We have so far proved that $x \neq 0$, and that $x \equiv 0 \pmod{p}$ if and only if $B_{(p-1)/4} \equiv 0 \pmod{p}$. Hence $x \not\equiv 0$, and so $u \not\equiv 0$ if $B_{(p-1)/4} \not\equiv 0$. If, however, $B_{(p-1)/4} \equiv 0$, then $x \equiv 0$, and we prove that now $u \equiv 0$. For since

$$\frac{y+x\sqrt{p}}{2} = \pm\left(\frac{t\pm u\sqrt{p}}{2}\right)^n \quad \text{for some positive integer } n,$$

it is obvious that if $u \not\equiv 0$, then $n \equiv 0$. But

$$\left|\frac{y+x\sqrt{p}}{2}\right| < 2^p, \quad \left|\frac{y-x\sqrt{p}}{2}\right| < 2^p,$$

and so

$$\left|\frac{t+u\sqrt{p}}{2}\right| < 2, \quad \left|\frac{t-u\sqrt{p}}{2}\right| < 2.$$

The cases so arising have already been disposed of.

This concludes the proof.

Note. I add a proof that the condition (13a) is sufficient. Let z be an integer in $K(\zeta)$ and let $(z^p-1)/p \equiv 0 \pmod{p}$. Since $(p) = (P)^{p-1}$, this congruence can have only the p obvious roots $z \equiv \zeta^t \pmod{p}$, $t = 0, 1, p-1$. Hence if (13a) is satisfied,

$$\prod_r (1+\zeta^r) / \prod_n (1+\zeta^n) \equiv \zeta^t \pmod{p}.$$

Take residues $\bmod P^2$. Since $\zeta = 1-P$,

$$\prod_r (2-Pr) / \prod_n (2-Pn) \equiv 1-tP \pmod{P^2},$$

and so

$$\sum \tfrac{1}{2}P(n-r) \equiv -tP \pmod{P^2}.$$

Since $\sum(n-r) \equiv 0 \pmod{p}$, $t \equiv 0 \pmod{p}$, and so $x \equiv 0 \pmod{p}$.

References

[1] N. C. Ankeny, E. Artin, S. Chowla, *The class-number of real quadratic number fields*, Annals of Mathematics 51 (1952), p. 479-493.

[2] Bachmann, *Nieder Zahlentheorie*, Erster Teil,

[3] L. Carlitz, *Note on the class number of real quadratic fields*, Proceedings of the American Mathematical Society 4 (1953), p. 535-537.

[4] J. Schumacher, Archiv Math. Phys. 3 (23) (1914-1915), p. 80-81.

COLORADO UNIVERSITY, BOULDER, U.S.A.
ST. JOHNS COLLEGE, CAMBRIDGE, ENGLAND

Reçu par la Rédaction le 23. 11. 1959

ACTA ARITHMETICA
VI (1960)

A note on the class number of real quadratic fields

by

N. C. Ankeny (Cambridge, Mass.) and S. Chowla (Boulder, Colo.)

1. Let $h = h(p)$ denote the class-number of the real quadratic field $R(\sqrt{p})$, where p is a prime $\equiv 1 \pmod 4$ and let $\varepsilon = t+u\sqrt{p}/2 > 1$ be its fundamental unit.

Ankeny, Artin, Chowla (also Kiselev, independently) have proved that (we gave details only for $p \equiv 5 \pmod 8$)

$$\frac{uh}{t} \equiv \frac{B_{p-1}}{4} \pmod{p},$$

where B_n is a Bernoulli number defined by

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

They also raised a question — still unsettled — can it happen that $u \equiv 0 \pmod{p}$ when $p \equiv 1 \pmod 4$? We had noticed at the time this paper was written that $h < p$, but we did not mention this. Hence, as Mordell has said in the preceding paper, $u \equiv 0 \pmod{p}$ if and only if $B_{p-1}/4 \equiv 0 \pmod{p}$, when $p \equiv 5 \pmod 8$. In the case when $p \equiv 5 \pmod 8$, Mordell has also given there a different proof of this. It seems now desirable to give the proof that $h < p$, especially as the work of other writers seems to indicate that this cannot be well known. Thus, Carlitz in Proc. Amer. Math. Soc. 4 (1953), p. 535-537, says (in our notation for the B's) "... $B_{p-1}/4 \equiv 0 \pmod{p}$ if and only if either $h \equiv 0$ or $u \equiv 0$". Selfridge, Nicol and Vandiver in their *Proof of Fermat's Last Theorem for all prime exponents less than 4002*, Proc. National Academy of Sciences, U. S. A. 41 (1955), p. 972, say "in particular the class number h of the field $K(\sqrt{l})$, where $l \equiv 1 \pmod 4$, is prime to l for the said l's". The "said" l's, here, are the primes < 4002.

2. We have

$$\varepsilon^{2h} = \frac{\prod_b \sin(b\pi/p)}{\prod_a \sin(a\pi/p)}$$

where a and b are typical numbers in the interval $0 < x < p$, such that $\left(\frac{a}{p}\right) = +1$ and $\left(\frac{b}{p}\right) = -1$.

Since $\prod_{m=1}^{p-1} \sin\frac{m\pi}{p} = \frac{p}{2^{p-1}}$, and $\prod_b \sin^2\frac{b\pi}{p} < 1$, we obtain:

$$\varepsilon^{2h} < \frac{2^{p-1}}{p} < 2^p.$$

Hence

$$h < \frac{p\log 2}{2\log\varepsilon} \leqslant \frac{p\log 2}{\log\left((1+\sqrt{5})/2\right)^2} < p.$$

Using $\varepsilon \geqslant \frac{1+\sqrt{p}}{2} \geqslant \frac{1+\sqrt{5}}{2}$. Hence $h \not\equiv 0 \pmod{p}$.

3. We observe also that for large p, we have from the classical expression of h as an infinite series (a proof of $h < p$ on these lines is also possible),

$$h\log\varepsilon = O(\sqrt{p}\log p)$$

whence

$$h = O(\sqrt{p}).$$

If we assume the "extended Riemann hypothesis", Littlewood has shown that

$$L(1) = \sum_1^\infty \frac{\chi(n)}{n} = O(\log\log k)$$

where $\chi(n)$ is a real primitive character $(\bmod k)$, $k > 3$. Hence, on this assumption,

$$h = O\left(\sqrt{p}\,\frac{\log\log p}{\log p}\right).$$

Postscript. Mordell observes that yet another proof of $h < p$ would follow from expressions for the class number of binary quadratic forms with a given discriminant, using $d(n) = O(n^\varepsilon)$, where $d(n)$ is the number of divisors of n and ε is an arbitrary positive number. In fact for a reduced form (a, b, c) with $b^2 - 4ac = p$, we have $ac < 0$, $0 < b < \sqrt{p}$ and so b has at most $[\sqrt{p}]$ values, and from $ac = \frac{1}{4}(p - b^2)$ we have p^ε values for a and c. Thus

$$h = O(p^{1/2+\varepsilon}).$$

MASSACHUSSETS INSTITUTE OF TECHNOLOGY
UNIVERSITY OF COLORADO

Reçu par la Rédaction le 15. 12. 1959