MA330
Sathaye **Note on Chakravāla Method of Bhāskara II Edited September 27, 2018**

Homework is included. It is to be submitted by October 10. I expect a pdf file from a typed or scanned document.

Each group submits complete answers.

We describe below a new technique inspired by the historical works of Bhāskara/Jayadeva/Brahmagupta for the solution in positive integers of the equation

$$x^2 - Dy^2 = \pm 1.$$

where D is a given positive integer which is not a complete square.

Notation We shall work in the field $F = \mathbb{Q}(\sqrt{D})$ where $\mathbb{Q}$ is the usual field of rational numbers.

For convenience, we shall display a typical element $a + b\sqrt{D} \in F$ where $a, b \in \mathbb{Q}$ as a pair (a, b). We also define its D norm $||(a,b)||_D$ by the formula $||(a,b)||_D = a^2 - Db^2$.

We may simply write $||(a,b)||$, provided D is already fixed.

It might be more convenient to name a Brahmagupta triple for D to be $< a, b, s >_D$ where $s = a^2 - Db^2 = ||(a,b)||_D$. As above, we can drop D from the notation, if it is already fixed.

Convention : Even though these concepts are defined for rational numbers, we generally assume that the entries are integers, because we are ultimately interested in integral solutions only.

Thus, our problem is to find all elements of norm ± 1 and this set is known to form the group of units in the ring $\mathbb{Z}[\sqrt{D}]$ of elements (a, b) with $a, b \in \mathbb{Z}$-the ring of integers.

A reader unfamiliar with this terminology can still follow the rest of the work!

Homework exercises:

(a) Let $g_1 =< a_1, b_1, s_1 >_D$ and $g_2 =< a_2, b_2, s_2 >_D$ be two Brahmagupta triples. Define the Brahmagupta product (bhāvanā) by: $g_1 * g_2 =< a, b, s >_D$ where

$$a = a_1 a_2 + D b_1 b_2, b = a_1 b_2 + a_2 b_1 \text{ and } s = s_1 s_2.$$

Prove that $s = ||(a,b)||_D$.

(b) Suppose that $< a, b, s >_D, < p, 1, t >_D$ are Brahmagupta triples (of integers) such that

- b and s are coprime and
- $a + bp \equiv 0 \pmod{s}$.

Let $< u, v, st >_D =< a, b, s >_D * < p, 1, t >_D$. Prove that s divides v and also u.

Hence deduce that $< u/s, v/s, t/s >_D$ is also a **Brahmagupta triple of integers.**

We will call this triple $< u/s, v/s, t/s >_D$ as a **reduction of** $< a, b, s >_D * < p, 1, t >_D$.

Method We now describe the steps.

Choose start: Choose a convenient pair $(a_1, 1)$ such that the norm $t_1 = a^2 - D$ is such that $|t_1|$ is as small as possible.

Set $s_1 = t_1$.

To choose t_1 you simply need to compare the floor and the ceiling of $\sqrt{D}$. Thus for $D = 43$ we try $a = 6, 7$. The resulting norms are $6^2 - 43 = -7$ and $7^2 - 43 = 6$. Since $|6| < |-7|$ we start with $(7, 1)$. As another example, for $D = 53$ we try $a = 7, 8$ and pick 7 with norm -4 rather than 8 with norm 11. We record the first pair, its norm t_1 and its " extended norm " s_1.

For the first pair, $s_1 = t_1$.

Now, we set $D = 43$ and drop D from our notation. We build a table with three rows from our value of D as follows. The first column is:

a-value	7
norm of $(a, 1)$	6
extended norm	6

Next step: Let $h_1 = |s_1|$ be the absolute value of the extended norm of the first pair $(a_1, 1)$. Choose an integer a_2 such that

$$a_1 + a_2 \equiv 0 \pmod{h_1} \text{ and the norm } ||(a_2, 1)||_D \text{ is as small as possible.}$$

Thus, we solve $a_1 + a_2 = 7 + a_2 \equiv 0 \pmod 6$. The value of a_2 is chosen from the sequence $5, 11, 17, \cdots$ and the minimality is obtained by choosing a numbers closest to the floor and ceiling of $\sqrt{D} = \sqrt{43}$ and comparing their norms. So, we only need to check of $5, 11$ and clearly 5 is the winner with $||(5, 1)|| = -18$ against 11 with $||(11, 1)|| = 85$.

