Conspectus materiae tomi XLI, fasciculi 4

	Pagina
R. H. Hudson and K. S. Williams, Congruences for representations of primes by binary quadratic forms	311–322
R. Matthews, Some generalisations of Chebyshev polynomials and their induced group structure over a finite field	323–335
H. Faure, Discrépance de suites associées à un système de numération (en dimension s)	337–351
M. Newman, Cyclotomic units and Hilbert's Satz 90	353–357
E. Fouvry, Répartition des suites dans les progressions arithmétiques	359–382
V. Schulze, Erweiterung eines Satzes von Schinzel über Potenzreste	383–394
P. Erdös and A. Sárközy, Some asymptotic formulas on generalized divisor functions, III	395–411

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

ISBN 83-01-03799-7 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

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

$$p = x_1^2+y_1^2 = x_2^2+2y_2^2. \tag{1.1}$$

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

$$x_1 \equiv x_2 \equiv 1 \pmod 4. \tag{1.2}$$

From (1.1) and (1.2) we see that

$$\begin{aligned} x_1 &\equiv 1-\tfrac12(p-1)+2y_1 \pmod{16},\\ x_2 &\equiv \tfrac12(p+1)+2y_2 \pmod 8. \end{aligned} \tag{1.3}$$

Criteria for 2 to be a quartic residue of p go back to Gauss [14] and Dirichlet [12], [13], see also [1], [32]. Appealing to (1.3) these criteria can be given as

$$\left(\frac{2}{p}\right)_4 = (-1)^{\frac12\left(\frac{x_1-1}{4}+\frac{p-1}{8}\right)} = (-1)^{y_1/4} = (-1)^{(x_2-1)/4} = (-1)^{(p-1)/8+y_2/2}. \tag{1.4}$$

From (1.4) we obtain the congruences

$$x_1-2x_2+\tfrac12(p+1) \equiv 0 \pmod{16}, \tag{1.5}$$

and

$$y_1+2y_2-\tfrac12(p-1) \equiv 0 \pmod 8, \tag{1.6}$$

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 $\left(\frac{m}{p}\right) = +1$ 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

$$\left(\frac{2}{p}\right)_4\left(\frac{m}{p}\right)_4=\left(\frac{2m}{p}\right)_4,$$

where m is an odd positive squarefree integer such that $\left(\frac{m}{p}\right) = +1$ 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

$$\left(\frac{m}{p}\right)_4\left(\frac{n}{p}\right)_4=\left(\frac{mn}{p}\right)_4,$$

where m and n are relatively prime odd positive squarefree integers such that $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) = +1$ 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 $-4m$, $-4n$ and $-4mn$ (see Theorem 3).

Results similar to those of Theorems 2 and 3 may be deduced by applying Theorem 1 to the identities

$$\left(\frac{2m}{p}\right)_4\left(\frac{n}{p}\right)_4=\left(\frac{2mn}{p}\right)_4,\qquad \left(\frac{2m}{p}\right)_4\left(\frac{2n}{p}\right)_4=\left(\frac{mn}{p}\right)_4.$$

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 ([26], p. 191), we deduce that there exist non-zero integers k_m, x_m and y_m such that

$$k_m^2 p = x_m^2 + m y_m^2, \tag{2.1}$$

and, if $p\equiv 1 \pmod 8$, there exist non-zero integers k_{2m}, x_{2m} and y_{2m} such that

$$k_{2m}^2 p = x_{2m}^2 + 2m y_{2m}^2. \tag{2.2}$$

Throughout the paper k_m and k_{2m} will be assumed positive. Without loss of generality we may take

$$(x_m, y_m) = 1, \tag{2.3}$$

from which it follows that

$$(x_m, p) = (y_m, p) = (k_m, x_m) = (k_m, y_m) = (k_m, m) = 1. \tag{2.4}$$

Similarly, we can assume that

$$(x_{2m}, y_{2m}) = 1, \tag{2.5}$$

which guarantees that

$$(x_{2m}, p) = (y_{2m}, p) = (k_{2m}, x_{2m}) = (k_{2m}, y_{2m}) = (k_{2m}, 2m) = 1. \tag{2.6}$$

