MATHEMATICS OF COMPUTATION
VOLUME 55, NUMBER 191
JULY 1990, PAGES 327-343

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 $n \geq f+g+1$, $(n, fg) = 1$. The running time of this algorithm is at most

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

uniformly in f and g.

1. INTRODUCTION

Throughout this paper, f and g denote integers such that

$$(1.1) \qquad f \geq 1, \quad g \geq 1, \quad (f, g) = 1,$$

and n denotes an integer such that

$$(1.2) \qquad n \geq f+g+1, \quad (n, fg) = 1.$$

We are interested in the problem of determining all positive integers u and v (if any) such that

$$(1.3) \qquad n = fu^2 + gv^2, \quad (u, v) = 1.$$

If (u, v) is a solution of (1.3) in positive integers, then

$$(1.4) \qquad (u, n) = (v, n) = 1,$$

and

$$(1.5) \qquad u \neq v.$$

In view of (1.4), we see that $v^{-1} \pmod{n}$ 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 $0 < y < n/2$.

Received March 14, 1988; revised November 17, 1988 and June 22, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11Y16.
The first and third authors' research was supported by Natural Sciences and Engineering Research Council of Canada Grants A-7823 and A-7233, respectively.

Conversely, suppose y is a solution of

$$fy^2 \equiv -g \pmod{n}, \qquad 0 < y < n/2. \tag{1.6}$$

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:

$$\begin{cases} n = fu^2 + gv^2, \quad (u, v) = 1, \quad uv^{-1} \equiv \pm y \pmod{n}, \\ \text{with} \begin{cases} u \geq 1, v \geq 1 & \text{if } fg \geq 2, \\ u > v \geq 1 & \text{if } fg = 1. \end{cases} \end{cases} \tag{1.7}$$

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 §2.

Theorem 1. *Let* y *be an integer satisfying* (1.6) *for which* $U(f, g, n, y)$ *is nonempty. Let*

$$r_0\ (= y) > r_1 > \cdots > r_{s-1}\ (= 1) > r_s\ (= 0) \tag{1.8}$$

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*

$$U(f, g, n, y) = \{(u, v)\}, \tag{1.9}$$

where

$$u = r_k, \qquad v = \sqrt{(n - fr_k^2)/g}. \tag{1.10}$$

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 §4, see Theorem 3.

Theorem 2 below, which is proved in §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*

$$v = \begin{cases} 1 & \text{if } k = 0, \\ r_{k+1} & \text{if } k \geq 1,\ fg = 1, \\ (r_{k-1} - cr_k)/g & \text{if } k \geq 1,\ fg \geq 2, \end{cases} \tag{1.11}$$

and c *is the unique integer satisfying*

$$r_k c \equiv r_{k-1} + (-1)^k fyr_k \pmod{n}, \qquad 0 \leq c < n. \tag{1.12}$$

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

$$U(f, g, n, y) \neq \varnothing. \tag{2.1}$$

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

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

We define ε $(= \pm 1)$ to be the *unique* integer satisfying

$$y \equiv \varepsilon uv^{-1} \pmod n. \tag{2.3}$$

Applying the Euclidean algorithm to y and n, we obtain

$$\begin{cases} y = q_0 n + r_0, \\ n = q_1 r_0 + r_1, \\ r_{i-2} = q_i r_{i-1} + r_i \qquad (i = 2, \ldots, s), \end{cases} \tag{2.4}$$

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

$$\begin{gathered} q_0 = [y/n] = 0, \qquad q_1 = [n/r_0] = [n/y] \geq 2, \\ q_i = [r_{i-2}/r_{i-1}] \geq 1 \qquad (i = 2, \ldots, s). \end{gathered} \tag{2.7}$$

The continued fraction for y/n is

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

The ith convergent to y/n is

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

so that, in particular, we have

$$\begin{array}{ll} A_0 = 0, & B_0 = 1, \\ A_1 = 1, & B_1 = q_1, \\ A_2 = q_2, & B_2 = q_1 q_2 + 1, \\ \vdots & \vdots \\ A_s = y, & B_s = n. \end{array} \tag{2.10}$$

