Acta Mathematica et Informatica Universitatis Ostraviensis

Tauno Metsänkylä
On the parity of the class numbers of real abelian fields

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 6 (1998), No. 1, 159--166

Persistent URL: `http://dml.cz/dmlcz/120530`

On the parity of the class numbers of real abelian fields

Tauno Metsänkylä

Abstract: Let K be a real abelian field with conductor q, an odd prime, and let h_K denote its class number. A result by Jakubec (1993) gives a criterion for the divisibility of h_K by an odd prime p. We state an analogous result for $p = 2$ and prove it by using the 2-adic class number formula. An application concerns the parity of h_K when $q = 4l + 1$, with l a prime.

Key Words: Cyclotomic fields, abelian fields, class numbers

Mathematics Subject Classification: Primary 11R18, 11R20, 11R29

1. Theorem

The main result of the present note is the following.

Theorem. *Let K be a real abelian field with conductor q, an odd prime. If the class number h_K of K is even, then*

$$\prod_{\chi\neq 1} \sum_{j=1}^{(q-1)/2} a_j\chi(j) \equiv 0 \pmod 2, \tag{1}$$

where the product extends over all nonprincipal characters χ of K and where

$$a_j = \begin{cases} 0 \text{ for } j \equiv 0 \text{ or } q \pmod 4, \\ 1 \text{ otherwise.} \end{cases} \tag{2}$$

Jakubec [J] has proved an analogous result about the divisibility of h_K by an odd prime p. In [M1], Jakubec's result was proved anew as an application of the p-adic class number formula. The present work arose from the idea to carry that proof over to the case $p = 2$. As it will turn out, the argument in [M1] needs some modifications that are not quite obvious. Actually, the proof below provides some additional information beyond that formulated in the theorem; see the remark in the end of §2.

The field K is contained in L^+, the maximal real subfield of the cyclotomic field $L = \mathbb{Q}(\zeta_q)$, where ζ_q denotes a primitive qth root of unity. It is well known that h_K divides h_{L^+}.

Results about the divisibility by 2 of h_K have a long history. A famous theorem by Kummer states that $2 \mid h_{L^+}$ implies $2 \mid h_L^-$, where $h_L^- = h_L/h_{L^+}$, the relative class number of L. Hasse in his monograph [H] generalized this result to all cyclic fields. A main tool in dealing with the parity of h_K has been its relationship to certain properties of the unit group of K. This topic was comprehensively studied by several authors in the sixties and seventies; see [G] and [D] and the references given therein. Feng [F] derived and applied a computational criterion for the parity of h_K; an error in his paper was pointed out by G. and M.-N. Gras (Zentralblatt für Mathematik 523.12006).

Compared to all this work the present result is quite different. Note, in particular, that the left hand side of (1) is a rational integer.

After proving the theorem in §2 we provide two applications in §3 and discuss some numerical examples in §4.

2. Proof of Theorem

Let Ω_2 denote a fixed algebraic closure of the 2-adic field $\mathbb{Q}_2$. Fix an embedding in Ω_2 of the field of algebraic numbers. All congruences in the sequel are to be understood in the 2-adic sense: for α, $\beta \in \Omega_2$, one writes $\alpha \equiv \beta \pmod{2^k}$ to mean that $v_2(\alpha - \beta) \geq k$. Here v_2 is the notation for the 2-adic exponential valuation on Ω_2, normalized by $v_2(2) = 1$.

Set $[K : \mathbb{Q}] = n$. The 2-adic class number formula for h_K reads

$$\frac{2^{n-1} h_K R_2}{\sqrt{d}} = \prod_{\chi \neq 1} \left(1 - \frac{\chi(2)}{2}\right)^{-1} L_2(1, \chi),$$

where R_2 and d denote the 2-adic regulator and the discriminant of K, respectively, and $L_2(s, \chi)$ is the 2-adic L-function attached to a Dirichlet character χ of K. Rewrite this equation as

$$h_K \frac{R_2}{2^{n-1}} = \sqrt{d} \prod_{\chi \neq 1} \tfrac{1}{4} \left(1 - \frac{\chi(2)}{2}\right)^{-1} L_2(1, \chi). \tag{3}$$

A known argument (recalled in [M1], proof of Proposition 1) shows that $R_2/2^{n-1}$ is a 2-adic integer. We will show that

$$\tfrac{1}{4} \left(1 - \frac{\chi(2)}{2}\right)^{-1} L_2(1, \chi) \equiv \overline{\chi}(2) \sum_{j=1}^{(q-1)/2} a_j \chi(j) \pmod{2}, \tag{4}$$

whenever $\chi \neq 1$, where a_j are the numbers given by (2) and $\overline{\chi}$ denotes the complex conjugate of χ. Since R_2 is nonzero and d, being a power of q, is odd, we see that the theorem follows from (3) and (4).

