PACIFIC JOURNAL OF MATHEMATICS
Vol. 104, No. 1, 1983

# EXTENSIONS OF THEOREMS OF CUNNINGHAM-AIGNER AND HASSE-EVANS

RICHARD H. HUDSON AND KENNETH S. WILLIAMS

**If $k$ is a positive integer and $p$ is a prime with $p \equiv 1 \pmod{2^k}$, then $2^{(p-1)/2^k}$ is a $2^k$th root of unity modulo $p$. We consider the problem of determining $2^{(p-1)/2^k}$ modulo $p$. This has been done for $k = 1, 2, 3$ and the present paper treats $k = 4$ and 5, extending the work of Cunningham, Aigner, Hasse, and Evans.**

**1. Introduction.** When $k = 1$, we have the familiar result

$$(1.1) \qquad 2^{(p-1)/2} \equiv \begin{cases} +1 \pmod{p}, & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 \pmod{p}, & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

When $k = 2$ and $p \equiv 1 \pmod 4$, there are integers $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 2$ such that $p = a^2 + b^2$, with $a$ and $|b|$ unique. If $b \equiv 0 \pmod 4$ (so that $p \equiv 1 \pmod 8$), Gauss [**8**: p. 89] (see also [**4**], [**16**]) has shown that

$$(1.2) \qquad 2^{(p-1)/4} \equiv \begin{cases} +1 \pmod{p}, & \text{if } b \equiv 0 \pmod{8}, \\ -1 \pmod{p}, & \text{if } b \equiv 4 \pmod{8}. \end{cases}$$

If $b \equiv 2 \pmod 4$ (so that $p \equiv 5 \pmod 8$), we can choose $b \equiv -2 \pmod 8$, by changing the sign of $b$, if necessary, and Gauss [**8**: p. 89] (see also [**4**], [**11**: p. 66], [**16**]) has shown that

$$(1.3) \qquad 2^{(p-1)/4} \equiv -b/a \pmod{p}.$$

We note that $(-b/a)^2 \equiv -1 \pmod{p}$.

When $k = 3$ and $p \equiv 1 \pmod 8$, there are integers $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$ such that $p = a^2 + b^2$, with $a$ and $|b|$ unique. Now $\{2^{(p-1)/8}\}^4 = 2^{(p-1)/2} \equiv 1 \pmod{p}$, as $p \equiv 1 \pmod 8$, so $2^{(p-1)/8}$ is a 4th root of unity modulo $p$. If $b \equiv 0 \pmod 8$, Reuschle [**14**] conjectured and Western [**15**] (see also [**16**]) proved that

$$(1.4) \qquad 2^{(p-1)/8} \equiv \begin{cases} (-1)^{(p-1)/8} \pmod{p}, & \text{if } b \equiv 0 \pmod{16}, \\ (-1)^{(p+7)/8} \pmod{p}, & \text{if } b \equiv 8 \pmod{16}. \end{cases}$$

If $b \equiv 4 \pmod 8$, we can choose $b \equiv 4(-1)^{(p+7)/8} \pmod{16}$, by changing the sign of $b$, if necessary, and Lehmer [**11**: p. 70] has shown that

$$(1.5) \qquad 2^{(p-1)/8} \equiv -\frac{b}{a} \pmod{p}.$$