John Simons
Universiteit Groningen
Technische Bedrijfskunde
Postbus 800, 9700 AV Groningen
j.l.simons@tbk.rug.nl

Benne de Weger
Technische Universiteit Eindhoven
Faculteit Wiskunde en Informatica
Postbus 513, 5600 MB Eindhoven
b.m.m.d.weger@tue.nl

NMC-225 prijsvraag

Mersenne en het Syracuseprobleem

In 2003 vierde het Koninklijk Wiskundig Genootschap haar 225-ste verjaardag. Ter gelegenheid hiervan schreef het bestuur een prijsvraag uit. Er viel 225 euro te verdienen met de formulering van het meest originele wiskundige probleem met uitkomst 225. Donderdag 1 mei 2003 werd tijdens het Nederlands Mathematisch Congres in Nijmegen deze prijs toegekend aan John Simons, hoogleraar Bestuurlijke Informatiekunde in Groningen. Samen met Benne de Weger, cryptoloog aan de Technische universiteit Eindhoven, doen zij onderzoek naar het $3x+1$-probleem. Hun oplossing voor de prijsvraag is aan dit probleem gerelateerd.

Wie het raadsel van Syracuse wil doorgronden
zal zelden een cyclus hebben gevonden.
Maar als het WG gaat verjaren
wel generale cycli ontwaren,
kwadratisch met Mersenne verbonden.

Het $3x+1$-probleem (ook bekend onder de namen 'Syracuse probleem' en 'Kakutani probleem' en 'probleem van Collatz') gaat om het volgende. Definieer een rij $(x_n)_{n\geq 0}$ door een geheel getal $x_0 > 0$ te kiezen, en verder $x_{n+1} = x_n/2$ voor even x_n en $x_{n+1} = (3x_n+1)/2$ voor oneven x_n. Het $3x+1$ vermoeden zegt dat voor iedere keuze x_0 op den duur de cykel $(1,2)$ verschijnt. Onder meer Paul Erdös bood een geldbedrag voor een bewijs van dit $3x+1$ vermoeden. Ondanks diverse benaderingen laat zo'n bewijs nog altijd op zich wachten.

Generalisaties van het probleem worden bijvoorbeeld gekregen door een oneven q te nemen in de stap $x_{n+1} = (3x_n+q)/2$ voor x_n oneven. Een vermoeden van Lagarias (1990) zegt dat als $q > 3$ (en $q \neq 3^t$), dan is er behalve de cykel $(q, 2q)$ nog minstens een andere cykel. Volgens een vermoeden van Möller (1978) is voor elke q het aantal cykels eindig. Als we uitgaan van de juistheid hiervan, dan is de notatie $S(q)$ voor de som van alle cykellengtes in het $3x+q$-probleem, goedgedefinieerd.

Voor het oneven getal q in deze generalisatie kan in het bijzonder het k-de Mersenne-getal $M_k := 2^k - 1$, of het kwadraat M_k^2 daarvan, genomen worden. In deze tekst schetsen we een aanpak om het al dan niet bestaan van cykels $\neq (1,2)$ voor het $3x+1$-probleem aan te tonen. Deze aanpak blijkt ook voor het meer algemene $3x+q$-probleem van toepassing. Verder behandelen we aanvullende vermoedens en resultaten ter ondersteuning van het *NMC-225 Vermoeden*, hetgeen zegt dat (voor $k > 2$) het getal $S(M_k^2) - S(M_k)$ minimaal is voor $M_k^2 = 225$.

Het $3x+1$-probleem (intuïtief)

Als er voor het $3x+1$-probleem een cykel is bestaande uit K oneven getallen en L even 'grote' getallen, dan is $2^{K+L} \approx 3^K$. Immers, na L keer door 2 delen en K keer met ongeveer $3/2$ vermenigvuldigen ben je terug bij af, dus $2^{-L} \cdot (3/2)^K \approx 1$. Er volgt, dat $(K+L)/K$ een 'goede' benadering voor $\log 3/\log 2$ is. De vraag is, wat 'groot' en 'goed' in dit argument inhouden. Om dit te illustreren, beperken we ons tot het speciale geval van een cykel $(x_0, \ldots, x_{K+L-1})$ bestaande uit K oneven gevolgd door L even getallen.

