Note on a result of Barrucand and Cohn

By *Kenneth S. Williams* at Ottawa

Let p be a prime $\equiv 1 \pmod 8$, say $p = 8n+1$, so that there are integers a, b, c, d, e, f such that

$$p = a^2 + 16b^2 = c^2 + 8d^2 = e^2 - 32f^2 \,, \tag{1}$$

with

$$\begin{aligned} &a \equiv 1 \pmod 4) \text{ (say } a = 4r+1) \,, \\ &c \equiv 1 \pmod 4 \text{ (say } c = 4s+1) \,, \\ &|e| \equiv 1 \pmod 2 \text{ (say } |e| = 2t+1) \,. \end{aligned} \tag{2}$$

The following are simple deductions from (1) and (2)

$$\begin{aligned} &\text{(i) } n \equiv r \pmod 2 \\ &\text{(ii) } n \equiv s + d \pmod 2 \\ &\text{(iii) } 2n \equiv t^2 + t \pmod 8 \,. \end{aligned} \tag{3}$$

In [1] Barrucand and Cohn proved that the octic residuacity property $\left(\frac{-4}{p}\right)_8 = 1$ is equivalent to each of

$$\begin{aligned} &\text{(i) } \frac{a-1}{4} + b \equiv 0 \pmod 2 \\ &\text{(ii) } d \equiv 0 \pmod 2 \\ &\text{(iii) } |e| \equiv 1 \pmod 4 \,. \end{aligned} \tag{4}$$

They pointed out that this result seems to have gone unnoticed before, despite many residuacity investigations on other small integers. In this note we give a very elementary proof of this result which follows the ideas of Dirichlet's delightfully simple proof [2] of Gauss' criterion for the biquadratic character of 2 namely

$$\left(\frac{2}{p}\right)_4 = (-1)^b \,. \tag{5}$$

Immediately from (3) (i) and (5) we obtain

$$\left(\frac{-4}{p}\right)_8=\left(\frac{-1}{p}\right)_8\left(\frac{2}{p}\right)_4=(-1)^{n+b}=(-1)^{r+b}=(-1)^{\frac{a-1}{4}+b},$$

which is 4 (i).

Next we prove 4 (ii). We let d' denote the largest positive odd divisor of d. By Jacobi's law of quadratic reciprocity we have

$$\left(\frac{c}{p}\right)=\left(\frac{|c|}{p}\right)=\left(\frac{p}{|c|}\right)=\left(\frac{8d^2}{|c|}\right)=\left(\frac{2}{|c|}\right)=(-1)^{\frac{c^2-1}{8}}=(-1)^{n-d^2}=(-1)^{n-d}$$

and

$$\left(\frac{d}{p}\right)=\left(\frac{d'}{p}\right)=\left(\frac{p}{d'}\right)=\left(\frac{c^2}{d'}\right)=+1$$

so that with $w^2\equiv 2 \pmod p$ we have

$$(c+2wd)^2\equiv 4wcd \pmod p$$

giving

$$\left(\frac{2}{p}\right)_4=\left(\frac{w}{p}\right)=\left(\frac{c}{p}\right)\left(\frac{d}{p}\right)=(-1)^{n-d}$$

that is

$$\left(\frac{-4}{p}\right)_8=(-1)^{2n-d}=(-1)^d.$$

Finally we prove 4 (iii). We let f' denote the largest positive odd divisor of f. By Jacobi's law of quadratic reciprocity we have

$$\left(\frac{e}{p}\right)=\left(\frac{|e|}{p}\right)=\left(\frac{p}{|e|}\right)=\left(\frac{-32f^2}{|e|}\right)=\left(\frac{-2}{|e|}\right)=(-1)^{\frac{|e|-1}{2}+\frac{|e|^2-1}{8}}=(-1)^{\frac{t^2+3t}{2}}$$

and

$$\left(\frac{f}{p}\right)=\left(\frac{f'}{p}\right)=\left(\frac{p}{f'}\right)=\left(\frac{e^2}{f'}\right)=+1$$

so that with $u^2\equiv -2 \pmod p$ we have

$$(e+4uf)^2\equiv 8uef \pmod p$$

giving

$$\left(\frac{-2}{p}\right)_4=\left(\frac{u}{p}\right)=\left(\frac{e}{p}\right)\left(\frac{f}{p}\right)=(-1)^{\frac{t^2+3t}{2}}$$

that is, by (3) (iii),

$$\left(\frac{-4}{p}\right)_8 = \left(\frac{-1}{p}\right)_8 \left(\frac{-2}{p}\right)_4 = (-1)^{n+\frac{t^2+3t}{2}} = (-1)^t .$$

References

[1] *P. Barrucand* and *H. Cohn*, Note on primes of type $x^2 + 32y^2$, class number, and residuacity, J. reine angew. Math. **238** (1969), 67—70.

[2] *G. Lejeune Dirichlet*, Über den biquadratischen Charakter der Zahl „Zwei“, J. reine angew. Math. **57** (1860), 187—188. (Gesammelte Werke, Berlin 1897, vol. 2, pp. 261—262).

Carleton University, Mathematics Department, Ottawa, K1S 5B6, Canada

Eingegangen 6. Mai 1974