Congruences for representations of primes by binary quadratic forms

by

RICHARD H. HUDSON (Columbia, S. C.) and KENNETH S. WILLIAMS* (Ottawa, Ontario)

1. Introduction. Let $p$ be a prime congruent to 1 modulo 8 so that there are integers $x_1$, $y_1$, $x_2$, $y_2$, with $x_1 \equiv x_2 \equiv 1 \pmod{2}$ and $y_1 \equiv y_2 \equiv 0 \pmod{2}$, such that

$$p = x_1^2 + y_1^2 = x_2^2 + 2y_2^2.$$  

Clearly $y_1 \equiv 0 \pmod{4}$ and we can choose the signs of $x_1$ and $x_2$ so that

$$x_1 = x_2 \equiv 1 \pmod{4}.$$  

From (1.1) and (1.2) we see that

$$x_1 = 1 - \frac{1}{8}(p-1) + 2y_1 \pmod{16},$$

$$x_2 = \frac{1}{8}(p-1) + 2y_2 \pmod{8}.$$  

Criterions for 2 to be a quartic residue of $p$ go back to Gauss [14] and Dirichlet [12], [13], see also [1], [39]. Appealing to (1.3) these criterions can be given as

$$\left( \frac{2}{p} \right) = (-1)^{\frac{(p-1)}{8} + \frac{y_1}{2}} = (-1)^{|y_1|/4} = (-1)^{|y_2|/4} = (-1)^{3/8 + y_2^2}.$$  

From (1.4) we obtain the congruences

$$x_1 - 2x_2 + \frac{1}{8}(p-1) \equiv 0 \pmod{16},$$

and

$$y_1 + 2y_2 - \frac{1}{8}(p-1) \equiv 0 \pmod{8},$$

relating the parameters in the two representations of $p$ in (1.1).

In this paper we extend these ideas to obtain congruences involving the parameters in two or more primitive representations of certain

* Research supported by grant no. A-7233 of the Natural Sciences and Engineering Research Council Canada.
multiples of a prime $p \equiv 1 \pmod{4}$ by positive binary quadratic forms. In Theorem 1 in § 2, we evaluate the Dirichlet symbols $\left(\frac{m}{p}\right)_4$ and $\left(\frac{2m}{p}\right)_4$, where $m$ is an odd positive squarefree integer such that $\left(\frac{m}{p}\right)_4 = +1$ with $p \equiv 1 \pmod{8}$ for the symbol $\left(\frac{2m}{p}\right)_4$, in terms of the representation of a multiple of $p$ by the principal form of discriminant $-4m$ or $-8m$ respectively. This theorem includes and extends results of Brown ([5], Theorem 2; [7], Theorem 3; [8], Theorem 1); Lehmer ([23], Theorem 1) and Kaplan ([18], § 13).

In § 3, we apply (1.4) and Theorem 1 to the identity
\[\left(\frac{2}{p}\right)_4 \cdot \left(\frac{m}{p}\right)_4 = \left(\frac{2m}{p}\right)_4,\]
where $m$ is an odd positive squarefree integer such that $\left(\frac{m}{p}\right)_4 = +1$ and $p$ is a prime congruent to 1 modulo 8, to obtain congruences relating the parameters in the representations of $p$ given in Theorem 1, see Theorem 2.

In § 4, we apply Theorem 1 (a) to the identity
\[\left(\frac{m}{p}\right)_4 \cdot \left(\frac{n}{p}\right)_4 = \left(\frac{mn}{p}\right)_4,\]
where $m$ and $n$ are relatively prime odd positive squarefree integers such that $\left(\frac{m}{p}\right)_4 = \left(\frac{n}{p}\right)_4 = +1$ and $p$ is a prime congruent to 1 modulo 4, to obtain congruences relating the parameters in primitive representations of certain multiples of $p$ by the principal forms of discriminants $-4m$, $-8n$ and $-4mn$ (see Theorem 3).

