UNIVERSITEIT GENT

FACULTEIT INGENIEURSWETENSCHAPPEN EN ARCHITECTUUR

Universiteit Gent

Faculteit Ingenieurswetenschappen en Architectuur

Bachelor in de industriële wetenschappen: informatica
Bachelor in de industriële wetenschappen: elektronica–ICT
Schakelprogramma tot Master in de industriële wetenschappen: informatica
Voorbereidingsprogramma tot Master in de industriële wetenschappen: informatica

Discrete wiskunde

Syllabus

Verantwoordelijke lesgever
Cedric De Boom

Verantwoordelijke oefeningen
Marleen Denert

Academiejaar 2020–2021

Inleiding

God schiep de natuurlijke getallen, de rest is het werk van de mens — Kronecker

Wat is discrete wiskunde?

De *natuurlijke getallen* hebben hun naam niet gestolen. Ze staan voor het meest (be)grijpbare begrip uit de getallenwereld — menig kleuterversje parafraseert dan ook het rijtje dat steevast begint met "1 2 3 ...". Pas in een later stadium komen de begrippen nul, negatieve getallen, breuken, niet-rationale getallen aan bod. Totdat op het einde van de middelbare school de natuurlijke getallen helemaal op de achtergrond verdwenen zijn. Ten voordele van de analyse van continue krommen met domein en beeld in $\mathbb{R}$, de analytische meetkunde met oneindig veel punten op een rechte (die dan 'oneindig dicht' bij elkaar liggen) enzovoort. De ideale wiskundige achtergrond om Newtoniaanse fysica mee te bedrijven.

Aan het begin van je hogere studies blijkt dan dat er toch wat problemen opduiken bij de wiskunde die gebruik maakt van reële getallen. Of niet zozeer met de wiskunde zelf, dan wel met de wijze waarop we exacte resultaten uit de theorie willen halen. Willen we berekeningen zeer nauwkeurig en snel uitvoeren (om te beginnen zonder logaritmetafels), dan moeten we beroep doen op computers. Maar zelfs de krachtigste computers hebben hun fysieke beperkingen... en laten dus geregeld een steekje (lees: een deel achter de komma) vallen. Om de problemen die hieruit voortkomen te onderkennen en op te vangen (afrondingsfouten, schijnbaar niet-convergerende berekeningen,...) maakt men gebruik van wiskundige methodes en theorieën die men onderbrengt onder de noemer *numerieke wiskunde*. Deze tak van de wiskunde houdt zich dus bezig met de discrepantie tussen de gewenste reële uitkomsten, en de gebruikte berekeningsmethodes die beperkt zijn in hun voorstellingsvermogen.

Laten we nu even de gekende toepassingsgebieden van de computer als krachtige rekenmachine buiten beschouwing, en kijken we alleen naar de machine zelf. Het staat buiten kijf dat de inwendige werking van een digitale computer een uitgesproken discreet karakter heeft: een bit heeft de waarde 0 dan wel 1, maar niets daartussen. Dit impliceert dat analyseren en logisch redeneren zoals dat in informatica-context voorkomt, ook een uitgesproken discreet karakter zal hebben. De deeltak van de wiskunde die zich ontfermt over alle methodes en theorieën met een *discrete* invalshoek, wordt de *discrete wiskunde* genoemd. Met 'discreet' bedoelt men dan 'afzonderlijk' of 'niet-verbonden'.

Dit houdt in dat we bij de in deze cursus bestudeerde objecten steeds een 'stapsgewijze' structuur zullen herkennen: een stap meer of een stap minder heeft betekenis, iets daartussen niet. Discrete wiskunde kan m.a.w. gezien worden als de tegenhanger van de continue wiskunde. Discrete wiskunde wordt bijvoorbeeld gebruikt als objecten dienen geteld te worden, bij het oplossen van logische problemen (waarbij slechts twee discrete waarden voorkomen, nl. 'waar' en 'vals'), bij het bestuderen van discrete structuren (bv. schema's, verzamelingen, permutaties, relaties, grafen, algoritmen, bomen)... Het mag dus duidelijk zijn dat discrete wiskunde heel veel toepassingen in de informatica kent, maar tevens een onmisbaar instrument vormt in tal van andere disciplines zoals statistiek, natuurkunde, telecommunicatie, besliskunde en andere takken van de wiskunde.

Wij zullen ons in deze cursus bezighouden met enkele elementaire begrippen en theorieën uit de discrete wiskunde—maar weet dat er nog veel meer rond te vertellen, onderzoeken en ontdekken valt (ook nú nog, de grote ontdekkingsreizigers van de wiskunde dateren niet allemaal uit de Griekse tijd of de Verlichting).

Om ons in genoeg houvast en links met de realiteit te voorzien, hieronder enkele toepassingsgebieden van de theorie(en) die de discrete wiskunde ons aanreikt.

- fysica
- chemie
- biologie
- communicatie
- elektronica en elektriciteit
- cryptografie
- codeertheorie
- akoestiek
- muziek
- informatica
  - computerarchitectuur en hardware design
  - design van softwaresystemen
  - beveiliging
  - generatie van random getallen
  - digitale signaalverwerking
  - computergrafiek en beeldverwerking
  - foutopsporing en -verbetering
  - analyse en design van algoritmen

Keer op het einde van de cursus nog eens terug naar dit lijstje, om na te gaan welke toepassingsgebieden van de discrete wiskunde we aanraakten in deze nota's.

Grieks alfabet

A	α	alpha	___	N	ν	nu	___
B	β	beta	___	Ξ	ξ	xi	___
Γ	γ	gamma	___	O	o	omikron	___
Δ	δ	delta	___	Π	π	pi	___
E	ϵ	epsilon	___	P	ρ	rho	___
Z	ζ	zèta	___	Σ	$\sigma\ \varsigma$	sigma	_____
H	η	èta	___	T	τ	tau	___
Θ	θ	thèta	___	U	υ	upsilon	___
I	ι	iota	___	Φ	$\varphi\ \phi$	phi	_____
K	κ	kappa	___	X	χ	chi	___
Λ	λ	lambda	___	Ψ	ψ	psi	___
M	μ	mu	___	Ω	ω	omega	___

Romeinse getallen

I	1
V	5
X	10
L	50
C	100
D	500
M	1000

Hoofdstuk 1

Basisbegrippen

In dit hoofdstuk gaan we eerst na welke soorten getalsystemen er bestaan en hoe we die getallen dan best noteren. Uiteraard zullen voornamelijk de discrete en de eindige systemen ($\mathbb{N}$ en $\mathbb{Z}_n$) van belang zijn voor het vervolg van de cursus.

Er komen al een aantal bewijzen voor in dit hoofdstuk. In het hoofdstuk rond bewijsstrategieën delen we bewijzen in naargelang de redenering die gebruikt werd (bewijs met inductie, bewijs uit het ongerijmde, gevallenstudie, ...). Keer nadien dus terug naar dit hoofdstuk, om na te gaan of je de (deel-)bewijzen kan classificeren volgens bewijsmethode.

1.1 Getallenverzamelingen

1.1.1 De natuurlijke getallen

$$\begin{array}{lcl} \mathbb{N} & = & \{0, 1, 2, 3, ...\} \\ \mathbb{N}_0 & = & \{1, 2, 3, ...\} \end{array}$$

Of nul al dan niet een natuurlijk getal genoemd wordt, is enkel een kwestie van definitie (lees: afspraak). Het is echter een feit dat het getal 0 pas lang na de andere getallen zijn intrede deed. En gelukkig maar dát het er is, anders telden we nog op zoals de Romeinen: uit 5+5=10 volgt makkelijk dat 50+50=100, maar uit V+V=X leid je niet zo makkelijk af dat L+L=C.

Eigenschappen van $\mathbb{N}$

- gesloten onder $+$ en $\times$ (als $a, b \in \mathbb{N}$, dan ook $a + b \in \mathbb{N}$ en $a \times b \in \mathbb{N}$)
- niet gesloten onder $-$ (uitbreiding tot $\mathbb{Z}$ nodig)
- niet gesloten onder $/$ (uitbreiding tot $\mathbb{Q}$ nodig)
- heeft natuurlijke ordening $<$
- getallen van $\mathbb{N}$ zijn ideale '*tellers*': ze vormen de natuurlijkste/eenvoudigste labels om een telling uit te voeren. Ze vormen uiteraard niet de enige mogelijkheid. Doch élk telproces gebruikt labels waarvan het patroon overeenkomt met dat van $\mathbb{N}$: je start met een eerste element, en voor elk element is er een uniek volgend element. Ga maar na: zelfs al tel je per 100 beginnend vanaf 50, dan heb je nog een eenvoudige overeenkomst tussen je zelfgekozen labels en $\mathbb{N}$ of $\mathbb{N}_0$:

50	150	250	350	450	...
↓	↓	↓	↓	↓	
1	2	3	4	...	

- elk getal uit $\mathbb{N}$ heeft dus een opvolger, en elk getal m van $\mathbb{N}$ kan uit 0 bekomen worden door (een eindig aantal) opeenvolgende opvolgers te beschouwen. Dit sluit zeer nauw aan bij iteratie of recursie en maakt meteen duidelijk dat $\mathbb{N}$ door een informaticus niet overschat kan worden.

1.1.2 De gehele getallen

$$\boxed{\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}}$$

De $\mathbb{Z}$ staat voor *Zahlen*, Duits voor *getallen*.

Voordelen ten opzichte van $\mathbb{N}$

- $\mathbb{Z}$ is een **ring**: gesloten voor $+, \times$ én $-$. Zie bijlage A.
- met minimale uitbreiding van $\mathbb{N}$ (nl. één extra element per element verschillend van nul), zijn de kansen om een wiskundige berekening te kunnen uitvoeren, merkbaar verhoogd.

Nadeel ten opzichte van $\mathbb{N}$

- cruciale inductie-eigenschap van $\mathbb{N}$ is verloren gegaan. Het is nu onmogelijk om bij een willekeurig element van $\mathbb{Z}$ uit te komen als je start bij een *vast gegeven geheel getal*, en enkel opvolgers mag nemen.

1.1.3 De rationale getallen

$$\boxed{\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0\}}$$

Voordeel ten opzichte van $\mathbb{Z}$

- $\mathbb{Q}$ is een **veld**: gesloten voor $+, \times, -$ én $/$.

Nadeel ten opzichte van $\mathbb{Z}$

- discrete ordening gaat verloren: je kan voor een rationaal getal niet aangeven wat zijn (unieke) opvolger is. Tussen elke twee rationale getallen x en y ligt namelijk een ander: $\frac{x+y}{2}$. De ordening is *dicht*.

1.1.4 De reële getallen

De reële getallenverzameling $\mathbb{R}$ kan niet zo eenvoudig omschreven worden als de vorige verzamelingen, tenzij we een meetkundige interpretatie aanhalen: de reële getallen stellen alle punten op een (geijkte) lijn voor; de reële getallenas. Hoewel de rationale getallen reeds dicht op elkaar zitten op die getallenas, zijn er altijd nog lengtes die we wel kunnen waarnemen, maar die niet overeenkomen met rationale getallen. Twee voorbeelden: $\sqrt{2}$ en π (de diagonaallengte van een vierkant met zijde 1, resp. de omtrek van een cirkel met diameter 1).

Stelling 1.1. *Het getal $\sqrt{2}$ is niet rationaal.*

Bewijs Dit wordt een bewijs uit het ongerijmde (zie hoofdstuk Bewijsstrategieën). We onderstellen dat $\sqrt{2} \in \mathbb{Q}$, en komen (na enig logisch redeneerwerk) uit op een contradictie. Daaruit valt (gezien het waterdichte redeneerwerk) uit te concluderen dat de premisse (de vooropgestelde onderstelling) fout is.

Stel $\sqrt{2} \in \mathbb{Q}$. Dus $\sqrt{2} = \frac{a}{b}$, met $a \in \mathbb{Z}$ en $b \in \mathbb{N}_0$. We kiezen a en b zó dat a en b onderling ondeelbaar zijn.[1] (Dus $\text{ggd}(a, b) = 1$; indien dit niet het geval was, stel $ggd(a, b) = c$, dan

[1] Twee getallen zijn onderling ondeelbaar als hun grootste gemene deler (ggd) gelijk is aan 1. Zie hoofdstuk rond modulorekening.

vervangen we a door $\frac{a}{c}$ en b door $\frac{b}{c}$.)

$\sqrt{2} = \frac{a}{b}$	
$\Rightarrow \quad 2 = \frac{a^2}{b^2}$	
$\Rightarrow \quad 2b^2 = a^2$	
$\overset{(1)}{\Rightarrow} \quad a^2$ is even	(1) : $b \in \mathbb{N}$
$\overset{(2)}{\Rightarrow} \quad a$ is even	(2) : kwadraat van oneven getal is oneven
$\Rightarrow \quad a = 2c,$ voor zekere $c \in \mathbb{Z}$	
$\Rightarrow \quad a^2 = 4c^2$	
$\Rightarrow \quad 4c^2 = 2b^2$	
$\Rightarrow \quad 2c^2 = b^2$	
$\overset{(3)}{\Rightarrow} \quad b$ is even	(3) : analoge redenering als bij a

Dit is een contraditie: als a en b beide even zijn (zoals hierboven aangetoond), is $\text{ggd}(a, b) \neq 1$. Dus is de oorspronkelijke onderstelling verkeerd, en $\sqrt{2} \notin \mathbb{Q}$. □

Voordeel ten opzichte van $\mathbb{Q}$

- Reële getallen spelen een cruciale rol in de ontwikkeling van de wiskundige analyse, en stemmen overeen met de natuurlijke intuïtie (denk maar aan de middelwaardestelling: niet mogelijk als er gaten in je getallenas zitten). Ook $\mathbb{R}$ is een veld.

1.1.5 Complexe getallen

$$\boxed{\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}}$$

Voordeel ten opzichte van $\mathbb{R}$

- Alle veeltermvergelijkingen in één onbekende kunnen nu opgelost worden (om te beginnen de vergelijking $x^2 + 1 = 0$). Zelfs de veeltermvergelijkingen met complexe coëfficiënten: $\mathbb{C}$ is een algebraïsch gesloten veld.

Nadeel ten opzichte van $\mathbb{R}$

- Getallen zijn niet meer op een natuurlijke manier te ordenen, maar het best gevisualiseerd in het vlak.

1.2 Modulorekenen

Tot nu toe herhaalden we de meest bekende getalsystemen (verzamelingen van getallen met bijhorende bewerkingen die altijd kunnen uitgevoerd worden in die verzameling). We zetten ze even op een rijtje:

$\mathbb{N}$	gesloten onder	$+$	$\times$			
$\mathbb{Z}$	gesloten onder	$+$	$\times$	$-$		
$\mathbb{Q}$	gesloten onder	$+$	$\times$	$-$	$/$	
$\mathbb{R}$	gesloten onder	$+$	$\times$	$-$	$/$	
$\mathbb{C}$	gesloten onder	$+$	$\times$	$-$	$/$	en algebraïsch gesloten (alle veeltermen in x hebben oplossing)

Er zijn echter nóg interessante getalsystemen. Veruit de meest interessante in de discrete wiskunde (en dus voor informatici) heb je al wel gebruikt, maar ben je misschien nog niet formeel tegengekomen. Het gaat om de eindige verzamelingen $\mathbb{Z}_n$ (de gehele getallen modulo n), met bijhorende optellings- en vermenigvuldigingsoperatoren.

$$\boxed{\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}, \quad n \in \mathbb{N}, n \geq 2}$$

Deze $+$ en $\times$ zijn echter niet dezelfde als de $+$ en $\times$ op gehele getallen: we willen immers dat $\mathbb{Z}_n$ gesloten is onder deze operatoren. Volgende definitie van $+$ en $\times$ in $\mathbb{Z}_n$ voldoet aan deze voorwaarde:

> *Optellen respectievelijk vermenigvuldigen gebeurt eerst zoals in $\mathbb{Z}$, waarna die (tussen-)uitkomst wordt vervangen door zijn rest bij deling door n.*

Opgelet! Als je de modulo-operator gebruikt in programmacode, ga dan eerst even na wat er gebeurt met negatieve getallen.

elementen van $\mathbb{Z}$	$\ldots$	-4	-3	-2	-1	0	1	2	3	4	$\ldots$
modulo 3 (wiskundig)	$\ldots$	2	0	1	2	0	1	2	0	1	$\ldots$
%-operator in C++	$\ldots$	-1	0	-2	-1	0	1	2	0	1	$\ldots$
%-operator in Python	$\ldots$	2	0	1	2	0	1	2	0	1	$\ldots$

Om berekeningen in $\mathbb{Z}_n$ vlot te laten verlopen, wordt er (voor kleine n) gebruik gemaakt van optellings- en vermenigvuldigingstabellen. Voor $\mathbb{Z}_8$ worden deze tabellen:

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$\times$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Gezien het binaire geval $\mathbb{Z}_2$ zeer belangrijk is voor de informatica, hieronder de $+$ en $\times$-tabellen voor $\mathbb{Z}_2$:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Twee bijkomende interpretaties van de optelling en vermenigvuldiging in $\mathbb{Z}_2$ springen hier in het oog:

- Staat 0 voor even en 1 voor oneven, dan lees je hier (o.a.) af dat oneven + oneven = even, en oneven $\times$ oneven = oneven.
- Anderzijds staan hierboven twee waarheidstabellen uit de logica (met 0=false, 1=true heb je respectievelijk de XOR-tabel en de AND-tabel).

