ON PRIMES OF THE FORM \( u^2 + 5v^2 \)

B. W. BREWER

1. Introduction. A prime \( p \) of the form \( 20k+1 \) or \( 20k+9 \) admits of the two integral representations \( u^2 + 5v^2 \) and \( a^2 + b^2 \) (\( a \) odd), each representation being essentially unique. Moreover, the only primes other than 5 admitting of the first representation are those of the indicated form. If \( p \) is a prime of the form \( 20k+1 \) or \( 20k+9 \) and \( a \not\equiv 0 \pmod{5} \), the author [1] has expressed \( u \) in terms of the sum

\[
\Lambda_5 = \sum_{x=0}^{p-1} \chi(x(x^4 - 5x^2 + 5)),
\]

where \( \chi(m) \) is the quadratic character of \( m \) modulo \( p \) and \( x(x^4 - 5x^2 + 5) \) is the fifth term of the sequence

\[
\begin{align*}
V_1(x) &= x, \\
V_2(x) &= x^2 - 2, \\
V_{n+2}(x) &= xV_{n+1}(x) - V_n(x) \quad (n = 1, 2, \ldots)
\end{align*}
\]

(see also A. L. Whiteman, [3], [4]). However, if \( a \equiv 0 \pmod{5} \), \( \Lambda_5 = 0 \).

In this paper, we consider the sequence \( V_1(x, Q) = x, \ V_2(x, Q) = x^2 - 2Q, \ V_{n+2}(x, Q) = xV_{n+1}(x, Q) - QV_n(x, Q) \ (n = 1, 2, \ldots) \), \( Q \) an integer, and study the sum \( \Lambda_5(Q) = \sum_{x=0}^{p-1} \chi(V_5(x, Q)) \). If \( p \) is a prime having one of the above forms, we show in general that \( \Lambda_5(Q) = \pm 4r \) when \( \chi(Q) = 1 \) and \( a \not\equiv 0 \pmod{5} \) or when \( \chi(Q) = -1 \) and \( a \equiv 0 \pmod{5} \).

Specifically, Theorem 2 is concerned with the first case and Theorem 3 with the second case. Theorem 2 reduces to Theorem 4 of [1] when \( Q = 1 \), and refinements of Theorem 3 for certain classes of primes and specific values of \( Q \) appear as Corollary 1 and Corollary 2.

Thanks are due the referee for suggesting certain improvements in Theorem 3.

2. Four lemmas. Let \( GF(p^m) \) denote the finite field of \( p^m \) elements (\( p \) a prime). We state Lemma 1 of [1] for completeness.

**Lemma 1.** If \( p \) is an odd prime, \( \lambda \) a nonzero element of \( GF(p^m) \), and \( \lambda \) is of multiplicative period \( e \), then for \( s \) a positive integer

\[
\sum_{k=0}^{e-1} \lambda^{ks} = \begin{cases} e & \text{if } s \equiv 0 \pmod{e}, \\ 0 & \text{if } s \not\equiv 0 \pmod{e}. \end{cases}
\]

The following lemma is a generalization of Lemma 2 of [1].

**Lemma 2.** Let \( p \) be an odd prime and \( \lambda \) a generating element of the multiplicative group of \( GF(p^2) \). Let \( V_1(x, Q) = x, \ V_2(x, Q) = x^2 - 2Q, \ V_{n+2}(x, Q) = xV_{n+1}(x, Q) - QV_n(x, Q) \ (n = 1, 2, \ldots) \), where \( Q \) is an integer, \( \chi(Q) = -1 \), and \( Q = \lambda^{r(p+1)} \ (0 < r \leq p - 1) \). Let

\[
\text{Presented to the Society, January 26, 1965; received by the editors May 15, 1965 and, in revised form, August 16, 1965.}
\]
ON PRIMES OF THE FORM $u^2 + 5v^2$

$\Delta_n(Q) = \sum_{x=0}^{p-1} \chi(V_n(x, Q)), \quad \Omega_n(Q) = \sum_{s=0}^{p-2} \chi(\lambda^{ns(p+1)} + Q^n\lambda^{-ns(p+1)})$

and

$\Theta_n(Q) = \sum_{i=0}^{p} \chi(\lambda^{n(i(p-1)+r)} + Q^n\lambda^{-n(i(p-1)+r)}).$

Then $2\Delta_n(Q) = \Omega_n(Q) + \Theta_n(Q)$ ($n = 1, 2, \cdots$).