Results similar to those of Theorems 2 and 3 may be deduced by applying Theorem 1 to the identities
\[\left(\frac{2m}{p}\right)_4 \cdot \left(\frac{n}{p}\right)_4 = \left(\frac{2mn}{p}\right)_4, \quad \left(\frac{2m}{p}\right)_4 \cdot \left(\frac{2n}{p}\right)_4 = \left(\frac{mn}{p}\right)_4.\]
Details are left to the reader.

Finally, in § 5 we apply the law of quartic reciprocity in conjunction with Theorem 1, to obtain some further congruences (see Theorem 4).

2. Evaluation of $\left(\frac{m}{p}\right)_4$ and $\left(\frac{2m}{p}\right)_4$. Throughout the rest of this paper $p$ denotes a prime congruent to 1 modulo 4 and $m$ denotes an odd positive squarefree integer $> 1$, all of whose prime factors are quadratic residues of $p$. Appealing to Legendre's theorem ([20], p. 191), we deduce that there exist non-zero integers $k_m$, $x_m$ and $y_m$ such that
\[k_m^2 p = x_m^4 + my_m^4,\]
and, if $p \equiv 1 \pmod{8}$, there exist non-zero integers $k_{2m}$, $x_{2m}$ and $y_{2m}$ such that
\[k_{2m}^2 p = x_{2m}^4 + 2my_{2m}^4.\]
Throughout the paper $k_m$ and $k_{2m}$ will be assumed positive. Without loss of generality we may take
\[(x_m, y_m) = 1,\]
from which it follows that
\[(x_m, p) = (y_m, p) = (k_m, x_m) = (k_m, y_m) = (k_m, m) = 1.\]
Similarly, we can assume that
\[(x_{2m}, y_{2m}) = 1,\]
which guarantees that
\[(x_{2m}, p) = (y_{2m}, p) = (k_{2m}, x_{2m}) = (k_{2m}, y_{2m}) = (k_{2m}, 2m) = 1.\]
We note that (2.1) gives:
\[k_m \equiv 0 \pmod{4} \Rightarrow x_m \equiv y_m \equiv 1 \pmod{2}, \quad m \equiv 7 \pmod{8},\]
\[k_m \equiv 2 \pmod{4} \Rightarrow x_m \equiv y_m \equiv 1 \pmod{2}, \quad m \equiv 3 \pmod{8},\]
\[k_m \equiv 1 \pmod{2}, \quad p \equiv 1 \pmod{8} \Rightarrow x_m \equiv y_m \equiv 0 \pmod{4}
\] or
\[x_m \equiv 0 \pmod{2}, \quad y_m \equiv 1 \pmod{2}, \quad m \equiv 1 \pmod{4},\]
\[k_m \equiv 1 \pmod{2}, \quad p \equiv 5 \pmod{8} \Rightarrow x_m \equiv 1 \pmod{2}, \quad y_m \equiv 2 \pmod{4}
\] or
\[x_m \equiv 0 \pmod{2}, \quad y_m \equiv 1 \pmod{2}, \quad m \equiv 1 \pmod{4}.\]
Moreover we have
\[k_m \equiv 1 \pmod{2}, \quad x_m \equiv 0 \pmod{2}, \quad p \equiv m \pmod{8} \Rightarrow x_m \equiv 2 \pmod{4}.
\]
Further (2.2) gives
\[k_{2m} \equiv 1 \pmod{2}, \quad x_{2m} \equiv 1 \pmod{2}, \quad y_{2m} \equiv 0 \pmod{2}.\]
For particular values of \( m \), the corresponding values of \( k_m \) and \( k_{2m} \) can be found by appealing to tables of the class structure of complex quadratic fields as given, for example, in [9], pp. 262–270 and [31]. If \( k_m = 1 \) (resp. \( k_{2m} = 1 \)) the integers \( x_m \) and \( y_m \) (resp. \( x_{2m} \) and \( y_{2m} \)) are unique up to sign (see for example [30], Theroem 101, p. 188). If \( k_m > 1 \) or \( k_{2m} > 1 \), this is not necessarily the case as the following examples show:

\[
9 \cdot 13 = 10^2 + 17 \cdot 1^2 = 7^2 + 17 \cdot 2^2,
\]
\[
49 \cdot 73 = 57^2 + 82 \cdot 2^2 = 25^2 + 82 \cdot 6^2.
\]