In het hoofdstuk rond modulorekenen komen we uitgebreid terug op $\mathbb{Z}_n$, vanuit een meer theoretische invalshoek.

Hoofdstuk 2

Verzamelingen, relaties en functies

In dit hoofdstuk wordt een overzicht gegeven van een aantal elementaire begrippen en essentiële eigenschappen uit de verzamelingenleer en omtrent relaties tussen verzamelingen. De klemtoon ligt in dit hoofdstuk op het introduceren van een aantal fundamentele begrippen, die in dit en andere opleidingsonderdelen van het curriculum geregeld gebruikt worden.

We beperken ons in deze cursus tot de zogenaamde intuïtieve of naïeve verzamelingenleer, d.w.z. dat verondersteld wordt dat de lezer een intuïtieve notie van het begrip 'verzameling' heeft: een verzameling is het resultaat van het samennemen van een aantal onderscheidbare objecten tot één geheel. De streng-wiskundige behandeling van de verzamelingenleer valt buiten het kader van deze cursus.

2.1 Verzameling, element

Een **verzameling** wordt volledig bepaald door zijn elementen. Hetzelfde element kan geen tweemaal in de verzameling zitten, en de elementen van een verzameling zijn (a priori) niet geordend. Twee verzamelingen zijn dus gelijk als ze dezelfde elementen bevatten; bijvoorbeeld $\{1, 2, 3, 1\} = \{3, 2, 1\}$. Voorts gelden volgende notaties, voor verzamelingen A, B, C, A_i en elementen x, y, a, b:

Volgende symbolen worden gebruikt:

$x \in A$	x is element van A
$x \notin A$	x is geen element van A
$\varnothing$	ledige verzameling

Om op een ondubbelzinnige manier aan te geven welke elementen een verzameling bevat, bestaan er twee veelgebruikte manieren:

- **opsomming** of **enumeratie** : de elementen van de verzameling worden één na één neergeschreven
  Vb. $\mathbb{N} = \{0, 1, 2, \ldots, n, n+1, \ldots\}$
- **definitievoorschrift** : er wordt aangegeven aan welke eigenschappen een object moet voldoen om tot de verzameling te behoren
  Vb. $V = \{x : x \in \mathbb{Z} \text{ en } x \text{ is deelbaar door } 5\}$ is de verzameling van de veelvouden van 5

Als twee verzamelingen A en B bestaan uit dezelfde elementen, dan worden deze verzamelingen gelijk genoemd, notatie $A = B$. Om aan te duiden dat twee verzamelingen A en B verschillend zijn, schrijven we $A \neq B$.

Het aantal elementen van een verzameling A noemt men de **cardinaliteit** (Eng. cardinal number) van die verzameling, notatie $\#A$.
Bv. de cardinaliteit van de lege verzameling is 0: $\#\varnothing = 0$.

2.2 Deelverzameling

Als A en B twee verzamelingen zijn, waarbij elk element van A ook tot B behoort, dan noemt men A een deelverzameling (Eng. subset) van B.
Dit impliceert o.a. dat de lege verzameling deelverzameling is van elke willekeurige verzameling en dat iedere verzameling een deelverzameling is van zichzelf. Deze twee speciale gevallen worden onechte (Eng. improper) deelverzamelingen genoemd, alle andere deelverzamelingen zijn echte of strikte (Eng. proper) deelverzamelingen.

$A \subseteq B$	A is deelverzameling van B
$A \subset B$	A is strikte deelverzameling van B
$A \not\subset B$	A is geen deelverzameling van B

Voorbeeld

Stel $A = \{\text{rood}, \text{geel}, \text{blauw}\}$. Deze verzameling heeft twee onechte deelverzamelingen $\varnothing$ en $\{\text{rood}, \text{geel}, \text{blauw}\}$ en zes echte deelverzamelingen $\{\text{rood}\}$, $\{\text{geel}\}$, $\{\text{blauw}\}$, $\{\text{geel}, \text{blauw}\}$, $\{\text{rood}, \text{blauw}\}$ en $\{\text{rood}, \text{geel}\}$.

We kunnen nu ook de **machtsverzameling** of **delenverzameling** (Eng. power set) $\mathcal{P}(A)$ van een verzameling A definiëren: dit is de verzameling van alle deelverzamelingen van A, i.e. $\mathcal{P}(A) = \{X : X \subset A\}$. Men kan eenvoudig inzien dat de cardinaliteit van de machtsverzameling gegeven wordt door:

$$\#\mathcal{P}(A) = 2^{\#A}$$

2.3 Elementaire bewerkingen tussen verzamelingen

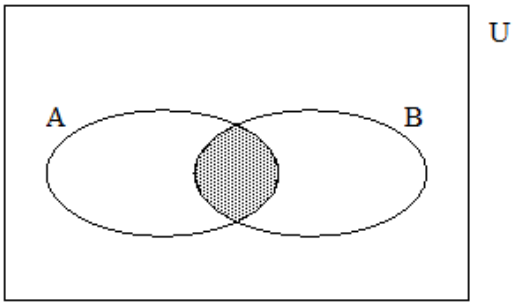
Indien men beschikt over een aantal verzamelingen, kan men verschillende bewerkingen definiëren tussen deze verzamelingen.

2.3.1 Doorsnede, unie, verschil, complement

Stel A en B zijn twee deelverzamelingen van een gegeven verzameling U, die de universele verzameling of het universum (Eng. universal set) wordt genoemd.

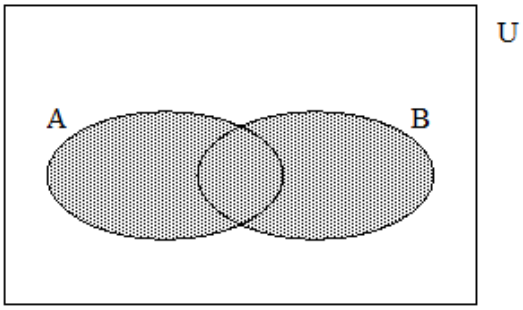
We definiëren:

doorsnede van A en B



$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

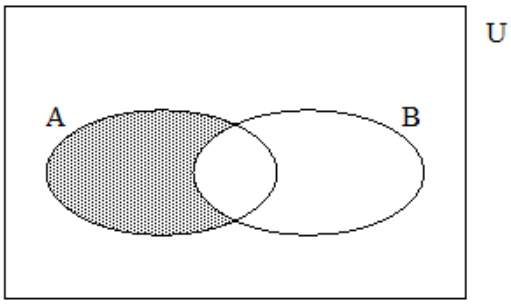
unie van A en B



$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

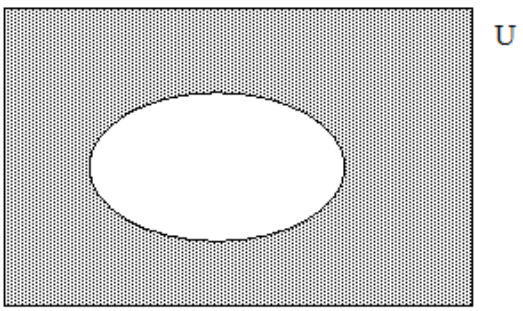
Twee verzamelingen A en B worden **disjunct** (Eng. disjoint) genoemd, als ze geen enkel element gemeen hebben : $A \cap B = \varnothing$.

verschil van A en B



$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$

complement van A tov een verzameling U



$$A^c = U \setminus A$$

De deelverzamelingen van een gegeven verzameling vormen een Booleaanse algebra onder de

operatoren $\cap$ en $\cup$. We kunnen nagaan dat commutativiteit, associativiteit, distributiviteit en De Morgans wetten van toepassing zijn; eventueel aan de hand van een Venndiagram.

$$\begin{array}{rcl|rcl} A \cap B & = & B \cap A & A \cup B & = & B \cup A \\ A \cap (B \cap C) & = & (A \cap B) \cap C & A \cup (B \cup C) & = & (A \cup B) \cup C \\ A \cap (B \cup C) & = & (A \cap B) \cup (A \cap C) & A \cup (B \cap C) & = & (A \cup B) \cap (A \cup C) \\ A \setminus (B \cap C) & = & (A \setminus B) \cup (A \setminus C) & A \setminus (B \cup C) & = & (A \setminus B) \cap (A \setminus C) \\ (B \cap C)^c & = & B^c \cup C^c & (B \cup C)^c & = & B^c \cap C^c \end{array}$$

2.3.2 Cartesisch product

Als A en B verzamelingen zijn, dan noemt men het **cartesisch product** (of kortweg product, Eng. product set) van A en$B$ de verzameling van alle koppels waarvan het eerste element tot A en het tweede element tot B behoort. Deze definitie wordt uitbreiden tot een product van meer dan twee verzamelingen:

$$\begin{array}{r|l|l} A \times B & \text{Cartesisch product van } A \text{ en } B & = \{(a,b) \mid a \in A \wedge b \in B\} \\ A_1 \times A_2 \times \ldots \times A_n & \text{Cartesisch product van } A_i \ (i = 1 \to n) & \\ & = \prod_{i=1}^{n} A_i = \prod A_i & \\ A^n & n\text{-voudig Cartesisch product van A} & = A \times A \times \ldots \times A \end{array}$$

Voorbeeld

$$\{a,b\} \times \{a,b,c\} = \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c)\}$$

2.4 Relaties en functies

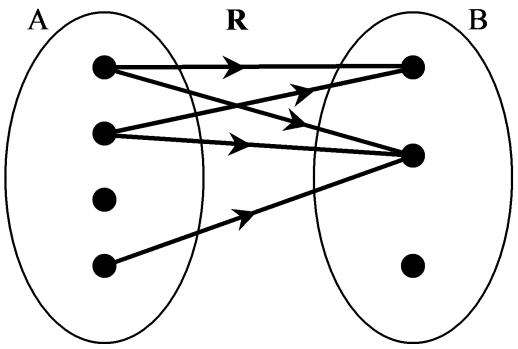
Steunende op bovenstaande definitie van cartesisch product kan men nu op eenvoudige wijze relaties en functies definiëren. Stel A en B zijn twee verzamelingen. Een binaire **relatie** (kortweg relatie, Eng. relation) R tussen A en B is een deelverzameling van het cartesisch product $A \times B$:

$$R \subset A \times B$$

dikwijls genoteerd als

$$R : A \to B$$

In een Venndiagram wordt een relatie weergegeven a.d.h.v. een aantal pijlen van A naar B :



Indien $B = A$, dan spreekt men over een relatie in A.

Het **domein** (Eng. domain) van de relatie R, notatie $dom\ R$, bestaat uit alle punten 'waaruit een pijl vertrekt' :

$$dom\ R = \{a \in A : \exists\, b \in B \text{ waarvoor } (a, b) \in R\}$$

Het **codomein** of bereik (Eng. range) van de relatie R, notatie $codom\ R$, bestaat uit alle punten 'waarin een pijl toekomt' :

$$codom\ R = \{b \in B : \exists\, a \in A \text{ waarvoor } (a, b) \in R\}$$

2.4.1 Speciale relaties

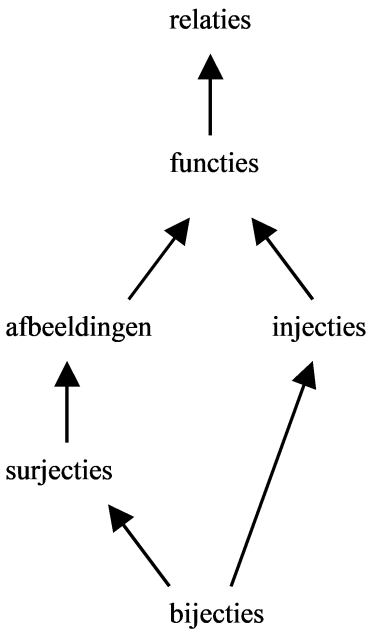
Bovenstaande definitie van een relatie laat heel veel vrijheid toe, voor vele wiskundige toepassingen moet een relatie aan strengere voorwaarden voldoen om zinvolle operaties te kunnen realiseren. Naargelang de bijkomende eigenschappen van een relatie, spreekt men van een functie, injectie, afbeelding, surjectie of bijectie.

- Een relatie R wordt een **functie** (Eng. function) als 'uit elk punt ten hoogste één pijl vertrekt'.
  Gezien het unieke beeld bij een functie, noteert men $(a, b) \in R$ in dit geval ook als $b = R(a)$, $a \in dom\ R$ wordt een argument voor de functie R genoemd .
- Een relatie R wordt een **afbeelding** (Eng. mapping) genoemd indien 'uit elk punt precies één pijl vertrekt'.
- Een relatie R wordt een **bijectie** (Eng. one-to-one mapping) genoemd indien 'uit elk punt precies één pijl vertrekt en in elk punt precies één pijl toekomt'.
- Een relatie R wordt een **injectie** (Eng. injection) genoemd indien 'uit elk punt ten hoogste één pijl vertrekt en in elk punt ten hoogste één pijl toekomt'.
- Een relatie R wordt een **surjectie** of opafbeelding (Eng. surjection, onto mapping) genoemd indien 'uit elk punt precies één pijl vertrekt en in elk punt tenminste één pijl toekomt'.

Deze definities worden samengevat in onderstaande tabel (waarbij '–' staat voor 'niet nader gespecificeerd') .

speciale relatie van A naar B	# pijlen vertrekkend uit punt van A	# pijlen toekomend in punt van B
functie	≤ 1	–
afbeelding	1	–
bijectie	1	1
injectie	≤ 1	≤ 1
surjectie	1	≥ 1

Uit deze eigenschappen kan volgende hiërarchische voorstelling afgeleid worden, waarbij een pijl staat voor een betekenisverruiming (ga zelf na !) :



2.4.2 Aantal elementen en aftelbaarheid

De definitie van een bijectie laat ons toe om terug te komen op de cardinaliteit van een verzameling. Twee verzamelingen A en B hebben per definitie evenveel elementen (of m.a.w. eenzelfde cardinaliteit) indien er een bijectie bestaat tussen A en B.

- Voor eindige verzamelingen A en B is deze definitie evident : het bestaan van een bijectie tussen twee eindige verzamelingen geeft aan dat deze verzamelingen eenzelfde aantal elementen bevatten.
- Voor oneindige verzamelingen is dit intuïtief minder evident. Men is bijvoorbeeld intuïtief geneigd om te zeggen dat $\mathbb{Z}$ meer elementen bevat dan $\mathbb{N}$, want alle natuurlijke getallen zijn ook gehele getallen en $\mathbb{Z}$ bevat daarnaast nog alle strikt negatieve gehele getallen. Nochtans, er bestaat een bijectie van $\mathbb{N}$ naar $\mathbb{Z}$, bijvoorbeeld

$$b : \mathbb{N} \to \mathbb{Z} : n \to z = \begin{cases} \dfrac{n}{2} & \text{als } n \text{ even} \\ -\dfrac{n+1}{2} & \text{als } n \text{ oneven} \end{cases}$$

  Dit impliceert dat $\mathbb{N}$ en $\mathbb{Z}$ in de wiskundige zin evenveel elementen bevatten !!

