A DETERMINISTIC ALGORITHM FOR SOLVING
\[ n = fu^2 + gv^2 \] IN COPRIME INTEGERS \( u \) AND \( v \)

KENNETH HARDY, JOSEPH B. MUSKAT, AND KENNETH S. WILLIAMS

Abstract. We give a deterministic algorithm for finding all primitive representations of a natural number \( n \) in the form \( fu^2 + gv^2 \), where \( f \) and \( g \) are given positive coprime integers, and \( n > f + g + 1 \), \( (n, fg) = 1 \). The running time of this algorithm is at most
\[
\Theta \left( n^{1/4} (\log n)^3 (\log \log n)(\log \log \log n) \right),
\]
uniformly in \( f \) and \( g \).

1. Introduction

Throughout this paper, \( f \) and \( g \) denote integers such that
\[
(1.1) \quad f \geq 1, \quad g \geq 1, \quad (f, g) = 1,
\]
and \( n \) denotes an integer such that
\[
(1.2) \quad n > f + g + 1, \quad (n, fg) = 1.
\]
We are interested in the problem of determining all positive integers \( u \) and \( v \) (if any) such that
\[
(1.3) \quad n = fu^2 + gv^2, \quad (u, v) = 1.
\]
If \( (u, v) \) is a solution of (1.3) in positive integers, then
\[
(1.4) \quad (u, n) = (v, n) = 1,
\]
and
\[
(1.5) \quad u \neq v.
\]
In view of (1.4), we see that \( v^{-1}(\mod n) \) exists, and so we can define an integer \( y \) by \( y \equiv uv^{-1} \pmod{n} \), \( 0 \leq y < n \). Clearly, \( (n, y) = 1 \), and \( y \) is a solution of \( fy^2 \equiv -g \pmod{n} \). In particular, we have \( y \neq 0 \), and \( y \neq n/2 \) if \( n \) is even. Replacing \( y \) by \( n - y \), if necessary, we obtain a solution \( y \) of \( fy^2 \equiv -g \pmod{n} \) satisfying \( y \equiv \pm uv^{-1} \pmod{n} \) and \( 0 < y < n/2 \).
Conversely, suppose \( y \) is a solution of
\[
fy^2 \equiv -g \pmod{n}, \quad 0 < y < n/2.
\]
Note that if (1.6) is insolvable, then so is (1.3). We define the (possibly empty) set \( U(f, g, n, y) \) to be the set of pairs of integers \((u, v)\) satisfying:
\[
\begin{aligned}
&\begin{cases}
n = fu^2 + gv^2, \quad (u, v) = 1, \quad uv^{-1} \equiv \pm y \pmod{n}, \\
&\quad \text{with } \begin{cases} u \geq 1, \quad v \geq 1 & \text{if } fg \geq 2, \\
&\quad \quad \quad u > v \geq 1 & \text{if } fg = 1.
\end{cases}
\end{cases}
\end{aligned}
\]
It is easily shown along the lines of the proof given in [18, pp. 332-335] that either \( U(f, g, n, y) \) is empty or contains exactly one pair of integers. The main result of this paper is the following theorem which is proved in \( \S 2 \).

**Theorem 1.** Let \( y \) be an integer satisfying (1.6) for which \( U(f, g, n, y) \) is nonempty. Let
\[
r_0 (= y) > r_1 > \cdots > r_{s-1} (= 1) > r_s (= 0)
\]
be the remainders obtained by applying the Euclidean algorithm to \( y \) and \( n \). Let \( r_k \) \((0 \leq k \leq s)\) be the first remainder \(< \sqrt{n/f} \). Then we have
\[
U(f, g, n, y) = \{(u, v)\},
\]
where
\[
u = r_k, \quad v = \sqrt{(n - fr_k^2)/g}.
\]

Theorem 1 enables us to give a simple algorithm for finding all the solutions (if any) of (1.3) in positive integers \( u \) and \( v \) as follows:

**Algorithm.** First determine all the solutions \( y \) of \( fy^2 \equiv -g \pmod{n} \), \( 0 < y < n/2 \). For each solution \( y \), apply the Euclidean algorithm to \( y \) and \( n \), and let \( r = r(f, g, n, y) \) denote the first remainder \(< \sqrt{n/f} \). Then all solutions \((u, v)\) of (1.3) (with \( u > v \) if \( fg = 1 \)) lie among the pairs \((r, \sqrt{(n - fr^2)/g})\).

A deterministic version of this algorithm is described and analyzed in \( \S 4 \), see Theorem 3.

Theorem 2 below, which is proved in \( \S 3 \), gives an alternative expression for \( v \) to that given in (1.10). We remark that Theorem 2 is not needed in the algorithm.

**Theorem 2.** With the notation of Theorem 1, we have
\[
v = \begin{cases} 
1 & \text{if } k = 0, \\
r_{k+1} & \text{if } k \geq 1, \quad fg = 1, \\
(r_{k-1} - cr_k)/g & \text{if } k \geq 1, \quad fg \geq 2,
\end{cases}
\]
and \( c \) is the unique integer satisfying
\[
r_k c \equiv r_{k-1} + (-1)^k fy r_k \pmod{n}, \quad 0 \leq c < n.
\]
A DETERMINISTIC ALGORITHM FOR SOLVING \( n = fu^2 + gv^2 \)

We remark that Brillhart’s modification [3] of the Hermite-Serret algorithm [8, 15] for solving \( p = u^2 + v^2 \), where \( p \equiv 1 \pmod{4} \) is prime, is a special case of Theorem 2. Our algorithm also contains those of Cornacchia [6] and Wilker [19] as special cases. Our proof is different from that of Brillhart in that the palindromic nature of the continued fraction used in [3] does not always hold.

