Solving $n = au^2 + buv + cv^2$ using the Euclidean algorithm

Kenneth Hardy[1], Joseph B. Muskat[2], Kenneth S. Williams[3]

[1, 3] Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario
CANADA K1S 5B6

[2] Department of Mathematics and Computer Science
Bar-Ilan University
52 100 Ramat-Gan
ISRAEL

Abstract. It is shown how all the primitive representations of a positive integer n by an integral, primitive, positive-definite, binary quadratic form can be determined using the Euclidean algorithm. The method works when the central coefficient of the form is small compared to the size of the discriminant of the form.

1. Introduction.

We begin by recalling briefly the algorithm given by the authors in [1] to determine all primitive representations of a positive integer n by the form $fu^2 + gv^2$, where f and g are positive coprime integers. We suppose that $n > f + g$ and that n is coprime to both f and g. For each solution y of the congruence $fy^2 + g \equiv 0 \pmod{n}$ with $0 < y < n/2$, the Euclidean algorithm is applied to y and n (in that order) to obtain the first remainder $r_y < \sqrt{n/f}$. Then all the solutions (u, v) of $n = fu^2 + gv^2$ in positive coprime integers lie among the pairs $(r_y, \sqrt{(n - fr_y^2)/g})$. If $fy^2 + g \equiv 0 \pmod{n}$ is insolvable then $n = fu^2 + gv^2$ has no solutions. The following example illustrates the algorithm.

Example 1: We seek all solutions in integers u and v of

$$69 = u^2 + 5v^2, \quad u \geq 1, \quad v \geq 1, \quad (u, v) = 1.$$

Here $n = 69$, $f = 1$, $g = 5$. The solutions y of $y^2 + 5 \equiv 0 \pmod{69}$ with $0 < y < 69/2$ are $y_1 = 8$ and $y_2 = 31$. Applying the Euclidean algorithm to each value of y and n, we obtain successive remainders as follows:

$$y_1 = 8: \quad 8, 5, 3, 2, 1, 0,$$
$$y_2 = 31: \quad 31, 7, 3, 1, 0.$$

[1] Research supported by Natural Sciences and Engineering Research Council Canada Grant A-7823.
[2] Research supported by a travel grant from Bar-Ilan University.
[3] Research supported by Natural Sciences and Engineering Research Council Canada Grant A-7233.

Since $\sqrt{n/f} \approx 8.3$, we have that $r_8 = 8$ and $r_{31} = 7$. These values of r_y give all the solutions, namely $(u, v) = (8, 1), (7, 2)$.

The aim of this note is to extend the algorithm in [1] to determine all coprime integers u, v (if any) for which $n = au^2 + buv + cv^2$, where n is a positive integer and $au^2 + buv + cv^2$ is an integral, primitive, positive-definite, binary quadratic form with discriminant $b^2 - 4ac = -\Delta < 0$. We suppose that

$$n > 2 \max(a, c) \text{ and } (n, ac) = 1.$$

The natural extension of the algorithm described above is as follows: for each solution y of $ay^2 + by + c \equiv 0 \pmod{n}$ with $0 < y < n$, apply the Euclidean algorithm to y and n to obtain the first remainder $r_y \leq \sqrt{4cn/\Delta}$ and then look for solutions of

$$n = au^2 + buv + cv^2, \quad u \geq 1, \quad (u, v) = 1$$

among the pairs $\left(r_y, (-br_y \pm \sqrt{4cn - \Delta r_y^2})/2c\right)$. Note that we use the range $0 < y < n$ for y and not $0 < y < n/2$. The congruence $fy^2 + g \equiv 0 \pmod{n}$ has its solutions equally distributed between the two intervals $0 < y < n/2$ and $n/2 < y < n$ but this is not generally the case for the congruence $ay^2 + by + c \equiv 0 \pmod{n}$. Unfortunately, this extension of the algorithm in [1] does not work in general as the following example shows.