Op basis van de cardinaliteit wordt onderscheid gemaakt tussen al dan niet aftelbare verzamelingen :

- Een verzameling V wordt **countable** (Eng. denumerable) genoemd indien de verzameling V een eindig aantal elementen bevat of indien er een bijectie bestaat die de verzameling van de natuurlijke getallen $\mathbb{N}$ afbeeldt op de verzameling V (m.a.w. indien V evenveel elementen bevat als $\mathbb{N}$).
- Indien er voor een oneindige verzameling V geen zo'n bijectie bestaat, dan noemt men de verzameling V **overaftelbaar** of niet-aftelbaar.

Een eindige verzameling (ook de ledige verzameling) is dus steeds aftelbaar, een oneindige verzameling is ofwel aftelbaar, ofwel overaftelbaar.

Uit deze definitie volgt meteen dat $\mathbb{Z}$ aftelbaar is. Men kan zelfs bewijzen (zie oefeningen) dat ook de verzameling $\mathbb{Q}$ aftelbaar is. Dit ondanks het feit dat de verzameling $\mathbb{Q}$ intuïtief enorm veel ruimer lijkt dan $\mathbb{N}$, er zijn bv. tussen twee opeenvolgende natuurlijke getallen al oneindig veel rationale getallen! De aftelbaarheid van $\mathbb{Q}$ druist dus op het eerste zicht enigszins in tegen de intuïtie. Dit kan voornamelijk worden toegeschreven aan onze gewoonte om oneindigheid te beschouwen als een limietgeval en dus een logische uitbreiding van eindigheid, alhoewel oneindige structuren fundamenteel verschillend zijn van eindige. Om de lezer enigszins gerust te stellen : de verzameling $\mathbb{R}$ is wel overaftelbaar (dit laatste wordt aangetoond met het diagonaalbewijs van Cantor). Toch hebben niet alle overaftelbare verzamelingen dezelfde grootte.

2.4.3 Orderelaties

Definitie. *Stel V is een niet-lege verzameling. Een relatie R in V wordt een **(partiële) orderelatie** (Eng. partial ordering relation) genoemd als aan de volgende drie voorwaarden voldaan is:*

- *reflexiviteit:* $x \in V : (x, x) \in R$
- *antisymmetrie:* $x, y \in V : (x, y) \in R$ *en* $(y, x) \in R \Rightarrow x = y$
- *transitiviteit:* $x, y, z \in V : (x, y) \in R$ *en* $(y, z) \in R \Rightarrow (x, z) \in R$

Voorbeeld

Beschouwen we als voorbeeld de relatie '$\subset$' in de machtsverzameling $\mathcal{P}(A)$ van een willekeurige verzameling A. Dan kan men eenvoudig inzien dat de drie voorwaarden voor een partiële orderelatie vervuld zijn. Dit voorbeeld verduidelijkt ook de benaming van dit type relaties. De relatie brengt een zekere 'orde' of hiërarchie in de verzameling A: een kleine verzameling $X \in \mathcal{P}(A)$ kan een deelverzameling zijn een grotere verzameling $Y \in \mathcal{P}(A)$, wat betekent dat X zich 'lager in de hiërarchie' bevindt dan Y. De ordening is echter slechts partieel: het is immers ook mogelijk dat een kleine verzameling X geen deelverzameling vormt van een grotere verzameling Y, wat betekent dat deze X en Y niet 'geordend' worden door de relatie '$\subset$'.

Definitie. *Een partiële orderelatie R in V wordt een* ***totale orderelatie*** *(Eng. total ordering relation) genoemd als bovendien aan een vierde voorwaarde voldaan is:*

- $\forall x, y \in V : (x, y) \in R$ *of* $(y, x) \in R$

Voorbeeld

Beschouwen we als voorbeeld de relatie '$\leq$' in $\mathbb{N}$. Deze relatie is een totale orderelatie (ga zelf na !). In tegenstelling tot vorig voorbeeld kan men hier twee willekeurige elementen steeds vergelijken en 'ordenen'.

Als een verzameling V geordend wordt m.b.v. een totale orderelatie, dan spreekt men over een **lineair geordende relatie** of **ketting**, om evidente redenen.

Definitie. *Met elke partiële of totale orderelatie correspondeert een* ***strikte orderelatie*** *(Eng. strict ordering relation), die bekomen wordt door alle reflexieve pijlen te verwijderen. Een strikte orderelatie is dus* ***antireflexief*** *i.p.v. reflexief.*

Voorbeeld

'$\leq$' is een gewone orderelatie, '$<$' is de strikte variant ervan.

Hoofdstuk 3

Modulorekenen

In dit hoofdstuk bespreken we modulorekenen (Eng. modular arithmetic) met gehele getallen. Deze theorie kent een aantal belangrijke toepassingen, zoals het schrijven van getallen in binaire of hexadecimale notatie, het genereren van (pseudo)random getallen in een computer en het coderen van een bericht in geheimschrift (cryptologie).

In wat volgt stellen n en p steeds strikt positieve gehele getallen voor ($m, p \in \mathbb{N}_o$). Alle andere symbolen $a, b, c, d, x, \cdots$ zijn willekeurige gehele getallen ($a, b, c, d, x, \cdots \in \mathbb{Z}$).

3.1 Priemgetallen en deelbaarheid

3.1.1 Fundamentele eigenschappen van deelbaarheid

Modulorekenen gebruikt enkel gehele getallen. Een belangrijk probleem daarbij is dat de deling niet inwendig is in $\mathbb{Z}$ (zie Hoofdstuk 1). Daar zal het dikwijls misgaan bij het oplossen van vergelijkingen. Vandaar de belangrijke plaats die deelbaarheid zal innemen in dit hoofdstuk.

Vooraleer in te gaan op modulorekening, herhalen we kort een aantal gekende eigenschappen omtrent deelbaarheid (zonder bewijzen).

Definitie. *Gegeven 2 gehele getallen a en b met $a \neq 0$. Als er een geheel getal c bestaat zodat $a \cdot c = b$, dan zeggen we a* **deelt** *b. In dat geval noteren we $a \mid b$, we noemen a een* **deler** *of* **factor** *van b, en b een* **veelvoud** *van a.*

Voorbeeld

- -2 is een deler van 6;
- 3 is geen deler van 5;
- 0 is enkel deler van zichzelf;
- alle gehele getallen zijn delers van 0.

Als a geen deler is van b, schrijven we $a \nmid b$. Als $a \mid b$ met a positief en verschillend van b, dan noemen we a een **eigenlijke deler van** b. We zullen ons in wat volgt ook enkel bezighouden met eigenlijke delers. Is a bovendien groter dan 1, dan noemen we a een **niet-triviale deler** van b. De triviale delers van a zijn 1 en a zelf.

Definitie. *Een* **priemgetal** *p is een positief geheel getal dat enkel triviale delers heeft (nl. 1 en p).*

Men heeft aangetoond dat er oneindig veel priemgetallen bestaan.

Voorbeeld

2, 3, 5, 7, 11, ... zijn priemgetallen. Merk op dat 1 geen priemgetal is, want 1 heeft slechts één positieve deler.

Stelling 3.1. Fundamentele stelling van de rekenkunde (priemontbinding) *Elk geheel getal groter dan 1 kan op unieke manier geschreven worden als product van priemgetallen:*

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

met $p_1, p_2, \ldots, p_k$ onderling verschillende priemgetallen, en $n_1, \ldots, n_k$ positieve gehele getallen. We noemen $\prod_{i=1}^{k} p_i^{n_i}$ de **priemontbinding** *of* **priemfactorisatie** *van n.*

Voorbeeld

Het getal 192 kan men schrijven als $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^6 \cdot 3$.

Gevolg 3.2. *Het aantal delers van n is exact gelijk aan:*

$$(n_1 + 1) \cdot (n_2 + 1) \cdot \ldots \cdot (n_k + 1) = \prod_{i=1}^{k} (n_i + 1)$$

Voorbeeld

Het getal 192 heeft $7 \cdot 2 = 14$ delers:

1	2	2^2	2^3	2^4	2^5	2^6
3	3.2	3.2^2	3.2^3	3.2^4	3.2^5	3.2^6

3.1.2 Delingsalgoritme

Het hiernavolgende delingsalgoritme drukt uit dat, ook als a geen deler is van b, we de deling op een unieke manier '*zo ver mogelijk*' kunnen uitvoeren – waarbij we dan met een rest (kleiner dan a) blijven zitten.

Stelling 3.3. Delingsalgoritme *Stel $a, b \in \mathbb{N}$, $b > 0$. Dan bestaan er unieke gehele getallen $q, r \in \mathbb{N}$ zodat*

$$a = b \cdot q + r \qquad 0 \leq r < b.$$

Hier is a het **deeltal**, *q het* **quotient**, *b de* **deler** *en r de* **rest**. *De rest $r \neq 0$ als en slechts als $b \nmid a$.*

Merk op dat de rest steeds positief is, ook al is het deeltal negatief! Bijvoorbeeld bij de gehele deling van -3 door 4 vinden we $q = -1$ en $r = 1$ (niet $q = 0$ en $r = -3$).

3.1.3 Grootste gemene deler en kleinste gemeen veelvoud

De **grootste gemene deler** (Eng. greatest common divisor) van a en b is het grootste getal d waarvoor $d \mid a$ en $d \mid b$. Notatie: $\text{ggd}(a, b)$.

Het **kleinste gemeen veelvoud** (Eng. least common multiple) van twee gehele getallen a en b is het kleinste positief getal d waarvoor $a \mid d$ en $b \mid d$. Notatie: $\text{kgv}(a, b)$.

Aan de hand van de ontbinding in priemfactoren van a en b kan men gemakkelijk aantonen dat steeds

$$\text{ggd}(a, b) \cdot \text{kgv}(a, b) = |a \cdot b|$$

Definitie. *Twee getallen a en b worden* **relatief priem** *genoemd als $ggd(a, b) = 1$. Getallen $a_1, a_2, \ldots, a_k$ worden* **paarsgewijs relatief priem** *genoemd als $ggd(a_i, a_j) = 1$ voor $i \neq j$.*

3.1.4 Algoritme van Euclides

Met het *algoritme van Euclides* kan de grootste gemene deler van a en b berekend worden zonder beide getallen eerst te ontbinden in priemfactoren. Het basisprincipe van dit algoritme is: "de grootste gemene deler van twee getallen verandert niet als het kleinere getal van het grotere wordt afgetrokken", in symbolen: $\text{ggd}(a, b) = \text{ggd}(a - b, b) = \text{ggd}(a, b - a)$.

Voorbeeld

$$\begin{array}{llll} \text{ggd}(14, 91) & = \text{ggd}(14, 77) & = \text{ggd}(14, 63) & = \text{ggd}(14, 49) \quad = \text{ggd}(14, 35) \\ & = \text{ggd}(14, 21) & = \text{ggd}(14, 7) & = \text{ggd}(7, 7) \quad = 7 \end{array}$$

In de praktijk gaat dit nog veel sneller als je gebruik maakt van het Delingsalgoritme (stelling 3.3). Om $\text{ggd}(a, b)$ te bepalen, bereken je $q, r \in \mathbb{N}$ zodat

$$a = b \cdot q + r \qquad 0 \leq r < b.$$

Dan is $\text{ggd}(a, b) = \text{ggd}(b, r)$: trek q keer het getal b af.

Praktische methode voor het berekenen van $\text{ggd}(a, b)$ met het Algoritme van Euclides:

$$\begin{array}{rcll} a & = & bq_0 + r_1 & 0 < r_1 < b \\ b & = & r_1q_1 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & r_2q_2 + r_3 & 0 < r_3 < r_2 \\ & \cdots & & \\ r_{n-2} & = & r_{n-1}q_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} & = & r_nq_n + 0 & \end{array}$$

De laatste niet-triviale rest, nl. r_n, is de grootste gemene deler van a en b.

Voorbeeld

Bepaal $\text{ggd}(91, 14)$

$$\begin{array}{rcl} 91 & = & 14 \cdot 6 + 7 \\ 14 & = & 7 \cdot 2 + 0 \end{array}$$

$\text{ggd}(91, 14) = \text{ggd}(14, 7) = 7$

Het algoritme van Euclides laat ons bovendien toe de lineaire combinatie van a en b te vinden, die precies gelijk is aan hun grootste gemene deler.

Stelling 3.4. Uitgebreid algoritme van Euclides *Voor twee gehele getallen a en b, niet beide nul bestaan er 2 gehele getallen x en y zodat*

$$d = ggd(a, b) = a \cdot x + b \cdot y$$

Bovendien kunnen de waarden van x en y in $\text{ggd}(a, b) = a \cdot x + b \cdot y$ bekomen worden door r_n (via r_{n-1}, r_{n-2},...) als lineaire combinatie van a en b te schrijven.

Voorbeeld

Schrijf $\text{ggd}(336, 1768)$ als $336 \cdot x + 1768 \cdot y$.
Uiteraard moeten we eerst de grootste gemene deler vinden.

$$\begin{array}{rcl} 1768 & = & 5 \cdot 336 + 88 \\ 336 & = & 3 \cdot 88 + 72 \\ 88 & = & 1 \cdot 72 + 16 \\ 72 & = & 4 \cdot 16 + 8 \\ 16 & = & 2 \cdot 8 + 0 \end{array}$$

De grootste gemene deler is dus 8. Daarna doorlopen we de stappen in omgekeerde volgorde, waarbij we de vermenigvuldigingen uiteraard niet expliciet uitwerken.

(Let op: we starten bij de voorlaatste regel van voorgaande afleiding!)

$$\begin{aligned} 8 &= 72 - 4 \cdot 16 \\ &= 72 - 4(88 - 1 \cdot 72) \\ &= -4 \cdot 88 + 5(336 - 3 \cdot 88) \\ &= 5 \cdot 336 - 19 \cdot 88 \\ &= 5 \cdot 336 - 19(1768 - 5 \cdot 336) \\ &= -19 \cdot 1768 + 100 \cdot 336 \end{aligned}$$

... en natuurlijk niet vergeten narekenen!

Gevolg 3.5. *Twee gehele getallen getallen a en b zijn relatief priem als en slechts als er gehele getallen x en y bestaan zodat*

$$a \cdot x + b \cdot y = 1$$

3.2 Rekenen in $\mathbb{Z}_n$

In de vorige paragraaf leerden we rekenen in $\mathbb{Z}$. Dit ligt al dichter bij de bitbewerkingen die een computer uitvoert, dan rekenen in $\mathbb{R}$. Toch zijn we er nog niet helemaal. Stelt men met een 32-bitspatroon natuurlijke getallen voor, dan weet je dat nà het getal 0 (bitpatroon 00..00) het getal 1 volgt (bitpatroon 00..01). Nà het getal $2^{32} - 1$ (bitpatroon 11..11) volgt echter 0 (bitpatroon 00..00) in plaats van 2^{32} : de computer rekent namelijk modulo 2^{32}. Vandaar dat modulair rekenen hier het logische verlengstuk vormt op vorige paragraaf.

