ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 19, Number 3, Summer 1989

ON THE PARITY OF THE CLASS NUMBER OF THE FIELD OF q-TH ROOTS OF UNITY

DENNIS R. ESTES

ABSTRACT. It is shown that the parity of the class number of the field $\mathbf{Q}(\zeta_q)$ of the q-th roots of unity over the rationals is odd whenever q and $p = (q-1)/2$ are primes and 2 is inert in the real subfield of p-th roots of unity over the rationals. As a consequence, the genus coincides with the spinor genus of the ring of integers in $\mathbf{Q}(\zeta_q)$ viewed as a lattice over the ring of integers in the real subfield.

Throughout this article, ζ_n denotes a primitive n-th root of unity, $k_n = \mathbf{Q}(\zeta_n)$ is the cyclotomic field of n-th roots of unity over the rationals $\mathbf{Q}$; k_n^+ denotes the real subfield of k_n; $\mathcal{O}_n^+$ and $\mathcal{O}_n^+$ are the rings of algebraic integers in k_n and k_n^+; $\mathbf{C}_n, \mathbf{C}_n^+$ are the class groups of the two rings; and their orders h_n, h_n^+ are the class numbers of the two fields. It is known that h_n^+ divides h_n with quotient h_n^-, the relative class number of k_n over k_n^+. Moreover, h_n is odd if and only if h_n^- is odd [**8**, Satz 45]. We prove in this note the following

THEOREM. *If q and $p = (q-1)/2$ are prime integers and 2 is inert in the real subfield of the cyclotomic field of p-th roots of unity over the rationals then the class number of the cyclotomic field of q-th roots of unity is odd.*

The study of the parity of the class number of number fields is motivated by the research of several authors. H. Hasse credits E. Kummer with the initial investigations on the parity of h_q, q a prime, based on a series of Kummer's papers between 1847 and 1870 (See [**8**] for a list of Kummer's articles and Satz 45 for extensions and refinements of Kummer's results to imaginary cyclic extensions of $\mathbf{Q}$). Kummer's work can be viewed as an analogue of Gauss' work on the 2 primary component of the class groups of binary quadratic forms for the binary quadratic lattice $\mathcal{O}_q$ over $\mathcal{O}_q^+$ (see Proposition below). In

Received by the editor on October 25, 1986.

[**16**], C.T.C. Wall shows that the topological classification of free group actions on S_n depends in part on the 2 primary component of $\mathbf{C}_q^+$. More recently, J. Hurrelbrink and M. Kolster [**11**] have shown that the 2 primary component of the Birch-Tate conjecture for cyclotomic fields is true in certain cases when the class number is odd (The Birch-Tate conjecture states that the order of the $\mathbf{K}$ group $\mathbf{K}_2(\mathcal{O}_E)$ is $w_2(E)\zeta_E(-1)$, where ζ_E is the zeta-function of E and $w_2(E)$ is twice the product $\prod p^{n(p)}$ with $n(p)$ the largest integer n such that E contains the maximal real subfield $k_{p^n}^+, p$ a prime. Mazur and Wiles [**12**] have shown that the odd parts are the same for abelian number fields). In particular, if $2^{[E:Q]}$ exactly divides $w_2(E)\zeta_E(-1), E = k_n^+$ and n a power of an odd prime, then the Birch-Tate conjecture holds if and only if h_n^- is odd.