Example 2: We seek all solutions in integers u and v of

$$577 = 3u^2 + 14uv + 17v^2, \quad u \geq 1, \quad (u, v) = 1.$$

Here $n = 577$ (a prime), $a = 3$, $b = 14$, $c = 17$ and $\Delta = 8$. There are two solutions y of

$$3y^2 + 14y + 17 \equiv 0 \pmod{577}, \quad 0 < y < 577,$$

namely,

$$y_1 = 462, \quad y_2 = 495.$$

Applying the Euclidean algorithm to each value of y and n, we obtain successive remainders as follows:

$$y_1 = 462\text{: } 462, 115, 2, 1, 0,$$
$$y_2 = 495\text{: } 495, 82, 3, 1, 0.$$

There are two solutions $(u, v) = (2, 5), (70, -29)$. The method finds the first solution. However, 70 is not a remainder and thus the algorithm does not find both solutions.

It is therefore necessary to put conditions on a, b, and c in such a way that the algorithm will find all the solutions. We will show that this occurs at least when $|b|$ is sufficiently small with respect to Δ. In Section 2 we prove the following theorem.

Theorem. *Let a, b, c be integers such that*

$$\begin{cases} (a,b,c) = 1, & a > 0, \quad c > 0, \\ & \text{with} \\ \Delta = 4ac - b^2 \geq 16 & \text{and } |b| \leq (\Delta - 16)/8. \end{cases} \tag{1.1}$$

Let n be a positive integer such that

$$n > 2\max(a,c), \quad (n, ac) = 1. \tag{1.2}$$

For each solution y of

$$ay^2 + by + c \equiv 0 \pmod{n}, \quad 0 < y < n, \tag{1.3}$$

let r_y be the first remainder obtained by applying the Euclidean algorithm to y and n (in that order) which is less than or equal to $\sqrt{4cn/\Delta}$. Then all the integral solutions (if any) of

$$n = au^2 + buv + cv^2, \quad u \geq 1, \quad (u,v) = 1, \tag{1.4}$$

are found among the pairs

$$\left(r_y, (-br_y \pm \sqrt{4cn - \Delta r_y^2})/2c\right), \tag{1.5}$$

where y runs through solutions of (1.3).

We close this introduction with a few remarks. First we observe that the condition $|b| \leq (\Delta - 16)/8$ is equivalent to

$$2\sqrt{ac} - |b| \geq 4. \tag{1.6}$$

Next we note that the assumption $(n, ac) = 1$ ensures that any solution y of (1.3) satisfies

$$(y, n) = 1, \tag{1.7}$$

and that any solution (u, v) of (1.4) satisfies

$$(u, n) = (v, n) = 1. \tag{1.8}$$

From (1.8) we see that any solution (u, v) of (1.4) satisfies

$$v \neq 0. \tag{1.9}$$

Finally, multiplying the equation in (1.4) by $4a$ and $4c$, and completing the square, we obtain respectively

$$4an = (2au + bv)^2 + \Delta v^2 \geq \Delta v^2$$

and

$$4cn = \Delta u^2 + (bu + 2cv)^2 \geq \Delta u^2,$$

so that

$$1 \leq u \leq \sqrt{4cn/\Delta}, \quad 1 \leq |v| \leq \sqrt{4an/\Delta}. \tag{1.10}$$

We now give an example to illustrate the algorithm.

Example 3: We seek all solutions in integers u and v of

$$18392 = 7u^2 - 6uv + 7v^2, \quad u \geq 1, \quad (u, v) = 1.$$

Here $n = 18392$ and $\Delta = 160$. The solutions y of $7y^2 - 6y + 7 \equiv 0 \pmod{18392}$ are $y = 745, 3197, 4165, 8973, 9941, 12393, 13361, 18169$. Applying the Euclidean algorithm to each value of y and n, we obtain successive remainders as follows:

$y = 745$: $745, 512, 233, 46^*, 3, 1, 0,$
$y = 3197$: $3197, 2407, 790, 37^*, 13, 11, 2, 1, 0,$
$y = 4165$: $4165, 1732, 701, 330, 41^*, 2, 1, 0,$
$y = 8973$: $8973, 446, 53^*, 22, 9, 4, 1, 0,$
$y = 9941$: $9941, 8451, 1490, 1001, 489, 23^*, 6, 5, 1, 0,$
$y = 12393$: $12393, 395, 74, 25^*, 24, 1, 0,$
$y = 13361$: $13361, 5031, 3299, 1732, 1567, 165, 82, 1^*, 0,$
$y = 18169$: $18169, 223, 106, 11^*, 4, 3, 1, 0,$

where the asterisk indicates the first remainder less than $\sqrt{4cn/\Delta} \approx 56.7$. There are four solutions, namely $(u, v) = (23, -37), (37, -23), (53, 41), (41, 53)$, and these are all obtained from some value of y.