We note that (2.1) gives:

$$k_m \equiv 0 \pmod 4 \Rightarrow x_m \equiv y_m \equiv 1 \pmod 2,\ m\equiv 7 \pmod 8, \tag{2.7}$$

$$\begin{aligned} k_m &\equiv 2 \pmod 4 \Rightarrow x_m \equiv y_m \equiv 1 \pmod 2,\ m\equiv 3 \pmod 8,\\ k_m &\equiv 1 \pmod 2,\ p\equiv 1 \pmod 8 \Rightarrow x_m\equiv 1 \pmod 2,\ y_m\equiv 0 \pmod 4\\ &\qquad\text{or}\\ &\qquad x_m\equiv 0 \pmod 2,\ y_m\equiv 1 \pmod 2,\\ &\qquad m\equiv 1 \pmod 4, \end{aligned} \tag{2.8}$$

$$\begin{aligned} k_m &\equiv 1 \pmod 2,\ p\equiv 5 \pmod 8 \Rightarrow x_m\equiv 1 \pmod 2,\ y_m\equiv 2 \pmod 4\\ &\qquad\text{or}\\ &\qquad x_m\equiv 0 \pmod 2,\ y_m\equiv 1 \pmod 2,\\ &\qquad m\equiv 1 \pmod 4. \end{aligned} \tag{2.9}$$

Moreover we have

$$\begin{aligned} &k_m\equiv 1 \pmod 2,\quad x_m\equiv 0 \pmod 2,\\ &p\not\equiv m \pmod 8 \Rightarrow x_m\equiv 2 \pmod 4. \end{aligned} \tag{2.10}$$

Further (2.2) gives

$$k_{2m}\equiv 1 \pmod 2,\quad x_{2m}\equiv 1 \pmod 2,\quad y_{2m}\equiv 0 \pmod 2. \tag{2.11}$$

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], Theorem 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 $k_m^2 p$ 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*

$$(2.12)\qquad \left(\frac{m}{p}\right)_4 = \begin{cases} \left(\dfrac{x_m}{m}\right), & \text{if } m \equiv 1 \pmod 8,\\[2mm] (-1)^{x_m+1}\left(\dfrac{x_m}{m}\right) = (-1)^{y_m}\left(\dfrac{x_m}{m}\right), & \text{if } m \equiv 5 \pmod 8.\end{cases}$$

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

$$(2.13)\qquad \left(\frac{m}{p}\right)_4 = \begin{cases} (-1)^{(x_m-1)/2}, & \text{if } p \equiv 1 \pmod 8,\\ (-1)^{(x_m-1)/2+(k_m+1)}, & \text{if } p \equiv 5 \pmod 8.\end{cases}$$

(b) *Let* $p \equiv 1 \pmod 8$. *Then we have*

$$(2.14)\qquad \left(\frac{2m}{p}\right)_4 = \left(\frac{2m}{|x_{2m}|}\right).$$

If $m \equiv 1 \pmod 4$ *we have*

$$(2.15)\qquad \left(\frac{2m}{p}\right)_4 = (-1)^{(x_{2m}^2-1)/8}\left(\frac{x_{2m}}{m}\right) = (-1)^{(k_{2m}^2p-1)/8+y_{2m}/2}\left(\frac{x_{2m}}{m}\right).$$

If $m \equiv 3 \pmod 4$ *we choose* x_{2m} *so that* $\left(\frac{x_{2m}}{m}\right) = +1$ *and we have*

$$(2.16)\qquad \left(\frac{2m}{p}\right)_4 = \begin{cases} +1, & \text{if } x_{2m} \equiv 1, 3 \pmod 8,\\ -1, & \text{if } x_{2m} \equiv 5, 7 \pmod 8.\end{cases}$$