For $L_2(1,\chi)$ one has the formula

$$\left(1-\frac{\chi(2)}{2}\right)^{-1} L_2(1,\chi) = -\frac{\tau(\chi)}{q}\sum_{a=1}^{q}\overline{\chi}(a)\log_2(1-\zeta^a),$$

where $\zeta = \zeta_q$ and $\tau(\chi) = \sum_{a=1}^{q}\chi(a)\zeta^a$, a Gauss sum. Modify the right hand side by writing

$$\begin{aligned}\sum_{a=1}^{q}\overline{\chi}(a)\log_2(1-\zeta^a) &= \sum_{a=1}^{(q-1)/2}\overline{\chi}(2a)\left(\log_2(1-\zeta^{2a})+\log_2(1-\zeta^{q-2a})\right)\\ &= 2\overline{\chi}(2)\sum_{a=1}^{(q-1)/2}\overline{\chi}(a)\log_2(1-\zeta^{2a}).\end{aligned}$$

To evaluate the 2-adic logarithm, choose $d \geq 1$ so that

$$\alpha^{2^d} \equiv \alpha \pmod 2$$

for all integers $\alpha \in \mathbb{Q}_2(\zeta)$. Then any unit ϵ in the local field $\mathbb{Q}_2(\zeta)$ satisfies

$$\epsilon^{2^{d+1}-2} \equiv 1 \pmod{2^2},$$

and thus

$$\log_2\epsilon = \frac{1}{2^{d+1}-2}\log_2\left(1+(\epsilon^{2^{d+1}-2}-1)\right) \equiv -\tfrac{1}{2}\left(\epsilon^{2^{d+1}-2}-1\right) \pmod{2^2}.$$

We apply this to $\epsilon = 1-\zeta^2$. Since $(\zeta+1)^4 \equiv (\zeta-1)^4 \pmod{2^3}$, one easily computes

$$(\zeta^2-1)^{2^{d+1}-2} = \frac{((\zeta-1)(\zeta+1))^{2^{d+1}}}{(\zeta^2-1)^2} \equiv \left(\frac{\zeta-1}{\zeta+1}\right)^2 \pmod{2^3}.$$

This yields

$$\log_2(1-\zeta^2) \equiv \tfrac{1}{2}\left(1-\left(\frac{\zeta-1}{\zeta+1}\right)^2\right) \equiv \frac{2\zeta}{(\zeta+1)^2} \pmod{2^2}.$$

Set

$$\lambda(\zeta) = \frac{\zeta}{(\zeta+1)^2}.$$

Since $\lambda(\zeta)$ is a unit in the field $\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta+\zeta^{-1})$, we may write

$$\lambda(\zeta) = \sum_{j=1}^{q-1} b_j\zeta^j = \sum_{j=1}^{(q-1)/2} b_j(\zeta^j+\zeta^{-j})$$

with rational integers b_j. It follows that

$$\sum_{a=1}^{(q-1)/2} \overline{\chi}(a)\tfrac{1}{2}\log_2(1-\zeta^{2a}) \equiv \sum_{a=1}^{(q-1)/2} \overline{\chi}(a)\lambda(\zeta^a) \equiv \sum_{a=1}^{(q-1)/2} \overline{\chi}(a) \sum_{j=1}^{(q-1)/2} b_j(\zeta^{aj}+\zeta^{-aj})$$
$$\equiv \sum_{j=1}^{(q-1)/2} b_j\chi(j) \sum_{a=1}^{(q-1)/2} \overline{\chi}(aj)(\zeta^{aj}+\zeta^{-aj}) \pmod 2.$$

Here, the last sum over a equals $\tau(\overline{\chi})$.