Our investigation and that of D. Davis' work in [**5**] were the result of inquiries by O. Taussky. Taussky considered the question as to when a unimodular circulant C factors integrally as AA^t, t denoting transpose. She proved that if such a factorization exists then A can be selected as a circulant, and verified that such a factorization exists for 5×5 symmetric positive definite circulants by translating the question into a question as to whether certain totally positive units in the real subfield of cyclotomic extensions are norms (see [**15**] and [**13**]). The connection with cyclotomic extensions can be deduced from the observation that $n \times n$ integral circulants are matrix representations of the elements of the group ring $\mathbf{Z}[G]$, G a cyclic group of order n and, when n is prime, $\mathbf{Z}[G]$ is a subdirect sum of $\mathcal{O}_n$ and $\mathbf{Z}$. From this imbedding, one can conclude that if totally positive units in $\mathcal{O}_q^+$ are norms of units from $\mathcal{O}_q$then each symmetric unimodular positive definite circulant C factors as AA^t with A integral. Since the image of the norm map to k_q^+ on the units in $\mathcal{O}_q$ is the group of squares of units in $\mathcal{O}_q^+$ [**17**, Proposition 1.5], each totally positive unit in $\mathcal{O}_q^+$ is a norm from $\mathcal{O}_q$ if and only if each totally positive unit in $\mathcal{O}_q^+$ is a square. D. Davis, with the assistance of E.C. Dade, computed the index of the totally positive real units modulo squares for all primes $q \leq 5,000$, and these computations led Taussky to the conjecture that this index is 1 whenever both q and $p = (q-1)/2$ are primes. In [**5**], Davis verified Taussky's conjecture in the event that 2 is a generator modulo p. With n a prime power, the totally positive units in $\mathcal{O}_n^+$ are squares of units from $\mathcal{O}_n^+$ if and only if h_n^- is odd [**6**, Lemma 5 and Theorem 3], and we prefer to consider in this note the

following variant of Taussky's conjecture: h_q^- is odd whenever q and $p = (q-1)/2$ are primes. It follows from Davis' work and is also shown in [**11**] that this conjecture holds when 2 is a generator modulo p.

Additional work on the parity of class numbers of abelian fields not previously cited can be found in [**1, 2, 3, 9, 10**] and their references. Most of these articles extended Hasse's Satz 45, providing more detailed relations between the class number of real abelian extensions and various subgroups of the group of units within. One of the more definitive results is that of Cornell and Rosen [**3**] who show that if n has five or more prime divisors then 2 divides h_n^+. Finally, K.F. Hettling has shown that the 2-part of the Birch-Tate conjecture is valid for all totally real number fields whenever $2^{[E;Q]}$ is the exact 2-power dividing $w_2(E)\zeta_E(-1)$ and, in this event, the orders of certain class groups are odd [**9**].

Connection with quadratic lattices. The relative norm from k_q to k_q^+ induces a quadratic lattice structure on $\mathcal{O}_q$ over $\mathcal{O}_q^+$, and the relation of the parity of the class number of k_q with quadratic lattices is provided by the following proposition.

PROPOSITION. *A necessary and sufficient condition that h_q^- is odd is that the genus and the spinor genus of $\mathcal{O}_q$ coincide. Equivalently, the number of classes in the genus of $\mathcal{O}_q$ is odd.*

PROOF. The map cls $(I) \to$ cls (I/I^*), * denoting complex conjugation, defines an epimorphism from $\mathbf{C}_q$ to the group $\mathcal{G}$ of classes in the genus of $\mathcal{O}_q$ [**4**, Proposition 2.6]. Since q is a prime, the unique ramified prime in $\mathcal{O}_q$ is principal, hence the kernel of this map is the image of $\mathbf{C}_q^+$ in $\mathbf{C}_q$. Since $\mathbf{C}_q^+$ injects into $\mathbf{C}_q$ [**17**, Theorem 4.14], $\mathcal{G}$ has odd order if and only if h_q^- is odd. Since $\mathcal{G}$ has odd order if and only if $\mathcal{G}/\mathcal{G}^2$ is a trivial group and the number of spinor genera in the genus of $\mathcal{O}_q$ is the cardinality of $\mathcal{G}/\mathcal{G}^2$ [**4**, Theorem 2.10], the proposition follows. □

