

Indian mathematics treatment of Pell's equation

We consider Diophantine equations of the form

$$x^2 - Dy^2 = 1$$

where D is a positive integer with no square divisors. The goal is to find integers x, y that solve this equation. This equation has been called Pell's Equation since the eighteenth century, even though Indian mathematicians have considered this equation and relatives since the time of Brahmagupta (c. 598-695 CE) with full solutions being given by Bhaskara (c. 1114-1185 CE).

One key part of the Indian method is to solve the more general problem

$$x^2 - Dy^2 = m$$

for m a nonzero integer, and use these solutions to solve the original Pell equation. Brahmagupta discovered a method of combining solutions of such equations that he used to solve many such problems.

We use the notation $(p, q; m)$ to mean that $p^2 - Dq^2 = m$. The text calls p, q a solution for *additive* m , thinking of m as the quantity added to D times the square q^2 to obtain a square.

Brahmagupta discovered that solutions $(p, q; m)$ and $(p', q'; m')$ can be used to solve the problem with additive mm' . In modern notation we can discover this result by formally factoring a difference of squares:

$$\begin{aligned} p^2 - Dq^2 &= (p + \sqrt{D}q)(p - \sqrt{D}q) = m \\ p'^2 - Dq'^2 &= (p' + \sqrt{D}q')(p' - \sqrt{D}q') = m' \end{aligned}$$

Everything is based on computing $(p + \sqrt{D}q)(p' + \sqrt{D}q') = (pp' + Dqq') + \sqrt{D}(pq' + qp')$ by the distributive law. Similarly $(p - \sqrt{D}q)(p' - \sqrt{D}q') = (pp' + Dqq') - \sqrt{D}(pq' + qp')$ and multiplying the two equations above then gives

$$((pp' + Dqq') + \sqrt{D}(pq' + qp'))((pp' + Dqq') - \sqrt{D}(pq' + qp')) = mm'$$

In our notation above we write

$$(p, q; m) * (p', q'; m') = ((pp' + Dqq'), (pq' + qp'); mm')$$

and say we have composed the solutions.

For example, we have $2^2 - 3 \cdot 1^2 = 1$ as a solution of Pell's equation for $D = 3$. Hence we have $(2, 1; 1)$ in the notation above. We can construct more solutions by composition.

$$(2, 1; 1) * (2, 1; 1) = (7, 4; 1)$$

so that we get the new solution $7^2 - 3 \cdot 4^2 = 1$. We can keep doing this to find infinitely many solutions to Pell's equation:

$$(2, 1; 1) * (7, 4; 1) = (26, 15; 1) \text{ so that } 26^2 - 3 \cdot 15^2 = 1$$

$$(2, 1; 1) * (26, 15; 1) = (97, 56; 1) \text{ so that } 97^2 - 3 \cdot 56^2 = 1$$

This is the first aspect of Pell's equation that the Indian mathematicians discovered — infinitely many solutions could be produced starting from one.

Brahmagupta applied this idea to solve many Pell type equations. As an example consider solving

$$x^2 - 5y^2 = 1.$$

Brahmagupta starts by choosing values v and m such that $5v^2 + m$ is a square. For example $v = 1, m = 4$ leads to the equation $3^2 - 5 \cdot 1^2 = 4$, which differs from Pell's equation by the right hand side equaling 4 not 1. If we divide both sides of the equation by 4 we obtain $(3/2)^2 - 5(1/2)^2 = 1$, which is a fractional solution of Pell's equation. In other words we have $(3/2, 1/2; 1)$ which we can compose with itself to get a new solution

$$(3/2, 1/2; 1) * (3/2, 1/2; 1) = (9/4 + 5/4, 3/4 + 3/4; 1) = (7/2, 3/2; 1)$$

We still don't have an integer solution, so we try another composition

$$(3/2, 1/2; 1) * (7/2, 3/2; 1) = (21/4 + 15/4, 9/4 + 7/4; 1) = (9, 4; 1)$$

so that we have the solution $9^2 - 5 \cdot 4^2 = 1$.

Using these ideas Brahmagupta provided solutions of many Pell type equations. Along the way he developed several shortcuts, noticing for example that a solution of $x^2 - Dy^2 = 4$ always leads to a solution of the original Pell equation. These shortcuts were extended by other Indian mathematicians to provide means for attacking many types of Pell's equation.

Shortcuts for solving Pell type equations:

I)

$$(p, q; \pm 1) \Rightarrow (2p^2 - +1, 2pq; 1)$$

II)

$$(p, q; \pm 2) \Rightarrow (p^2 - +1, pq; 1)$$

III)

$$(p, q; 4) \Rightarrow \begin{cases} (p^2/2 - 1, pq/2; 1) & \text{if } p \text{ is even} \\ (p(p^2 - 3)/2, q(p^2 - 1)/2; 1) & \text{if } p \text{ is odd} \end{cases}$$

IV)

$$(p, q; -4) \Rightarrow \begin{cases} ((p^2 + 2)/2, pq/2; 1) & \text{if } p \text{ is even} \\ (P, Q; q) & \text{if } p \text{ is odd} \end{cases}$$

where $P = (p^2 + 2)((p^2 + 1)(p^2 + 3) - 2)/2, Q = pq(p^2 + 1)(p^2 + 3)/2$

For example, in the example above we had the solution (3,1;4) for $D = 5$, so that shortcut II would immediately give (9,4;1) which we found above after several compositions.

The shortcuts follow by the methods used by Brahmagupta. For example, to show I, suppose we have $(p, q; \pm 1)$. By composition we have $(p, q, \pm 1) * (p, q, \pm 1) = (p^2 + Dq^2, 2pq; 1)$ and using $p^2 - Dq^2 = \pm 1$ we can write $Dq^2 = p^2 - \pm 1$ to give the result of I. The other shortcuts arise by composition and dividing the results by powers of 2.

Bhaskara solves Pell's equation by starting with some solution $p_0^2 - Dq_0^2 = m_0$ of a related problem with additive m_0 , that is $(p_0, q_0; m_0)$ in our notation above. He then constructs $(p_i, q_i; m_i), i = 1, 2, \dots$ and claims that eventually a solution $(p_k, q_k; 1)$ of Pell's equation will be obtained. He starts with the equation $p_0^2 - D \cdot 1^2 = m_0$ by choosing p_0 the largest integer less than \sqrt{D} , and then $q_0 = 1, m_0 = p_0^2 - D$. He then composes $(p_0, 1, p_0^2 - D) * (x_1, 1; x_1^2 - D)$ to get $(p_0x_1 + D, p_0 + x_1; m_0(x_1^2 - D))$ and chooses x_1 so that the equation can be divided by m_0^2 . So we must choose x_1 so that $p_0x_1 + D$ is a multiple of m_0 and $p_0 + x_1$ is a multiple of m_0 . Of course there are many choices for x_1 , since altering it by adding a multiple of m_0 does not change the property we desire. Indian mathematicians knew how to solve $rx + sm_0 = c$ so that solving these equations involves the Euclidean algorithm. In fact it is enough to find x_1 so that $p_0 + x_1 = sm_0$, for then $p_0x_1 + D = p_0(sm_0 - p_0) + D = p_0^2 - D + m_0sp_0 = m_0 + m_0sp_0$. Further, $x_1^2 - D = (sm_0 - p_0)^2 - D = s^2m_0^2 - 2sm_0p_0 + p_0^2 - D = (s^2m_0 - 2sp_0 + 1)m_0$. Once x_1 is chosen we would then have a new integer solution to the equation $((p_0x_1 + D)/|m_0|, (p_0 + x_1)/|m_0|, (x_1^2 - D)/m_0)$. It is natural to choose x_1 so that $x_1^2 - D$ is as small as possible so that the new equation we get is of the form $(p_1, q_1; m_1)$ with $m_1 = (x_1^2 - D)/m_0$ as small as possible. So we agree to choose $p_0 + x_1 \equiv 0 \pmod{m_0}, x_1 < \sqrt{N} < x - 1 + |m_0|$.

We then continue in this manner. If we have constructed $(p_i, q_i; m_i)$ we choose x_{i+1} and form $(p_i, q_i; m_i) * (x_{i+1}, 1, x_{i+1}^2 - D) = (p_ix_{i+1} + Dq_i, p_i + q_ix_{i+1}, m_i(x_{i+1}^2 - D))$. As before we have many possible x_{i+1} such that $p_i + q_ix_{i+1}$ is a multiple of m_i and we choose the one closest to \sqrt{D} (in the sense $x_{i+1} < \sqrt{D} < x_{i+1} + |m_i|$). Then we get $(p_{i+1}, q_{i+1}, m_{i+1}) = ((p_ix_{i+1} + Dq_i)/|m_i|, (p_i + q_ix_{i+1})/|m_i|, (x_{i+1}^2 - D)/m_i)$.

Bhaskara carried this out in many examples and observed that eventually a solution to Pell's equation resulted. In fact the m_i produced are all between $-2\sqrt{D}$ and $2\sqrt{D}$ and are integers, so they keep cycling around and repeating, which perhaps gave rise to the Sanskrit name chakravala (the Sanskrit name for wheel or cycle).

We summarize the steps of the chakravala algorithm to solve $x^2 - Dy^2 = 1$:

- i) Choose p_0 to be the largest integer less than \sqrt{D} and $q_0 = 1, m_0 = p_0^2 - D$
- ii) When $(p_i, q_i; m_i)$ has been obtained, choose x_{i+1} so that

$$p_i + x_{i+1}q_i \equiv 0 \pmod{m_i}, x_{i+1} < \sqrt{D} < x_{i+1} + |m_i|$$

and define

$$p_{i+1} = \frac{p_ix_{i+1} + q_iD}{|m_i|}, q_{i+1} = \frac{p_i + q_ix_{i+1}}{|m_i|}, m_{i+1} = \frac{x_{i+1}^2 - D}{m_i}$$

- iii) Continue the chakravala until $m_k = 1$ is obtained.

The solution of $x^2 - 5y^2 = 1$ can be done by this method and compared to Brahmagupta's method. We start with p_0 the largest integer less than $\sqrt{5}$, so $p_0 = 2, q_0 = 1, m_0 = -1$. We choose x_1 so that $p_0 + x_1$ is a multiple of $m_0 = -1$ and so that x_1 is near $\sqrt{5}$. So $x_1 = 2$ works and gives the new solution $(9, 4; 1)$ which we found before.

The method is more interesting for larger D . We consider the example on page 147 to solve $x^2 - 92y^2 = 1$. We begin with p_0 the greatest integer less than $\sqrt{92}$, that is 9, and $q_0 = 1$, and obtain the following:

$$\begin{aligned} (9, 1; -11) \quad x_1 &= 2 \\ (10, 1; 8) \quad x_2 &= 6 \\ (19, 2; -7) \quad x_3 &= 8 \\ (48, 5; 4) \quad x_4 &= 6 \\ (211, 22; -7) \quad x_5 &= 6 \\ (470, 49; 8) \quad x_6 &= 2 \\ (681, 71; -11) \quad x_7 &= 9 \\ (1151, 120, 1) \end{aligned}$$

so the solution is $1151^2 - 92 \cdot 120^2 = 1$.

The example on page 148 to solve $x^2 - 67y^2 = 1$ begins with p_0 the greatest integer less than $\sqrt{67}$, that is 8, and $q_0 = 1$, and results in the following:

$$\begin{aligned} (8, 1; -3) \quad x_1 &= 7 \\ (41, 5; 6) \quad x_2 &= 5 \\ (90, 11; -7) \quad x_3 &= 2 \\ (131, 16; 9) \quad x_4 &= 7 \\ (221, 27; -2) \quad x_5 &= 7 \\ (1678, 205; 9) \quad x_6 &= 2 \\ (1899, 232; -7) \quad x_7 &= 5 \\ (3577, 437; 6) \quad x_8 &= 7 \\ (9053, 1106; -3) \quad x_9 &= 8 \\ (48842, 5967; 1) \end{aligned}$$

References: V.S. Varadarajan, Algebra in Ancient and Modern Times, American Math. Soc. 1998