References

[1] S. U. Chase and W. C. Waterhouse, *Moore's theorem on uniqueness of reciprocity laws*, Invent. Math. 16 (1972), p. 267–270.

[2] Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. 29 (1967), p. 281–285.

[3] H. Hasse, *Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols*, J. Reine Angew. Math. 162 (1931), p. 134–144.

UNIVERSITÉ DE FRANCHE-COMTÉ
FACULTÉ DES SCIENCES-MATHÉMATIQUES
25030 Besançon Cedex

Reçu le 6.12.1983 (1388)

ACTA ARITHMETICA
XLV (1985)

On the evaluation of the Legendre symbol $\left(\frac{A+B\sqrt{m}}{p}\right)$

by

KENNETH S. WILLIAMS*, KENNETH HARDY** (Ottawa, Ont., Canada)
and CHRISTIAN FRIESEN*** (Fredericton, N. B., Canada)

1. Introduction. Let m be a positive squarefree integer which is either of the form

$$m = p_1 p_2 \dots p_r \equiv 1 \pmod 4 \quad (r \geqslant 1) \tag{1.1}$$

or of the form

$$m = 2p_1 p_2 \dots p_r \equiv 2 \pmod 8 \quad (r \geqslant 0), \tag{1.2}$$

where $p_1, \dots, p_r$ are primes congruent to 1 modulo 4. Let (A, B, C) be a triple of positive integers such that

$$A^2 = m(B^2 + C^2). \tag{1.3}$$

(The form of m guarantees that there are infinitely many such triples (A, B, C).) From (1.3) we see that the greatest common divisor of B and C must divide A and so can be divided out of the equation (1.3). Hence we may assume that

$$(A, B) = (A, C) = (B, C) = 1. \tag{1.4}$$

Let p be an odd prime, not dividing ABC, which is such that

$$\begin{cases} \left(\dfrac{p_i}{p}\right) = 1 & (i = 1, \dots, r), \quad \text{if} \quad m \equiv 1 \pmod 4, \\ \left(\dfrac{2}{p}\right) = \left(\dfrac{p_i}{p}\right) = 1 & (i = 1, \dots, r), \quad \text{if} \quad m \equiv 2 \pmod 8, \end{cases} \tag{1.5}$$

* Research supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233.

** Research supported by Natural Sciences and Engineering Research Council Canada Grant No. A-8049.

*** Research supported by a Natural Sciences and Engineering Research Council Canada Undergraduate Summer Research Award.

so that for both $m \equiv 1 \pmod 4$ and $m \equiv 2 \pmod 8$ we have

$$\left(\frac{m}{p}\right) = 1. \tag{1.6}$$

Hence there exists an integer w such that $w^2 \equiv m \pmod p$. Further, by the law of quadratic reciprocity (LQR), we have from (1.5)

$$\left(\frac{p}{p_i}\right) = 1 \quad (i = 1, \ldots, r). \tag{1.7}$$

The Dirichlet symbols $\left(\frac{p}{m}\right)_4$ (if $m \equiv 1 \pmod 4$) and $\left(\frac{p}{m/2}\right)_4$ (if $m \equiv 2 \pmod 8$) of quartic residuacity are defined by

$$\left(\frac{p}{p_1 \cdots p_r}\right)_4 = \prod_{i=1}^{r} \left(\frac{p}{p_i}\right)_4, \tag{1.8}$$

and for $i = 1, \ldots, r$

$$\left(\frac{p}{p_i}\right)_4 \tag{1.9}$$

$$= \begin{cases} +1, & \text{if } p \text{ is a quartic residue } (\bmod p_i), \\ -1, & \text{if } p \text{ is a quadratic residue but a quartic nonresidue } (\bmod p_i). \end{cases}$$

The purpose of this paper is to determine the value of the Legendre symbol $\left(\frac{A+B\sqrt{m}}{p}\right)$, where $\sqrt{m} = \pm w \pmod p$. The value of $\left(\frac{A+B\sqrt{m}}{p}\right)$ is independent of the choice of $\pm w$ for $\sqrt{m}$ as

$$\left(\frac{A+B\sqrt{m}}{p}\right)\left(\frac{A-B\sqrt{m}}{p}\right) = \left(\frac{A^2-mB^2}{p}\right) = \left(\frac{mC^2}{p}\right) = 1,$$

so that

$$\left(\frac{A+B\sqrt{m}}{p}\right) = \left(\frac{A-B\sqrt{m}}{p}\right). \tag{1.10}$$

The evaluation of $\left(\frac{A+B\sqrt{m}}{p}\right)$ is carried out in a completely elementary way, requiring nothing more than the manipulation of Jacobi symbols by means of Jacobi's law of quadratic reciprocity, although the method of proof is complicated by the necessity of keeping track of the exact powers of 2 dividing the integers involved. Our theorem provides a unifying result in the theory of rational quartic reciprocity laws as a number of such laws are either special cases of our theorem or can easily be deduced from it. In

particular Scholz's reciprocity law [10] is a special case of our theorem, as are Emma Lehmer's criterion for quartic residuacity ([7], p. 24) and Burde's biquadratic reciprocity law ([4], p. 183). Scholz proved his reciprocity law by means of class field theory. Later authors have given more elementary proofs of it ([5], [9], [12]). Emma Lehmer proved her criterion by studying the rationality of the roots of the period equation of degree 4 considered as a congruence modulo a prime. Burde proved his reciprocity law by means of a study of lattice points. More elementary proofs have been given of Burde's law in [9], [13]. There are many other rational reciprocity results which are also special cases or simple consequences of our theorem (see for example [1], [2], [3], [6], [8], [11]).

After a number of lemmas we prove the following Theorem in Section 2.