It should also be noted that for a given prime \( p \) there may be more than one \( k_m \) such that \( k_m p \) is represented primitively by \( x^2 + my^2 \); for example, \( 81p \) is represented by \( x^2 + 113y^2 \) if and only if \( 169p \) is represented by \( x^2 + 113y^2 \). It follows from a theorem of Holzer [16], see also Mordell [27], that \( k_m \) and \( k_{2m} \) can always be chosen to satisfy \( 0 < k_m < \sqrt{m} \) and \( 0 < k_{2m} < \sqrt{2m} \).

With the notation specified above, we prove

**Theorem 1.** (a) Let \( p \equiv 1 \pmod{4} \). If \( m \equiv 1 \pmod{4} \) then we have

\[
\left( \frac{m}{p} \right) = \left( \frac{\alpha_m}{m} \right), \quad \text{if } m \equiv 1 \pmod{8},
\]

\[
\left( \frac{-1}{p} \right)^{\alpha_m} \left( \frac{\alpha_m}{m} \right) = (-1)^{\alpha_m} \left( \frac{\alpha_m}{m} \right), \quad \text{if } m \equiv 5 \pmod{8}.
\]

If \( m \equiv 3 \pmod{4} \) we choose \( \alpha_m \) so that \( \left( \frac{\alpha_m}{m} \right) = +1 \). Then we have

\[
\left( \frac{m}{p} \right) = \left( \frac{\alpha_m}{m} \right), \quad \text{if } p \equiv 1 \pmod{8},
\]

\[
\left( \frac{-1}{p} \right)^{\alpha_m-\frac{m}{4}} \left( \frac{\alpha_m}{m} \right) = (-1)^{\alpha_m-\frac{m}{4}} \left( \frac{\alpha_m}{m} \right), \quad \text{if } p \equiv 5 \pmod{8}.
\]

(b) Let \( p \equiv 1 \pmod{8} \). Then we have

\[
\left( \frac{2m}{p} \right) = \left( \frac{2m}{\alpha_{2m}} \right).
\]

If \( m \equiv 1 \pmod{4} \) we have

\[
\left( \frac{2m}{p} \right) = (-1)^{\alpha_m} \left( \frac{\alpha_m}{m} \right) = (-1)^{\alpha_m} \left( \frac{\alpha_m}{m} \right).
\]

If \( m \equiv 3 \pmod{4} \) we choose \( \alpha_m \) so that \( \left( \frac{\alpha_m}{m} \right) = +1 \) and we have

\[
\left( \frac{2m}{p} \right) = +1, \quad \text{if } \alpha_m = 1, 3 \pmod{8},
\]

\[
\left( \frac{2m}{p} \right) = -1, \quad \text{if } \alpha_m = 5, 7 \pmod{8}.
\]

**Proof.** (a) We set

\[
2a_m \equiv 2a_m \pmod{2}, \quad \alpha > 0, \quad a_m \equiv 1 \pmod{2},
\]

\[
y_m \equiv y_m \pmod{2}, \quad \beta > 0, \quad y_m \equiv 1 \pmod{2}.
\]

Now from (2.1) we obtain

\[
\left( \frac{-m}{p} \right) = \left( \frac{x_m y_m}{p} \right),
\]

so that \( \left( \frac{-1}{p} \right) \left( \frac{2}{p} \right) \) for \( p \equiv 1 \pmod{4} \) we have

\[
\left( \frac{m}{p} \right) = \left( \frac{2}{p} \right)^{\alpha+\beta-1} \left( \frac{x_m y_m}{p} \right).
\]