PROOF OF THE THEOREM. We start with the formula $h_q^- = 2q\prod[B(1,\chi)/2]$ which expresses the relative class number in terms of the generalized Bernoulli numbers $B(1,\chi) = [\Sigma a\chi(a)]/q$, χ an odd char-

acter for k_q and $a = 1, \ldots q-1$ [**17**, Theorem 4.17]. Among these characters is the quadratic character $\chi_2(a)$ defined by the Legendre symbol which is 1 or -1 according to whether a is or is not a square modulo q. Since the Gauss character theory implies that $\mathbf{Q}(\sqrt{-q})$ has the odd class number $-B(1,\chi_2), h_q^-$ is odd if and only if $h_0 = \prod[qB(1,\chi)/2]$ is odd, the product taken over the characters modulo q of order $2p$. Note that $qB(1,\chi)/2$ is an integer in k_p and, as p is prime, the galois group of this field acts transitively on the $qB(1,\chi)$. Thus, $qB(1,\chi)/2$ has norm h_0 from k_p to $\mathbf{Q}$. Consequently, h_q^- is odd if and only if $qB(1,\chi)/2$ is coprime to each of the primes in k_p dividing 2 for any choice of χ of order $2p$. It will be convenient in what follows to select a choice of χ. Since p is prime, 2 is either inert or splits completely in k_q^+. Since $q > 3$, the latter cannot occur, hence 2 is inert or the product of two prime ideals in k_q. Thus, either 2 or -2 is a primitive root modulo q. Let $b = 2$ or -2 depending on which generates the units modulo q and define χ by $\chi(a) = \zeta_{2p}^t$ when $a \equiv b^t \bmod q (b = 2$ if $q = 5)$. Then χ generates the group of characters modulo q, and its conjugates under the galois group of k_p over $\mathbf{Q}$ are the odd nonquadratic characters modulo q.

Since 2 is inert in $k_q^+, qB(1,\chi)/2$ is coprime to the dyadic primes in k_p if and only if its norm $\delta = qB(1,\chi)qB(1,\chi^*)/4$ to k_q^+ is coprime to 2, $*$ denoting complex conjugation. Thus, h_q^- is odd if 4δ is not in the ideal in k_q^+ generated by 8; i.e., the expression for 4δ as an integral linear combination of $1, \zeta_p, \ldots, \zeta_p^{p-2}$ has at least one coefficient not divisible by 8. Now

$$4\delta = \sum_{c=1}^{p} (d_c - d_{-c})\chi(c)$$

where $d_c = \sum ab, 1 \le a, b \le q-1$ and $ab^{-1} \equiv c \bmod q$.

Let $\chi_1 = \chi\chi_2$. Then χ_1 is an even character of order p and, as c varies from 1 to p, χ_1 runs through all the p-th roots of unity. The choice of c which gives the value ζ_p^{p-1} is determined by the equation $b^{p-1} = 2^{p-1} \equiv \chi_2(2)2^{-1} \equiv -\chi_2(2) p \bmod q$. Thus, $\chi_1(p) = \zeta_p^{p-1}$. The expression for 4δ in terms of a basis for k_p is therefore

$$4\delta = \sum[(d_c - d_{-c})\chi_2(c) - (d_p - d_{-p})\chi_2(p)]\chi_1(c), \quad 1 \le c \le p-1,$$

and 4δ is not divisible by 8 if

$$D_c = (d_c - d_{-c})\chi_2(c) \not\equiv (d_p - d_{-p})\chi_2(p) \bmod 8$$

for some c between 1 and $p-1$. Now

$$d_c = \sum_{a=1}^{q-1}(ca-[ca/q]q)a = \sum_{a=1}^{q-1} q^2((ca/q))((a/q))+qa/2 = q^2 s(c,q)+pq^2$$

where $((x)) = x-[x]-1/2$ or 0 according to whether x is or is not an integer, $[x]$ the greatest integer not exceeding x and $s(c,q)$ the Dedekind sum

$$s(c,q) = \sum_{a=1}^{q-1}((ca/q))((a/q)) = \sum_{a=1}^{q-1}((ca/q))a/q \quad \text{(see [14, pp. 1,8])}.$$

Therefore, $D_c = q^2(s(c,q) - s(-c,q))\chi_2(c)$.