THEOREM. *Let m be a positive squarefree integer of the form* (1.1) *or* (1.2). *Let A, B, C be positive integers satisfying* (1.3) *and* (1.4), *then if $m \equiv 1 \pmod 4$ we have*

$$\left(\frac{A+B\sqrt{m}}{p}\right) = (-1)^{(p-1)(m-1)/8}\left(\frac{2}{p}\right)^B\left(\frac{p}{m}\right)_4,$$

and if $m \equiv 2 \pmod 8$ we have

$$\left(\frac{A+B\sqrt{m}}{p}\right) = \begin{cases} (-1)^{(p-1)/8}\left(\frac{p}{m/2}\right)_4, & \text{if} \quad p \equiv 1 \pmod 8, \\ (-1)^{(p+m-1)/8}\left(\frac{p}{m/2}\right)_4, & \text{if} \quad p \equiv 7 \pmod 8. \end{cases}$$

We note that the identity

$$2(A+B\sqrt{m})(A+C\sqrt{m}) = (A+B\sqrt{m}+C\sqrt{m})^2$$

gives

$$\left(\frac{A+C\sqrt{m}}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{A+B\sqrt{m}}{p}\right). \tag{1.11}$$

Hence, when $m \equiv 1 \pmod 4$, in which case B and C are of opposite parity, we may interchange B and C so that B is odd, and to prove the theorem in this case it suffices to show that

$$\left(\frac{A+B\sqrt{m}}{p}\right) = (-1)^{(p-1)(m-1)/8}\left(\frac{2}{p}\right)\left(\frac{p}{m}\right)_4.$$

Throughout the rest of the paper it will be assumed that B is odd when $m \equiv 1 \pmod 4$.

We now show that Scholz's reciprocity law is a special case of our theorem.

COROLLARY 1 (Scholz, [10]). *Let* $p \equiv 1 \pmod 4$ *and* $q \equiv 1 \pmod 4$ *be distinct primes such that* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. *Let* ε_p *(resp.* ε_q*) denote the fundamental unit* (>1) *of the quadratic field* $Q(\sqrt{p})$ *(resp.* $Q(\sqrt{q})$*). Then we have*

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{\varepsilon_q}{p}\right) = \left(\frac{\varepsilon_p}{q}\right).$$

Proof. In view of the symmetry in p and q, it suffices to prove the first equality. We set

$$\lambda = \begin{cases} 1, & \text{if} \quad q \equiv 1 \pmod 8, \\ 3, & \text{if} \quad q \equiv 5 \pmod 8. \end{cases}$$

Then there are positive integers T and U such that

$$\varepsilon_q^{\lambda} = T + U\sqrt{q}, \qquad T \equiv 0 \pmod 2, \qquad U \equiv 1 \pmod 2,$$

and

$$T^2 - qU^2 = -1.$$

Taking $m = q$, $A = qU$, $B = T$, $C = 1$ in the theorem, we obtain

$$\left(\frac{qU + T\sqrt{q}}{p}\right) = \left(\frac{p}{q}\right)_4,$$

that is

$$\left(\frac{\sqrt{q}}{p}\right)\left(\frac{T + U\sqrt{q}}{p}\right) = \left(\frac{p}{q}\right)_4,$$

or

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4$$

as required.

Next we show that Lehmer's criterion is a special case of our theorem.

COROLLARY 2 (Lehmer, [7]). *Let* $r = a^2 + b^2 = 4n+1$ *(*a *and* b *are positive integers with* a *odd and* b *even) be a prime, and let* q *be an odd prime not dividing* ab *such that* $\left(\frac{q}{r}\right) = 1$. *Then we have*

$$\left(\frac{q}{r}\right)_4 = \left(\frac{(-1)^n 2\lambda(\lambda+1)}{q}\right), \qquad \text{where} \qquad r \equiv \lambda^2 a^2 \pmod q.$$

Proof. Taking $p = q$, $m = r$, $A = r$, $B = a$, $C = b$ in the theorem we obtain

$$\left(\frac{2r + 2a\sqrt{r}}{q}\right) = (-1)^{(q-1)n/2}\left(\frac{q}{r}\right)_4,$$

so that

$$\left(\frac{q}{r}\right)_4 = \left(\frac{(-1)^n(2\lambda^2 a^2 + 2\lambda a^2)}{q}\right) = \left(\frac{(-1)^n 2\lambda(\lambda+1)}{q}\right)$$

as required.

We remark that Lehmer's criterion ([7], p. 24) included the case $q \mid ab$. This possibility is not covered by our theorem as we exclude $p \mid ABC$ from the outset, but is easily treated by the methods employed in this paper.

Finally we show that Burde's reciprocity law also follows from our theorem.

COROLLARY 3 (Burde, [4]). *Let* $p \equiv 1 \pmod 4$ *and* $q \equiv 1 \pmod 4$ *be distinct primes such that* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$. *Define positive integers* a, b, c, d *by*

$$p = a^2 + b^2, \quad a \equiv 1 \pmod 2, \quad b \equiv 0 \pmod 2,$$
$$q = c^2 + d^2, \quad c \equiv 1 \pmod 2, \quad d \equiv 0 \pmod 2.$$

Then

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{(p-1)/4}\left(\frac{ad - bc}{p}\right).$$

Proof. By the law of quadratic reciprocity we have

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2 + b^2}{a}\right) = \left(\frac{b^2}{a}\right) = 1.$$

Also from the congruence

$$2a(ad - bc)(d + \sqrt{q}) \equiv (ad - bc + a\sqrt{q})^2 \pmod p$$

we deduce that

$$\left(\frac{d + \sqrt{q}}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right)\left(\frac{ad - bc}{p}\right) = (-1)^{(p-1)/4}\left(\frac{ad - bc}{p}\right)$$

Applying the theorem with $m = q$, $A = q$, $B = d$, $C = c$, we obtain

$$\left(\frac{q + d\sqrt{q}}{p}\right) = \left(\frac{p}{q}\right)_4,$$

that is

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4=\left(\frac{d+\sqrt{q}}{p}\right).$$

This completes the proof.

We close this section by noting that from (1.3) we have $m\mid A^2$, and so, as m is squarefree, we have $m\mid A$, say,

$$A=ma. \tag{1.12}$$

Then, from (1.3) and (1.4), we obtain

$$ma^2=B^2+C^2, \tag{1.13}$$

and

$$(a, B)=(a, C)=(B, C)=(m, B)=(m, C)=1. \tag{1.14}$$

2. Proof of theorem. In this section we shall prove a number of technical results leading to Lemmas 9 and 10 from which the theorem follows.

