Canad. Math. Bull.Vol. 36 (2), 1993 pp. 139–143

A SEQUENCE OF RESULTS ON CLASS NUMBER CONGRUENCES

ANTONE COSTA

ABSTRACT. Let $p \equiv 1 \bmod 8$ be a rational prime and let $h(-p)$ be the class number of $\mathbb{Q}(\sqrt{-p})$. In [1], Barrucand and Cohn show that $h(-p) \equiv 0 \bmod 8$ iff $p = x^2 + 32y^2$ for some $x, y \in \mathbb{Z}$. In this article, we generalize their result to a family of relative quadratic extensions K/F, where F_k is the maximum totally real subfield of $\mathbb{Q}(\zeta_{2^{k+2}})$, and $K = F_k(\sqrt{-p_k})$, p_k a power of a prime of F_k from a family of positive density.

1. **Introduction.** Let $p \equiv 1 \bmod 8$ be a positive prime integer, and for any integer n, let $h(n)$ be the narrow class number of $\mathbb{Q}(\sqrt{n})$. It is well known that $h(-p) \equiv 0 \bmod 4$ and $h(-2p) \equiv 0 \bmod 4$, and that the following statements are, in fact, true;

(A_0) $h(-p) \equiv 0 \bmod 8$ iff $(1 - i/p) = 1$ *i.e.* iff $1 - \sqrt{-1}$ is a square modulo p.

(B_0) $h(-2p) \equiv 0 \bmod 8$ iff $(\sqrt{-2}/p) = 1$.

(C_0) $h(-p) + h(-2p) \equiv \frac{p-1}{2} \bmod 8$.

(D_0) $h(-2p) \equiv 0 \bmod 8$ iff $p = a^2 + 2b^2$ with $a^2 \equiv 1 \bmod 16$

$h(-p) \equiv 0 \bmod 8$ iff $p = a^2 + 2b^2$ with $a^2 \equiv p \bmod 16$ (where $a, b \in \mathbb{Z}$).

We note that any two of the statements in C_0 and D_0 implies the third.

In more recent work, numerous authors, for instance Gras [3], Pioui [4], Stevenhagen [6] and Williams [7], have demonstrated that these results are actually part of a much broader family of congruences involving the various weighted sums of the class numbers of certain related quadratic number fields. In this article, we show that they can also be viewed as members of a sequence of results on the class numbers of more general relative quadratic extensions. More specifically, if $F_k = \mathbb{Q}(\zeta_{2^{k+2}})^+$, $k \geq 0$ (ζ_n being any primitive n-th root of unity, E^+ the maximal totally real subfield of a CM extension E), $\tau_k = 2 + 2\cos(\pi/2^{k+1})$ and $A(2)^k = \{p \in \mathbb{Z}, p \text{ prime} : p \equiv 1 \bmod 2^{k+3}$ with all the units of F_k being squares $\bmod p\}$, (note $A(2)^k \supseteq A(2)^{k+1}$), then we have the following;

PROPOSITION. *Let p_k be a totally positive representative of a principal ideal $\rho_k^{f_k}$ where f_k is the narrow class number of F_k, and ρ_k is a prime ideal dividing $p \in A(2)^k$. Then, if $h(\mu)$ is the class number of $F_k(\sqrt{\mu})$, we have $h(-p_k) \equiv 0 \bmod 4$ and $h(-\tau_k p_k) \equiv 0 \bmod 4$, and in fact*

(A_k) $h(-p_k) \equiv 0 \bmod 8$ *iff* $(1 - \zeta_{2^{k+2}}/p) = 1$.

(B_k) $h(-\tau_k p_k) \equiv 0 \bmod 8$ *iff* $(\sqrt{-\tau_k}/p) = 1$.

(C_k) $h(-p_k) + h(-\tau_k p_k) \equiv \frac{p-1}{2^{k+1}} \bmod 8$.

Partially supported by NSA/MSP grant #MDS90-H-1019.
Received by the editors October 3, 1991; revised February 5, 1992.
AMS subject classification: 11R11.

