfrak{L}$ *of* l *in* $\mathbb{Q}_{2q}$ *and a character* $\chi \in X_{2q}^-$ *such that* $(F\Phi)_\chi \equiv 0 \bmod \mathfrak{L}$.

(iii) *There is a prime divisor* $\mathfrak{L}$ *of* l *in* $\mathbb{Q}_{2q}$ *and an orbit* $Y = \langle\tau_l\rangle \circ \chi_1$ ($\subseteq X_{2q}^-$) *such that*, *for all* $\chi \in Y$, $(F\Phi)_\chi \equiv 0 \bmod \mathfrak{L}$.

Proof. The equivalence of (i) and (ii) is an immediate consequence of formula (2). Because of $\tau_l(\mathfrak{L}) = \mathfrak{L}$, assertion (iii) is equivalent to (ii). ∎

The congruence $(F\Phi)_\chi \equiv 0 \bmod \mathfrak{L}$ can be considered as an equation over the field $\mathcal{O}_{2q}/\mathfrak{L}$, of course. Then (iii) says that $\overline{\Phi} = (\overline{\Phi}_0, \ldots, \overline{\Phi}_{q-1}) \in \mathbb{F}_l^q$ is a solution of the system of linear equations

$$\sum_{j=0}^{q-1} \overline{\chi(g^j)}\,\overline{\Phi}_j = \overline{0}\,, \qquad \chi \in Y\,, \tag{5}$$

with coefficients $\overline{\chi(g^j)}$ in $\mathcal{O}_{2q}/\mathfrak{L}$. In the next theorem we transform (5) into an equivalent system with coefficients in $\mathbb{F}_l$ and determine its rank. For this purpose we need the *trace map*

$$T_l : \mathbb{Q}_{2q} \to L_l : x \mapsto \sum(\tau(x)\ ;\ \tau \in \langle\tau_l\rangle)\,.$$

By φ we denote Euler's function, as usual.

THEOREM 2. *In the situation above suppose that* $l \nmid \varphi(q)$. *Let* $\chi_1 \in X_{2q}^-$ *and* $Y = \langle\tau_l\rangle \circ \chi_1$. *The vector* $\overline{\Phi} = (\overline{\Phi}_0, \ldots, \overline{\Phi}_{q-1}) \in \mathbb{F}_l^q$ *is a solution of* (5) *if and only if it is a solution of the system*

$$\sum_{j=0}^{q-1} \overline{T_l(\chi_1(g)^{j-k})}\,\overline{\Phi}_j = \overline{0}\,, \qquad k = 0, \ldots, |Y| - 1\,, \tag{6}$$

with coefficients in $\mathcal{O}_L/\mathfrak{l} = \mathbb{F}_l$. *The dimension of the space* $V_{Y,g}$ *of solutions of* (6) *is* $q - |Y|$.

Proof. Suppose that $r = |Y|$ and $Y = \{\chi_1, \ldots, \chi_r\}$. By means of the Fourier transform of Section 1 we define the linear map

$$\lambda : (\mathcal{O}_{2q}/\mathfrak{L})^q \to (\mathcal{O}_{2q}/\mathfrak{L})^r : \overline{a} \mapsto (\overline{(Fa)_{\chi_1}}, \ldots, \overline{(Fa)_{\chi_r}}) .$$

The matrix of λ (with respect to the standard bases) is

$$A = (\overline{\chi_i(g^j)} \; ; \; i = 1, \ldots, r \, , \; j = 0, \ldots, q-1) .$$

Because of (1), $G_p/G_p^{2q} = \langle -\overline{\overline{1}}, \overline{g} \rangle$, which implies that the values $\chi_i(g)$, $i = 1, \ldots, r$, are all different. Moreover, l does not divide $2q$, hence the $2q$th roots of unity $\overline{\chi_i(g)}$ are all different, too. This means that the minor $(\overline{\chi_i(g^j)} \; ; \; i = 1, \ldots, r, \; j = 0, \ldots, r-1)$ of A is a regular matrix (of Vandermonde type). Therefore the rank of A is r and λ is surjective. Let c be the natural number

$$c = \mathrm{ord}(\tau_l)/r \, ,$$

with $\mathrm{ord}(\tau_l) = |\langle \tau_l \rangle|$. Since $\varphi(2q) = [\mathbb{Q}_{2q} : \mathbb{Q}] \not\equiv 0 \bmod l$, $\overline{c} \in \mathbb{F}_l$ is different from $\overline{0}$. We define another linear map

$$\mu : (\mathcal{O}_{2q}/\mathfrak{L})^r \to (\mathcal{O}_{2q}/\mathfrak{L})^r$$

by putting

$$\mu(\overline{b}_1, \ldots, \overline{b}_r) = \Big(\overline{c} \sum_{i=1}^{r} \overline{\chi_i(g^{-j})} \, \overline{b}_i \; ; \; j = 0, \ldots, r-1 \Big) .$$

The matrix of μ (with respect to the standard bases) is

$$B = (\overline{c} \, \overline{\chi_i(g^{-j})} \; ; \; j = 0, \ldots, r-1 \, , \; i = 1, \ldots, r) .$$

By the above, B is regular and μ bijective. Thus $\mu \circ \lambda$ is surjective. The kth component of $\mu \circ \lambda(\overline{a})$ is

$$(7) \qquad (\mu \circ \lambda(\overline{a}))_k = \sum_{j=0}^{q-1} \overline{c} \sum_{i=1}^{r} \overline{\chi_i(g^{j-k})} \, \overline{a}_j = \sum_{j=0}^{q-1} \overline{T_l(\chi_1(g^{j-k}))} \, \overline{a}_j \, ,$$

$k = 0, \ldots, r-1$. Now $\overline{\Phi}$ is in the space $V_{Y,g}$ of solutions if and only if $\lambda(\overline{\Phi}) = 0$. Since μ is bijective, this is equivalent to $\mu \circ \lambda(\overline{\Phi}) = 0$. By (7), this means that $\overline{\Phi}$ is a solution of (6).

