Mathematica Slovaca

Pavel Trojovský

On divisibility of the class number h^+ of the real cyclotomic fields $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ by primes $q < 10000$

Mathematica Slovaca, Vol. 50 (2000), No. 5, 541--555

Persistent URL: http://dml.cz/dmlcz/132741

Mathematica Slovaca
© 2000
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **50** (2000), No. 5, 541–555

ON DIVISIBILITY OF THE CLASS NUMBER h^+ OF THE REAL CYCLOTOMIC FIELDS $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ BY PRIMES $q < 10000$

PAVEL TROJOVSKÝ

(*Communicated by Stanislav Jakubec*)

ABSTRACT. Let l, p be primes such that $p = 2l + 1$. The paper deals with divisibility of the class number of the real cyclotomic field $\mathbf{Q}(\zeta + \zeta^{-1})$ by the primes $q < 10000$ having order mod l equal to $(l-1)/2$. This paper is extension of [JAKUBEC, S.—TROJOVSKÝ, P.: *On divisibility of the class number h^+ of the real cyclotomic fields $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ by primes $q \leq 5000$*, Abh. Math. Sem. Univ. Hamburg **67** (1997), 269–280] and included computations are based mainly on some criteria from [JAKUBEC, S.: *On divisibility of the class number h^+ of the real cyclotomic fields of prime degree l*, Math. Comp. **67** (1998), 396–398].

Introduction

First of all we summarize the results concerning this problem which were obtained up to the present time.

To consider divisibility of the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$ by primes q it is appropriate to classify primes q according to their order modulo l:

(I) The order q modulo l is $l-1$ (thus q is a primitive root modulo l).

In this case the problem is completely solved. Davis in [1] proved that 2 does not divide h^+ and for all $q > 2$ Jakubec in [3] proved that q does not divide h^+.

(II) The order of q modulo l is $\frac{l-1}{2}$ (hence when q generates the group of quadratic residues modulo l) with $l \equiv 3 \pmod 4$.

In this case it was proved:

2000 Mathematics Subject Classification: Primary 11R29.
Key words: class number, cyclotomic field, computation, divisibility.

1) 2 does not divide h^+. (Estes [2])
2) 3 does not divide h^+. (Jakubec [4])
3) 5 does not divide h^+. (Jakubec [5])
4) For $q \leq 23$ prime q does not divide h^+. (Jakubec [8])
5) For $q \leq 5000$ prime q does not divide h^+. (For the proof see [9])

The following theorem was proved in [9]:

THEOREM. ([9; Theorem 1]) *Let q be a prime, $q < 5000$. Let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$, and let the order of the prime q modulo l be $l - 1$ or $\frac{l-1}{2}$. Then the prime q does not divide h^+, the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.*

The aim of this paper is to prove the following theorem, which is a stronger version of [9; Theorem 1]:

THEOREM 1. *Let q be a prime, $q < 10000$. Let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$, and let the order of the prime q modulo l be $l - 1$ or $\frac{l-1}{2}$. Then the prime q does not divide h^+, the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.*

Theorem 1 implies the following Theorem 2:

THEOREM 2. *Let p be a prime such that $\frac{p-1}{2}$ and $\frac{p-3}{4}$ are primes. Then there is no prime $q < 10000$ dividing the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.*

Table 1.

q	p	q	p	q	p	q	p
5011	359	6143	167	7877	359	8963	167
5147	167	6473	167	8233	359	9461	167
5477	167	6803	359	8467	167	9463	167
5479	167	6971	167	8627	1439	9629	167
5743	719	7159	359	8629	1439		
6113	2039	7517	359	8951	359		

It is an open question whether there exist infinitely many primes p which satisfy the assumptions of Theorem 2.

We wish to state that the answer is positive, provided one assumes the following hypothesis of SCHINZEL (1958):

SCHINZEL'S HYPOTHESIS. *Let $s \geq 1$, let $f_1(X), \ldots, f_s(X)$ be irreducible polynomials with integral coefficients; assume that the leading coefficient of $f_i(X)$ is positive and that no integer $n > 1$ divides all the numbers $f_1(m), f_2(m), \ldots, f_s(m)$. Then there exists one (and it may be proved, necessarily infinitely many) natural number(s) m such that $f_1(m), f_2(m), \ldots, f_s(m)$ are all primes.*

Proof of Theorem 2. For $q < 5000$ the theorem holds by [9; Theorem 2], therefore we will consider $5000 < q < 1000$ only. The assumptions of Theorem 2 imply that each prime $q \not\equiv 0, \pm 1 \pmod{l}$ is a primitive root modulo l or the order of q modulo l is $\frac{l-1}{2}$, hence q satisfies the assumptions of Theorem 1. But we must check the cases $q \equiv 0$ or $\pm 1 \pmod{l}$. For $q \equiv 0 \pmod{l}$ the prime q does not divide h^+ by [13; Theorem 10.4] and for $q \equiv \pm 1 \pmod{l}$ we must consider the following cases:

(i) $q = p$. But by [12], q does not divide h^+.

