ACTA ARITHMETICA
VII (1962)

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 $\frac{1}{2}(t+u\sqrt{p})$ in the field $R(\sqrt{p})$ has $u \equiv 0 \pmod p$ if and only if

$$B_m \equiv 0 \pmod p \quad \textit{where} \quad m = \tfrac{1}{4}(p-1)$$

and B_n is the n-th Bernoulli number defined by (2) *bellow.*

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),

$$\frac{uh}{t} \equiv B_m \pmod p \qquad [m = \tfrac{1}{4}(p-1)], \tag{1}$$

where h is the class number of $R(\sqrt{p})$ and B_n is the n-th Bernoulli number defined by

$$\frac{x}{2}\cdot\frac{e^x+1}{e^x-1} = \sum_{0}^{\infty} \frac{B_n x^{2n}}{(2n)!} \tag{2}$$

(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 $\equiv 5 \pmod 8$. 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 $p \equiv 1 \pmod 4$ we have (theorem 3 of the Annals paper)

$$4\frac{u}{t}h \equiv -\sum_{1\leqslant n<p} \frac{1}{gn}\left(\frac{n}{p}\right)\left[\frac{gn}{p}\right] \pmod p, \tag{3}$$

where g is a primitive root $(\mathrm{mod}\, p)$, $\left(\frac{n}{p}\right)$ is Legendre's symbol, and $[x]$ 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)

$$(a^{2k}-1)P_k \equiv (-1)^{k-1}2k\cdot a^{2k-1}Q_k \sum_{S=1}^{N-1} S^{2k-1}\left[\frac{Sa}{N}\right] \pmod N. \tag{4}$$

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 C_k (where C_k is our B_k except for sign when k is even) in its lowest terms. We apply (4) to (3) with $N=p$, $a=g$, $k=\frac{1}{4}(p-1)=m$. When $p\equiv 1 \pmod 8$, it follows that

$$\sum_{S=1}^{p-1} \frac{1}{gS}\left(\frac{S}{p}\right)\left[\frac{gS}{p}\right] \equiv 4C_m \pmod p, \tag{5}$$

on using $S^{2m} \equiv \left(\frac{S}{p}\right) \pmod p$, $g^{2m} \equiv -1 \pmod p$.

From (3) and (5)

$$\frac{u}{t}h \equiv -C_m \pmod p. \tag{6}$$

Since $p\equiv 1 (8)$, we have $B_m = -C_m$, and (6) becomes (1).

4. Combining the result: "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* $p\equiv 1 \pmod 4$ *we have*:

$$u \equiv 0 \pmod p \quad \textit{if and only if} \quad B_m \equiv 0\ (p),$$

where $m=\frac{1}{4}(p-1)$; this is the extension of Mordell's result (Acta Arith. 6 (1960), pp. 137-144, theorem II) mentioned in paragraph 1 of this paper.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
UNIVERSITY OF NOTRE DAME, INDIANA
MARCH 8, 1961

Reçu par la Rédaction le 5. 6. 1961

ACTA ARITHMETICA
VII (1962)

Note on Weyl's inequality

by

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

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

$$S=\sum_{x=1}^{P} e(\alpha x^d+\alpha_{d-1}x^{d-1}+\ldots), \tag{1}$$

where $\alpha, \alpha_{d-1}, \ldots$ are real, and $e(\theta)$ denotes $e^{2\pi i\theta}$. Let h/q be any rational approximation to α satisfying

$$|\alpha-h/q|<q^{-2}, \qquad (h,q)=1. \tag{2}$$

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

$$|S|^K \ll P^{\varepsilon}(P^{K-1}+P^Kq^{-1}+P^{K-d}q) \tag{3}$$

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

$$|S| \ll P^{1-\frac{1}{K}+\varepsilon}. \tag{4}$$

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

$$S_2=\sum_{x=1}^{P}\sum_{y=1}^{Q} e[\alpha f(x,y)+\Phi(x,y)] \qquad (0<Q\leqslant P) \tag{5}$$

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*