Het is eenvoudig na te gaan dat $x_0 = a \cdot 2^K - 1$ en $x_K = a \cdot 3^K - 1$ voor zeker oneven getal a. Verder is $x_K/2^L = x_0$. Dit levert de vergelijking $(2^{K+L} - 3^K) \cdot a = 2^L - 1$, die we herschrijven als $1 - 3^K/2^{K+L} = (2^L-1)/(a \cdot 2^{K+L})$. Het rechterlid is kleiner dan $1/(a \cdot 2^K)$, dus een noodzakelijke voorwaarde voor het bestaan van onze cykel is een oplossing van de ongelijkheid $1 < 2^{K+L}/3^K < 1 + 1/(a \cdot 2^K - 1)$. Omdat $\log(1+x) < x$ voor $0 < x < 1$, volgt dat $0 < (K+L)\log 2 - K \log 3 < 1/(a \cdot 2^K - 1)$, oftewel $0 < (K+L)/K - \log 3/\log 2 < 1/(K \cdot \log 2 \cdot (a \cdot 2^K - 1))$.

Het rechterlid is kleiner dan $1/(2 \cdot K^2)$, mits $K \geq 4$. Uit de theorie over rationale benaderingen van reële getallen volgt nu, dat $(K+L)/K$ een convergent is in de kettingbreukontwikkeling van $\log 3/\log 2$. We concluderen dat voor een cykel zoals hier wordt bekeken, geldt dat als $K \geq 4$ dan is $(K+L)/K$ een convergent in de kettingbreukontwikkeling van $\log 3/\log 2$. Merk op, dat $K \geq 4$ impliceert dat $x_0 = a \cdot 2^K - 1 \geq 15$ en dus ook alle $x_i \geq 15$.

Voor $K < 4$ blijkt alleen $K = L = 1$ een oplossing te zijn. Voor $K \geq 4$ bestaan er evenwel oneindig veel convergenten (zoals $8/5,\ 65/41,\ 485/306,\ \ldots$), dus is een extra argument nodig om het aantal oplossingen te beperken. Dit wordt gegeven door de theorie van *lineaire vormen in logaritmen*. Een fundamenteel resultaat van A. Baker (1968), later door anderen verfijnd, zegt dat lineaire vormen van het type $(K+L)\log 2 - K\log 3$, mits ze positief zijn, van beneden kunnen worden begrensd door een subexponentiele functie in K. Gecombineerd met de bovengrens $1/(a \cdot 2^K - 1)$ levert deze ondergrens een bovengrens voor K. Hiermee volstaat het, slechts een eindig aantal convergenten te testen.

De zo geschetste aanpak beschrijft de essentie van het bewijs van Steiner (1977) voor de stelling, dat $(1, 2)$ de enige cykel is bestaande uit K oneven getallen gevolgd door L even getallen.

Steiners aanpak uitgebreid

Een hypothetische cykel voor het $3x + 1$-probleem zou ook ingewikkelder kunnen zijn dan hierboven beschreven. In het algemeen bestaat zo'n cykel uit k_0 oneven getallen, gevolgd door l_0 even getallen, gevolgd door k_1 oneven getallen, gevolgd door ... enzovoort, met uiteindelijk k_{m-1} en l_{m-1} oneven/even getallen. Hierin zijn alle $k_i, l_i \geq 1$. We noemen dit een m-cykel. Een niet-triviale m-cykel is er per definitie een met alle $x_n > 2$. Het totaal aantal oneven getallen in een m-cykel is dus $K := \sum k_i$ en $L := \sum l_i$ is het aantal even getallen.

Voortbordurend op het werk van Steiner, bewees een van ons in 2003 dat er geen niet-triviale 2-cykels bestaan. In hetzelfde jaar konden we dit uitbreiden tot de stelling, dat er geen niet-triviale m-cykels bestaan, als tenminste $m \leq 68$. Dit bewijs maakt gebruik van een ondergrens voor K die gebaseerd is op een generalisatie van een lemma van Crandall (1978), en een bovengrens voor K, verkregen uit diophantische approximatie technieken. Een belangrijk ingredient hierbij is een diep resultaat van Laurent, Mignotte en Nesterenko (1995) over lineaire vormen in twee logaritmen. De ondergrens is een dalende functie van m. De bovengrens is een stijgende functie van m. Voor kleine m is de ondergrens groter dan de bovengrens, dus zijn er geen oplossingen voor K. Voor grotere m ontstaat een interval van mogelijke K-waarden. Voor $m > 68$ zijn er K, L-waarden die aan de noodzakelijke approximatie voorwaarde voor $\log 3 / \log 2$ voldoen. Dat zijn daarmee potentiële oplossingen. Voor een potentiële oplossing moeten op een efficiënte manier alle partities $K = k_0 + k_1 + \ldots + k_{m-1}$ worden geanalyseerd. Vooralsnog lijkt dit een blokkade voor een bewijs van het $3x + 1$ vermoeden.

