Chakravala method

From Wikipedia, the free encyclopedia

The ***chakravala* method** (Sanskrit: चक्रवाल विधि) is a cyclic algorithm to solve indeterminate quadratic equations, including Pell's equation. It is commonly attributed to Bhāskara II, (c. 1114 – 1185 CE)[1][2] although some attribute it to Jayadeva (c. 950 ~ 1000 CE).[3] Jayadeva pointed out that Brahmagupta's approach to solving equations of this type could be generalized, and he then described this general method, which was later refined by Bhāskara II in his *Bijaganita* treatise. He called it the Chakravala method: *chakra* meaning "wheel" in Sanskrit, a reference to the cyclic nature of the algorithm.[4] E. O. Selenius held that no European performances at the time of Bhāskara, nor much later, exceeded its marvellous height of mathematical complexity.[1][4]

This method is also known as the **cyclic method** and contains traces of mathematical induction.[5]

Contents [hide]

History [edit]

Chakra in Sanskrit means cycle. As per popular legend, Chakravala indicates a mythical range of mountains which orbits around the earth like a wall and not limited by light and darkness.[6]

Brahmagupta in 628 CE studied indeterminate quadratic equations, including Pell's equation

$$x^2 = Ny^2 + 1,$$

for minimum integers *x* and *y*. Brahmagupta could solve it for several *N*, but not all.

Jayadeva (9th century) and Bhaskara (12th century) offered the first complete solution to the equation, using the *chakravala* method to find for $x^2 = 61y^2 + 1$, the solution

$$x = 1766319049, y = 226153980.$$

This case was notorious for its difficulty, and was first solved in Europe by Brouncker in 1657–58 in response to a challenge by Fermat, using continued fractions. A method for the general problem was first completely described rigorously by Lagrange in 1766.[7] Lagrange's method, however, requires the calculation of 21 successive convergents of the continued fraction for the square root of 61, while the *chakravala* method is much simpler. Selenius, in his assessment of the *chakravala* method, states

> "The method represents a best approximation algorithm of minimal length that, owing to several minimization properties, with minimal effort and avoiding large numbers automatically produces the best solutions to the equation. The *chakravala* method anticipated the European methods by more than a thousand years. But no European performances in the whole field of algebra at a time much later than Bhaskara's, nay nearly equal up to our times, equalled the marvellous complexity and ingenuity of *chakravala*."[1][4]

Hermann Hankel calls the *chakravala* method

> "the finest thing achieved in the theory of numbers before Lagrange."[8]

The method [edit]

From Brahmagupta's identity, we observe that for given *N*,

$$(x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) = (x_1x_2 + Ny_1y_2)^2 - N(x_1y_2 + x_2y_1)^2$$

For the equation $x^2 - Ny^2 = k$, this allows the "composition" (*samāsa*) of two solution triples (x_1, y_1, k_1)

and (x_2, y_2, k_2) into a new triple

$$(x_1x_2 + Ny_1y_2\,,\; x_1y_2 + x_2y_1\,,\; k_1k_2).$$

In the general method, the main idea is that any triple (a, b, k) (that is, one which satisfies $a^2 - Nb^2 = k$) can be composed with the trivial triple $(m, 1, m^2 - N)$ to get the new triple $(am + Nb, a + bm, k(m^2 - N))$ for any *m*. Assuming we started with a triple for which $\gcd(a, b) = 1$, this can be scaled down by *k* (this is Bhaskara's lemma):

$$a^2 - Nb^2 = k \Rightarrow \left(\frac{am + Nb}{k}\right)^2 - N\left(\frac{a + bm}{k}\right)^2 = \frac{m^2 - N}{k}$$

Since the signs inside the squares do not matter, the following substitutions are possible:

$$a \leftarrow \frac{am + Nb}{|k|}, b \leftarrow \frac{a + bm}{|k|}, k \leftarrow \frac{m^2 - N}{k}$$

When a positive integer *m* is chosen so that (*a* + *bm*)/*k* is an integer, so are the other two numbers in the triple. Among such *m*, the method chooses one that minimizes the absolute value of $m^2 - N$ and hence that of $(m^2 - N)/k$. Then the substitution relations are applied for *m* equal to the chosen value. This results in a new triple (*a*, *b*, *k*). The process is repeated until a triple with $k = 1$ is found. This method always terminates with a solution (proved by Lagrange in 1768).[9] Optionally, we can stop when *k* is ±1, ±2, or ±4, as Brahmagupta's approach gives a solution for those cases.

