[4] H. Delange, *Sur des formules de Atle Selberg*, Acta Arith. 19 (1971), pp. 105–146.
[5] E. Fogels, *Zur Arithmetik quadratischer Zahlenkörper*, Wissenschaftliche Abhandlungen der Universität Riga, Kl. Math., Abt. 1 (1943), pp. 23–47.
[6] G. H. Hardy and M. Riesz, *The general theory of Dirichlet series*, Cambridge 1915.
[7] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Würzburg 1965.
[8] J. Kaczorowski, *On completely irreducible algebraic integers*, to appear in Coll. Math. Soc. János Bolyai 34.
[9] G. Kolesnik and E. G. Straus, *On the distribution of integers with a given number of prime factors*, Acta Arith. 37 (1980), pp. 181–199.
[10] Й. Кубилюс, *Вероятностные методы в теории чисел*, Вильнюс 1962.
[11] J. Kubilius, *On local theorems for additive number theoretic functions*, Abhandlungen aus Zahlentheorie und Analysis, edited by P. Turán, Berlin 1968.
[12] E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Leipzig 1918.
[13] — *Über Ideale und Primideale in Idealklassen*, Math. Z. 2 (1918), pp. 52–154.
[14] W. Narkiewicz, *On natural numbers having unique factorization in a quadratic number field*, Acta Arith. 12 (1966), pp. 1–22.
[15] — *Numbers with unique factorization in an algebraic number field*, ibid. 21 (1972), pp. 313–322.
[16] — *Elementary and analytic theory of algebraic numbers*, Warszawa 1974.
[17] — *Finite abelian groups and factorization problems*, Colloq. Math. 42 (1979), pp. 319–330.
[18] R. W. K. Odoni, *On a problem of Narkiewicz*, J. Reine Angew. Math. 288 (1976), pp. 160–167.
[19] J. P. Rémond, *Évaluations asymptotiques dans partitions certaines semi-groupes*, C. R. Acad. Sci. Paris 260 (1965), pp. 6250–6251; 262 (1966), pp. A271–A273.
[20] — *Étude asymptotique de certaines partitions dans certaines semi-groupes*, Ann. Sci. École Norm. Sup. 83 (1966), pp. 343–410.
[21] E. J. Scourfield, *On the divisibility of $\sigma_\nu(n)$*, Acta Arith. 10 (1964), pp. 245–286.
[22] A. Selberg, *Note on a paper by L. G. Sathe*, J. Indian Math. Soc. 18 (1954), pp. 83–87.
[23] J. Śliwa, *Factorizations of distinct lengths in algebraic number fields*, Acta Arith. 31 (1976), pp. 399–417.
[24] — *A note on factorization in algebraic number fields*, Bull. Acad. Polon. Sci., Sér. Sci. Math. Astronom. Phys. 24 (1976), pp. 313–314.

INSTITUTE OF MATHEMATICS OF THE ADAM MICKIEWICZ UNIVERSITY
Poznań, Poland

Received on 13. 1. 1982
and in revised form on 18. 6. 1982 (1285)

ACTA ARITHMETICA
XLIII (1983)

On the 2-primary part of a conjecture of Birch and Tate

by

JERZY URBANOWICZ (Warszawa)

1. Introduction. The conjecture of Birch and Tate states that

$$|K_2 O_F| = w_F \zeta_F(-1),$$

where O_F is the ring of integers of a totally real number field F, ζ_F is the Dedekind zeta function of F, K_2 is the functor of Milnor, and

$$w_F = 2 \prod_{l\,\text{prime}} l^{n(l)}.$$

Here $n(l)$ is the maximal integer $n \geqslant 0$ such that F contains the maximal real subfield of the cyclotomic field $Q(\zeta_{l^n})$.

The conjecture has recently been proved for abelian fields F by B. Mazur and A. Wiles [8], up to the 2-primary part. In the present paper we investigate the divisibility of $w_F\zeta_F(-1)$ by powers of 2 for real quadratic fields F. It enables us, in view of a paper by J. Browkin and A. Schinzel [3], to prove the 2-primary part of the conjecture for infinitely many fields.

I wish to express my sincere thanks to J. Browkin and A. Schinzel for many helpful suggestions and ideas used in this paper.

2. Notation. Let $F = Q(\sqrt{D})$, where D is a positive square-free integer, and let d be the discriminant of F. Denote by $\left(\frac{a}{b}\right)$ the Kronecker symbol, and let $P_2(x) = x^2 - x + 1/6$ be the second Bernoulli polynomial.

It is easy to see that $w_F = 24k$, where $k = D$ for $D = 2$ or 5, and $k = 1$ otherwise.

For a positive number x and a positive integer n let $A(x, n)$ be the number of positive integers $\leqslant x$ that are prime to n.

