Voorwoord

Getaltheorie voor beginners is een boek waarin ik mij richt tot een ieder die geen of weinig kennis van de getaltheorie heeft, maar er wel graag kennis mee wil maken. Als ingangsvivte heb ik getracht mij te richten tot een denkbeeldig publiek van eerstejaars studenten, leraren VWO en misschien zelfs een gemotiveerde VWO-leerling.

Getaltheorie gaat, zoals de benaming reeds zegt, over getallen en wel de gehele getallen. Hieronder verstaan we de natuurlijke getallen 1, 2, 3, 4, ..., samen met het getal 0 en de negatieve gehele getallen $-1, -2, -3, ...$ Natuurlijk spelen gehele getallen een belangrijke rol in ons dagelijks leven. We staan er mee op, tijden op de wekker worden immers met getallen aangegeven, en we gaan ermee naar bed. Transacties in een winkel, opbellen van een vriend, de AEX-index, de postcode-loterij, overal zien we gehele getallen om ons heen. Hiermee hebben we echter nog geen getaltheorie.


Maar ook met getallensymboliek hebben we nog geen getaltheorie. Het is echter wel het begin. Mensen kunnen door getallen gebiologeerd raken. Door de eeuwen heen is er altijd een kleine groep mensen geweest die zag dat getallen aan bepaalde wetten voldoen die het opmerken waard zijn. Op deze wijze is langzaam de getaltheorie ontstaan. En ze wordt nog steeds beoefend door mensen die gefascineerd kunnen raken door getallen en hun opmerkelijke eigenschappen. Ik denk dat kinderen deze attractie al voelen. Een prachtig voorbeeld is het boek van H.J. Enzensberger, de *Telduivel* (Bezige Bij Uitgaven), dat gaat over een driftig mannetje dat veel van getallen weet en gedurende twaalf nachten in de droom van een klein jongetje verschijnt. De spelletjes die ze daarin met getallen spelen brengen de hoofdpersoon, en ook de lezers, in de ban van de getallen. Mijn dochter van negen heeft het in korte tijd uitgelezen en ik denk dat talloze andere kinderen hetzelfde gedaan hebben. Op mijn vraag of ze nu alles begrepen had
antwoordde ze dat ze het een leuk boek vond, maar lang niet alles had begrepen. Desondanks had het spel met de getallen een onmiskenbare aantrekking op haar en ik denk, op vele andere kinderen. Mijn dochter en ik hebben in ieder geval nog ‘prima’ getallen gezeeft en het aantal lijnen, punten en vlakken in allerlei patronen geteld.

Als eenvoudig voorbeeld van de elegantie die van getallen uitgaat wil ik de opmerkelijke gelijkheid

\[(1 + 2 + 3 + \cdots + 100)^2 = 1^3 + 2^3 + 3^3 + \cdots + 100^3\]

noemen. Het geldt zelfs algemener. Voor elke keuze van \(n\) geldt namelijk de gelijkheid

\[(1 + 2 + 3 + \cdots + n)^2 = 1^3 + 2^3 + 3^3 + \cdots + n^3\]

Zelf ben ik al jaren op de hoogte van dit makkelijk te bewijzen feit, maar toch vind ik het nog steeds een verrassing dat zo iets waar kan zijn. Het is met deze instelling, de verwondering en het plezier met getallen, dat ik dit boek geschreven heb. Mijn stille hoop is dat dit boek ook anderen met een zelfde belangstelling op weg zal helpen in de wereld van de getaltheorie.

Hoewel dit boek in eerste instantie gericht is aan beginners en liefhebbers, is het toch een echt wiskundebloek. Dat betekent bijvoorbeeld dat we de beweringen die we doen ook zo veel mogelijk met argumenten zullen ondersteunen, ofwel bewijzen. Het volgen van bewijzen zal zeker voor de prille beginners niet altijd even eenvoudig zijn. Het vereist enige vertrouwdheid met het opzetten van een wiskundig logische redenatie. Ik heb zeker in het begin van het boek getracht bewijzen tot op kleine details uit te werken. In latere hoofdstukken zal op sommige punten de moeilijkheidsgraad enigszins steil oplopen. Voor diegenen voor wie dat te steil is, zullen hopelijk de resultaten nog aansprekend zijn.