Finally, observe that the matrix of $\mu \circ \lambda$ is

$$BA = (\overline{T_l(\chi_1(g^{j-k}))} \; ; \; k = 0, \ldots, r-1 \, , \; j = 0, \ldots, q-1) .$$

Its coefficients are in $\mathcal{O}_L/\mathfrak{l} = \mathbb{F}_l$, and the fact that $\mu \circ \lambda$ is surjective shows that its rank is r. Thus $V_{Y,g}$ has dimension $q - r = q - |Y|$. ∎

Remark. Theorem 2 can be rephrased without the assumption $l \nmid \varphi(q)$. But then the trace T_l must be replaced by a trace $T_{l,Y} : L_{l,Y} \to L_l$, where $L_{l,Y}$ is a subfield of $\mathbb{Q}_{2q}$ depending on l and Y.

Let $\mathcal{Y}$ be the set of all orbits Y of the group $\langle \tau_l \rangle$ on X_{2q}^-. We define the linear manifold

$$M_{l,g} = \bigcup (V_{Y,g} \; ; \; Y \in \mathcal{Y})$$

in $\mathbb{F}_l^q$ and show

LEMMA 1. *Let p run through all primes $\equiv 2q+1 \bmod 4q$, $p > 2q+1$, and suppose that the elements $g = g_p$ are chosen such that Assumption* A *of the Introduction holds. Then $M_{l,g}$ is independent of the choice of g and p.*

Proof. Let

$$E_{2q}^- = \{\eta \in \mathbb{C} \; ; \; \eta^q = -1\} \quad (\subseteq \mathbb{Q}_{2q}) .$$

Then $\langle \tau_l \rangle$ acts in the usual way on E_{2q}^-. Let $\mathcal{Z}$ be the set of orbits under this action. Since $G_p/G_p^{2q} = \langle \overline{g} \rangle$, there is a bijection

$$X_{2q}^- \to E_{2q}^- : \chi \mapsto \chi(g) ,$$

which induces the bijection

$$\mathcal{Y} \to \mathcal{Z} : Y = \langle \tau_l \rangle \circ \chi_1 \mapsto Z = \langle \tau_l \rangle (\chi_1(g)) .$$

The system (6) defining the space $V_{Y,g}$ can be written as

$$\sum_{j=0}^{q-1} \overline{T_l(\eta^{j-k})}\, \overline{\Phi}_j = \overline{0} , \qquad k = 0, \ldots, |Z| - 1 , \tag{8}$$

with $\eta \in Z$ arbitrary. By the systems (8) belonging to the orbits Z, the manifold $M_{l,g}$ is defined in an invariant way. ■

LEMMA 2. *Let q be odd and suppose that the elements $g \in G_p$ are always chosen such that Assumption* B *of the Introduction holds. Then $M_{l,g}$ is independent of the choice of g and p.*

Proof. One argues as in the case of Lemma 1, but the role of E_{2q}^- is played by $E_q = \{\eta \in \mathbb{C} \; ; \; \eta^q = 1\}$; and in (8), Z means an orbit of $\langle \tau_l \rangle$ on E_q. ■

If Z is an orbit on E_{2q}^- (on E_q, resp.), put

$$V_Z = \{\overline{\Phi} \in \mathbb{F}_l^q \; ; \; \overline{\Phi} \text{ satisfies (8)}\} \quad \text{and} \quad M_l = \bigcup (V_Z \; ; \; Z \in \mathcal{Z}) .$$

In the situation of Lemmas 1 and 2 we have

$$M_{l,g} = M_l .$$

The spaces V_Z defining the manifold M_l have dimension $q - |Z|$, in accordance with Theorem 2. We have shown:

THEOREM 3. *Let $q \in \mathbb{N}$, l an odd prime, $l \nmid q$, $l \nmid \varphi(q)$. Suppose that for each prime number p, $p \equiv 2q+1 \bmod 4q$, $p > 2q+1$, the element g is chosen such that Assumption* A *of the Introduction holds. Then there exists a linear manifold $M_l \subseteq \mathbb{F}_l^q$ with the following property*: $C_{2q}h_{2q}^-(p) \equiv 0 \bmod l$ *if and only if* $\overline{\Phi}(g) \in M_l$.

This assertion remains valid if "Assumption A*" is replaced by "Assumption* B*".*

3. Special cases of systems of equations. The foregoing section sets the following task: bring the systems (8) describing M_l into a form which is as explicit as possible. We shall do this in some special cases (e.g., for all $q \le 6$) and discuss the choice of these special cases.