We know that

$$A\left(\frac{mn}{2}, n\right) = \frac{m}{2}\varphi(n), \tag{1}$$

where $m = 1$ or 2, and φ is Euler's totient function,

(2) $$A\left(\frac{mn}{4}, n\right) = \begin{cases} \frac{m}{4}\varphi(n) & \text{if } x > 0, \\ \frac{m}{4}\varphi(n) + (-1)^{(n-m)/2}2^{y-2} & \text{if } x = 0 \end{cases}$$

for $2 \nmid n$ and $m = 1$ or 3, where x (resp. y) is the number of prime factors of n of the form $4t+1$ (resp. $4t+3$),

(3) $$A\left(\frac{mn}{8}, n\right) - \frac{m}{8}\varphi(n) = R\left(\frac{mn}{8}, n\right),$$

$$R\left(\frac{mn}{8}, n\right) = \begin{cases} 0 & \text{if } x > 0 \text{ or } x = 0,\ y \geqslant 0,\ z > 0,\ u > 0, \\ r_1(-1)^{(n-1)(n-3)/8}2^{y+u-2} & \text{if } x = 0,\ y \geqslant 0,\ z = 0,\ u > 0, \\ r_2(-1)^{(n-1)/2}2^{y+z-3} & \text{if } x = 0,\ y \geqslant 0,\ z > 0,\ u = 0, \\ (2r_1+r_2)(-1)^{(n-1)/2}2^{y-3} & \text{if } x = 0,\ y > 0,\ z = 0,\ u = 0 \end{cases}$$

for $2 \nmid n$ and $m = 1, 3, 5$, or 7, where x, y, z, u are respectively the numbers of prime divisors of n of the form $8t+1$, $8t-1$, $8t+3$ and $8t-3$,

$$r_1 = (-1)^{(m-1)(m-3)/8}, \quad r_2 = (-1)^{(m-1)/2},$$

and

(4) $$A\left(\frac{(m+1)n}{r}, n\right) - A\left(\frac{mn}{r}, n\right) = \sum_{\substack{l \equiv -mn \bmod r \\ 1 \leqslant l \leqslant n, (l,n)=1}} 1,$$

for $2 \nmid n$, $0 \leqslant m \leqslant r-1$ and $r = 2, 4$, or 8 (see T. Nagell [9]).

3. Formulas for $w_F\zeta_F(-1)$. From the functional equation for ζ_F it follows that

$$\zeta_F(-1) = \frac{d\sqrt{d}}{4\pi^4}\zeta_F(2).$$

C. L. Siegel [11] proved that

(5) $$\zeta_F(2) = \frac{\pi^4}{6\sqrt{d}}\sum_{l=1}^{d}\left(\frac{d}{l}\right)P_2\left(\frac{l}{d}\right).$$

In view of $P_2(x) = P_2(1-x)$ and $\left(\frac{d}{l}\right) = \left(\frac{d}{d-l}\right)$ for $1 \leqslant l < d$, (5) can be transformed to the form

$$w_F\zeta_F(-1) = \begin{cases} 2kD\sum_{l=1}^{(D-1)/2}\left(\frac{D}{l}\right)P_2\left(\frac{l}{D}\right) & \text{if } D \equiv 1 \bmod 4, \\ 8kD\sum_{l=1}^{2D-1}\left(\frac{4D}{l}\right)P_2\left(\frac{l}{4D}\right) & \text{if } D \not\equiv 1 \bmod 4. \end{cases}$$

For $D \equiv 1 \bmod 4$ we evidently have

$$\sum_{l=1}^{D}\left(\frac{D}{l}\right)l = 0.$$

Hence in view of (5) we obtain

$$w_F\zeta_F(-1) = \frac{k}{D}\sum_{l=1}^{D}\left(\frac{D}{l}\right)l^2 \quad \text{for } D \equiv 1 \bmod 4,$$

and after transformations

(6) $$w_F\zeta_F(-1) = -\frac{4k}{4-\left(\frac{2}{D}\right)}\sum_{l=1}^{(D-1)/2}\left(\frac{D}{l}\right)l.$$

(Since $D \equiv 1 \bmod 4$, we have

$$\sum_{l=1}^{D-1}\left(\frac{D}{l}\right)l^2 = 2A - 2DB,$$

where

$$A = \sum_{l=1}^{(D-1)/2}\left(\frac{D}{l}\right)l^2 \quad \text{and} \quad B = \sum_{l=1}^{(D-1)/2}\left(\frac{D}{l}\right)l.$$

On the other hand,

$$\sum_{l=1}^{D-1}\left(\frac{D}{l}\right)l^2 = 4\left(\frac{2}{D}\right)A + 4\sum_{l=1}^{(D-1)/2}\left(\frac{2l-1}{D}\right)l^2 - 4\sum_{l=1}^{(D-1)/2}\left(\frac{2l-1}{D}\right)l,$$

$$\sum_{l=1}^{(D-1)/2}\left(\frac{2l-1}{D}\right)l^2 = \frac{1}{4}\left(\frac{2}{D}\right)\sum_{l=1}^{(D-1)/2}\left(\frac{l}{D}\right)(D+1-2l)^2$$
$$= -\left(\frac{2}{D}\right)(D+1)B + \left(\frac{2}{D}\right)A$$

and

$$-\sum_{l=1}^{(D-1)/2}\left(\frac{2l-1}{D}\right)l = \left(\frac{2}{D}\right)B.$$