LEMMA 1. *Let m be a positive squarefree integer of the form* (1.1) *or* (1.2). *Let p be an odd prime satisfying* (1.5). *Then there exist positive integers e, f, k such that*

$$k^2p=e^2-mf^2, \tag{2.1}$$

$$(e, f)=(f, k)=(e, k)=(e, p)=(f, p)=(e, m)=(k, m)=1. \tag{2.2}$$

Proof. The condition (1.5) guarantees that m is a quadratic residue (mod p) and that p is a quadratic residue (mod m). Hence, by Legendre's theorem, the equation (2.1) is solvable in non-negative integers e, f, k, which are not all zero. Clearly none of e, f, k can be zero so they are in fact all positive. If r is a prime dividing both e and f then $r^2\mid k^2p$ and so $r\mid k$. Thus r is a common factor of e, f and k which can be cancelled throughout the equation (2.1). Hence we may assume without loss of generality that $(e, f)=1$. It is then easy to check that, as m is squarefree and $p\nmid m$, we have (2.2).

LEMMA 2. *With the notation of Lemma* 1 *we have the congruences for e, f, k given in Table* 1.

Proof. The congruences for e, f and k follow easily by considering (2.1) modulo 8.

LEMMA 3. *With the notation of Lemma* 1, *the solution e, f, k of* (2.1) *and* (2.2) *can be chosen to satisfy*

$$\begin{cases} f\equiv 0\pmod 2, & k\equiv 1\pmod 2, \quad \text{if} \quad p\equiv m\pmod 4,\\ e\equiv 0\pmod 2, & k\equiv 1\pmod 2, \quad \text{if} \quad p\equiv 3\pmod 4,\ m\equiv 1\pmod 4.\end{cases}$$

Table 1

$p \pmod 8$	$m \pmod 8$	congruences for e, f, k
1	1	$e\equiv 1\pmod 2,\ f\equiv 0\pmod 4,\ k\equiv 1\pmod 2$ *or* $e\equiv f\equiv 1\pmod 2,\ k\equiv 0\pmod 4$
1	2	$e\equiv 1\pmod 2,\ f\equiv 0\pmod 2,\ k\equiv 1\pmod 2$
1	5	$e\equiv 1\pmod 2,\ f\equiv 0\pmod 4,\ k\equiv 1\pmod 2$ *or* $e\equiv f\equiv 1\pmod 2,\ k\equiv 2\pmod 4$
3	1	$e\equiv f\equiv 1\pmod 2,\ k\equiv 0\pmod 4$ *or* $e\equiv 2\pmod 4,\ f\equiv k\equiv 1\pmod 2$
3	2	this case cannot occur
3	5	$e\equiv f\equiv 1\pmod 2,\ k\equiv 2\pmod 4$ *or* $e\equiv 0\pmod 4,\ f\equiv k\equiv 1\pmod 2$
5	1	$e\equiv f\equiv 1\pmod 2,\ k\equiv 0\pmod 4$ *or* $e\equiv 1\pmod 2,\ f\equiv 2\pmod 4,\ k\equiv 1\pmod 2$
5	2	this case cannot occur
5	5	$e\equiv f\equiv 1\pmod 2,\ k\equiv 2\pmod 4$ *or* $e\equiv 1\pmod 2,\ f\equiv 2\pmod 4,\ k\equiv 1\pmod 2$
7	1	$e\equiv f\equiv 1\pmod 2,\ k\equiv 0\pmod 4$ *or* $e\equiv 0\pmod 4,\ f\equiv k\equiv 1\pmod 2$
7	2	$e\equiv f\equiv k\equiv 1\pmod 2$
7	5	$e\equiv f\equiv 1,\ k\equiv 2\pmod 4$ *or* $e\equiv 2\pmod 4,\ f\equiv k\equiv 1\pmod 2$

Proof. If $p\equiv m\pmod 4$ and e, f, k is a solution of (2.1) and (2.2) with $f\equiv 1\pmod 2$ and $k\equiv 0\pmod 2$ then e', f', k' defined by

$$e'=e\left(\frac{p+m}{2}\right),\quad f'=\left|\frac{(p-m)}{2}f-pk\right|,\quad k'=\left|\frac{(p-m)}{2}k+mf\right|$$

is a solution in positive integers of (2.1) with

$$f' \equiv 0 \pmod 2, \quad k' \equiv 1 \pmod 2.$$

Dividing each of e', f', k' by their G.C.D. we obtain the required solution.

If $p \equiv 3 \pmod 4$, $m \equiv 1 \pmod 4$ let e, f, k be a solution in positive integers of (2.1) and (2.2) with $e \equiv 1 \pmod 2$, $k \equiv 0 \pmod 2$. Let X, Y be the smallest solution in positive integers of $X^2 - pY^2 = 1$. Then it is well known and easily verified that

$$X \equiv 0 \pmod 2, \quad Y \equiv 1 \pmod 2.$$

Replacing e, f, k by $e' = eX + pkY$, $f' = f$, $k' = kX + eY$, we obtain a solution in positive integers of (2.1) with $e' \equiv 0 \pmod 2$, $k' \equiv 1 \pmod 2$. Dividing each of e', f', k' by their G.C.D. we obtain the required solution.

In view of Lemmas 2 and 3 and the choice $B \equiv 1 \pmod 2$ it suffices to consider the following cases.

