51. A Note on a Recent Paper on Iwasawa on the Capitulation Problem

By R. W. K. ODONI
Department of Mathematics, University of Exeter

(Communicated by Shokichi IYANAGA, M. J. A., June 13, 1989)

Introduction. Let $n \geq 1$ and let $p_1, \cdots, p_n$ be distinct primes in $N=\{z \in \boldsymbol{Z}; z>0\}$, each congruent to $1 (\bmod 4)$. Let K_n be the quadratic field $\boldsymbol{Q}(\sqrt{p_1 \cdots p_n})$, and let $\mathcal{O}_n$ be the ring of algebraic integers in K_n. It is a famous unsolved problem to give simple conditions on $p_1, \cdots, p_n$ which are necessary and sufficient to ensure that $N_n(\varepsilon)=+1$ for every unit ε of $\mathcal{O}_n$. (Here N_n is the $K_n/\boldsymbol{Q}$-norm.) Legendre in 1785 showed [3] that if $n=1$ there is always an ε in $\mathcal{O}_1$ with $N_1(\varepsilon)=-1$. However, for $n>1$, the present state of knowledge is still unsatisfactory. The aim of this note is to give a simple proof of

Theorem 1. *Let $n \geq 2$ be fixed, and let $p_1, \cdots, p_{n-1}$ be such that the Legendre symbol (p_j/p_k) equals $+1$ whenever $j \neq k$ and $j, k \leq n-1$. Then there are infinitely many choices of p_n such that $N_n(\varepsilon)=+1$ for every unit ε of $\mathcal{O}_n$.*

Theorem 1 answers a generalisation of a question raised by K. Iwasawa in a recent paper [2] on the capitulation problem. Theorem 1 is not a new result; the case $n=2$ occurs in work of A. Scholz [6], while the general case is implicit in work of L. Rédei [5], although his proof is very complicated. We should perhaps remark that the long series of papers Rédei over the years 1932–53 still contains almost all the significant known results on the signs of the $N_n(\varepsilon)$ (see [5] and the bibliography (and Chapter III) of [4]). The reader is warned that there is a serious error in the "analytical" part of [5], which the author hopes to correct in a forthcoming paper. Our proof of Theorem 1 is quite simple, relying only on standard properties of biquadratic residues in $\boldsymbol{Z}[i]$ $(i=\sqrt{-1})$. For these we refer the reader to the excellent book of K. Ireland and M. Rosen [1]; all results which we state without proof are contained in the text and exercises of Chapter 9 of their book.

1. *A necessary condition for $N_n(\varepsilon)=-1$.* We retain the notation of the introduction. A number λ in $R=\boldsymbol{Z}[i]$ is called *primary* if $\lambda \equiv 1 (\bmod (1+i)^3)$. If $p \in N$ is prime and $p \equiv 1 \ (\bmod 4)$ we have $p=\pi\bar{\pi}$, where π is primary and irreducible, while $\bar{\pi}$ is the complex conjugate of π. If also σ is primary irreducible and $p=\sigma\bar{\sigma}$, then $\sigma=\pi$ or $\bar{\pi}$.

If π is primary irreducible and $\alpha \in R$, $\pi \nmid \alpha$, the biquadratic residue symbol $(\alpha/\pi)_4$ is defined to be the unique power of $i=\sqrt{-1}$ such that $(\alpha/\pi)_4 \equiv \alpha^{(p-1)/4} \ (\bmod \pi)$, where $p=\pi\bar{\pi}$ is prime in N, $p \equiv 1 \ (\bmod 4)$.

If $\lambda, \mu \in R$ we write $\lambda \sim \mu$ if and only if $\lambda^4 = 1 = \mu^4$ and $\lambda^2 = \mu^2$.

Now let $p_1, \cdots, p_n$ be as in the introduction. We choose fixed primary irreducible π_j in R such that $p_j = \pi_j \bar{\pi}_j$ $(1 \leq j \leq n)$.

Now let C_n be the set of all ordered n-tuples $\underline{c} = (c(1), \cdots, c(n))$, where each $c(j) = 0$ or 1 in $\boldsymbol{Z}$; we denote by $\underline{o}$ the n-tuple $\underline{c}$ where each $c(j) = 0$.