Finally, for $D \equiv 1 \bmod 4$ we have

$$4\left(\frac{2}{D}\right)A - 2\left(\frac{2}{D}\right)DB = A - DB, \quad \text{i.e.} \quad \sum_{l=1}^{D-1}\left(\frac{D}{l}\right)l^2 = \frac{-4D}{4-\left(\frac{2}{D}\right)}B.)$$

For $D \not\equiv 1 \bmod 4$ we have

$$\left(\frac{D}{2l-1}\right) = -\left(\frac{D}{2(D-l+1)-1}\right) \quad \text{for } 1 \leqslant l \leqslant D$$

$$\text{and} \quad \sum_{l=1}^{2D-1}\left(\frac{4D}{l}\right) = 0.$$

Consequently,

$$w_F\zeta_F(-1) = 2k \sum_{1 \leqslant l \leqslant D/2}\left(\frac{D}{2l-1}\right)(D-2l+1) \quad \text{if } D \not\equiv 1 \bmod 4$$

and after changing indices

$$(7) \qquad w_F\zeta_F(-1) = \begin{cases} 4\displaystyle\sum_{l=1}^{(D-1)/2}\left(\frac{D}{D-2l}\right) l & \text{if } D \equiv 3 \bmod 4, \\ 2k\displaystyle\sum_{l=1}^{D/2}\left(\frac{D}{D-2l+1}\right)(2l-1) & \text{if } D \equiv 2 \bmod 4. \end{cases}$$

Next, let $h = h(Q(\sqrt{-D}))$ be the class number. It is known that or $D \equiv 3 \bmod 4$

$$h = -\frac{1}{D}\sum_{l=1}^{D-1}\left(\frac{l}{D}\right) l = \frac{1}{2-\left(\frac{2}{D}\right)}\sum_{l=1}^{(D-1)/2}\left(\frac{l}{D}\right),$$

for $D \equiv 1 \bmod 4$

$$h = 2\sum_{l=1}^{(D-1)/4}\left(\frac{l}{D}\right),$$

and for $D \equiv 2 \bmod 4$

$$h = \sum_{\substack{1 \leqslant l \leqslant D \\ 2 \nmid l}}(-1)^{(l-1)/2}\left(\frac{D}{l}\right) \quad \text{or} \quad h = 2\sum_{\substack{1 \leqslant l \leqslant D/2 \\ l \equiv 1 \bmod 4}}\left(\frac{D}{l}\right) \quad \text{for} \quad D > 2$$

(see [2]).

Consequently for $D \equiv 3 \bmod 4$ we have

$$\sum_{l=1}^{(D-1)/2}\left(\frac{D}{D-2l}\right) l = \left(\frac{2}{D}\right)\sum_{l=1}^{(D-1)/2}(-1)^l\left(\frac{l}{D}\right) l$$

$$= -\left(\frac{2}{D}\right)\sum_{l=1}^{(D-1)/2}\left(\frac{l}{D}\right) l + 2\left(\frac{2}{D}\right)\sum_{\substack{1 \leqslant l \leqslant (D-1)/2 \\ 2 \mid l}}\left(\frac{l}{D}\right) l$$

$$= -\frac{1}{2}Dh\left(\left(\frac{2}{D}\right)-1\right) + 4\sum_{l=1}^{(D-3)/4}\left(\frac{l}{D}\right) l.$$

Hence from (7) we infer that

$$(8) \quad w_F\zeta_F(-1) = -2Dh\left(\left(\frac{2}{D}\right)-1\right) + 16\sum_{l=1}^{(D-3)/4}\left(\frac{l}{D}\right) l \quad \text{for } D \equiv 3 \bmod 4.$$

Similarly, transforming (6), we obtain

$$(9) \quad w_F\zeta_F(-1) = -\frac{8k}{4-\left(\frac{2}{D}\right)}\left(\sum_{l=1}^{(D-1)/4}\left(\frac{D}{2l}\right) l + \sum_{l=1}^{(D-1)/4}\left(\frac{D}{2l-1}\right) l\right) - \frac{2k\left(\frac{2}{D}\right)}{4-\left(\frac{2}{D}\right)} h$$

since in view of

$$\sum_{l=1}^{(D-1)/2}\left(\frac{l}{D}\right) = 0 \quad \text{for } D \equiv 1 \bmod 4,$$

we have

$$\sum_{l=1}^{(D-1)/4}\left(\frac{2l-1}{D}\right) = -\left(\frac{2}{D}\right)\sum_{l=1}^{(D-1)/4}\left(\frac{l}{D}\right).$$