Definitie. *Stel $a, n \in \mathbb{Z}$ en $n > 1$.*

$r = a \bmod n$ *wordt gelezen als 'r is a modulo n' of*
'r is de rest van a bij deling door n'
(gevolg: $a \leq r < n$ en $r = a - \left\lfloor \frac{a}{n} \right\rfloor n$)

$a \stackrel{n}{=} b$ *wordt gelezen als 'a is congruent met b modulo n'*
en staat voor $a \bmod n = b \bmod n$
(let op: hier hoeven a noch b kleiner te zijn dan n)

Twee getallen zijn dus congruent modulo n als ze dezelfde rest bij deling door n hebben. De congruentierelatie ($\stackrel{n}{=}$) is reflexief, symmetrisch en transitief, net zoals de '*ordinaire*' gelijkheid:

Stelling 3.6. *Stel n een positief geheel getal. De congruentierelatie ($\stackrel{n}{=}$) is een **equivalentierelatie** op de verzameling $\mathbb{Z}$, nl.*

reflexief	$a \stackrel{n}{=} a$	$\forall a \in \mathbb{Z}$
symmetrisch	$a \stackrel{n}{=} b \Rightarrow b \stackrel{n}{=} a$	$\forall a, b \in \mathbb{Z}$
transitief	$a \stackrel{n}{=} b$ en $b \stackrel{n}{=} c \Rightarrow a \stackrel{n}{=} c$	$\forall a, b, c \in \mathbb{Z}$

Vorige stelling zegt dat de congruentierelatie een equivalentierelatie is op $\mathbb{Z}$. De congruentierelatie $\stackrel{n}{=}$ deelt $\mathbb{Z}$ op in n verschillende equivalentieklassen. In getaltheorie spreken we van de **congruentieklassen**, **residuklassen** of **restklassen**. Formeel:

$$\begin{aligned} [a]_n &= \{x \mid x \in \mathbb{Z} \text{ en } x \stackrel{n}{=} a\} \\ &= \{a + k \cdot n \mid k \in \mathbb{Z}\} \end{aligned}$$

Gezien $[a]_n = [a + ln]_n = [a - ln]_n = \ldots$, doen we er goed aan de notatie voor een equivalentieklasse éénduidig te maken door een vaste representant van de klasse te kiezen. Dit wordt het kleinste niet-negatieve getal a uit de congruentieklasse. Dit getal a is dus kleiner dan n (anders is $a - n$ kleiner dan a en toch nog niet negatief). De verzameling van alle residuklassen modulo n wordt genoteerd als

$$\mathbb{Z}_n = \{[a]_n \mid 0 \leq a < n\}.$$

Merk op: in hoofdstuk 1 zagen we de definitie

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

Dit is uiteraard equivalent met bovenstaande definitie, in zoverre we 0 interpreteren als de restklasse $[0]_n$, 1 als de restklasse $[1]_n$ enzovoort. In plaats van de congruentieklasse, wordt enkel zijn representant gebruikt — maar de onderliggende klasse hou je best in gedachten! (Zo is -2 in $\mathbb{Z}_5$ gelijk aan 3.)

3.2.1 Rekenregels in $\mathbb{Z}_n$

Om vlot te rekenen in $\mathbb{Z}_n$, kunnen we rekenregels opstellen zoals in $\mathbb{Z}$.

Eerst tonen we aan dat de congruentieklassen stabiel zijn onder de optelling, vermenigvuldiging en machtsverheffing in $\mathbb{Z}_n$: de congruentieklasse die hoort bij de som van twee representanten zal goed gedefinieerd zijn, ongeacht de keuze van de representant. Analoog voor de andere bewerkingen.

Stelling 3.7. *Gegeven $a, b, A, B \in \mathbb{Z}$. Als $[a]_n = [A]_n$ en $[b]_n = [B]_n$, dan geldt*

$$\begin{aligned} [a \pm b]_n &= [A \pm B]_n \\ [a \cdot b]_n &= [A \cdot B]_n \\ [a^m]_n &= [A^m]_n \end{aligned}$$

Dit laat ons nu toe volgende bewerkingen op congruentieklassen te definiëren:

$$\begin{aligned} [a]_n + [b]_n &= [a + b]_n \\ [a]_n - [b]_n &= [a - b]_n \\ [a]_n \cdot [b]_n &= [a \cdot b]_n \\ [a]_n^m &= [a^m]_n \end{aligned}$$

Voorbeeld

$[2]_3 + [1]_3 = [3]_3 = [0]_3$
$[12]_{32} \cdot [17]_{32} = [204]_{32} = [12]_{32}$

3.2.2 Toepassing: genereren van pseudorandom getallen

Bij computersimulaties heeft men dikwijls nood aan random gegenereerde getallen. Verschillende methoden werden ontwikkeld om getallen te genereren die karakteristieken vertonen van random gekozen getallen. Omdat getallen gegenereerd door systematische methoden niet echt random zijn, spreekt men van **pseudorandom getallen** (Eng. pseudorandom numbers).

De meest gebruikte techniek voor het genereren van pseudorandom getallen is de lineaire-congruentiemethode. Hierbij kiezen we 4 gehele getallen :

- de modulus m ($m > 0$) ;
- de factor a ;
- het increment c ;
- de kiem (Eng. seed) x_0.

Uitgaande van deze getallen kunnen we pseudorandom getallen genereren via de recurrente betrekking

$$x_{i+1} = (a \cdot x_i + c) \bmod m \qquad (i \in \mathbb{N})$$

Dit levert een rij van pseudorandom getallen $x_0,\ x_1,\ x_2,\ \cdots$ op waarbij steeds $x_i \in \{0, 1, \cdots, m\}$.

Voorbeeld

> Indien we bijvoorbeeld $m = 9, a = 7, c = 4, x_0 = 3$ kiezen, dan bekomen we de rij
> 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6,$\cdots$
> Na 9 getallen herhaalt de rij zichzelf (periode = 9).

Zoek zelf een voorbeeld van een pseudorandom generator waarbij de periode kleiner is dan m ! Om een rij te bekomen die er 'zo random mogelijk' uitziet, heeft men liefst een zo groot mogelijke periode voor m. Een veelgebruikte generator in de praktijk, met $m = 2^{31} - 1, a = 75$ en $c = 0$, heeft periode van $2^{31} - 1$.

Er zijn in de literatuur volgende drie keuzes :

1. (Lehmer random number generator) m is een priemgetal en $c = 0$
   De periode is $m - 1$ indien de factor a een 'generator' is voor $\mathbb{Z}_m$. D.w.z. dat a, $2a$, $3a$, ... alle elementen van $\mathbb{Z}_m$ doorlopen.
2. $m = 2^k$ en $c = 0$
   Veelgebruikt zijn $m = 2^{32}$ of $m = 2^{64}$.
   De maximale periode is $m/4$.
3. $c \neq 0$ en bovendien $\text{ggd}(c, m) = 1$, $a - 1$ is deelbaar door alle priemfactoren van m, $a - 1$ is deelbaar door 4 als m deelbaar is door 4. Dit is gekend als het Hull–Dobell Theorem.

3.3 Elementaire vergelijkingen bij modulorekenen

Een belangrijk probleem in $\mathbb{Z}_n$ is uiteraard het oplossen van vergelijkingen.

De meest elementaire vergelijking is (onbekende $x \in \mathbb{Z}$)

$$a + x \stackrel{n}{=} b \qquad (*)$$

Oplossing van deze vergelijking is eenvoudig :

$$x \stackrel{n}{=} b - a$$

of nog :

$$x = b - a + k \cdot n,\ k \in \mathbb{Z}$$

In $\mathbb{Z}$ heeft de vergelijking (*) dus oneindig veel oplossingen. Deze oplossingen zijn echter onderling allemaal congruent modulo n. Er is dus slechts één oplossing van de vergelijking (*) in $\mathbb{Z}_n$, nl. $[b-a]_n$. Nog anders gezegd, de vergelijking (*) heeft slechts één oplossing x in $\mathbb{Z}$ die voldoet aan $x \in 0, 1, 2, \cdots, n-1$, nl. $(b-a) \bmod n$.

Voorbeeld

De vergelijking $5 + x \stackrel{3}{=} -2$ heeft in $\mathbb{Z}_3$ als unieke oplossing $[-2-5]_3$ of nog $[2]_3$.

3.3.1 Lineaire congruenties

De multiplicatieve tegenhanger van vergelijking (2.2):

$$a \cdot x \stackrel{n}{=} b$$

is (helaas) minder triviaal.

Een vergelijking van deze vorm wordt een lineaire congruentie (Eng. linear congruence) genoemd.

Om deze vergelijking op te lossen zouden we moeten "delen door a". In $\mathbb{Z}$ is dit niet (altijd) mogelijk ($\mathbb{Z}$ werd uitgebreid tot $\mathbb{Q}$ om de verzameling wél gesloten te maken voor de deling). Maar hoe zit het met $\mathbb{Z}_n$?

We moeten dus een manier zoeken om te bepalen wanneer een deling $\frac{1}{a}$ mogelijk is in $\mathbb{Z}_n$.

Merk eerst op dat $\frac{b}{a} = b \cdot \frac{1}{a}$. We noemen $\frac{1}{a}$ het **multiplicatief invers** of **modulair inverse** van a modulo n. Of nog: twee getallen x en y zijn elkaars inverse voor de vermenigvuldiging in $\mathbb{Z}_n$ als

$$x \cdot y \stackrel{n}{=} 1 \stackrel{n}{=} y \cdot x$$

Merk op dat, voor gegeven (x, n), het getal y niet altijd bestaat. Kijk maar in de vermenigvuldigingstabellen in Hoofdstuk 1: niet elke kolom in de vermenigvuldigingstabel voor $\mathbb{Z}_8$ bevat een 1, dus de getallen 2, 4 en 6 hebben geen modulair invers in $\mathbb{Z}_8$. (Het getal 0 heeft uiteraard nooit een modulair invers.)

Stelling 3.8. *Als ggd$(a, n) = 1$, dan bestaat er precies één geheel getal $x \in \{0, 1, 2, \cdots, n-1\}$ waarvoor:*

$$a \cdot x \stackrel{n}{=} 1 \stackrel{n}{=} x \cdot a$$

Dit getal x wordt de inverse van a modulo n genoemd.

Bewijs
Het bewijs verloopt in twee stappen. We bewijzen eerst dat er steeds zo'n x bestaat, daarna tonen we aan dat deze x uniek is.

1. Als $\text{ggd}(a, n) = 1$, dan weten we dankzij het uitgebreid algoritme van Euclides (stelling 2.3) dat er gehele getallen u en v bestaan waarvoor $u \cdot a + v \cdot n = 1$. Daaruit volgt meteen dat $u \cdot a \stackrel{n}{=} 1$. Het getal $x = u \bmod n$ is dus een inverse van a modulo n die voldoet aan $0 \leq x < n$. Er bestaat dus tenminste één inverse van a modulo n.

2. (Bewijs uit het ongerijmde) Stel nu dat er twee verschillende gehele getallen x_1 en x_2 bestaan die voldoen aan de vergelijking en waarvoor $0 \leq x_i < n$. Uit $a \cdot x_1 \stackrel{n}{=} 1$ en $a \cdot x_2 \stackrel{n}{=} 1$ volgt dat $a \cdot (x_1 - x_2) \stackrel{n}{=} 0$. M.a.w. $n \mid a \cdot (x_1 - x_2)$.

   Aangezien $\text{ggd}(a, n) = 1$, volgt daaruit dat $n \mid (x_1 - x_2)$. Dit leidt tot een contradictie, want $0 \leq x_i < n$.

   Besluit: er bestaat ten hoogste één inverse van a modulo n.

Stelling 3.9. *Het aantal oplossingen $x \in \{0, 1, \cdots n-1\}$ van de lineaire congruentie*

$$a \cdot x \stackrel{n}{=} b \quad (*)$$

hangt af van de ggd(a, n) en b:

- *als b geen veelvoud is van ggd(a, n) dan heeft de vergelijking (*) geen oplossingen in $\mathbb{Z}$.*
- *als b wel een veelvoud is van ggd(a, n), dan heeft de vergelijking (*) precies $d =$ ggd(a, n) oplossingen $x \in \{0, 1, 2, \cdots, n-1\}$.*
  Als x_0 een oplossing is, dan zijn alle andere oplossingen in $\{0, 1, \cdots, n\}$ gegeven door:

$$x = x_0 + t \cdot \frac{n}{d} \ (mod\ n) \qquad t = 0, 1, \cdots, d-1$$

Bewijs
We onderscheiden 3 gevallen in de bewijsvoering.

1. b is geen veelvoud van $\text{ggd}(a, n)$ - (Bewijs uit het ongerijmde)
   Stel dat er een geheel getal x bestaat dat voldoet aan vergelijking (*).

Uit $a \cdot x \overset{n}{=} b$ volgt dat er een geheel getal k bestaat waarvoor $a \cdot x - b = k \cdot n$ of nog $b = a \cdot x - k \cdot n$. Het rechterlid is een veelvoud van $\text{ggd}(a, n)$, dus is ook het linkerlid b een veelvoud van $\text{ggd}(a, n)$. Dit is in contradictie!
Besluit: de beginonderstelling (er bestaat een oplossing $x \in \mathbb{Z}$) was verkeerd.

2. $\text{ggd}(a, n) = 1$ (en dus $\text{ggd}(a, n) \mid b$)
In dit geval weten we dankzij bovenstaand stelling dat a een unieke inverse modulo n bezit, die stellen we voor als i. Stel dat er een geheel getal $x \in \{0, 1, 2, \cdots, n-1\}$ bestaat dat voldoet aan vergelijking (*). Dan weten we dat $i \cdot (a \cdot x) \overset{n}{=} i \cdot b$ of wegens de associativiteit van de vermenigvuldiging is $(i \cdot a) \cdot x \overset{n}{=} x \overset{n}{=} i \cdot b$.
Het getal $x = i \cdot b \bmod n$ is dus een oplossing van de vergelijking (*). Er is dus minstens één oplossing van de vergelijking (*) $\in \{0, 1, 2, \cdots, n-1\}$.
Net zoals in het bewijs van de vorige stelling toon je aan dat deze oplossing ook uniek is.

3. $\text{ggd}(a, n) = d > 1$ en b is een veelvoud van d.
Dit betekent dat d een deler is van a, b en n.
Herschrijf (*) als: $a \cdot x = b + k \cdot n$ en deel beide leden door d:

$$\frac{a}{d} \cdot x = \frac{b}{d} + k \cdot \frac{n}{d}$$

Alle coëfficiënten zijn gehele getallen, dus bekomen we een gelijkwaardige congruentie:

$$\frac{a}{d} \cdot x \overset{\frac{n}{d}}{=} \frac{b}{d}$$

Aangezien $\text{ggd}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, weten we uit geval 2 dat deze vergelijking precies één oplossing r heeft in $\left\{0, 1, 2, \cdots, \frac{n}{d} - 1\right\}$.
Alle gehele oplossingen van deze vergelijking zijn dus van de gedaante $r + t\frac{n}{d} \quad (t \in \mathbb{Z})$.
Precies d van deze oplossingen liggen in $\{0, 1, 2, \cdots, n-1\}$.

Opmerkingen

1. Bovenstaand bewijs legt niet alleen het aantal oplossingen vast, het geeft meteen ook aan hoe deze oplossingen kunnen gevonden worden: via het uitgebreid algoritme van Euclides en de daaruit voortvloeiende lineaire combinatie $u \cdot a + v \cdot n = \text{ggd}(a, n)$.

2. De oplossingsmethode herleid een lineaire congruentie van de algemene gedaante

$$a \cdot x \overset{n}{=} b$$

tot een lineaire congruentie waarbij de coëfficiënt a gelijk aan 1 is.
Dit impliceert dat we ons hierna kunnen concentreren op lineaire congruenties van de gedaante

$$x \overset{n}{=} b$$

(d.w.z. coëfficiënt $a = 1$) zonder aan algemeenheid in te boeten.

3.4 Lineaire Diophantische vergelijkingen.

Probleemstelling: een **lineare Diophantische vergelijking** heeft de vorm $ax + by = c$ met $a, b, c \in \mathbb{Z}$, met a en b niet beide nul. We zoeken alle oplossingen $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. We willen weten wanneer er oplossingen zijn, en hoeveel oplossingen er zijn.

Stelling 3.10. *De lineaire Diophantische vergelijking*

$$ax + by = c \qquad (*)$$

heeft oplossingen $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ als en slechts als c veelvoud is van $ggd(a, b)$. Als (x_0, y_0) een oplossing is, dan is de algemene oplossing van de vorm

$$(x, y) = \left(x_0 + t \cdot \frac{b}{d} \ , \ y_0 - t \cdot \frac{a}{d} \right) \qquad t \in \mathbb{Z},\ d = ggd(a, b).$$

Bewijs
Merk op: Er is een duidelijk verband tussen de lineaire Diophantische vergelijking (*) en de lineaire congruentie:

$$a \cdot x \stackrel{b}{=} c \qquad (**)$$

1) Voor elke oplossing xb van (**) bestaat $k \in \mathbb{Z}$ zodat $a \cdot xb = c + k \cdot b$. Dus is $(xb, -k) \in \mathbb{Z} \times \mathbb{Z}$ een oplossing van de Diophantische vergelijking (*).