Table 2

Case	$p \pmod 8$	$m \pmod 8$	congruences for A, B, C	congruences for e, f, k
I	1	1	$A \equiv B \equiv 1 \pmod 2$, $C \equiv 0 \pmod 4$	$e \equiv 1 \pmod 2$, $f \equiv 0 \pmod 4$, $k \equiv 1 \pmod 2$
II	1	2	$A \equiv 2 \pmod 4$, $B \equiv C \equiv 1 \pmod 2$	$e \equiv 1 \pmod 2$, $f \equiv 0 \pmod 2$, $k \equiv 1 \pmod 2$
III	1	5	$A \equiv B \equiv 1 \pmod 2$, $C \equiv 2 \pmod 4$	$e \equiv 1 \pmod 2$, $f \equiv 0 \pmod 4$, $k \equiv 1 \pmod 2$
IV	3	1	$A \equiv B \equiv 1 \pmod 2$, $C \equiv 0 \pmod 4$	$e \equiv 2 \pmod 4$, $f \equiv k \equiv 1 \pmod 2$
V	3	5	$A \equiv B \equiv 1 \pmod 2$, $C \equiv 2 \pmod 4$	$e \equiv 0 \pmod 4$, $f \equiv k \equiv 1 \pmod 2$
VI	5	1	$A \equiv B \equiv 1 \pmod 2$, $C \equiv 0 \pmod 4$	$e \equiv 1 \pmod 2$, $f \equiv 2 \pmod 4$, $k \equiv 1 \pmod 2$
VII	5	5	$A \equiv B \equiv 1 \pmod 2$, $C \equiv 2 \pmod 4$	$e \equiv 1 \pmod 2$, $f \equiv 2 \pmod 4$, $k \equiv 1 \pmod 2$
VIII	7	1	$A \equiv B \equiv 1 \pmod 2$, $C \equiv 0 \pmod 4$	$e \equiv 0 \pmod 4$, $f \equiv k \equiv 1 \pmod 2$
IX	7	2	$A \equiv 2 \pmod 4$, $B \equiv C \equiv 1 \pmod 2$	$e \equiv f \equiv k \equiv 1 \pmod 2$
X	7	5	$A \equiv B \equiv 1 \pmod 2$, $C \equiv 2 \pmod 4$	$e \equiv 2 \pmod 4$, $f \equiv k \equiv 1 \pmod 2$

The following simple observations will be important in what follows:

$$a \equiv B \equiv k \equiv 1 \pmod 2, \tag{2.3}$$

$$Af + Be \equiv 1 \pmod 2, \tag{2.4}$$

$$ae + Bf \equiv \begin{cases} 0 \pmod 2, & \text{in case IX,} \\ 1 \pmod 2, & \text{otherwise.} \end{cases} \tag{2.5}$$

It is convenient at this point to introduce the following notation: if n is a positive integer the largest odd divisor of n is denoted by n^*. In particular we set

$$e = 2^\varepsilon e^*, \quad \varepsilon \geqslant 0, \quad e^* \equiv 1 \pmod 2, \tag{2.6}$$

$$f = 2^\zeta f^*, \quad \zeta \geqslant 0, \quad f^* \equiv 1 \pmod 2, \tag{2.7}$$

$$m = 2^\mu m^*, \quad \mu = 0 \text{ or } 1, \quad m^* \equiv 1 \pmod 4. \tag{2.8}$$

We note that

$$\varepsilon = 0, \quad \text{if} \quad p \equiv 1 \pmod 4, \tag{2.9}$$

$$\zeta = 0, \quad \text{if} \quad p \equiv 3 \pmod 4, \tag{2.10}$$

$$\mu = \begin{cases} 0, & \text{if} \quad m \equiv 1 \pmod 4, \\ 1, & \text{if} \quad m \equiv 2 \pmod 8. \end{cases} \tag{2.11}$$

LEMMA 4. *With the notation of Lemma 1 and Table 2, we have*

$$\left(\frac{e}{p}\right) = \left(\frac{-1}{e^*}\right)^{(p+1)/2} \left(\frac{2}{pm^*}\right)^\varepsilon \left(\frac{2}{ke^*}\right)^\mu \left(\frac{p}{m^*}\right)_4 \tag{2.12}$$

and

$$\left(\frac{f}{p}\right) = \left(\frac{-1}{f^*}\right)^{(p-1)/2} \left(\frac{2}{p}\right)^\zeta. \tag{2.13}$$

Proof. We have

$$\begin{aligned}
\left(\frac{e}{p}\right) &= \left(\frac{2}{p}\right)^\varepsilon \left(\frac{e^*}{p}\right) && \text{(by (2.6))} \\
&= \left(\frac{2}{p}\right)^\varepsilon \left(\frac{-1}{e^*}\right)^{(p-1)/2} \left(\frac{p}{e^*}\right) && \text{(by LQR)} \\
&= \left(\frac{-1}{e^*}\right)^{(p-1)/2} \left(\frac{2}{p}\right)^\varepsilon \left(\frac{k^2 p}{e^*}\right) && \text{(by (2.2))} \\
&= \left(\frac{-1}{e^*}\right)^{(p-1)/2} \left(\frac{2}{p}\right)^\varepsilon \left(\frac{e^2 - mf^2}{e^*}\right) && \text{(by (2.1))} \\
&= \left(\frac{-1}{e^*}\right)^{(p+1)/2} \left(\frac{2}{p}\right)^\varepsilon \left(\frac{m}{e^*}\right) && \text{(by (2.2))} \\
&= \left(\frac{-1}{e^*}\right)^{(p+1)/2} \left(\frac{2}{p}\right)^\varepsilon \left(\frac{2}{e^*}\right)^\mu \left(\frac{m^*}{e^*}\right) && \text{(by (2.8))} \\
&= \left(\frac{-1}{e^*}\right)^{(p+1)/2} \left(\frac{2}{p}\right)^\varepsilon \left(\frac{2}{e^*}\right)^\mu \left(\frac{e^*}{m^*}\right) && \text{(by LQR)}
\end{aligned}$$

$$= \left(\frac{-1}{e^*}\right)^{(p+1)/2}\left(\frac{2}{pm^*}\right)^{\varepsilon}\left(\frac{2}{e^*}\right)^{\mu}\left(\frac{e}{m^*}\right) \qquad \text{(by (2.6))}$$

$$= \left(\frac{-1}{e^*}\right)^{(p+1)/2}\left(\frac{2}{pm^*}\right)^{\varepsilon}\left(\frac{2}{e^*}\right)^{\mu}\left(\frac{e^2}{m^*}\right)_4 \qquad \text{(by (1.1), (1.2))}$$

