

De cyclische methode in India.

Samenvatting van de methoden van Bhaskara (1117-1184) in moderne notatie. Alle getallenvoorbeelden hieronder staan bij Bhaskara.

1. **Het probleem:** gegeven $N \in \mathbf{N}$, geen kwadraat. Gevraagd: $x, y \in \mathbf{N}$ zodat

$$y^2 - Nx^2 = 1.$$

2. **Vermenigvuldigingsformule:**

$$(a^2 - Nb^2)(c^2 - Nd^2) = (ac + Nbd)^2 - N(ad + bc)^2.$$

Toepassing: o.a. om uit oplossingen nieuwe oplossingen te maken. Bijvoorbeeld:

$N = 8$. Gemakkelijke oplossing: $3^2 - 8 \cdot 1^2 = 1$. Hieruit:

$$1 = 1 \cdot 1 = (3^2 - 8 \cdot 1^2)(3^2 - 8 \cdot 1^2) = (3 \cdot 3 + 8 \cdot 1 \cdot 1)^2 - 8(3 \cdot 1 + 1 \cdot 3)^2 = 17^2 - 8 \cdot 6^2.$$

$$1 = 1 \cdot 1 = (17^2 - 8 \cdot 6^2)(3^2 - 8 \cdot 1^2) = (17 \cdot 3 + 8 \cdot 6 \cdot 1)^2 - 8(17 \cdot 1 + 6 \cdot 3)^2 = 99^2 - 8 \cdot 35^2$$

enzovoort. Zo krijg je 'oneindig veel' oplossingen, zegt Bhaskara.

3. **Moeilijker gevallen: nieuw probleem en wegdeeltruc.**

Als je een probleem niet meteen kunt oplossen, kijk dan naar een verwant probleem. Bijvoorbeeld: Gegeven $N \in \mathbf{N}$. Is er een klein getal $p \in \mathbf{Z}$ (het 'toevoegsel' van Bhaskara) zodat $y^2 - Nx^2 = p$? Soms lukt het dan m.b.v. de vermenigvuldigingsformule.

Voorbeeld: $N = 11$, $3^2 - 11 \cdot 1^2 = -2$. Hieruit:

$$4 = (-2) \cdot (-2) = (3^2 - 11 \cdot 1^2)(3^2 - 11 \cdot 1^2) = (3 \cdot 3 + 11 \cdot 1 \cdot 1)^2 - 11 \cdot (3 \cdot 1 + 1 \cdot 3)^2 = 20^2 - 11 \cdot 6^2.$$

Alles door 4 delen geeft: $1 = 10^2 - 11 \cdot 3^2$. Deze wegdeeltruc werkt volgens Bhaskara bij

$$p = -1, \pm 2, \pm 4.$$

4. **Nog moeilijkere gevallen: de 'cyclische methode'.**

Voorbeeld: $N = 67$. Het dichtstbijzijnde kwadraat is $64 = 8^2$. We hebben nu: $8^2 - 67 \cdot 1^2 = -3$.

Vermenigvuldig dit met $r^2 - 67 \cdot 1^2 = s$ met r, s nog te bepalen. Dit geeft:

$$-3 \cdot s = (8^2 - 67 \cdot 1^2)(r^2 - 67 \cdot 1^2) = (8r + 67)^2 - 67(r + 8)^2.$$

Omdat we de wegdeeltruc willen toepassen kiezen we r zodat $r + 8$ deelbaar is door 3, en daarbij $|s|$ zo klein mogelijk (maar niet nul). Oplossing: $r = 7, s = -18$. We krijgen $123^2 - 67 \cdot 15^2 = 54$. We kunnen nu delen door 3^2 ! Resultaat: $41^2 - 67 \cdot 5^2 = 6$. Helaas geen 1, maar 6 is niet te groot.

Volgende stap: vermenigvuldig dit weer met $r^2 - 67 \cdot 1^2 = s$ met r, s nog te bepalen.

Resultaat: $(41r + 67 \cdot 5)^2 - 67 \cdot (5r + 41)^2 = 6s$. Kies nu weer r, s zodat $5r + 41$ deelbaar is door 6 en $|s|$ zo klein mogelijk is, niet 0. Antwoord: $r = 5, s = -42$, $540^2 - 67 \cdot 66^2 = -6 \cdot 42$. Delen door 6^2 geeft $90^2 - 67 \cdot 11^2 = -7$.

Volgende stap: Vermenigvuldigingen met $r^2 - 67 \cdot 1^2 = s$ met r, s nog te bepalen.