2. Proof of the theorem: If (1.3) is insolvable so is (1.4). Thus we may suppose that (1.3) is solvable. For y a solution of (1.3), we define the (possibly empty) set $U(a, b, c, n, y)$ to be the set of pairs of integers (u, v) satisfying:

$$\begin{cases} n = au^2 + buv + cv^2, & (u, v) = 1, \\ uv^{-1} \equiv y \pmod{n}, & u \geq 1. \end{cases} \tag{2.1}$$

We show first that either $U(a,b,c,n,y)$ is empty or contains exactly one pair of integers. Suppose that $U(a,b,c,n,y)$ is nonempty and $(u,v),(u_1,v_1)$ are two solutions of (2.1). We will show that $u_1 = u, v_1 = v$. We have

$$4n^2 = (2n)(2n) = (2au^2 + 2buv + 2cv^2)(2au_1^2 + 2bu_1v_1 + 2cv_1^2),$$

so that

$$4n^2 = (2auu_1 + buv_1 + bvu_1 + 2cvv_1)^2 + \Delta(uv_1 - vu_1)^2. \tag{2.2}$$

Now $uv^{-1} \equiv u_1v_1^{-1} (\equiv y) \pmod{n}$ so that

$$uv_1 - u_1v \equiv 0 \pmod{n}. \tag{2.3}$$

Hence, from (2.2) and (2.3), we see that there exist integers X and Y such that

$$2auu_1 + buv_1 + bvu_1 + 2cvv_1 = nX, \tag{2.4}$$

$$uv_1 - u_1v = nY, \tag{2.5}$$

$$X^2 + \Delta Y^2 = 4. \tag{2.6}$$

As $\Delta \geq 16 > 4$ we see that $(X,Y) = (\pm 2, 0)$ are the only solutions of (2.6). Then, from (2.5), we deduce that

$$uv_1 = u_1v. \tag{2.7}$$

Since $u \geq 1, u_1 \geq 1, (u,v) = 1$ we see from (2.7) that there is a positive integer t such that

$$u_1 = tu, \quad v_1 = tv.$$

Moreover we have

$$t = t(u,v) = (tu,tv) = (u_1,v_1) = 1.$$

Hence, we have $u_1 = u, v_1 = v$ as claimed.

If $U(a,b,c,n,y)$ is nonempty, we let (u,v) be the unique pair of integers satisfying (2.1). Applying the Euclidean algorithm to y and n, we obtain

$$\begin{cases} y = q_0n + r_0, \\ n = q_1r_0 + r_1, \\ r_{i-2} = q_ir_{i-1} + r_i \quad (i = 2, \ldots, s), \end{cases} \tag{2.8}$$

where

$$s \geq 1, \tag{2.9}$$

$$r_0(=y) > r_1 > r_2 > \ldots > r_{s-1}(=1) > r_s(=0), \tag{2.10}$$

and

$$\begin{cases} q_0 = [y/n] = 0, \quad q_1 = [n/r_0] = [n/y] \geq 1, \\ q_i = [r_{i-2}/r_{i-1}] \geq 1, \quad (i = 2, \ldots, s). \end{cases} \tag{2.11}$$

We show that

$$u = r_k, \quad v = (-1)^k B_k,$$

where r_k is the first remainder $\leq \sqrt{4cn/\Delta}$. Clearly, replacing u by r_k in the equation (1.4), and solving the resulting quadratic equation for v, we obtain

$$v = \left(-br_k \pm \sqrt{4cn - \Delta r_k^2}\right)/2c.$$

The continued fraction for y/n is

$$\frac{y}{n} = [q_0, q_1, q_2, \ldots, q_s]. \tag{2.12}$$

The i th convergent to y/n is

$$\frac{A_i}{B_i} = [q_0, q_1, q_2, \ldots, q_i] \quad (i = 0, 1, \ldots, s), \tag{2.13}$$

so that, in particular, we have

$$\begin{cases} A_0 = 0, & B_0 = 1, \\ A_1 = 1, & B_1 = q_1, \\ A_2 = q_2, & B_2 = q_1 q_2 + 1, \\ \vdots & \vdots \\ A_s = y, & B_s = n. \end{cases} \tag{2.14}$$