2. The integers \( c_i \) and \( d_i \) and the proof of Theorem 1

Let \( y \) be an integer satisfying (1.6) for which

\[ U(f, g, n, y) \neq \emptyset. \tag{2.1} \]

By the remarks following (1.7), there is a unique pair of integers \((u, v)\) such that

\[ \begin{cases} n = fu^2 + gv^2, & (u, v) = 1, \quad uv^{-1} \equiv \pm y \pmod{n}, \\ \text{with} & \begin{cases} u \geq 1, & v \geq 1 \quad \text{if } fg \geq 2, \\ u > v \geq 1 & \text{if } fg = 1. \end{cases} \end{cases} \tag{2.2} \]

We define \( \epsilon \) \((= \pm 1)\) to be the unique integer satisfying

\[ y \equiv \epsilon uv^{-1} \pmod{n}. \tag{2.3} \]

Applying the Euclidean algorithm to \( y \) and \( n \), we obtain

\[ \begin{align*}
\begin{cases}
y = q_0n + r_0, \\
n = q_1r_0 + r_1, \\
r_{i-2} = q_ir_{i-1} + r_i \quad (i = 2, \ldots, s),
\end{cases}
\end{align*} \tag{2.4} \]

where

\[ s \geq 1, \tag{2.5} \]

\[ r_0 (= y) > r_1 > r_2 > \cdots > r_{s-1} (= 1) > r_s (= 0), \tag{2.6} \]

and

\[ q_0 = \lfloor y/n \rfloor = 0, \quad q_1 = \lfloor n/r_0 \rfloor = \lfloor n/y \rfloor \geq 2, \]

\[ q_i = \lfloor r_{i-2}/r_{i-1} \rfloor \geq 1 \quad (i = 2, \ldots, s). \tag{2.7} \]

The continued fraction for \( y/n \) is

\[ \frac{y}{n} = [q_0, q_1, q_2, \ldots, q_s]. \tag{2.8} \]

The \( i \)th convergent to \( y/n \) is

\[ \frac{A_i}{B_i} = [q_0, q_1, q_2, \ldots, q_i] \quad (i = 0, 1, \ldots, s), \tag{2.9} \]

so that, in particular, we have

\[ \begin{align*}
A_0 &= 0, & B_0 &= 1, \\
A_1 &= 1, & B_1 &= q_1, \\
A_2 &= q_2, & B_2 &= q_1q_2 + 1, \\
& \vdots & & \vdots \\
A_s &= y, & B_s &= n \tag{2.10}.
\end{align*} \]
Moreover, we have
\begin{align}
A_i &= q_i A_{i-1} + A_{i-2} \quad (i = 2, \ldots, s), \\
B_i &= q_i B_{i-1} + B_{i-2} \quad (i = 2, \ldots, s).
\end{align}
(2.11)

From (2.4) and (2.11), we obtain, for \( i = 1, \ldots, s - 1 \),
\((B_{i+1} - B_{i-1})r_i = q_{i+1}B_ir_i = (r_{i-1} - r_{i+1})B_i,
so that
\[ r_iB_{i+1} + r_{i+1}B_i = r_{i-1}B_i + r_iB_{i-1} \quad (i = 1, \ldots, s - 1), \]
and so, for \( i = 1, \ldots, s - 1 \), we have
\[ r_iB_{i+1} + r_{i+1}B_i = r_0B_1 + r_1B_0 = r_0q_1 + r_1 = n, \]
and thus
\[ r_iB_{i+1} + r_{i+1}B_i = n \quad (i = 0, 1, \ldots, s - 1). \]
(2.12)

An easy induction argument on \( i \), using (2.4), (2.6), and (2.11), shows that
\[ r_i = (-1)^i(B_iv - A_in) \quad (i = 0, 1, \ldots, s), \]
so that
\[ r_i \equiv (-1)^iB_iv \pmod{n} \quad (i = 0, 1, \ldots, s). \]
(2.13)

From (2.2), (2.3), and (2.14), we see that for \( i = 0, 1, \ldots, s \),
\begin{align}
\begin{cases}
fr_iu + \varepsilon (-1)^i gB_iv &\equiv 0 \pmod{n}, \\
r_iu - \varepsilon (-1)^i B_iv &\equiv 0 \pmod{n}.
\end{cases}
\end{align}
(2.15)

Hence, we may define integers \( c_i \) and \( d_i \) \( (i = 0, 1, \ldots, s) \) by
\begin{align}
\begin{cases}
c_i = (fr_iu + \varepsilon (-1)^i gB_iv)/n, \\
d_i = (ru - \varepsilon (-1)^i Biv)/n.
\end{cases}
\end{align}
(2.16)

Using (2.2), (2.4), (2.11), and (2.16), it is easy to show that
\begin{align}
\begin{cases}
c_i = -q_ic_{i-1} + c_{i-2} \quad (i = 2, 3, \ldots, s), \\
d_i = -q_id_{i-1} + d_{i-2} \quad (i = 2, 3, \ldots, s),
\end{cases}
\end{align}
(2.17)

\[ c_i^2 + fg d_i^2 = (fr_i^2 + gB_i^2)/n \quad (i = 0, 1, \ldots, s), \]
(2.18)

and
\[ c_id_{i+1} - c_{i+1}d_i = (-1)^i \varepsilon \quad (i = 0, 1, \ldots, s - 1). \]
(2.19)

We note that
\begin{align}
&c_0 = (fyu + \varepsilon gv)/n, \quad d_0 = (yu - \varepsilon u)/n, \\
c_1 = fu - q_1c_0, \quad d_1 = v - q_1d_0, \\
c_s = \varepsilon (-1)^sgv, \quad d_s = \varepsilon (-1)^{s+1}u.
\end{align}
(2.20)

We emphasize that \( c_s \) and \( d_s \) are nonzero.
Lemma 1. Suppose that $c_i = 0$ for some integer $i$ with $0 \leq i \leq s - 1$. Set

$$a = \begin{cases} 
0, & i \text{ even}, \\
1, & i \text{ odd}, 
\end{cases} \quad b = \begin{cases} 
0, & s - i \text{ even}, \\
1, & s - i \text{ odd}. 
\end{cases}$$

Then we have $\varepsilon = (-1)^{i+1}$ and

(a) $c_i > \cdots > c_{i-2} > c_i = 0 > c_{i+2} > \cdots > c_{s-b},$

(b) $c_{i-a} > \cdots > c_{i-3} > c_{i-1} = 1 = c_{i+1} < c_{i+3} < \cdots < c_{s-(1-b)},$

(c) $d_{i-a} > \cdots > d_{i-1} > d_{i+1} > d_{i+3} > \cdots > d_{s-(1-b)}$, where at most one of the equality signs holds, and

(d) $d_a > \cdots > d_{i-2} \geq d_i = 1 \leq d_{i+2} \cdots < d_{s-b}.$

Proof. As $c_i = 0$, appealing to (2.16), we obtain $fr_iu = \varepsilon(-1)^{i+1} gB_i v$. Now $r_i \geq 1$, as $0 \leq i \leq s - 1$, and so, as $f, g, u, v, B_i$ are all positive, we see that $\varepsilon = (-1)^{i+1}$.