Bij de keuze van onderwerpen heb ik er in de eerste plaats naar gestreefd de minimale basis van een elementaire getaltheoriecursus te behandelen, zoals die ook in talloze andere boeken behandeld wordt. Deze bestaat grofweg uit de Hoofdstukken 3, 4, 5, 6, 7. De leidraad hierin heb ik getracht te motiveren door uit te gaan van het probleem van de perfecte getallen en hun eigenschappen. Vandaar is het een kleine stap naar de Mersenne-getallen. Deze getallen bevatten op hun beurt weer voldoende motivatie voor het begrip multiplicatieve orde in de congruentierekening. De overige hoofdstukken kunnen in vrij willekeurige volgorde gelezen worden, er bestaat geen grote onderlinge afhankelijkheid. Deze hoofdstukken bevatten een selectie van zaken die een elementaire behandeling toelaten. De onderwerpen zijn deels klassiek, zoals de kettingbreuken, vergelijking van Pell, en deels het gevolg van ontwikkelingen van de laatste twintig jaar, zoals het abc-vermoe- den, ontbinding in priemfactoren en cryptografie. Er zijn ook onderwerpen waarvan ik helaas niet ben toegekomen. De voornaamste slachtoffers zijn een hoofdstuk over \(\pi\) en een hoofdstuk over recurrente rijen (bijv.}
VOORWOORD

Fibonacci-getallen). Ook ontbreken in dit boek oefeningen en opgaven. Hopelijk blijft er nog genoeg interessants over.

Dan nog een woord over computers. Zeker in de getaltheorie is de computer een grote rol gaan spelen. Voor experimenten met getallen is de computer een prachtig instrument waar al veel waardevols uit is gekomen. Zonder daarbij overigens de rol van de wiskundige over te nemen. De wiskundige beslist uiteindelijk wat er berekend gaat worden en zorgt ook voor de interpretaties en verklaringen van dingen die gevonden worden.


Tenslotte, er zijn talloze boeken op het gebied van de elementaire getaltheorie verschenen. In de referenties aan het eind van dit boek staan een paar titels, waarvan het ingangs niveau vergelijkbaar of iets hoger is met dat van dit boek, apart aangegeven. Het merendeel van de boeken is echter in het Engels. Door dit boek in het Nederlands te schrijven hoop ik te bereiken dat dit werk voor een breed Nederlands publiek een goed bereikbare toegang geeft tot de wonderlijke wereld van de getaltheorie.

Utrecht, 20 november 1998

In deze tweede druk zijn een groot aantal kleinere en grotere fouten gecorrigeerd. Met veel dank aan Peter van Dulst voor de assistentie hierbij.

Utrecht, 10 december 1999
# Inhoudsopgave

1 De pioniers 5
   1.1 Wiskunde is mensenwerk 5

2 De regels van het spel 11
   2.1 De gehele getallen 11
   2.2 Deelbaarheid 13
   2.3 Volledige inductie 15

3 Priemontbinding en ggd’s 18
   3.1 Priemgetallen 18
   3.2 Priemontbinding 20
   3.3 GGD’s en KGV’s 23
   3.4 Het Euclidisch algoritme 25

4 Delers 29
   4.1 Delers (op)tellen 29
   4.2 Multiperfecte getallen 32
   4.3 Het gemiddelde van $\sigma(n)/n$ 33
   4.4 Aliquote rijen 35

5 Mersenne- en Fermatgetallen 37
   5.1 Mersennegetallen 37
   5.2 Mersenne priemgetallen 41
   5.3 Fermatgetallen 43

6 Congruentierekening 46
   6.1 Congruenties 46
   6.2 Toepassingen 48
   6.3 Inverse restklassen 50
   6.4 Lineaire congruentievergelijkingen 51
   6.5 Chinese reststelling 52
7 Congruenties in actie 56
   7.1 Het aantal inverteerbare restklassen .......................... 56
   7.2 De stelling van Euler ........................................... 58
   7.3 Ordes ............................................................. 59
   7.4 Primitieve wortels ............................................. 61

8 Priemtesten en priemontbinding 65
   8.1 Complexiteit ....................................................... 65
   8.2 Pseudo-priemgetallen ......................................... 67
   8.3 Priemtesten ....................................................... 70
   8.4 De rho-methode van Pollard .................................. 72
   8.5 De kwadratische zee ............................................ 74

9 Cryptografie 79
   9.1 Geheimtaal ....................................................... 79
   9.2 Publieke sleutels ............................................... 81
   9.3 Zero-knowledge proofs ....................................... 84

10 Decimale ontwikkeling 87
    10.1 Inleiding ....................................................... 87
    10.2 Periodieke breuken .......................................... 88
    10.3 Normale getallen ............................................ 91
    10.4 Kunstjes met decimaal ....................................... 92
    10.5 De wet van Benford ......................................... 95