Moreover we have

$$\begin{cases} A_i = q_i A_{i-1} + A_{i-2} \quad (i = 2, \ldots, s), \\ B_i = q_i B_{i-1} + B_{i-2} \quad (i = 2, \ldots, s). \end{cases} \tag{2.15}$$

An easy induction argument on i shows that

$$r_i B_{i+1} + r_{i+1} B_i = n \qquad (i = 0, 1, \ldots, s-1) \tag{2.16}$$

and

$$r_i = (-1)^i(B_i y - A_i n) \qquad (i = 0, 1, \ldots, s). \tag{2.17}$$

(See [1, Section 2]). From (2.17) we see that

$$r_i \equiv (-1)^i B_i y \pmod{n} \qquad (i = 0, 1, \ldots, s) \tag{2.18}$$

and so, using (2.1), for $i = 0, 1, \ldots, s$ we have

$$\begin{cases} r_i(au + \frac{b}{2}v) + (-1)^i B_i(\frac{b}{2}u + cv) \equiv 0 \pmod{n}, & (b \text{ even}), \\ r_i(au + \frac{(b-1)}{2}v) + (-1)^i B_i(\frac{(b+1)}{2}u + cv) \equiv 0 \pmod{n}, & (b \text{ odd}), \end{cases} \tag{2.19}$$

as well as

$$r_i v - (-1)^i B_i u \equiv 0 \pmod{n}. \tag{2.20}$$

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

$$c_i = \begin{cases} \left(r_i(au + \frac{b}{2}v) + (-1)^i B_i(\frac{b}{2}u + cv)\right)/n, & (b \text{ even}), \\ \left(r_i(au + \frac{(b-1)}{2}v) + (-1)^i B_i(\frac{(b+1)}{2}u + cv)\right)/n, & (b \text{ odd}) \end{cases} \tag{2.21}$$

and

$$d_i = (r_i v - (-1)^i B_i u)/n. \tag{2.22}$$

A simple consequence of (2.16) and (2.22) is the relation

$$u = (-1)^i(d_{i+1} r_i - d_i r_{i+1}) \qquad (i = 0, 1, \ldots, s-1). \tag{2.23}$$

A straightforward calculation shows that for $i = 0, 1, \ldots, s$ we have

$$\begin{cases} c_i^2 + \frac{\Delta}{4} d_i^2 = \frac{ar_i^2 + b(-1)^i r_i B_i + cB_i^2}{n}, & (b \text{ even}), \\ c_i^2 + c_i d_i + \frac{(\Delta+1)}{4} d_i^2 = \frac{ar_i^2 + b(-1)^i r_i B_i + cB_i^2}{n}, & (b \text{ odd}) \end{cases} \tag{2.24}$$

and

$$c_i d_{i+1} - c_{i+1} d_i = (-1)^i \qquad (i = 0, 1, \ldots, s-1). \tag{2.25}$$

Next set

$$\alpha = \sqrt{\frac{(\Delta - 4|b|) - \sqrt{\Delta(\Delta - 8|b| - 16)}}{8a}}.$$

From (1.1) we have $\Delta - 8|b| - 16 \geq 0$ and it is easy to check that α is a positive real number. Moreover we have

$$a\alpha^2 + |b| + \frac{c}{\alpha^2} = \frac{\Delta}{4}, \tag{2.26}$$

from which we deduce

$$\sqrt{\frac{4c}{\Delta}} < \alpha < \sqrt{\frac{\Delta}{4a}}. \tag{2.27}$$

Let r_l $(0 \leq l \leq s)$ be the largest remainder $< \alpha\sqrt{n}$. We consider two cases according as $l \geq 1$ or $l = 0$.