Proof. (a) We set

$$(2.17)\qquad \begin{cases} x_m = 2^\alpha x_m', & \alpha \geqslant 0,\ x_m' \equiv 1 \pmod 2,\\ y_m = 2^\beta y_m', & \beta \geqslant 0,\ y_m' \equiv 1 \pmod 2.\end{cases}$$

Now from (2.1) we obtain

$$\left(\frac{-m}{p}\right)_4 = \left(\frac{x_m y_m}{p}\right),$$

so that (as $\left(\frac{-1}{p}\right)_4 = \left(\frac{2}{p}\right)$ for $p \equiv 1 \pmod 4$) we have

$$\left(\frac{m}{p}\right)_4 = \left(\frac{2}{p}\right)^{\alpha+\beta+1}\left(\frac{x_m'}{p}\right)\left(\frac{y_m'}{p}\right).$$

By the law of quadratic reciprocity we have

$$\left(\frac{x_m'}{p}\right) = \left(\frac{|x_m'|}{p}\right) = \left(\frac{p}{|x_m'|}\right) = \left(\frac{k_m^2p}{|x_m'|}\right) = \left(\frac{m}{|x_m'|}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{|x_m'|-1}{2}}\left(\frac{|x_m'|}{m}\right)$$

and

$$\left(\frac{y_m'}{p}\right) = \left(\frac{|y_m'|}{p}\right) = \left(\frac{p}{|y_m'|}\right) = \left(\frac{k_m^2p}{|y_m'|}\right) = \left(\frac{x_m^2}{|y_m'|}\right) = +1,$$

so that

$$(2.18)\qquad \left(\frac{m}{p}\right)_4 = \left(\frac{2}{p}\right)^{\alpha+\beta+1}(-1)^{\frac{m-1}{2}\cdot\frac{|x_m'|-1}{2}}\left(\frac{|x_m'|}{m}\right).$$

If $m \equiv 1 \pmod 8$ we deduce from (2.7) and (2.8) that $k_m \equiv 1 \pmod 2$. Thus, from (2.9) and (2.10), if $p \equiv 5 \pmod 8$ we have $\alpha+\beta+1 = 2$, and (2.18) gives, for both $p \equiv 1 \pmod 8$ and $p \equiv 5 \pmod 8$,

$$\left(\frac{m}{p}\right)_4 = \left(\frac{x_m}{m}\right).$$

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

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

and so (2.18) gives

$$\left(\frac{m}{p}\right)_4 = (-1)^{x_m+1}\left(\frac{x_m}{m}\right) = (-1)^{y_m}\left(\frac{x_m}{m}\right).$$

If $m \equiv 3 \pmod 4$, choosing x_m so that $\left(\frac{x_m}{m}\right) = +1$, we have

$$(-1)^{(|x_m|-1)/2}\left(\frac{|x_m|}{m}\right) = (-1)^{(x_m-1)/2},$$

so that (2.18) becomes

$$\left(\frac{m}{p}\right)_4 = \left(\frac{2}{p}\right)^{\alpha+\beta+1}(-1)^{(x_m-1)/2}.$$

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 $\alpha = \beta = 0$ proving (2.13) in this case. If k_m is odd, by (2.9) and (2.10), we have $\alpha = 0$, $\beta = 1$, which completes the proof of (a).

(b) From (2.2) we obtain

$$\left(\frac{-2m}{p}\right)_4 = \left(\frac{x_{2m}y_{2m}}{p}\right).$$

By (2.11), k_{2m} and x_{2m} are odd and y_{2m} is even. Setting $y_{2m} = 2^\beta y'_{2m}$, $\beta \geqslant 1$, y'_{2m} odd, we obtain (as $p \equiv 1 \pmod 8$)

$$\left(\frac{2m}{p}\right)_4 = \left(\frac{x_{2m}}{p}\right)\left(\frac{y'_{2m}}{p}\right).$$