2) Voor elke oplossing $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ van de Diophantische vergelijking (*) is $a \cdot x = c - y \cdot b$, dus voldoet $xb = x \bmod b$ aan de lineaire congruentie (**) en bovendien is $xb \in \{0, 1, 2, \cdots, b-1\}$

Gebruik nu de stelling 3.9:

Als c geen veelvoud is van $\text{ggd}(a, b)$ dan heeft de lineaire congruentie (**) geen oplossingen, dus heeft de Diophantische vergelijking (*) ook geen oplossingen.

Als c wel een veelvoud is van $\text{ggd}(a, b)$ dan heeft de lineaire congruentie (**) minstens één oplossing x_0, en dus heeft de Diophantische vergelijking (*) ook minstens één oplossing.

Alle oplossingen van de lineaire congruentie (**) zijn van de vorm:

$$x = x_0 + t \cdot \frac{b}{d} \pmod{b} \qquad t = 0, 1, \cdots, d-1 \qquad \text{met } d = \text{ggd}(a, b)$$

Voor $x = x_0 + t \cdot \dfrac{b}{d}$ zoeken we de bijhorende y. Omdat $a \cdot x_0 + b \cdot y_0 = c$ is ook:

$$a \cdot \left(x_0 + t \cdot \frac{b}{d} \right) + b \cdot \left(y_0 - t \cdot \frac{a}{d} \right) = c$$

Dus zijn alle oplossingen van de Diophantische vergelijking (*) bepaald door:

$$(x, y) = \left(x_0 + t \cdot \frac{b}{d} \ , \ y_0 - t \cdot \frac{a}{d} \right) \qquad t \in \mathbb{Z},\ d = \text{ggd}(a, b).$$

Voorbeeld

Bepaal de oplossing(en) $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ van de vergelijking $1734x + 221y = 340$.

We weten dat elke lineaire combinatie van 1734 en 221 een veelvoud is van de grootste gemene deler van 1734 en 221. Daarom bepalen we eerst deze grootste gemene deler (met het algoritme van Euclides). Na enig rekenwerk vinden we de grootste gemene deler (nl. 17), en de lineaire combinatie die gelijk is aan de grootste gemene deler:

$$1734(6) + 221(-47) = 17$$

Omdat het rechterlid van de opgave niet 17 is maar 340, moeten we uiteraard nog beide leden vermenigvuldigen in de gelijkheid hier net boven.

$$1734(6 \cdot 20) + 221(-47 \cdot 20) = 17 \cdot 20$$

Daaruit halen we al één oplossing van de gegeven vergelijking: $(x_0, y_0) = (120, -940)$. De algemene oplossing wordt gegeven door

$$(x, y) = (120 + 13t, -940 - 102t), \qquad t \in \mathbb{Z}$$

3.5 Chinese reststelling

Deze formuleert een oplossing van 2 of meer lineraire congruenties $x \overset{m_i}{=} a_i$

De Chinese reststelling combineert het oplossen van aparte lineaire congruenties tot het oplossen van een stelsel lineaire congruenties. Dat wil zeggen dat alle oplossingen worden gezocht die tegelijkertijd aan 2 of meer lineaire congruenties voldoen. Deze methode werd ontdekt door de Chinese wiskundige Sun Zi, die leefde in de periode tussen 200 voor en 200 na Christus.

Stelling 3.11. Chinese reststelling *Als $m_1, \ldots, m_n$ onderling priem zijn (en groter dan 1), en $a_1, \ldots, a_n \in \mathbb{Z}$, dan is er unieke oplossing $x \in \{0, 1, 2, \ldots, M-1\}$ voor het stelsel lineaire congruenties*

$$\begin{cases} x & \overset{m_1}{=} a_1 \\ x & \overset{m_2}{=} a_2 \\ & \cdots \\ x & \overset{m_n}{=} a_n \end{cases} \qquad (*)$$

Als x en x' beide oplossingen zijn, is $x = x'$ mod M, met $M = m_1 \cdot m_2 \cdots m_n$.

Bewijs
Het bewijs verloopt in twee stappen. In de eerste stap construeren we een oplossing $x \in \{0, 1, 2, \ldots, M-1\}$ voor het stelsel (*). Daarmee is het bestaan van zo'n oplossing aangetoond. In de tweede stap tonen we aan dat deze oplossing uniek is mod M.

- We geven de constructie van een oplossing $x \in \{0, 1, 2, \ldots, M-1\}$.

  We stellen $M_i = \dfrac{M}{m_i}$.

  Aangezien $m_1, m_2, \ldots, m_n$ onderling ondeelbaar zijn, geldt steeds : $\text{ggd}(m_i, M_i) = 1$.

  Uit stelling 2.8 volgt dan dat er een geheel getal y_i bestaat waarvoor $M_i \cdot y_i \overset{m_i}{=} 1$.

  Beschouw nu het gehele getal:

$$x = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \cdots + a_n \cdot M_n \cdot y_n \qquad (**)$$

  Het getal x voldoet aan alle vergelijking in (*). Immers, bij deling van het rechterlid van (**) door m_i bekomen we voor elke term rest 0 ($m_i \mid M_j$ als $i \neq j$), behalve voor de term $a_i \cdot M_i \cdot y_i$. Dus is

$$x \overset{m_i}{=} a_i \cdot M_i \cdot y_i \overset{m_i}{=} a_i \cdot 1 \overset{m_i}{=} a_i$$

  Dit betekent dat x een oplossing is elke vergelijking in (*).

  En dus is x mod M een oplossing van het stelsel (*) die voldoet aan $x \in \{0, 1, 2, \ldots, M-1\}$

- Stel nu dat twee verschillende gehele getallen x_1 en x_2 allebei voldoen aan de vergelijkingen van het stelsel (*), m.a.w.

$$\begin{cases} x_1 \overset{m_1}{=} a_1 \\ x_1 \overset{m_2}{=} a_2 \\ \quad \cdots \\ x_1 \overset{m_n}{=} a_n \end{cases} \qquad \text{en} \qquad \begin{cases} x_2 \overset{m_1}{=} a_1 \\ x_2 \overset{m_2}{=} a_2 \\ \quad \cdots \\ x_2 \overset{m_n}{=} a_n \end{cases}$$

  Wat kunnen we daaruit besluiten omtrent het gehele getal $y = x_1 - x_2$? We vinden dat

$$\begin{cases} y \overset{m_1}{=} 0 \\ y \overset{m_2}{=} 0 \\ \quad \cdots \\ y \overset{m_n}{=} 0 \end{cases}$$

  Dit betekent dat y een veelvoud is van m_1 en van $m_2, \cdots$ en van m_n. Omdat m_i onderling ondeelbaar zijn is y ook een veelvoud van $M = m_1 \cdot m_2 \cdots m_n$.

  De twee verschillende oplossingen x_1 en x_2 zullen dus steeds een veelvoud van M van elkaar verschillen, het stelsel (*) heeft dus een unieke oplossing modulo M.

Voorbeeld

Als voorbeeld bekijken we het oorspronkelijk probleem van de Chinese wiskundige Sun Zi (of Sun Tsu):

$$\begin{cases} x \overset{3}{=} 2 \\ x \overset{5}{=} 3 \\ x \overset{7}{=} 2 \end{cases}$$

$M = 3 \cdot 5 \cdot 7 = 105$, dus $M_1 = 5 \cdot 7$, $M_2 = 3 \cdot 7$, $M_3 = 3 \cdot 5$

De geconstrueerde oplossing is:

$$x \overset{105}{=} 2 \cdot 5 \cdot 7 \cdot y_1 + 3 \cdot 3 \cdot 7 \cdot y_2 + 2 \cdot 3 \cdot 5 \cdot y_3$$

Daarbij is $M_i \cdot y_i \overset{m_i}{=} 1$. Dit geeft drie onafhankelijke congruenties:

$$\begin{cases} 35 \cdot y_1 & \overset{3}{=} & 1 \\ 21 \cdot y_2 & \overset{5}{=} & 1 \\ 15 \cdot y_3 & \overset{7}{=} & 1 \end{cases}$$

Met het uitgebreid algoritme van Euclides vinden we:

$$\begin{cases} 1 & = & -1 \cdot 35 + 12 \cdot 3 \\ 1 & = & 1 \cdot 21 + (-4) \cdot 5 \\ 1 & = & -2 \cdot 7 + 1 \cdot 15 \end{cases} \quad \text{of dus} \quad \begin{cases} 1 & \overset{3}{=} & 2 \cdot 35 \\ 1 & \overset{5}{=} & 1 \cdot 21 \\ 1 & \overset{7}{=} & 1 \cdot 15 \end{cases}$$

Vermenigvuldigen met de inverse mod m_i geeft:

$$\begin{cases} y_1 & \overset{3}{=} & 2 \\ y_2 & \overset{5}{=} & 1 \\ y_3 & \overset{7}{=} & 1 \end{cases}$$

En dus:

$$x \overset{105}{=} 2 \cdot 5 \cdot 7 \cdot 2 + 3 \cdot 3 \cdot 7 \cdot 1 + 2 \cdot 3 \cdot 5 \cdot 1 \overset{105}{=} 233 \overset{105}{=} 23$$

De unieke oplossing in $\{0, 1, \ldots, 104\}$ is $x = 23$. Controleer dat dit getal voldoet aan het stelsel.

Opmerking: Als de voorwaarde $m_1, \ldots, m_n$ onderling priem niet voldaan is, dan moeten de congruenties eerst gereduceerd worden naar een vorm waarbij alle m_i onderling priem zijn. Hieronder twee voorbeelden.

Voorbeeld

Gegeven is het volgende stelsel van lineaire congruenties:

$$\begin{cases} x & \overset{3}{=} & 2 \\ x & \overset{6}{=} & 5 \end{cases}$$

Omdat $\text{ggd}(3, 6) = 3$ zijn m_1 en m_2 niet onderling priem.
Omdat $6 = 2 \cdot 3$, valt de laatste vergelijking uiteen in twee vergelijkingen $x \overset{2}{=} 5$ en $x \overset{3}{=} 5$. Het equivalent stelsel is dus:

$$\begin{cases} x & \overset{3}{=} & 2 \\ x & \overset{2}{=} & 5 \\ x & \overset{3}{=} & 5 \end{cases}$$

In dit stelsel zijn de eerste en laatste vergelijking equivalent, want 5 mod 3 = 2 mod 3. We mogen de derde vergelijking dus weglaten:

$$\begin{cases} x & \overset{3}{=} & 2 \\ x & \overset{2}{=} & 1 \end{cases}$$

Hier is de voorwaarde dat 3 en 2 wel onderling priem zijn wel voldaan, en vinden we een unieke oplossing $x = 5 \in \{0, 1, 2, 3, 4, 5\}$.

Voorbeeld

Gegeven is het volgende stelsel van lineaire congruenties:

$$\begin{cases} x & \overset{3}{=} & 2 \\ 3x & \overset{9}{=} & 12 \end{cases}$$

We zien opnieuw dat $m_1 = 3$ en $m_2 = 9$ niet onderling priem zijn, dus het stelsel moet eerst gereduceerd worden. Daarnaast is de coëfficiënt van x in de tweede vergelijking niet gelijk aan 1. Het valt op dat we deze coëfficiënt 1 kunnen maken door alle getallen te delen door 3, want $\text{ggd}(3, 9) = 3 \mid 12$. Het stelsel wordt aldus:

$$\begin{cases} x & \overset{3}{=} & 2 \\ x & \overset{3}{=} & 4 \end{cases}$$

Of nog:

$$\begin{cases} x & \overset{3}{=} & 2 \\ x & \overset{3}{=} & 1 \end{cases}$$

In dit geval spreken de vergelijkingen elkaar tegen. Er zijn m.a.w. geen oplossingen te vinden voor dit stelsel. Het stelsel is strijdig.

3.6 Residugetalsystemen: rekenen met grote getallen

Er doen zich twee problemen voor bij het rekenen met grote getallen. Enerzijds hebben we een fysische grens (`MAXINT`) die grote berekeningen in de weg staat. Anderzijds krijgen we bij bvb. optellen van zeer grote getallen tijdverlies omwille van 'overdracht' van cijfers / bits: eerst dienen de bits op de minst beduidende plaats opgeteld te worden, vóór de bits op de plaats er net links van opgeteld kunnen worden. Ze wachten namelijk op de overdracht van de bewerking die 'rechts van hen' gebeurde. Met de Chinese reststelling kunnen we beide problemen omzeilen.

3.6.1 Principe van residugetalsystemen

Stel dat $m_1, m_2, \ldots, m_n \in \mathbb{N}_0$ onderling ondeelbaar zijn, waarbij het product M van deze getallen een heel groot getal is. Dan volgt uit de Chinese reststelling dat elk natuurlijk getal

x kleiner dan M op unieke wijze voorgesteld kan worden a.d.h.v. n getallen die de rest van x bij deling door m_i voorstellen : ($x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_n$). Een dergelijke techniek waarbij elk getal a.d.h.v. resten t.o.v. verschillende grondtallen wordt voorgesteld, wordt een **residutalstelsel** genoemd.

Dit betekent dat als we van een getal $\in \{0, 1, \ldots, M-1\}$ de moduli kennen genomen ten opzichte van $m_1, m_2, \ldots, m_n$ (met $\prod m_i = M$ en m_i onderling ondeelbaar), dan kennen we het getal zelf.

Voorbeeld

Aan de hand van de getallen 99, 98, 97 en 95 kan men alle gehele getallen x waarvoor $0 \leq x < 89403930$ op unieke wijze voorstellen. Het getal 123684 wordt bijvoorbeeld voorgesteld als (33,8,9,89). Ga na dat $x = 123684$ voldoet aan:

$$\begin{cases} x \overset{99}{=} 33 \\ x \overset{98}{=} 8 \\ x \overset{97}{=} 9 \\ x \overset{95}{=} 89 \end{cases}$$

3.6.2 Voor- en nadelen t.o.v. enkelvoudige talstelsels

Berekenen via een residutalstelsel bieden belangrijke voordelen :

- Sommige veelvoorkomende bewerkingen (zoals optellingen en vermenigvuldigingen) kunnen eenvoudig en snel worden uitgevoerd via modulorekening.
- De berekeningen voor de verschillende grondtallen m_i kunnen volledig in parallel gebeuren (geen overdracht van een cijfer naar het hogere niveau zoals bij enkelvoudige talstelsels). Dit laat toe om de parallelle rekencapaciteiten van computerprocessoren ten volle uit te buiten.

Daarnaast kennen berekeningen via residutalstelsels ook heel wat inherente nadelen :

- Enkel gehele getallen kunnen via residutalstelsels worden voorgesteld.
- Sommige bewerkingen zoals delingen zijn veel complexer bij residutalstelsels.

Residutalstelsels worden dan ook voornamelijk aangewend bij zeer specifieke toepassingen : zware, tijdgevoelige (real-time) berekeningen met grote gehele getallen.

Voorbeeld

Bereken $z = x + y = 12345 + 23456$ op een computer die maximaal getalwaarde 100 kan voorstellen.
Kan je ook $u = x \times y = 12345 \cdot 23456$ berekenen in hetzelfde residutalstelsel?

We maken eerst een ruwe schatting voor de uitkomst, zodat we weten in welke verzameling $\mathbb{Z}_m$ deze uitkomst nog kan geschreven worden — zonder 'overflow' te genereren. Gezien $10.000 + 30.000 = 40.000$, moet $m \approx 40.000$. We zoeken een aantal grote getallen, kleiner dan 100, die onderling ondeelbaar zijn en zo dat hun product ongeveer gelijk is aan 40.000. De getallen $m_1 = 99$ en $m_2 = 98$ voldoen samen niet, nemen we er $m_3 = 97$ bij, dan voldoet de verzameling $\{m_1, m_2, m_3\}$ wel.
De getallen m_i zijn onderling priem en $M = 99 \cdot 98 \cdot 97 = 941094$ is voldoende groot.

We berekenen:

$$\begin{cases} 12345 &= 69 \bmod 99 \\ 12345 &= 95 \bmod 98 \\ 12345 &= 26 \bmod 97 \end{cases} \quad \text{en} \quad \begin{cases} 23456 &= 92 \bmod 99 \\ 23456 &= 34 \bmod 98 \\ 23456 &= 79 \bmod 97 \end{cases}$$

Daaruit volgt $x = (69, 95, 26)$ en $y = (92, 34, 79)$ en dus $z = x + y = (62, 31, 8)$.
Het product $u = x * y$ kan niet berekend worden in dit residugetalsysteem. Een ruwe schatting voor $x * y$ is $10000 \cdot 25000 = 25000000$ en dit is groter is dan M!!