For $0 \leq i \leq s - 1$, from (2.19), we obtain $c_{i+1}d_i = (-1)^{i+1}\varepsilon = 1$. As $c_{i+1}$ and $d_i$ are both integers, we must have $c_{i+1} = d_i = \pm 1$. But, from (2.16), we obtain $d_i = (r_i u + B_i u)/n > 0$, so we must have

$$c_{i+1} = d_i = 1 \quad (0 \leq i \leq s - 1).$$

For $1 \leq i \leq s - 1$, from (2.19), we obtain (as $c_i = 0$, $d_i = 1$)

$$c_{i-1} = 1 \quad (1 \leq i \leq s - 1).$$

For $0 \leq i \leq s - 2$, from (2.16), we have

$$c_i - c_{i+2} = (fu(r_i - r_{i+2}) + g v(B_{i+2} - B_i))/n > 0,$$

so that $c_{i+2} < 0 \quad (0 \leq i \leq s - 2).$

For $2 \leq i \leq s - 1$, from (2.16), we obtain

$$c_{i-2} - c_i = (fu(r_{i-2} - r_i) + g v(B_i - B_{i-2}))/n > 0,$$

so that $c_{i-2} > 0 \quad (2 \leq i \leq s - 1).$

For $2 \leq i \leq s - 1$, from (2.16), we obtain

$$d_{i-2} = (r_{i-2} u + B_{i-2} u)/n > 0,$$

so that $d_{i-2} \geq 1 \quad (2 \leq i \leq s - 1)$. Further, for $2 \leq i \leq s - 1$, appealing to (2.19), we obtain

$$c_{i-2}d_{i-1} - c_{i-1}d_{i-2} = (-1)^{i-2} = -1,$$

so that $c_{i-2}d_{i-1} = d_{i-2} - 1 \geq 0$, and thus $d_{i-1} \geq 0 \quad (2 \leq i \leq s - 1)$. This inequality is also true for $i = 1$ as we now show. When $i = 1$ we have $\varepsilon = 1$, $c_0 = 1$, and so, by (2.20),

$$n = nc_0 = fu + gv \quad \text{and} \quad n = fu + gv \quad \text{and}$$

$$d_0 = \frac{v(u - u)}{n} = \frac{fu v - f u^2}{fu} = \frac{fu v - (n - gv^2)}{fu} = \frac{v(fu v + gv) - n}{fu} = \frac{v - 1}{fu} \geq 0.$$ 

Hence we have $d_{i-1} \geq 0 \quad (1 \leq i \leq s - 1).$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
For $0 \leq i \leq s - 2$, from (2.16), we obtain $d_{i+2} = (r_{i+2}v + B_{i+2}u)/n > 0$, so that $d_{i+2} \geq 1$ ($0 \leq i \leq s - 2$). Further, for $0 \leq i \leq s - 2$, from (2.19), we have $c_{i+1}^2d_{i+1}^2 - c_{i+2}^2d_{i+1}^2 = 1$, so that $c_{i+2}^2d_{i+1} = d_{i+2} - 1 \geq 0$, and thus $d_{i+1} \leq 0$ ($0 \leq i \leq s - 2$). But the last inequality also holds for $i = s - 1$, as $d_{s+1} = d_{s} = e(-1)^{s-1}u = -u < 0$. Hence we have $d_{i+1} \leq 0$ ($0 \leq i \leq s - 1$).

For $a < t < s - b - 2$ and $t \equiv i \pmod{2}$, we have, by (2.16),

$$c_t - c_{t+2} = \frac{(fu(r_t - r_{t+2}) + gv(B_{t+2} - B_t))/n}{n} > 0,$$

so that $c_t > c_{t+2}$ ($a \leq t \leq s - b - 2$, $t \equiv i \pmod{2}$). This completes the proof of (a).

For $1 - a \leq t < i - 3$ and $t \equiv i + 1 \pmod{2}$, we have, by (2.17) and (a),

$$c_t - c_{t+2} = q_{t+2}c_{t+1} \geq q_{t+2}c_{t-2} > 0,$$

so that $c_t > c_{t+2}$ ($1 - a \leq t < i - 3$, $t \equiv i + 1 \pmod{2}$). For $i + 1 \leq t \leq s - 3 + b$ and $t \equiv i + 1 \pmod{2}$, we have, by (2.17) and (a),

$$c_t - c_{t+2} = q_{t+2}c_{t+1} \leq q_{t+2}c_{t+2} < 0,$$

so that $c_t < c_{t+2}$ ($i + 1 \leq t \leq s - 3 + b$, $t \equiv i + 1 \pmod{2}$). This completes the proof of (b).

For $1 - a \leq t < s - 3 + b$ and $t \equiv i + 1 \pmod{2}$, we have, by (2.16),

$$d_t - d_{t+2} = \frac{(r_t - r_{t+2})v + (B_{t+2} - B_t)u)/n}{n} > 0,$$

so that $d_t > d_{t+2}$ ($1 - a \leq t < s - 3 + b$, $t \equiv i + 1 \pmod{2}$). This completes the proof of (c).

For $a \leq t < i - 4$ and $t \equiv i \pmod{2}$, we have, by (2.17) and (c),

$$d_t - d_{t+2} = q_{t+2}d_{t+1} \geq q_{t+2}d_{t-3} > 0,$$

so that $d_t > d_{t+2}$ ($a \leq t < i - 4$, $t \equiv i \pmod{2}$).