Moreover, we have

$$(2.11)\qquad \begin{aligned} A_i &= q_iA_{i-1} + A_{i-2} \qquad (i = 2, \dots, s), \\ B_i &= q_iB_{i-1} + B_{i-2} \qquad (i = 2, \dots, s). \end{aligned}$$

From (2.4) and (2.11), we obtain, for $i = 1, \dots, s-1$,

$$(B_{i+1} - B_{i-1})r_i = q_{i+1}B_ir_i = (r_{i-1} - r_{i+1})B_i,$$

so that

$$r_iB_{i+1} + r_{i+1}B_i = r_{i-1}B_i + r_iB_{i-1} \qquad (i = 1, \dots, s-1),$$

and so, for $i = 1, \dots, s-1$, 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

$$(2.12)\qquad r_iB_{i+1} + r_{i+1}B_i = n \qquad (i = 0, 1, \dots, s-1).$$

An easy induction argument on i, using (2.4), (2.6), and (2.11), shows that

$$(2.13)\qquad r_i = (-1)^i(B_iy - A_in) \qquad (i = 0, 1, \dots, s),$$

so that

$$(2.14)\qquad r_i \equiv (-1)^iB_iy \pmod n \qquad (i = 0, 1, \dots, s).$$

From (2.2), (2.3), and (2.14), we see that for $i = 0, 1, \dots, s$,

$$(2.15)\qquad \begin{cases} fr_iu + \varepsilon(-1)^igB_iv \equiv 0 \pmod n, \\ r_iv - \varepsilon(-1)^iB_iu \equiv 0 \pmod n. \end{cases}$$

Hence, we may define integers c_i and d_i $(i = 0, 1, \dots, s)$ by

$$(2.16)\qquad \begin{cases} c_i = (fr_iu + \varepsilon(-1)^igB_iv)/n, \\ d_i = (r_iv - \varepsilon(-1)^iB_iu)/n. \end{cases}$$

Using (2.2), (2.4), (2.11), and (2.16), it is easy to show that

$$(2.17)\qquad \begin{cases} c_i = -q_ic_{i-1} + c_{i-2} \qquad (i = 2, 3, \dots, s), \\ d_i = -q_id_{i-1} + d_{i-2} \qquad (i = 2, 3, \dots, s), \end{cases}$$

$$(2.18)\qquad c_i^2 + fgd_i^2 = (fr_i^2 + gB_i^2)/n \qquad (i = 0, 1, \dots, s),$$

and

$$(2.19)\qquad c_id_{i+1} - c_{i+1}d_i = (-1)^i\varepsilon \qquad (i = 0, 1, \dots, s-1).$$

We note that

$$(2.20)\qquad c_0 = (fyu + \varepsilon gv)/n, \qquad d_0 = (yv - \varepsilon u)/n,$$

$$(2.21)\qquad c_1 = fu - q_1c_0, \qquad d_1 = v - q_1d_0,$$

$$(2.22)\qquad c_s = \varepsilon(-1)^sgv, \qquad d_s = \varepsilon(-1)^{s+1}u.$$

We emphasize that c_s and d_s are nonzero.

Lemma 1. *Suppose that* $c_i = 0$ *for some integer* i *with* $0 \le i \le s-1$. *Set*

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

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

(a) $c_a > \cdots > c_{i-2} > c_i = 0 > c_{i+2} > \cdots > c_{s-b}$,
(b) $c_{1-a} > \cdots > c_{i-3} > c_{i-1} = 1 = c_{i+1} < c_{i+3} < \cdots < c_{s-(1-b)}$,
(c) $d_{1-a} > \cdots > d_{i-1} \ge 0 \ge d_{i+1} > d_{i+3} > \cdots > d_{s-(1-b)}$, *where at most one of the equality signs holds, and*
(d) $d_a > \cdots > d_{i-2} \ge d_i = 1 \le d_{i+2} < \cdots < d_{s-b}$.