Bij deze berekening hebben we geen grote getallen nodig gehad.

Ter controle berekenen we nu de getalwaarde van z met de Chinese reststelling:

$$\begin{cases} z &= 62 \bmod 99 \\ z &= 31 \bmod 98 \\ z &= 8 \bmod 97 \end{cases}$$

De geconstrueerde oplossing (uit de Chinese reststelling) is

$$z = 62 \cdot 98 \cdot 97 \cdot y_1 + 31 \cdot 99 \cdot 97 \cdot y_2 + 8 \cdot 99 \cdot 98 \cdot y_3$$

Daarbij is $M_i \cdot y_i \overset{m_i}{=} 1$. Dit geeft drie onafhankelijke congruenties:

$$\begin{cases} 98 \cdot 97 \cdot y_1 &\overset{99}{=} 1 \\ 99 \cdot 97 \cdot y_2 &\overset{98}{=} 1 \\ 99 \cdot 98 \cdot y_3 &\overset{97}{=} 1 \end{cases}$$

Omdat we zoveel mogelijk rekenwerk (lees: grote getallen) willen vermijden, doen we eerst een vereenvoudiging:

$$\Leftrightarrow \begin{cases} (99-1)(99-2) & y_1 &= 1 \bmod 99 \\ (98+1)(98-1) & y_2 &= 1 \bmod 98 \\ (97+2)(97+1) & y_3 &= 1 \bmod 97 \end{cases}$$

$$\Leftrightarrow \begin{cases} (-1)(-2) & y_1 &= 1 \bmod 99 \\ (1)(-1) & y_2 &= 1 \bmod 98 \\ (2)(1) & y_3 &= 1 \bmod 97 \end{cases}$$

$$\Leftrightarrow \begin{cases} 2 & y_1 &= 1 \bmod 99 \\ 1 & y_2 &= -1 \bmod 98 \\ 2 & y_3 &= 1 \bmod 97 \end{cases}$$

Met het uitgebreid algoritme van Euclides (voor de eerste en de derde vergelijking) vinden we:

$$\begin{cases} 1 &= 1 \cdot 99 + (-49) \cdot 2 \\ 1 &= 1 \cdot 97 + (-48) \cdot 2 \end{cases} \quad \text{of dus} \quad \begin{cases} 1 \overset{99}{=} 2 \cdot (99 - 49) &= 2 \cdot 50 \\ 1 \overset{97}{=} 2 \cdot (97 - 48) &= 2 \cdot 49 \end{cases}$$

Vermenigvuldigen met de inverse mod m_i geeft:

$$\begin{cases} y_1 \overset{99}{=} 50 \\ y_2 \overset{98}{=} -1 \\ y_3 \overset{97}{=} 49 \end{cases}$$

En dus:

$$z = 62 \cdot 98 \cdot 97 \cdot 50 + 31 \cdot 99 \cdot 97 \cdot (-1) + 8 \cdot 99 \cdot 98 \cdot 49 = 35801 \bmod M$$

Dit komt overeen met de verwachte waarde: $12345 + 23456 = 35801$.

Bij het terugrekenen van de getalwaarde hebben we dus wel grotere getallen nodig!

Zoals reeds aangegeven, omzeilen we met het rekenen in een residugetalsysteem twee belangrijke nadelen van het gewone (binair geprogrammeerde) optellen in $\mathbb{Z}$ (of $\mathbb{Z}_m$, met m de maximale getalwaarde die voorgesteld kan worden).

Enerzijds moet er niet gewacht worden op de overdracht van de minderbeduidende digit naar de volgende; anderzijds is elke m_i beduidend kleiner dan m, zodat berekeningen in $\mathbb{Z}_{m_i}$ eenvoudiger zullen zijn dan in $\mathbb{Z}_m$. Dit is het principe waarop de werking van de residucomputer gebaseerd is, een speciaal type van highspeed computer, met belangrijke toepassingen in onder andere beeld- en signaalverwerking.

3.7 Toepassing: cryptologie

Cryptologie (Eng. cryptology) is de studie van geheime berichten. Hierbij wordt een gegeven bericht bij de afzender versleuteld tot een onleesbaar bericht (encryptie), dit onleesbaar bericht wordt verzonden naar de bestemmeling en daar wordt de inverse versleuteling uitgevoerd om uit het onleesbare bericht terug het oorspronkelijke bericht af te leiden (decryptie). Op die manier kan een – al dan niet kwaadwillige - persoon die de boodschap onderschept het bericht niet lezen. Cryptologie kent belangrijke toepassingen bij hedendaagse communicatienetwerken en meer bepaald bij het realiseren van veiligheid en privacy voor de gebruikers van deze netwerken.

3.7.1 Caesar's encryptie - private sleutel

Een van de eenvoudigste en ook oudste manieren om een tekst te encrypteren, is Caesar's encryptie . Hierbij wordt elke letter van het alfabet cyclisch k letters verschoven in het alfabet

(de laatste k letters van het alfabet worden verschoven naar de eerste k letters). Wiskundig gezien kan men deze encryptie als volgt beschrijven :

- Elke letter van het bericht wordt omgezet in het corresponderende natuurlijk getal : A wordt 0, B wordt 1, $\cdots$, Z wordt 25.
- Bij elk van de aldus bekomen getallen wordt k bijgeteld en daarna de rest bij deling door 26 genomen :
$$f(n) = (n + k) \bmod 26$$
- Het aldus bekomen getal wordt terug omgezet in de corresponderende letter.

Voorbeeld

> Met $k = 3$, dan wordt het bericht "julius caesar" omgezet in "mxolxv fdhvdu", wat volslagen onleesbaar is voor een derde persoon, maar voor de bestemmeling net dezelfde informatie bevat als het oorspronkelijke bericht (op voorwaarde dat de bestemmeling weet welke encryptiemethode werd gebruikt en welke k werd gehanteerd bij de encryptie).

Het getal k wordt de sleutel (Eng. key) van de encryptiemethode genoemd. Het spreekt voor zich dat deze sleutel niet door derden mag gekend zijn, anders kunnen de geëncrypteerde berichten gemakkelijk ontcijferd worden. Men spreekt in dit geval van **private sleutel cryptologie** (Eng. private key cryptology) : de kennis van de sleutel mag niet in handen van derden vallen, anders kan die het bericht ontcijferen.

Het grote voordeel van Caesar's encryptiemethode is zijn eenvoud. Een belangrijk nadeel is echter dat het geheimschrift gemakkelijk te ontcijferen valt. Bijvoorbeeld via de frequentie van de voorkomende symbolen (de letter 'e' komt het meest voor in een normale Nederlandse tekst), kan gemakkelijk de sleutel k teruggevonden. Eens deze sleutel gekend is, is het decrypteren kinderspel.

3.7.2 RSA encryptie - publieke sleutel

De filosofie van publieke sleutel cryptologie is geniaal en verrassend eenvoudig : men ontwerpt een methode waarbij de sleutel toelaat om berichten te encrypteren maar niet te decrypteren! Deze sleutel wordt gekozen door de bestemmeling, die de sleutel via het netwerk doorstuurt naar de afzender. De afzender maakt dan gebruik van deze sleutel om het bericht te encrypteren. Derden mogen gerust de sleutel opvangen, ze kunnen er niets mee aanvangen om het onderschepte bericht te ontcijferen. Daarmee is de Achillespees van private sleutel cryptologie – het afluisteren van de sleutelinformatie – vermeden: de sleutel mag hier gerust publiek verspreid raken, vandaar de naam. Hoe het geheimschrift ontcijferd moet worden, blijft de gepriviligeerde kennis van de bestemmeling, deze informatie dient niet over het netwerk verstuurd te worden en kan dus niet onderschept worden.

Vraag blijft natuurlijk: hoe ontwerp je zo'n methode die mits een sleutel eenvoudige encryptie toelaat, maar waarvan de decryptiemethode niet kan achterhaald worden? In 1976 ontdekten onderzoekers van M.I.T. de RSA-encryptiemethode. Deze techniek werkt als volgt.

Het oorspronkelijke bericht stellen we voor d.m.v. een geheel getal M, het geëncrypteerde bericht d.m.v. een geheel getal C.

- De bestemmeling kiest 2 grote priemgetallen p en q, en een exponent e (waarbij $\text{ggd}(e, (p-1)\cdot(q-1)) = 1$)
- De bestemmeling berekent ook de inverse d van e: $d \cdot e \overset{(p-1)\cdot(q-1)}{=} 1$. Dit kan omdat $\text{ggd}(e, (p-1)\cdot(q-1)) = 1$.
- Nu berekent de bestemmeling $n = p \cdot q$ en stuurt de encryptiesleutel (n, e) naar de afzender.
- De afzender encrypteert de boodschap :

$$C = M^e \bmod n \qquad (*)$$

- Het geëncrypteerde bericht C wordt via het netwerk naar de bestemmeling gestuurd.
- Nu kan het bericht C gedecrypteerd worden:

$$M = C^d \bmod n \qquad (**)$$

(zonder bewijs, dit steunt op de zogenaamde 'kleine stelling van Fermat', zie vakliteratuur)

Essentieel bij de RSA-encryptiemethode is dat een derde niet genoeg heeft aan de sleutel (n, e) om de decryptie (**) uit te voeren. Decryptie kan enkel met de kennis van d en daarvoor heb je ook de priemgetallen p en q nodig (om $(p-1)\cdot(q-1)$) te kunnen berekenen). De enige manier om die te bekomen, is het ontbinden van het getal n in zijn twee priemfactoren $(n = p \cdot q)$. Het is vandaan de dag nog niet mogelijk om deze ontbinding in priemfactoren binnen een redelijke rekentijd uit te voeren indien n heel groot wordt (bv. een getal met 600-tal cijfers).

Merk op dat de bestemmeling moet zoeken naar 2 astronomisch grote priemgetallen p en q, bv. elk met 300-tal cijfers, dit kan binnen een doenbare rekentijd (via gespecialiseerde algoritmen).

Voorbeeld

We leggen het principe uit aan de hand van kleine priemgetallen.

Het bericht dat moet verstuurd worden beperken we tot één letter : 'Y'. Deze wordt omgezet naar zijn ascii-code 89.

- De bestemmeling kiest 2 de priemgetallen $p = 11$ en $q = 29$, en een exponent $e = 3$.
  Daarbij is $\text{ggd}(e, (p-1)\cdot(q-1)) = ggd(3, 280) = 1$.

- De bestemmeling berekent ook de inverse d van e: $d \cdot 3 \overset{280}{=} 1$
  Omdat $280-1 = 3 \cdot 93$ en dus $3 \cdot (-93) \overset{280}{=} 1$, vind je $d \overset{280}{=} -93 = 187 \bmod 280$
- Nu berekent de bestemmeling $n = p \cdot q = 319$ en stuurt de encryptiesleutel $(319, 3)$ naar de afzender.
- De afzender encrypteert $M = 89$:

$$C = M^e \bmod n = 89^3 \bmod 319 = 298$$

- Het geëncrypteerde bericht $C = 298$ wordt via het netwerk naar de bestemmeling gestuurd.
- Nu kan het bericht gedecrypteerd worden:

$$M = C^d \bmod n = 298^{187} \bmod 319 = 89$$

  En dit is de letter 'Y'

Naast de RSA-encryptiemethode bestaan ook andere publieke sleutel encryptiemethoden, die minder zware berekeningen vergen voor de bestemmeling. De RSA-methode wordt voornamelijk aangewend bij heel gevoelige toepassingen.

Hoofdstuk 4

Eindige velden

4.1 Constructie van eindige velden: intuïtie

Om vlot te kunnen rekenen in $\mathbb{Z}_n$, kunnen we rekenregels opstellen zoals in $\mathbb{Z}$. We weten dat de verzameling $\mathbb{Z}$ met de binaire operatoren $+$ en $\cdot$ een commutatieve ring met eenheidselement vormt, zie bijlage A. We kunnen nl. alle eigenschappen uit die bijlage één voor één controleren; ze vormen de rekenregels waaraan we ons in $\mathbb{Z}$ moeten houden (of beter: die logischerwijze volgen uit de fysische betekenis van optellen en vermenigvuldigen van gehele grootheden). Voor $\mathbb{Z}_n$ kunnen we hetzelfde doen: we definiëren een bewerking $+$ en een bewerking $\cdot$, en controleren dan of de eigenschappen van deze bewerkingen ook voldoen aan de voorwaarden voor een commutatieve ring met eenheidselement. Gezien we de bewerkingen in $\mathbb{Z}_n$ kunnen terugvoeren op bewerkingen in $\mathbb{Z}$, is dit eenvoudig aan te tonen (probeer dit zelf eens). We hebben echter méér: we kunnen aantonen dat – voor bepaalde n – de verzameling $\mathbb{Z}_n$ met bewerkingen $+, \cdot$ een veld is. Dit vereist de bijkomende eigenschap dat elk element (uitgezonderd 0) een invers heeft voor de vermenigvuldiging.

Stelling 4.1. *$\mathbb{Z}_n$ is een veld als en slechts als n priem is.*

Bewijs We weten al dat $\mathbb{Z}_n$ (met n willekeurig) een commutatieve ring met eenheidselement is. Rest er aan te tonen dat elke element een invers element heeft voor de vermenigvuldiging.

Gebruik stelling 3.8: indien $\text{ggd}(a, n) = 1$ ($a \in \mathbb{Z}_n$) dan bestaat er precies één getal $x \in \mathbb{Z}_n$ waarvoor geldt:

$$a \cdot x \overset{n}{=} x \cdot a \overset{n}{=} 1.$$

Elk element $a \in \mathbb{Z}_n$ heeft dus een invers element voor de vermenigvuldiging.

We moeten nog aantonen dat $\mathbb{Z}_n$ geen veld is als n geen priemgetal is. Dan heeft n een niet-triviale deler p die zelf een priemgetal is. We bewijzen dat p geen invers element heeft in $\mathbb{Z}_n$.
Veronderstel dat p wel een invers element x heeft, dan geldt:

$$p \cdot x = 1 + k \cdot n$$

Uit $p \mid n$ volgt dat $p \mid (k \cdot n - p \cdot x)$ dus $p \mid 1$. Dit is een contradictie.

□

Het is dus duidelijk dat $\mathbb{Z}_p$ met de bewerkingen $+$ en $\times$ en met p priem een veld vormt. We vinden dus een eindige verzameling met mooie eigenschappen voor optelling en vermenigvuldiging. Eindige verzamelingen interesseren ons, omdat software in se bestaat uit een eindige reeks nullen en enen. Stel dat we die reeksen opdelen in groepjes van 1 bit, dan werken we dus met 2 verschillende elementen, of met de verzameling $\mathbb{Z}_2$. Dit is echter amper bruikbaar. Groeperen we de bits in groepjes van 8 (of 16 of 25 of 32 of...) dan werken we dus met 2^8 (of 2^{16} of 2^{32} of...) verschillende elementen. Probleem: de gekende verzameling van 2^8 elementen is $\mathbb{Z}_{2^8}$, maar dat is geen veld. We gaan dus op zoek naar een veld van 2^8 elementen. Of nog: we zoeken een manier om optelling en vermenigvuldiging te definiëren op een verzameling van 2^8 verschillende elementen, zodat alle eigenschappen van een veld voldaan zijn. Uiteraard zullen we niet enkel zoeken naar dit specifieke veld, maar meteen naar het algemene geval: een veld van de orde p^k met p priem en $k > 1$.

Daarvoor keren we even terug naar hoofdstuk 1, waar we de uitbreiding zagen van $\mathbb{N}$ naar $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$. De uitbreiding naar $\mathbb{Q}$ en $\mathbb{R}$ levert ons niets dat navolging verdient: we willen vooral niet dat er tussen 2 bestaande elementen plots een oneindig aantal elementen toegevoegd wordt. Maar misschien levert de uitbreiding naar $\mathbb{C}$ ons iets op? Vertrek van de getallenas van $\mathbb{Z}$. De uitbreiding tot het complexe vlak zou dan een (oneindige) verzameling van rasterpunten $a + bi$ geven, met $a, b \in \mathbb{Z}$ en $i^2 = -1$. Merk op: de imaginaire eenheid i is een (in $\mathbb{Z}$ ongekend) element dat de oplossing is van de vierkantsvergelijking $x^2 + 1 = 0$ die in $\mathbb{Z}$ geen oplossingen heeft. Bovendien is $i \cdot i = -1 \in \mathbb{Z}$.
Merk echter op dat deze geconstrueerde verzameling oneindig is, en dus niet bruikbaar voor ons doel.