For $i + 2 \leq t < s - 2 - b$ and $t \equiv i \pmod{2}$, we have, by (2.17) and (c),

$$d_t - d_{t+2} = q_{t+2}d_{t+1} \leq q_{t+2}d_{t+3} < 0,$$

so that $d_t < d_{t+2}$ ($i + 2 \leq t < s - 2 - b$, $t \equiv i \pmod{2}$). This completes the proof of (d). The proof of Lemma 1 is now complete. □

**Lemma 2.** Suppose that $d_i = 0$ for some integer $i$ with $0 \leq i \leq s - 1$. Set

$$a = \left\{ \begin{array}{ll} 0, & i \text{ even,} \\ 1, & i \text{ odd,} \end{array} \right. \quad b = \left\{ \begin{array}{ll} 0, & s - i \text{ even,} \\ 1, & s - i \text{ odd.} \end{array} \right.$$

Then we have $e = (-1)^i$ and

(a) $c_{i-a} > \cdots > c_{i-1} \geq 0 \geq c_{i+1} > \cdots > c_{s-(1-b)}$, where at most one of the equality signs holds,

(b) $c_a > \cdots > c_{i-4} > c_{i-2} \geq c_i = 1 \leq c_{i+2} < c_{i+4} < \cdots < c_{s-b}$,

(c) $d_a > \cdots > d_{i-2} > d_i = 0 > d_{i+2} > \cdots > d_{s-b}$, and

(d) $d_{i-a} > \cdots > d_{i-3} > d_{i-1} = 1 = d_{i+1} < d_{i+3} < \cdots < d_{s-(1-b)}$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
A DETERMINISTIC ALGORITHM FOR SOLVING \( n = fu^2 + gv^2 \)

\[ \frac{c_p}{c_q} = 0 \text{ with } 0 \leq p \leq q \leq s - 1, \text{ then } p = q. \]

\[ \frac{d_p}{d_q} = 0 \text{ with } 0 \leq p \leq q \leq s - 1, \text{ then } p = q. \]

\[ \frac{c_p}{d_q} = 0 \text{ with } 0 \leq p \leq s - 1, 0 \leq q \leq s - 1, \text{ then either } p = q + 1 \] or \( p = q - 1. \)

Proof. (a) Immediate from Lemma 1(a), (b).

(b) Immediate from Lemma 2(c), (d).

(c) Immediate from Lemma 1 (or from Lemma 2). \( \square \)

We now define the nonnegative integers \( k \) and \( j \) which are central to the proofs of Theorems 1 and 2. We let \( r_k (0 \leq k \leq s) \) be the largest remainder which is less than \( \sqrt{n/f} \), and \( B_j (0 \leq j \leq s) \) the largest denominator of the convergents to \( y/n \) which is less than \( \sqrt{n/g} \). Clearly, \( r_{s-1} = 1 < \sqrt{n/f} \), showing that \( 0 \leq k \leq s - 1 \). Also we have \( \sqrt{n/g} \leq \sqrt{n} < n = B_s \), so that \( 0 \leq j \leq s - 1 \).

If \( k = 0 \), then \( y = r_0 < \sqrt{n/f} \), \( fy^2 + g \equiv 0 \pmod{n} \), \( fy^2 + g < 2n \), so that \( n = fy^2 + g \leq 1 \), showing that \( (y, 1) \in U(f, g, n, y) \). Hence we have \( (y, 1) = (u, v) \), and so in the case \( k = 0 \) we have

\[ u = y = r_0, \quad v = 1 = B_0, \]

as asserted in Theorems 1 and 2. When \( k = 0 \) we also show that

\[ j = \begin{cases} 0 & \text{if } fg \geq 2, \\ 1 & \text{if } fg = 1, \end{cases} \]

as follows. From \( n = fy^2 + g \leq 1 \) and \( n > f + g + 1 \), we obtain \( y^2 \geq 1 + 1/f > 1 \), so that (as \( 0 < y < n/2 \)) we have \( y \geq 2 \).

We first treat the case \( fg \geq 2 \). We suppose that \( j \geq 1 \) and obtain a contradiction. We have

\[ fy \leq fy + \left[ \frac{g}{y} \right] = \left[ fy + \frac{g}{y} \right] = \left[ \frac{fy^2 + g}{y} \right] = \left[ \frac{n}{y} \right] = q_1, \]

\[ = B_1 \leq B_j < \sqrt{\frac{n}{g}} = \sqrt{\frac{fy^2 + g}{g}} = \sqrt{1 + \frac{fy^2}{g}}, \]

so that

\[ f^2 y^2 < 1 + \frac{fy^2}{g}. \]

If \( f = 1 \), we have \( g \geq 2 \), and the inequality becomes

\[ y^2 \leq 1 + \frac{y^2}{g} \leq 1 + \frac{y^2}{2}, \]

which is impossible, as \( y \geq 2 \). On the other hand, if \( f \geq 2 \), the inequality gives

\[ 2y^2 \leq f(f-1)y^2 < 1 - fy^2(g-1)/g < 1, \]

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
which is again impossible. Hence we must have $j = 0$ as claimed.

Next we treat the case $fg = 1$, that is, $f = g = 1$. In this case we have $n = fy^2 + g1^2 = y^2 + 1$, where $y \geq 2$, and the Euclidean algorithm applied to $y$ and $n$ just consists of three lines, namely

\[
\begin{align*}
    y &= 0n + y, \\
    n &= yy + 1, \\
    y &= y1 + 0,
\end{align*}
\]

so that $s = 2$, $r_0 = y$, $r_1 = 1$, $r_2 = 0$, $q_0 = 0$, and $q_1 = q_2 = y$. Thus we have

\[
B_1 = q_1 = y < \sqrt{n} < n = B_2,
\]

and $j = 1$ as claimed.

This completes the treatment of the case $k = 0$, and so from here until the end of §3, we may assume $k \geq 1$. Thus we have

(2.24) \[ r_k < \sqrt{n/f} \leq r_{k-1} \quad (1 \leq k \leq s - 1), \]

and

(2.25) \[ B_j < \sqrt{n/g} \leq B_{j+1} \quad (0 \leq j \leq s - 1). \]

We are now ready to prove Theorem 1.