By the law of quadratic reciprocity, we have

$$\left(\frac{x_{2m}}{p}\right) = \left(\frac{|x_{2m}|}{p}\right) = \left(\frac{p}{|x_{2m}|}\right) = \left(\frac{k_{2m}^2 p}{|x_{2m}|}\right) = \left(\frac{2m}{|x_{2m}|}\right)$$

and

$$\left(\frac{y'_{2m}}{p}\right) = \left(\frac{|y'_{2m}|}{p}\right) = \left(\frac{p}{|y'_{2m}|}\right) = \left(\frac{k_{2m}^2 p}{|y'_{2m}|}\right) = \left(\frac{x_{2m}^2}{|y'_{2m}|}\right) = +1,$$

so that

$$\left(\frac{2m}{p}\right)_4 = \left(\frac{2m}{|x_{2m}|}\right),$$

which complete the proof of (2.14).

If $m \equiv 1 \pmod 4$ we have

$$\left(\frac{m}{|x_{2m}|}\right) = \left(\frac{|x_{2m}|}{m}\right) = \left(\frac{x_{2m}}{m}\right)$$

and

$$\left(\frac{2}{|x_{2m}|}\right) = (-1)^{(x_{2m}^2-1)/8} = (-1)^{(k_{2m}^2 p-1)/8+y_{2m}/2},$$

which proves (2.15).

If $m \equiv 3 \pmod 4$ we choose $\left(\frac{x_{2m}}{m}\right) = +1$, and it follows that

$$\left(\frac{2m}{|x_{2m}|}\right) = \left(\frac{2}{|x_{2m}|}\right)\left(\frac{|x_{2m}|}{m}\right)(-1)^{(|x_{2m}|-1)/2} = \left(\frac{2}{|x_{2m}|}\right)(-1)^{(x_{2m}-1)/2}$$
$$= \begin{cases} +1, & \text{if } x_{2m} \equiv 1, 3 \pmod 8, \\ -1, & \text{if } x_{2m} \equiv 5, 7 \pmod 8, \end{cases}$$

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:

(2.19) $$\left(\frac{m}{p}\right)_4\left(\frac{p}{m}\right)_4 = \begin{cases} (-1)^{(k_m-1)/2}, & \text{if } m \equiv 1 \pmod 8, \\ (-1)^{(k_m-1)/2+y_m}, & \text{if } m \equiv 5 \pmod 8, \end{cases}$$

(2.20) $$\left(\frac{2m}{p}\right)_4\left(\frac{p}{2m}\right)_4 = (-1)^{(y_{2m}+k_{2m}-1)/2},$$

where $\left(\frac{p}{2}\right)_4 = (-1)^{(p-1)/8}$ (see for example [18], p. 319).

The result (2.19) follows from (2.12) as

(2.21) $$\left(\frac{x_m}{m}\right) = \prod_{q(\text{prime})|m}\left(\frac{x_m}{q}\right) = \prod_{q|m}\left(\frac{x_m^2}{q}\right)_4 = \prod_{q|m}\left(\frac{k_m^2 p}{q}\right)_4$$
$$= \prod_{q|m}\left(\frac{k_m}{q}\right)\left(\frac{p}{q}\right)_4 = \left(\frac{k_m}{m}\right)\left(\frac{p}{m}\right)_4,$$

and

(2.22) $$\left(\frac{k_m}{m}\right) = \left(\frac{m}{k_m}\right) = \left(\frac{my_m^2}{k_m}\right) = \left(\frac{-x_m^2}{k_m}\right) = \left(\frac{-1}{k_m}\right).$$

The result (2.20) follows from (2.15) as

(2.23) $$\left(\frac{x_{2m}}{m}\right) = \left(\frac{k_{2m}}{m}\right)\left(\frac{p}{m}\right)_4$$

and

(2.24) $$\left(\frac{k_{2m}}{m}\right) = \left(\frac{m}{k_{2m}}\right) = \left(\frac{2my_{2m}^2}{k_{2m}}\right)\left(\frac{2}{k_{2m}}\right) = \left(\frac{-x_{2m}^2}{k_{2m}}\right)\left(\frac{2}{k_{2m}}\right) = \left(\frac{-2}{k_{2m}}\right).$$