Generalisaties

Soms wordt een beter begrip van een probleem gekregen door het in te bedden in een klasse van meer algemene problemen. Er bestaan diverse generalisaties van het $3x + 1$-probleem. Voor de hand liggen het $3x + q$-probleem ($q > 1$ oneven), het $px + 1$-probleem ($p > 3$ oneven) en het $px + q$-probleem ($p > 3, q > 1$ beide oneven). Een ander soort generalisatie wordt gekregen door de speciale rol van 2 in het probleem door een ander getal te laten overnemen.

In de richting van het vermoeden van Lagarias hebben we het volgende resultaat.

Lemma 1. *Stel $q > 0$ is een oneven getal dat geschreven kan worden als $q = 2^r - 3^s$ met $s \geq 1$ en $(r, s) \neq (2, 1)$. Dan heeft het $3x + q$-probleem naast de cykel $(q, 2q)$ nog een andere 1-cykel.*

Bewijs. We beginnen net als bij het resultaat van Steiner. Is m voor het eerste oneven getal in de cykel, schrijf dan $m + q = a \cdot 2^k$ met a oneven. De cykel bestaat uit precies k oneven getallen, en het eerste even getal in de cykel is $a \cdot 3^k - q$. Dit is gelijk aan $2^l \cdot m$ omdat de cykel verder uit alleen nog even getallen (zeg $l \geq 1$ zulke getallen) bestaat. Zo krijgen we de vergelijking

$$a \cdot \left(2^{k+l} - 3^k\right) = q \cdot \left(2^l - 1\right).$$

De oplossing $a = q, k = l = 1$ correspondeert met de cykel $(q, 2q)$. In het geval dat q te schrijven is als $q = 2^r - 3^s$, is ook $a = 2^l - 1$, $k = s$, $l = r - s$ een oplossing. Deze levert een 1-cykel met s oneven en $r - s$ even getallen, mits $s > 0$. Als bovendien $(r, s) \neq (2, 1)$ dan is de tweede cykel verschillend van de eerste. □

Als voorbeeld bij dit lemma nemen we het $3x + 997$-probleem ($997 = 2^{10} - 3^3$). Dit heeft de niet-triviale 1-cykel $(19, 527, 1289, 2432, 1216, 608, 304, 152, 76, 38)$.

Het $px + q$-probleem (experimenteel)

Crandall liet in 1978 zien, dat voor veel beginwaarden x_0, de bijbehorende rij van het $px + 1$-probleem ($p > 3$) divergeert. Ditzelfde geldt voor het $px + q$-probleem met $p > 3$ en $q > 1$, maar in dit geval komen ook niet-triviale cykels voor. Zo heeft het $7x + 11$-probleem een cykel van lengte 34 bestaande uit getallen in het interval $(23, 34092)$. Experimenten voor allerlei waarden p, q geven dan aanleiding tot de volgende uitspraak: voor elk paar p, q is het aantal niet-triviale cykels eindig. Voor $p = 3$ blijkt dit aantal een stijgende functie van q.

Het $3x + q$-probleem (theoretisch)

Onze uitbreiding van de aanpak van Steiner generaliseert ook naar het $3x + q$-probleem. De onderstaande regels geven een summiere schets hiervan.

Stel dat een m-cykel voor het $3x + q$-probleem bestaat. Deze bevat dan een aantal (zeg K) oneven getallen en een aantal (zeg L) even getallen. We mogen veronderstellen dat het eerste getal in de cykel oneven is en het laatste even. De cykel bestaat dan uit $k_0 > 0$ oneven getallen, gevolgd door $l_0 > 0$ even getallen, gevolgd door $k_1 > 0$ oneven getallen, enzovoort, tot een zekere $l_{m-1} > 0$ even getallen. Dan is $K = \sum_i k_i$ en $L = \sum_i l_i$.

Evenals in het bewijs van lemma 1 kunnen we schrijven $x_0 = a_0 \cdot 2^{k_0} - q$ voor zekere oneven a_0, en $x_{k_0} = a_0 \cdot 3^{k_0} - q$. Dan is $x_{k_0+l_0} = [a_0 \cdot 3^{k_0} - q]/2^{l_0} = a_1 \cdot 2^{k_1} - q$ voor zekere oneven a_1. Zo redenerend komen we tot oneven getallen $a_2, \ldots, a_{m-1}$ met de eigenschap $x_{k_i+l_i} = [a_i \cdot 3^{k_i} - q]/2^{l_i} = a_{i+1} \cdot 2^{k_{i+1}} - q$.