Finally, for $D = 2D'$, $D > 2$ we have

$$\sum_{\substack{1 \leqslant l \leqslant D \\ 2 \nmid l}}(-1)^{(l+1)/2}\left(\frac{D}{l}\right) l = \sum_{\substack{1 \leqslant l \leqslant D' \\ 2 \nmid l}}(-1)^{(l+1)/2}\left(\frac{D}{l}\right) l - \sum_{\substack{1 \leqslant l \leqslant D' \\ 2 \nmid l}}\left(\frac{D}{l}\right)(D-l)$$

$$= \sum_{\substack{1 \leqslant l \leqslant D' \\ 2 \nmid l}}\left[(-1)^{(l+1)/2}+1\right]\left(\frac{D}{l}\right) l - D\sum_{\substack{1 \leqslant l \leqslant D' \\ 2 \nmid l}}\left(\frac{D}{l}\right)$$

$$= 2\sum_{\substack{1 \leqslant l \leqslant D' \\ l \equiv 3 \bmod 4}}\left(\frac{D}{l}\right) l - D\sum_{\substack{1 \leqslant l \leqslant D' \\ l \equiv 3 \bmod 4}}\left(\frac{D}{l}\right) - \frac{1}{2}Dh$$

$$= 8\sum_{\substack{1 \leqslant l \leqslant D' \\ l \equiv 3 \bmod 4}}\left(\frac{D}{l}\right)\frac{l+1}{4} - (D+2)\sum_{\substack{1 \leqslant l \leqslant D' \\ l \equiv 3 \bmod 4}}\left(\frac{D}{l}\right) - \frac{1}{2}Dh$$

since

$$\left(\frac{D}{D-l}\right) = -(-1)^{(l+1)/2}\left(\frac{D}{l}\right) \qquad (2\nmid l)$$

for $D \equiv 2 \bmod 4$.

Hence from (7) we infer that

$$(10) \quad w_F\zeta_F(-1) = -16 \sum_{\substack{1\leqslant l\leqslant D'\\ l\equiv 3 \bmod 4}} \left(\frac{D}{l}\right)\frac{l+1}{4} + 2(D+2) \sum_{\substack{1\leqslant l\leqslant D'\\ l\equiv 3 \bmod 4}} \left(\frac{D}{l}\right) + Dh$$

for $D = 2D'$, $D > 2$.

4. $w_F\zeta_F(-1) \bmod 8$, $\bmod 16$, and $\bmod 32$.

THEOREM 1. *Let x (resp. y) be the number of prime factors of D, $D > 2$, of the form $4t+1$ (resp. $4t+3$). Then*

$$w_F\zeta_F(-1) \equiv \begin{cases} \varphi(D) \bmod 8 & \text{if } x > 0,\\ \varphi(D) + 2^y \bmod 8 & \text{if } x = 0. \end{cases}$$

Proof. If $D \equiv 1 \bmod 4$, then from (6) it follows that

$$w_F\zeta_F(-1) \equiv 4\sum_{l=1}^{(D-1)/2}\left(\frac{D}{l}\right) l \equiv 4\sum_{l=1}^{(D-1)/4}\left(\frac{2l-1}{D}\right)$$

$$\equiv 4\sum_{l=1}^{(D-1)/4}\left(\frac{l}{D}\right) \equiv 4A\left(\frac{D}{4}, D\right) \bmod 8.$$

If $D \equiv 3 \bmod 4$, then from (7) it follows that

$$w_F\zeta_F(-1) \equiv 4\sum_{l=1}^{(D-1)/2}\left(\frac{l}{D}\right) l \equiv 4\sum_{l=1}^{(D+1)/4}\left(\frac{2l-1}{D}\right)$$

$$\equiv 4\left(\sum_{l=1}^{(D-1)/2}\left(\frac{l}{D}\right) - \sum_{l=1}^{(D-3)/4}\left(\frac{l}{D}\right)\right)$$

$$\equiv 4\left(A\left(\frac{D}{2}, D\right) - A\left(\frac{D}{4}, D\right)\right) \bmod 8.$$

Finally, if $D = 2D'$, $D > 2$, then from (10) and (4) it follows that

$$w_F\zeta_F(-1) \equiv Dh \equiv 4D' \sum_{\substack{1\leqslant l\leqslant D'\\ l\equiv 1 \bmod 4}}\left(\frac{D}{l}\right) \equiv 4 \sum_{\substack{1\leqslant l\leqslant D'\\ l\equiv 1 \bmod 4}}\left(\frac{D}{l}\right)$$

$$\equiv 4\left(A\left(\frac{m+1}{4}D', D'\right) - A\left(\frac{m}{4}D', D'\right)\right) \bmod 8,$$

where $m \equiv -D' \bmod 4$, $m = 1$ or 3. Now, in view of (1) and (2) the result follows.

THEOREM 2. *If $D \equiv 3 \bmod 4$, then*

$$w_F\zeta_F(-1) \equiv -2Dh\left(\left(\frac{2}{D}\right) - 1\right) \bmod 16.$$

Proof. The result follows from (8).

THEOREM 3. *Let $D \equiv -1 \bmod 8$, and let x, y, z, u be respectively the numbers of prime divisors of D of the form $8t+1$, $8t-1$, $8t+3$ and $8t-3$. Then*

$$w_F\zeta_F(-1) - 2\varphi(D) \equiv \begin{cases} 0 & \text{if } x > 0 \text{ or } x = 0, y \geqslant 0, z > 0, u > 0,\\ 2^{y+u+2} & \text{if } x = 0, y \geqslant 0, z = 0, u > 0,\\ -2^{y+z+1} & \text{if } x = 0, y \geqslant 0, z > 0, u = 0,\\ 2^{y+1} & \text{if } x = 0, y > 0, z = 0, u = 0, \end{cases}$$

where all congruences are mod 32.