11 Kwadraatresten 99
    11.1 Inleiding ....................................................... 99
    11.2 Toepassingen van kwadratische wederkerigheid ............. 102
    11.3 Bewijs van de kwadratische wederkerigheid ............... 105
    11.4 Het Jacobi-symbool ......................................... 108
    11.5 Oplossen van kwadratische congruenties .................. 111

12 Sommen van kwadraten 115
    12.1 Sommen van twee kwadraten .................................. 115
    12.2 Sommen van vier kwadraten .................................. 118
    12.3 Variaties op sommen van kwadraten ......................... 121
    12.4 Het probleem van Waring ................................... 124

13 De laatste stelling van Fermat 126
    13.1 Pythagoreïsche drietallen .................................. 126
    13.2 Oude geschiedenis .......................................... 128
    13.3 Recent geschiedenis ........................................ 130
    13.4 Euler’s generalisatie ....................................... 133
    13.5 De super Fermat vergelijking ............................... 134
14 Kettingbreuken \hspace{1cm} 138
\hspace{0.5cm} 14.1 Eindige kettingbreuken \hspace{0.5cm} 138
\hspace{0.5cm} 14.2 Oneindige kettingbreuken \hspace{0.5cm} 139
\hspace{0.5cm} 14.3 Benaderingseigenschappen \hspace{0.5cm} 142
\hspace{0.5cm} 14.4 Kwadratische getallen \hspace{0.5cm} 146
\hspace{0.5cm} 14.5 Symmetrieën \hspace{0.5cm} 151

15 De vergelijking van Pell \hspace{1cm} 157
\hspace{0.5cm} 15.1 De oplossing \hspace{0.5cm} 157
\hspace{0.5cm} 15.2 Enkele toepassingen \hspace{0.5cm} 160
\hspace{0.5cm} 15.3 Een miraculeuze formule \hspace{0.5cm} 164

16 Diophantische vergelijkingen \hspace{1cm} 166
\hspace{0.5cm} 16.1 Inleiding \hspace{0.5cm} 166
\hspace{0.5cm} 16.2 Twee variabelen, graad 1 \hspace{0.5cm} 167
\hspace{0.5cm} 16.3 Twee variabelen, graad 2 \hspace{0.5cm} 168
\hspace{0.5cm} 16.4 Twee variabelen, graad 3 \hspace{0.5cm} 170
\hspace{0.5cm} 16.5 De vergelijking $y^2 = x^4 + A$ \hspace{0.5cm} 174
\hspace{0.5cm} 16.6 Twee variabelen, graad $> 3$ \hspace{0.5cm} 175
\hspace{0.5cm} 16.7 Willekeurige diophantische vergelijkingen \hspace{0.5cm} 177

17 Het abc-vermoeden \hspace{1cm} 179
\hspace{0.5cm} 17.1 Introductie \hspace{0.5cm} 179
\hspace{0.5cm} 17.2 Gevolgen van het abc-vermoeden \hspace{0.5cm} 183
\hspace{0.5cm} 17.3 Waarom geloven we in het abc-vermoeden? \hspace{0.5cm} 186

18 Irrationaliteit en transcendentie \hspace{1cm} 188
\hspace{0.5cm} 18.1 Irrationele getallen \hspace{0.5cm} 188
\hspace{0.5cm} 18.2 Irrationaliteit van $e^a$ en $\pi$ \hspace{0.5cm} 190
\hspace{0.5cm} 18.3 Transcendentie \hspace{0.5cm} 194
\hspace{0.5cm} 18.4 Aftelbaarheid \hspace{0.5cm} 196

19 Priemgetallen \hspace{1cm} 199
\hspace{0.5cm} 19.1 Het aantal priemgetallen < $X$ \hspace{0.5cm} 199
\hspace{0.5cm} 19.2 De Riemann zeta-functie \hspace{0.5cm} 202
\hspace{0.5cm} 19.3 Lokale verdeling \hspace{0.5cm} 206
\hspace{0.5cm} 19.4 Elementaire beschouwingen \hspace{0.5cm} 207

20 Het $3n + 1$ probleem \hspace{1cm} 211
\hspace{0.5cm} 20.1 Stopgetallen \hspace{0.5cm} 212
21 Appendix

21.1 Binomiaalcoëfficienten ................................................... 216
21.2 De harmonische reeks ...................................................... 221
21.3 Polynomen ................................................................. 224