$$= \left(\frac{-1}{e^*}\right)^{(p+1)/2}\left(\frac{2}{pm^*}\right)^{\varepsilon}\left(\frac{2}{e^*}\right)^{\mu}\left(\frac{k^2p}{m^*}\right)_4 \qquad \text{(by (2.1))}$$

$$= \left(\frac{-1}{e^*}\right)^{(p+1)/2}\left(\frac{2}{pm^*}\right)^{\varepsilon}\left(\frac{2}{e^*}\right)^{\mu}\left(\frac{k}{m^*}\right)\left(\frac{p}{m^*}\right)_4$$

$$= \left(\frac{-1}{e^*}\right)^{(p+1)/2}\left(\frac{2}{pm^*}\right)^{\varepsilon}\left(\frac{2}{e^*}\right)^{\mu}\left(\frac{m^*}{k}\right)\left(\frac{p}{m^*}\right)_4 \qquad \text{(by LQR)}$$

$$= \left(\frac{-1}{e^*}\right)^{(p+1)/2}\left(\frac{2}{pm^*}\right)^{\varepsilon}\left(\frac{2}{ke^*}\right)^{\mu}\left(\frac{m}{k}\right)\left(\frac{p}{m^*}\right) \qquad \text{(by (2.8))}$$

$$= \left(\frac{-1}{e^*}\right)^{(p+1)/2}\left(\frac{2}{pm^*}\right)^{\varepsilon}\left(\frac{2}{ke^*}\right)^{\mu}\left(\frac{p}{m^*}\right)_4,$$

as

$$\left(\frac{m}{k}\right) = \left(\frac{mf^2}{k}\right) = \left(\frac{e^2-k^2p}{k}\right) = \left(\frac{e^2}{k}\right) = 1.$$

This completes the proof of (2.12).

Next we have

$$\left(\frac{f}{p}\right) = \left(\frac{2}{p}\right)^{\zeta}\left(\frac{f^*}{p}\right) \qquad \text{(by (2.7))}$$

$$= \left(\frac{2}{p}\right)^{\zeta}\left(\frac{-1}{f^*}\right)^{(p-1)/2}\left(\frac{p}{f^*}\right) \qquad \text{(by LQR)}$$

$$= \left(\frac{-1}{f^*}\right)^{(p-1)/2}\left(\frac{2}{p}\right)^{\zeta}\left(\frac{k^2p}{f^*}\right) \qquad \text{(by (2.2))}$$

$$= \left(\frac{-1}{f^*}\right)^{(p-1)/2}\left(\frac{2}{p}\right)^{\zeta}\left(\frac{e^2-mf^2}{f^*}\right) \qquad \text{(by (2.1))}$$

$$= \left(\frac{-1}{f^*}\right)^{(p-1)/2}\left(\frac{2}{p}\right)^{\zeta}\left(\frac{e^2}{f^*}\right)$$

$$= \left(\frac{-1}{f^*}\right)^{(p-1)/2}\left(\frac{2}{p}\right)^{\zeta}$$

which completes the proof of (2.13).

LEMMA 5. *With the notation of Lemma 1 and Table 2, we have*

$$\left(\frac{B}{m^*}\right) = \left(\frac{2}{B}\right)^{\mu}, \tag{2.14}$$

$$\left(\frac{k}{m^*}\right) = \left(\frac{2}{k}\right)^{\mu}, \tag{2.15}$$

$$\left(\frac{e}{m^*}\right) = \left(\frac{2}{k}\right)^{\mu}\left(\frac{p}{m^*}\right)_4. \tag{2.16}$$

Proof. We have

$$\left(\frac{B}{m^*}\right) = \left(\frac{m^*}{B}\right) \qquad \text{(by LQR)}$$

$$= \left(\frac{2}{B}\right)^{\mu}\left(\frac{m}{B}\right) \qquad \text{(by (2.8))}$$

$$= \left(\frac{2}{B}\right)^{\mu}\left(\frac{ma^2}{B}\right) \qquad \text{(by (1.14))}$$

$$= \left(\frac{2}{B}\right)^{\mu}\left(\frac{B^2+C^2}{B}\right) \qquad \text{(by (1.13))}$$

$$= \left(\frac{2}{B}\right)^{\mu}.$$

This completes the proof of (2.14).

Next we have

$$\left(\frac{k}{m^*}\right) = \left(\frac{m^*}{k}\right) \qquad \text{(by LQR)}$$

$$= \left(\frac{2}{k}\right)^{\mu}\left(\frac{m}{k}\right) \qquad \text{(by (2.8))}$$

$$= \left(\frac{2}{k}\right)^{\mu}\left(\frac{mf^2}{k}\right) \qquad \text{(by (2.2))}$$

$$= \left(\frac{2}{k}\right)^{\mu}\left(\frac{e^2-k^2p}{k}\right) \qquad \text{(by (2.1))}$$

$$= \left(\frac{2}{k}\right)^{\mu}.$$

This completes the proof of (2.15).

Finally we have

$$\left(\frac{e}{m^*}\right)=\left(\frac{e^2}{m^*}\right)$$
$$=\left(\frac{e^2-mf^2}{m^*}\right)_4$$
$$=\left(\frac{k^2p}{m^*}\right)_4 \qquad \text{(by (2.1))}$$
$$=\left(\frac{k}{m^*}\right)\left(\frac{p}{m^*}\right)_4$$
$$=\left(\frac{2}{k}\right)^{\mu}\left(\frac{p}{m^*}\right)_4 \qquad \text{(by (2.15))}.$$

This completes the proof of (2.16).