By the law of quadratic reciprocity we have

\[
\left( \frac{x_m}{p} \right) = \left( \frac{\left| x_m \right|}{p} \right) = \left( \frac{p}{\left| x_m \right|} \right) = \left( \frac{m}{\left| x_m \right|} \right) = (-1)^{\frac{m-1}{2}} \left( \frac{\left| x_m \right|}{m} \right)
\]

and

\[
\left( \frac{y_m}{p} \right) = \left( \frac{\left| y_m \right|}{p} \right) = \left( \frac{p}{\left| y_m \right|} \right) = \left( \frac{2m}{\left| y_m \right|} \right) = \left( \frac{\left| y_m \right|}{y_m} \right) = -1,
\]

so that

\[
\left( \frac{m}{p} \right) = \left( \frac{2}{p} \right)^{\alpha+\beta-1} (-1)^{\frac{m-1}{2}} \left( \frac{\left| x_m \right|}{m} \right).
\]

If \( m \equiv 1 \pmod{8} \) we deduce from (2.7) and (2.8) that \( k_m = 1 \pmod{2} \). Thus, from (2.9) and (2.10), if \( p \equiv 0 \pmod{8} \), we have \( \alpha + \beta + 1 = 2 \), and (2.18) gives, for both \( p \equiv 1 \pmod{8} \) and \( p \equiv 0 \pmod{8} \),

\[
\left( \frac{m}{p} \right) = \left( \frac{x_m}{m} \right).
\]

If \( m \equiv 5 \pmod{8} \), again from (2.7) and (2.8), we have \( k_m = 1 \pmod{2} \). Thus, from (2.9) and (2.10), we have

\[
\left( \frac{2}{p} \right)^{\alpha+\beta+1} (-1)^{\alpha} = (-1)^{\alpha+\beta+1} = (-1)^{y_m},
\]

and so (2.18) gives

\[
\left( \frac{m}{p} \right) = (-1)^{y_m+1} \left( \frac{x_m}{m} \right) = (-1)^{y_m} \left( \frac{x_m}{m} \right).
\]
If \( m \equiv 3 \pmod{4} \), choosing \( z_m \) so that \( \left( \frac{z_m}{m} \right) = +1 \), we have

\[
(-1)^{(z_m-1)/2} \left( \frac{|z_m|}{m} \right) = (-1)^{(z_m-1)/2},
\]
so that (2.18) becomes

\[
\left( \frac{m}{p} \right)_4 = \left( \frac{2}{p} \right)_4 \left( \frac{|z_m|}{m} \right) \left( \frac{|z_m|}{p} \right) \left( -1 \right)^{(z_m-1)/2} = \left( \frac{2}{|z_m|} \right)_4 \left( -1 \right)^{(z_m-1)/2}.
\]

This completes the proof of (2.13) when \( p \equiv 1 \pmod{8} \). Suppose \( p \equiv 5 \pmod{8} \). If \( k_m \) is even, by (2.7) and (2.8), we have \( a = \beta = 0 \) proving (2.13) in this case. If \( k_m \) is odd, by (2.9) and (2.10), we have \( a = 0, \beta = 1 \), which completes the proof of (a).

(b) From (2.2) we obtain

\[
\left( \frac{-2m}{p} \right)_4 = \left( \frac{z_{2m} y_{2m}}{p} \right).
\]

By (2.11), \( z_{2m} \) and \( y_{2m} \) are odd and \( y_{2m} \) is even. Setting \( y_{2m} = 2^k y^*_m, z_{2m} = 2^\gamma y^{**}_m, \beta > 1, y^*_m \) odd, we obtain as \( p \equiv 1 \pmod{8} \)

\[
\left( \frac{2m}{p} \right)_4 = \left( \frac{z_{2m}}{p} \right) \left( \frac{y^*_m}{p} \right).
\]

By the law of quadratic reciprocity, we have

\[
\left( \frac{z_{2m}}{p} \right) = \left( \frac{|z_{2m}|}{p} \right) = \left( \frac{p}{|z_{2m}|} \right) = \left( \frac{2m}{|z_{2m}|} \right),
\]
and

\[
\left( \frac{y^*_m}{p} \right) = \left( \frac{|y^*_m|}{p} \right) = \left( \frac{p}{|y^*_m|} \right) = \left( \frac{z_{2m}}{|y^*_m|} \right) = +1,
\]
so that

\[
\left( \frac{2m}{p} \right)_4 = \left( \frac{2m}{|z_{2m}|} \right),
\]
which completes the proof of (2.14).

