Canadian Mathematical Society
Conference Proceedings
Volume 15, 1995

Some Refinements of an Algorithm of Brillhart

KENNETH S. WILLIAMS

ABSTRACT. Refinements of an algorithm of Brillhart for finding the representation of a prime $p \equiv 1 \pmod 4$ as the sum of two integral squares are discussed.

1. Introduction

In this talk, we briefly survey some refinements that have been made to a beautifully simple algorithm of Brillhart [1] for finding the representation of a prime $p \equiv 1 \pmod 4$ as the sum of two integral squares.

We begin by giving Brillhart's algorithm, which is in fact a shortened form of an algorithm given by Hermite in 1848. Hermite, in a one-page note [4], gave the following efficient method for finding the representation of a given prime $p \equiv 1 \pmod 4$ as a sum of two integral squares. Hermite's method appeared simultaneously with a paper of Serret [6] on the same subject. However, Hermite's method is superior to Serret's as it gives a criterion for ending the algorithm at the right place.

Hermite's algorithm

(i) Find the solution z of $z^2 \equiv -1 \pmod p$, where $0 < z < p/2$.

(ii) Expand z/p into a simple continued fraction to the point where the denominators B_i of its convergents A_i/B_i satisfy the inequality $B_k < \sqrt{p} < B_{k+1}$. Then $p = u^2 + v^2$ with

$$u = zB_k - pA_k, \quad v = B_k.$$

1991 *Mathematics Subject Classification.* Primary 11Y16, 11Y50; Secondary 11A05, 11E16.
The author was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

In 1972, Brillhart [1] pointed out that the calculation of the convergents A_k and B_k can be dispensed with, since the values needed for the representation (u, v) of p are already available in the continued fraction expansion itself.

Brillhart's algorithm

(i) Find the solution z of $z^2 \equiv -1 \pmod{p}$ where $0 < z < p/2$.

(ii) Apply the Euclidean algorithm to z and p (in that order) and determine the first remainder $r_k (k \geq 0)$ satisfying $r_k < \sqrt{p}$. Then $p = u^2 + v^2$ with

$$u = r_k, \quad v = r_{k+1}.$$

We note that the first step of the Euclidean algorithm is not actually performed. It is present just to ensure that $r_0 = z$. We also note that we can take z in step (i) to be $c^{(p-1)/4} \pmod{p}$, where c is a quadratic non-residue $(\bmod\ p)$. Methods of determining a quadratic non-residue $c \pmod{p}$ are well-known, and will not be discussed here. Brillhart's proof of his algorithm uses the fact that the continued fraction expansion of p/z is palindromic.

Before continuing, we pause to give a simple example to illustrate Brillhart's algorithm. We take $p = 61$ so that $z = 11$. Applying the Euclidean algorithm to 11 and 61, we obtain successively the remainders 11, 6, 5, 1, 0. As $\sqrt{p}$ is approximately 7.81, we see that $k = 1$, $r_1 = 6$, $r_2 = 5$, and $61 = 6^2 + 5^2$.

2. Refinements to Brillhart's Algorithm

In 1990 Hardy, Muskat and Williams [2] extended Brillhart's algorithm to the following more general situation. Let f and g denote positive integers. For a positive integer n, we are interested in determining all positive integers u and v (if any) such that

$$n = fu^2 + gv^2, \quad u \geq 1, \quad v \geq 1, \quad (u, v) = 1. \tag{1}$$

Clearly we may assume that $(f, g) = 1$, otherwise, we consider the equation $n_1 = f_1 u^2 + g_1 v^2$, where $n_1 = n/d$, $f_1 = f/d$, $g_1 = g/d$, $d = (f, g)$. Similarly, if $(n, f) > 1$ and/or $(n, g) > 1$, we may reduce the problem to one in which $(n, fg) = 1$. Further, if $n \leq f + g$, the solutions of $n = fu^2 + gv^2$ are easily found, so we may assume that $n \geq f + g + 1$. Under these assumptions, it was shown in [2] that the solutions of (1) are determined by the following algorithm.

Hardy-Muskat-Williams algorithm

(i) Determine all solutions z of $fz^2 + g \equiv 0 \pmod{n}$, where $0 < z < n/2$.