The norm of $(5, 1)$ is $25 - 43 = -18$. It is not a surprise that this is divisible by s_1. (Use one of the homework exercises.)

So now we have the next column, using $a_2 = 5, t_2 = -18, s_2 = t_2/s_2 = -3$.

So our record is now:

a-value	7	5
norm of $(a, 1)$	6	-18
extended norm	6	-3

Continue: Now we repeat the above steps by using $a_2 = 5$ and $s_2 = -3$. The choices for a_3 are $1, 4, 7, 10, \cdots$ and the winner among $a_3 = 4, 7$ is seen to be 7 with the norm of $7^2 - 43 = 6 = t_3$. Again, this norm is divisible by $s_2 = -3$, as expected and the quotient is $s_3 = -2$, our next extended norm. So our record is, now,

a-value	7	5	7
norm of $(a, 1)$	6	-18	6
extended norm	6	-3	-2

To repeat the step, we use $a_3 = 7, s_3 = -2$ and choose a_4 from $1, 3, 5, 7, 9, \cdots$ with the clear winner 7. So the new display is:

a-value	7	5	7	7
norm of $(a, 1)$	6	-18	6	6
extended norm	6	-3	-2	-3

Stop: Verify that by continuing this way, we get:

a-value	7	5	7	7	5	7
norm of $(a, 1)$	6	-18	6	6	-18	6
extended norm	6	-3	-2	-3	6	1

When the extended norm becomes ± 1 we stop!

Conclusion: We have the necessary information to find our x, y. We first multiply the various numbers in our first row in the field F and notice that at each stage certain integers can be factored, i.e. the products are "reduced" as described.

Here is an explicit record of the products and the reductions.

number	product	Factor out s	The extended norm s.
$7 + \sqrt{D}$	$7 + \sqrt{D}$		
$(5 + \sqrt{D})$	$78 + 12\sqrt{D}$	$13 + 2\sqrt{D}$	6
$(7 + \sqrt{D})$	$177 + 27\sqrt{D}$	$-(59 + 9\sqrt{D})$	-3
$(7 + \sqrt{D})$	$-(800 + 122\sqrt{D})$	$400 + 61\sqrt{D}$	-2
$(5 + \sqrt{D})$	$4623 + 705\sqrt{D}$	$-(1541 + 235\sqrt{D})$	-3
$(7 + \sqrt{D})$	$-(20892 + 3186\sqrt{D})$	$-(3482 + 531\sqrt{D})$	6

Our answer is $x = -3482, y = -531$ and hence also $x = 3482, y = 531$.

How do we know that we are done? We multiplied the pairs in the top row whose norms were in the second row and also in the third row in two parts. Thus the norm of the whole product is

$$(6)(-18)(6)(6)(-18)(6) = (6)[(6)(-3)][(-3)(-2)][(-2)(-3)][(-3)(6)][(6)(1)] = (6{\cdot}3{\cdot}2{\cdot}3{\cdot}6)^2.$$

But we clearly divided by the same amount due to factoring, so the resulting norm is 1.

More Homework.

1. **Brahmagupta Theorems.**

   It is possible to shorten the work considerably, if we have triples of the form $< a, b, s >$ where $s = \pm 2$ or ± 4.

   The following homework problems give Brahmagupta's theorems for this.

   (a) Suppose that we have $g =< a, b, s >_D$ with $s = \pm 2$. Show that $g * g =< p, q, 4 >_D$ where p, q are necessarily divisible by 2. Hence it gives a reduction $< p/2, q/2, 1 >_D$, a solution to the problem.

   (b) Suppose that we have $g =< a, b, s >_D$ with $s = \pm 4$. Calculate $g * g$ and $g * g * g$. Show that reduction of one of these two triples gives a desired solution with norm 1.

2. Carry out the above algorithm for the following values of D.

   $$D = 61, 67, 97, 137.$$

   You should report the final answer in each case, namely (x, y) such that $x^2 - Dy^2 = 1$.

   Hint: Be sure to use Brahmagupta theorems when possible. It will reduce the work. If you wish to use a computer program (Maple, e.g.), be sure to show the steps. I can supply Maple routines if desired.