(D_k) $h(-\tau_k p_k) \equiv 0 \bmod 8$ *iff* $p_k^{c_k} = a^2 + \tau_k b^2$ $a, b \in O_{F_k}$, *with* $\mathcal{N}_{F_k/\mathbb{Q}}(a^2) \equiv 1 \bmod 2^{k+4}$
$h(-p_k) \equiv 0 \bmod 8$ *iff* $p_k^{c_k} = a^2 + \tau_k b^2$ *with* $\mathcal{N}_{F_k/\mathbb{Q}}(a^2) \equiv p \bmod 2^{k+4}$
where c_k *is the class number of* $F_k(\sqrt{-\tau_k})$ *which, like* f_k, *is odd. [2; 13.7]*

In Section 2 of this paper, we obtain (A_k) and (B_k), essentially using an extension of Redei's [5] machinery for determining the 8-rank of the classgroup of any quadratic number field. In Section 3 we make some elementary computations involving units to obtain (C_k), and use the reciprocity laws for Hilbert symbols to prove (D_k). Finally, in Section 4, we compute the Dirichlet density of the sets $A(2)^k$.

2. Let p be in $A(2)^k$, and let p_k be a totally positive representative of a principal ideal $\rho_k^{c_k}$, ρ_k a prime ideal dividing p. Moreover, let $E_k = F_k(\sqrt{p_k})$, and $L_k = F_k(\sqrt{-p_k})$. By class field theory we note that E_k/F_k is ramified only at ρ_k and that L_k/F_k is ramified at ρ_k, the infinite places of F_k, and τ_k—a uniformizer for the unique dyadic prime of F_k. (Since all of the units of F_k are squares modulo ρ_k, there exists a unique quadratic mod ρ_k ray class character on the ideals of F_k. If $F_k(\sqrt{\beta_k})$ is the corresponding quadratic extension, then β_k is totally positive, and is divisible by only one prime ideal, ρ_k. Thus we see that $p_k | \beta_k^{c_k}$, and that we may assume $\beta_k = \varepsilon p_k$, ε being some totally positive unit of F_k. But since F_k has odd narrow class number, any totally positive unit must be a square. Therefore $E_k = F_k(\sqrt{p_k}) = F_k(\sqrt{\beta_k})$. To obtain the conductor for L_k, we simply observe that it is one of the three quadratic subfields of $E_k R_k$, where $R_k = \mathbb{Q}(\zeta_{2^{k+2}})$.)

We now let F be any totally real number field with odd narrow class number, $E = F(\sqrt{D})$ a totally complex quadratic extension of F. In [2; 19.2,19.3], it is shown that the 2-torsion subgroup of $C(E)$, ${}_2C(E)$, is generated by the classes of those prime ideals of E dividing D. Moreover, every unramified quartic extension corresponds to a 'splitting' of these primes into disjoint sets D_1, D_2 for which D_2 is a square modulo all the primes in D_1, and D_1 is a square modulo those primes in D_2. In our case, we see immediately that 2-rank $C(L_k)$ = 4-rank $C(L_k)$ = 1. To determine the 8-rank, we follow Redei's constructions.

We begin by observing that the extension $F_k(\sqrt{p_k}, i){=}M_k \supseteq L_k$ is unramified of degree 2. Moreover, there exists an extension $Q_k \supseteq M_k \supseteq L_k$ such that Q_k/L_k is unramified of degree 4. This can actually be constructed by observing that if $\rho_k = \rho_k' \rho_k''$ in $\mathbb{Q}(\zeta_{2^{k+2}}) = F_k(i)$, the fact that the units of F_k, hence of $F_k(i) = R_k$, are all squares modulo p (*i.e.* R_k/F_k is a type I CM extension [C-H 13.4,13.6]), implies by class field theory the existence of quadratic extensions $H_k' = \mathbb{Q}(\zeta_{2^{k+2}}, \alpha_k')$, $H_k'' = \mathbb{Q}(\zeta_{2^{k+2}}, \alpha_k')$ of $\mathbb{Q}(\zeta_{2^{k+2}})$ ramified only at ρ_k' and ρ_k'' respectively. If we set $Q_k = M_k(\alpha_k') = M_k(\alpha_k'')$, then Q_k/L_k will be unramified of degree 4 and $\mathrm{Gal}(Q_k/F_k) \simeq D_8$.