(ii) $q \neq p$. In this case we use the following fact:

If $q \mid h^+$, then $q \mid N_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\tau)$, where

$$\tau = \sum_{0<i<\frac{p}{2}} A_{\frac{-i}{p}} \chi(i)$$

with $\chi(x)$ a Dirichlet character modulo p of the order l (the numbers $A_{\frac{-i}{p}}$ will be defined latter), which is implied by [10; Proposition 2] and [8; Lemma 1]. By computation, it has been checked that all q except $q = 8629$ from the previous Table 1 do not divide $N_{\mathbf{Q}(\zeta_l)/\mathbf{Q}}(\tau)$, therefore they do not divide h^+. The remaining $q = 8629$ ($p = 1439$) does not divide h^+, it follows from [13; pp. 421–423, Table]. □

Proof of Theorem 1. For $q < 5000$ the theorem holds by [9; Theorem 1], thus we will consider $5000 < q < 1000$ only. We will use the results from [8], hence we introduce the needed results and the notation now.

Let q be an odd prime. Define the numbers $A_0, A_1, A_2, \ldots, A_{q-1}$ as follows:

$$A_0 = 0\,, \qquad A_j = \sum_{i=1}^{j} \frac{1}{i} \quad \text{for } j = 1, 2, \ldots, q-1\,.$$

Let s be a rational q-integer. Put $A_s = A_j$ for an integer j, $0 \leq j < q$, $s \equiv j \pmod{q}$. Let m, n be natural numbers $m \equiv 1 \pmod{2}$, $(m,n) = 1$. Associate to the number n the permutation $\phi_{m,n}$ of the numbers $1, 2, \ldots, \frac{m-1}{2}$ as follows:

$$\phi_{m,n}(x) \equiv \pm nx \pmod{m} \qquad \text{for} \quad x = 1, 2, \ldots, \frac{m-1}{2}\,.$$

Further, associate to the number n the quadratic form $Q_{m,n}(x_1, x_2, \dots x_{\frac{m-1}{2}})$,

$$Q_{m,n}(x_1, x_2, \dots x_{\frac{m-1}{2}}) = x_1^2 + x_2^2 + \dots + x_{\frac{m-1}{2}}^2 - \sum_{i=1}^{\frac{m-1}{2}} x_i x_{\phi_{m,n}(i)} .$$

Then the following theorems hold:

THEOREM. ([8; Theorem 1]) *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -m \pmod q$, $m \equiv 1 \pmod 2$, $m > 0$, and let the order of the prime q modulo l be $\frac{l-1}{2}$. Suppose that q divides the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then for each divisor n of the number $p+m$, $(n,q) = 1$, the following congruence holds*

$$\frac{p+m}{2q} \frac{n^{q-1}-1}{q} \equiv Q_{m,n}(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \dots, A_{\frac{-t}{m}}) \pmod q . \tag{i}$$

If $nq \mid \frac{p+m}{q}$, then

$$\frac{p+m}{2q^2} \equiv -Q_{m,qn}(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \dots, A_{\frac{-t}{m}}) \pmod q , \tag{ii}$$

where $t = \frac{m-1}{2}$.

But we will need only the congruence (i) in this article.

Let j be an integer, $0 < j < 2q$. Define the sums

$$S_j = \sum_{i=1}^{\frac{q-1}{2}} A_i \sum_{\substack{k=1 \\ k \equiv 1 \pmod 2 \\ 2ji \not\equiv -k \pmod q}}^{j-1} \frac{1}{2ji+k} - \sum_{i=\frac{q+1}{2}}^{q-1} A_i \sum_{\substack{k=1 \\ k \equiv 1 \pmod 2 \\ 2ji \not\equiv -k \pmod q}}^{j-1} \frac{1}{2ji+k} .$$

THEOREM. ([8; Theorem 5]) *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -1 \pmod q$, and let the order of the prime q modulo l be $\frac{l-1}{2}$. Suppose that for each j such that $S_j \equiv 0 \pmod q$ there exists n, $(n, 2q) = 1$, $n \mid p+1$, such that $S_{j^*} \not\equiv 0 \pmod q$, where $j^* \equiv nj \pmod{2q}$. Then q does not divide the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.*

Theorem 1 will be proved by computations. We check consecutively the primes $q = 5003, \dots, 9973$. If we take a concrete q, then for each prime p, $p \neq q$ the following holds:

$$p \equiv -m \pmod q , \qquad \text{where} \quad m = 1, 3, \dots, 2q-3 .$$

Therefore, for this q we must make for each value m the corresponding computations, which we divide into two parts:

(A) For each concrete q we check values $m \neq -1$, thus $p \not\equiv -1 \pmod q$ and we make computations by [8; Theorem 1].

(B) By [8; Theorem 5], we make computations for $m = 1$, we set $n = 3$.

The part (A) is divided again into two parts:

a) We make computations with the help of the following corollary of [9]:

COROLLARY 1. ([8; Corollary]) *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -m \pmod q$ for $m = 3, 5, \ldots, 2q-3$, and let the order of the prime q modulo l be $\frac{l-1}{2}$. Suppose that q divides the class number h^+ of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then the following congruences hold:*

(1) *If $m \equiv 1 \pmod 4$, then*

$$Q_{m,4}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \equiv 2Q_{m,2}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \pmod q,$$

where $t = \frac{m-1}{2}$.

(2) *If $m \equiv 3 \pmod 4$, then*

$$Q_{m+2q,4}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \equiv 2Q_{m+2q,2}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \pmod q,$$

where $t = \frac{2q+m-1}{2}$.

The Table 2 determines the values q, m for which Corollary 1 does not give any answer.

b) Each pair (q, m) from Table 2 was checked by the following corollary:

COROLLARY 2. *Let q be an odd prime. Let l, p be primes such that $p = 2l+1$, $l \equiv 3 \pmod 4$, $p \equiv -m \pmod q$ for $m = 1, 3, 5, \ldots 2q-3$, $m \equiv 0, 2 \pmod 3$, and let the order of the prime q modulo l be $\frac{l-1}{2}$. Suppose that q divides h^+, the class number of the real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Then the following holds:*

(1) *If $m \equiv 0 \pmod 3$, $q \equiv 1 \pmod 3$, then*

$$Q_{m+4q,2}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) + Q_{m+4q,3}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \equiv Q_{m+4q,6}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \pmod q,$$

where $t = \frac{4q+m-1}{2}$.

(2) *If $m \equiv 0 \pmod 3$, $q \equiv 2 \pmod 3$, then*

$$Q_{m+2q,2}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) + Q_{m+2q,3}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \equiv Q_{m+2q,6}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \pmod q,$$

where $t = \frac{2q+m-1}{2}$.

(3) *If $m \equiv 2 \pmod 3$, $q \equiv 1 \pmod 3$, then*

$$Q_{m+2q,2}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) + Q_{m+2q,3}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \equiv Q_{m+2q,6}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \pmod q,$$

where $t = \frac{2q+m-1}{2}$.

(4) *If* $m \equiv 2 \pmod 3$, $q \equiv 2 \pmod 3$, *then*

$$Q_{m+4q,2}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) + Q_{m+4q,3}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \equiv Q_{m+4q,6}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \pmod q,$$

where $t = \frac{4q+m-1}{2}$.

(5) *If* $m \equiv 1 \pmod 3$, *then*

$$Q_{m,2}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) + Q_{m,3}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \equiv Q_{m,6}\left(A_{\frac{-1}{m}}, A_{\frac{-2}{m}}, \ldots, A_{\frac{-t}{m}}\right) \pmod q,$$

where $t = \frac{m-1}{2}$.

P r o o f. The proof follows from the congruence (i), [8; Theorem 1] and the fact that

$$\frac{2^{q-1}-1}{q} + \frac{3^{q-1}-1}{q} \equiv \frac{6^{q-1}-1}{q} \pmod q.$$

□

By a computation, it was checked that [8; Theorem 3] gives the answer in all cases and therefore $q < 10000$ does not divide h^+ for $p \not\equiv -1 \pmod q$.

(B) $p \equiv -1 \pmod q$.