If \( m \equiv 1 \pmod{4} \) we have

\[
\left( \frac{m}{|z_{2m}|} \right) = \left( \frac{|z_{2m}|}{m} \right) = \left( \frac{z_{2m}}{m} \right)
\]
and

\[
\left( \frac{2}{|z_{2m}|} \right) = (-1)^{(z_{2m}-1)/2} = (-1)^{(z_{2m}^2-1)/2 + 2m/z_{2m}/2},
\]
which proves (2.15).

If \( m \equiv 3 \pmod{4} \) we choose \( \left( \frac{z_m}{m} \right) = +1 \), and it follows that

\[
\left( \frac{2m}{p} \right)_4 = \left( \frac{2}{|z_{2m}|} \right) \left( \frac{|z_{2m}|}{m} \right) \left( -1 \right)^{(z_{2m}-1)/2} = \left( \frac{2}{|z_{2m}|} \right) \left( -1 \right)^{(z_{2m}-1)/2} =
\]

\[
+1, \quad \text{if}\quad z_{2m} \equiv 1, 3 \pmod{8},
\]
\[-1, \quad \text{if}\quad z_{2m} \equiv 5, 7 \pmod{8},
\]
which proves (2.16).

We remark that if all the prime factors of \( m \) are congruent to \( 1 \) modulo \( 4 \) then (2.12) and (2.15) can be expressed as follows:

\[
\left( \frac{m}{p} \right)_4 \left( \frac{p}{m} \right)_4 = \left( \frac{-1}{p} \right)^{k_{2m} - \gamma_m}, \quad \text{if}\quad m \equiv 1 \pmod{8},
\]
\[
\left( \frac{m}{p} \right)_4 \left( \frac{p}{2m} \right)_4 = \left( \frac{-1}{p} \right)^{k_{2m} - \gamma_m}, \quad \text{if}\quad m \equiv 5 \pmod{8},
\]
where \( \left( \frac{p}{2} \right)_4 = (-1)^{(p-1)/4} \) (see for example [18], p. 319).

The result (2.19) follows from (2.12) as

\[
\left( \frac{m}{p} \right)_4 = \prod_{q \mid m, q \equiv 1 \pmod{8}} \left( \frac{q}{p} \right)_4 = \prod_{q \mid m} \left( \frac{k_m}{q} \right)_4 = \frac{k_m}{m} \left( \frac{p}{m} \right)_4,
\]
and

\[
\left( \frac{k_m}{m} \right)_4 = \left( \frac{m/y_m}{k_m} \right) = \left( -\frac{y_m^2}{k_m} \right)_4 = \left( -\frac{1}{k_m} \right)_4.
\]

The result (2.20) follows from (2.15) as

\[
\left( \frac{m}{k_m} \right)_4 = \frac{k_m}{m} \left( \frac{p}{m} \right)_4
\]
and

\[
\left( \frac{k_m}{m} \right)_4 = \left( \frac{m}{k_m} \right)_4 \left( \frac{2m/y_m}{k_m} \right)_4 = \left( \frac{-x_m^2}{k_m} \right)_4 \left( \frac{2}{k_m} \right)_4 = \left( -\frac{2}{k_m} \right)_4.
\]

3. Congruences relating \( z_m, y_m, x_m, y_m, x_m, z_m, y_{2m} \). Applying Theorem 1 and (L.4) to the identity \( \left( \frac{2}{p} \right)_4 \left( \frac{m}{p} \right)_4 = \left( \frac{2m}{p} \right)_4 \), we obtain the following theorem.