Vertrek nu van de eindige verzameling $\mathbb{Z}_5$, en voeg een imaginaire eenheid α toe. Het is belangrijk dat α nog niet tot $\mathbb{Z}_5$ behoort, maar $\alpha \cdot \alpha$ moet wel tot $\mathbb{Z}_5$ behoren. Indien α een oplossing is van een vierkantsvergelijking dan is $\alpha \cdot \alpha \in \mathbb{Z}_5$. In dit voorbeeld kiezen we voor α de oplossing van de vergelijking $x^2 = 2$. Controleer dat deze vergelijking geen oplossingen heeft in $\mathbb{Z}_5$ en $\alpha \cdot \alpha = 2 \in \mathbb{Z}_5$. De geconstrueerde verzameling $\{a + b\alpha \mid \alpha^2 = 2 \text{ en } a, b \in \mathbb{Z}_5\}$ bevat precies 25 punten.

Tweede voorbeeld: Vertrek van $\mathbb{Z}_2$ en construeer de verzameling van 4 elementen, nl. $\{0, 1, \alpha, \alpha + 1\}$ waarbij α een oplossing is van een vierkantsvergelijking die geen oplossing heeft in $\mathbb{Z}_2 = \{0, 1\}$. Controleer dat de vierkantsvergelijking $x^2 + x + 1 = 0$ geen oplossing heeft in $\mathbb{Z}_2$, en dus heeft de verzameling $\{0, 1, \alpha, \alpha + 1\}$ met $\alpha^2 + \alpha + 1 = 0$ exact 4 elementen. Merk op dat $\alpha^2 = -\alpha - 1 = \alpha + 1$ (coëfficiënten in $\mathbb{Z}_2$!).

Werk hieronder de optellings- en vermenigvuldigingstabel voor deze verzameling $\{0, 1, \alpha, \alpha+1\}$ uit.

$+$	0	1	α	$1+\alpha$
0				
1				
α				
$1+\alpha$				

$\times$	0	1	α	$1+\alpha$
0				
1				
α				
$1+\alpha$				

Als je deze optellings- en vermenigvuldigingstabellen vergelijkt met die van $\mathbb{Z}_4$ zou je moeten opvallen dat de nieuwe verzameling geen nuldelers meer heeft! (Je vindt geen getallen a, b verschillend van 0 waarvoor $a \times b = 0$.)

Kunnen we dit nu doortrekken? Kunnen we nu imaginaire éénheden blijven verzinnen, zodat we naast de reële en de imaginaire α-as nog een β-as kunnen toevoegen? Dan zou elk element bepaald worden door 3 getallen uit $\mathbb{Z}_p$, en hebben we $p \cdot p \cdot p = p^3$ elementen. De truc (zeg maar deus ex machina) bestaat er nu in om geen totaal nieuwe, onafhankelijke imaginaire éénheid β op te dissen, maar een getal α te zoeken dat oplossing is van een derdegraadsvergelijking die geen oplossingen heeft in $\mathbb{Z}_p$, en dan α en α^2 als twee (verschillende) imaginaire eenheden te nemen. Omdat α oplossing is van een derdegraadsvergelijking kan α^3 uitgedrukt worden als $a_0 + a_1\alpha + a_2\alpha^2$. De p^3 elementen uit onze nieuwe verzameling worden dan genoteerd als $a_0 + a_1\alpha + a_2\alpha^2$ met $a_i \in \mathbb{Z}_p$.

In de volgende sectie wordt een optelling en vermenigvuldiging verder gedefiniëerd en wordt aangetoond dat deze nieuwe verzameling een veld.

4.2 Afspraken en naamgevingen

Voor p een priemgetal en $k \in \mathbb{N}_0$ construeren we een veld met p^n elementen.

Voortbrengende veelterm De veelterm met $x^n + c_1x^{n-1} + c_2x^{n-2} + \ldots + c_n$ van graad n, die geen oplossing heeft in $\mathbb{Z}_p$ noemen we de **voortbrengende veelterm** en noteren we in wat volgt als $h(x)$.
Noteer met α een imaginaire oplossing van de voorbrengende veelterm $h(x)$.
Merk op dat de voortbrengende veelterm altijd een **monische veelterm** is. Dit is een veelterm in één variabele waarvan de leidende coëfficiënt gelijk is aan 1. Bijv. $x^5+3x^3+4x^2+2$ is een monische veelterm. Omdat $\mathbb{Z}_p$ een veld is (p is een priemgetal) kan je elke veelterm monisch maken, door te vermenigvuldigen met de inverse van de hoogstegraadscoëfficiënt.

Notatie van een element Elk element uit de verzameling van p^n elementen, noteren we aan de hand van een n-tuple $(a_0, a_1, \ldots, a_{n-1})$ met $a_i \in \mathbb{Z}_p$, of nog als $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$. De getallen a_i kunnen we ook de coördinaten van het getal noemen ten opzichte van de basis $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$.

Optelling Optellen gebeurt zoals in $\mathbb{C}$: overeenkomstige coördinaten worden opgeteld. Daarbij gelden de rekenregels van $\mathbb{Z}_p$, dus er wordt modulo p gerekend.

Vermenigvuldiging Hier gebruiken we bij voorkeur de veeltermnotatie. Stel $a = \sum_{i=0}^{n-1} a_i\alpha^i$ en $b = \sum_{i=0}^{n-1} b_i\alpha^i$. We volgen eerst de rekenregels van de formele machtreeksen:

$$\begin{aligned} ab &= (\textstyle\sum_{i=0}^{n-1} a_i\alpha^i)(\sum_{i=0}^{n-1} b_i\alpha^i) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)\alpha + (a_0b_2 + a_1b_1 + a_2b_0)\alpha^2 + \ldots + (a_{n-1}b_{n-1})\alpha^{2n-2} \end{aligned}$$

We stellen hier echter vast dat er machten van α te voorschijn komen, die niet voorkomen in de vooropgestelde vorm van een element uit onze verzameling. We willen immers dat de hoogst voorkomende exponent bij α gelijk is aan $n-1$. We weten echter dat α een wortel is van $h(x)$, een monische veelterm van graad n, dus $\alpha^n + c_1\alpha^{n-1} + c_2\alpha^{n-2} + \ldots + c_n = 0$. Dus vervangen we α^n door $-c_1\alpha^{n-1} - c_2\alpha^{n-2} - \ldots - c_n$, tot elke $\alpha^n, \alpha^{n+1}, \ldots$ vervangen werd door kleinere machten van α.

Notatie Bij de optelling en de vermenigvuldiging worden de coëfficiënten mod p verkleind, zodat ze altijd tot $\mathbb{Z}_p$ behoren. Bovendien wordt elke hogere macht van α vervangen door kleinere machten van α met behulp van de voortbrengende veelterm. Voortaan gebruiken we hiervoor de notatie $\equiv$ in plaats van $=$ of $\stackrel{p}{=}$.

Voorbeeld

In $\mathbb{Z}_2$ is α de imaginaire oplossing van $x^3 + x + 1 = 0$. Dan is:
$(\alpha^2 + 1)^2 \equiv a^4 + 2 \cdot a^2 + 1 \equiv \alpha \cdot (-\alpha - 1) + 1 \equiv \alpha^2 + \alpha$

Invers element Merk op, nu heb je optelling en vermenigvuldiging goed gedefinieerd, maar om aan te tonen dat deze bewerkingen samen met onze verzameling ook een *veld* uitmaken, is er nog een extra voorwaarde nodig: **elk element heeft een multiplicatief inverse** - zie bijlage A. Voor $\mathbb{Z}_p$ werd bewezen dat dit een veld is enkel indien p een priemgetal is, zie stelling 4.1. In deze verzameling met p^n elementen moeten we een gelijkaardige voorwaarde opleggen aan de voorbrengende veelterm $h(x)$: de veelterm moet '*priem*' zijn, of in termen van veeltermen gesproken: onontbindbaar. Soms wordt ook wel de term *irreducibel* gebruikt.

Naamgeving Nu wordt het ook dringend tijd om onze nieuwe verzameling een naam te geven. Zouden we – via een totaal andere constructie – een andere verzameling van p^n elementen gevonden hebben, met andere notaties en andere definities van $+$ en $\times$, dan zullen we een één-op-éénrelatie tussen de p^n elementen van beide verzamelingen kunnen vinden, waarbij bovendien de uitkomsten van de bewerkingen $+$ en $\times$ overeenkomen. Er bestaat dus in se maar één veld van de orde p^n. De theorie van de eindige velden werd ontwikkeld door Evariste Galois (1811-1832), vandaar de benaming voor een eindig veld van de orde p^n:

Definitie Het eindig veld van de orde p^n noteren we als $\mathbf{GF}(p^n)$, en noemen we **het Galoisveld** (Galois Field) van de orde p^n.

4.3 Rekenen in eindige velden

Vóór we het veld van p^n elementen verder bestuderen, moeten we gewoon worden aan rekenen met polynomen (eindige machtreeksen) over eindige verzamelingen (al dan niet een veld). Hiervoor verwijzen we naar de oefenlessen.

4.3.1 Ontbinden in factoren in het veld $\mathbb{Z}_p = \mathbf{GF}(p^1)$

De constructie van het veld $\mathbf{GF}(p^n)$, $n > 1$ is gebaseerd op een veelterm van graad n over $\mathbb{Z}_p$ die irreduciebel is. Hiervoor moeten we een veelterm kunnen ontbinden in factoren over $\mathbb{Z}_p$ (of op z'n minst kunnen aantonen dat een ontbinding niet mogelijk is).

Gegeven een veelterm/polynoom $f(x)$ van graad n over $\mathbb{Z}_p$. Om deze veelterm zo ver mogelijk te ontbinden in factoren, nemen we volgende stappen.

1. Eerst worden alle mogelijke lineaire factoren afgezonderd: $(x-a) \mid f(x) \Leftrightarrow f(a) = 0$. Omdat $\mathbb{Z}_p$ eindig is, kunnen we alle waarden voor a aflopen. Elke lineaire factor wordt uitgedeeld door middel van het algoritme van Horner (let vooral op meervoudige nulpunten!). De quotiëntveelterm die overblijft noemen we $f_1(x)$.[1]
2. Kan $f_1(x)$ nog verder ontbonden worden, dan zal elke factor in de ontbinding een veelterm van graad 2 of hoger zijn. We stellen een mogelijke ontbinding voorop (met voorlopig onbepaalde coëfficiënten), en passen de methode van gelijkstelling van coëfficiënten toe. Leidt het bekomen stelsel tot een tegenstrijdigheid, dan is $f_1(x)$ niet te ontbinden in factoren – of alleszins niet volgens de vooropgestelde verdeling.

Voorbeeld

Ontbind $f(x) = x^6 + x^3 + x + 1$ over $\mathbb{Z}_3$.

1. Eerst gaan we na of $f(x)$ lineaire factoren bevat. We rekenen uit: $f(0)$, $f(1)$ en $f(-1)$. (Merk op: machten van -1 zijn makkelijker te berekenen dan die van 2, dus gebruiken we $\{0, 1, -1\}$ als voorstelling voor $\mathbb{Z}_3$.) Gezien $f(0) \neq 0$, $f(1) \neq 0$ en $f(-1) = 0$ is -1 het enige mogelijke nulpunt. Met de methode van Horner gaan we na of dit nulpunt enkelvoudig is of niet.

	1	0	0	1	0	1	1
-1		-1	1	-1	0	0	-1
	1	-1	1	0	0	1	0
-1		-1	-1	0	0	0	
	1	1	0	0	0	1	

We zien dat $f(x) = (x+1)(x^5 - x^4 + x^3 + 1)$, maar dat de laatste factor (genaamd $f_1(x)$) geen nulpunten meer heeft. En dus ook geen lineaire factoren meer.

[1] Toen je de regel van Horner destijds aanleerde, werd je waarschijnlijk verteld om enkel de delers van de constante term te controleren. (Weet je nog welke redenering hier achter stak?) In $\mathbb{Z}_p$ echter is elk getal deler van elk ander getal, dus controle van *alle* getallen uit $\mathbb{Z}_p$ blijft nodig!

2. Daarom is de enige mogelijke opsplitsing van de graad van $f_1(x)$ gelijk aan $5 = 2 + 3$. We stellen een veelterm van de 2^e en een veelterm van de 3^e graad met nog onbepaalde coëfficiënten voorop:

$$(a_2x^2 + a_1x + a_0)(b_3x^3 + b_2x^2 + b_1x + b_0)$$

Omdat de coëfficiënt van x^5 gelijk is aan 1, mogen we $a_2 = b_3 = 1$ kiezen (de veeltermfactoren zijn op een constante na bepaald). We krijgen dus

$$\begin{aligned} h_1(x) &= x^5 - x^4 + x^3 + 1 \\ &= (x^2 + a_1x + a_0)(x^3 + b_2x^2 + b_1x + b_0) \\ \Leftrightarrow & \begin{cases} 1 = 1 & (5) \\ -1 = b_2 + a_1 & (4) \\ 1 = b_1 + a_1b_2 + a_0 & (3) \\ 0 = b_0 + a_1b_1 + a_0b_2 & (2) \\ 0 = a_1b_0 + a_0b_1 & (1) \\ 1 = a_0b_0 & (0) \end{cases} \end{aligned}$$

Uit (0) halen we twee mogelijkheden: ofwel is $a_0 = b_0 = -1$ ofwel is $a_0 = b_0 = 1$.

Eerste geval: $a_0 = b_0 = -1$.
Dan wordt het stelsel

$$\begin{cases} 1 = 1 \\ -1 = b_2 + a_1 \\ 1 = b_1 + a_1b_2 - 1 \\ 0 = -1 + a_1b_1 - b_2 \\ 0 = -a_1 - b_1 \\ 1 = a_0b_0 \end{cases}$$

De eerste en laatste gelijkheid zijn al voldaan. Werken we verder met de voorlaatste, dan onderscheiden we weer drie gevallen.

stel $a_1 = b_1 = 0$

$$\begin{cases} 1 = 1 \\ -1 = b_2 \\ 1 = -1 \\ \quad ... \end{cases}$$

stel $a_1 = 1 = -b_1$

$$\begin{cases} 1 = 1 \\ -1 = b_2 + 1 \\ 1 = -1 + b_2 - 1 \\ \quad ... \end{cases}$$

stel $a_1 = -1 = -b_1$

$$\begin{cases} 1 = 1 \\ -1 = b_2 - 1 \\ 1 = 1 - b_2 - 1 \\ 0 = -1 - 1 - b_2 \\ \quad ... \end{cases}$$

In elk van deze gevallen leidt $a_0 = b_0 = -1$ tot een tegenstrijdigheid.

Tweede geval: $a_0 = b_0 = 1$
Dan wordt het stelsel

$$\begin{cases} 1 = 1 \\ -1 = b_2 + a_1 \\ 1 = b_1 + a_1b_2 + 1 \\ 0 = 1 + a_1b_1 + b_2 \\ 0 = a_1 + b_1 \\ 1 = a_0b_0 \end{cases}$$

Uit de voorlaatste gelijkheid halen we volgende gevallen:

stel $a_1 = b_1 = 0$

$$\begin{cases} 1 &= 1 \\ -1 &= b_2 \\ 1 &= 1 \\ 0 &= 1 + b_2 \\ 0 &= 0 + 0 \\ 1 &= a_0 b_0 \end{cases}$$

$$\Leftrightarrow \begin{cases} a_0 &= 1 \\ a_1 &= 0 \\ b_0 &= 1 \\ b_1 &= 0 \\ b_2 &= -1 \end{cases}$$

$\Rightarrow$ ontbinding van $f_1(x)$ is $(x^2+1)(x^3-x^2+1)$

stel $a_1 = 1 = -b_1$

$$\begin{cases} 1 &= 1 \\ -1 &= b_2 + 1 \\ 1 &= -1 + b_2 + 1 \\ 0 &= 1 - 1 + b_2 \\ &... \end{cases}$$

strijdigheid

stel $a_1 = -1 = -b_1$

$$\begin{cases} 1 &= 1 \\ -1 &= b_2 - 1 \\ 1 &= 1 - b_2 + 1 \\ &... \end{cases}$$

strijdigheid

... en UITERAARD reken je de oplossing na: $f(x) \stackrel{?}{=} (x+1)(x^2+1)(x^3-x^2+1)$.