Resultaat: $(90r + 67 \cdot 11)^2 - 67 \cdot (90 + 11r)^2 = -7s$. Nu r bepalen zodat $90 + 11r$ deelbaar is door 7 en $|s|$ zo klein mogelijk is. Antwoord: $r = 9, s = 14$. We krijgen

$1547^2 - 67 \cdot 189^2 = -7 \cdot 14$. Delen door 7^2 geeft $221^2 - 67 \cdot 27^2 = -2$. We hebben nu één van de gevallen $p = -1, \pm 2, \pm 4$ gekregen.

Tenslotte: Vermenigvuldig dit met zichzelf: $(221 \cdot 221 + 67 \cdot 27 \cdot 27)^2 - 67 \cdot (2 \cdot 221 \cdot 27)^2 = 4$.

Delen door 4 geeft $48842^2 - 67 \cdot 5967^2 = 1$.

5. Het allermoeilijkste geval onder de $N=100$. Op dezelfde manier behandelt Bhaskara $N = 61$. Resultaat: $1766319049^2 - 61 \cdot 226153980^2 = 1$.

Teksten. Bhāskara II (1114-1178), deel 2, de *Bījaganita* (Algebra) van zijn *Siddhānta-Śiromani* (Krans der Wetenschappen).

Hoofdstuk 3. (Colebrooke pp. 170-176).

75. Zes en een half coupletten. Regels voor het onderzoeken van de vierkantswortel van een grootheid met één erbij: laat een getal aangenomen worden, en de “kleinste” wortel genoemd worden. Het getal dat opgeteld moet worden bij het product van zijn kwadraat met de gegeven coëfficiënt om de som of het verschil een wortel te laten hebben, noemen de wiskundigen een positief of negatief toevoegsel; en zij noemen die wortel de “grootste”.

76. Als de “kleinste” en “grootste” wortels en het toevoegsel naast elkaar geschreven worden, en dezelfde of andere eronder gezet worden, kunnen daaruit vele wortels afgeleid worden door “compositie”. Daarom wordt de compositie nu uiteengezet.

77. De “grootste” en de “kleinste” wortels moeten kruiselings met elkaar vermenigvuldigd worden, en de som van de producten als (nieuwe) “kleinste” wortel genomen worden. Het product van de twee “kleinste” wortels en de gegeven coëfficiënt, opgeteld bij het product van de twee “grootste” wortels, is de (nieuwe) “grootste” wortel, en het product van de toevoegsels is het (nieuwe) toevoegsel.

...

83-86. Regel voor de methode van de cirkel. Maak de ‘kleinste’ en de ‘grootste’ wortel en het ‘toevoegsel’ een ‘deeltal’, ‘toevoegsel’ en ‘deler’, en vind hieruit de ‘factor’. Als het kwadraat van deze factor van de geveel coëfficiënt afgetrokken wordt of de coëfficiënt van het kwadraat afgetrokken wordt (zodat de rest klein is), dan is de rest, gedeeld door het oorspronkelijke toevoegsel, een nieuw toevoegsel, die van teken verwisseld wordt als (het kwadraat) van de coëfficiënt afgetrokken is. Het quotiënt dat met de factor overeenkomt is de ‘kleinste’ wortel, en daaruit kan de ‘grootste’ wortel worden afgeleid. Hiermee wordt het proces herhaald, waarbij je de vorige wortels en het (vorige) toevoegsel terzijde legt. Deze methode noemen de wiskundigen de methode van de cirkel. Daarmee vind je gehele wortels met vier, twee of één als toevoegsel, en door ‘compositie’ kun je wortels voor toevoegsel één afleiden uit de wortels voor toevoegsel twee en vier.

87. Voorbeeld. Wat is het kwadraat dat vermenigvuldigd met zeven en zestig en één bij het product opgeteld, weer een kwadraatswortel heeft? En wat is het kwadraat dat, vermenigvuldigd met één en zestig, met één bij het product opgeteld, dezelfde eigenschap heeft? Geef dat, vriend, als de methode van het ‘kwadraat met toevoegsel’ als een klimplant grondig over je geest verspreid is.

Literatuur

1. *Algebra with arithmetic and mensuration from the Sanscrit of Brahme Gupta and Bhāscara*. Translated by H. T. Colebrooke. London 1817. (Herdruk Wiesbaden 1973). [MI Utr. BR 01.75-1] (zie vooral pp. 156-178)
2. Harold M. Edwards. *Fermat’s last theorem. A genetic introduction to algebraic number theory*. New York etc. (Springer-Verlag) 1977. (Zie vooral pp. 25-36).