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

For $0 \le i \le s-1$, 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 $d_i = (r_iv + B_iu)/n > 0$, so we must have

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

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

$$c_{i-1} = 1 \qquad (1 \le i \le s-1).$$

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

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

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

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

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

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

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

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

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

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

so that $c_{i-2}d_{i-1} = d_{i-2} - 1 \ge 0$, and thus $d_{i-1} \ge 0$ $(2 \le i \le s-1)$. 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), $n = nc_0 = fyu + gv$ and

$$d_0 = \frac{yv - u}{n} = \frac{fuyv - fu^2}{fun} = \frac{fuyv - (n - gv^2)}{fun} = \frac{v(fuy + gv) - n}{fun} = \frac{v-1}{fu} \ge 0.$$

Hence we have $d_{i-1} \ge 0$ $(1 \le i \le s-1)$.

For $0 \le i \le s-2$, from (2.16), we obtain $d_{i+2} = (r_{i+2}v + B_{i+2}u)/n > 0$, so that $d_{i+2} \ge 1$ $(0 \le i \le s-2)$. Further, for $0 \le i \le s-2$, from (2.19), we have $c_{i+1}d_{i+2} - c_{i+2}d_{i+1} = 1$, so that $c_{i+2}d_{i+1} = d_{i+2} - 1 \ge 0$, and thus $d_{i+1} \le 0$ $(0 \le i \le s-2)$. But the last inequality also holds for $i = s-1$, as $d_{i+1} = d_s = \varepsilon(-1)^{s+1}u = -u < 0$. Hence we have $d_{i+1} \le 0$ $(0 \le i \le s-1)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

so that $d_t < d_{t+2}$ $(i+2 \le t \le s-2-b,\ t \equiv i \pmod 2)$. 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* $0 \le i \le s-1$. *Set*

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

Then we have $\varepsilon = (-1)^i$ *and*

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

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

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

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

Proof. The proof of Lemma 2 is similar to that of Lemma 1 and will be omitted. □

Lemma 3. (a) *If* $c_p = c_q = 0$ *with* $0 \le p \le q \le s-1$, *then* $p = q$.

(b) *If* $d_p = d_q = 0$ *with* $0 \le p \le q \le s-1$, *then* $p = q$.

(c) *If* $c_p = d_q = 0$ *with* $0 \le p \le s-1$, $0 \le q \le s-1$, *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). □

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

If $k = 0$, then $y = r_0 < \sqrt{n/f}$, $fy^2 + g \equiv 0 \pmod{n}$, $fy^2 + g < 2n$, so that $n = fy^2 + g1^2$, 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

$$u = y = r_0, \qquad v = 1 = B_0, \tag{2.23}$$

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

$$j = \begin{cases} 0 & \text{if } fg \ge 2, \\ 1 & \text{if } fg = 1, \end{cases}$$

as follows. From $n = fy^2 + g1^2$ and $n > f+g+1$, we obtain $y^2 \ge 1 + 1/f > 1$, so that (as $0 < y < n/2$) we have $y \ge 2$.

We first treat the case $fg \ge 2$. We suppose that $j \ge 1$ and obtain a contradiction. We have

$$\begin{aligned} fy \le fy + \left[\frac{g}{y}\right] &= \left[fy + \frac{g}{y}\right] = \left[\frac{fy^2+g}{y}\right] = \left[\frac{n}{y}\right] = q_1 \\ &= B_1 \le B_j < \sqrt{\frac{n}{g}} = \sqrt{\frac{fy^2+g}{g}} = \sqrt{1 + \frac{fy^2}{g}}, \end{aligned}$$

so that

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

If $f = 1$, we have $g \ge 2$, and the inequality becomes

$$y^2 < 1 + \frac{y^2}{g} \le 1 + \frac{y^2}{2},$$

which is impossible, as $y \ge 2$. On the other hand, if $f \ge 2$, the inequality gives

$$2y^2 \le f(f-1)y^2 < 1 - fy^2(g-1)/g < 1,$$

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

$$\begin{cases} y = 0n + y, \\ n = yy + 1, \\ y = y1 + 0, \end{cases}$$

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

$$r_k < \sqrt{n/f} \leq r_{k-1} \qquad (1 \leq k \leq s-1), \tag{2.24}$$

and

$$B_j < \sqrt{n/g} \leq B_{j+1} \qquad (0 \leq j \leq s-1). \tag{2.25}$$

We are now ready to prove Theorem 1.