We will need the following properties of Dedekind sums ([**14**, pp. 1, 4-5, 8, 26-27, 70]):

(1) $s(h+kt,k) = s(h,k)$ for t an integer,

(2) $s(-h,k) = -s(h,k)$,

(3) $12hks(h,k) + 12hks(k,h) = -3hk + h^2 + k^2 + 1$,

(4) $12hks(h,k) = (k-1)(k-h^2-1)$ if $k \equiv 1 \bmod h$,

(5) $12hks(h,k) = (k-2)(k-(h^2+1)/2)$ if $k \equiv 2 \bmod h$,

(6) $12hks(h,k) = k^2 + (h^2-6h+2)k + h^2 + 1$ if $k \equiv -1 \bmod h$,

(7) $2kds(h,k)$ is an integer, d the greatest common divisor of 3 and k, and

(8) $s(1,k) = -1/4 + 1/6k + k/12$.

Thus, by (2), $D_c = 2q^2 s(c,q)\chi_2(c)$, and, in view of (7), we have only to exhibit a c between 1 and $p-1$ for which $2qs(c,q)\chi_2(c) \not\equiv 2qs(p,q)\chi_2(p) \bmod 8$.

Case 1. $p \equiv 3 \bmod 8$. Then $q \equiv 7 \bmod 8$, and $\chi_2(p) = \chi_2(-2) = -1$. Since $q \equiv 1 \bmod p$, (4) implies that $2qs(p,q)\chi_2(p) = -p(2-p)/3 \equiv 1 \bmod 8$. However, $2qs(1,q)\chi_2(1) = p(2p-1)/3 \equiv 5 \bmod 8$.

Case 2. $p \equiv 5 \bmod 8$. Then $q \equiv 3 \bmod 8$ and $\chi_2(p) = \chi(-2) = 1$. Therefore $2qs(p,q)\chi_2(p) = p(2-p)/3 \equiv 3 \bmod 8$, while $2qs(1,q)\chi_2(1) = p(2p-1)/3 \equiv 7 \bmod 8$.

We should remark that when 2 is inert in k_p^+, the condition that $p \equiv 3$ or 5 mod 8 is equivalent to 2 being a generator for the units modulo

p. Thus, the argument given in the above two cases provides another proof of a result of D. Davis in [**5**].

Case 3. $p \equiv 7 \bmod 8$. Then $q \equiv -1 \bmod 16$ and $2qs(p,q)\chi_2(p) \equiv 1 \bmod 8$. Note that since q and $p = (q-1)/2$ are primes and $p \neq 3, q \equiv -1 \bmod 3$. Let a denote the largest positive integer such that 3^a divides $q+1$. Then $q \equiv -1 + 3^a e \bmod 3^{a+1}$ with $e = 1$ or -1.

Case 3.1. $e = 1$. Apply (3) and then (1) to obtain

$$\begin{aligned} s(3^{a+1}, q) &= -s(q, 3^{a+1}) - \frac{1}{4} + \frac{q^2 + 3^{2a+2} + 1}{12q3^{a+1}} \\ &= -s(-1 + 3^a e, 3^{a+1}) - \frac{1}{4} + \frac{q^2 + 3^{2a+2} + 1}{12q3^{a+1}}. \end{aligned}$$

Set $e = 1$ and apply (3) again to obtain

$$s(3^{a+1}, q) = s(3^{a+1}, -1+3^a) - \frac{3^{2a+2} + (-1+3^a)^2 + 1}{12(-1+3^a)3^{a+1}} + \frac{q^2 + 3^{2a+1} + 1}{12q3^{a+1}}.$$

Since $3^{a+1} \equiv 3 \bmod (-1+3^a)$, (1) implies

$$s(3^{a+1}, q) = s(3, -1+3^a) - \frac{3^{2a+2} + (-1+3^a)^2 + 1}{12(-1+3^a)3^{a+1}} + \frac{q^2 + 3^{2a+1} + 1}{12q3^{a+1}}.$$

Since $-1 + 3^a \equiv -1 \bmod 3$, (6) gives

$$\begin{aligned} s(3^{a+1}, q) = &\frac{(-1+3^a)^2 - 7(-1+3^a) + 10}{12(-1+3^a)3} \\ &- \frac{3^{2a+2} + (-1+3^a)^2 + 1}{12(-1+3^a)3^{a+1}} + \frac{q^2 + 3^{2a+2} + 1}{12q3^{a+1}} \end{aligned}$$

which, upon simplification, is

$$s(3^{a+1}, q) = \frac{q(3^{2a} - 18 \cdot 3^a + 2) + q^2 + 3^{2a+2} + 1}{12q3^{a+1}},$$

and since $q \equiv -1 \bmod 16$,

$$4qs(3^{a+1}, q) \equiv \frac{8 \cdot 3^{2a} + 2 \cdot 3^{a+2}}{3^{a+2}} \bmod 16.$$