In this case we use [8; Theorem 5], where we set $n = 3$ (because $3 \mid p+1$).

By this theorem it is necessary to compute the sums S_j for $j = 2, 4, \ldots, 2q-2$ but with respect to [9; Lemma] it suffices to compute $j = 2, 4, \ldots, q-1$ only. Then the computation is much faster.

The Table 3 contains the values j for which is $S_j \equiv 0 \pmod q$. The primes q for which there is just one $j \leq q-1$ such that $S_j \equiv 0 \pmod q$ are not written in Table 3.

By computation, it has been checked that $S_{j^*} \not\equiv 0 \pmod q$ with $j^* \equiv 3j \pmod{2q}$ for each j from Table 3. Therefore, Theorem 1 is proved. □

Remark. To compute the sums S_j, a program written in PASCAL was employed and the system *Mathematica* for the other computations. The computation was done by a PC PENTIUM II. The total machine time was approximately 50000 h. The computation of the sums S_j took the major part of this time.

Table 2.

q	m	q	m	q	m	q	m	q	m
5009	91	5387	7085	5701	9201	6067	7519	6367	12111
5009	6339	5393	1157	5701	11399	6073	1027	6373	12743
5009	10015	5393	10783	5711	2597	6073	12143	6379	2891
5011	7687	5399	4953	5717	2325	6079	437	6389	2461
5021	109	5413	1681	5717	11431	6089	12175	6389	4413
5021	2629	5413	4475	5737	505	6101	9693	6389	12775
5021	4739	5413	10823	5737	11471	6101	12199	6397	12791
5021	8857	5417	10831	5741	11479	6113	12223	6421	12839
5021	10039	5419	4809	5749	11447	6121	12239	6427	161
5039	2273	5419	10831	5749	11495	6133	1131	6449	12895
5039	7291	5437	10871	5791	4671	6133	5567	6451	3033
5059	9849	5441	8589	5791	11103	6133	12263	6469	11997
5077	3191	5441	10879	5801	11599	6173	12343	6469	12935
5077	10151	5443	10093	5807	929	6197	12391	6473	12333
5081	10159	5449	9697	5813	11623	6199	5733	6473	12943
5099	3537	5449	10895	5821	11639	6199	8433	6481	12959
5099	8731	5477	10951	5849	9185	6217	7785	6491	2153
5101	7275	5501	10999	5849	11695	6217	12431	6491	11491
5101	10199	5521	3317	5851	8035	6221	6367	6521	13039
5107	9759	5521	6961	5857	7691	6221	12439	6529	13055
5113	2475	5521	11039	5857	11711	6229	449	6551	6923
5113	10223	5557	11111	5861	11719	6229	12455	6551	10437
5153	10303	5569	11135	5869	11735	6247	1047	6553	3455
5171	5055	5573	6877	5881	2951	6257	12511	6553	13103
5189	10375	5573	11143	5881	11759	6269	7025	6569	11971
5197	10391	5581	3249	5897	1507	6269	12535	6569	13135
5209	10415	5581	11159	5897	3245	6271	7099	6571	5409
5227	6101	5639	3171	5897	11791	6277	12551	6577	13151
5227	8883	5641	11279	5923	8363	6299	5727	6581	8815
5233	10463	5651	3239	5953	11903	6301	1941	6581	13159
5237	10471	5653	8055	5981	11523	6301	12599	6599	115
5261	10519	5653	11303	5981	11959	6311	157	6599	7845
5273	8519	5657	6341	6007	951	6317	10203	6607	5799