**Theorem 2.** Let \( p \equiv 1 \pmod{8} \) be prime and let \( m \) be an odd positive squarefree integer, all of whose prime factors are quadratic residues \( \pmod{p} \),
so that there exist integers $x_2, y_2, x_m, y_m, x_{2m}, y_{2m}, k_m, k_{2m}$ such that

$$p = x_2^2 + 2y_2^2, \quad k_m^2p = x_m^2 + my_m^2, \quad k_{2m}^2p = x_{2m}^2 + 2my_{2m}^2.$$  

(a) If $m \equiv 1 \pmod{4}$ we have

$$y_{2m} = y_2 + \left\lfloor \frac{1}{2} (m-1) \right\rfloor y_m + \frac{1}{2} (k_{2m}^2 - 1) \pmod{4} \iff \left( \frac{y_{2m}}{m} \right) = -1.$$  

(b) If $m \equiv 3 \pmod{4}$, choose $x_m$ and $x_{2m}$ to satisfy

$$\left( \frac{x_m}{m} \right) = \left( \frac{x_{2m}}{m} \right) = +1,$$  

then

$$x_m \equiv 1, 3 \pmod{8} \iff x_2 + 2x_m \equiv 3 \pmod{8}.$$  

We remark that if all the prime factors of $m$ are congruent to 1 modulo 4, by (2.21), (2.22), (2.23) and (2.24),

$$\left( \frac{x_m}{m} \right) \left( \frac{x_{2m}}{m} \right) \text{ in Theorem 2(a)}$$

can be replaced by $\left( \frac{-1}{k_m} \right) \left( \frac{-2}{k_{2m}} \right)$, for any choice of $k_m$ and $k_{2m}$. We note that when $m = 5$, Theorem 2 is a special case of a theorem of Leonard and Williams [24], p. 169 or [25]. Theorem 2, and that when $m = 65$, Theorem 2 gives a "predictive" criterion for determining whether $p$ or $2p$ is represented by $x_2^2 + 65y_2^2$ (compare [28], Theorem 1).

4. Congruences relating $x_m, y_m, x_n, y_n, x_{mn}, y_{mn}$. Applying Theorem 1 to the identity

$$\left( \frac{m}{p} \right) \left( \frac{n}{p} \right) = \left( \frac{mn}{p} \right)$$

we obtain the following theorem.

THEOREM 3. Let $p \equiv 1 \pmod{4}$ be prime and let $m, n, mn$ be distinct odd positive squarefree integers, all of whose prime factors are quadratic residues $(\pmod{p})$, so that there exist integers $x_m, y_m, x_n, y_n, x_{mn}, y_{mn}, k_m, k_n, k_{mn}$ such that

$$k_m^2p = x_m^2 + my_m^2, \quad k_n^2p = x_n^2 + my_n^2, \quad k_{mn}^2p = x_{mn}^2 + my_{mn}^2.$$  

Then we have:

(i) if $m \equiv n \equiv 1 \pmod{8}$

$$\left( \frac{x_m}{m} \right) \left( \frac{x_n}{n} \right) \equiv \left( \frac{x_{mn}}{mn} \right);$$

(ii) if $m \equiv 1 \pmod{8}$, $n \equiv 3 \pmod{4}$

$$x_{mn} - x_n + \frac{p-1}{2} (k_{mn} - k_n) \equiv 0 \pmod{4} \iff \left( \frac{x_{mn}}{m} \right) = +1,$$  

with $x_n$ and $x_{mn}$ chosen so that

$$\left( \frac{x_n}{n} \right) = \left( \frac{x_{mn}}{mn} \right) = \pm 1;$$

(iii) if $m \equiv 1 \pmod{8}$, $n \equiv 5 \pmod{8}$

$$y_{mn} \equiv y_n (\pmod{2}) \iff \left( \frac{x_m}{m} \right) \left( \frac{x_n}{n} \right) \left( \frac{x_{mn}}{mn} \right) = +1;$$

(iv) if $m \equiv 3 \pmod{4}$, $n \equiv 3 \pmod{4}$, $mn \equiv 1 \pmod{8}$

$$x_m - x_n + \frac{p-1}{2} (k_m - k_n) \equiv 0 \pmod{4} \iff \left( \frac{x_m}{m} \right) = +1,$$  

with $x_n$ and $x_m$ chosen so that

$$\left( \frac{x_n}{n} \right) = \left( \frac{x_m}{m} \right) = +1;$$

(v) if $m \equiv 3 \pmod{4}$, $n \equiv 5 \pmod{4}$

$$x_m - x_n + \frac{p-1}{2} (k_m - k_n) \equiv 2 \pmod{4} \iff \left( \frac{x_m}{m} \right) = +1,$$  