De laatste gelijkheid kan worden herschreven als $2^{k_{i+1}+l_i}/3^{k_i} = [a_i - q \cdot 3^{-k_i}]/[a_{i+1} - q \cdot 2^{-k_{i+1}}]$. Vermenigvuldigen van deze vergelijkingen levert $1 < 2^{K+L}/3^K < \prod_i [a_i \cdot 2^{k_i}]/[a_i \cdot 2^{k_i} - q]$. Dit impliceert $0 < (K + L)\log 2 - K \log 3 < \sum_i q/[a_i \cdot 2^{k_i} - q] = q \sum_i 1/x_i$.

We kunnen zonder verlies van algemeenheid aannemen, dat x_0 het minimale element is in de cykel, en dan volgt

$$0 < (K + L)\log 2 - K \log 3 < m \cdot q/x_0.$$

Op analoge wijze als voor het $3x + 1$-probleem kan vervolgens een bovengrens en een ondergrens voor K worden afgeleid. Zo kunnen voor kleine m alle m-cykels worden gevonden.

Mersenne generalisaties

Berekeningen suggereren, dat het $3x + 7$-probleem precies 2 cykels heeft, namelijk met lengtes 2, 4 (dus som $S(7) = 6$). En het $3x + 49$-probleem zou precies 3 cykels hebben, met lengtes 2, 4, 38 (en som $S(49) = 44$).

Voor kleine waarden van k zijn de sommen $S(M_k)$ en $S(M_k^2)$ van de cykellengtes te vinden in de tabel op de volgende pagina. (Deze is berekend onder de aanname dat in elke cykel een getal ≤ 500000 voorkomt).

k	M_k	$S(M_k)$	$S(M_k^2)$	$S(M_k^2) - S(M_k)$
1	1	2	2	0
2	3	2	2	0
3	7	6	44	38
4	15	69	93	34
5	31	25	380	355
6	63	6	44	38
7	127	76	1174	1098
8	255	207	1047	840
9	511	318	17597	17279

Tabel 1

Evidentie voor het MC-225 vermoeden

De volgende lemma's en een verwachting geven aan, waarom we denken dat het verschil $S(M_k^2) - S(M_k)$ minimaal is voor $k = 4$.

Lemma 2. *De cykels voor het $3x + 3^t$-probleem komen overeen met die voor het $3x + 1$-probleem.*

Voor het bewijs merken we op, dat uit een rij voor het $3x + 1$-probleem na vermenigvuldigen met 3^t een rij voor het $3x + 3^t$-probleem ontstaat. En omgekeerd zijn de termen in een rij voor het $3x + 3^t$-probleem op den duur deelbaar door 3^t; na deling ontstaat dan een rij voor het $3x + 1$-probleem.

Lemma 3. *Met $n(q)$ geven we het aantal cykels voor het $3x + q$-probleem aan.*
Als $p_i > 3$ een priemdeler van q is, dan geldt $n(q) \geq 1 + \sum_i [n(p_i) - 1]$.

Bewijs. Een niet-triviale cykel voor het $3x + p_i$-probleem levert door vermenigvuldigen met q/p_i er een voor het $3x + q$-probleem. Met de triviale cykel $(q, 2q)$ erbij volgt het lemma. □

Numerieke aanwijzingen leiden tot de verwachting, dat als q uitsluitend kleine priemfactoren heeft, dan is $n(q)$ ongeveer gelijk aan $1 + \sum_i [n(p_i) - 1]$.

Lemma 4. *(a) De enige oplossingen van $M_k = 3^m$ zijn $k = 1, m = 0$ en $k = 2, m = 1$.*
(b) De enige oplossing van $M_k = 5 \cdot 3^m$ is $k = 4, m = 1$.

Bewijs. (a) Dit is een resultaat van Hebraeus, alias Levi ben Gerson of Gersonides (1288–1344); zie ook de inauguratie van H.W. Lenstra jr. in het maart 2001 nummer van dit tijdschrift. Merk overigens op (vergelijk het bewijs van lemma 1), dat het bestaan van nog een oplossing ook het bestaan van nog een cykel (met een rij oneven gevolgd door een rij even getallen) voor het $3x + 1$-probleem zou impliceren.
(b) Dit is een resultaat van Størmer (1897).