If now we set $(\tau_k) = \tau^2 = 1$ in $\mathrm{C}(L_k)$, then $\tau \neq 1$, since τ_k, ρ_k are the only finite primes ramifying to L_k, and the prime above ρ_k must have odd order (since $(\sqrt{-p_k})$ is already principal), the class of τ must generate $C(L_k)_2$ by itself. Therefore 8-rank $C(L_k) = 1$ iff τ splits to Q_k, iff the unique dyadic prime of $\mathbb{Q}(\zeta_{2^{k+2}})$ splits to Q_k, iff $\chi_{\rho_k'}(1 - \zeta_{2^{k+2}}) = 1$, where $\chi_{\rho_k'}$ is the unique mod ρ_k' quadratic ray class character on the ideals of $\mathbb{Q}(\zeta_{2^{k+2}})$, iff

$1-\zeta_{2^{k+2}}$ is a square modulo p (*i.e.* $(1-\zeta_{2^{k+2}}/p)=1$). This gives us (A_k) simply as a consequence of Redei's machinery.

To obtain (B_k) we argue similarly, replacing $F_k(\sqrt{-p_k})$ with $F_k(\sqrt{-\tau_k p_k})$ for L_k, $F_k(\sqrt{p_k},\sqrt{-\tau_k})$ for M_k and $F_k(\sqrt{-\tau_k})$ for $\mathbb{Q}(\zeta_{2^{k+2}})$. We need only note that here $\sqrt{-\tau_k}$ serves as a uniformizer for the dyadic prime of $F_k(\sqrt{-\tau_k})$, and that the units here continue to be squares modulo p [C-H 13.4,13.6].

3. For $k\geq 0$, let $\varepsilon_k=\cot(\pi/2^{k+2})=\cot(\pi/2^{k+1})+\csc(\pi/2^{k+1})\in F_k$. We note

$$\varepsilon_k=\cot(\pi/2^{k+1})+\sqrt{1+\cot^2(\pi/2^{k+1})}$$

and let

$$\bar{\varepsilon}_k=\cot(\pi/2^{k+1})-\sqrt{1+\cot^2(\pi/2^{k+1})}$$

so that $\varepsilon_k\bar{\varepsilon}_k=-1$, $k\geq 1$ (for example, $\varepsilon_0=1$, $\varepsilon_1=1+\sqrt{2}$, $\varepsilon_2=1+\sqrt{2}+\sqrt{2(2+\sqrt{2})}$). Now recall that $\zeta_{2^{k+3}}=\cos(\pi/2^{k+2})+i\sin(\pi/2^{k+2})$, so that

$$\varepsilon_k+i=\csc(\pi/2^{k+2})\zeta_{2^{k+3}}$$

implying that if $p\equiv 1 \bmod 2^{k+3}$, ε_k+i is in the same square class modulo p as $\csc(\pi/2^{k+2})$ iff $p\equiv 1 \bmod 2^{k+4}$. Taking norms, we find that

$$\begin{aligned}
\mathcal{N}_{\mathbb{R}_1/\mathbb{Q}}(\varepsilon_1+i)&=\mathcal{N}_{\mathbb{R}_1/\mathbb{Q}}(1+\sqrt{2}+i)=2^3=2^2 2^1\\
\mathcal{N}_{\mathbb{R}_2/\mathbb{Q}}(\varepsilon_2+i)&=\mathcal{N}_{\mathbb{R}_1/\mathbb{Q}}\big((\varepsilon_2+i)(\bar{\varepsilon}_2+i)\big)\\
&=\mathcal{N}_{\mathbb{R}_1/\mathbb{Q}}(-2+2\varepsilon_1 i)\\
&=\mathcal{N}_{\mathbb{R}_1/\mathbb{Q}}(2i)\mathcal{N}_{\mathbb{R}_1/\mathbb{Q}}(\varepsilon_1+i)\\
&=2^4 2^2 2^1
\end{aligned}$$

and in general, by induction,

$$\begin{aligned}
\mathcal{N}_{\mathbb{R}_k/\mathbb{Q}}(\varepsilon_k+i)&=\mathcal{N}_{\mathbb{R}_{k-1}/\mathbb{Q}}\big((\varepsilon_k+i)(\bar{\varepsilon}_k+i)\big)\\
&=\mathcal{N}_{\mathbb{R}_{k-1}/\mathbb{Q}}(-2+2\varepsilon_{k-1}i)\\
&=\mathcal{N}_{\mathbb{R}_{k-1}/\mathbb{Q}}(2i)\mathcal{N}_{\mathbb{R}_{k-1}/\mathbb{Q}}(\varepsilon_{k-1}+i)\\
&=2^{2^k}\cdots 2^4 2^2 2^1
\end{aligned}$$

which in turn implies

$$\frac{\varepsilon_k+i}{1-\zeta_{2^{k+2}}}=(1-\zeta_{2^{k+2}})^{2+4+\cdots+2^k}\mu$$

where μ is a unit in $\mathbb{Q}(\zeta_{2^{k+2}})$.