with $x_n$ and $x_m$ chosen so that

$$\left( \frac{x_n}{n} \right) = \left( \frac{x_m}{m} \right) = +1;$$

(vi) if $m \equiv 3 \pmod{4}$, $n \equiv 5 \pmod{8}$

$$x_m - x_n + \frac{p-1}{2} (k_m - k_n) \equiv 2 \pmod{4} \iff \left( \frac{x_m}{m} \right) = +1,$$  

with $x_n$ and $x_m$ chosen so that

$$\left( \frac{x_n}{n} \right) = \left( \frac{x_m}{m} \right) = +1;$$

(vii) if $m \equiv n \equiv 5 \pmod{8}$

$$y_m \equiv y_n (\pmod{2}) \iff \left( \frac{x_m}{m} \right) \left( \frac{x_n}{n} \right) \left( \frac{x_{mn}}{mn} \right) = +1.$$  

We remark that if all the prime factors of $m$ and $n$ are congruent to 1 modulo 4, we have

$$\left( \frac{x_m}{m} \right) = \left( \frac{-1}{k_m} \right) \left( \frac{p}{m} \right), \quad \left( \frac{x_n}{n} \right) = \left( \frac{-1}{k_n} \right) \left( \frac{p}{n} \right), \quad \left( \frac{x_{mn}}{mn} \right) = \left( \frac{-1}{k_{mn}} \right) \left( \frac{p}{mn} \right),$$

so that

$$\left( \frac{x_m}{m} \right) \left( \frac{x_n}{n} \right) \left( \frac{x_{mn}}{mn} \right) = \left( \frac{-1}{k_m k_n k_{mn}} \right).$$

We remark that when $m = 5$, $n = 13$, Theorem 3 gives another "predictive" criterion for determining whether $p$ or $2p$ is represented by $x_2^2 + 65y_2^2$ (compare Kuroda [20], pp. 155-156).
5. Theorem 1 and the law of quartic reciprocity. Theorem 1 can be used in conjunction with the law of quartic reciprocity to obtain congruences relating \( x_1, y_1; x_2, y_2 \), where \( q \) is an odd prime satisfying \( \left( \frac{q}{p} \right) = +1 \).

We use Gauss' law of quartic reciprocity in the form given by Gosset [15], namely,

\[
\left( \frac{-1}{q} \right)^{\frac{q-1}{2}} \left( \frac{p}{q} \right) = \left( \frac{x_1 + y_1 i}{x_1 - y_1 i} \right)^{\frac{q-1}{2}} \left( \frac{x_1 + y_1 i}{x_1 - y_1 i} \right)^{\frac{q-1}{2}} \pmod{q},
\]

where \( p = x_1^2 + y_1^2, x_1 \equiv 1 \pmod{2}, y_1 \equiv 0 \pmod{2} \). Appealing to Theorem 1, we obtain

**Theorem 4.** Let \( p \equiv 1 \pmod{4} \) be a prime, and let \( q \) be an odd prime satisfying \( \left( \frac{q}{p} \right) = +1 \), so that there are integers \( x_q, y_q, k_q \) such that \( k_q p = x_q^2 + y_q^2 = \frac{q}{2} \left( \frac{q}{2} - 1 \right) \). Then, if \( q \equiv 1 \pmod{8} \)

\[
\left( \frac{x_q}{q} \right) = +1 \iff \left( \frac{x_1 + y_1 i}{x_1 - y_1 i} \right)^{\frac{q-1}{2}} = 1 \pmod{q};
\]

if \( q \equiv 5 \pmod{8} \),

\[
\left( \frac{x_q}{q} \right) = +1 \iff \left( \frac{x_1 + y_1 i}{x_1 - y_1 i} \right)^{\frac{q-1}{2}} = +1 \pmod{q};
\]

\[
\left( \frac{x_q}{q} \right) = -1 \iff \left( \frac{x_1 + y_1 i}{x_1 - y_1 i} \right)^{\frac{q-1}{2}} = -1 \pmod{q};
\]