Finally, let $\underline{c} \in C_n$, $k \leq n$. We define

$$U(n, k, \underline{c}) = \prod_{k \neq j \leq n} (\pi_j^{1-c(j)} \bar{\pi}_j^{c(j)} / \pi_k^{c(k)} \bar{\pi}_k^{1-c(k)})_4. \tag{1.1}$$

We now prove two simple lemmas.

Lemma 1.1. *Let $n \geq 1$, and suppose that $N_n(\varepsilon) = -1$ for some ε in $\mathcal{O}_n$. Then, for at least one $\underline{c} \in C_n$, we have $U(n, k, \underline{c}) \sim 1$ for all $k \leq n$.*

Proof. Let $\varepsilon \in \mathcal{O}_n$ be a unit. Then it is easily seen that $\varepsilon^3 \in \boldsymbol{Z}[\sqrt{p_1 \cdots p_n}]$, $\varepsilon^3 = z + y\sqrt{p_1 \cdots p_n}$ with $z, y \in \boldsymbol{Z}$. Suppose that $N_n(\varepsilon) = -1$. Then

$$N_n(\varepsilon^3) = -1 = z^2 - (p_1 \cdots p_n) y^2. \tag{1.2}$$

By reduction (mod 4) we see that $y \in 1 + 2\boldsymbol{Z}$ and $z = 2x$, $x \in \boldsymbol{Z}$, while $4x^2 + 1 = (p_1 \cdots p_n) y^2 > 1$. Hence $x^2 > 0$ and, without loss of generality, $x, y \in \boldsymbol{N}$. Moreover, $(2x)^2 \equiv -1 \pmod{y}$, so that every prime factor q of y in $\boldsymbol{N}$ satisfies $q \equiv 1 \pmod 4$. (Possibly $y = 1$.) Thus, for some $m \geq 0$, we have $y = \prod_{s=1}^m q_s^{e_s}$, where the q_s are distinct primes $\equiv 1 \pmod 4$ and the $e_s \geq 1$ $(s \leq m)$. We now work in $R = \boldsymbol{Z}[i]$, $(i = \sqrt{-1})$. We have $q_3 = \rho_s \bar{\rho}_s$, ρ_s primary irreducible in R, while

$$4x^2 + 1 = (2x+i)(2x-1) = \prod_{j=1}^n \pi_j \bar{\pi}_j \prod_{s=1}^m (\rho_s \bar{\rho}_s)^{2e_s}. \tag{1.3}$$

Now, in R, the ideal $(2x+i, 2x-i)$ contains $2i$, hence also 2, hence also i, and so $(2x+i, 2x-i) = R$. Thus, $2x+i$ and $2x-i$ have no common irreducible factor in R, while neither is divisible by $(1+i)$. From this and (1.3) we see that, for some $\underline{c} \in C_n$, we have $2x+i = i^a \mu$, $2x - i = i^{-a} \bar{\mu}$, where

$$\mu = \prod_{j=1}^n \pi_j^{c(j)} \bar{\pi}_j^{1-c(j)} \prod_{s=1}^m \sigma_s^{2e_s}; \tag{1.4}$$

here $\sigma_s \in \{\rho_s, \bar{\rho}_s\}$, and $a \in \boldsymbol{Z}$, while $\mu R + \bar{\mu} R = R$ and μ is primary. From this we have $2i = i^a \mu - i^{-a} \bar{\mu}$, from which, on reduction $(\mathrm{mod}(1+i)^3)$, we see that a is odd, and

$$\pm 2 = \mu + \bar{\mu}. \tag{1.5}$$

Now let $k \leq n$. We reduce (1.5) $(\mathrm{mod}(\pi_k^{c(k)} \bar{\pi}_k^{1-c(k)}))$, obtaining

$$(\pm 2 / \pi_k^{c(k)} \bar{\pi}_k^{1-c(k)})_4 \sim \prod_{j \leq n} (\pi_j^{1-c(j)} \bar{\pi}_j^{c(j)} / \pi_k^{c(k)} \bar{\pi}_k^{1-c(k)})_4. \tag{1.6}$$

However, $(-1/\pi_k)_4 \sim 1 \sim (-1/\bar{\pi}_k)_4$ and $(2/\pi_k)_4 \sim (\bar{\pi}_k/\pi_k)_4 \sim (\pi_k/\bar{\pi}_k)_4 \sim (2/\bar{\pi}_k)_4$, from which Lemma 1.1 follows.