But as $p\in A(2)^k$, all units of $\mathbb{Q}(\zeta_{2^{k+2}})$ are squares mod p, hence $1-\zeta_{2^{k+2}}$ and $\csc(\pi/2^{k+2})$ belong in the same square class. Moreover

$$\csc(\pi/2^{k+2})=\frac{2\cos(\pi/2^{k+2})}{\sin(\pi/2^{k+1})}=\csc(\pi/2^{k+1})\sqrt{2+2\cos(\pi/2^{k+1})}=\csc(\pi/2^{k+1})\sqrt{\tau_k}$$

essentially by half angle formula. But we claim that $\csc(\pi/2^{k+1})$ is itself a square mod p and as such, $\csc(\pi/2^{k+2})$, $\sqrt{\tau_k}$ and $\sqrt{-\tau_k}$ are all in the same square class. To justify this claim, we need only note the following sequence of identities. Let $\theta_k = -i\varepsilon_k$ and $\bar{\theta}_k = -i\bar{\varepsilon}_k$. As $\varepsilon_k\bar{\varepsilon}_k = -1$, $\theta_k\bar{\theta}_k = 1$. Therefore

$$\begin{aligned}(1+\bar{\theta}_k)^2\theta_k &= 2+\theta_k+\bar{\theta}_k\\ (1-i\bar{\varepsilon}_k)^2(-i\varepsilon_k) &= 2-2i\varepsilon_{k-1}\\ (1-i\bar{\varepsilon}_k)^2\varepsilon_k &= 2(\varepsilon_{k-1}+i)\\ \left(\frac{1-i\bar{\varepsilon}_k}{\sqrt{2}}\right)^2\varepsilon_k &= \varepsilon_{k-1}+i\end{aligned}$$

($k \geq 1$) implying that mod p, ε_k and $\varepsilon_{k-1}+i$, hence $\csc(\pi/2^{k+1})$ are all in the same square class. But again, $p \in A(2)^k$, and as such ε_k, a unit in $\mathbb{Q}(\zeta_{2^{k+2}})^+$ is a mod p square by assumption. Thus we have C_k.

Given this, to show D_k, we need only compute $(\sqrt{-\tau_k}/p) = (-\tau_k/p)_4$. To this end we note that if c_k is the narrow class number of $F_k(\sqrt{-\tau_k})$, then c_k is odd [2; 13.7] and we may write $p_k^{c_k} = a_k^2 + \tau_k b_k^2$ with $a_k, b_k \in O_{F_k}$. Now mod p_k, $a_k^2 \equiv -\tau_k b_k^2$, implying that $-\tau_k$ is a 4th power iff $a_k b_k$ is a square mod p_k *i.e.* iff $(a_k b_k, p_k)_{p_k} = 1$. By Hilbert reciprocity, we have

$$(a_k b_k, p_k)_{p_k} = \prod_{\omega \nmid p_k}(a_k b_k, p_k)_\omega = \prod_{\omega \nmid p_k}(a_k, p_k)_\omega \prod_{\omega \nmid p_k}(b_k, p_k)_\omega$$

We note that as p_k is totally positive, we may ignore infinite primes as for these $(x, p_k)_\omega = 1\ \forall x \in O_{F_k}$. Now if $b_k = \tau_k^{\beta_k} b_k'$, then

$$\prod_{\omega \nmid p_k}(b_k, p_k)_\omega = \prod_{\omega \nmid p_k\tau_k}(b_k', p_k)_\omega(\tau_k, p_k)_{\tau_k}^{\beta_k}$$

