# Gevaarlijke helpers?

**F. van der Blij.**

*Summary*

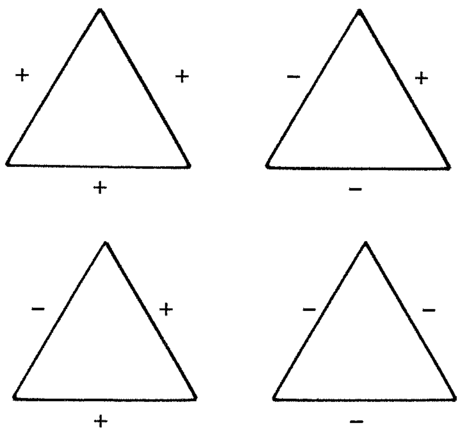
*Mathematicians sometimes have the habit to wander from a real problem proposed to them in the context of (social) science to mathematically nice looking theories, which, however cannot, or not as nicely, be applied to the proposed problem. Graph theory is an example. In spite of nice and not so nice ways to apply graph theory in the social sciences, the present author starts with a problem of card shuffling and deals with graphical illustrations of sequences* $x_{n+1} \equiv f(x_n)$ *mod N. As simple a case as* $f(x) = ax$ *leads to interesting number theoretical discussions.*

U kent wel de helpers van de wal in de sloot. Sommige wiskundigen zijn op een wat andere manier gevaarlijke helpers. Speciaal zuivere wiskundigen kunnen soms een afwijking vertonen, die hen als helpers (als onderhorigen van de dienstmaagd van alle wetenschappen) ongeschikt maakt. Op de vraag: "Kun je me helpen dit probleem op te lossen" is hun antwoord: "Nee, maar ik kan wel een ander en heus erg leuk probleem oplossen."
Toepassingen, beter gezegd het toepassen, van wiskunde in bijvoorbeeld de sociale wetenschappen laat zo iets zien. Er wordt begonnen met een wiskundig model, daarin komt een functie, een matrix of een graaf voor. En de sluizen van de theorie over functies, matrices of grafen worden wijd open gezet. Het probleem dreigt vergeten te worden, welk stukje theorie zou nodig zijn? Theorie is nooit weg. "Iedere natuurkundige kan precies alle wiskunde gebruiken die hij kent" zegt een bon mot en dat zal ook wel voor andersdenkenden gelden. Maar toch blijkt soms na alle theorie dat het ene gestelde probleem er eigenlijk niet behoorlijk mee te behandelen is. Omdat het zonde lijkt van de theorie doet men dan het model maar geweld aan om toch iets van het gestelde probleem aan de orde te stellen. Of men verdringt (Freudiaans) het probleem maar. Verzamelingenleer, echt een goed stuk wiskunde, laat duidelijk de moeilijkheden van toepassingen zien. Verzamelingen, getallen, functies, driehoeken enz. zijn duidelijk, je kunt er goed mee werken. Verzamelingen postzegels zijn al veel moeilijker. Wat te zeggen over dubbele, over gestempelde en ongestempelde exemplaren, over een postfris en wat smoezelig exemplaar? De ene postzegel is toch nooit de ander! De verzameling letters in het woord "Amsterdam" geeft ook al zoveel problemen. De hoofdletter A is iets anders dan de kleine letter a. En wordt de tweede letter m niet anders uitgesproken dan de laatste? Maar het lemma van Zorn is goed te formuleren!