On putting the results together we get

$$\tfrac{1}{4}\left(1-\frac{\chi(2)}{2}\right)^{-1} L_2(1,\chi) \equiv \overline{\chi}(2) \sum_{j=1}^{(q-1)/2} b_j\chi(j) \pmod 2.$$

It remains to compute b_j mod 2. We have

$$\lambda(\zeta) \equiv \frac{\zeta}{\zeta^2-1} \equiv \sum_{j=1}^{q-1} j\zeta^{2j+1} \pmod 2$$

because of the identity $q/(\zeta^2-1) = \sum_{j=1}^{q-1} j\zeta^{2j}$. Hence

$$\lambda(\zeta) \equiv \sum_{j=1}^{(q-1)/2} \left(2j\zeta^{4j+1} + (q-2j)\zeta^{2(q-2j)+1}\right) \equiv \sum_{j=1}^{(q-1)/2} \zeta^{-4j+1} \pmod 2$$

and so

$$\lambda(\zeta) = \lambda(\zeta^{-1}) \equiv \sum_{j=1}^{(q-1)/2} \zeta^{4j-1} \pmod 2.$$

For $q \equiv 1 \pmod 4$ this becomes, with the notation $w = \frac{q-1}{4}$,

$$\lambda(\zeta) \equiv \sum_{j=1}^{w} \left(\zeta^{4j-1} + \zeta^{4(2w+1-j)-1}\right) = \sum_{j=1}^{w}(\zeta^{4j-1}+\zeta^{q-4j+1}) = \sum_{\substack{j=1 \\ j\equiv 2 \text{ or } 3(4)}}^{q-1} \zeta^j \pmod 2.$$

Similarly, for $q \equiv 3 \pmod 4$ we obtain, with $w = \frac{q-3}{4}$,

$$\lambda(\zeta) \equiv 1 + \sum_{\substack{j=1 \\ j\neq w+1}}^{2w+1} \zeta^{4j-1} = 1 + \sum_{j=1}^{w}(\zeta^{4j-1}+\zeta^{q-4j+1}) = \sum_{\substack{j=1 \\ j\equiv 1 \text{ or } 2(4)}}^{q-1} \zeta^j \pmod 2,$$

since $1 = -\sum_{j=1}^{q-1}\zeta^j$. These results yield the congruences

$$b_j \equiv \begin{cases} 0 \pmod 2 \text{ for } j \equiv 0 \text{ or } q \pmod 4, \\ 1 \pmod 2 \text{ otherwise.} \end{cases}$$

Hence (4) is proved.

REMARK. We in fact proved somewhat more than asserted in the theorem: the formulas (3) and (4) show that

$$v_2\left(h_K \frac{R_2}{2^{n-1}}\right) \geq \begin{cases} 1 & \iff \quad v_2\left(\prod_{\chi\neq 1} S_\chi\right) \geq 1, \\ \sum_{\chi\neq 1} \min(1,\ v_2(S_\chi)), & \end{cases}$$

where $S_\chi = \sum_{j=1}^{(q-1)/2} a_j \chi(j)$.

3. Applications

As in §1, let $L = \mathbb{Q}(\zeta_q)$, the qth cyclotomic field.

The next result was first proved by Davis [D]. Subsequently, several other proofs have appeared, including one by the author [M2] (see that paper for further references). Note that the proof below, like that of Davis, avoids the use of the relative class number of L.

Corollary 1 (Davis). *If $q = 2l + 1$, where l is an odd prime, and if 2 is a primitive root* mod l, *then the class number of L^+ is odd.*

Proof. Assume that the class number of L^+ is even.

For $K = L^+$, the sums $\sum_j a_j \chi(j)$ appearing in the theorem are elements of the field $\mathbb{Q}(\zeta_l)$. The assumption about 2 mod l implies that the prime 2 is inert in $\mathbb{Q}(\zeta_l)$. Hence it follows from the theorem that

$$\sum_{j=1}^{l} a_j \chi(j) \equiv 0 \pmod 2$$

for every nonprincipal character χ of L^+. On multiplying by $\overline{\chi}(m)$, $1 \leq m \leq l$, and summing over χ we get

$$\sum_{j=1}^{l} a_j \sum_{\chi\neq 1} \chi(j)\overline{\chi}(m) \equiv 0 \pmod 2,$$

or

$$\sum_{j=1}^{l} a_j \sum_{\chi} \chi(j)\overline{\chi}(m) \equiv \sum_{j=1}^{l} a_j \pmod 2,$$

where χ runs through all even characters mod q. Consequently, by the orthogonality relations of characters,

$$l a_m \equiv \sum_{j=1}^{l} a_j \pmod 2 \qquad (m = 1, \ldots, l).$$

It follows that a_m mod 2 is constant for all $m = 1, \ldots, l$. By (2), this is not true. Hence the result. □