Proof. From (8) it follows that

$$w_F\zeta_F(-1) = 16\sum_{l=1}^{(D-3)/4}\left(\frac{l}{D}\right) l \equiv 16\sum_{l=1}^{(D+1)/8}\left(\frac{2l-1}{D}\right)$$

$$\equiv 16\left(A\left(\frac{D}{4}, D\right) - A\left(\frac{D}{8}, D\right)\right) \bmod 32.$$

Now it is sufficient to apply the result of (3).

THEOREM 4. *If $D \equiv 1 \bmod 4$, then*

$$w_F\zeta_F(-1) \equiv 2kh \bmod 16.$$

Proof. Since $D \equiv 1 \bmod 4$, we have

$$\sum_{l=1}^{(D-1)/4}\left(\frac{D}{2l}\right) l + \sum_{l=1}^{(D-1)/4}\left(\frac{D}{2l-1}\right) l \equiv \sum_{1\leqslant l\leqslant D/8}\left(\frac{D}{8l-4}\right) + \sum_{1\leqslant l\leqslant D/8}\left(\frac{D}{8l-6}\right)$$

$$\equiv \sum_{\substack{1\leqslant l\leqslant D\\ l\equiv 4 \bmod 8}}\left(\frac{D}{l}\right) - \sum_{\substack{1\leqslant l\leqslant D\\ l\equiv 2 \bmod 8}}\left(\frac{D}{l}\right)$$

$$\equiv \left(A\left(\frac{5}{8}D, D\right) - A\left(\frac{4}{8}D, D\right)\right) -$$

$$-\left(A\left(\frac{7}{8}D, D\right) - A\left(\frac{6}{8}D, D\right)\right)$$

$$\equiv 0 \bmod 2$$

(see (3) and (4)).

Now from (9) we obtain

$$w_F\zeta_F(-1) \equiv \frac{-2k\left(\frac{2}{D}\right)}{4-\left(\frac{2}{D}\right)} h \bmod 16.$$

Since in view of Theorem 1 $4\,|\,w_F\zeta_F(-1)$, the result follows.

THEOREM 5. *Let $D = 2D'$, $D > 2$, and let x (resp. y) be the number of prime factors of D of the form $4t+1$ (resp. $4t+3$). Then*

$$w_F\zeta_F(-1) \equiv \begin{cases} (D'+1)\varphi(D')+Dh \bmod 16 & \text{if } x > 0, \\ (D'+1)\varphi(D')-(D'+1)2^y+Dh \bmod 16 & \text{if } x = 0. \end{cases}$$

Proof. If $D = 2D'$, $D > 2$, then from (10) and (4) it follows that

$$w_F\zeta_F(-1) \equiv 2(D+2)\sum_{\substack{1\leqslant l\leqslant D' \\ l\equiv 3 \bmod 4}} \left(\frac{D}{l}\right) + Dh$$

$$\equiv 2(D+2)\left(A\left(\frac{m+1}{4}D', D'\right) - A\left(\frac{m}{4}D', D'\right)\right) + Dh \bmod 16,$$

where $m \equiv D' \bmod 4$, $m = 1$ or 3.

Now, in view of (1) and (2) the result follows.

5. Divisibility of $w_F\zeta_F(-1)$ by powers of 2.

THEOREM 6. *We have*

$$8\,|\,w_F\zeta_F(-1),$$

unless $D = 2$, p or $2p$, $p \equiv \pm 3 \bmod 8$ a prime, in which case $4\,\|\,w_F\zeta_F(-1)$.

Proof. If $D = 2$, then (7) implies that $w_F\zeta_F(-1) = 4$.

If $D = p$ or $2p$, where p is an odd prime, then

(i) for $p \equiv 1 \bmod 4$ we have in Theorem 1 $x = 1$, $y = 0$, hence

$$w_F\zeta_F(-1) \equiv p-1 \equiv \begin{cases} 0 \bmod 8 & \text{if } p \equiv 1 \bmod 8, \\ 4 \bmod 8 & \text{if } p \equiv -3 \bmod 8; \end{cases}$$

(ii) for $p \equiv 3 \bmod 4$ we have in Theorem 1 $x = 0$, $y = 1$, hence

$$w_F\zeta_F(-1) \equiv p+1 \equiv \begin{cases} 0 \bmod 8 & \text{if } p \equiv -1 \bmod 8, \\ 4 \bmod 8 & \text{if } p \equiv 3 \bmod 8. \end{cases}$$

If D has at least two odd prime factors, then from Theorem 1 it follows that $8\,|\,w_F\zeta_F(-1)$.

THEOREM 7. *If $D \equiv \pm 1 \bmod 8$, then*

$$16\,|\,w_F\zeta_F(-1),$$

unless $D = p = u^2-2w^2$ a prime, $u > 0$, $u \equiv 3 \bmod 4$, $w \equiv 0 \bmod 4$, or $D = pq$, $p \equiv q \equiv 3 \bmod 8$ primes, in which cases $8\,\|\,w_F\zeta_F(-1)$.