Examples [edit]

n = 61 [edit]

The *n* = 61 case (determining an integer solution satisfying $a^2 - 61b^2 = 1$), issued as a challenge by Fermat many centuries later, was given by Bhaskara as an example.[9]

We start with a solution $a^2 - 61b^2 = k$ for any *k* found by any means. In this case we can let *b* be 1, thus, since $8^2 - 61 \cdot 1^2 = 3$, we have the triple $(a, b, k) = (8, 1, 3)$. Composing it with $(m, 1, m^2 - 61)$ gives the triple $(8m + 61, 8 + m, 3(m^2 - 61))$, which is scaled down (or Bhaskara's lemma is directly used) to get:

$$\left(\frac{8m + 61}{3}, \frac{8 + m}{3}, \frac{m^2 - 61}{3}\right).$$

For 3 to divide $8 + m$ and $|m^2 - 61|$ to be minimal, we choose $m = 7$, so that we have the triple $(39, 5, -4)$. Now that *k* is −4, we can use Brahmagupta's idea: it can be scaled down to the rational solution $(39/2, 5/2, -1)$, which composed with itself three times, with $m = 7, 11, 9$ respectively, when k becomes square and scaling can be applied, this gives $(1523/2, 195/2, 1)$. Finally, such procedure can be repeated until the solution is found (requiring 9 additional self-compositions and 4 additional square-scalings): $(1766319049,\ 226153980,\ 1)$. This is the minimal integer solution.

n = 67 [edit]

Suppose we are to solve $x^2 - 67y^2 = 1$ for *x* and *y*.[10]

We start with a solution $a^2 - 67b^2 = k$ for any *k* found by any means; in this case we can let *b* be 1, thus producing $8^2 - 67 \cdot 1^2 = -3$. At each step, we find an *m* > 0 such that *k* divides *a* + *bm*, and $|m^2 - 67|$ is minimal. We then update *a*, *b*, and *k* to $\frac{am + Nb}{|k|}, \frac{a + bm}{|k|}, \text{ and } \frac{m^2 - N}{k}$ respectively.

First iteration

We have $(a, b, k) = (8, 1, -3)$. We want a positive integer *m* such that *k* divides *a* + *bm*, i.e. 3 divides 8 + m, and $|m^2 - 67|$ is minimal. The first condition implies that *m* is of the form 3*t* + 1 (i.e. 1, 4, 7, 10,… etc.), and among such *m*, the minimal value is attained for *m* = 7. Replacing (*a*, *b*, *k*) with $\left(\frac{am + Nb}{|k|}, \frac{a + bm}{|k|}, \frac{m^2 - N}{k}\right)$, we get the new values $a = (8 \cdot 7 + 67 \cdot 1)/3 = 41, b = (8 + 1 \cdot 7)/3 = 5, k = (7^2 - 67)/(-3) = 6$. That is, we have the new solution:

$$41^2 - 67 \cdot (5)^2 = 6.$$

At this point, one round of the cyclic algorithm is complete.

Second iteration

We now repeat the process. We have $(a, b, k) = (41, 5, 6)$. We want an $m > 0$ such that k divides $a + bm$, i.e. 6 divides 41 + 5m, and $|m^2 - 67|$ is minimal. The first condition implies that m is of the form 6t + 5 (i.e. 5, 11, 17,… etc.), and among such m, $|m^2 - 67|$ is minimal for m = 5. This leads to the new solution a = (41·5 + 67·5)/6, etc.:

$$90^2 - 67 \cdot 11^2 = -7.$$

Third iteration

For 7 to divide 90 + 11m, we must have m = 2 + 7t (i.e. 2, 9, 16,… etc.) and among such m, we pick m = 9.

$$221^2 - 67 \cdot 27^2 = -2.$$

Final solution

At this point, we could continue with the cyclic method (and it would end, after seven iterations), but since the right-hand side is among ±1, ±2, ±4, we can also use Brahmagupta's observation directly. Composing the triple (221, 27, −2) with itself, we get

$$\left(\frac{221^2 + 67 \cdot 27^2}{2}\right)^2 - 67 \cdot (221 \cdot 27)^2 = 1,$$

that is, we have the integer solution:

$$48842^2 - 67 \cdot 5967^2 = 1.$$

This equation approximates $\sqrt{67}$ as $\dfrac{48842}{5967}$ to within a margin of about 2×10^{-9}.