3. Congruences relating $x_2, y_2, x_m, y_m, x_{2m}, y_{2m}$. Applying Theorem 1 and (1.4) 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* (mod p), *so that there exist integers* $x_2, y_2, x_m, y_m, x_{2m}, y_{2m}, k_m, k_{2m}$ *such that*

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

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

$$y_{2m} \equiv y_2+\tfrac{1}{2}(m-1)y_m+\tfrac{1}{4}(k_{2m}^2-1) \pmod 4 \Leftrightarrow \left(\frac{x_m x_{2m}}{m}\right) = +1.$$

(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*

$$x_{2m} \equiv 1, 3 \pmod 8 \Leftrightarrow x_2+2x_m \equiv 3 \pmod 8.$$

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), $\left(\frac{x_m x_{2m}}{m}\right)$ in Theorem 2(a) can be replaced by $\left(\frac{-1}{k_m}\right)\left(\frac{-2}{k_{2m}}\right)$. We note that when $m = 5$, Theorem 2 is a special case of a theorem of Leonard and Williams [24], p. 102 or [25], Theorem 2, and that when $m = 65$, Theorem 2 gives a "predictive" criterion for determining whether p or $9p$ is represented by $x_{65}^2+65y_{65}^2$ (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 $\left(\frac{m}{p}\right)_4\left(\frac{n}{p}\right)_4 = \left(\frac{mn}{p}\right)_4$, 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*

$$k_m^2 p = x_m^2+my_m^2, \qquad k_n^2 p = x_n^2+ny_n^2, \qquad k_{mn}^2 p = x_{mn}^2+mny_{mn}^2.$$

Then we have:

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

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

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

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

with x_n *and* x_{mn} *chosen so that* $\left(\frac{x_n}{n}\right) = \left(\frac{x_{mn}}{mn}\right) = +1$;

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

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

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

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

with x_m *and* x_n *chosen so that* $\left(\frac{x_m}{m}\right) = \left(\frac{x_n}{n}\right) = +1$;

(v) *If* $m \equiv 3 \pmod 4$, $n \equiv 3 \pmod 4$, $mn \equiv 5 \pmod 8$

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

with x_m *and* x_n *chosen so that* $\left(\frac{x_m}{m}\right) = \left(\frac{x_n}{n}\right) = +1$;

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

$$x_{mn}-x_m+2x_n+\frac{p-1}{2}(k_{mn}-k_m) \equiv 2 \pmod 4 \Leftrightarrow \left(\frac{x_n}{n}\right) = +1,$$

with x_m *and* x_{mn} *chosen so that* $\left(\frac{x_m}{m}\right) = \left(\frac{x_{mn}}{mn}\right) = +1$;

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

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

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

$$\left(\frac{x_m}{m}\right) = \left(\frac{-1}{k_m}\right)\left(\frac{p}{m}\right)_4, \qquad \left(\frac{x_n}{n}\right) = \left(\frac{-1}{k_n}\right)\left(\frac{p}{n}\right)_4, \qquad \left(\frac{x_{mn}}{mn}\right) = \left(\frac{-1}{k_{mn}}\right)\left(\frac{p}{mn}\right)_4,$$

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 $9p$ is represented by $x_{65}^2+65y_{65}^2$ (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_q, y_q, 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,

$$(5.1) \qquad \left(\frac{(-1)^{\frac{1}{2}(q-1)}q}{p}\right)_4 \equiv \left\{\frac{x_1+y_1 i}{x_1-y_1 i}\right\}^{\frac{1}{4}((-1)^{(q-1)/2}q-1)} \pmod q,$$

