A further note on the class number of real quadratic fields

by

N. C. Ankeny (Cambridge, Mass.)

and

S. Chowla (Boulder, Colo.)

1. In his paper *On a Pellian equation conjecture* (Acta Arith. 6 (1960), pp. 137-144), Mordell proved (his theorem II):

If \( p \) is a prime \( \equiv 5 \pmod{8} \), the fundamental unit \( \frac{1}{2}(1 + \sqrt{p}) \) in the field \( \mathbb{Q}(\sqrt{p}) \) has \( u \equiv 0 \pmod{p} \) if and only if

\[
B_m \equiv 0 \pmod{p}
\]

where \( m = \frac{1}{2}(p-1) \)

and \( B_n \) is the \( n \)-th Bernoulli number defined by (2) below.

In this paper we extend Mordell’s theorem by proving that in his enunciation of the above theorem we can replace “\( p \) is a prime \( \equiv 5 \pmod{8} \)” by “\( p \) is a prime \( \equiv 1 \pmod{4} \)”.

We observe that Artin, Ankeny, Chowla (Annals of Math. 56 (1952), p. 479) conjectured that \( u \not\equiv 0 \pmod{p} \), but this is still unproved.

2. In the Annals paper cited above, Ankeny, Artin, Chowla proved that (we take our fundamental unit to be greater than 1),

\[
\frac{u}{\frac{1}{2}(p-1)} = B_m \pmod{p}
\]

where \( k \) is the class number of \( \mathbb{Q}(\sqrt{p}) \) and \( B_n \) is the \( n \)-th Bernoulli number defined by

\[
x \sum_{k=0}^{\infty} \frac{B_n x^n}{2^k (2k)!} = \frac{x^{\frac{p}{2}} + 1}{2 - \frac{p}{x} - 1}
\]

(1) was also proved independently by Kiselev. In a previous note (Acta Arith. 6 (1960), pp. 145-147) the present authors pointed out that, a fact brought to their notice by Professor Mordell, that the Annals paper contained a proof of (1) only in the case when \( p \) is a prime \( \equiv 3 \pmod{8} \).

At Professor Mordell’s suggestion we now supply the proof of (1), omitted by oversight in the Annals paper, also in the case \( p \equiv 1 \pmod{8} \).
3. For primes \( p = 1 \pmod{4} \) we have (theorem 3 of the Annals paper)

\[
4^{n-1}h = -\sum_{1 \leq \epsilon \leq p} \frac{1}{\epsilon p} \left( \frac{m}{p} \right) \left( \frac{p}{m} \right) \pmod{p},
\]

where \( g \) is a primitive root \( \pmod{p} \), \( \left( \frac{m}{p} \right) \) is Legendre's symbol, and \( \lfloor x \rfloor \) denotes the greatest integer in \( x \).

To the right hand side of (3) we apply Voronoi's theorem (J. V. Uspensky and M. A. Heaslet, Elementary number theory, New York and London 1939, p. 261)

\[
(a^{2^k} - 1)P_k = (-1)^{k-1} 2k \cdot a^{2^k-1}Q_k \sum_{b=1}^{N-1} g^{2^k-1} \left( \frac{S_b}{N} \right) \pmod{N}.
\]

Here \( N \) is an arbitrary positive integer, \( a \) is prime to \( N \), while \( P_k \) and \( Q_k \) are the numerator and denominator of the \( k \)-th Bernoulli number \( B_k \) (where \( B_k \) is our \( B_k \) except for sign \( k \) is even) in its lowest terms. We apply (4) to (3) with \( N = p \), \( a = g \), \( k = \frac{1}{2} (p-1) = m \). When \( p = 1 \pmod{8} \), it follows that

\[
\sum_{b=1}^{N-1} \frac{1}{\epsilon} \left( \frac{S_b}{N} \right) \left( \frac{g^b}{\epsilon} \right) = 4B_m \pmod{p},
\]

on using \( g^m = \left( \frac{S_m}{p} \right) \pmod{p} \), \( g^m = -1 \pmod{p} \).

From (3) and (5)

\[
\frac{u}{\epsilon} h = -C_m \pmod{p}.
\]

Since \( p = 1(p) \), we have \( B_m = -C_m \), and (6) becomes (1).

4. Combining the results: "\( h \) is prime to \( p \)" of our previous note (Acta Arith. 6 (1960), pp. 145-147) with the result of the present note, we see that for primes \( p = 1 \pmod{4} \) we have:

\[
u = 0 \pmod{p} \quad \text{if and only if} \quad B_m = 0 (p),
\]

where \( m = \frac{1}{2} (p-1) \); this is the extension of Mordell's result (Acta Arith. 6 (1960), pp. 137-144, theorem II) mentioned in paragraph 1 of this paper.

Note on Weyl's inequality

by

R. J. Birch and H. Davenport (Cambridge)

1. Weyl's inequality relates to exponential sums of the form

\[
S = \sum_{x=1}^{P} e(\alpha x^{d} + \nu_{d-1} x^{d-1} + \ldots),
\]

where \( \alpha, \nu_{d-1}, \ldots \) are real, and \( e(\theta) \) denotes \( e^{i\theta} \). Let \( h/q \) be any rational approximation to \( \alpha \) satisfying

\[
|\alpha - h/q| < q^{-3}, \quad (h, q) = 1.
\]

The form [see (4)] of Weyl's inequality with which we are concerned asserts that, if \( K = 2d - 1 \), then

\[
|S| < P^{1/2} + P^{1/3} q + P^{1/4} q^{1/2},
\]

for any \( \varepsilon > 0 \), where the implied constant depends only on \( d \) and \( \varepsilon \). In particular, if \( P < q < P^{d-1} \) (this corresponds roughly to \( \alpha \) being on the minor arcs in Waring's problem for \( d \)-th powers) we get

\[
|S| < P^{-1/12 + \varepsilon}.
\]

In a recent paper [1] Chowla and Davenport have shown that this form of Weyl's inequality with \( d = 3 \) can be extended without loss of precision to double sums of the form

\[
S_{d} = \sum_{x=1}^{p} \sum_{y=1}^{p} e(\alpha(x,y) + \Phi(x,y)) \quad (0 < Q < P)
\]

where \( f(x,y) \) is a fixed binary cubic form with integral coefficients and non-zero discriminant, and \( \Phi(x,y) \) is any real polynomial of degree 2 at most. In the present note we give an extension to a class of forms of degree \( d \) in \( n \) variables. We prove:

**Theorem.** Let \( f(x_1, \ldots, x_n) \) be any form of degree \( d \) in \( n \) variables with integral coefficients which is expressible as a sum of \( n \) \( d \)-th powers of linear

*Acta Arithmetica VII*