Proof. If $D \equiv -1 \bmod 8$, then $\left(\frac{2}{D}\right) = 1$, and from Theorem 2 it follows that $16\,|\,w_F\zeta_F(-1)$.

If $D \equiv 1 \bmod 8$, and D has $t \geqslant 3$ prime factors, then from Theorem 4 and $2^t\,|\,h$ (see [2]) it follows that

$$w_F\zeta_F(-1) \equiv 2h \equiv 0 \bmod 16.$$

If $D = p \equiv 1 \bmod 8$ is a prime, then $h = h(Q(\sqrt{-p})) \equiv 0 \bmod 8$ iff $p = u^2-2w^2$, $u > 0$, $u \equiv 1 \bmod 4$, $w \equiv 0 \bmod 4$; otherwise evidently $4\,\|\,h$ (see P. Barrucand and H. Cohn [1]). Thus Theorem 4 gives the result.

If $D = pq \equiv 1 \bmod 8$, p, q primes, then $h \equiv 0 \bmod 8$ unless $p \equiv q \equiv 3 \bmod 8$. In this last case we have $4\,\|\,h$ (see E. Brown [4] or A. Pizer [10]), and result follows from Theorem 4.

THEOREM 8. *If $D \equiv -1 \bmod 8$, then*

$$32\,|\,w_F\zeta_F(-1),$$

unless $D = p \equiv 7 \bmod 16$ a prime or $D = pq$, $p \equiv -q \equiv 3 \bmod 8$ primes, in which cases $16\,\|\,w_F\zeta_F(-1)$.

Proof. We adopt the notation of Theorem 3. Let $D = p \equiv -1 \bmod 8$ be a prime. Then $x = z = u = 0$, $y = 1$, and from Theorem 3 it follows that

$$w_F\zeta_F(-1) \equiv 2\varphi(D)+4 = 16\,\frac{p+1}{8} \bmod 32.$$

Thus $16\,\|\,w_F\zeta_F(-1)$ if $p \equiv 7 \bmod 16$, and $32\,|\,w_F\zeta_F(-1)$ if $p \equiv -1 \bmod 16$.

Let $D = pq \equiv -1 \bmod 8$ be the product of two prime factors. Then evidently $x = y = 1$, $z = u = 0$ or $x = y = 0$, $z = u = 1$. In both cases from Theorem 3 we obtain

$$w_F\zeta_F(-1) \equiv 2\varphi(D) = 2(p-1)(q-1) \bmod 32.$$

Now, if $x = y = 1$, then $16\,|\,(p-1)(q-1)$, and $w_F\zeta_F(-1) \equiv 0 \bmod 32$. If $z = u = 1$, then $8\,\|\,(p-1)(q-1)$, and $16\,\|\,w_F\zeta_F(-1)$. Finally, let D have at least three prime factors, i.e. $x+y+z+u \geqslant 3$. Since $2^{3x+y+z+2u}\,|\,\varphi(D)$, it follows that $32\,|\,2\varphi(D)$ with the one exception: $x = u = 0$, $y+z = 3$, when $16\,\|\,2\varphi(D)$. In this case from Theorem 3 we obtain

$$w_F\zeta_F(-1) \equiv 2\varphi(D)-2^{y+z+1} \equiv 0 \bmod 32.$$

In all other cases, from Theorem 3 easily follows that $w_F\zeta_F(-1) \equiv 0 \bmod 32$.

THEOREM 9. *If $D \equiv 3 \bmod 8$ has at least two prime factors, then*

$$16 \mid w_F \zeta_F(-1),$$

unless $D = pq$, p, q primes, $\left(\frac{p}{q}\right) = -1$, in which case $8 \| w_F \zeta_F(-1)$.

Proof. From Theorem 2 it follows that

$$w_F \zeta_F(-1) \equiv 4Dh \bmod 16.$$

Since $2^{t-1} \mid h$, where t is the number of prime factors of D, it is sufficient to consider the case $t = 2$, i.e. $D = pq$. From the result of H. Hasse [7] it follows that $4 \mid h$ if $\left(\frac{p}{q}\right) = 1$, and $2 \| h$ if $\left(\frac{p}{q}\right) = -1$. This proves the theorem.

THEOREM 10. *If $D \equiv -3 \bmod 8$ has at least two prime factors, then*

$$16 \mid w_F \zeta_F(-1),$$

unless $D = pq$, p, q primes, $\left(\frac{p}{q}\right) = -1$, $p \not\equiv -1 \bmod 8$, in which case $8 \| w_F \zeta_F(-1)$.

Proof. Since $2^t \mid h$, where t is the number of prime factors of D (see [2]), in view of Theorem 4 it is sufficient to consider the case $D = pq$.

From the results of E. Brown [4] or A. Pizer [10] it follows that:

If $p \equiv q \equiv 1 \bmod 4$, then $\left(\frac{p}{q}\right) = 1$ implies $8 \mid h$, and $\left(\frac{p}{q}\right) = -1$ implies $4 \| h$. If $p \equiv q \equiv 3 \bmod 4$, then $\left(\frac{p}{q}\right) = -1$, $p \equiv -1 \bmod 8$ implies $8 \mid h$, and $\left(\frac{p}{q}\right) = -1$, $p \equiv 3 \bmod 8$ implies $4 \| h$. Thus from Theorem 4 the result follows.