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 $k_q^2 p = x_q^2+qy_q^2$. Then, if $q \equiv 1 \pmod 8$*

$$(5.2) \qquad \left(\frac{x_q}{q}\right) = +1 \Leftrightarrow \left\{\frac{x_1+y_1 i}{x_1-y_1 i}\right\}^{\frac{1}{4}(q-1)} \equiv 1 \pmod q;$$

if $q \equiv 5 \pmod 8$,

$$(5.3) \qquad y_q \equiv 0 \pmod 2 \Leftrightarrow \begin{cases} \left(\frac{x_q}{q}\right) = +1, & \left\{\frac{x_1+y_1 i}{x_1-y_1 i}\right\}^{\frac{1}{4}(q-1)} \equiv +1 \pmod q; \\ & \text{or} \\ \left(\frac{x_q}{q}\right) = -1, & \left\{\frac{x_1+y_1 i}{x_1-y_1 i}\right\}^{\frac{1}{4}(q-1)} \equiv -1 \pmod q; \end{cases}$$

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

$$(5.4) \qquad \begin{cases} x_q \equiv 1 \pmod 4 \Leftrightarrow \left\{\frac{x_1+y_1 i}{x_1-y_1 i}\right\}^{\frac{1}{4}(q+1)} \equiv +1 \pmod q, \\ \qquad\qquad\qquad \text{when } p \equiv 1 \pmod 8, \\ x_q \equiv 1+2k_q \pmod 4 \Leftrightarrow \left\{\frac{x_1+y_1 i}{x_1-y_1 i}\right\}^{\frac{1}{4}(q+1)} \equiv +1 \pmod q, \\ \qquad\qquad\qquad \text{when } p \equiv 5 \pmod 8. \end{cases}$$

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 3.35; [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

[1] Pierre Barrucand and Harvey Cohn, *Note on primes of type x^2+32y^2, class number, and residuacity*, J. Reine Angew. Math. 238 (1969), pp. 67–70.

[2] Bruce C. Berndt and Ronald J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory 11 (1979), pp. 349–398.

[3] —, —, *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer*, Illinois J. Math. 23 (1979), pp. 374–437.

[4] Jacob A. Brandler, *Residuacity properties of real quadratic units*, J. Number Theory 5 (1973), pp. 271–286.

[5] Ezra Brown, *A theorem on biquadratic reciprocity*, Proc. Amer. Math. Soc. 30 (1971), pp. 220–222.

[6] —, *Representations of discriminantal divisors of binary quadratic forms*, J. Number Theory 3 (1971), pp. 213–225.

[7] —, *Quadratic forms and biquadratic reciprocity*, J. Reine Angew. Math. 253 (1972), pp. 214–220.

[8] —, *Biquadratic reciprocity laws*, Proc. Amer. Math. Soc. 37 (1973), pp. 374–376.

[9] Harvey Cohn, *A second course in number theory*, John Wiley and Sons, Inc., New York 1962.

[10] Allan Cunningham, *Quadratic partitions*, London 1904.

[11] Allan Cunningham and Thorold Gosset, *4-tic & 3-bic residuacity-tables*, Mess. Math. 50 (1920), pp. 1–30.

[12] G. Lejeune Dirichlet, *Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré*, J. Reine Angew. Math. 3 (1828), pp. 35–69.

[13] —, *Ueber den biquadratischen Charakter der Zahl "Zwei"*, ibid. 57 (1860), pp. 187–188.

[14] Carl Friedrich Gauss, *Theoria residuorum biquadraticorum I*, Art. 13.

[15] Thorold Gosset, *On the law of quartic reciprocity*, Mess. Math. 41 (1911), pp. 65–90.

[16] L. Holzer, *Minimal solutions of diophantine equations*, Canad. J. Math. 2 (1950), pp. 238–244.

[17] Richard H. Hudson and Kenneth S. Williams, *Some new residuacity criteria*, Pacific J. Math. 91 (1980), pp. 135–143.

[18] Pierre Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. 283/284 (1976), pp. 313–363.