Therefore, $2qs(3^{a+1}, q) \equiv 5 \bmod 8$. Since $q \equiv -1 \bmod 3$, quadratic reciprocity implies that $\chi_2(3^{a+1}) = 1$. Thus, $2qs(3^{a+1}, q)\chi_2(3^{a+1}) \neq 2ps(p, q)\chi_2(p) \bmod 8$.

Case 3.2. The argument is similar to the previous case. First apply (3) then (1) to express $s(3^{a+1}, q)$ in terms of $s(-1 - 3^a, 3^{a+1})$. Next use (2), then (3), the property that $3^{a+1} \equiv -3 \bmod (1 + 3^a)$, then (1), (2) and finally (4) to conclude that $2qs(3^{a+1}, q) \equiv 5 \bmod 8$. Thus, $2qs(3^{a+1}, q)\chi_2(3^{a+1}) \neq 2qs(p, q)\chi_2(p) \bmod 8$.

The proof is now concluded with the observation that when $p \equiv 1 \bmod 8$, 2 splits in $\mathbf{Q}(\sqrt{p})$ and is therefore not inert in k_q^+.

Acknowledgement. Conversations with R.M. Guralnick and O. Taussky were most helpful in the preparation of this article.

REFERENCES

1. N. Adachi, *On the class number of an absolutely cyclic number field of prime degree,* Proc. Japan Acad. **45** (1969), 647-650.

2. J.V. Armitage and A. Fröhlich, *Class numbers and unit signature,* Mathematika **14** (1967), 94-98.

3. G. Cornell and M.I. Rosen, *The l-rank of the real class group of cyclotomic fields,* Composito Math. **53** (1984), 133-141.

4. A.G. Earnest and Dennis R. Estes, *Class groups in the genus and spinor genus of binary quadratic lattices,* Proc. London Math. Soc. **40** (1980), 40-52.

5. Daniel Davis, *Computing the number of totally positive circular units which are squares,* J. Number Th. **10** (1978), 1-9.

6. D. Garbanati, *Unit signatures, and even class numbers, and relative class numbers,* J. Reine Angew. Math. **274** (1975), 376-384.

7. G. Gras, *Critère de parité du numbre de classes,* Bull. Soc. Math. France **103** (1975), 177-190.

8. H. Hasse, *Über Die Klassenzahl Abelscher Zahlkorper,* Akademie-Verlag, Berlin, 1952.

9. K.F. Hettling, *A note on the 2-part of $K_2(O_F)$ for totally real number fields F,* preprint.

10. I. Hughes and R. Mollin, *Totally positive units and squares,* Proc. AMS, **87** (1983), 613-616.

11. Jurgen Hurrelbrink and Manfred Kolster, *On the 2-primary part of the Birch-Tate conjecture for cyclotomic fields,* Contemporary Math., Proc AMS Boulder Conf. (1983).

12. B Mazur and A. Wiles, *Class fields of abelian extensions of* **Q**, Inv. Math. **76** (1974), 179-330.

13. M. Newman and O. Taussky, *On a generalization of the normal basis in abelian algebraic number fields,* Comm. Pure Appl. Math **9** (1956), 85-91.

14. H. Rademacher and Emil Grosswald, *Dedekind Sums, Carus Mathematical Monographs,* AMS, 1972.

15. O. Taussky, *Unimodular integral circulants,* Math Z. **63** (1955), 286-298.

16. C.T.C. Wall, *Classification of hermitian forms,* Ann Math. **1** (1976) 1-80.

17. L.C. Washington, *Introduction to Cyclotomic Fields,* Springer-Verlag, New York, 1982.

Department of Mathematics, University of Southern California, Los Angelos, CA 90089-1113