## Grafen

We willen niet over verzamelingen praten, maar als onderwerp eens de graaf nemen. Wiskundig een heel helder gedefinieerd begrip, al zijn er nog al wat bijvoeglijke naamwoorden voor te zetten, zoals gerichte, reguliere, complete, pseudo, di-, bi-; enzovoorts. De grafen lijken bruikbaar in een vak als aardrijkskunde, de punten zijn steden, de verbindingsstreepjes spoorlijnen, de kaartjes in het spoorboekje zijn grafen. We zien er cycles (rondreizen) in, eindpunten (als Den Helder en Rodeschool), valentie (het aantal richtingen waarin je kunt vertrekken of aankomen). Een stadsplattegrond met autowegen en verkeerspleinen geeft een variant door het voorkomen van straten voor éénrichting verkeer. Ook in de scheikunde is er veel met grafen te doen, de atomen zijn punten, de chemische bindingen geven we aan door verbindingsstreepjes. Zowel koolstofcycles als lange bomen zijn mooie voorbeelden.
Moeilijker wordt het als we in de sociale wetenschappen grafen gaan toepassen. De personen worden punten, verbindingsstreepjes communicatielijnen. Of nog moeilijker machtsrelaties (is dat éénrichting verkeer?). En wat als de punten b.v. landen zijn en de verbindingsstreepjes politieke coalities? Moeten de streepjes een richting of misschien een zeker gewicht hebben? Kun je grafen gebruiken voor beschrijvingen of nog sterker, voor voorspellingen van ontwikkelingen binnen een sociaal of politiek systeem? Kunnen de streepjes emotionele relaties voorstellen en kun je met grafen vooraf of achteraf schema's maken voor het plot van een romancyclus? Als je in de politiek werkt met coalities en de tijd niet wilt uitschakelen, moet je omdat er òf een verdrag òf geen verdrag is, discontinu grafen van de ene vorm in de andere laten overgaan. Maar ja er is zo'n mooie theorie, wiskundig gezien over Hamilton grafen, over gewortelde bomen, en zoveel meer. Dikke boeken over grafentheorie (en

natuurlijk een eigen wetenschappelijk tijdschrift) geven een mooi stuk wiskunde, dat in het bijzonder in de wiskunde goed toepasbaar is. Voordat we ons in de Nieuwe Wiskrant gaan bezighouden, en dat zal heus gaan gebeuren, met toepassingen van grafen in de sociale wetenschappen, vandaag nog iets makkelijks, toepassen in de wiskunde. Inspiratie voor dit verhaal kwam uit een telefoontje van een geestdriftig amateur en scriptiewerk van twee studenten (1). En daarbij een persoonlijk plezier in elementaire, niet geheel triviale problemen. Ik vertel het niet alleen als afschrikkend voorbeeld van "gevaarlijk helpen", mijn grafentheorie helpt niet bij de toepassingen in de sociale wetenschappen, maar toch ook omdat in wiskundige vraagstellingen een directe prikkel ligt om zelf verder te gaan spelen en er vertrouwd mee te raken. En daarna kunt u wellicht gaan denken over "uitgebalanceerde grafen". O ja, u wilt misschien weten wat dat zijn, uitgebalanceerde grafen? De punten zijn mensen, tussen de mensen kan òf geen, òf een positieve (+), òf een negatieve (–) relatie bestaan. Hebben we drie mensen dan zijn er vele plaatjes mogelijk, onder andere:




Een hypothese zegt nu dat een driehoeksverhouding in balans is als het "produkt" van de tekens een + is. Dus in de twee voorbeelden links, en uit balans als het produkt een – is, de twee voorbeelden rechts. Iedereen ruzie met iedereen is uit balans, met z'n tweeën een gemeenschappelijke vijand is in balans. Wanneer de vriend, van mijn vriend niet mijn vriend is (+, +, –) is de situatie uit balans. Natuurlijk is er een generalisatie naar vier of meer personen ontwikkeld. Maar zowel generalisatie als kritiek laat ik aan de lezer over (2).

## Kaarten schudden

Wij gaan nu verder met meer wiskundige kanten. O ja, een instap. Ik heb 52 kaarten op volgorde 1, 2, 3, 4, ...., 52 gelegd en wil deze schudden. Ik doe het zo', dat ik twee stapels maak, om de beurt een kaart op iedere stapel. De ene stapel wordt 1, 3, 5, 7, ..., 51; de andere 2, 4, 6, 8, ..., 52. Nu leg ik ze weer op elkaar zodat er 2, 4, 6, ..., 52, 1, 3, ..., 51 komt. Alles is van zijn plaats geraakt. Op de nieuwe stapel pas ik hetzelfde procédé nog eens toe, enzovoorts. Na een aantal keren schudden, zal alles lekker in de war liggen. Als proef, om niet te veel te schrijven moeten we het eerst doen met een kleiner aantal b.v. 6 kaarten.