THEOREM 11. *If $D \equiv 2 \bmod 4$, $D = 2p$, $p \equiv \pm 1 \bmod 8$ a prime or D has at least two odd prime factors, then*

$$16 \mid w_F \zeta_F(-1),$$

unless $D = 2p$, $p \equiv \pm 1 \bmod 8$ a prime, $-2p = u^2 - 2w^2$, $w > 0$, $w \not\equiv 1, 3 \bmod 8$ if $p \equiv 1 \bmod 8$ and $w \not\equiv \pm 1 \bmod 8$ if $p \equiv -1 \bmod 8$, or $D = 2pq$, p, q primes, $p \equiv q \not\equiv 1 \bmod 8$, or $p \equiv -q \equiv 3 \bmod 8$, or $p \equiv 1 \bmod 8$, $q \equiv \pm 3 \bmod 8$ and $\left(\frac{p}{q}\right) = -1$, or $p \equiv -3 \bmod 8$, $q \equiv -1 \bmod 8$ and $\left(\frac{p}{q}\right) = -1$, or $p \equiv 3 \bmod 8$, $q \equiv -1 \bmod 8$ and $\left(\frac{p}{q}\right) = 1$, in which cases $8 \| w_F \zeta_F(-1)$.

Proof. Since $2^t \mid h$, where t is the number of odd prime factors of D (see [2]), in view of Theorem 5 it is sufficient to consider the cases $D = 2p$, $p \equiv \pm 1 \bmod 8$ a prime or $D = 2pq$, p, q primes.

From the result of H. Hasse [6] it follows that for $D = 2p$:

(i) $4 \mid h \Leftrightarrow p \equiv \pm 1 \bmod 8$,

(ii) $8 \mid h \Leftrightarrow -2p = u^2 - 2w^2$, $w > 0$, $w \equiv 1, 3 \bmod 8$, if $p \equiv 1 \bmod 8$ and $w \equiv \pm 1 \bmod 8$, if $p \equiv -1 \bmod 8$.

From the result of A. Pizer [10] it follows that for $D = 2pq$:

(iii) $h \equiv 4 \bmod 8$ if $p \equiv 3 \bmod 8$, $q \equiv -3 \bmod 8$; $p \equiv -3 \bmod 8$, $q \equiv -3 \bmod 8$; $p \equiv 1 \bmod 8$, $q \equiv 3$ or $-3 \bmod 8$ and $\left(\frac{p}{q}\right) = -1$; $q \equiv -1 \bmod 8$, $p \equiv 3$ or $-3 \bmod 8$ and $\left(\frac{p}{q}\right) = -1$; $h \equiv 0 \bmod 8$ otherwise.

Thus from Theorem 5 the result follows, since $w_F \zeta_F(-1) \equiv 2ph \bmod 16$ for $D = 2p$, p a prime and

$$8 \| w_F \zeta_F(-1) \Leftrightarrow \begin{cases} 4 \| h & \text{if } x > 0 \\ 8 \mid h & \text{if } x = 0 \end{cases} \quad \text{for } D = 2pq,\ p,\ q \text{ primes}.$$

6. The conjecture of Birch and Tate. We quote here some results on the Sylow p-subgroups $(K_2 O_F)_p$ of the group $K_2 O_F$ for a number field F.

THEOREM 12 (B. Mazur, A. Wiles [8]). *If p is an odd prime and F is an abelian totally real number field, then*

$$|(K_2 O_F)_p| \,\|\, w_F \zeta_F(-1).$$

THEOREM 13 (J. Browkin, A. Schinzel [3]). *If $F = Q(\sqrt{D})$ is a real quadratic field, $D \not\equiv \pm 1 \bmod 8$, $D > 2$, then $|(K_2 O_F)_2| \geqslant 8$, unless $D = p$ or $2p$, $p \equiv \pm 3 \bmod 8$ a prime, in which cases $(K_2 O_F)_2 = Z/2Z \oplus Z/2Z$.*

THEOREM 14 (J. Browkin, A. Schinzel [3]). *If $F = Q(\sqrt{D})$ is a real quadratic field, $D \equiv \pm 1 \bmod 8$, then $|(K_2 O_F)_2| \geqslant 16$, unless $D = p = u^2 - 2w^2$, a prime, $u > 0$, $u \equiv 3 \bmod 4$, $w \equiv 0 \bmod 4$, or $D = pq$, $p \equiv q \equiv 3 \bmod 8$ primes, in which cases $(K_2 O_F)_2 = Z/2Z \oplus Z/2Z \oplus Z/2Z$.*