(I) *The case* $\tau_l = \mathrm{id}$. Let $\tau_l = \mathrm{id}$, which means $l \equiv 1 \bmod 2q$. Here l splits completely in $\mathbb{Q}_{2q}$ and $T_l = \mathrm{id}$. The set $\{\overline{\eta} \in \mathcal{O}_{2q}/\mathfrak{L} \,;\, \eta \in E_{2q}^-\}$ ($\{\overline{\eta} \in \mathcal{O}_{2q}/\mathfrak{L} \,;\, \eta \in E_q\}$ in the case of Assumption B) can be identified with $\overline{E}_{2q}^- = \{w \in \mathbb{F}_l \,;\, w^q = -1\}$ ($\overline{E}_q = \{w \in \mathbb{F}_l \,;\, w^q = 1\}$, resp.). The systems (8) take the form

$$\sum_{j=0}^{q-1} w^j\, \overline{\Phi}_j = \overline{0}\,. \tag{9}$$

We obtain: The prime l divides $C_{2q}h_{2q}^-$ if and only if equation (9) holds for at least one $w \in \overline{E}_{2q}^-$ ($\overline{E}_q$, resp.). In the case of Assumption B this assertion was just the content of Theorem 4 in [4].

Suppose now that $\tau_l \ne \mathrm{id}$ has a small order. Then $[L : \mathbb{Q}]$ is large and the elements $T_l(\eta^{j-k}) \in \mathcal{O}_L$ occurring in (8) are irrationalities of high degree, in general. It seems to be difficult to identify $\overline{T_l(\eta^{j-k})} \in \mathcal{O}_L/\mathfrak{l}$ with an appropriate element of $\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$ in this general context. For instance, let $l \equiv -1 \bmod 2q$, which implies $\mathrm{ord}(\tau_l) = 2$. If $\mathrm{ord}(\eta) = 2q$, the element $T_l(\eta) = \eta + \eta^{-1}$ generates the maximal real subfield of $\mathbb{Q}_{2q}$. Apparently, the minimal polynomial P of $\eta+\eta^{-1}$ over $\mathbb{Q}$ is not explicitly known (in general); the zeros of $\overline{P}$ in $\mathbb{F}_l$ are even less known. But these zeros occur, arranged in some way, as coefficients of equations (8). This discussion suggests to investigate the case when $\mathrm{ord}(\tau_l)$ is large, rather. Indeed, we shall only consider examples with $\mathrm{ord}(\tau_l) \in \{\varphi(2q), \varphi(2q)/2\}$.

(II) *The case* $\mathrm{ord}(\tau_l) = \varphi(2q)$. Here $\mathrm{Gal}(\mathbb{Q}_{2q}/\mathbb{Q}) = \langle \tau_l \rangle$ is cyclic, which requires that $q \in \{1, 2\}$ or that q is an odd prime power. For $q = 1$, $\Phi_0 = C_{2q}h_{2q}^-$ and (8) reads $\overline{\Phi}_0 = \overline{0}$. If $q = 2$, the set $E_4^- = \{\pm\sqrt{-1}\}$ consists of a unique orbit, and (8) means $\overline{\Phi}_0 = \overline{\Phi}_1 = \overline{0} \in \mathbb{F}_l$. Therefore let $q = n^r$, $n \ge 3$ prime, $r \ge 1$. Furthermore, let Assumption B of the Introduction hold. Put $Z_s = \{\eta \in E_q \,;\, \mathrm{ord}(\eta) = n^s\}$, $s = 0, 1, \ldots, r$. Then $|Z_s| = \varphi(n^s)$, and $\mathcal{Z} = \{Z_0, Z_1, \ldots, Z_r\}$. For an element $\eta \in E_q$,

$$T_l(\eta) = \begin{cases} 0 & \text{if } \eta \notin Z_0 \cup Z_1, \\ -q/n & \text{if } \eta \in Z_1, \\ q - q/n & \text{if } \eta \in Z_0. \end{cases}$$

The system (8) belonging to Z_0 is

$$\overline{\Phi}_0 + \overline{\Phi}_1 + \ldots + \overline{\Phi}_{q-1} = \overline{0}\,.$$

Let $s \geq 1$ and $\eta \in Z_s$ be arbitrary. Then the system (8) attached to Z_s takes the form

$$(10) \quad \overline{n-1}\,\overline{\Phi}_k - \sum(\overline{\Phi}_j \ ; \ \eta^{j-k} \in Z_1\,,\ j \in \{0, \ldots, q-1\}) = \overline{0}\,, \qquad k = 0, \ldots, \varphi(n^s) - 1\,.$$

Let us inspect the particular case $s = r \geq 1$. Here (10) reads

$$\overline{n}\,\overline{\Phi}_k = \sum(\overline{\Phi}_j \ ; \ j \equiv k \bmod q/n\,,\ j \in \{0, \ldots, q-1\})\,, \qquad k = 0, \ldots, \varphi(q) - 1\,;$$

this system can be transformed into

$$\overline{\Phi}_j = \overline{\Phi}_k\,, \qquad k = 0, \ldots, q/n - 1\,,\ j = 0, \ldots, q-1\,,\ j \equiv k \bmod q/n\,.$$

If $r = 1$ we obtain: Let q be an odd prime, $l \nmid q$, $l \nmid q-1$. Then l divides $C_{2q} h_{2q}^-$ if and only if $\overline{\Phi}_0 + \ldots + \overline{\Phi}_{q-1} = \overline{0}$ or $\overline{\Phi}_0 = \overline{\Phi}_1 = \ldots = \overline{\Phi}_{q-1}$. This statement is contained in Theorem 3 of [4].