Case (i) $l \geq 1$. We have

$$r_l < \alpha\sqrt{n} \leq r_{l-1}. \tag{2.28}$$

Now, from (2.16) and (2.28), we have

$$\alpha\sqrt{n}B_l \leq r_{l-1}B_l \leq r_{l-1}B_l + r_lB_{l-1} = n,$$

so that

$$B_l \leq \sqrt{n}/\alpha. \tag{2.29}$$

Hence, using (2.26), (2.28) and (2.29), we have (recalling that $ax^2 + bxy + cy^2$ is a positive-definite form)

$$0 < \frac{ar_l^2 + b(-1)^l r_l B_l + cB_l^2}{n} < a\alpha^2 + |b| + c/\alpha^2 = \Delta/4. \tag{2.30}$$

Thus, appealing to (2.24) and (2.30), we have

$$\begin{cases} 0 < c_l^2 + \frac{\Delta}{4}d_l^2 < \frac{\Delta}{4}, & (b \text{ even}), \\ 0 < c_l^2 + c_l d_l + \frac{(\Delta+1)}{4}d_l^2 < \frac{\Delta}{4}, & (b \text{ odd}), \end{cases} \tag{2.31}$$

so that for any b we have

$$d_l = 0. \tag{2.32}$$

From (2.22) and (2.32), we deduce

$$r_l v = (-1)^l B_l u, \tag{2.33}$$

which implies $r_l \neq 0$ showing that $l \leq s - 1$. Hence, we have $r_l \geq 1$, and as $u \geq 1$ and $B_l \geq 1$, we see from (2.33) that

$$|v| = (-1)^l v, \quad r_l|v| = B_l u.$$

Next, appealing to (2.25) and (2.32), we have

$$c_l d_{l-1} = c_l d_{l-1} - c_{l-1}d_l = (-1)^l,$$

so that

$$c_l = \epsilon, \quad d_{l-1} = \epsilon(-1)^l, \quad \epsilon = \pm 1. \tag{2.34}$$

From (2.23), (2.32) and (2.34), we obtain $u = \epsilon r_l$. Now $r_l \geq 1$ and $u \geq 1$, so we must have $\epsilon = 1$, and thus

$$u = r_l, \quad v = (-1)^l|v| = (-1)^l B_l.$$

We now define r_k $(0 \leq k \leq s)$ to be the largest remainder $\leq \sqrt{4cn/\Delta}$. Then, from (1.10), we have $r_l = u \leq \sqrt{4cn/\Delta}$, so that $l \geq k$. On the other hand, appealing to (2.27), we obtain $r_k \leq \sqrt{4cn/\Delta} < \alpha\sqrt{n}$, showing that $k \geq l$. Hence, we have $k = l$ and

$$u = r_k, \quad v = (-1)^k B_k,$$

as asserted.

Case (ii) $l = 0$. In this case we have

$$0 < y = r_0 < \alpha\sqrt{n}. \tag{2.35}$$

Since (u, v) is a solution of (2.1), $(u, -v)$ is a solution of (2.1) with b replaced by $-b$ and y replaced by $n - y$. Hence, we have

$$U(a, -b, c, n, n-y) \neq \emptyset.$$

Applying the Euclidean algorithm to $n - y$ and n, we obtain analogously to (2.8)

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

where

$$q_0' = \left[\frac{n-y}{n}\right] = 0, \quad r_0' = n - y.$$

We now consider two cases according as $n > 4\alpha^2$ or $n \leq 4\alpha^2$. First we treat the case $n > 4\alpha^2$. This inequality implies that

$$y < \alpha\sqrt{n} < n/2, \tag{2.36}$$

so that

$$1 < \frac{n}{n-y} < 2,$$

and thus

$$q_1' = \left[\frac{n}{r_0'}\right] = \left[\frac{n}{n-y}\right] = 1,$$

and

$$r_1' = n - q_1' r_0' = n - r_0' = n - (n-y) = y. \tag{2.37}$$

Next, by (2.36) and (2.37), we note that

$$r_0' = n - y > n/2 > \alpha\sqrt{n} > y = r_1',$$

so that the first remainder less than $\alpha\sqrt{n}$ is r_1'. Hence, by the argument of Case (i) applied to $a, -b, c, n, n-y$ rather than a, b, c, n, y, we deduce that

$$r_1' = u, \qquad B_1' = (-1)(-v) = v.$$

Thus we have

$$u = r_1' = y = r_0, \qquad v = B_1' = q_1' = 1 = B_0,$$

as asserted. This completes the treatment of the case $n > 4\alpha^2$.