We note that the conclusion of Lemma 2 also follows if $\chi(Q) = 1$, but we do not have need for this case.

**Proof of Lemma 2.** Consider the quadratics $y^2 - Py + Q$ obtained by letting $P$ run over the set $0$, $1$, $\cdots$, $p-1$, and let $\Delta = P^2 - 4Q$. Since $\chi(Q) = -1$ and $\sum_{p=0}^{p-1} \chi(\Delta) = -1$, we obtain $(p-1)/2$ quadratics with $\chi(\Delta) = 1$ and $(p+1)/2$ quadratics with $\chi(\Delta) = -1$. If $\chi(\Delta) = 1$, the roots of $y^2 - Py + Q = 0$ in $GF(p^2)$ are of the form $\lambda^{(r-s)(p+1)}$ for some $s$, $0 \leq s \leq p-2$. If $\chi(\Delta) = -1$, the roots of $y^2 - Py + Q = 0$ in $GF(p^2)$ are of the form $\lambda^{(r-1)(p-1)+r}$ for some $t$, $0 \leq t \leq p$. Conversely, $\lambda^{(r-1)(p+1)}$ are roots of $y^2 - Py + Q = 0$ for some integer $P$ such that $\chi(\Delta) = 1$, and $\lambda^{(r-1)(p-1)+r}$ are roots of $y^2 - Py + Q = 0$ for some integer $P$ such that $\chi(\Delta) = -1$.

Let $H$ denote the set of pairs $\alpha = \lambda^{(p+1)}$, $\alpha' = \lambda^{(r-s)(p+1)}$ ($s = 0$, $1$, $\cdots$, $p-2$) and $K$ denote the set of pairs $\beta = \lambda^{(r-1)(p-1)+r}$ and $\beta' = \lambda^{(r-1)(p-1)+r}$ ($t = 0$, $1$, $\cdots$, $p$). Now $\alpha = \alpha'$ if and only if $i = j$, and $\beta = \beta'$ if and only if $i+j \equiv r \pmod{p-1}$. Likewise, $\beta = \beta'$ if and only if $i = j$, and since $r$ is odd, $\beta = \beta'$ if and only if $i+j \equiv r \pmod{p+1}$. Hence there are $(p-1)/2$ distinct pairs in the set $H$, each pair occurring twice, and $(p+1)/2$ distinct pairs in the set $K$, each pair occurring twice. Since $\Omega_n(Q) = \sum_{s=0}^{p-2} \chi(\alpha^{n} + \alpha'^{n})$ and $\Theta_n(Q) = \sum_{s=0}^{p-2} \chi(\beta^{n} + \beta'^{n})$, the lemma follows.

Applying Euler's criterion to $\Omega_n(Q)$ and $\Theta_n(Q)$ in Lemma 2, we obtain

**Lemma 3.** Let $\lambda$, $\Omega_n(Q)$ and $\Theta_n(Q)$ be defined as in Lemma 2. Then

$\Omega_n(Q) = \sum_{h=0}^{(p-1)/2} \sum_{s=0}^{p-2} \binom{(p-1)/2}{h} Q^n\lambda^{ns(p+1)}(p - 4h - 1)/2$

and

$\Theta_n(Q) = \sum_{h=0}^{(p-1)/2} \sum_{t=0}^{p} \binom{(p-1)/2}{h} Q^n\lambda^{n((t(p-1)+r)(p - 4h - 1)/2}$

in $GF(p^2)$. 

Whiteman has given a proof of the following lemma. Part (1) is proved in [3] and part (2) in [4].

**Lemma 4.** (1) If \( p \) is prime and \( p = 20k + 1 = u^2 + 5v^2 = a^2 + b^2 \) (a odd), then

\[
\binom{10k}{k} \binom{10k}{3k} \equiv 4u^2 \pmod{p}
\]

and

\[
\binom{10k}{k} = -\binom{10k}{3k} \text{ or } \binom{10k}{k} \equiv \binom{10k}{3k} \pmod{p}
\]

according as \( a \equiv 0 \pmod{5} \) or \( a \not\equiv 0 \pmod{5} \).