if \( q \equiv 3 \pmod{4} \), with \( x_q \) chosen so that \( \left( \frac{x_q}{q} \right) = +1 \),

\[
x_q \equiv 1 \pmod{4} \iff \left( \frac{x_1 + y_1 i}{x_1 - y_1 i} \right)^{\frac{q-1}{2}} = +1 \pmod{q};
\]

\[
x_q \equiv 1 + 2k (4 \pmod{4}) \iff \left( \frac{x_1 + y_1 i}{x_1 - y_1 i} \right)^{\frac{q-1}{2}} = +1 \pmod{q},
\]

when \( p \equiv 1 \pmod{8} \),

\[
x_q \equiv 1 + 2k (4 \pmod{4}) \iff \left( \frac{x_1 + y_1 i}{x_1 - y_1 i} \right)^{\frac{q-1}{2}} = +1 \pmod{q},
\]

when \( p \equiv 5 \pmod{8} \).

The special case of Theorem 4 when \( q = 3 \) appears in [17], Theorem 2. Variants of the special case of Theorem 4 when \( q = 5 \) appear in a number of papers, see for example [2], Corollary 3.38; [3], Corollary 4.25; [4], Theorem 4; [5], Theorem 3; [6], Lemma 6.3; [21], p. 24; [22], Theorem 1; [23], p. 367; [24], p. 102; [25]; [28], § 3; [29], p. 198.

References


Some generalisations of Chebyshev polynomials
and their induced group structure over a finite field

by

REX MATTHEWS (Hobart)

1. Introduction. If \( a, b \) are rational integers then the polynomial
\[
f(z) = z^2 - wz + b \]
has roots \( \sigma_1, \sigma_2 \) in the complex field, such that \( w = \sigma_1 + \sigma_2 \)
and \( b = \sigma_1 \sigma_2 \). The polynomial \( g_k(u; b) \) may be defined by requiring
\[
f_k(z) = z^k - g_k(u; b) z^{k-1} \]
to have roots \( \sigma_1^k, \sigma_2^k \). Thus
\[
g_k(u; b) = \sigma_1^k + \sigma_2^k = \sigma_1^k + b \sigma_2^{-k} \]
and \( b^k = \sigma_1^k \sigma_2^{-k} \) and Waring's formula (see Lausch–Nobauer
[7], p. 297) allows the expression of \( g_k(u; b) \) as a polynomial in \( u \) and \( b \).
These polynomials \( g_k(u; b) \) are known as Dickson polynomials ([7], p. 209),
the case \( b = 1 \) being the classical Chebyshev polynomials of the first
kind. When these polynomials are considered as being defined over a finite
field \( F_q \) (i.e., the coefficients are reduced modulo the field characteristic)
it eventuates that some of them are so called permutation polynomials, i.e.,
the mapping of the field into itself induced by these polynomials is a
permutation. The necessary and sufficient condition for \( g_k(u; b) \) to be a
permutation polynomial is that \( (b, q^2 - 1) = 1 \) where \( q \) is the order of
the field (see [7], p. 209). Nobauer [14] showed that the set \( \{ g_k(u; b), b \} \)
is closed under composition of polynomials if and only if \( b = 0, 1, \) or \(-1, \)
and determined the structure of the groups of permutations induced by
polynomials of this type in these cases.

Lidl [19] extended this definition to an \( n \)-variable form of the Chebyshev
polynomials and their algebraic properties were considered by
Lidl and Wells [11]. In this formulation the quadratic \( f(z) \) is replaced
by a polynomial
\[
r(u_1, \ldots, u_n; z) = z^{n+1} - u_n z^n + \cdots + (-1)^n u_n z + (-1)^{n+1} b
= (z - \sigma_1) \cdots (z - \sigma_{n+1}),
\]
where \( u_n \in \mathbb{Z}, \sigma_i \in \mathbb{C} \). When taken over \( F_q \), \( r \) has \( n+1 \) not necessarily
distinct roots in \( F_q^{n+1} \).

If \( k \) is a positive integer, set
\[
r^k(u_1, \ldots, u_n; z) = (z - \sigma_1^k) \cdots (z - \sigma_{n+1}^k),
\]