Next we treat the case $n \leq 4\alpha^2$. From (1.10) and (2.27), we have

$$1 \leq |v| \leq \sqrt{4an/\Delta} < \sqrt{n}/\alpha \leq 2,$$

so that

$$v = \pm 1.$$

Also from (1.10) and (2.27), we have

$$0 < u \leq \sqrt{4cn/\Delta} < \alpha\sqrt{n}. \tag{2.38}$$

Adding (2.35) and (2.38) we deduce

$$0 < y + u < 2\alpha\sqrt{n}.$$

Next we observe, from (2.27) and $n > 2\max(a, c)$, that

$$\alpha < \sqrt{\frac{\Delta}{4a}} \leq \sqrt{\frac{4ac}{4a}} = \sqrt{c} < \sqrt{2c} < \sqrt{n},$$

so that

$$0 < y + u < 2n. \tag{2.39}$$

We now show that $v \neq -1$. Suppose on the contrary that $v = -1$. Then, as $y \equiv uv^{-1} \equiv -u \pmod{n}$, we have

$$y + u \equiv 0 \pmod{n}. \tag{2.40}$$

From (2.39) and (2.40) we deduce that

$$y + u = n.$$

Hence, we have $(u, v) = (n - y, -1)$, and so from (1.4), we obtain

$$n = a(n - y)^2 - b(n - y) + c,$$

which gives

$$2ay - an + b = \frac{ay^2 + by + c}{n} - 1 \geq 0,$$

as $(ay^2 + by + c)/n$ is a positive integer. Thus, we have

$$y \geq \frac{n}{2} - \frac{b}{2a}.$$

But, as $y < \alpha\sqrt{n}$, we must have

$$\alpha\sqrt{n} > \frac{n}{2} - \frac{b}{2a},$$

from which we deduce that

$$(\sqrt{n} - \alpha)^2 < \alpha^2 + \frac{b}{a},$$

so

$$\begin{aligned}
\sqrt{n} &< \alpha + \sqrt{\alpha^2 + \frac{b}{a}} \\
&\leq \alpha + \sqrt{\alpha^2 + \frac{|b|}{a}} \\
&= \sqrt{\frac{(\Delta - 4|b|) - \sqrt{\Delta(\Delta - 8|b| - 16)}}{8a}} \\
&\quad + \sqrt{\frac{(\Delta + 4|b|) - \sqrt{\Delta(\Delta - 8|b| - 16)}}{8a}} \\
&\leq 2\sqrt{\frac{\Delta - \sqrt{\Delta(\Delta - 8|b| - 16)}}{8a}} \\
&\leq 2\sqrt{\frac{\Delta}{8a}} = \sqrt{\frac{\Delta}{2a}} \leq \sqrt{2c} < \sqrt{n},
\end{aligned}$$

which is impossible.

Hence, we have $v = 1$, and $y \equiv uv^{-1} \equiv u \pmod{n}$. As

$$0 \leq |y - u| < \max(y, u) < \alpha\sqrt{n} < n,$$

we deduce that

$$u = y = r_0, \quad v = 1 = B_0,$$

as required. This completes the treatment of the case $n \leq 4\alpha^2$.

Finally, as any solution (u, v) of (1.4) gives rise to a solution $y \equiv uv^{-1} \pmod{n}$ of (1.3), this completes the proof of the theorem.

3. Concluding remarks.

Numerical calculations indicate that the algorithm described in our theorem applies to certain forms $au^2 + buv + cv^2$ not satisfying (1.1) and to some positive integers n not satisfying (1.2). However, our method of proof relies heavily on the condition $|b| \leq (\Delta - 16)/8$ which is required to define α. What further or different conditions are needed to encompass other cases for which the algorithm is seen to work remain to be discovered.

4. Acknowledgement.

The authors would like to acknowledge the help of Mr. Nicholas Buck of the College of New Caledonia, Prince George, British Columbia, who prepared some numerical data in connection with this research.

Reference

1. K. Hardy, J.B. Muskat and K.S. Williams, *A deterministic algorithm for solving* $n = fu^2 + gv^2$ *in coprime integers* u *and* v, Mathematics of Computation (to appear).