LEMMA 6. *With the notation of Lemma 1 and Table 2, we have*

$$\left(\frac{Af+Be}{m^*}\right)=\left(\frac{2}{Bk}\right)^{\mu}\left(\frac{p}{m^*}\right)_4.$$

Proof. This follows immediately from Lemma 5 as

$$\left(\frac{Af+Be}{m^*}\right)=\left(\frac{maf+Be}{m^*}\right)=\left(\frac{Be}{m^*}\right)=\left(\frac{B}{m^*}\right)\left(\frac{e}{m^*}\right).$$

LEMMA 7. *With the notation of Lemma 1 and Table 2, we have*

$$(Af+Be,\ ae+Bf)=l^2, \tag{2.17}$$

where l is an odd positive integer such that

$$(l,\ maBefp)=1. \tag{2.18}$$

Proof. We first recall from (2.4) that $Af+Be$ is odd. Therefore $(Af+Be,\ ae+Bf)$ is odd. Suppose q is an odd prime such that

$$q^{2h+1}\,\|\,(Af+Be,\ ae+Bf).$$

From

$$(Af+Be)^2-m(ae+Bf)^2=(B^2-ma^2)(e^2-mf^2)=-C^2k^2p, \tag{2.19}$$

we have $q^{4h+2}\,|\,C^2k^2p$, so $q^{2h+1}\,|\,Ck$. Hence either $q^{h+1}\,|\,C$ or $q^{h+1}\,|\,k$.

Suppose first that $q^{h+1}\,|\,C$. It is easy to check that $(q,\ aBmp)=1$. Further as $(e,f)=1$ and $q^{2h+1}\,|\,ae+Bf$ we have $(q,\ ef)=1$. Then eliminating B from the congruences

$$Be\equiv -maf\ (\mathrm{mod}\ q^{2h+1}),\qquad Bf\equiv -ae\ (\mathrm{mod}\ q^{2h+1})$$

we obtain $a(e^2-mf^2)\equiv 0\ (\mathrm{mod}\ q^{2h+1})$, so that $k^2p\equiv 0\ (\mathrm{mod}\ q^{2h+1})$, giving $q^{h+1}\,|\,k$.

Suppose now that $q^{h+1}\,|\,k$. It is easy to check that $(q,\ efm)=1$. Further as $(a,\ B)=1$ and $q^{2h+1}\,|\,ae+Bf$ we have $(q,\ aB)=1$. Then eliminating f from the congruences

$$maf\equiv -Be\ (\mathrm{mod}\ q^{2h+1}),\qquad Bf\equiv -ae\ (\mathrm{mod}\ q^{2h+1}),$$

we obtain $e(ma^2-B^2)\equiv 0\ (\mathrm{mod}\ q^{2h+1})$, so that $C^2\equiv 0\ (\mathrm{mod}\ q^{2h+1})$, giving $q^{h+1}\,|\,C$, $(q,\ p)=1$.

Hence in both cases we have $q^{h+1}\,|\,C$, $q^{h+1}\,|\,k$, and $(q,\ aBmefp)=1$. Then from $ma^2-B^2=C^2\equiv 0\ (\mathrm{mod}\ q^{2h+2})$ and $e^2-mf^2=k^2p\equiv 0\ (\mathrm{mod}\ q^{2h+2})$, we obtain on eliminating m

$$a^2e^2-B^2f^2\equiv 0\ (\mathrm{mod}\ q^{2h+2}),$$

so that

$$(ae+Bf)(ae-Bf)\equiv 0\ (\mathrm{mod}\ q^{2h+2}).$$

Further we have

$$a^2m^2f^2-B^2e^2\equiv mf^2(B^2+C^2)-B^2e^2\ (\mathrm{mod}\ q^{2h+2})$$
$$\equiv -B^2k^2p\ (\mathrm{mod}\ q^{2h+2})$$
$$\equiv 0\ (\mathrm{mod}\ q^{2h+2}),$$

so that

$$(amf+Be)(amf-Be)\equiv 0\ (\mathrm{mod}\ q^{2h+2}).$$

As $(q,\ aBmef)=1$ q cannot divide both of $ae+Bf$, $ae-Bf$ nor both of $amf+Be$, $amf-Be$. Since q divides $amf+Be$ and $ae+Bf$ we must have

$$q^{2h+2}\,|\,amf+Be,\qquad q^{2h+2}\nmid ae+Bf.$$

This contradicts the definition of h. Thus every odd prime divisor of $(Af+Be,\ ae+Bf)$ must divide $(Af+Be,\ ae+Bf)$ to an even power, so that as $(Af+Be,\ ae+Bf)$ is odd we have

$$(Af+Be,\ ae+Bf)=l^2,$$

where l is an odd positive integer. It is easy to check that $(l,\ maBefp)=1$. We just show that $(l,\ p)=1$. For suppose $p\,|\,l$ then we have $p\,|\,Af+Be$, giving

$$mC^2f^2\equiv mC^2f^2-B^2(e^2-mf^2)\ (\mathrm{mod}\ p)$$
$$\equiv A^2f^2-B^2e^2\ (\mathrm{mod}\ p)$$
$$\equiv 0\ (\mathrm{mod}\ p),$$

which is impossible as $p\nmid m$, $p\nmid C$, $p\nmid f$.

This completes the proof of Lemma 7.

LEMMA 8. *With the notation of Lemmas* 1, 7 *and Table* 2, *we set*

$$Af+Be = l^2 t, \quad ae+Bf = l^2 u, \tag{2.20}$$

so that t *and* u *are positive integers such that*

$$(t, u) = 1 \tag{2.21}$$

and

$$t \equiv 1 \pmod 2, \quad u \equiv \begin{cases} 0 \pmod 2, & \text{in case IX,} \\ 1 \pmod 2, & \text{otherwise.} \end{cases} \tag{2.22}$$

Then there exists a positive integer v *such that*

$$Ck = l^2 v, \tag{2.23}$$

$$t^2 - mu^2 = -pv^2. \tag{2.24}$$

Moreover setting

$$u = 2^\theta u^*, \quad u^* \equiv 1 \pmod 2, \quad \theta \geqslant 0, \tag{2.25}$$

so that $\theta = 0$ *except in case* IX, *we have*

$$\left(\frac{Af+Be}{p}\right) = \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{2}{Bkt}\right)^\mu \left(\frac{p}{m^*}\right)_4 \tag{2.26}$$

and

$$\left(\frac{ae+Bf}{p}\right) = \left(\frac{-1}{u^*}\right)^{(p+1)/2}. \tag{2.27}$$