(ii) For each z, apply the Euclidean algorithm to z and n, and let $r(z)$ denote the first remainder $< \sqrt{n/f}$. Then all solutions (u, v) in positive integers of $n = fu^2 + gv^2$ with $(u, v) = 1$ and $u > v$ if $f = g = 1$ lie among the pairs

$$\left(r(z), \sqrt{(n - f\{r(z)\}^2/g}\right).$$

Before making a few comments on this algorithm, we present an example.

We choose $n = 128744$, $f = 1$, $g = 40$, so we are seeking the solutions (u, v) in positive integers of $128744 = u^2 + 40v^2$ with $(u, v) = 1$. We note that $(n, g) > 1$ but this is unimportant. The solutions z of the congruence $z^2 \equiv -40 \pmod{128744}$ are listed below together with the remainders $r(z)$ obtained by applying the Euclidean algorithm to each z and 128744. We note that $\sqrt{128744} \approx 358.8$.

z	$r(z)$
1564	76
5212	76
22376	328
29152	128
35220	256
41996	132
59160	272
62808	248

Computing $v = \sqrt{(128744 - r(z)^2)/40}$, we find that the solutions are

$$(u, v) = (328, 23),\ (128, 53),\ (272, 37),\ (248, 41).$$

We emphasize that the algorithm did not produce the solutions with $(u, v) > 1$, namely, $(u, v) = (352, 11)$ and $(88, 55)$.

It is shown in [2, Theorem 2], when $(u, v) = (r(z), \sqrt{(n - f\{r(z)\}^2)/g})$ is a solution of (1), how v can be expressed in terms of the remainders preceding and following $r(z)$. Brillhart's algorithm is then seen to be the special case $n = p$ (prime) $\equiv 1 \pmod 4$, $f = 1$, $g = 1$ of the Hardy-Muskat-Williams algorithm. The proof of the Hardy-Muskat-Williams algorithm is much more involved than Brillhart's proof of his algorithm as the palindromic nature of the continued fraction used in [1] does not usually hold in the more general situation. A deterministic version of this algorithm is described and analyzed in [3] and an estimate of the worst case running time given. A refinement of this algorithm has been given by Muskat [5].

A natural extension of the Hardy-Muskat-Williams algorithm would be to replace $fu^2 + gv^2$ by a general positive-definite, primitive, integral binary quadratic form $au^2 + buv + cv^2$. We might hope for an algorithm of the following type.

Proposed extension of the Hardy-Muskat-Williams algorithm.

Let a, b, c be integers with

$$(a, b, c) = 1,\ a > 0,\ c > 0,\ \Delta = 4ac - b^2 > 0.$$

Let n be a "suitably large" positive integer with $(n, ac) = 1$.

(i) Find all the solutions z of

$$az^2 + bz + c \equiv 0 \pmod{n}, \quad 0 < z < n.$$

(ii) Apply the Euclidean algorithm to each z and n, and let $r(z)$ be the first remainder $\leq \sqrt{4cn/\Delta}$.

Then all integral solutions (u, v) of

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

lie among the pairs

$$\left(r(z), (-br(z) \pm \sqrt{4cn - \Delta r(z)^2})/2c\right). \tag{3}$$

Unfortunately this algorithm does not always work! To see this consider

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

which has the solutions

$$(u, v) = (2, 5) \quad \text{and} \quad (70, -29).$$

However, the algorithm proposed above yields only the solution $(2, 5)$.

Hardy, Muskat, Williams [3] have shown that the proposed algorithm does work for $n > 2\max(a, c)$ under the additional assumptions

$$\Delta = 4ac - b^2 \geq 16, \quad |b| \leq (\Delta - 16)/8.$$

For example applying the algorithm to solve

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

we obtain

z	$r(z)$
745	46
3197	37
4165	41
8973	53
9941	23
12393	25
13361	1
18169	11

from which we obtain the solutions

$$(u, v) = (37, -23), \ (41, 53), \ (53, 41), \ (23, -37).$$

Note that $\Delta = 160$ and $(\Delta - 16)/8 = 18$.

