PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 56, April 1976

# NOTE ON A RESULT OF KAPLAN

KENNETH S. WILLIAMS[1]

ABSTRACT. A simple proof is given of a congruence (due to Kaplan) involving the number of solutions of a certain biquadratic congruence.

Let $p$ be a prime $\equiv 1 \pmod 4$ and let $q$ be an odd prime distinct from $p$. Let $N$ denote the number of solutions of $x_1^4 + \cdots + x_q^4 \equiv q \pmod p$. In [2] Kaplan claims to compute $N$ exactly (see pp. 115, 140, 141) but in fact he only determines $N$ modulo $q$ (for counterexample see example at end of this note). Fortunately this is all that is needed for his delightful proof of the law of biquadratic reciprocity. In this note we give a very simple derivation of Kaplan's congruence for $N$ modulo $q$ based on properties of Gauss and Jacobi sums (see for example [1]).

We let $a$, $b$ be such that $p = a^2 + b^2$, $a \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$, $a - b + 1 \equiv 0 \pmod 4$, and set $\pi = a + bi$, so that $p = \pi\bar{\pi}$, with

$$\pi \equiv -1 \pmod{(1+i)^3}.$$

Next we let $\chi_\pi$ be the (nonprincipal) biquadratic character (mod $p$) given by

$$\chi_\pi(t) = \left(\frac{t}{\pi}\right)_4$$

$$= \begin{cases} i^e & \text{if } t \not\equiv 0 \pmod p \text{ and } t^{(p-1)/4} \equiv i^e \pmod \pi \ (0 \leqslant e \leqslant 3), \\ 0 & \text{if } t \equiv 0 \pmod p, \end{cases}$$

and set for $1 \leqslant k \leqslant 3$, $1 \leqslant l \leqslant p-1$,

$$\tau_k(l) = \sum_{x=1}^{p-1} \chi_\pi^k(x) e(lx) \quad (e(u) \equiv \exp(2\pi i u/p))$$

so that $\tau_k(l) = \chi_{\bar\pi}^k(l)\tau_k$, where $\tau_k \equiv \tau_k(1)$. It is known (see for example [1, pp. 430, 463]) that

$$\tau_1\bar\tau_1 = \tau_3\bar\tau_3 = p, \quad \tau_3 = (-1)^{(p-1)/4}\bar\tau_1, \quad \tau_1\tau_3 = (-1)^{(p-1)/4}p,$$

$$\tau_2 = p^{1/2}, \quad \tau_1^4 = p\pi^2, \quad \tau_3^4 = p\bar\pi^2,$$

$$\sum_{x=0}^{p-1} e(tx^4) = \tau_3\chi_\pi(t) + \tau_2\chi_\pi^2(t) + \tau_1\chi_\pi^3(t) \quad (t \not\equiv 0 \pmod p).$$

Received by the editors June 3, 1975.
*AMS (MOS) subject classifications* (1970). Primary 10A10; Secondary 10A15.
*Key words and phrases.* Biquadratic congruences, biquadratic residue character, Gauss and Jacobi sums.
[1] Research supported under National Research Council of Canada Grant No. A-7233.

Then we have

$$N = \frac{1}{p} \sum_{x_1,\ldots,x_q=0}^{p-1} \sum_{t=0}^{p-1} e(t(x_1^4 + \cdots + x_q^4 - q))$$

$$= p^{q-1} + \frac{1}{p} \sum_{t=1}^{p-1} e(-qt) \left\{ \sum_{x=0}^{p-1} e(tx^4) \right\}^q$$

$$= p^{q-1} + \frac{1}{p} \sum_{t=1}^{p-1} e(-qt) \{\tau_3 \chi_\pi(t) + \tau_2 \chi_\pi^2(t) + \tau_1 \chi_\pi^3(t)\}^q$$

$$\equiv p^{q-1} + \frac{1}{p} \sum_{t=1}^{p-1} e(-qt) \{\tau_3^q \chi_\pi^q(t) + \tau_2^q \chi_\pi^{2q}(t) + \tau_1^q \chi_\pi^{3q}(t)\} \pmod{q}.$$

*Case* (i): $q \equiv 1 \pmod 4$. We have modulo $q$,

$$N \equiv p^{q-1} + p^{-1}\{\chi_{\bar\pi}(-q)\tau_1 \tau_3^q + \chi_{\bar\pi}^2(-q)\tau_2^{q+1} + \chi_{\bar\pi}^3(-q)\tau_1^q \tau_3\}$$

$$\equiv p^{q-1} + \chi_{\bar\pi}(q)(p\bar\pi^2)^{(q-1)/4} + (q/p)p^{(q-1)/2} + \chi_\pi(q)(p\pi^2)^{(q-1)/4}.$$

*Case* (ii): $q \equiv 3 \pmod 4$. We have modulo $q$,

$$N \equiv p^{q-1} + \frac{1}{p}\{\chi_{\bar\pi}^3(-q)\tau_3^{q+1} + \chi_{\bar\pi}^2(-q)\tau_2^{q+1} + \chi_{\bar\pi}(-q)\tau_1^{q+1}\}$$

$$\equiv p^{q-1} + \frac{1}{p}(-1)^{(p-1)/4}\chi_\pi(q)(p\bar\pi^2)^{(q+1)/4} + \left(\frac{q}{p}\right)p^{(q-1)/2}$$

$$+ \frac{1}{p}(-1)^{(p-1)/4}\chi_{\bar\pi}(q)(p\pi^2)^{(q+1)/4}.$$

Thus we have established

THEOREM.

$$N \equiv \begin{cases} p^{q-1} + \left(\dfrac{q}{p}\right)p^{(q-1)/2} \\ \qquad + \left(\dfrac{q}{\pi}\right)_4 p^{(q-1)/4}\pi^{(q-1)/2} + \left(\dfrac{q}{\bar\pi}\right)_4 p^{(q-1)/4}\bar\pi^{(q-1)/2} \pmod q, \\ \qquad\qquad \text{if } q \equiv 1 \pmod 4, \\ p^{q-1} + \left(\dfrac{q}{p}\right)p^{(q-1)/2} + (-1)^{(p-1)/4}\left(\dfrac{q}{\bar\pi}\right)_4 p^{(q-3)/4}\pi^{(q+1)/2} \\ \quad + (-1)^{(p-1)/4}\left(\dfrac{q}{\pi}\right)_4 p^{(q-3)/4}\bar\pi^{(q+1)/2} \pmod q, \quad \text{if } q \equiv 3 \pmod 4. \end{cases}$$

EXAMPLE. Take $p = 5$, $q = 3$, $\pi = 1 + 2i$, so that $(q/p) = -1$, $(q/\pi)_4 = -i$, $(q/\bar\pi)_4 = i$. The theorem gives $N \equiv 28 \pmod 3$. It is easy to see that $x_1^4 + x_2^4 + x_3^4 \equiv 3 \pmod 5$ has $N = 64$.

## REFERENCES

**1.** H. Hasse, *Vorlesungen über Zahlentheorie*, Die Grundlehren der math. Wissenschaften, Band 59, Springer-Verlag, Berlin, 1950. MR **14**, 534.

**2.** P. Kaplan, *Démonstration des lois de réciprocité quadratique et biquadratique*, J. Fac. Sci. Univ. Tokyo Sect. I **16** (1969), 115–145. MR **41** #1683.

DEPARTMENT OF MATHEMATICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA