MA330
Sathaye **Note on Chakravāla Method of Bhāskara** **Edited February 24, 2017**

We describe below a new technique inspired by the historical works of Bhāskara/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 write a typical element $a + b\sqrt{D} \in F$ where $a, b \in \mathbb{Q}$ as a pair (a, b) and by its norm we shall mean $a^2 - Db^2$ and we shall write it as $||(a, b)||_D$ or just $||(a, b)||$ D is already fixed.

It might be more convenient to name a Brahmagupta triple for D to be $< a, b, s >_D$ where $s = a^2 - Db^2$. 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) Suppose $t_1 :=< a_1, b_1, s_1 >_D$ and $t_2 :=< a_2, b_2, s_2 >_D$ be two Brahmagupta triples. Define the Brahmagupta product (bhāvanā) by: $t_1 * t_2 =< a, b, s >_D$ where

$$a = a_1a_2 + Db_1b_2, b = a_1b_2 + a_2b_1 \text{ and } s = s_1s_2.$$

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

(b) Suppose that $< a, b, s >_D$ is a Brahmagupta triple. If an integer m divides both b and s, then show that m divides a as well. Moreover, we can deduce that $< a/m, b/m, s/m^2 >_D$ is a Brahmagupta triple (of integers).

We may call this the m-reduction of $< a, b, s >_D$.

(c) Suppose that $< a, b, s >_D$ is a Brahmagupta triple (of integers) and m divides s, then there is a Brahmagupta triple $< p, 1, r >_D$ such that $a + bp$ is divisible by m. Moreover, it is possible modify p such that $r = ||(p, 1)||_D$ is as small as possible.

Method We now describe the steps.

Choose start: Choose a convenient pair $(a, 1)$ such that the norm $||(a, 1)|| = a^2 - D$ is as small as possible **in the absolute value.** 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 and its " extended norm ". For the first pair the extended norm is the same as the norm.

Now, we set $D = 43$ we write:

pair	$(7, 1)$
norm	6
extended norm	6

Choose second: Let h be the absolute value of the extended norm of the first pair $(a, 1)$ Choose an integer b such that

$$a + b \equiv 0 \pmod{h} \text{ and } (b, 1) \text{ has minimal norm.}$$

Thus, we solve $a + b = 7 + b \equiv 5 \pmod{6}$. The value of b is chosen from the sequence $5, 11, 17, \cdots$ and clearly 5 is a winner! The norm of $(5, 1)$ is $25 - 43 = -18$. It is no accident that it is divisible by 6. This can be proved! **Challenge: How?**

We shall record the leftover part of its norm as the extended norm, namely $h = \frac{-18}{6} = -3$.
So our record is now:

pair	$(7, 1)$	$(5, 1)$
norm	6	-18
extended norm	6	-3

Continue: Now we repeat the above step by setting $a = 5$ and $h = 3$. The choices for b are $1, 4, 7, 10, \cdots$ and the winner again will be the one closest to the $\sqrt{D} = \sqrt{43}$. Now $b = 7$ is the winner with the norm of $(7, 1)$ being $7^2 - 43 = 6$. Again, it is divisible by -3 and the quotient is $h = -2$, our next extended norm. So our record is, now,

pair	$(7, 1)$	$(5, 1)$	$(7, 1)$
norm	6	-18	6
extended norm	6	-3	-2

To repeat the step, we take $a = 7, h = -2$ and deduce $b = 1, 3, 5, 7, 9, \cdots$ with the clear winner 7. So the new display is:

pair	$(7, 1)$	$(5, 1)$	$(7, 1)$	$(7, 1)$
norm	6	-18	6	6
extended norm	6	-3	-2	-3

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

pair	$(7, 1)$	$(5, 1)$	$(7, 1)$	$(7, 1)$	$(5, 1)$	$(7, 1)$
norm	6	-18	6	6	-18	6
extended norm	6	-3	-2	-3	6	1

When h 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. We throw away these common factors. Here are the explicit steps:

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

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 at the bottom 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.

Modification Clearly, it is wasteful to write the pairs on top, since the second number is always 1. So, we shall shorten our display to:

7	5	7	7	5	7
6	-18	6	6	-18	6
6	-3	-2	-3	6	1