THEOREM 15. *The conjecture of Birch and Tate:*

$$|K_2 O_F| = w_F |\zeta_F(-1)|$$

holds for $F = Q(\sqrt{D})$, where

$$D = 2,\ p \text{ or } 2p, \quad p \equiv \pm 3 \bmod 8 \text{ a prime},$$

or

$$D = p = u^2 - 2w^2 \text{ a prime},\ u > 0,\ u \equiv 3 \bmod 4,\ w \equiv 0 \bmod 4,$$

or

$$D = pq, \quad p \equiv q \equiv 3 \bmod 8 \text{ primes}.$$

Moreover,

$$w_F \zeta_F(-1) \equiv |K_2 O_F| \bmod 8 \quad \text{if } D \not\equiv \pm 1 \bmod 8,$$

and

$$w_F\zeta_F(-1) \equiv |K_2O_F| \bmod 16 \quad \text{if } D \equiv \pm 1 \bmod 8.$$

Proof. If $D = 2$, then $K_2O_F = Z/2Z \oplus Z/2Z$, i.e. $|K_2O_F| = 4$ (see [5]). The result follows immediately from Theorems 6, 7, 12, 13 and 14.

In view of Theorems 8, 9, 10, 11 one may expect that the following conjecture holds.

CONJECTURE. (i) If $F = Q(\sqrt{D})$ is a real quadratic field, $D \equiv -1 \bmod 8$, then $|(K_2O_F)_2| \geqslant 32$, unless $D = p \equiv 7 \bmod 16$ a prime or $D = pq$, $p \equiv -q \equiv 3 \bmod 8$ primes, in which cases $(K_2O_F)_2 = Z/2Z \oplus \oplus Z/8Z$.

(ii) If $F = Q(\sqrt{D})$ is a real quadratic field, $D \not\equiv \pm 1 \bmod 8$ has at least two prime factors, then $|(K_2O_F)_2| \geqslant 16$, unless $D = pq$, p, q primes, $\left(\frac{p}{q}\right) = -1$, and $pq \equiv 3 \bmod 8$ or $pq \equiv -3 \bmod 8$, $p \not\equiv -1 \bmod 8$, in which cases $(K_2O_F)_2 = Z/2Z \oplus Z/2Z \oplus Z/2Z$ or $Z/2Z \oplus Z/4Z$.

(iii) If $F = Q(\sqrt{D})$ is a real quadratic field, $D \equiv 2 \bmod 4$, $D = 2p$, $p \equiv \pm 1 \bmod 8$ a prime or D has at least two odd prime factors, then $|(K_2O_F)_2| \geqslant 16$, unless $D = 2p$, $p \equiv \pm 1 \bmod 8$ a prime, $-2p = u^2 - 2w^2$, $w > 0$, $w \not\equiv 1$, 3 mod 8 if $p \equiv 1 \bmod 8$ and $w \not\equiv \pm 1 \bmod 8$ if $p \equiv -1 \bmod 8$, or $D = 2pq$, p, q primes, $p \equiv q \not\equiv 1 \bmod 8$, or $p \equiv -q \equiv 3 \bmod 8$, or $p \equiv 1 \bmod 8$, $q \equiv \pm 3 \bmod 8$ and $\left(\frac{p}{q}\right) = -1$, or $p \equiv -3 \bmod 8$, $q \equiv -1 \bmod 8$ and $\left(\frac{p}{q}\right) = -1$, or $p \equiv 3 \bmod 8$, $q \equiv -1 \bmod 8$ and $\left(\frac{p}{q}\right) = 1$, in which cases $(K_2O_F)_2 = Z/2Z \oplus Z/2Z \oplus Z/2Z$ or $Z/2Z \oplus Z/4Z$.

References

[1] P. Barrucand and H. Cohn, *Note on primes of type x^2+32y^2, class number, and residuacity*, J. Reine Angew. Math. 238 (1969), pp. 67–70.

[2] Z. I. Borevič and I. R. Šafarevič, *Number theory*, Academic Press, New York 1966.

[3] J. Browkin and A. Schinzel, *On Sylow 2-subgroup of K_2O_F for quadratic number fields F*, J. Reine Angew. Math. 331 (1982), pp. 104–113.

[4] E. Brown, *Class number of complex quadratic fields*, J. Number Theory 6 (1974), pp. 185–191.

[5] H. M. Gebhardt, *Zur Berechnung des Funktors K_2 von einigen euklidischen Ringen*, Schriftreihe des Math. Inst. der Universität Münster, 2. Serie, Heft 13, 1977.

[6] H. Hasse, *Über die Klassenzahl des Körpers $Q(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$*, J. Number Theory 1 (1969), pp. 231–234.

[7] H. Hasse, *Über die Teilbarkeit durch 2^3 der Klassenzahl imaginärquadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, J. Reine Angew. Math. 241 (1970), pp. 1–6.

[8] B. Mazur and A. Wiles, to appear.

[9] T. Nagell, *Sur la distribution des nombres qui sont premiers avec un nombre entier donné*, Archiv for Math. og Naturvidenskab B. XXXVIII, Nr 2 (1923).

[10] A. Pizer, *On the 2-part of the class number of imaginary quadratic number fields*, J. Number Theory 8 (1976), pp. 184–192.

[11] C. L. Siegel, *Bernoullische Polynome und quadratische Zahlkörper*, Nachrichten der Akad. der Wissenschaften in Göttingen, Nr 2, 1968.

Received on 19. 1. 1982
and in revised form on 11. 3. 1982 (1290)