Lemma 1.2. *Let $n \geq 1$, and suppose that each Legendre symbol (p_j/p_k) equals $+1$, for $j \neq k$, $j, k \leq n$. Then for all $\underline{c} \in C_n$, $k \leq n$, we have $U(n, k, \underline{c}) \sim U(n, k, \underline{o})$, where $\underline{o}$ is the zero vector in C_n.*

Proof. Let $j \leq n$, $j \neq k$. We have $(\pi_j/\pi_k)_4 (\bar{\pi}_j/\pi_k)_4 = (p_j/\pi_k)_4$, while $p_j^{(p_k-1)/2} \equiv 1 \,(\mathrm{mod}(\pi_k$, (resp. $\bar{\pi}_k))$. Hence $(\pi_j/\pi_k)_4 \sim (\bar{\pi}_j/\pi_k)_4 \sim (\pi_j/\bar{\pi}_k)_4 \sim (\bar{\pi}_j/\bar{\pi}_k)_4$; Lemma 1.2 follows immediately from these relations.

2. Proof of Theorem 1. Now let $n \geq 2$. We assume that $p_1, \cdots, p_{n-1}$ have been chosen such that the Legendre symbol (p_j/p_k) equals $+1$ whenever $j, k \leq n-1$ and $j \neq k$. If $\underline{c} \in \mathcal{C}_n$ we denote by $\hat{\underline{c}}$ the vector $(c(1), \cdots, c(n-1)) \in \mathcal{C}_{n-1}$. Now let p_n be distinct from $p_1, \cdots, p_{n-1}$. Then, for every $\underline{c} \in \mathcal{C}_n$ and $k < n$ we have

$$U(n, k, \underline{c}) = (\pi_n^{1-c(n)} \bar{\pi}_n^{c(n)} / \pi_k^{c(k)} \bar{\pi}_k^{1-c(k)})_4 U(n-1, k, \hat{\underline{c}}), \tag{2.1}$$

while $U(n-1, k, \hat{\underline{c}}) \sim U(n-1, k, \hat{\underline{o}})$ by Lemma 2.2. We shall choose p_n by specifying π_n in terms of congruences (mod π_k) and (mod $\bar{\pi}_k$) for the $k < n$. We impose on π_n the conditions

$$\left.\begin{aligned} &(\pi_n/\pi_1)_4 \sim (\pi_n/\bar{\pi}_1)_4 \sim iU(n-1, 1, \hat{\underline{o}}), \\ &(\pi_n/\pi_k)_4 \sim (\pi_n/\bar{\pi}_k)_4 \quad \text{when} \quad 1 < k < n. \end{aligned}\right\} \tag{2.2}$$

Clearly there are infinitely irreducible π_n in R which satisfy (2.2), since there are infinitely many prime ideals of R of residual degree 1 in every ray-class (to any modulus). Suppose now that (2.2) is satisfied. Then certainly $(p_n/p_k) = +1$ for all $k < n$. Hence, by Lemma 2.2, we have $U(n, k, \underline{c}) \sim U(n, k, \underline{o})$ for all $\underline{c} \in \mathcal{C}_n$ and all $k \leq n$. However, by (2.2) and (2.1), we have $U(n, 1, \underline{o}) \sim i$. Thus, by Lemma 1.1, we have $N_n(\varepsilon) = +1$ for every unit in $\mathcal{O}_n$, and we have proved Theorem 1.

References

[1] K. Ireland and M. Rosen: A Classical Introduction to Modern Number Theory. 2nd ed., Springer-Verlag, New York (1982).
[2] K. Iwasawa: A note on the capitulation problem for number fields. Proc. Japan Acad., 65A, 59–61 (1989).
[3] T. Nagell: Introduction to Number Theory. Almqvist & Wiksell, Stockholm (esp. p. 203) (1951).
[4] W. Narkiewicz: Elementary and Analytic Theory of Algebraic Numbers. PWN, Warszawa (1974).
[5] L. Rédei: Über einige Mittelwertfragen im quadratischen Zahlkörper. J. Reine Angew. Math., **174**, 15–55 (1935).
[6] A. Scholz: Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$. Math. Z., **39**, 95–111 (1935).