q	m	q	m	q	m	q	m	q	m
5273	10431	5657	11157	6029	2365	6317	12631	6637	2729
5273	10543	5657	11311	6027	12055	6329	12655	6637	13271
5281	8539	5669	11335	6037	7783	6337	1157	6653	13303
5281	10559	5683	6323	6037	12071	6337	2747	6659	10201
5297	10591	5683	6855	6043	11225	6337	12671	6661	3687
5309	10615	5689	713	6047	10389	6343	10953	6661	4453
5323	9781	5689	6825	6053	2941	6353	2221	6661	13319
5333	10663	5689	11375	6053	9835	6337	6093	6673	13343
5351	2573	5693	11383	6053	12103	6337	12703	6689	13375
5381	10759	5701	7263	6067	3659	6361	12719	6691	5393
6691	11759	7039	4591	7547	9871	7873	15743	8231	5771
6701	2777	7043	2245	7549	15095	7877	15751	8233	339
6701	13399	7057	13441	7561	15119	7879	12419	8233	16463
6709	13415	7057	14111	7573	15143	7883	8663	8237	16471
6733	13463	7069	14135	7577	2751	7901	15799	8243	9041
6737	1099	7109	5609	7577	4243	7933	6393	8263	5663
6737	13471	7109	14215	7577	15151	7933	15863	8263	9705
6761	13191	7121	8181	7589	1631	7937	15871	8263	10215
6761	13519	7121	14239	7589	2709	7949	13493	8269	16535
6763	10895	7129	691	7589	11005	7949	15723	8273	9283
6781	2963	7129	14255	7589	15175	7949	15895	8273	16543
6781	13559	7177	14351	7591	8703	7963	2227	8287	6867
6793	13049	7193	14383	7591	14303	7963	4891	8287	7879
6793	13583	7213	14423	7603	5555	7963	10067	8291	67
6803	5447	7229	14455	7607	14929	7963	11835	8293	16583
6829	13655	7237	10941	7621	15239	7993	15983	8317	16631
6833	11639	7237	14471	7639	5741	8009	16015	8329	16655
6833	13663	7247	1837	7643	2967	8011	889	8353	121
6841	8309	7253	14503	7643	3171	8011	1101	8353	9853
6841	13679	7297	14591	7649	15295	8011	11213	8353	16703
6857	13711	7309	14615	7669	15335	8017	16031	8369	14873
6863	8641	7321	14639	7673	15343	8053	12015	8369	16735
6869	13735	7331	1587	7681	4839	8053	16103	8377	16751
6917	6061	7333	13993	7681	15359	8081	6537	8387	12483

q	m	q	m	q	m	q	m	q	m
6917	9849	7333	14663	7691	3357	8081	9321	8389	16775
6917	10933	7349	14695	7691	9605	8081	11209	8429	16855
6917	13831	7369	14735	7717	9273	8081	14541	8461	16919
6947	8813	7393	14783	7717	15431	8081	16159	8501	16999
6949	13895	7417	14831	7741	15479	8087	1155	8513	503
6959	3705	7433	501	7753	15503	8089	16175	8513	17023
6961	3315	7433	14863	7757	15511	8093	16183	8521	17039
6961	13919	7457	10867	7759	563	8101	14901	8537	17071
6967	10441	7457	14911	7789	15575	8101	16199	8543	6547
6977	13951	7459	3119	7793	77	8117	16231	8573	17143
6991	8041	7477	9221	7793	15583	8161	16319	8581	17159
6997	10607	7477	14951	7817	15631	8179	309	8597	17191
6997	13991	7481	14959	7823	2697	8191	11487	8599	4911
7001	12557	7489	14975	7829	15655	8209	15877	8609	17215
7001	13999	7517	9069	7841	15679	8209	16415	8629	17255
7013	14023	7517	15031	7853	2653	8219	1095	8641	17279
7019	13447	7529	15055	7853	15703	8219	10745	8677	17351
7027	2293	7537	15071	7873	2851	8221	16439	8681	17359
7027	10463	7541	15079	7873	10171	8221	10481	8689	17375
8693	14011	8969	17935	9221	18439	9473	18943	9733	19463
8693	17383	9001	5457	9227	8755	9479	7507	9749	2151
8699	15121	9001	17999	9241	18479	9479	12435	9749	19495
8707	11165	9011	4461	9257	18511	9497	18991	9767	10893
8713	17423	9011	16837	9277	18551	9521	19039	9769	19535
8731	15357	9013	18023	9281	17689	9533	19063	9781	19559
8737	17471	9029	7567	9281	18559	9539	16883	9817	19631
8741	17479	9029	18055	9293	18583	9601	19199	9829	7245
8753	17503	9041	7171	9319	9755	9613	4477	9829	19655
8761	17203	9041	18079	9319	13393	9613	14173	9833	19663
8761	17519	9043	1275	9337	18671	9613	17827	9839	18837
8779	5835	9049	18095	9341	18679	9613	19223	9857	7177
8807	711	9059	4397	9343	3779	9619	2967	9857	16467
8807	1579	9091	4203	9349	7019	9629	15415	9857	19711
8807	3513	9091	11889	9349	14937	9629	19255	9901	19799