**Proof of Theorem 1.** From (2.12) and (2.24), we obtain

\[
\sqrt{n/fB_k} \leq r_{k-1}B_k \leq r_{k-1}B_k + r_kB_{k-1} = n,
\]

so that

(2.26) \[ B_k \leq \sqrt{fn}. \]

From (2.12) and (2.25), we obtain

\[
\sqrt{n/gr_j} \leq r_jB_{j+1} \leq r_jB_{j+1} + r_{j+1}B_j = n,
\]

so that

(2.27) \[ r_j \leq \sqrt{gn}. \]

Then, by (2.18), (2.24), and (2.26), we have

(2.28) \[ c_k^2 + fgd_k^2 = (fr_k^2 + gB_k^2)/n < 1 + fg, \]

and, by (2.18), (2.25), and (2.27), we have

(2.29) \[ c_j^2 + fgd_j^2 = (fr_j^2 + gB_j^2)/n < fg + 1. \]

Hence, from (2.28), we deduce

(2.30) \[ d_k = 0 \quad \text{or} \quad d_k = \pm 1, \quad c_k = 0, \]

and, from (2.29), we deduce

(2.31) \[ d_j = 0 \quad \text{or} \quad d_j = \pm 1, \quad c_j = 0. \]
We first show that neither of the possibilities

\begin{enumerate}
  \item[(a)] \(d_k = \pm 1, \quad c_k = 0, \quad d_j = 0,\)
  \item[(b)] \(d_k = \pm 1, \quad c_k = 0, \quad d_j = \pm 1, \quad c_j = 0,\)
\end{enumerate}
can occur.

\begin{enumerate}
  \item[(a)] \(d_k = \pm 1, \quad c_k = 0, \quad d_j = 0.\) By Lemma 3(c) we have \(j = k + 1\) or \(j = k - 1.\) First, suppose that \(j = k + 1.\) By Lemma 1(b), (d), we have
  \[c_k = 0, \quad d_k = 1, \quad c_{k+1} = 1, \quad d_{k+1} = 0, \quad \varepsilon = (-1)^{k+1}.\]
  Appealing to (2.16), we obtain
  \[fu r_k - gv B_k = 0, \quad vr_k + u B_k = n,\]
  and
  \[fu r_{k+1} + gv B_{k+1} = n, \quad vr_{k+1} - u B_{k+1} = 0.\]
  Solving these linear equations for \(r_k, B_k\) and \(r_{k+1}, B_{k+1},\) we obtain
  \[r_k = g v, \quad B_k = f u, \quad r_{k+1} = u, \quad B_{k+1} = v.\]
  As \(r_{k+1} < r_k < \sqrt{n/f}\) and \(B_k < B_{k+1} < \sqrt{n/g},\) we deduce that
  \[u < g v < \sqrt{n/f}, \quad f u < v < \sqrt{n/g}.\]
  Further, as \(u > v\) for \(fg = 1,\) we see that \(fg \geq 2.\) Then we have
  \[1 + fg < (fg)^2 < \frac{fn}{v^2} = \frac{f^2u^2}{v^2} + fg < 1 + fg,\]
  which is impossible.
  
  Next, suppose that \(j = k - 1.\) By Lemma 1(b), (d), we have
  \[c_k = 0, \quad d_k = 1, \quad c_{k-1} = 1, \quad d_{k-1} = 0, \quad \varepsilon = (-1)^{k+1}.\]
  Appealing to (2.16), we obtain
  \[fu r_k - gv B_k = 0, \quad vr_k + u B_k = n,\]
  and
  \[fu r_{k-1} + gv B_{k-1} = n, \quad vr_{k-1} - u B_{k-1} = 0.\]
  Solving these linear equations for \(r_k, B_k\) and \(r_{k-1}, B_{k-1},\) we obtain
  \[r_k = g v, \quad B_k = f u, \quad r_{k-1} = u, \quad B_{k-1} = v.\]
  Appealing to (2.24), we obtain \(\sqrt{n/f} \leq u,\) and so
  \[n = f u^2 + g v^2 > f u^2 > n,\]
  which is impossible. Thus case (a) cannot occur.

  \begin{enumerate}
  \item[(b)] \(d_k = \pm 1, \quad c_k = 0, \quad d_j = \pm 1, \quad c_j = 0.\) By Lemma 3(a) we have \(j = k,\)
  and by Lemma 1(d) we have \(c_k = 0, \quad d_k = 1, \quad d_{k-1} = 1, \quad \varepsilon = (-1)^{k+1}.\) Appealing to (2.16), we obtain
  \[fu r_k - gv B_k = 0, \quad vr_k + u B_k = n.\]
Solving these linear equations for \( r_k \) and \( B_k \), we obtain \( r_k = g v \), \( B_k = f u \).

Then, from (2.24) and (2.25), we deduce
\[
g v < \sqrt{n/f}, \quad f u < \sqrt{n/g}.
\]

If \( f g \geq 2 \), then we have
\[
n = f u^2 + g v^2 < \frac{n}{f g} + \frac{n}{f g} = \frac{2n}{f g} \leq n,
\]
which is impossible. Thus we must have \( f g = 1 \), so that
\[
f = g = 1, \quad r_k = v, \quad B_k = u.
\]

Then, as \( c_{k-1} = 1 \) by Lemma 1(b), we obtain from (2.12) (with \( i = k - 1 \))
\( n = u r_{k-1} + v B_{k-1} \). Thus, as \((u, v) = 1\), there is an integer \( t \) such that
\[
r_{k-1} = u + vt, \quad B_{k-1} = v - ut.
\]

As \( 0 < B_{k-1} \leq B_k \) and \( u > v > 0 \), we have \(-1 < v/u - 1 \leq t < v/u < 1\), so that \( t = 0 \), and thus \( r_{k-1} = u, B_{k-1} = v \).

Then, from (2.24) and (2.25), we obtain the contradiction \( \sqrt{n} \leq u, u < \sqrt{n} \). Thus case (b) cannot occur.