There exist further results about the parity of h_{L^+}, when q is of the form $q = 2l + 1$, l prime; see [M2]. It is conjectured that h_{L^+} be odd for *every* prime q of this kind. Recently, Shokrollahi [S] has computationally confirmed this in the range $q < 10^4$.

Corollary 2. *If $q = 4l + 1$, where l is an odd prime, and if 2 is a primitive root* mod l, *then the class numbers of L^+ and its subfields are odd.*

Proof. The proper subfields ($\neq \mathbb{Q}$) of L^+ are the quadratic field $\mathbb{Q}(\sqrt{q})$ and the field, say K, of degree l over $\mathbb{Q}$. It suffices to show that h_K is odd. Indeed, it is a classical result that the class number of $\mathbb{Q}(\sqrt{q})$ is odd (alternatively, one could use the fact that this class number divides h_K), and the relation $2 \nmid h_{L^+}$ is implied by $2 \nmid h_K$ (see [Wa, Theorem 10.4]).

Let r denote a primitive root mod q. Denote by X_K the group of characters of K. ¿From $2 \mid h_K$ it would follow, as in the proof of Corollary 1, that

$$\sum_{j=1}^{2l} a_j \sum_{\chi \in X_K} \chi(j)\overline{\chi}(m) \equiv \sum_{j=1}^{2l} a_j \pmod 2 \qquad (m = 1, \ldots, (q-1)/2).$$

By the orthogonality relations of characters, this congruence reduces to

$$l(a_m + a_{j(m)}) \equiv \sum_{j=1}^{2l} a_j \pmod 2,$$

where $j(m)$ is uniquely defined by

$$1 \leq j(m) \leq \tfrac{q-1}{2}, \qquad j(m) \equiv \pm m r^l \pmod q.$$

Therefore, $a_m + a_{j(m)} \equiv c \pmod 2$ for all $m = 1, \ldots, (q-1)/2$, where $c = 0$ or 1. Let $j_0 = j(1)$, so that $j(m) \equiv \pm m j_0 \pmod q$. Noting that $a_{q-j} = a_j$ we thus have

$$a_m + a_{i(m)} \equiv c \pmod 2 \qquad (m = 1, \ldots, (q-1)/2) \tag{5}$$

with $i(m)$ defined by the conditions $1 \leq i(m) \leq q-1$, $i(m) \equiv m j_0 \pmod q$.

By the theorem,

$$a_j = \begin{cases} 0 \text{ for } j \equiv 0 \text{ or } 1 \pmod 4, \\ 1 \text{ for } j \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

Hence the congruence (5) for $m = 1$ and $m = 2$ yields

$$a_{j_0} \equiv c, \qquad a_{2j_0} \equiv c - 1 \pmod 2.$$

This shows that $j_0 \equiv 1$ or $2 \pmod 4$.

Assume first that $j_0 \equiv 2 \pmod 4$; then $c = 1$. If $j_0 < q/3$, apply (5) for $m = 3$ to get $a_3 + a_{3j_0} \equiv 1 \pmod 2$. This is impossible. Similarly, if $q/3 < j_0 < q/2$, we find that the congruence $a_5 + a_{i(5)} \equiv 1 \pmod 2$ is absurd. Indeed, $i(5)$ equals either $5j_0 - q$ or $5j_0 - 2q$, so that anyway $a_{i(5)} = 0$.

If $j_0 \equiv 1 \pmod 4$, look at the congruence

$$\sum_{j=1}^{2l} a_j \sum_{\chi \in X_K \setminus \{1\}} \chi(j) \equiv 0 \pmod 2.$$

For $j \equiv 2$ or $3 \pmod 4$, the inner sum always equals -1 (because $j \neq 1$ and $j \neq j_0$). Hence the congruence reduces to $-l \equiv 0 \pmod 2$, a contradiction. □

4. Examples

In conclusion we illustrate the theorem by numerical examples. We let $q = 29$, 113, 163 and 197, which are the least four primes such that the relative class number of $L = \mathbb{Q}(\zeta_q)$ is even.