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

$$\sqrt{n/f}B_k \leq r_{k-1}B_k \leq r_{k-1}B_k + r_kB_{k-1} = n,$$

so that

$$B_k \leq \sqrt{fn}. \tag{2.26}$$

From (2.12) and (2.25), we obtain

$$\sqrt{n/g}r_j \leq r_jB_{j+1} \leq r_jB_{j+1} + r_{j+1}B_j = n,$$

so that

$$r_j \leq \sqrt{gn}. \tag{2.27}$$

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

$$c_k^2 + fgd_k^2 = (fr_k^2 + gB_k^2)/n < 1 + fg, \tag{2.28}$$

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

$$c_j^2 + fgd_j^2 = (fr_j^2 + gB_j^2)/n < fg + 1. \tag{2.29}$$

Hence, from (2.28), we deduce

$$d_k = 0 \quad \text{or} \quad d_k = \pm 1, \quad c_k = 0, \tag{2.30}$$

and, from (2.29), we deduce

$$d_j = 0 \quad \text{or} \quad d_j = \pm 1, \quad c_j = 0. \tag{2.31}$$

We first show that neither of the possibilities

(a) $d_k = \pm 1$, $c_k = 0$, $d_j = 0$,

(b) $d_k = \pm 1$, $c_k = 0$, $d_j = \pm 1$, $c_j = 0$,

can occur.

(a) $d_k = \pm 1$, $c_k = 0$, $d_j = 0$. 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

$$fur_k - gvB_k = 0, \qquad vr_k + uB_k = n,$$

and

$$fur_{k+1} + gvB_{k+1} = n, \qquad vr_{k+1} - uB_{k+1} = 0.$$

Solving these linear equations for r_k, B_k and r_{k+1}, B_{k+1}, we obtain

$$r_k = gv, \quad B_k = fu, \qquad r_{k+1} = u, \quad B_{k+1} = v.$$

As $r_{k+1} < r_k < \sqrt{n/f}$ and $B_k < B_{k+1} < \sqrt{n/g}$, we deduce that

$$u < gv < \sqrt{n/f}, \qquad fu < v < \sqrt{n/g}.$$

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

$$fur_k - gvB_k = 0, \qquad vr_k + uB_k = n,$$

and

$$fur_{k-1} + gvB_{k-1} = n, \qquad vr_{k-1} - uB_{k-1} = 0.$$

Solving these linear equations for r_k, B_k and r_{k-1}, B_{k-1}, we obtain

$$r_k = gv, \quad B_k = fu, \qquad r_{k-1} = u, \quad B_{k-1} = v.$$

Appealing to (2.24), we obtain $\sqrt{n/f} \leq u$, and so

$$n = fu^2 + gv^2 > fu^2 \geq n,$$

which is impossible. Thus case (a) cannot occur.

(b) $d_k = \pm 1$, $c_k = 0$, $d_j = \pm 1$, $c_j = 0$. By Lemma 3(a) we have $j = k$, and by Lemma 1(d) we have $c_k = 0$, $d_k = 1$, and $\varepsilon = (-1)^{k+1}$. Appealing to (2.16), we obtain

$$fur_k - gvB_k = 0, \qquad vr_k + uB_k = n.$$

Solving these linear equations for r_k and B_k, we obtain $r_k = gv$, $B_k = fu$. Then, from (2.24) and (2.25), we deduce

$$gv < \sqrt{n/f}, \qquad fu < \sqrt{n/g}.$$

If $fg \geq 2$, then we have

$$n = fu^2 + gv^2 < \frac{n}{fg} + \frac{n}{fg} = \frac{2n}{fg} \leq n,$$

which is impossible. Thus we must have $fg = 1$, 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 $i = k-1$) $n = ur_{k-1} + vB_{k-1}$. Thus, as $(u, v) = 1$, there is an integer t such that