Beschouw het verschil $S(M_k^2) - S(M_k)$ als functie van $k > 2$. Met p_i geven we priemfactoren van M_k aan. Dan is $S(M_k^2) - S(M_k) = [S(M_k^2) - \sum_i S(p_i)] - [S(M_k) - \sum_i S(p_i)]$. Goede kandidaten M_k voor een klein verschil $S(M_k^2) - S(M_k)$ zijn, met behulp van lemma 3, de M_k van de vorm $3^m \cdot 5$. Volgens lemma 4 is M_4 de enige van deze soort. Zo komen we tot het vermoeden, dat $S(M_k^2) - S(M_k) \geq S(M_4^2) - S(M_4)$. De gegeven tabel ondersteunt deze ongelijkheid. □

Veel generalisaties van het $3x + 1$-probleem hebben niet-triviale cykels. Het $3x + 1$-probleem heeft zulke cykels niet en lijkt daarom uniek. De onderliggende theorie laat zien dat het $3x + 1$ een grensgeval is, waarbij de 'ruimte' voor niet triviale cykels zo klein is geworden, dat zij niet voor blijken te komen.

Referenties

1 Baker, A., Linear forms in logarithms of algebraic numbers IV, *Mathematica* 15, 1968, p. 204–216.

2 Crandall, R.E., On the $3x + 1$ problem, *Mathematics of Computation*, Volume 32, 1978, p. 1281–1292.

3 Dickson, L.E., History of the Theory of Numbers, Vol. II, p. 731, Carnegie Institute, Washington, *Chelsea* 1992, New York.

4 Ellison, W.J., On a theorem of S. Sivasankaranarayana Pillai, Sem. Th. Nombr 1970–1971, Exp. No.12, *Lab.Theorie Nombres*, CNRS, Talence, 1971.

5 Guy, R.K., Unsolved Problems in Number Theory, Volume 1, 2th edition, *Springer publishers*, 1994, p. 215–218.

6 Hardy, G.H., Wright E M, An introduction to the theory of numbers, *Clarendon press*, 1975, p. 129–151.

7 Lagarias, J.C., The $3x + 1$ problem and its generalizations, *American Mathematical Monthly* 92, 1985, p. 3–23.

8 Lagarias, J.C., The set of rational cycles for the $3x + 1$ problem, *Acta Arithmetica*, 1990, p. 33–53.

9 Laurent, M., Mignotte M, Nesterenko Y, Formes linéaires en deux logarithmes et déterminants d'interpolation, *Journal of Number Theory* 55, 1995, p. 285–321.

10 Matthews, K.R., The generalized $3x + 1$ mapping, www.numbertheory.org/pdfs/survey.pdf

11 Über Hasses veralgemeinerung des Syracus-Algorithmus (Kakutanis Problem), *Acta Arithmetica* 34, 1978, p. 219–226.

12 Roosendaal, E., On the $3x + 1$ problem, http://personal.computrain.nl/eric/wondrous/index.html

13 Simons, J.L., On the non-existence of 2-cycles for the $3x + 1$ problem, 2003, preprint

14 Simons, J.L., Weger, B.M.M. de, Theoretical and computational bounds for m-cycles of the $3n + 1$ problem, 2003, see www.win.tue.nl/~bdeweger

15 Steiner, R.P., A theorem on the Syracuse problem, *Proceedings of the 7th Manitoba Conference on Numerical Mathematics and Computation*, 1977, p. 553–559

16 Størmer, Carl, Quelques théorèmes sur l'équation de Pell $x^2 - Dy^2 = \pm 1$ et leurs applications, *Skrifter Videnskabs-Selskabet I Mat. Naturv. Kl.* (Christiania), 1897, no. 2 (p. 48)

17 Stroeker, R.J., Tijdeman, R., "Diophantine Equations", p. 321–369 in: H.W. Lenstra Jr., R. Tijdeman (eds.), "Computational Methods in Number Theory", Part II, MC Tract 155, Mathematisch Centrum Amsterdam, 1982

18 Weger, B.M.M. de, Algorithms for diophantine equations, CWI tract 65, *Centre for Mathematics and Computer Science*, 1990, p. 104.

19 Wirsching, G.J., The Dynamical System Generated by the $3n + 1$ Function, Lecture Notes in Mathematics 1681, *Springer publishers*, 1998, p. 23.