Proof. Appealing to (2.19) and (2.20) we obtain

$$l^4(t^2 - mu^2) = -C^2 k^2 p. \tag{2.28}$$

As p is an odd prime, which is coprime with l, we have $l^2 \mid Ck$, so that there is a positive integer v such that $Ck = l^2 v$, which is (2.23). Then from (2.29) we obtain $t^2 - mu^2 = -pv^2$, which is (2.24). As $(t, u) = 1$ and m is squarefree, it is easy to verify that

$$(t, v) = (t, p) = (u, v) = (t, m) = (v, m) = (u, p) = 1. \tag{2.29}$$

Next we have

$$\begin{aligned} \left(\frac{Af+Be}{p}\right) &= \left(\frac{l^2 t}{p}\right) && \text{(by (2.20))} \\ &= \left(\frac{t}{p}\right) && \text{(by (2.18))} \\ &= \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{p}{t}\right) && \text{(by LQR)} \end{aligned}$$

$$\begin{aligned} &= \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{pv^2}{t}\right) && \text{(by (2.29))} \\ &= \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{mu^2 - t^2}{t}\right) && \text{(by (2.24))} \\ &= \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{m}{t}\right) && \text{(by (2.21))} \\ &= \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{2}{t}\right)^\mu \left(\frac{m^*}{t}\right) && \text{(by (2.8))} \\ &= \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{2}{t}\right)^\mu \left(\frac{t}{m^*}\right) && \text{(by LQR)} \\ &= \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{2}{t}\right)^\mu \left(\frac{l^2 t}{m^*}\right) && \text{(by (2.18))} \\ &= \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{2}{t}\right)^\mu \left(\frac{Af+Be}{m^*}\right) && \text{(by (2.20))} \\ &= \left(\frac{-1}{t}\right)^{(p-1)/2} \left(\frac{2}{Bkt}\right)^\mu \left(\frac{p}{m^*}\right)_4 && \text{(by Lemma 6).} \end{aligned}$$

This completes the proof of (2.26).

Also we have

$$\begin{aligned} \left(\frac{ae+Bf}{p}\right) &= \left(\frac{l^2 u}{p}\right) && \text{(by (2.20))} \\ &= \left(\frac{2}{p}\right)^\theta \left(\frac{u^*}{p}\right) && \text{(by (2.18), (2.25))} \\ &= \left(\frac{2}{p}\right)^\theta \left(\frac{-1}{u^*}\right)^{(p-1)/2} \left(\frac{p}{u^*}\right) && \text{(by LQR)} \\ &= \left(\frac{2}{p}\right)^\theta \left(\frac{-1}{u^*}\right)^{(p-1)/2} \left(\frac{pv^2}{u^*}\right) && \text{(by (2.29))} \\ &= \left(\frac{2}{p}\right)^\theta \left(\frac{-1}{u^*}\right)^{(p-1)/2} \left(\frac{mu^2 - t^2}{u^*}\right) && \text{(by (2.24))} \\ &= \left(\frac{2}{p}\right)^\theta \left(\frac{-1}{u^*}\right)^{(p+1)/2} \\ &= \left(\frac{-1}{u^*}\right)^{(p+1)/2}. \end{aligned}$$

This completes the proof of (2.27).

LEMMA 9. *With the notation of Lemmas* 1, 7, 8 *and Table* 2, *we have*

$$\left(\frac{A+B\sqrt{m}}{p}\right)=\left(\frac{-1}{tf^*}\right)^{(p-1)/2}\left(\frac{2}{p}\right)^{\zeta}\left(\frac{2}{Bkt}\right)^{\mu}\left(\frac{p}{m^*}\right)_4 \tag{2.30}$$

and

$$\left(\frac{A+B\sqrt{m}}{p}\right)=\left(\frac{-1}{u^*e^*}\right)^{(p+1)/2}\left(\frac{2}{pm^*}\right)^{\varepsilon}\left(\frac{2}{ke^*}\right)^{\mu}\left(\frac{p}{m^*}\right)_4. \tag{2.31}$$

Proof. Equation (2.30) follows from the equation

$$\left(\frac{f}{p}\right)\left(\frac{A+B\sqrt{m}}{p}\right)=\left(\frac{Af+Be}{p}\right)$$

by appealing to (2.13) and (2.26).

Equation (2.31) follows from the equation

$$\left(\frac{e}{p}\right)\left(\frac{A+B\sqrt{m}}{p}\right)=\left(\frac{ae+Bf}{p}\right)$$

by appealing to (2.12) and (2.27).

LEMMA 10. *With the notation of Lemmas* 1, 7, 8 *and Table* 2, *in case* II *we have*

$$\left(\frac{2}{Bkt}\right)=(-1)^{(p-1)/8},$$

and in case IX *we have*

$$\left(\frac{2}{ke}\right)=(-1)^{(p+m-1)/8}.$$

Proof. In case II we have

$$\left(\frac{2}{Bet}\right)=\left(\frac{2}{Bel^2t}\right)=\left(\frac{2}{Be(Af+Be)}\right)=\left(\frac{2}{ABef+B^2e^2}\right)=\left(\frac{2}{ABef+1}\right)=(-1)^{f/2},$$

and

$$\left(\frac{2}{ke}\right)=\left(\frac{2}{k}\right)^{-p}\left(\frac{2}{e}\right)=(-1)^{(-(k^2-1)p+(e^2-1))/8}$$
$$=(-1)^{mf^2/8+(p-1)/8}=(-1)^{f/2+(p-1)/8},$$

so

$$\left(\frac{2}{Bkt}\right)=\left(\frac{2}{Bet}\right)\left(\frac{2}{ke}\right)=(-1)^{(p-1)/8}$$

as required.

In case IX, similarly to above, we have

$$\left(\frac{2}{ke}\right)=(-1)^{(p-1+mf^2)/8}=(-1)^{(p+m-1)/8}$$

as required.

Proof of theorem. The theorem now follows by a case by case examination from (2.30) of Lemma 9 when $p\equiv 1\pmod 4$ and from (2.31) of Lemma 9 when $p\equiv 3\pmod 4$ together with Lemma 10 in Cases II and IX.