$$r_{k-1} = u + vt, \qquad B_{k-1} = v - ut.$$

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 $\varepsilon = (-1)^k$ and $c_k = 1$. Appealing to (2.16) (with $i = k$), we obtain

$$fur_k + gvB_k = n, \qquad vr_k - uB_k = 0.$$

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. □

We finish this section by showing that

$$j = \begin{cases} k & \text{if } fg \geq 2, \\ k+1 & \text{if } fg = 1. \end{cases} \tag{2.32}$$

Equation (2.32) has already been proved when $k = 0$, so we may assume that $k \geq 1$. We have shown that

$$c_k = 1, \quad d_k = 0, \quad \varepsilon = (-1)^k, \quad r_k = u, \quad B_k = v. \tag{2.33}$$

Hence we have $B_k = v < \sqrt{n/g}$, so that

$$j \geq k. \tag{2.34}$$

From (2.31) we see that either

$$d_j = 0 \tag{2.35}$$

or

$$c_j = 0, \qquad d_j = \pm 1. \tag{2.36}$$

If (2.36) holds, we have $c_j = d_k = 0$, 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

$$fur_{k+1} - gvB_{k+1} = 0, \qquad vr_{k+1} + uB_{k+1} = n.$$

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 $v < fu < \sqrt{n/g}$, so that

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

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

$$ur_{k+1} - vB_{k+1} = c_{k+1}n, \qquad vr_{k+1} + uB_{k+1} = n.$$

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

$$r_{k+1} = v + c_{k+1}u, \qquad B_{k+1} = u - c_{k+1}v.$$

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

$$0 \leq v + c_{k+1}u < u \tag{2.37}$$

and

$$v < \sqrt{n} \leq u - c_{k+1}v. \tag{2.38}$$

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). □

3. Proof of Theorem 2

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

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

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

$$r_k c \equiv r_{k-1} + (-1)^k fyr_k \pmod{n}, \qquad 0 \leq c < n,$$

has a *unique* solution c. From (2.16) (with $i = k-1$), recalling that $\varepsilon = (-1)^k$ and noting that $d_{k-1} = 1$ by Lemma 2(d), we obtain

$$fur_{k-1} - gvB_{k-1} = c_{k-1}n, \qquad vr_{k-1} + uB_{k-1} = n,$$

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

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

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

$$0 \le c_{k-1} \le c_{k-1}v = fu - B_{k-1} < fu \le fu^2 < n,$$

and modulo n we observe that

$$\begin{aligned} r_k c_{k-1} &\equiv uv^{-1}(vc_{k-1}) \equiv uv^{-1}(fr_k - B_{k-1}) \equiv \varepsilon y(fr_k - B_{k-1}) \\ &\equiv (-1)^k yfr_k - (-1)^k yB_{k-1} \equiv r_{k-1} + (-1)^k fyr_k. \end{aligned}$$

This shows that

$$r_k c_{k-1} \equiv r_{k-1} + (-1)^k fyr_k \pmod n, \qquad 0 \le c_{k-1} < n,$$

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 $\mathscr{O}((\log n)^{\alpha \log\log\log n})$, where $\alpha > 0$ is an absolute constant and the constant implied by the $\mathscr{O}$-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

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

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

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \tag{4.1}$$

where $a_1, a_2, \ldots, a_r$ are r (≥ 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, $p_1 = 2$, $a_1 \ge 1$. If $a_1 = 2$ and $m \equiv 1 \pmod 4$, or $a_1 \ge 3$ and $m \not\equiv 7 \pmod 8$, the congruence

$$y_1^2 \equiv -m \pmod{2^{a_1}} \tag{4.2}$$

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

$$y_i^2 \equiv -m \pmod{p_i^{a_i}} \tag{4.3}$$

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

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

where the constant implied by the $\mathscr{O}$-symbol is absolute.