(2) If \( p \) is prime and \( p = 20k + 9 = u^2 + 5v^2 = a^2 + b^2 \) (a odd), then

\[
\binom{10k+4}{k} \binom{10k+4}{3k+1} \equiv 4u^2 \pmod{p}
\]

and

\[
\binom{10k+4}{k} = -\binom{10k+4}{3k+1} \text{ or } \binom{10k+4}{k} \equiv \binom{10k+4}{3k+1} \pmod{p}
\]

according as \( a \equiv 0 \pmod{5} \) or \( a \not\equiv 0 \pmod{5} \).

3. \( \Lambda_5(Q) \). We first prove

**Theorem 1.** Let \( p \) be an odd prime, \( \Lambda_n(Q) \) be defined as in Lemma 2, and \( \chi(Q) = \pm 1 \). If \( \chi(Q') = \chi(Q) \) and \( Q' \equiv m^2Q \pmod{p} \), then \( \Lambda_n(Q') = \chi(m)^n\Lambda_n(Q) \) \((n = 1, 2, \ldots)\).

**Proof.** Clearly, Theorem 1 will follow if we show that

\[
(1) \quad V_n(mx, Q') \equiv m^nV_n(x, Q) \pmod{p}
\]

for \( n = 1, 2, \ldots \). We use induction. Now (1) is certainly true for \( n = 1 \) and \( n = 2 \). Assume (1) to be true for all \( k < n \). Then

\[
V_n(mx, Q') \equiv mxV_{n-1}(mx, Q') - Q'V_{n-2}(mx, Q')
= mxm^{n-1}V_{n-1}(x, Q) - m^2Qm^{n-2}V_{n-2}(x, Q)
= m^n[xV_{n-1}(x, Q) - QV_{n-2}(x, Q)] \equiv m^nV_n(x, Q) \pmod{p},
\]

and Theorem 1 is proved.

Noting that \( \Lambda_5(Q) = \sum_{x=0}^{p-1} \chi(x(x^4 - 5Qx^2 + 5Q^2)) \), Theorem 1 and Theorem 4 of [1] imply
Theorem 2. Let \( p \) be an odd prime \((p \neq 5)\), \( \chi(Q) = 1 \), and \( Q \equiv m^2 \pmod{p} \). If \( p \neq u^2 + 5v^2 \), then \( p = 20k + r \) \((r = 3, 7, 11, 13, 17, \text{ or } 19)\) and
\[
\sum_{x=0}^{p-1} \chi(x(x^4 - 5Q^2 + 5Q^2)) = 0.
\]

If \( p = u^2 + 5v^2 \), then either \( p = 20k + 1 = a^2 + b^2 \) \((a \equiv 1 \pmod{4})\), and
\[
\sum_{x=0}^{p-1} \chi(x(x^4 - 5Q^2 + 5Q^2)) = 0
\]
\[
\begin{cases}
0 & \text{if } a \equiv 0 \pmod{5}, \\
-4ux(m) \quad (u \equiv a \pmod{5}) & \text{if } a \neq 0 \pmod{5},
\end{cases}
\]

or \( p = 20k + 9 = a^2 + b^2 \) \((a \equiv 1 \pmod{4})\), and
\[
\sum_{x=0}^{p-1} \chi(x(x^4 - 5Q^2 + 5Q^2)) = 0
\]
\[
\begin{cases}
0 & \text{if } a \equiv 0 \pmod{5}, \\
4ux(m) \quad (u \equiv a \pmod{5}) & \text{if } a \neq 0 \pmod{5},
\end{cases}
\]

To obtain a representation of \( u \) in terms of a character sum under the hypothesis that \( a \equiv 0 \pmod{5} \), we consider \( \Lambda_6(Q) \) where \( \chi(Q) = -1 \). We prove

Theorem 3. Let \( p \) be an odd prime \((p \neq 5)\) and \( \chi(Q) = -1 \). If \( p \neq u^2 + 5v^2 \), then \( p = 20k + r \) \((r = 3, 7, 11, 13, 17, \text{ or } 19)\), and
\[
\sum_{x=0}^{p-1} \chi(x(x^4 - 5Q^2 + 5Q^2)) = 0.
\]