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 4 | 6 | 1 | 3 | 5 |
| 4 | 1 | 5 | 2 | 6 | 3 |
| 1 | 2 | 3 | 4 | 5 | 6 |

Na drie keer is het oude rijtje in de nette volgorde weer terug. Gaat dat bij 52 ook zo, en zo ja, na hoeveel keer? We gaan nu gewoon rekenen.
We beginnen met een even aantal kaarten, 2n. Voor de eerste n is het eenvoudig; k wordt 2k. Voor de volgende gaat het zo dat waar n + k stond nu 2k – 1 staat (voor k = 1, 2, 3, ..., n). We kunnen dit beschrijven: waar x stond staat nu f (x) met

$$f(x) = \begin{cases} 2x & ; \quad 1 \leq x \leq n. \\ 2x - 2n - 1; & n + 1 \leq x \leq 2n. \end{cases}$$

Schrijven we 2n + 1 = N en gaan we modulo N rekenen, dan zien we $f(x) \equiv 2x \pmod N$.
Met deze formule kunnen we de loopbaan van x beschrijven, x wordt f (x), daarna f(f(x)), daarna f(f(f(x))). Als er een k is zodat

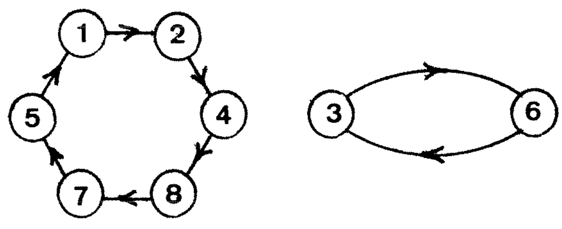
$$\underbrace{f(f(\ldots\ldots f}_{k \text{ keer}}(x)) \equiv x \pmod N\ ,$$

dan zal na k keer schudden alles weer op zijn plaats zijn.
Nu wat theorie. We beginnen met 6 kaarten, N = 7. Verdubbelen geeft de levensloop; (we rekenen dus modulo 7).

1 → 2 → 4 → 1 → enzovoorts
2 → 4 → 1 → 2 → „
3 → 6 → 5 → 3 → „
4 → 1 → 2 → 4 → „
5 → 3 → 6 → 5 → „
6 → 5 → 3 → 6 → „

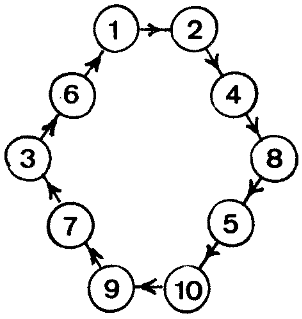
Maar dit is veel eenvoudiger en mooier in een graaf te demonstreren:


Zelfwerkzaamheid geeft voor n = 4, N = 9 de graaf




Drie en zes spelen stuivertje wisselen, maar na zes keer schudden is alles weer op zijn oude plaats.

Nog een voorbeeld n = 5, N = 11 geeft



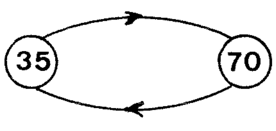

Nu ben je na 10 keer schudden terug. Hoe gaat het verder?

Mensen met liefde voor getaltheorie kunnen aan het werk.

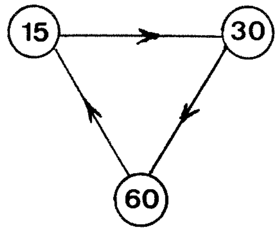
We willen dat $2^k x \equiv x \pmod{N}$. Dus

$$(2^k-1)x \equiv 0 \pmod{N}.$$
$$\text{Dus } (2^k-1) \equiv 0 \bmod \frac{N}{(N,x)},$$