In the remainder of this section $\operatorname{ord}(\tau_l) = \varphi(2q)/2$. Again, we restrict our interest to the simplest cases: viz., $q \geq 3$ prime, $q = 2^r$, and $q = 6$.

(III) *The case* $\operatorname{ord}(\tau_l) = (q-1)/2$, $q \geq 3$ *prime.* Let Assumption B of the Introduction hold. We put

$$Q = \{k \in \mathbb{Z} \ ; \ q \nmid k\,,\ k \text{ a quadratic residue } \bmod q\}$$

and

$$N = \{k \in \mathbb{Z} \ ; \ q \nmid k\,,\ k \notin Q\}\,.$$

Moreover, let $q^* = q$ if $q \equiv 1 \bmod 4$, and $q^* = -q$ if $q \equiv 3 \bmod 4$. Then $\langle \tau_l \rangle = \{\tau_k \ ; \ k \in Q\}$, and $L = \mathbb{Q}(\sqrt{q^*})$. Take an element $\eta \in E_q \setminus \{1\}$. The set E_q splits into the orbits

$$Z_1 = \{1\}\,, \quad Z_2 = \{\eta^k \ ; \ k \in Q\}\,, \quad Z_3 = \{\eta^k \ ; \ k \in N\}\,.$$

By means of Gauss sums we obtain (cf. [1], p. 195)

$$T_l(\eta^k) = \begin{cases} (q-1)/2 & \text{if } q \mid k, \\ (-1 + \sqrt{q^*})/2 & \text{if } k \in Q, \\ (-1 - \sqrt{q^*})/2 & \text{if } k \in N. \end{cases}$$

Here $\sqrt{q^*}$ depends on the choice of η. The elements $\overline{-1+\sqrt{q^*}}$, $\overline{-1-\sqrt{q^*}}$ of $\mathcal{O}_L/\mathfrak{l}$ can be identified with the zeros w, w' in $\mathbb{F}_l$ of the equation

$$w^2+\overline{2}w+\overline{1-q^*}=\overline{0}\,.$$

The system (8) belonging to Z_1 is $\overline{\Phi}_0+\ldots+\overline{\Phi}_{q-1}=\overline{0}$. For the orbit Z_2 it reads

$$(11)\quad \overline{q-1}\,\overline{\Phi}_k+\sum_{\substack{j=0\\ j-k\in Q}}^{q-1} w\overline{\Phi}_j+\sum_{\substack{j=0\\ j-k\in N}}^{q-1} w'\overline{\Phi}_j=\overline{0}\,,\qquad k=0,\ldots,(q-3)/2\,.$$

The corresponding system for Z_3 arises from (11) by interchanging w and w'.

(IV) *The case* $\mathrm{ord}(\tau_l)=q/2$, $q=2^r$. Let the Assumption A of the Introduction hold. We may suppose that $q\ge 4$. In general, only two groups $\langle\tau_l\rangle$ can occur, viz., $\langle\tau_l\rangle=\langle\tau_5\rangle$, if $l\equiv 5 \bmod 8$, and $\langle\tau_l\rangle=\langle\tau_{-5}\rangle$, if $l\equiv 3 \bmod 8$. In the case $q=4$ there is an additional group, viz., $\langle\tau_7\rangle=\langle\tau_{-1}\rangle$.

We consider the case $\langle\tau_l\rangle=\langle\tau_5\rangle$ first. The set E_{2q}^- consists of two orbits Z_1, Z_2 of length $|Z_1|=|Z_2|=q/2$. Furthermore, $L=\mathbb{Q}(\sqrt{-1})$, and for $\eta\in E_{2q}^-$, $k\in\mathbb{Z}$,

$$T_l(\eta^k)=\begin{cases}(q/2)\eta^k & \text{if } k\equiv 0 \bmod q/2,\\ 0 & \text{otherwise.}\end{cases}$$

We identify $\overline{\eta^{q/2}}=\overline{\sqrt{-1}}\in\mathcal{O}_L/\mathfrak{l}$ with the corresponding root $w\in\mathbb{F}_l$ of the equation $w^2+\overline{1}=\overline{0}$. Then the equations (8) for Z_1 take the form

$$\overline{\Phi}_{k+q/2}=w\overline{\Phi}_k\,,\qquad k=0,\ldots,q/2-1\,.$$

In the equations for Z_2, w must be replaced by $-w$.

If $\langle\tau_l\rangle=\langle\tau_{-5}\rangle$, there are also two orbits Z_1, Z_2 of equal length. Here $L=\mathbb{Q}(\sqrt{-2})$, and for $\eta\in E_{2q}^-$, $k\in\mathbb{Z}$,

$$T_l(\eta^k)=\begin{cases}(q/4)(\eta^k+\eta^{3k}) & \text{if } k\equiv 0 \bmod q/4,\\ 0 & \text{otherwise.}\end{cases}$$

Let $w\in\mathbb{F}_l$ be a root of $w^2+\overline{2}=\overline{0}$. Then the first system (8) reads

$$\begin{aligned}\overline{\Phi}_{k+q/2}&=-\overline{\Phi}_k+w\overline{\Phi}_{k+q/4}\,,\\ \overline{\Phi}_{k+3q/4}&=w\overline{\Phi}_k-\overline{\Phi}_{k+q/4}\,,\end{aligned}\qquad k=0,\ldots,q/4-1\,.$$

In the second system (8) the root w is replaced by $-w$.