If \( p = u^2 + 5v^2 \), then either \( p = 20k + 1 = a^2 + b^2 \) \((a \equiv 1 \pmod{4})\), \( b \equiv aQ^{(p-1)/4} \pmod{p} \), and
\[
\sum_{x=0}^{p-1} \chi(x(x^4 - 5Q^2 + 5Q^2)) = \begin{cases}
0 & \text{if } a \neq 0 \pmod{5}, \\
-4u(x) \quad (u \equiv b \pmod{5}) & \text{if } a \equiv 0 \pmod{5},
\end{cases}
\]

or \( p = 20k + 9 = a^2 + b^2 \) \((a \equiv 1 \pmod{4})\), \( b \equiv aQ^{(p-1)/4} \pmod{p} \), and
\[
\sum_{x=0}^{p-1} \chi(x(x^4 - 5Q^2 + 5Q^2)) = \begin{cases}
0 & \text{if } a \neq 0 \pmod{5}, \\
4u(x) \quad (u \equiv b \pmod{5}) & \text{if } a \equiv 0 \pmod{5},
\end{cases}
\]

Proof. That \( p = u^2 + 5v^2 \) if and only if \( p = 20k + 1 \) or \( p = 20k + 9 \) is well known. We are concerned, therefore, with the evaluation of the sum \( \Lambda_6(Q) \). If \( p = 20k + r \) \((r = 3, 7, 11, \text{ or } 19)\), \( \Lambda_6(Q) = 0 \) since \( V_6(-x, Q) = -V_6(x, Q) \) and \( \chi(-1) = -1 \). If \( p = 20k + r \) \((r = 13 \text{ or } 17)\), we apply Lemma 3 and then Lemma 1 to \( \Omega_6(Q) \) and \( \Theta_6(Q) \). We obtain
\[ \Omega_6(Q) \equiv (p - 1) \left( \frac{\phi - 1}{2} \right)^{\phi(p-1)/4} (\text{mod } p) \]

and

\[ \Theta_6(Q) \equiv (p + 1) \left( \frac{\phi - 1}{2} \right)^{\phi(p-1)/4} (\text{mod } p). \]

Hence from Lemma 2, we have \( \Lambda_6(Q) \equiv 0 \pmod{p} \). Since \( \Lambda_6(Q) \) is even and numerically less than \( p \), this in turn implies that \( \Lambda_6(Q) = 0 \).

To obtain the value of \( \Lambda_6(Q) \) when \( p = u^2 + 5v^2 \), we again apply Lemma 1 and Lemma 3 to \( \Omega_6(Q) \) and \( \Theta_6(Q) \). If \( p = 20k + 1 \), we obtain

\[ \Omega_6(Q) = 2(p - 1) \left[ \binom{10k}{k} Q^{6k} + \binom{10k}{3k} Q^{15k} \right] \]

(2)

\[ + (p - 1) \binom{10k}{5k} Q^{25k} \pmod{p} \]

and

(3)

\[ \Theta_6(Q) = (p + 1) \binom{10k}{5k} Q^{25k} \pmod{p}. \]

If \( p = 20k + 9 \), we obtain

(4)

\[ \Omega_6(Q) = (p - 1) \binom{10k + 4}{5k + 2} Q^{6k+2} \pmod{p} \]

and

(5)

\[ \Theta_6(Q) = (p + 1) \binom{10k + 4}{k} \left[ Q^{6k+2} + Q^{3(6k+2)} \right] \]

\[ + (p + 1) \binom{10k + 4}{3k + 1} \left[ Q^{3(6k+2)} + Q^{7(6k+2)} \right] \]

\[ + (p + 1) \binom{10k + 4}{5k + 2} Q^{5(6k+2)} \pmod{p}. \]