Hence, from (2.30) and (2.31), we see that we must have \( d_k = 0 \). By Lemma 2(b) we have \( e = (-1)^k \) and \( c_k = 1 \). Appealing to (2.16) (with \( i = k \)), we obtain
\[
fr u r_k + g v B_k = n, \quad vr_k - u B_k = 0.
\]

Solving these linear equations for \( r_k \) and \( B_k \), we obtain \( r_k = u, B_k = v \). This completes the proof of Theorem 1. \( \square \)

We finish this section by showing that
\[
(2.32) \quad j = \begin{cases} k & \text{if } f g \geq 2, \\ k + 1 & \text{if } f g = 1. \end{cases}
\]

Equation (2.32) has already been proved when \( k = 0 \), so we may assume that \( k \geq 1 \). We have shown that
\[
(2.33) \quad c_k = 1, \quad d_k = 0, \quad e = (-1)^k, \quad r_k = u, \quad B_k = v.
\]

Hence we have \( B_k = v < \sqrt{n/g} \), so that
\[
(2.34) \quad j \geq k.
\]

From (2.31) we see that either
\[
(2.35) \quad d_j = 0
\]
or
\[
(2.36) \quad c_j = 0, \quad d_j = \pm 1.
\]

If (2.36) holds, we have \( c_j = d_j = 0 \), and so by Lemma 2(c) we have \( j = k + 1 \) or \( j = k - 1 \). The second possibility is excluded by (2.34). Thus, \( j = k + 1 \).
and \( c_{k+1} = 0, d_{k+1} = \pm 1 \). By Lemma 1(d) we deduce \( d_{k+1} = 1 \). Appealing to (2.16), we obtain

\[
fr_{k+1} - gvB_{k+1} = 0, \quad ur_{k+1} + uB_{k+1} = n.
\]

Solving for \( r_{k+1}, B_{k+1} \), we deduce \( r_{k+1} = gv, B_{k+1} = fu \). Since \( r_{k+1} < r_k < \sqrt{n/f} \) and \( B_k < B_{k+1} < \sqrt{n/g} \), we have \( gv < u < \sqrt{n/f} \) and \( u < fu < \sqrt{n/g} \), so that

\[
n = fu^2 + gv^2 < f \left( \frac{1}{g} \sqrt{\frac{n}{f}} \right)^2 + g \left( \frac{1}{g} \sqrt{\frac{n}{f}} \right)^2 = \frac{n}{fg} + \frac{n}{fg} = \frac{2n}{fg}.
\]

But this is a contradiction when \( fg \geq 2 \). Hence (2.35) holds when \( fg \geq 2 \) and so, by Lemma 3(b), we have \( j = k \) as asserted.

Finally, we treat the case \( fg = 1 \), that is, \( f = g = 1 \). If (2.35) holds, we have \( d_k = d_j = 0 \), and so, by Lemma 3(b), we have \( j = k \). By Lemma 2(a), (d), we obtain \( 0 \geq c_{k+1}, d_{k+1} = 1 \). By (2.16) we have

\[
ur_{k+1} - vB_{k+1} = c_{k+1}n, \quad vr_{k+1} + uB_{k+1} = n.
\]

Solving for \( r_{k+1}, B_{k+1} \), we deduce

\[
r_{k+1} = v + c_{k+1}u, \quad B_{k+1} = u - c_{k+1}v.
\]

Since \( 0 \leq r_{k+1} < r_k \) and \( B_k < \sqrt{n} \leq B_{k+1} \), we have

\[
0 \leq v + c_{k+1}u < u
\]

and

\[
v < \sqrt{n} \leq u - c_{k+1}v.
\]

But, by (1.7), we have \( u > v \), so that by (2.37)

\[-1 < -v/u \leq c_{k+1} < 1 - v/u < 1,
\]

and so \( c_{k+1} = 0 \). But then from (2.38) we have \( u \geq \sqrt{n} \), contradicting \( u < \sqrt{n} \). Hence, (2.36) must hold, and so \( j = k + 1 \) as before.

This completes the proof of (2.32). \( \square \)

3. Proof of Theorem 2

In §2 we showed that \( c_k = 1, d_k = 0, e = (-1)^k, u = r_k, \) and \( v = B_k \). Thus, to prove Theorem 2, we must show that

\[
B_k = \begin{cases} 
fr_{k+1} & \text{if } k \geq 1, \ fg = 1, \\
(r_{k-1} - cr_k)/g & \text{if } k \geq 1, \ fg \geq 2.
\end{cases}
\]

We first suppose that \( k \geq 1 \) and \( fg = 1 \). From the analysis at the end of §2 we have \( c_{k+1} = 0, \) and \( r_{k+1} = v, B_{k+1} = u \). Hence, \( B_k = v = r_{k+1} \) as required.

Next we suppose that \( k \geq 1 \) and \( fg \geq 2 \). As \( (u, n) = 1 \), we have \( (r_k, n) = 1 \), and so the congruence

\[
r_k c \equiv r_{k-1} + (-1)^k f vr_k \pmod{n}, \quad 0 \leq c < n,
\]

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
has a unique solution $c$. From (2.16) (with $i = k - 1$), recalling that $e = (-1)^k$ and noting that $d_{k-1} = 1$ by Lemma 2(d), we obtain

$$f r_{k-1} - g v B_{k-1} = c_{k-1} n,$$

$$v r_{k-1} + u B_{k-1} = n,$$

so that $r_{k-1} = c_{k-1} u + g v$, $B_{k-1} = f u - c_{k-1} v$, and hence

$$v = (r_{k-1} - c_{k-1} r_k)/g.$$

Next, appealing to Lemma 2(a), we note that

$$0 \leq c_{k-1} \leq c_{k-1} v = f u - B_{k-1} < f u \leq f u^2 < n,$$

and modulo $n$ we observe that

$$r_k c_{k-1} \equiv u v^{-1} (v c_{k-1}) \equiv u v^{-1} (f r_k - B_{k-1}) \equiv e v (f r_k - B_{k-1})$$

$$\equiv (-1)^k y f r_k - (-1)^k y B_{k-1} \equiv r_{k-1} + (-1)^k f y r_k.$$

This shows that

$$r_k c_{k-1} \equiv r_{k-1} + (-1)^k f y r_k \pmod{n}, \quad 0 \leq c_{k-1} < n,$$

proving that $c_{k-1} = c$. The proof of Theorem 2 is now complete. □

4. The algorithm

Step 1. Use the Adleman-Pomerance-Rumely primality test [1] on the integer $n$. This is a deterministic algorithm with a worst case running time of $\mathcal{O}\left((\log n)^\alpha \log \log \log n\right)$, where $\alpha > 0$ is an absolute constant and the constant implied by the $\mathcal{O}$-symbol is also absolute. If $n$ is composite, go to Step 2; else set $r = 1$, $n = p_1$, $a_1 = 1$ and go to Step 3.