Finally, if $q=4$ and $l\equiv 7 \bmod 8$, there are also two orbits of equal length, and $L=\mathbb{Q}(\sqrt{2})$. Let $w\in\mathbb{F}_l$ be a root of $w^2-\overline{2}=\overline{0}$. The first system (8) is

$$(12)\qquad \begin{cases}\overline{\Phi}_2=w\overline{\Phi}_1-\overline{\Phi}_0,\\ \overline{\Phi}_3=\overline{\Phi}_1-w\overline{\Phi}_0.\end{cases}$$

Again, the substitution $w\mapsto -w$ yields the second system.

(V) *The case* $q = 6$. If $\tau_l \neq \mathrm{id}$, the order of τ_l is 2, and the cases $l \equiv 5, 7, 11 \bmod 12$ must be distinguished. All of them are treated similarly, hence we pick out the case $l \equiv 5 \bmod 12$ only. Let $\eta \in E_{12}^-$, $\mathrm{ord}(\eta) = 12$. There are four orbits: $Z_1 = \{\eta^3\}$, $Z_2 = \{\eta^9\}$, $Z_3 = \{\eta, \eta^5\}$, $Z_4 = \{\eta^7, \eta^{11}\}$. Moreover, $\eta^3 = \sqrt{-1}$ and $L = \mathbb{Q}(\sqrt{-1})$. By means of the relation $\eta^4 = \eta^2 - 1$ arising from the 12th cyclotomic polynomial, one obtains

$$T_l(\eta^k) = \begin{cases} \eta^{3k} & \text{if } (k, 12) = 1, \\ 2\eta^k & \text{if } k \equiv \pm 3 \bmod 12, \\ -1 & \text{if } k \equiv \pm 4 \bmod 12, \\ 1 & \text{if } k \equiv \pm 2 \bmod 12. \end{cases}$$

Let w be a root of $w^2 + \overline{1} = \overline{0}$. The system (8) of Z_1 consists of the equation

$$\overline{\Phi}_0 - \overline{\Phi}_2 + \overline{\Phi}_4 = w(\overline{\Phi}_1 - \overline{\Phi}_3 + \overline{\Phi}_5)\,.$$

In the case of Z_3 there are two equations:

$$\overline{2\Phi_0} + \overline{\Phi}_2 - \overline{\Phi}_4 = w(\overline{\Phi}_1 + \overline{2\Phi_3} + \overline{\Phi}_5)\,,$$
$$\overline{\Phi}_0 - \overline{\Phi}_2 - \overline{2\Phi_4} = w(\overline{2\Phi_1} + \overline{\Phi}_3 - \overline{\Phi}_5)\,.$$

The substitution $w \mapsto -w$ yields the systems (8) belonging to Z_2 and Z_4.

Remark. From the systems of equations occurring in cases (III)–(V) one can deduce quadratic congruences mod l which are very convenient in practice. For instance, the equations (12) imply

$$2\Phi_0^2 \equiv (\Phi_1 - \Phi_3)^2 \bmod l\,, \qquad 2\Phi_1^2 \equiv (\Phi_0 + \Phi_2)^2 \bmod l\,.$$

4. Numerical results. Let the above notations hold. We are interested in applying Theorem 3 to $q = 1, 2, \ldots, 6$. The hypothesis $l \nmid \varphi(q)$ of this theorem is meaningless here, since $\varphi(q)$ is a power of 2. In the sequel we must exclude the case that l divides C_{2q}. For this reason we collect up the pairs (q, f_{2q}), $q \leq 6$, for which a prime $l \geq 3$ divides C_{2q} (cf. formula (3)).

$$\begin{aligned} l = 3:&\ \ (q, f_{2q}) \in \{(1,2), (3,2), (3,6), (4,2), (5,2), (5,10)\}\,; \\ l = 5:&\ \ (q, f_{2q}) \in \{(2,4), (4,4), (6,4), (6,12)\}\,; \\ l = 7:&\ \ (q, f_{2q}) = (3,3)\,; \\ l = 11:&\ (q, f_{2q}) = (5,10)\,; \\ l = 13:&\ (q, f_{2q}) = (6,12)\,; \\ l = 31:&\ (q, f_{2q}) = (5,5)\,. \end{aligned}$$

In what follows let Assumption A hold for even q's and Assumption B for odd ones. The set $\mathcal{Z}$ consists of all orbits of $\langle \tau_l \rangle$ on E_{2q}^- (on E_q, resp.) and, as above,

$$M_l = \bigcup (V_Z\ ;\ Z \in \mathcal{Z})\,.$$

Let p denote a prime, $p \equiv 2q+1 \bmod 4q,\ p > 2q+1$. If l divides $C_{2q} = C_{2q}(p)$, the vector $\overline{\Phi} = \overline{\Phi}(g)$ is in M_l, of course. However, if p runs through all primes with $l \nmid C_{2q}$, it could happen that the excess vectors $\overline{\Phi}$ were *equally distributed* in the space $\mathbb{F}_l^q$. Suppose this is true. Then the number

$$m_l = |M_l|/|\mathbb{F}_l^q| = |M_l|/l^q$$

is the probability that l divides the class number $h_{2q}^-(p)$, by Theorem 3.