Since \( \chi(Q) = -1 \), \( Q^{(p-1)/4} \equiv i \pmod{p} \), where \( i^2 \equiv -1 \pmod{p} \). Moreover,

\[ \left( \frac{\phi - 1}{2} \right) \equiv 2a \pmod{p}, \]

where \( a \equiv 1 \pmod{4} \) (Gauss). Hence if \( p = 20k + 1 \), (2) and (3) give
(6) \[ \Omega_s(Q) \equiv -2 \left( \binom{10k}{k} - \binom{10k}{3k} \right) i - 2ai \pmod{p} \]

and

(7) \[ \Theta_s(Q) \equiv 2ai \pmod{p}; \]

and if \( p = 20k + 9 \), (4) and (5) give

(8) \[ \Omega_s(Q) \equiv -2ai \pmod{p} \]

and

\[ \Theta_s(Q) \equiv 2 \left[ \binom{10k+4}{k} - \binom{10k+4}{3k+1} \right] i + 2ai \pmod{p}. \]

With a suitable choice of the sign of \( u \) when \( a \equiv 0 \pmod{5} \), Lemma 4 implies that

\[ \binom{10k}{k} - \binom{10k}{3k} \equiv \begin{cases} 0 \pmod{p} & \text{if } a \not\equiv 0 \pmod{5} , \\ -4ui \pmod{p} & \text{if } a \equiv 0 \pmod{5} , \end{cases} \]

when \( p = 20k + 1 \), and

\[ \binom{10k+4}{k} - \binom{10k+4}{3k+1} \equiv \begin{cases} 0 \pmod{p} & \text{if } a \not\equiv 0 \pmod{5} , \\ -4ui \pmod{p} & \text{if } a \equiv 0 \pmod{5} , \end{cases} \]

when \( p = 20k + 9 \). Thus if \( p = 20k + 1 \),

\[ \Omega_s(Q) \equiv \begin{cases} -2ai \pmod{p} & \text{if } a \not\equiv 0 \pmod{5} , \\ -8u - 2ai \pmod{p} & \text{if } a \equiv 0 \pmod{5} , \end{cases} \]

and \( \Theta_s(Q) \equiv 2ai \pmod{p} \); and if \( p = 20k + 9 \), \( \Theta_s(Q) \equiv -2ai \pmod{p} \) and

\[ \Theta_s(Q) \equiv \begin{cases} 2ai \pmod{p} & \text{if } a \not\equiv 0 \pmod{5} , \\ 8u + 2ai \pmod{p} & \text{if } a \equiv 0 \pmod{5} . \end{cases} \]

Hence from Lemma 2, we have

(9) \[ \Lambda_s(Q) \equiv \begin{cases} 0 \pmod{p} & \text{if } a \not\equiv 0 \pmod{5} , \\ -4u \pmod{p} & \text{if } a \equiv 0 \pmod{5} , \end{cases} \]

when \( p = 20k + 1 \), and

(10) \[ \Lambda_s(Q) \equiv \begin{cases} 0 \pmod{p} & \text{if } a \not\equiv 0 \pmod{5} , \\ 4u \pmod{p} & \text{if } a \equiv 0 \pmod{5} , \end{cases} \]

when \( p = 20k + 9 \).
Since \( p \geq 29 \) and \( |u| < p^{1/2} \), it follows that \( |4u| < p \). Then as before, \( \Lambda_6(Q) \) being even and numerically less than \( p \), (9) and (10) imply that

\[
\Lambda_6(Q) = \begin{cases} 
0 & \text{if } a \not\equiv 0 \pmod{5}, \\
-4u & \text{if } a \equiv 0 \pmod{5},
\end{cases}
\]

when \( p = 20k + 1 \), and

\[
\Lambda_6(Q) = \begin{cases} 
0 & \text{if } a \not\equiv 0 \pmod{5}, \\
4u & \text{if } a \equiv 0 \pmod{5},
\end{cases}
\]

when \( p = 20k + 9 \).