Step 2. Factor $n$ into primes. The fastest known, fully proven, deterministic factoring algorithm is the Pollard-Strassen method discussed by Pomerance in [11, §4]. This algorithm has a running time of

$$\mathcal{O}\left(n^{1/4}(\log n)^3 \log \log n \log \log \log n\right),$$

where the constant implied by the $\mathcal{O}$-symbol is absolute. This step in the algorithm is the dominant one. In practice, one would use one of the following methods: $\rho$ method, $p - 1$ method, elliptic curve method, quadratic sieve, etc. (see [10, 11, 13]). Set

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

where $a_1, a_2, \ldots, a_r$ are $r \geq 1$ positive integers and $p_1, p_2, \ldots, p_r$ are distinct primes with $p_1 = 2$ if $n$ is even. Continue with Step 3.

Step 3. Calculate $f^{-1} \pmod{n}$ and determine $m \equiv f^{-1} g \pmod{n}$, $0 < m < n$. Note $(m, n) = 1$. The congruence (1.6) is equivalent to $y^2 \equiv -m \pmod{n}$.

(a) If $n$ is odd go to (b). Else $n$ is even, $m$ is odd, $p_1 = 2$, $a_1 \geq 1$. If $a_1 = 2$ and $m \equiv 1 \pmod{4}$, or $a_1 \geq 3$ and $m \not\equiv 7 \pmod{8}$, the congruence

$$y^2 \equiv -m \pmod{2^{a_1}}$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
A deterministic algorithm for solving \( n = fu^2 + gv^2 \) is insolvable and the algorithm terminates at this point. Otherwise the congruence (4.2) is solvable and we continue with (b).

(b) For each odd prime \( p_i \), compute the Legendre symbol \((-m/p_i)\), using the Euclidean algorithm. If any of these symbols has the value \(-1\), the congruence

\[
y_i^2 \equiv -m \pmod{p_i^{a_i}}
\]

is insolvable and the algorithm terminates, else all the Legendre symbols have the value \(+1\) and we go to Step 4.

Step 3(a),(b) has a running time of at most

\[
\mathcal{O}(\log n) + \sum_{i=1}^{r} \mathcal{O}(\log^2 p_i) = \mathcal{O}(\log n) + \mathcal{O}(\log^2 p_1 \cdots p_r) = \mathcal{O}(\log^2 n),
\]

where the constant implied by the \( \mathcal{O} \)-symbol is absolute.

Step 4. For each odd prime \( p_i \) a solution \( z_i \) of the congruence

\[
z_i^2 \equiv -m \pmod{p_i}
\]

is found. The congruence (4.4) is solvable as \((-m/p_i) = +1\), and a solution \( z_i \) can be found in

\[
\mathcal{O}(p_i^{4\sqrt{\varepsilon}})^{-1+\varepsilon})
\]

steps, where \( \varepsilon > 0 \) and the constant implied by the \( \mathcal{O} \)-symbol depends only on \( \varepsilon \). This is clear, as (4.4) can be solved in time \( \mathcal{O}(\log p_i) \), once some quadratic nonresidue \((\mod{p_i})\) has been found (see, for example, \([2, 5, 9, 16, 17]\)), and it is known \([4]\) that the least quadratic nonresidue \((\mod{p_i})\) can be found in

\[
\mathcal{O}(p_i^{4\sqrt{\varepsilon}})^{-1+\varepsilon})
\]

steps, where the implied constant depends only on \( \varepsilon \). The two solutions \( \pm y_i \) of the congruence (4.3) are then found by means of the recurrence relation

\[
y_{i,1} = z_i,
\]

\[
y_{i,k+1} = y_{i,k} - (2y_{i,k})^{-1}(y_{i,k}^2 + m) \pmod{p_i^{k+1}}
\]

\[
(k = 1, \ldots, a_i - 1),
\]

\[
y_i = y_{i,a_i},
\]

where the inverse of \( 2y_{i,k} \) is taken modulo \( p_i \). Knowing \( z_i, y_i \) can be determined in \( \mathcal{O}(a_i \log p_i) \) steps.

When \( n \) is even, it is also necessary to solve the congruence (4.2), which is known to be solvable from Step 3. For \( a_i = 1 \) or 2, the solution \( y_1 \) of (4.2) is given by

\[
y_1 \equiv \begin{cases} 
1 \pmod{2} & \text{if } a_i = 1, \\
\pm 1 \pmod{4} & \text{if } a_i = 2.
\end{cases}
\]
For $a_i \geq 3$ the solutions of (4.2) are computed by means of the recurrence relation

\[
y_{1,3} = 1, \\
y_{1,k+1} \equiv (y_{1,k}^3 + (m + 2)y_{1,k})/2 \pmod{2^k} \quad (k = 3, 4, \ldots, a_i - 1), \\
y_{1,1} = y_{1,a_i}.
\]  

(4.7)

The four solutions of (4.2) are given by

\[
y \equiv \pm y_1, \pm(y_1 + 2^{a_i-1}) \pmod{2^{a_i}},
\]

(4.8)

and can be calculated in $O(a_i)$ steps.

Step 4 has a running time of

\[
\sum_{i=1}^{r} \Theta(p_i^{(4\sqrt{\varepsilon})^{-1} + \varepsilon}) O(a_i \log p_i) = O \left( \sum_{i=1}^{r} a_i p_i^{(4\sqrt{\varepsilon})^{-1} + 2\varepsilon} \right) = O \left( n^{(4\sqrt{\varepsilon})^{-1} + 2\varepsilon} \log n \right) = O(n^{(4\sqrt{\varepsilon})^{-1} + 3\varepsilon}),
\]

where the constant implied by the $\Theta$-symbol depends only upon $\varepsilon$. Thus the time for Step 4 is $O(n^{-\varepsilon + 3\varepsilon})$ uniformly in $f$ and $g$.

We remark that if Schoof's algorithm [14] is used for solving (4.4), Step 4 has a running time of $O(\log^{10} n)$ but the implied constant depends (strongly) on $m$.