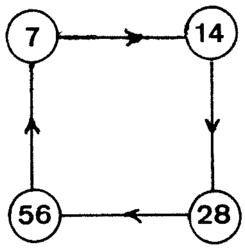
waarin (N,x) de g.g.d. van N en x is. De getaltheorie leert dat voor $k = \Phi\left(\frac{N}{(N,x)}\right)$, waarin $\Phi$ de Euler indicatrix (3) is de congruentie in ieder geval geldt en dat de kleinste k ($\geq 1$) waarvoor de congruentie geldt een deler van deze Eulerfunctie is. Nu is er altijd een x met $(N,x) = 1$. De kleinste k ($\geq 1$) waarvoor $2^k \equiv 1 \bmod \left(\frac{N}{(N,x)}\right)$ zal dus de periode geven; het minimum aantal keren schudden om alles weer op de oude plaats te krijgen.
We controleren onze getalvoorbeelden. Als n = 3, N = 7 geldt $\Phi(N) = 6$. En inderdaad $2^6 \equiv 1 \pmod{7}$. Maar ook $2^3 \equiv 1 \pmod{7}$. En 3 is de kleinste exponent bij 2; zodat de macht een 7-voud plus 1 is. Als n = 4, N = 9 geldt $\Phi(N) = 6$. En nu is de periode precies 6. Voor n = 5, N = 11 geldt $\Phi(N) = 10$ en periode 10. Voor 2n = 52, N = 53 geldt $\Phi(N) = 52$. En uit het feit dat $2^{26} \equiv -1 \pmod{53}$ kunnen we (u ook?) afleiden dat de periode 52 moet zijn.
Twee spel kaarten 2n = 104, N = 105 is veel en veel mooier. Immers $105 = 3 \cdot 5 \cdot 7$. Dus $\Phi(105) = 105 \cdot (1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7}) = 48$. De periode zal een deler van 48 zijn. Kiezen we x zodat $(x, 105) = 1$, dan moet $2^k \equiv 1 \pmod{105}$ gelden. De kleinste k ($\geq 1$) die voldoet is 12, want $2^{12} = 4096 \equiv 1 \pmod{105}$ en voor kleinere k geldt $2^k \not\equiv 1 \pmod{105}$. Dus na 12 keer schudden ligt alles al weer in de oude volgorde. Maar hebben getallen x met $(x, 105) > 1$ een kortere levensloop? En hoe ziet de hele graaf er uit? Duidelijk is