We remark that every primitive, positive-definite, integral, binary quadratic form $au^2 + buv + cv^2$ is equivalent to a unique reduced form $Au^2 + Buv + Cv^2$, that is, one satisfying

$$-A < B \leq A \leq C, \quad \text{with} \quad B \geq 0 \text{ if } A = C.$$

However not every reduced form with $\Delta \geq 16$ satisfies the assumption $|b| \leq (\Delta - 16)/8$ of (4). To see this take, for example, the form $u^2 + uv + 5v^2$, which is reduced, but $\Delta = 19$ and $(\Delta - 16)/8 = 3/8 < 1$. Moreover the proposed algorithm sometimes works when $\Delta \leq 15$ or $\Delta \geq 16$, $|b| > (\Delta - 16)/8$. Examples are given below.

Example

$$107 = u^2 + 5uv + 8v^2, \quad u \geq 1, \quad (u, v) = 1.$$

$\Delta = 7$

z	$r(z)$
46	15
56	5

All solutions are $(15, -2), (5, 2)$.

Example

$$134 = u^2 + 4uv + 9v^2, \quad u \geq 1, \quad (u, v) = 1.$$

$\Delta = 20 \qquad (\Delta - 16)/8 = 0.5$

z	$r(z)$
51	13
79	7

All solutions are $(13, -5), (7, -5)$.

Necessary and sufficient conditions are not known under which the proposed algorithm gives all solutions (u, v) of (2) in the form (3).

Before continuing, we explain briefly why the assumptions in (4) guarantee that the proposed algorithm works. The reader is referred to [3] for complete details.

Let z denote a solution of

$$az^2 + bz + c \equiv 0 \pmod{n}, \; 0 < z < n.$$

Applying the Euclidean algorithm to z and n, we obtain,

$$z = q_0 n + r_0,$$
$$n = q_1 r_0 + r_1,$$
$$r_0 = q_2 r_1 + r_2,$$
$$\cdots$$

where

$$r_0(=z) > r_1 > r_2 > \ldots > r_{s-1} > r_s(=0), \ s \geq 1.$$

The continued fraction for z/n is

$$\frac{z}{n} = [q_0, q_1, q_2, \ldots, q_s],$$

and the ith convergent to z/n is

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

An easy induction argument shows that

$$r_{i-1}B_i + r_iB_{i-1} = n \quad (i = 1, 2, \ldots, s). \tag{5}$$

Now let α be a positive number to be chosen later, and let $r_k (k \geq 0)$ be the first remainder $\leq \alpha\sqrt{n}$. If $k \geq 1$ (the case $k = 0$ must be treated separately) then

$$r_k \leq \alpha\sqrt{n} < r_{k-1}, \tag{6}$$

and (5) gives

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

so that

$$B_k < \frac{1}{\alpha}\sqrt{n}. \tag{7}$$

In [3] integers c_i and d_i $(i = 0, 1, \ldots, s)$ are defined in such a way that

$$\left\{\begin{array}{ll} c_i^2 + \frac{\Delta}{4}d_i^2, & \text{if } \Delta \equiv 0 \pmod 4 \\ c_i^2 + c_id_i + \frac{(\Delta+1)}{4}d_i^2, & \text{if } \Delta \equiv 3 \pmod 4 \end{array}\right\} = \frac{ar_i^2 + b(-1)^ir_iB_i + cB_i^2}{n} \quad (i = 0, 1, \ldots, s)$$

and

$$d_k = 0 \text{ if and only if } r_k = u.$$

One way of forcing $d_k = 0$ is by requiring

$$\frac{ar_k^2 + b(-1)^kr_kB_k + cB_k^2}{n} < \frac{\Delta}{4}.$$

This can be guaranteed in view of (6) and (7) by choosing α so that

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

A solution of this equation is

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

and α is real and positive provided

$$\Delta - 8|b| - 16 \geq 0,$$

which requires

$$\Delta \geq 16, \quad |b| \leq (\Delta - 16)/8,$$

that is, the conditions given in (4). The inequalities

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

show that r_k is also the first remainder $\leq \sqrt{4cn/\Delta}$.

We close by giving a modification of the proposed algorithm which works for any integer $n \geq 1$ and any primitive, positive-definite, integral binary quadratic form $au^2 + buv + cv^2$. This algorithm no longer requires that the solutions (u, v) of (2) be given in the form $u = r(z)$.