[19] —, *Representations of prime numbers by classes of binary quadratic forms*, International Symposium on Algebraic Number Theory, Kyoto, Japan (1976).

[20] Sigekatu Kuroda, *Über die Zerlegung rationaler Primzahlen in gewissen nicht-abelschen galoisschen Korpern*, J. Math. Soc. Japan 3 (1951), pp. 148–156.

[21] Emma Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika 5 (1958), pp. 20–29.

[22] —, *On the quadratic character of the Fibonacci root*, Fibonacci Quart. 4 (1966), pp. 135–138.

[23] —, *On some special quartic reciprocity laws*, Acta Arith. 21 (1972), pp. 367–377.

[24] Philip A. Leonard and Kenneth S. Williams, *The quadratic and quartic character of certain quadratic units I*, Pacific J. Math. 71 (1977), pp. 101–106.

[25] —, —, *The quadratic and quartic character of certain quadratic units II*, Rocky Mountain J. Math. 9(1979), pp. 683–692.

[26] William J. LeVeque, *Fundamentals of number theory*, Addison-Wesley Publishing Co., Reading, Mass., 1977.

[27] L. J. Mordell, *On the magnitude of the integer solutions of the equation $ax^2+by^2+cz^2=0$*, J. Number Theory 1 (1969), pp. 1–3.

[28] Joseph B. Muskat, *On simultaneous representations of primes by binary quadratic forms*, Preprint.

[29] Joseph B. Muskat and Albert L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. 17 (1970), pp. 185–216.

[30] Trygve Nagell, *Introduction to number theory*, 2nd ed., Chelsea, New York 1964.

[31] Bernard Oriat, *Groupe des classes des corps quadratiques imaginaires* $Q(\sqrt{-a})$, $a < 10000$, Faculté des Sciences de Besançon, France.

[32] Kenneth S. Williams, *Note on a result of Barrucand and Cohn*, J. Reine Angew. Math. 285 (1976), pp. 218–220.

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF SOUTH CAROLINA
Columbia, South Carolina, U.S.A.
29208

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
Ottawa, Ontario, Canada
K1S 5B6

Received on 18. 4. 1980
and in revised form on 2. 1. 1981 (1205)

ACTA ARITHMETICA
XLI (1982)

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

by

REX MATTHEWS (Hobart)

1. Introduction. If u, b are rational integers then the polynomial $f(z) = z^2 - uz + b$ has roots σ_1, σ_2 in the complex field, such that $u = \sigma_1 + \sigma_2$ and $b = \sigma_1\sigma_2$. The polynomial $g_k(u; b)$ may be defined by requiring $f_k(z) = z^2 - g_k(u; b)z + b^k$ to have roots σ_1^k, σ_2^k. Thus $g_k(u; b) = \sigma_1^k + \sigma_2^k = \sigma_1^k + b^k\sigma_1^{-k}$ and $b^k = \sigma_1^k\sigma_2^k$ and Waring's formula (see Lausch–Nöbauer [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 $\boldsymbol{F}_q$ (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 $(k, q^2-1) = 1$ where q is the order of the field (see [7], p. 209). Nöbauer [14] showed that the set $\{g_k(u; b), b \text{ fixed}\}$ 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 [10] 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

$$\begin{aligned} r(u_1, \ldots, u_n, z) &= z^{n+1} - u_1 z^n + \ldots + (-1)^n u_n z + (-1)^{n+1} b \\ &= (z-\sigma_1)\ldots(z-\sigma_{n+1}), \end{aligned}$$

where $u_i \in \boldsymbol{Z}$, $\sigma_i \in \boldsymbol{C}$. When taken over $\boldsymbol{F}_q$, r has $n+1$ not necessarily distinct roots in $\boldsymbol{F}_{q^{(n+1)!}}$.

If k is a positive integer, set

$$r^{(k)}(u_1, \ldots, u_n, z) = (z-\sigma_1^k)\ldots(z-\sigma_{n+1}^k).$$