In order to compute m_l one has to determine the cardinality of M_l. This can be done by means of the well-known sieve formula (cf. [1], p. 123)

$$\text{(13)}\qquad M_l = \sum(|V_Z|\ ;\ Z \in \mathcal{Z}) - \sum(|V_Z \cap V_{Z'}|\ ; \{Z, Z'\} \subseteq \mathcal{Z}) + \sum(|V_Z \cap V_{Z'} \cap V_{Z''}|\ ; \{Z, Z', Z''\} \subseteq \mathcal{Z}) - \ldots$$

According to Theorem 2, $|V_Z| = l^{q-|Z|}$ for all $Z \in \mathcal{Z}$. From the proof of Theorem 2 it is clear that

$$\text{(14)}\qquad \bigcap(V_Z\ ;\ Z \in \mathcal{Z}) = \{0\}\,,$$

i.e., the union of all systems (8) forms a linearly independent system of equations. For these reasons (13) yields

$$\text{(15)}\qquad |M_l| = \sum(l^{q-|Z|}\ ;\ Z \in \mathcal{Z}) - \sum(l^{q-|Z|-|Z'|}\ ; \{Z, Z'\} \subseteq \mathcal{Z}) + \sum(l^{q-|Z|-|Z'|-|Z''|}\ ; \{Z, Z', Z''\} \subseteq \mathcal{Z}) - \ldots$$

Moreover, if all orbits $Z \in \mathcal{Z}$ have the same length $|Z| = z$, (15) takes the simplified form

$$\text{(16)}\qquad |M_l| = l^q(1 - (1 - 1/l^z)^{q/z})\,.$$

If q is an odd prime number, one orbit has length 1 and the remaining ones the same length z. From (16) we deduce for this situation

$$\text{(17)}\qquad |M_l| = l^{q-1}(1 + (l-1)(1 - 1/l^z)^{(q-1)/z})\,.$$

The values of m_l given in Table 1 have been found by means of (15)–(17).

We put

$$P = \{p\ ;\ p \text{ prime}\,,\ p < 500000\,,\ p \equiv 2q+1 \bmod 4q\,,\ p > 2q+1\}$$

and

$$n_l = |\{p \in P\ ;\ l \mid h_{2q}^-(p)\}|/|P|\,.$$

For small primes $l \ge 3,\ l \nmid q,\ l \nmid C_{2q},\ q \le 6$, the number n_l can serve as an approximation of the probability that l divides $h_{2q}^-(p)$. In the few cases where l divides a number $C_{2q} = C_{2q}(p)$ (cf. the above list), we define n_l as

$$n_l = |\{p \in P\ ;\ l \nmid C_{2q}(p)\,,\ l \mid h_{2q}^-(p)\}|/|\{p \in P\ ;\ l \nmid C_{2q}(p)\}|\,.$$

Table 1

l-divisibility of $h_2^-(p)$ for $p < 500000$; total number of p's: 20805

l	n_l	m_l	l	n_l	m_l
3*	0.4063	0.3333	5	0.2313	0.2000
7	0.1634	0.1429	11	0.0992	0.0909
13	0.0817	0.0769	17	0.0636	0.0588
19	0.0545	0.0526	23	0.0453	0.0435
29	0.0343	0.0345	31	0.0344	0.0323
37	0.0263	0.0270	41	0.0256	0.0244
43	0.0246	0.0233	47	0.0219	0.0213
53	0.0192	0.0189	59	0.0175	0.0169
61	0.0170	0.0164	67	0.0146	0.0149
71	0.0158	0.0141	73	0.0129	0.0137
79	0.0146	0.0127	83	0.0125	0.0120
89	0.0115	0.0112	97	0.0106	0.0103

l-divisibility of $h_4^-(p)$ for $p < 500000$; total number of p's: 10396

l	n_l	m_l	l	n_l	m_l
3	0.1293	0.1111	7	0.0189	0.0204
11	0.0082	0.0083	13	0.1513	0.1479
17	0.1238	0.1142	19	0.0036	0.0028
23	0.0009	0.0019	29	0.0676	0.0678
31	0.0013	0.0010	37	0.0526	0.0533
41	0.0518	0.0482	43	0.0007	0.0005
47	0.0001	0.0005	53	0.0374	0.0374
59	0.0003	0.0003	61	0.0368	0.0325
67	0.0002	0.0002	71	0.0002	0.0002
73	0.0261	0.0272	79	0.0003	0.0002
83	0.0003	0.0001	89	0.0209	0.0223
97	0.0187	0.0205			

In Table 1 we display both "probabilities" n_l and m_l for $q \le 6$ and $3 \le l < 100$, $l \nmid q$. The primes l for which $l \mid C_{2q}(p)$ can occur are distinguished by an asterisk.