q	m	q	m	q	m	q	m	q	m
8821	17639	9109	18215	9349	18695	9643	18545	9907	12607
8837	17671	9127	4599	9371	12843	9649	19295	9923	6227
8849	17695	9133	18263	9377	18751	9661	8897	9929	19855
8861	2835	9137	18271	9397	18791	9661	13365	9931	6245
8861	6659	9157	10645	9413	18823	9661	19319	9941	19879
8861	13629	9157	18311	9419	1569	9677	2469	9949	19895
8861	17719	9161	18319	9421	18839	9677	19351	9973	19943
8863	16151	9173	9357	9433	18863	9689	19375		
8893	16503	9173	10259	9437	7321	9697	12095		
8893	17783	9173	18343	9437	18871	9697	19391		
8929	17855	9181	18359	9461	18919	9719	3429		
8933	4451	9209	18415	9463	6635	9719	10085		
8933	17863	9221	325	9473	6373	9721	18785		
8941	17879	9221	14783	9473	16201	9721	19439		

Table 3.

q	j			
5059	1812	5058		
5081	3264	5080		
5099	1342	4164	5098	
5101	1998	4280	4822	5100
5147	3610	5146		
5153	2500	5152		
5167	2916	5166		
5179	612	5178		
5197	902	2942	5196	
5227	1622	3018	5226	
5233	2698	5232		
5237	1024	5236		
5281	232	5280		
5303	4630	5302		
5309	970	5308		
5323	2294	5322		
5351	748	2414	5350	
5387	910	5386		
5393	1114	5392		
5399	2890	5398		
5407	4406	5406		
5413	3212	5412		
5417	2202	5416		
5419	2680	5418		
5443	1806	5442		
5449	1094	5448		
5477	2188	5476		
5479	4736	5478		
5519	1668	5518		
5527	2132	5526		
5531	5280	5530		
5563	3092	5562		
5581	1450	1608	2694	5580
5623	3444	5622		

q	j				
5821	3276	5820			
5857	2890	4622	5856		
5869	5510	5868			
5927	1782	5926			
5953	626	1346	5952		
6011	4740	6010			
6037	2574	6036			
6053	4134	6052			
6073	4140	6072			
6079	5158	6078			
6089	1346	4920	6088		
6113	1580	6112			
6131	4646	6130			
6133	478	1892	6132		
6143	10	6142			
6173	3142	6172			
6197	3770	6196			
6217	3032	6216			
6221	5534	6220			
6229	2970	6228			
6247	210	6246			
6271	4340	6270			
6287	4726	6286			
6317	872	1754	2974	5584	6316
6329	2756	4634	6328		
6361	6234	6360			
6367	2848	4942	6366		
6389	1730	3142	6388		
6397	4662	6396			
6547	854	5298	6546		
6637	734	6636			
6653	5254	6652			
6659	2086	6658			
6673	1268	6672			

q	j			
5641	5234	5640		
5651	4134	4814	5650	
5683	1956	5682		
5711	5500	5710		
5743	794	5742		
5801	2790	5800		
5807	5592	5806		
5813	4386	5812		
6841	4584	6840		
6857	530	3928	6856	
6883	4236	6882		
6899	188	6898		
6971	6906	6970		
6983	2000	6982		
7039	1738	7038		
7057	5570	7056		
7069	2426	2828	7068	
7079	2956	5670	7078	
7103	6118	7102		
7177	4518	7176		
7211	3484	7210		
7213	6	6228	7212	
7219	116	7218		
7237	3010	7236		
7283	2310	7282		
7331	6746	7330		
7333	5722	7332		
7351	3234	7350		
7369	1762	7368		
7417	1556	7416		
7433	6228	7432		
7489	5298	7488		
7507	2034	7506		
7517	2518	3094	7516	
7537	5466	7536		

q	j				
6691	3296	6690			
6703	852	6702			
6733	844	5816	6732		
6763	3014	6762			
6779	2652	6778			
6793	3886	6792			
6803	2524	6802			
6829	1062	6828			
7919	4128	7918			
7927	1420	6470	7926		
7933	1080	7932			
7951	688	7950			
7963	6360	7962			
8087	6764	8086			
8089	3520	8088			
8093	574	8092			
8117	5422	8116			
8167	2756	8166			
8171	3746	8170			
8219	3696	8218			
8231	866	2596	8230		
8237	852	8236			
8243	206	3052	8242		
8263	1652	8262			
8269	6322	8268			
8287	6944	8286			
8291	2632	8290			
8311	5356	8310			
8329	3306	8328			
8369	1056	8368			
8389	1644	8388			
8429	884	8428			
8501	1408	8500			
8527	8118	8526			
8563	5666	8562			