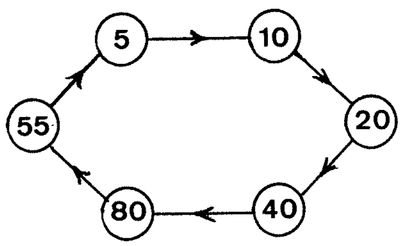

en




en

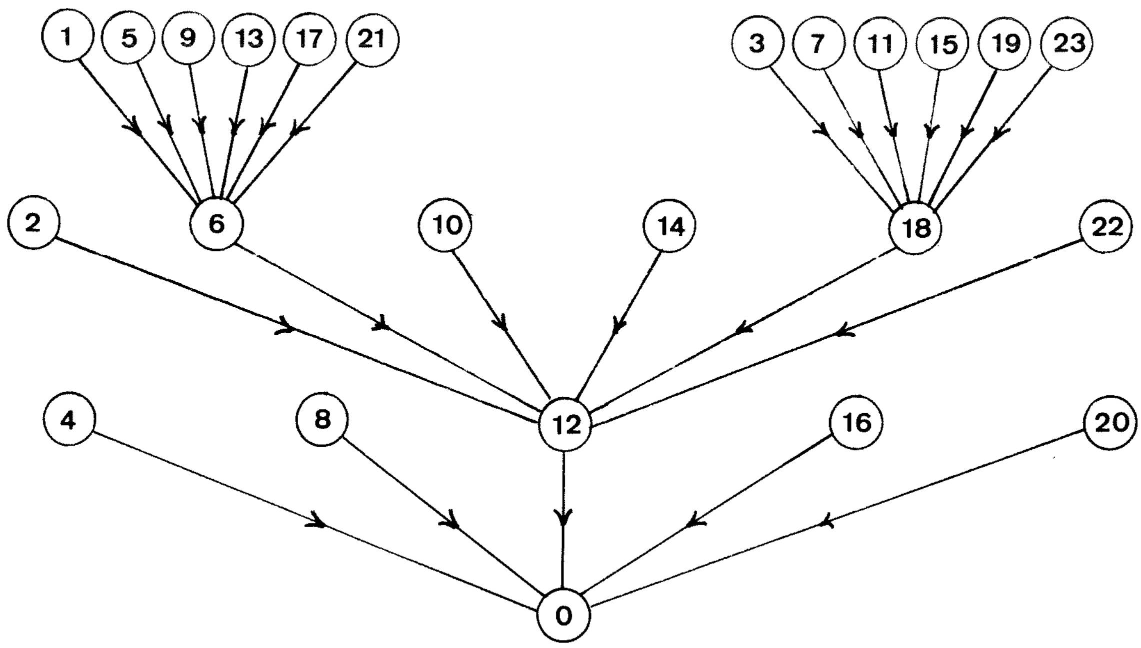



en




terwijl b.v. 1 in een twaalfhoek terechtkomt. Hoeveel kringen van 2, 3, 4, 6 en 12 punten vormen het hele patroon van de getallen 1 tot en met 104? De gevaarlijke helper is tot een gevaarlijke maniak geworden. Het kaartschudden lijkt opgelost, maar zijn er niet voor allerlei f's zulke grafen te maken?
Voor de hand ligt nu te beginnen met $f(x) = ax$ en dan weer modulo N te werken. Het kan er heel anders uit gaan zien. Als voorbeeld kiezen we a = 6 en N = 24.
Een beetje proberen geeft:
$1 \to 6 \to 12 \to 0 \to$
$2 \to 12 \to 0 \to$

Hoe ziet de graaf er uit?




Voor maniakken nog even $f(x) = x^2$. Als u modulo een priemgetal p werkt, dat u zo kiest dat een regelmatige p-hoek met passer en liniaal te construeren is, dus b.v. p = 3, 5, 17, 257 (enzovoorts?) dan krijgt u een bijzonder mooie graaf!
Wilt u een mooie graaf, die in de tijd verandert? We nemen gewoon voor f(x,t) een functie die voor gehele x en alle t een gehele waarde oplevert en kunnen b.v. weer modulo N gaan werken. Met de entier functie [ ], "het grootste gehele getal kleiner dan", gaat het best. Bijvoorbeeld $f(x) = [tx]$ en dan weer mod N gaan rekenen. Erg boeiend is $f(x) = [\,tx\,(1 - \frac{x}{N})]$, voor t niet te groot b.v. $t \in [0,4]$ worden de getallen zelf al periodiek of komen terecht in cycles. De grafen variëren als functie van t, natuurlijk discontinu.

## Gevaarlijke helpers

Ergens in een hoekje staat de arme welzijnswerker, die ons vroeg of we met uitgebalanceerde grafen konden toelichten waarom die plotselinge ruzie tussen twee tot nu toe bevriende achterneven in de familie zo'n veel stabielere toestand had geschapen. (Door één teken van + naar – te veranderen was er iets gebeurd met de "uitgebalanceerdheidscoëfficiënt"). Wij waren hem door onze Eulerfunctie helemaal vergeten. Wiskundigen zijn gevaarlijke helpers, gevaarlijke maniakken. Van wie zegt de legende ook weer: verstoor mijn cirkels niet? Maar ach, stak hij door geometrische optica weer niet de zeilen in brand?
Voor de wiskundedocent die in het V.W.O. (Hewet A-programma) grafen gaat behandelen, dreigt het gevaar van uitglijden naar zulke leuke wiskundige figuurtjes om maar te ontsnappen aan moeilijke discussies over de geldigheid van mathematische modellen en om maar niet steeds te behoeven waarschuwen dat de werkelijkheid, speciaal in vakken als die van de sociale wetenschappen, zo gecompliceerd is dat onze modellen daar nog niet zo adequaat zijn als de wetten van Kepler voor de voorspelling van de planetenbeweging.
Grafentheorie als mogelijk mathematisch model in relaties tussen mensen of groepen van mensen. Er moet nog veel gedacht worden over het evenwicht tussen wat boeiend is voor de wiskundige maniak en nuttig voor de gebruiker, onze onderwijscliënt.
Het hewetwerk dat in nauwe samenwerking met de vakgroep "OW & OC" van de utrechtse subfaculteit wiskunde op gang gaat komen zal ook moeten gaan over grafen en hun toepassingen. In tegenstelling met dit verhaal, met nadruk op de toepassingen!

(1) Met dank aan Marijke Butselaar en Jeroen Weesie.

(2) Walther G., 1976 *Balancierte Graphen – ein Thema für didaktische Diskussion zum Geometrieunterricht,* Educational Studies in Math 7, 465 – 495 en de daar geciteerde literatuur.

(3) De Eulerfunctie is te berekenen uit:

$$\Phi\,(T) = T \cdot \prod_{p/T} (1 - \tfrac{1}{p})$$

(het produkt over alle priemdelers van T). Is T een priemgetal dan $\Phi\,(T) = T - 1$.
In ieder inleidend boek over getaltheorie zijn de bewijzen te vinden.