If q is odd, the number $C_{2q}h_{2q}^-$ is divisible by $C_2h_2^-$. Theorem 3 and formula (2) yield the following

Corollary. *Let $q \ge 1$ be odd, p prime, $p \equiv 2q+1 \bmod 4q$, $p > 2q+1$. Let $l \ge 3$ be a prime, $l \nmid q$, $l \nmid q-1$. Then l divides $C_{2q}h_{2q}^-/(C_2h_2^-)$ if and only if the vector $\overline{\Phi} \in \mathbb{F}_l^q$ is in the linear manifold*

$$M_l^* = \bigcup (V_Z\ ;\ Z \in \mathcal{Z}\,,\ Z \ne \{1\})\,.$$

Table 1 (cont.)

l-divisibility of $h_6^-(p)$ for $p < 500000$; total number of p's: 10402

l	n_l	m_l	n_l^*	m_l^*	l	n_l	m_l	n_l^*	m_l^*
5	0.2701	0.2320	0.0386	0.0400	7*	0.4104	0.3703	0.2899	0.2653
11	0.1055	0.0984	0.0074	0.0083	13	0.2269	0.2135	0.1578	0.1479
17	0.0663	0.0621	0.0030	0.0035	19	0.1543	0.1497	0.1073	0.1025
23	0.0480	0.0453	0.0010	0.0019	29	0.0349	0.0356	0.0012	0.0012
31	0.0976	0.0937	0.0673	0.0635	37	0.0822	0.0789	0.0567	0.0533
41	0.0254	0.0250	0.0004	0.0006	43	0.0705	0.0682	0.0473	0.0460
47	0.0221	0.0217	0.0004	0.0005	53	0.0184	0.0192	0.0003	0.0004
59	0.0195	0.0172	0.0002	0.0003	61	0.0477	0.0484	0.0316	0.0325
67	0.0441	0.0441	0.0289	0.0296	71	0.0174	0.0143	0.0002	0.0002
73	0.0385	0.0405	0.0261	0.0272	79	0.0392	0.0375	0.0248	0.0252
83	0.0138	0.0122	0.0002	0.0001	89	0.0130	0.0114	0.0001	0.0001
97	0.0327	0.0306	0.0225	0.0205					

l-divisibility of $h_8^-(p)$ for $p < 500000$; total number of p's: 5165

l	n_l	m_l	l	n_l	m_l
3*	0.2151	0.2099	5*	0.0794	0.0784
7	0.0414	0.0404	11	0.0170	0.0165
13	0.0112	0.0118	17	0.2290	0.2153
19	0.0048	0.0055	23	0.0043	0.0038
29	0.0031	0.0024	31	0.0017	0.0021
37	0.0019	0.0015	41	0.0931	0.0940
43	0.0019	0.0011	47	0.0010	0.0009
53	0.0004	0.0007	59	0.0002	0.0006
61	0.0002	0.0005	67	0.0010	0.0004
71	0.0002	0.0004	73	0.0511	0.0537
79	0.0004	0.0003	83	0.0008	0.0003
89	0.0409	0.0442	97	0.0451	0.0406

In view of the Corollary we also render the numbers

$$n_l^* = |\{p \in P\ ;\ l \mid (h_{2q}^-(p)/h_2^-(p))\}|/|P|$$

and

$$m_l^* = |M_l^*|/l^q$$

in Table 1, for $q = 3, 5$. If l divides some quotient C_{2q}/C_2, the definition of n_l^* has been modified appropriately.

Let $q = 6$. Then $C_4 h_4^-$ divides $C_{12} h_{12}^-$. Again, l divides the quotient $C_{12} h_{12}^-/(C_4 h_4^-)$ if and only if $\overline{\Phi}$ is in a certain linear manifold $M_l^* \subseteq \mathbb{F}_l^6$. Table 1 contains $m_l^* = |M_l^*|/l^6$ and the comparative figure n_l^*.

Table 1 (cont.)

l-divisibility of $h_{10}^-(p)$ for $p < 500000$; total number of p's: 5208

l	n_l	m_l	n_l^*	m_l^*	l	n_l	m_l	n_l^*	m_l^*
3*	0.4181	0.3416	0.0054	0.0123	7	0.1674	0.1432	0.0006	0.0004
11*	0.4203	0.3791	0.3514	0.3170	13	0.0816	0.0770	0.0000	0.0000
17	0.0588	0.0588	0.0000	0.0000	19	0.0613	0.0579	0.0056	0.0055
23	0.0432	0.0435	0.0000	0.0000	29	0.0313	0.0368	0.0021	0.0024
31*	0.1602	0.1512	0.1281	0.1229	37	0.0244	0.0270	0.0000	0.0000
41	0.1171	0.1161	0.0916	0.0940	43	0.0246	0.0233	0.0000	0.0000
47	0.0236	0.0213	0.0000	0.0000	53	0.0173	0.0189	0.0000	0.0000
59	0.0207	0.0175	0.0010	0.0006	61	0.0762	0.0793	0.0618	0.0640
67	0.0134	0.0149	0.0000	0.0000	71	0.0672	0.0685	0.0545	0.0552
73	0.0113	0.0137	0.0000	0.0000	79	0.0180	0.0130	0.0004	0.0003
83	0.0132	0.0120	0.0000	0.0000	89	0.0119	0.0115	0.0006	0.0003
97	0.0117	0.0103	0.0000	0.0000					