Williams' algorithm [7]

(i) Determine all the solutions z of

$$az^2 + bz + c \equiv 0 \pmod{n}, \quad 0 < z < n, \quad (z, n) = 1.$$

(ii) Apply the Euclidean algorithm to each z and n and stop at the first remainder $r_k \leq \sqrt{4cn/\Delta}$, and calculate the denominator B_k of the kth convergent to z/n. (Note that k depends upon z).

(iii) Calculate the positive integer Q_z given by

$$Q_z = \frac{ar_k^2 + br_k(-1)^k B_k + cB_k^2}{n}.$$

(It is known that Q_z satisfies the inequality

$$Q_z \leq \max\left(\frac{4ac}{\Delta} + |b| + \frac{\Delta}{4}, \frac{4ac}{\Delta} + |b|\sqrt{\frac{2c}{4}} + \frac{c}{2}\right)$$

so that Q_z is bounded independently of n). Find all integral solutions (x, y) of

$$\left.\begin{cases} x^2 + \dfrac{\Delta}{4}y^2 \text{ if } \Delta \equiv 0 \pmod{4} \\ x^2 + xy + \dfrac{\Delta}{4}y^2 \text{ if } \Delta \equiv 3 \pmod{4} \end{cases}\right\} = Q_z.$$

(iv) Eliminate those solutions (x, y) which do not satisfy the technical conditions given in [7, eqns. (19)-(26)]. Either no pairs remain or a unique pair (x, y) is left. In the latter case

$$(u, v) = \left(\frac{r_k x - ([\frac{b}{2}]r_k + c(-1)^k B_k)y}{Q_z}, \frac{(-1)^k B_k x + (ar_k + (-1)^k[\frac{b+1}{2}]B_k)y}{Q_z}\right)$$

is an integral solution of

$$n = au^2 + buv + cv^2, \quad (u, v) = (u, n) = (v, n) = 1. \tag{8}$$

Moreover all solutions of (8) are easily obtained from these solutions ([7, eqn. (28)]).

We close with a simple example illustrating this algorithm.

Example Find all integral solutions (u, v) of

$$577 = 3u^2 + 14uv + 17v^2, \quad u \geq 1, \quad (u, v) = (u, 577) = (v, 577) = 1. \tag{9}$$

The solutions of

$$3z^2 + 14z + 17 \equiv 0 \pmod{577}, \quad 0 < z < 577, \quad (z, 577) = 1,$$

are $z = 462,\ 495$. With $z = 462$ we have

$$r_2 = 2,\ B_2 = 5,\ Q_{462} = 1.$$

The solutions of $x^2 + 2y^2 = 1$ are $(x, y) = (\pm 1, 0)$. Only $(x, y) = (1, 0)$ satisfies the technical conditions of [7]. This pair gives the solutions $(u, v) = \pm(2, 5)$. With $z = 495$ we have

$$r_2 = 1,\ B_2 = 7,\ Q_{495} = 2.$$

The solutions of $x^2 + 2y^2 = 2$ are $(x, y) = (0, \pm 1)$. Only $(x, y) = (0, -1)$ satisfies the technical conditions of [7]. This pair gives the solutions $(u, v) = \pm(70, -29)$. Thus $(u, v) = \pm(2, 5),\ \pm(70, -29)$ comprise all the integral solutions of (9).

References

1. J. Brillhart, *Note on representing a prime as a sum of two squares*, Math. Comp. **26** (1972), 1011–1013.
2. 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*, Math. Comp. **55** (1990), 327–343.
3. ———, *Solving $n = au^2 + buv + cv^3$ using the Euclidean algorithm*, Utilitas Math. **38** (1990), 225–236.
4. C. Hermite, *Note au sujet de l'article précédent*, J. Math. Pures Appl. **13** (1848), 15.
5. J.B. Muskat, *A refinement of the Hardy-Muskat-Williams algorithm for solving $n = fu^2 + gv^2$*, Utilitas Math. **4** (1992), 109–117.
6. J.A. Serret, *Sur un théorème rélatif aux nombres entières*, J. Math. Pures Appl. **13** (1848), 12–14.
7. K.S. Williams, *On finding the solutions of $n = au^2 + buv + cv^2$ in integers u and v*, Utilitas Math. **46** (1994), 3–19.

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada K1S 5B6

E-mail address: williams@mathstat.carleton.ca