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

$$z_i^2 \equiv -m \pmod{p_i} \tag{4.4}$$

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

$$\mathscr{O}(p_i^{(4\sqrt{e})^{-1}+\varepsilon})$$

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

$$\mathscr{O}(p_i^{(4\sqrt{e})^{-1}+\varepsilon})$$

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

$$\begin{cases} y_{i,1} = z_i, \\ y_{i,k+1} \equiv y_{i,k} - (2y_{i,k})^{-1}(y_{i,k}^2 + m) \pmod{p_i^{k+1}} \\ \qquad\qquad (k = 1, \ldots, a_i - 1), \\ y_i = y_{i,a_i}, \end{cases} \tag{4.5}$$

where the inverse of $2y_{i,k}$ is taken modulo p_i. Knowing z_i, y_i can be determined in $\mathscr{O}(a_i \log p_i)$ 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 $a_1 = 1$ or 2, the solution y_1 of (4.2) is given by

$$y_1 \equiv \begin{cases} 1 \pmod 2 & \text{if } a_1 = 1, \\ \pm 1 \pmod 4 & \text{if } a_1 = 2. \end{cases} \tag{4.6}$$

For $a_1 \geq 3$ the solutions of (4.2) are computed by means of the recurrence relation

$$\text{(4.7)} \qquad \begin{cases} y_{1,3} = 1, \\ y_{1,k+1} \equiv (y_{1,k}^3 + (m+2)y_{1,k})/2 \pmod{2^k} \\ \qquad\qquad (k = 3, 4, \ldots, a_i - 1), \\ y_1 = y_{1,a_1}. \end{cases}$$

The four solutions of (4.2) are given by

$$\text{(4.8)} \qquad y \equiv \pm y_1, \pm(y_1 + 2^{a_1-1}) \pmod{2^{a_1}},$$

and can be calculated in $\mathscr{O}(a_1)$ steps.

Step 4 has a running time of

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

where the constant implied by the $\mathscr{O}$-symbol depends only upon ε. Thus the time for Step 4 is $\mathscr{O}(n^{(4\sqrt{e})^{-1}+\varepsilon})$ 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 $\mathscr{O}(\log^{10} n)$ but the implied constant depends (strongly) on m.

Step 5. The Chinese remainder theorem is used to find the 2^r solutions $y \pmod n$ of

$$\text{(4.9)} \qquad y \equiv \pm y_i \pmod{p_i^{a_i}} \qquad (i = 1, 2, \ldots, r), \quad \text{if } n \equiv 1 \pmod 2;$$

the 2^{r-1} solutions $y \pmod n$ of

$$\text{(4.10)} \qquad y \equiv \begin{cases} 1 \pmod 2, \\ \pm y_i \pmod{p_i^{a_i}} \qquad (i = 2, \ldots, r), \quad \text{if } n \equiv 2 \pmod 4; \end{cases}$$

the 2^r solutions $y \pmod n$ of

$$\text{(4.11)} \qquad y \equiv \begin{cases} \pm 1 \pmod 4, \\ \pm y_i \pmod{p_i^{a_i}} \qquad (i = 2, \ldots, r), \quad \text{if } n \equiv 4 \pmod 8; \end{cases}$$

and the 2^{r+1} solutions $y \pmod n$ of

$$\text{(4.12)} \qquad y \equiv \begin{cases} \pm y_1, \pm(y_1 + 2^{a_1-1}) \pmod{2^{a_1}}, \\ \pm y_i \pmod{p_i^{a_i}} \qquad (i = 2, \ldots, r), \quad \text{if } n \equiv 0 \pmod 8. \end{cases}$$

The values y obtained are the solutions $\pmod n$ of $y^2 \equiv -m \pmod n$. Step 5 can be accomplished in $\mathscr{O}(2^r \log^2 n) = \mathscr{O}(2^{\beta \log n/\log\log n})$ steps, where β is a positive absolute constant, and the constant implied by the $\mathscr{O}$-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 $\mathcal{O}(2^r \log n) = \mathcal{O}(2^{\beta \log n / \log\log n})$ 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*

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

where the constant implied by the $\mathcal{O}$-symbol is independent of f and g.