l-divisibility of $h_{12}^-(p)$ for $p < 500000$; total number of p's: 5191

l	n_l	m_l	n_l^*	m_l^*	l	n_l	m_l	n_l^*	m_l^*
5*			0.0820	0.0784	7	0.0543	0.0600	0.0358	0.0404
11	0.0235	0.0246	0.0171	0.0165	13*	0.4038	0.3814	0.2993	0.2740
17	0.1310	0.1203	0.0060	0.0069	19	0.0100	0.0083	0.0062	0.0055
23	0.0056	0.0057	0.0046	0.0038	29	0.0657	0.0700	0.0025	0.0024
31	0.0029	0.0031	0.0017	0.0021	37	0.1516	0.1516	0.1063	0.1038
41	0.0541	0.0493	0.0012	0.0012	43	0.0025	0.0016	0.0019	0.0011
47	0.0008	0.0014	0.0006	0.0009	53	0.0364	0.0381	0.0006	0.0007
59	0.0006	0.0009	0.0004	0.0006	61	0.0896	0.0944	0.0584	0.0640
67	0.0000	0.0007	0.0000	0.0004	71	0.0006	0.0006	0.0002	0.0004
73	0.0746	0.0794	0.0516	0.0537	79	0.0008	0.0005	0.0002	0.0003
83	0.0006	0.0004	0.0002	0.0003	89	0.0223	0.0226	0.0000	0.0003
97	0.0599	0.0603	0.0403	0.0406					

In Table 2 we have collected up the relative class numbers $h_{12}^-(p)$ for all $p < 10000$ ($p \equiv 13 \bmod 24$, of course).

Table 2. Relative class numbers h_{12}^-

p	h_{12}^-	p	h_{12}^-	p	h_{12}^-
13	1	37	1	61	1
109	17	157	65	181	925
229	221	277	272	349	1040
373	305	397	832	421	925
541	2257	613	2425	661	1053

Table 2 (cont.)

p	h_{12}^-	p	h_{12}^-	p	h_{12}^-
709	12688	733	3645	757	157625
829	26245	853	2516	877	22681
997	1825	1021	3977	1069	13949
1093	555185	1117	577405	1213	94357
1237	42125	1381	166617	1429	288353
1453	270725	1549	17725	1597	682541
1621	1441557	1669	1512745	1693	314237
1741	116285	1789	57616	1861	132977
1933	24737	2029	3922321	2053	92537
2221	1797497	2269	67625	2293	171593
2341	1173037	2389	23725	2437	660857
2557	514345	2677	1338949	2749	1112905
2797	1502800	2917	300913	3037	469456
3061	102245	3109	350649	3181	7938905
3229	3985097	3253	9983713	3301	369313
3373	7747909	3469	821881	3517	186004
3541	152165	3613	2595125	3637	3896505
3709	6131905	3733	20787845	3853	14944265
3877	3801037	4021	849433	4093	37654825
4261	570704	4357	1633360	4549	457145
4597	1505969	4621	5254945	4789	3930768
4813	3288745	4861	21461193	4909	5479825
4933	24722117	4957	15291185	5077	601625
5101	5343205	5197	623376	5413	2707549
5437	1916217	5557	6719089	5581	1208453
5653	8808669	5701	7036165	5749	6233305
5821	907985	5869	1652813	6037	1839188
6133	1254509	6229	5476409	6277	6378125
6301	74076509	6373	7973593	6397	11072477
6421	20553277	6469	8725853	6637	9356180
6661	13352065	6709	1458500	6733	3908125
6781	18425549	6829	12125605	6949	5479825
6997	5553841	7069	43433797	7213	1275625
7237	14537637	7309	5188433	7333	6472325
7477	8024605	7549	2665345	7573	124889341
7621	26335985	7669	345404785	7717	95208637
7741	2900269	7789	10178869	7933	19589465
8053	88674769	8101	20686509	8221	6688625
8269	283411453	8293	14654925	8317	7268249
8389	7384609	8461	5808245	8581	2116585
8629	77909364	8677	550198737	8821	120093581
8893	2169593	8941	43577965	9013	27373801

Table 2 (cont.)

p	h_{12}^-	p	h_{12}^-	p	h_{12}^-
9109	1759504	9133	10980625	9157	2655065
9181	4484077	9277	156931101	9349	20541845
9397	22924681	9421	397973056	9613	406792061
9661	44395585	9733	26450125	9781	34076653
9829	7163125	9901	661365493	9949	15834377
9973	286173589				

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York 1976.

[2] S. I. Borevič und I. R. Šafarevič, *Zahlentheorie*, Birkhäuser, Basel 1966.

[3] K. Girstmair, *The relative class numbers of imaginary cyclic fields of degrees* 4, 6, 8, *and* 10, Math. Comp., to appear.

[4] —, *On the cosets of the* 2q*-power group in the unit group modulo* p, Abh. Math. Sem. Univ. Hamburg 62 (1992), 217–232.

[5] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper* (Nachdruck der ersten Auflage), Springer, Berlin 1985.

[6] R. H. Hudson, *Class numbers of imaginary cyclic quartic fields and related quaternary systems*, Pacific J. Math. 115 (1984), 129–142.

INSTITUT FÜR MATHEMATIK
UNIVERSITÄT INNSBRUCK
TECHNIKERSTRASSE 25/7
A-6020 INNSBRUCK, ÖSTERREICH

Received on 19.9.1992 (2305)