For $q = 29$ we have

$$S_\chi = \sum_{j=1}^{(q-1)/2} a_j\chi(j) \equiv \chi(2)+\chi(3)+\chi(6)+\chi(7)+\chi(10)+\chi(11)+\chi(14) \pmod 2.$$

The field $\mathbb{Q}(\zeta_{29})^+$ has class number 1. Note that $29 = 4\cdot 7+1$ but 2 is not a primitive root mod 7. If $K \subset \mathbb{Q}(\zeta_{29})^+$ is of degree 7, we may define χ by $\chi(j) = \zeta_7^{\mathrm{ind}(j)}$, where $\mathrm{ind}(j)$ is determined by the primitive root 2 mod 29. This yields $S_\chi \equiv \zeta_7 + \zeta_7^2 + \zeta_7^4 \pmod 2$. In $\mathbb{Q}(\zeta_7)$, the prime 2 splits into the product of a prime ideal and its complex conjugate. A short evaluation gives $S_\chi S_{\overline{\chi}} \equiv 0 \pmod 2$. Thus the result that h_K is odd cannot be deduced from our theorem. In fact, the remark in the end of §2 together with the fact that $v_2(h_K) = 0$ implies that $v_2(R_2/2^6) \geq 3$.

The case of the seven-degree subfield K of $\mathbb{Q}(\zeta_{113})^+$ turns out to be similar. This time one obtains, for χ defined analogously (with 3 as the primitive root mod 113),

$$S_\chi \equiv \zeta_7 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 \pmod 2.$$

Hence, $S_\chi S_{\overline{\chi}} \equiv 0 \pmod 2$.

Next, let K be the cubic subfield of $\mathbb{Q}(\zeta_{163})^+$. Then 2 is inert in $\mathbb{Q}(\zeta_3)$ and we have

$$S_\chi \equiv 1 + \zeta_3 + \zeta_3^2 \equiv 0 \pmod 2.$$

Thus, h_K has again the possibility of being even. In this case it is indeed known that $h_K = 4$.

Finally, take K the subfield of $\mathbb{Q}(\zeta_{197})^+$ of degree 7. Choose 2 as the primitive root mod 197. For χ defined as above one computes

$$S_\chi \equiv 1 + \zeta_7 + \zeta_7^2 \pmod 2.$$

Since the cyclotomic polynomial $\Phi_7(X)$ factors as

$$\Phi_7(X) \equiv (1+X+X^3)(1+X^2+X^3) \pmod 2,$$

we find that S_χ is prime to 2. It follows that $\prod_{\chi\neq 1} S_\chi \not\equiv 0 \pmod 2$ and so h_K is odd. This result was also obtained in [F].

A computation with the program package KASH gives that $h_K = 1$. Moreover, the computations by R. Schoof show with a very high probability that $h_{L^+} = 1$ in this case (see [Wa, p. 421]).

Ackowledgment

I am indebted to Radan Kučera for making critical comments on an early draft of this paper.

References

[D] D. Davis, *Computing the number of totally positive circular units which are squares*, J. Number Theory **10** (1978), no. 1, 1–9.

[F] K. Feng, *An elementary criterion on parity of class number of cyclic number field*, Sci. Sin., Ser. A **25** (1982), no. 10, 1032–1041.

[G] D. A. Garbanati, *Unit signatures, and even class numbers, and relative class numbers*, J. Reine Angew. Math. **274/275** (1975), 376–384.

[H] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952; Nachdruck: Springer-Verlag, Berlin–New York–Tokyo, 1985.

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

[M1] T. Metsänkylä, *An application of the p-adic class number formula*, Manuscr. Math. **93** (1997), no. 4, 481–498.

[M2] T. Metsänkylä, *Some divisibility results for the cyclotomic class number*, Tatra Mt. Math. Publ. **11** (1997), 59–68.

[S] M. A. Shokrollahi, *Relative class number of abelian* CM-*fields of prime conductor below* 10000, manuscript.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer-Verlag, New York–Berlin– Heidelberg, 1996.

Author's address: Department of Mathematics, University of Turku, FIN-20014 Turku, Finland

E-mail: taumets@utu.fi

Received: December 29, 1997