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

$$\mathcal{O}(2^{\beta \log n / \log\log n}) \qquad (\beta > 0),$$

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:

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

Step 3. We have

$$f^{-1} \pmod{n} = 6{,}899{,}226{,}275{,}326,$$
$$m = 6{,}899{,}226{,}275{,}341,$$

$$\left(\frac{-m}{12613}\right) = \left(\frac{-m}{20333}\right) = \left(\frac{-m}{35869}\right) = +1.$$

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

$$y_1 = 4853, \qquad y_2 = 9570, \qquad y_3 = 14037.$$

Step 5. The four solutions y of $y^2 \equiv -m \pmod{n}$ with $0 < y < n/2$ are

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

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 $r_k < \sqrt{n/f} \le r_{k-1}$. All four of the values of y give rise to solutions of (1.3) as follows:

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

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

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

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

1. L. M. Adleman, C. Pomerance, and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), 173–206.

2. W. S. Anglin, $x^2 \equiv R \pmod{p}$, Preprint, McGill University, 1987.

3. J. Brillhart, *Note on representing a prime as a sum of two squares*, Math. Comp. **26** (1972), 1011–1013.

4. D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika **4** (1975), 106–112.

5. M. Cipolla, *Un metodo per la risoluzione della congruenza di secondo grado*, Rend. Accad. Sci. Fis. Mat. Napoli (3) **9** (1903), 154–163.

6. G. Cornacchia, *Su di un metodo per la risoluzione in numeri interi dell' equazione* $\sum_{h=0}^{n} c_h x^{n-h} y^h = P$, Giornale di Matematiche di Battaglini **46** (1908), 33–90.

7. L. E. Dickson, *History of the theory of numbers*, vol. I, Chelsea, New York, 1952.

8. C. Hermite, *Note au sujet de l'article précédent*, J. Math. Pures Appl. **13** (1848), 15.

9. D. H. Lehmer, *Computer technology applied to the theory of numbers*, Studies in Number Theory (W. J. LeVeque, ed.), MAA Studies in Math., vol. 6, Math. Assoc. America, Washington, D. C., 1969, pp. 117–151.

10. C. Pomerance, *Lecture notes on primality testing and factoring*, MAA Notes No. 4 (1984).

11. ——, *Fast, rigorous factorization and discrete logarithm algorithms*, Discrete Algorithms and Complexity (D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, eds.), Academic Press, 1987, pp. 119–143.

12. ——, *Analysis and comparison of some integer factoring algorithms*, Computational Methods in Number Theory (Part I) (H. W. Lenstra and R. Tijdeman, eds.), Math. Centre Tracts, vol. 154, Mathematisch Centrum, Amsterdam, 1982, pp. 89–139.

13. H. Riesel, *Prime numbers and computer methods for factorization*, Birkhäuser, Basel and New York, 1985.

14. R. Schoof, *Elliptic curves over finite fields and the computation of square roots* mod p, Math. Comp. **44** (1985), 483–494.

15. J. A. Serret, *Sur un théorème rélatif aux nombres entières*, J. Math. Pures Appl. **13** (1848), 12–14.

16. D. Shanks, *Five number-theoretic algorithms*, Proc. Second Manitoba Conference on Numerical Mathematics, University of Manitoba, Winnipeg, Canada, 1972, pp. 51–70.

17. A. Tonelli, *Bemerkung über die Auflösung quadratischer Congruenzen*, Gött. Nachr. (1891), 344–346.

18. J. V. Uspensky and M. A. Heaslet, *Elementary number theory*, McGraw-Hill, New York, 1939.

19. P. Wilker, *An efficient algorithmic solution of the Diophantine equation* $u^2 + 5v^2 = m$, Math. Comp. **35** (1980), 1347–1352.

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6 (Hardy and Williams). *E-mail*: kennethhardy@carleton.bitnet; kswilliams@carleton.bitnet

Department of Mathematics and Computer Science, Bar-Ilan University, 52 100 Ramat-Gan, Israel (Muskat)