Now suppose that \( a \equiv 0 \pmod{5} \). Since \( p = a^2 + b^2 \) \( (a \equiv 1 \pmod{4}) \), the sign of \( b \) can be chosen such that \( b \equiv ai \pmod{p} \). Since \( \Omega_6(Q) = \sum_{x=1}^{p-1} \chi(x^6 + Q^8x^{-6}) = \sum_{x=0}^{p-1} \chi(x(x^{10} + Q^5)) \), \( \Omega_6(Q) \) is even. From Lemma 2, we have \( 2\Lambda_6(Q) = \Omega_6(Q) + \Theta_6(Q) \), and hence \( \Theta_6(Q) \) is even. Moreover, since \( p \geq 29 \) and \( |b| < p^{1/2} \), it follows that \( |2b| < p - 1 \), and then (7) and (8) imply that \( \Theta_6(Q) = 2b \) when \( p = 20k + 1 \) and \( \Omega_6(Q) = -2b \) when \( p = 20k + 9 \). Then from Lemma 2, we have \(-8u = 2b + \Omega_6(Q)\) if \( p = 20k + 1 \), and \( 8u = -2b + \Theta_6(Q)\) if \( p = 20k + 9 \). Now it is easily seen that \( \Omega_6(Q) \equiv 0 \pmod{5} \) if \( p = 20k + 1 \), and \( \Theta_6(Q) \equiv 0 \pmod{5} \) if \( p = 20k + 9 \). Hence \( u = b \pmod{5} \) when \( p = 20k + 1 \) or \( p = 20k + 9 \) and Theorem 3 is proved.

If \( p \) is prime and \( p = 8k + 5 = a^2 + b^2 \) \( (a \equiv 1 \pmod{4}) \), E. Lehmer [2] has shown that \( 2^{(p-1)/4} \equiv b/a \pmod{p} \). If \( p \) is prime and \( p = 12k + 5 = a^2 + b^2 \) \( (a \equiv 1 \pmod{4}) \), the author [1] has shown that the Jacobsthal sum \( \Phi_2(-3) = 2b \), and hence \( (-3)^{(p-1)/4} \equiv \Phi_2(-3)/\Phi_2(1) \equiv b/a \pmod{p} \). Using these results and Theorem 1, we obtain the following two corollaries to Theorem 3.

**Corollary 1.** Let \( p \) be a prime of the form \( 40k + 21 \) or \( 40k + 29 \), \( \chi(Q) = -1 \), and \( Q \equiv 2m^2 \pmod{p} \). If \( p = 40k + 21 \), then \( p = u^2 + 5v^2 = a^2 + b^2 \) \( (b \text{ even}, b/2 \equiv 1 \pmod{4}) \), and

\[
\sum_{x=0}^{p-1} \chi(x(x^4 - 5Qx^2 + 5Q^2)) = \begin{cases} 
0 & \text{if } a \not\equiv 0 \pmod{5}, \\
-4u\chi(m) & \text{if } a \equiv 0 \pmod{5}.
\end{cases}
\]

If \( p = 40k + 29 \), then \( p = u^2 + 5v^2 = a^2 + b^2 \) \( (b \text{ even}, b/2 \equiv 1 \pmod{4}) \), and
\[
\sum_{x=0}^{p-1} x(x^4 - 5Qx^2 + 5Q^2)) = \begin{cases} 
0 & \text{if } a \not\equiv 0 \pmod{5}, \\
4ux(m) (u \equiv b \pmod{5}) & \text{if } a \equiv 0 \pmod{5}.
\end{cases}
\]

**Corollary 2.** Let \( p \) be a prime of the form \( 60k+41 \), or \( 60k+29 \), \( x(Q) = -1 \), and \( Q \equiv -3m^2 \pmod{p} \). If \( p = 60k+41 \), then \( p = u^2 + 5v^2 = a^2 + b^2 \) \( (a \equiv 1 \pmod{4}, b \equiv a \pmod{3}) \), and

\[
\sum_{x=0}^{p-1} x(x^4 - 5Qx^2 + 5Q^2)) = \begin{cases} 
0 & \text{if } a \not\equiv 0 \pmod{5}, \\
4ux(m) (u \equiv b \pmod{5}) & \text{if } a \equiv 0 \pmod{5}.
\end{cases}
\]

If \( p = 60k+29 \), then \( p = u^2 + 5v^2 = a^2 + b^2 \) \( (a \equiv 1 \pmod{4}, b \equiv a \pmod{3}) \), and

\[
\sum_{x=0}^{p-1} x(x^4 - 5Qx^2 + 5Q^2)) = \begin{cases} 
0 & \text{if } a \not\equiv 0 \pmod{5}, \\
-4ux(m) (u \equiv b \pmod{5}) & \text{if } a \equiv 0 \pmod{5}.
\end{cases}
\]

**References**


**Texas A & M University**