NOTE ON THE CLASS NUMBER OF REAL QUADRATIC FIELDS

L. CARLITZ

1. Let p be a prime $\equiv 1 \pmod 4$ and let $h(p)$ denote the class number of the real quadratic field $R(p^{1/2})$; let $\epsilon=(t+up^{1/2})/2$ denote the fundamental unit of the field ($\epsilon>1$). Ankeny, Artin, and Chowla [1] have stated the following results, as well as certain more general ones.

$$(1.1) \qquad 4uh/t \equiv -\sum_{r=1}^{(p-1)/4} \frac{1}{r}\left(\frac{r}{p}\right) \pmod p \qquad (p \equiv 5 \pmod 8));$$

$$(1.2) \qquad uh/t \equiv B_{(p-1)/2} \pmod p,$$

where B_m denotes a Bernoulli number in the even suffix notation;

$$(1.3) \qquad 2uh/t \equiv (A+B)/p \pmod p,$$

where A is the product of the quadratic residue of p between 0 and p, and B is the product of the nonresidues of p between 0 and p. Proofs of these results (except (1.3)) appear in [2].

In this note we wish to point out that if we assume (1.2), then (1.1) and (1.3) can be proved quite simply. We remark that for $p\equiv 1 \pmod 8$ the right member of (1.1) is congruent to $0 \pmod p$.

2. To show that (1.2) implies (1.1) we have

$$(2.1) \qquad \begin{aligned} S = \sum_{r=1}^{(p-1)/4} \frac{1}{r}\left(\frac{r}{p}\right) &\equiv \sum_{1}^{(p-1)/4} r^{(p-3)/2} \\ &\equiv \frac{B_{(p-1)/2}(3/4) - B_{(p-1)/2}}{(p-1)/2} \pmod p, \end{aligned}$$

where $B_m(x)$ is the Bernoulli polynomial of degree m. Since [4, p. 22]

$$B_{2m}(3/4) = B_{2m}(1/4) = (2^{1-4m} - 2^{-2m})B_{2m},$$

we see that (2.1) becomes

$$S \equiv -2(1-2^{(p-1)/2})B_{(p-1)/2} \equiv \begin{cases} 0 & p \equiv 1 \pmod 8, \\ -4B_{(p-1)/2} & p \equiv 5 \pmod 8. \end{cases}$$

This evidently proves (1.1).

The question is raised in [2, p. 480] whether u can be divisible by p. According to (1.2) this can only happen if $B_{(p-1)/2}\equiv 0 \pmod p$.

Received by the editors December 6, 1952.

More precisely $B_{(p-1)/2}\equiv 0$ if and only if either $h\equiv 0$ or $u\equiv 0$. In this connection it is of interest to note that for $p\equiv 3 \pmod 4$, $B_{(p+1)/2} \not\equiv 0 \pmod p$. This is a consequence of the well known formula ($p>3$)

$$\begin{aligned} H(p) &= \frac{1}{2-(2/p)} \sum_{r=1}^{(p-1)/2} \left(\frac{r}{p}\right) \\ &\equiv \frac{2}{2-(2/p)} \left\{B_{(p-1)/2}(1/2) - B_{(p+1)/2}\right\} \\ &\equiv -2B_{(p+1)/2} \pmod p; \end{aligned}$$

here $H(p)$ denotes the class number of the imaginary quadratic field $R((-p)^{1/2})$; clearly $H(p)<p$.

3. To prove (1.3) we follow Nielsen [3, Chapter 20]. Put

$$\prod_{s=1}^{(p-1)/2} a_s = -1 + p\Omega_p, \qquad \prod_{s=1}^{(p-1)/2} b_s = 1 - p\Omega_p', \tag{3.1}$$

where the a_s denote the quadratic residues in the interval 0, p, and the b_s denote the non residues. Thus, in the notation of (1.3), we have

$$A + B = p(\Omega_p - \Omega_p'). \tag{3.2}$$

Now if we put

$$r^{p-1} = 1 + pk(r) \qquad (p\nmid r),$$

then it follows from (3.1) that

$$\Omega_p \equiv \sum_{s=1}^{(p-1)/2} k(a_s), \qquad \Omega_p' \equiv \sum_{s=1}^{(p-1)/2} k(b_s) \pmod p.$$

Consequently

$$\Omega_p - \Omega_p' \equiv \frac{1}{p}\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)(r^{p-1}-1) \pmod p,$$

so that

$$\begin{aligned} p(\Omega_p - \Omega_p') &\equiv \sum_{1}^{p-1} \left(r^{3(p-1)/2} - r^{(p-1)/2}\right) \\ &\equiv \frac{B_{(3p-1)/2}(p) - B_{(3p-1)/2}}{(3p-1)/2} - \frac{B_{(p+1)/2}(p) - B_{(p+1)/2}}{(p+1)/2} \\ &\equiv p(B_{3(p-1)/2} - B_{(p-1)/2}) \pmod{p^2}, \end{aligned}$$

and

$$\Omega_p - \Omega_p' \equiv B_{3(p-1)/2} - B_{(p-1)/2} \pmod{p}. \tag{3.3}$$

Since by Kummer's congruence [3, Chapter 14]

$$\frac{B_{3(p-1)/2}}{3(p-1)/2} \equiv \frac{B_{(p-1)/2}}{(p-1)/2} \pmod{p},$$

it is clear that (3.3) reduces to

$$\Omega_p - \Omega_p' \equiv 2B_{(p-1)/2} \pmod{p}.$$

Hence (3.2) implies

$$\frac{1}{p}(A+B) \equiv 2B_{(p-1)/2},$$

which evidently proves (1.3).

References

1. N. C. Ankeny, E. Artin, and S. Chowla, *The class-number of real quadratic fields*, Proc. Nat. Acad. Sci. U.S.A. vol. 37 (1951) pp. 524–525.

2. ———, *The class-number of real quadratic fields*, Ann. of Math. (2) vol. 56 (1952) pp. 479–493.

3. N. Nielsen, *Traité élémentaire des nombres de Bernoulli*, Paris, 1923.

4. N. E. Nörlund, *Vorlesungen über Differenzenrechnung*, Berlin, 1924.

Duke University