q	j			
7547	1680	7546		
7559	3962	7558		
7573	160	3472	4142	7572
7577	6306	7576		
7583	438	5766	7582	
7673	1508	7672		
7691	3218	7690		
7699	586	7698		
7717	2916	7716		
7727	1354	2836	7726	
7793	2876	3542	7792	
7823	662	7822		
7841	1684	7840		
7883	4934	7882		
7907	4732	7906		

q	j				
8609	2414	2750	4000	5250	8608
8663	2598	8662			
8677	80	5224	8676		
8713	2794	8712			
8737	4542	6508	8736		
8779	6190	8778			
8783	6894	8782			
8803	4468	5734	8226	8802	
8831	7452	8830			
8839	5778	8838			
8863	1794	2838	8862		
8887	3764	8146	8886		
8933	5706	8932			
8969	3732	8968			
8971	2994	8970			

q	j			
9001	2788	7078		
9059	1156	9058		
9067	400	9066		
9091	808	2048	9090	
9133	8952	9132		
9137	3656	9136		
9181	5540	5862	9180	
9209	2764	9208		
9293	2504	9292		
9311	5630	9310		
9343	1178	9342		
9349	4844	9348		
9371	3918	9370		
9377	2374	3362	9376	
9421	2368	9420		

q	j			
9433	8168	9432		
9439	2372	8844	9438	
9461	3658	9460		
9463	3620	9462		
9467	3836	9466		
9511	3618	8716	9510	
9533	5788	9532		
9631	7258	9630		
9679	202	1422	9678	
9719	528	4378	9718	
9743	1074	9742		
9749	610	9748		
9781	1166	7772	9780	
9787	7082	9786		
9829	316	9828		
9833	1444	3616	9832	
9839	4714	9838		
9851	4466	9850		
9871	8448	9870		
9887	3100	9886		
9901	2044	9900		
9907	1236	8096	9906	
9923	7724	9922		
9949	1544	1682	5724	9948

REFERENCES

[1] DAVIS, D.: *Computing the number of totally positive circular units which are squares*, J. Number Theory **10** (1978), 1–9.

[2] ESTES, D. R.: *On the parity of the class number of the field of q-th roots of unity*, Rocky Mountain J. Math. **19** (1989), 675–681.

[3] JAKUBEC, S.: *On divisibility of class number or real abelian fields of prime conductor*, Abh. Math. Sem. Univ. Hamburg **63** (1993), 67–86.

[4] JAKUBEC, S.: *On Divisibility of h^+ by the prime* 3, Rocky Mountain J. Math. **24** (1994), 1467–1473.

[5] JAKUBEC, S.: *On Divisibility of h^+ by the prime* 5, Math. Slovaca **44** (1994), 650 700.

[6] JAKUBEC, S.: *Connection between Wiefferich congruence and divisibility of* h^+, Acta Arith. **71** (1995), 55–64.

[7] JAKUBEC, S.: *Connection between congruences* $n^{q-1} \equiv 1 \pmod{q^2}$ *and divisibility of* h^+, Abh. Math. Sem. Univ. Hamburg **66** (1996), 151–158.

[8] JAKUBEC, S.: *On divisibility of the class number* h^+ *of the real cyclotomic fields of prime degree* l, Math. Comp. **67** (1998), 396–398.

[9] JAKUBEC, S.—TROJOVSKÝ, P.: *On divisibility of the class number* h^+ *of the real cyclotomic fields* $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ *by primes* $q \leq 5000$, Abh. Math. Sem. Univ. Hamburg **67** (1997), 269–280.

[10] METSÄNKYLÄ, T.: *An application of the p-adic class number formula*, Manuscripta Math. **93** (1997), 481–498.

[11] VAN DER LINDEN, F.: *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), 693–707.

[12] WAGSTAFF, S. S.: *The irregular primes to* 125000, Math. Comp. **32** (1978), 583–592.

[13] WASHINGTON, L. C.: *Introduction to Cyclotomic Fields*. Grad Texts in Math., Springer-Verlag, New York-Heidelberg-Berlin, 1982.

Received February 26, 1999
Revised May 27, 1999

Department of Mathematics
University of Education
Víta Nejedlého 573
CZ–500 03 Hradec Králové
CZECH REPUBLIC