Notes [edit]

1. ^ a b c Hoiberg & Ramchandani – Students' Britannica India: Bhaskaracharya II, page 200
2. ^ Kumar, page 23
3. ^ Plofker, page 474
4. ^ a b c Goonatilake, page 127 – 128
5. ^ Cajori (1918), p. 197

   > "The process of reasoning called "Mathematical Induction" has had several independent origins. It has been traced back to the Swiss Jakob (James) Bernoulli, the Frenchman B. Pascal and P. Fermat, and the Italian F. Maurolycus. [...] By reading a little between the lines one can find traces of mathematical induction still earlier, in the writings of the Hindus and the Greeks, as, for instance, in the "cyclic method" of Bhaskara, and in Euclid's proof that the number of primes is infinite."

6. ^ Gopal, Madan (1990). K.S. Gautam, ed. *India through the ages*. Publication Division, Ministry of Information and Broadcasting, Government of India. p. 79.
7. ^ O'Connor, John J.; Robertson, Edmund F., "Pell's equation", *MacTutor History of Mathematics archive*, University of St Andrews.
8. ^ Kaye (1919), p. 337.
9. ^ a b John Stillwell (2002), *Mathematics and its history* (2 ed.), Springer, pp. 72–76, ISBN 978-0-387-95336-6
10. ^ The example in this section is given (with notation Q_n for k, P_n for m, etc.) in: Michael J. Jacobson; Hugh C. Williams (2009), *Solving the Pell equation*, Springer, p. 31, ISBN 978-0-387-84922-5

References [edit]

- Florian Cajori (1918), Origin of the Name "Mathematical Induction", *The American Mathematical Monthly* **25** (5), p. 197-201.
- George Gheverghese Joseph, *The Crest of the Peacock: Non-European Roots of Mathematics* (1975).
- G. R. Kaye, "Indian Mathematics", *Isis* **2**:2 (1919), p. 326–356.
- C. O. Selenius, "Rationale of the chakravala process of Jayadeva and Bhaskara II", *Historia Mathematica* **2** (1975), pp. 167-184.
- C. O. Selenius, "Kettenbruch theoretische Erklarung der zyklischen Methode zur Losung der Bhaskara-Pell-Gleichung", *Acta Acad. Abo. Math. Phys.* **23** (10) (1963).
- Hoiberg, Dale & Ramchandani, Indu (2000). *Students' Britannica India*. Mumbai: Popular Prakashan. ISBN 0-

85229-760-2

- Goonatilake, Susantha (1998). *Toward a Global Science: Mining Civilizational Knowledge*. Indiana: Indiana University Press. ISBN 0-253-33388-1.
- Kumar, Narendra (2004). *Science in Ancient India*. Delhi: Anmol Publications Pvt Ltd. ISBN 81-261-2056-8
- Ploker, Kim (2007) "Mathematics in India". *The Mathematics of Egypt, Mesopotamia, China, India, and Islam: A Sourcebook* New Jersey: Princeton University Press. ISBN 0-691-11485-4
- Edwards, Harold (1977). *Fermat's Last Theorem*. New York: Springer. ISBN 0-387-90230-9.

External links [edit]

- Introduction to chakravala

V · T · E

Number-theoretic algorithms [hide]	
Primality tests	AKS TEST · APR TEST · Baillie–PSW · ECPP TEST · Elliptic curve · Pocklington · Fermat · Lucas · *LUCAS–LEHMER* · *LUCAS–LEHMER–RIESEL* · *PROTH'S THEOREM* · *PÉPIN'S* · Quadratic Frobenius test · Solovay–Strassen · Miller–Rabin
Prime-generating	Sieve of Atkin · Sieve of Eratosthenes · Sieve of Sundaram · Wheel factorization
Integer factorization	Continued fraction (CFRAC) · Dixon's · Lenstra elliptic curve (ECM) · Euler's · Pollard's rho · $p - 1$ · $p + 1$ · Quadratic sieve (QS) · General number field sieve (GNFS) · *Special number field sieve (SNFS)* · Rational sieve · Fermat's · Shanks' square forms · Trial division · Shor's
Multiplication	Ancient Egyptian · Long · Karatsuba · Toom–Cook · Schönhage–Strassen · Fürer's
Discrete logarithm	BABY-STEP GIANT-STEP · Pollard rho · Pollard kangaroo · POHLIG–HELLMAN · Index calculus · Function field sieve
Greatest common divisor	Binary · Euclidean · Extended Euclidean · Lehmer's
Modular square root	Cipolla · Pocklington's · Tonelli–Shanks
Other algorithms	**Chakravala** · Cornacchia · Integer relation · Integer square root · Modular exponentiation · Schoof's
Italics indicate that algorithm is for numbers of special forms · SMALLCAPS indicate a deterministic algorithm	

Categories: Brahmagupta | Diophantine equations | Number theoretic algorithms | Indian mathematics