3. Tables. A DEC Professional 350 minicomputer was programmed to calculate A, B, C, e, f, k, $\left(\frac{A+B\sqrt{m}}{p}\right)$, $\left(\frac{p}{m^*}\right)_4$, etc. for a variety of values of m (<200) and primes p (<150). Tables of these values were used effectively in checking results and in formulating the correct form of the theorem. For the convenience of the reader a short list of these values is given below.

Table 3

m	A	B	C	p	$\left(\frac{A+B\sqrt{m}}{p}\right)$	$(-1)^{(p-1)(m-1)/8}$	$\left(\frac{2}{p}\right)^B$	$\left(\frac{m}{p}\right)_4$
5	25	2	11	19	1	−1	1	−1
5	65	2	29	11	−1	−1	1	1
13	65	1	18	17	−1	1	1	−1
13	65	6	17	23	1	−1	1	−1
17	17	1	4	13	−1	1	−1	1
17	17	4	1	13	1	1	1	1
29	29	2	5	7	−1	−1	1	1
29	29	5	2	7	−1	−1	1	1
37	37	1	6	7	−1	−1	1	1
37	37	6	1	7	−1	−1	1	1
41	41	4	5	23	1	1	1	1
41	41	5	4	23	1	1	1	1
53	53	2	7	11	1	−1	1	−1
53	53	7	2	11	−1	−1	−1	−1
61	61	5	6	13	−1	1	−1	1
61	61	6	5	13	1	1	1	1
65	65	1	8	29	1	1	−1	−1
65	65	4	7	29	−1	1	1	−1
73	73	3	8	19	1	1	−1	−1
73	73	8	3	19	−1	1	1	−1
85	85	2	9	19	−1	−1	1	1
85	85	6	7	19	−1	−1	1	1
89	89	5	8	11	−1	1	−1	1
89	89	8	5	11	1	1	1	1
97	97	4	9	11	−1	1	1	−1
97	97	9	4	11	1	1	−1	−1

m	A	B	C	p	$\left(\frac{A+B\sqrt{m}}{p}\right)$	$(-1)^{(p-1)/8}$, if $p\equiv 1(8)$ $(-1)^{(p+m-1)/8}$, if $p\equiv 7(8)$	$\left(\frac{p}{m/2}\right)_4$
10	50	9	13	31	−1	−1	1
10	50	13	9	31	−1	−1	1
26	130	11	23	17	−1	1	−1
26	130	17	19	23	−1	1	−1
34	34	3	5	47	1	1	1
34	170	3	29	47	1	1	1
58	58	3	7	23	1	1	1
58	58	7	3	23	1	1	1
74	74	5	7	41	1	−1	−1
74	74	7	5	41	1	−1	−1
82	82	1	9	23	−1	−1	1
82	82	9	1	23	−1	−1	1

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

[3] — *On a theorem of Barrucand*, Bollettino U. M. I. (4), 12 (1975), pp. 50–55.

[4] Klaus Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. 235 (1969), pp. 175–184.

[5] Dennis R. Estes and Gordon Pall, *Spinor genera of binary quadratic forms*, J. Number Theory 5 (1973), pp. 421–432.

[6] Yoshiomi Furuta, *Norm of units of quadratic fields*, J. Math. Soc. Japan 11 (1959), pp. 139–145.

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

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

[9] — *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. 250 (1971), pp. 42–48.

[10] Arnold Scholz, *Über die Lösbarkeit der Gleichung $t^2-Du^2=-4$*, Math. Zeit. 39 (1934), pp. 95–111.

[11] Hugh C. Williams, *The quadratic character of a certain quadratic surd*, Utilitas Math. 5 (1974), pp. 49–55.

[12] K. S. Williams, *On Scholz's reciprocity law*, Proc. Amer. Math. Soc. 64 (1977), pp. 45–46.

[13] — *Note on Burde's rational biquadratic reciprocity law*, Canad. Math. Bull. 20 (1977), pp. 145–146.

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

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF NEW BRUNSWICK
Fredericton, New Brunswick, Canada E3B 5A3

Received on 16.12.1983 (1389)

ACTA ARITHMETICA
XLV (1985)

The divisor problem for arithmetic progressions

by

J. B. Friedlander* and H. Iwaniec* (Princeton, N. J.)

1. Introduction. Let $n \geqslant 1$ and $r \geqslant 2$ be integers and let $d_r(n)$ denote the number of ordered r-tuples $(n_1, \ldots, n_r)$ of positive integers for which $\prod_{1\leqslant j\leqslant r} n_j = n$.

For $(a, q) = 1$ define

$$D_r(X, q, a) = \sum_{\substack{n\leqslant X\\ n\equiv a(\mathrm{mod}\, q)}} d_r(n).$$

We are interested here in finding real numbers θ_r, as large as possible, such that the following statement holds.

(S) *For each $\varepsilon > 0$ there exists $\delta > 0$ such that*

$$D_r(X, q, a) - \frac{X}{\varphi(q)} P_r(\log X) \ll_\varepsilon \frac{X^{1-\delta}}{\varphi(q)},$$

provided that $q < X^{\theta_r-\varepsilon}$.

Here $P_r(\log X)$ is the residue at $s = 1$ of $s^{-1} L(s, \chi_0) X^{s-1}$, where χ_0 is the principal character of modulus q.

It was discovered independently by Selberg and by Hooley that Weil's estimate for the Kloosterman sum yielded the above statement with $\theta_2 = 2/3$. The authors [2] recently proved that one may take $\theta_3 = 1/2+1/230$. The result with $\theta_4 = 1/2$ seems harder to trace but was known to Linnik. In this paper we are able to improve the results $\theta_r = 8/(3r+4)$ for $r \geqslant 5$ which are due to Lavrik [5].

Theorem. *The statement* (S) *holds in the following cases*:

(I) $\theta_5 = 9/20$,

(II) $r \geqslant 6$ *and* $\theta_r = \min\{8/3r,\ 5/12\}$,

(III) *q is restricted to cube-free integers*, $r \geqslant 7$, *and* $\theta_r = \min\{4/r,\ 5/12\}$.

Although the proof of this result involves some fairly deep arguments, these are for the most part already recorded in the literature and we shall quote liberally therefrom.

* Supported in part by NSF grant MCS-8108814(A02).