**Step 5.** The Chinese remainder theorem is used to find the $2^k$ solutions $y$ (mod $n$) of

\[
y \equiv \pm y_i \pmod{p_i^{a_i}} \quad (i = 1, 2, \ldots, r), \quad \text{if } n \equiv 1 \pmod{2};
\]

(4.9)

the $2^{r-1}$ solutions $y$ (mod $n$) of

\[
y \equiv \begin{cases} 1 \pmod{2}, \\ \pm y_i \pmod{p_i^{a_i}} \end{cases} \quad (i = 2, \ldots, r), \quad \text{if } n \equiv 2 \pmod{4};
\]

(4.10)

the $2^r$ solutions $y$ (mod $n$) of

\[
y \equiv \begin{cases} \pm 1 \pmod{4}, \\ \pm y_i \pmod{p_i^{a_i}} \end{cases} \quad (i = 2, \ldots, r), \quad \text{if } n \equiv 4 \pmod{8};
\]

(4.11)

and the $2^{r+1}$ solutions $y$ (mod $n$) of

\[
y \equiv \begin{cases} \pm y_1, \pm(y_1 + 2^{a_i-1}) \pmod{2^{a_i}}, \\ \pm y_i \pmod{p_i^{a_i}} \end{cases} \quad (i = 2, \ldots, r), \quad \text{if } n \equiv 0 \pmod{8}.
\]

(4.12)

The values $y$ obtained are the solutions (mod $n$) of $y^2 \equiv -m$ (mod $n$). Step 5 can be accomplished in $O(2^r \log^2 n) = O(2^{\beta \log n/\log \log n})$ steps, where $\beta$ is a positive absolute constant, and the constant implied by the $O$-symbol is absolute.
Step 6. For each of the solutions $y$ of $y^2 \equiv -m \pmod{n}$ with $0 < y < n/2$ found in Step 5, we apply the Euclidean algorithm to $y$ and $n$, and determine the first remainder $r$ less than $\sqrt{n/f}$. By Theorem 1 all the solutions $(u, v)$ of $n = fu^2 + gv^2$, $(u, v) = 1$, in positive integers (with $u > v$ if $fg = 1$) lie among the pairs $(r, \sqrt{(n - fr^2)/g})$. They are easily found by checking whether $\sqrt{(n - fr^2)/g}$ is an integer. Step 6 takes $\Theta(2^r \log n) = \Theta(2^{\beta \log n / \log \log n})$ steps, where the implied constant is absolute.

We have thus proved the following theorem.

**Theorem 3.** Let $n$, $f$, $g$ be integers satisfying (1.1) and (1.2). Then there is a deterministic algorithm which gives all the solutions of $n = fu^2 + gv^2$ in positive coprime integers $u$ and $v$, with a worst case running time of

$$\Theta(n^{1/4} (\log n)^3 (\log \log n) (\log \log \log n)),$$

where the constant implied by the $\Theta$-symbol is independent of $f$ and $g$.

We remark that the worst case running time for a rigorous random version of our algorithm is

$$\Theta(2^{\beta \log n / \log \log n}), \quad (\beta > 0),$$

with the dominant steps being Step 5 and Step 6.

5. Numerical example

This algorithm was implemented in ALGEB on a RAVEN 286/10 IBM AT clone at Carleton University. The following example illustrates the calculation of solutions $(u, v)$ to (1.3) in the case

$$n = 9,198,968,367,101, \quad f = 4, \quad g = 61,$$

using Steps 1–6 as described in §4.

**Steps 1, 2.** $n$ is composite and the parameters in (4.1) are:

$$p_1 = 12613, \quad a_1 = 1; \quad p_2 = 20333, \quad a_2 = 1; \quad p_3 = 35869, \quad a_3 = 1.$$

**Step 3.** We have

$$f^{-1} \pmod{n} = 6,899,226,275,326,$$

$$m = 6,899,226,275,341,$$

$$\begin{pmatrix} -m \\ 12613 \end{pmatrix} = \begin{pmatrix} -m \\ 20333 \end{pmatrix} = \begin{pmatrix} -m \\ 35869 \end{pmatrix} = +1.$$

**Step 4.** The solutions $y_i$ of (4.3) corresponding to the primes $p_i$, $i = 1, 2, 3$, are

$$y_1 = 4853, \quad y_2 = 9570, \quad y_3 = 14037.$$
Step 5. The four solutions $y$ of $y^2 \equiv -m \pmod{n}$ with $0 < y < n/2$ are

$$382,072,735,980,\quad 1,154,613,726,359,\quad 1,579,334,330,612,\quad 3,116,020,792,951.$$  

Step 6. Applying the Euclidean algorithm to $n$ and each of the solutions $y$ from Step 5 above, we find the corresponding remainders $r_k$ with $r_k < \sqrt{n/\sqrt{f}} \leq r_{k-1}$.  

All four of the values of $y$ give rise to solutions of (1.3) as follows:

<table>
<thead>
<tr>
<th>$y$</th>
<th>$r_k$</th>
<th>$\sqrt{(n - fr_k^2)/g}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>382,072,735,980</td>
<td>717,088</td>
<td>342,175</td>
</tr>
<tr>
<td>1,154,613,726,359</td>
<td>577,520</td>
<td>359,071</td>
</tr>
<tr>
<td>1,579,334,330,612</td>
<td>1,376,188</td>
<td>163,135</td>
</tr>
<tr>
<td>3,116,020,792,951</td>
<td>381,100</td>
<td>375,871</td>
</tr>
</tbody>
</table>

The values of $r_{k-1}$ and $c$ corresponding to the four solutions above are:

<table>
<thead>
<tr>
<th>$k$</th>
<th>$r_{k-1}$</th>
<th>$c$</th>
<th>$(r_{k-1} - cr_k)/g$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>26,609,379</td>
<td>8</td>
<td>342,175</td>
</tr>
<tr>
<td>10</td>
<td>25,368,451</td>
<td>6</td>
<td>359,071</td>
</tr>
<tr>
<td>13</td>
<td>55,365,439</td>
<td>33</td>
<td>163,135</td>
</tr>
<tr>
<td>9</td>
<td>24,452,531</td>
<td>4</td>
<td>375,871</td>
</tr>
</tbody>
</table>

in accordance with Theorem 2.

Acknowledgments

The authors would like to thank Dr. J. Brillhart (University of Arizona), Dr. R. H. Hudson (University of South Carolina), Dr. S. Wagon (Smith College), and an unknown referee for their valuable comments on preliminary drafts of this paper.

Bibliography

2. W. S. Anglin, $x^2 \equiv R \pmod{p}$, Preprint, McGill University, 1987.
6. G. Cornacchia, Su di un metodo per la risoluzione in numeri interi dell' equazione $\sum_{h=0}^{n} c_h a^{-h} b^h = P$. Giornale di Matematiche di Battaglini 46 (1908), 33–90.