But $p \in A(2)^k$ implies that p splits to F_{k+1}, hence $(\tau_k, p_k)_{\tau_k} = (\tau_k, p_k)_{p_k} = 1$. Moreover, if $v|b_k$, v finite and nondyadic, then mod v, $p_k \equiv a_k^2$. Therefore $(b_k', p_k)_v = 1$ and $\prod_{\omega \nmid p_k}(b_k, p_k)_\omega = 1$

Finally, we note both $p_k, \tau_k | a_k$ and if $v|a_k$, then mod v, $p_k \equiv \tau_k b_k^2$, hence $(a_k, p_k)_v = (a_k, \tau_k)_v$. Thus we have

$$\begin{aligned}\prod_{\omega \nmid p_k}(a_k, p_k)_\omega = \prod_{\omega \nmid p_k\tau_k}(a_k, p_k)_\omega &= \prod_{\omega \nmid p_k\tau_k}(a_k, \tau_k)_\omega\\ &= \prod_{\omega \nmid \tau_k}(a_k, \tau_k)_\omega\\ &= (a_k, \tau_k)_{\tau_k}\end{aligned}$$

since τ_k is totally positive. But $(a_k, \tau_k)_{\tau_k} = 1$ iff $\mathcal{N}_{F_k/\mathbb{Q}}(a_k)^2 \equiv 1 \bmod 2^{k+4}$, the Hilbert symbol $(\alpha, \tau_k)_{\tau_k}$ corresponding to the extension F_{k+1}/F_k. Thus, by (C_k), we have *both* parts of (D_k).

https://doi.org/10.4153/CMB-1993-020-x Published online by Cambridge University Press

4. In this section, we compute the density in the set of primes of $A(2)^k$. We begin by noting [C-H 13.7] that as F_k has units with independent signs, $U_k^+ = U_k^2$, where U_k, U_k^+ are, respectively, the units and totally positive units of F_k. As such, there exists a unit $\varepsilon^{(1)}$, which is negative at precisely one embedding of F_k. Thus by considering the various conjugates of $\varepsilon^{(1)}$, $\{\varepsilon^{(1)}, \dots, \varepsilon^{(k)}\}$, we obtain a complete system of representatives for U_k / U_k^2.

Therefore, $p \in A(2)^k$ iff $p \equiv 1 \bmod 2^{k+3}$ and p splits to $E_k = F_k(\sqrt{\varepsilon^{(1)}}, \dots, \sqrt{\varepsilon^{(k)}})$, that is, iff p splits to $E_k F_{k+1}$. As $E_k \cap F_{k+1} = F_k$ (by checking ramification at the infinite primes), we have $[E_k F_{k+1} : \mathbb{Q}]=2^{k+2^k+1} = d_k$ and that the Dirichlet density, $\delta(A(2)^k) = 1/d_k$.

In conclusion, the author wishes to thank Drs. P. E. Conner, J. Hurrelbrink and P. Stevenhagen, for their support and numerous helpful conversations.

References

1. P. Barrucand, H. Cohn *Primes of type $x^2 + 32y^2$, class numbers and residuacity*, J. Reine Angew. Math **238**(1969) 67–70.
2. P. E. Conner, J. Hurrelbrink, *Class Number Parity*, World Scientific Publ., (1988).
3. G. Gras, *Relations congruentielles entre nombres de classes de corps quadratiques*, Acta Arith. **52**(1989), 147–162.
4. R. Pioui, *Mesures de Haar p-adiques et interprétation arithmétique de $\frac{1}{2}L_2(\chi, s) - \frac{1}{2}L_2(\chi, t)$, $s, t \in \mathbb{Q}_2$ (χ quadratique)*, Thèse, Université de Franche-Comté, Besançon, (1990).
5. L. Redei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkorper*, J. Reine Angew. Math. **180**(1939), 1–43.
6. P. Stevenhagen, *Class groups and governing fields*, Thesis, University of California at Berkeley, 1988.
7. K. S. Williams, *On the class number of $\mathbb{Q}(\sqrt{-p})$ modulo 16, for $p \equiv 1 \bmod 8$ a prime*, Acta Arith **39**(1981), 381–398.

Department of Mathematics
The American University
4400 Massachusetts Avenue NW
Washington D.C. 20016
U.S.A.

https://doi.org/10.4153/CMB-1993-020-x Published online by Cambridge University Press