4.3.2 De Rabin test voor ondeelbaarheid

Zoals reeds eerder vermeld, steunt de structuur van en het rekenen binnen een eindig veld $\mathbf{GF}(p^n)$, $n > 1$ op een voortbrengende veelterm $h(x)$ van graad n die ondeelbaar (of: irreduciebel, irreduceerbaar) is. Hiervoor zagen we dat het niet kunnen ontbinden in factoren over $\mathbb{Z}_p$ van een dergelijke veelterm een nodige en voldoende voorwaarde is om te besluiten dat deze veelterm ondeelbaar is. Voor veeltermen van beperkte graad is het een haalbare kaart om dit (met de hand) uit te rekenen, zoals we in het voorbeeld hierboven hebben beschreven. Echter, voor veeltermen van een hogere graad wordt dit al gauw een heel complexe, uitgebreide en weinig gestructureerde berekening.

De Rabin test voor irreduceerbaarheid is een alternatieve en rigoureuze methode om te bepalen of een veelterm al dan niet ondeelbaar is. Ze steunt op volgende stelling (zonder bewijs).

Stelling 4.2. *Voor $f(x)$ een monische veelterm van graad n met coëfficienten in $\mathbb{Z}_p$. Noem $p_1, p_2, \ldots, p_k$ de unieke priemdelers van n, en noem $n_i = \frac{n}{p_i}$, met $1 \leq i \leq k$. De veelterm f is ondeelbaar in $\mathbb{Z}_p$ als en slechts als ggd $\left(f, x^{p^{n_i}} - x\right) = 1$, voor $1 \leq i \leq k$, en f deelt $x^{p^n} - x$.*

Stelling 4.2 kan ook in de vorm van een algoritme worden neergeschreven, zie Algoritme 1. De input van het algoritme is een monische veelterm f en de output is de binaire beslissing: deelbaar of ondeelbaar in $\mathbb{Z}_p$.

Input : Een monische veelterm f van graad n met coëfficiënten in $\mathbb{Z}_p$, alle priemdelers $p_1, p_2, \ldots, p_k$ van n
Output : "f is deelbaar" of "f is ondeelbaar"

for $i \leftarrow 1$ **to** k **do**
  $n_i \leftarrow \frac{n}{p_i}$
end
for $i \leftarrow 1$ **to** k **do**
  $g \leftarrow \text{ggd}\left(f, x^{p^{n_i}} - x\right)$
  if $g \neq 1$ **then**
    return "f is deelbaar"
  end
end
$g \leftarrow \text{ggd}\left(f, x^{p^n} - x\right)$
if $g == 0$ **then**
  return "f is ondeelbaar"
end
return "f is deelbaar"

Algoritme 1: De Rabin test voor ondeelbaarheid.

Volgend voorbeeldje illustreert de toepasbaarheid van het algoritme.

Voorbeeld

Beschouw de monische veelterm $f(x) = x^6 + x^3 + 1$ over $\mathbb{Z}_2$. Om aan te tonen dat h ondeelbaar is, passen we de Rabin test toe. Vermits $n = 6$ zijn er twee unieke priemdelers: $p_1 = 2$ en $p_2 = 3$. We bepalen hiermee vervolgens $n_1 = \frac{n}{p_1} = 3$ en $n_2 = \frac{n}{p_2} = 2$. We controleren nu achtereenvolgens de volgende voorwaarden om te kunnen besluiten dat f ondeelbaar is:

1. $\text{ggd}\left(f, x^{2^3} - x\right) \stackrel{?}{=} 1$

   Bemerk vooreerst dat $-x \equiv x$ in $\mathbb{Z}_2$. Herhaaldelijk toepassen van een Euclidische deling en het (uitgebreide) algoritme van Euclides leert ons achtereenvolgens dat (ga zelf na!):

   $\text{ggd}(x^6+x^3+1, x^8+x) = \text{ggd}(x^6+x^3+1, x^5+x^2+x) = \text{ggd}(x^2+1, x^5+x^2+x) = \text{ggd}(x^2+1, 1) = 1$

   Deze voorwaarde is dus vervuld.
2. $\text{ggd}\left(f, x^{2^2} - x\right) \stackrel{?}{=} 1$

   Via dezelfde procedure vinden we dat:

   $\text{ggd}(x^6 + x^3 + 1, x^4 + x) = \text{ggd}(1, x^4 + x) = 1$

   Ook deze voorwaarde is dus vervuld.
3. Is f een deler van $x^{2^6} - x$?

   Via een Euclidische deling vinden we dat:

$x^{64} + x = (x^6 + x^3 + 1) \cdot (x^{58} + x^{55} + x^{49} + x^{46} + x^{40} + x^{37} + x^{31} + x^{28} + x^{22} + x^{19} + x^{13} + x^{10} + x^4 + x)$

De veelterm f is dus duidelijk een deler van $x^{64} + x$, waarmee we besluiten dat ook de laatste voorwaarde vervuld is.

Vermits alle voorwaarden vervuld zijn, kunnen we besluiten dat f inderdaad ondeelbaar is in $\mathbb{Z}_2$.
Omdat $f(x) = 0$ ook geen oplossing heeft in $\mathbb{Z}_2$ kan $f(x) = x^6 + x^3 + 1$ gebruikt worden als voortbrengende veelterm bij de constructie van $\mathbf{GF}(2^6)$.

Voorbeeld

Is de veelterm $f(x) = 2x^4 + x + 2$ ondeelbaar over $\mathbb{Z}_3$? We gebruiken opnieuw de Rabin test. De veelterm is monisch en is van graad $n = 4$. Er is dus slechts één unieke priemdeler $p_1 = 2$, zodat $n_1 = \frac{n}{p_1} = 2$. We controleren nu opnieuw alle voorwaarden:

1. $\text{ggd}\left(f, x^{3^2} - x\right) \stackrel{?}{=} 1$

   Door herhaaldelijk toepassen van een Euclidische deling vinden we:

   $\text{ggd}(2x^4+x+2, x^9-x) = \text{ggd}(2x^4+x+2, x^3+x^2) = \text{ggd}(2x^2+x+2, x^3+x^2) = \text{ggd}(2x^2 + x + 2, x + 1) = \text{ggd}((x + 1) \cdot (2x + 2), x + 1) = x + 1$

   De grootste gemene deler is niet gelijk aan 1, en deze voorwaarde is dus niet vervuld.

We mogen dus meteen stoppen en concluderen dat f niet ondeelbaar is. Inderdaad, via ontbinden in factoren kan je vinden dat $f(x) = (x + 1) \cdot (2x^3 + x^2 + 2x + 2)$.

4.4 Notatie van de elementen van het eindig veld $\mathbf{GF}(p^n)$

Zoals vermeld is er slechts één veld van de orde p^n, voor gegeven priemgetal p en exponent n. Er zijn echter verschillende manieren om de p^n elementen van dit veld te noteren.

We zagen al dat de elementen genoteerd kunnen worden als veeltermen van maximale graad $n - 1$ met coëfficiënten in het veld $\mathbb{Z}_p$, waarbij de 'onbekende' α in de veelterm opgevat kan worden als een symbool (net zoals het symbool i in $\mathbb{C}$). (We gebruiken het symbool α en niet x, zodat x nog gebruikt kan worden om vergelijkingen over $\mathbb{Z}_p$ op te lossen.)

Hadden we ook andere keuzes kunnen maken? Zouden we de elementen van bijvoorbeeld $\mathbf{GF}(4)$ ook eenvoudiger kunnen benoemen? Uiteraard. We zouden de namen a_0, a_1, a_2 en a_3 kunnen kiezen. We komen dan echter op een ander punt in de problemen: zodra we bewerkingen in $\mathbf{GF}(4) = \{a_0, a_1, a_2, a_3\}$ willen uitvoeren $(+, \times)$, zullen we ons moeten beroepen op de definitie van $+$ en $\times$ in dit veld: we zullen de optellings- en vermenigvuldigingstabel moeten kennen. Elke berekening impliceert dan uiteraard opzoekingswerk in de tabellen: plaats- en tijdrovend.

We zouden ook kunnen kiezen voor de notatie $\mathbf{GF}(4) = \{0, 1, 2, 3\}$. Opnieuw moeten we ons dan beroepen op de optellings- en vermenigvuldigingstabellen om bewerkingen op te zoeken. Laten we α met 2 overeenkomen en $\alpha + 1$ met 3, dan komt er (zie ook de oefeningen):

$\mathbf{GF}(4), +$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Dit is echter tegennatuurlijk: de optelling van de symbolen 1 en 3 resulteert dan in het symbool 2. Dit heeft niets meer vandoen met de fysische optelling van 2 aantallen (zoals 2+3=5 staat voor "2 appels en dan nog eens 3 appels geeft samen 5 appels"). Het is echter perfect mógelijk, als we ons niet verliezen in het vreemde hergebruik van symbolen.

Een derde mogelijkheid: we zouden de symbolen $\{0, 1, 2, 3\}$ kunnen vervangen door hun binaire voorstelling $\{(00), (01), (10), (11)\}$. Dit klinkt nu nog uit de lucht gegrepen, maar zal op blz 49 van nut blijken én dichter bij reële toepassingen liggen dan de notatie $\{0, 1, 2, 3\}$.

Laat ons echter voorlopig bij de notatie $\mathbf{GF}(4) = \{0, 1, \alpha, 1 + \alpha\}$ blijven. Voordeel hiervan: optellen is zeer eenvoudig (overeenkomstige termen van de veeltermen in α optellen, en coëfficiënten in $\mathbb{Z}_p$ berekenen). Vermenigvuldigen gaat zoals bij gewone veeltermen, maar telkens er een term opduikt in α^n (of hoger), wordt α^n vervangen door $\alpha^n - h(\alpha)$, met $h(x)$ de onontbindbare veelterm die je uitkoos om de bewerkingen in $\mathbf{GF}(p^n)$ vast te leggen (zie ook oefeningeen). We hebben dus geen optellings- en vermenigvuldigingstabellen meer nodig (al is die soms wel handig als je berekeningen op papier maakt).

4.5 Toepassing in cryptografie

We hebben nu eindige velden geconstrueerd waarvan de kardinaliteit gelijk is aan een priemmacht. Kunnen we de typische veldeigenschap (nl. er bestaat altijd een multiplicatief invers) nu ook effectief gebruiken in informaticatoepassingen?

Stel dat we een bestand willen encrypteren. Dit hoeven we zelfs niet te onderstellen: zowat alle bitsgewijze informatie wordt geëncrypteerd. Is het niet om identiteit van zender / ontvanger en inhoud van de boodschap te beveiligen of om bestanden minder zwaar te maken, dan gebeurt het wel om extra controlemechanismen toe te voegen zodat storingen bij verzending opgevangen kunnen worden.

Elk encryptie-algoritme bestaat uit het omzetten van reeksen bits naar andere reeksen bits; telkens te interpreteren als gehele getallen. Deze omzettingen worden veelal gedefinieerd aan de hand van de bewerkingen $+$, $-$, $\times$, en... deling. Van zodra er een deling aan te pas komt, moeten we dus werken met bewerkingen in een veld. Anderzijds werken we best met gehele getallen die netjes passen binnen een gegeven aantal bits. Stel dat we data willen omzetten door telkens 8 bits tegelijk te bewerken. Met 8 bits kunnen we de getallen 0 tot en met 255 voorstellen. Maar $\mathbb{Z}_{256}$ is geen veld, dus deling is niet altijd mogelijk. Gebruiken we berekeningen in het veld $\mathbb{Z}_{251}$ (dichtste priemgetal), dan worden niet alle bitpatronen gebruikt, wat neerkomt op inefficiënt gebruik van geheugenruimte.

Maar zelfs als we een encryptie-algoritme opbouwen met enkel $+$, $-$, en $\times$ komen we met een verzameling die geen veld is in de problemen. Beschouw de vermenigvuldigingstabel van $\mathbb{Z}_8$ (blz 9). Daar zien we dat er meer kans zal zijn om een 4 tegen te komen in de uitkomst, dan een oneven getal. De vermenigvuldigingstabel van het veld $\mathbf{GF}(2^3)$ heeft dit onevenwicht niet, en is daarom geschikter voor codering van gegevens[2].

4.5.1 Coderen aan de hand van $\mathbf{GF}(2^n)$

Herneem de optellings- en vermenigvuldigingstabel van oefening 10 (zie blz **??**). We noteren de acht elementen van $\mathbf{GF}(2^3) = \mathbf{GF}(8)$ nu in de vorm van 3-bitswoorden. De coëfficiënt van α^2 staat vooraan. Vul bovenaan in elk kader de bitsgewijze representatie in; daaronder in potlood de decimale notatie (0-7).

- Wat merk je op voor de optelling? Welke operatie op bits heb je telkens doorgevoerd?
- Voor de vermenigvuldiging is een bitsgewijze operatie niet zo snel af te leiden. Laten we eerst nagaan wat een vermenigvuldiging met α (of bitpatroon (0 1 0)) betekent. Het element $a_2\alpha^2 + a_1\alpha + a_0$ (bitpatroon $(a_2\ a_1\ a_0)$) vermenigvuldigen met α levert $a_2\alpha^3 + a_1\alpha^2 + a_0\alpha$ op. De laatste 2 termen, $a_1\alpha^2 + a_0\alpha$, komen overeen met bitpatroon $(a_1\ a_0\ 0)$. Dit is de left shift over 1 bit toegepast op het oorspronkelijke patroon. De eerste term, $a_2\alpha^3$, vervangen we door $a_2(\alpha + 1)$ (want $h(x) = x^3 + x + 1$). Dit komt overeen met a_2 keer het bitpatroon (0 1 1). In woorden: een gegeven bitpatroon vermenigvuldigen met bitpatroon (0 1 0) komt neer op een left shift over 1 bit, met een voorwaardelijke bitsgewijze XOR operator met (0 1 1) (nl. enkel indien het eerste bit van het gegeven bitpatroon 1 is).

  Vermenigvuldiging met andere bitpatronen ((1 0 0), (1 1 0), (0 1 1), ...) wordt afgeleid uit de vermenigvuldiging met (0 1 0). Inderdaad:

$$\begin{array}{lll} (1\,0\,0) & \text{is gelijk aan} & (0\,1\,0) \times (0\,1\,0) \\ (1\,1\,0) & \text{is gelijk aan} & (1\,0\,0) + (0\,1\,0) \\ (0\,1\,1) & \text{is gelijk aan} & (0\,1\,0) + (0\,0\,1) \text{ enz.} \end{array}$$

Voorbeeld

Werk uit via bitoperaties; gebruik $h(x) = x^3 + x + 1$ als voorbrengende veelterm van $\mathbf{GF}(2^3)$.

$$(0\,1\,1) \times (1\,1\,0) = \ldots$$

We schrijven eerst alle resultaten uit van vermenigvuldiging met machten van x.

$$\begin{array}{lcl} (0\,1\,1) \times (0\,1\,0) & = & (1\,1\,0) \\ (0\,1\,1) \times (1\,0\,0) & = & (1\,1\,0) \times (0\,1\,0) \;=\; (1\,0\,0) + (0\,1\,1) \;=\; (1\,1\,1) \end{array}$$

Samenge(s)teld geeft dit:

$$\begin{array}{rcl} (0\,1\,1) \times (1\,1\,0) & = & (0\,1\,1) \times (1\,0\,0) \;+\; (0\,1\,1) \times (0\,1\,0) \\ & = & (1\,1\,0) + (1\,1\,1) \\ & = & (0\,0\,1) \end{array}$$

[2] Waarom is het beter om een evenwicht te hebben in symbolen?

Controle: $(x+1)(x^2+x) = x^3+x^2+x^2+x = x^3+x = x+1+x = 1$.

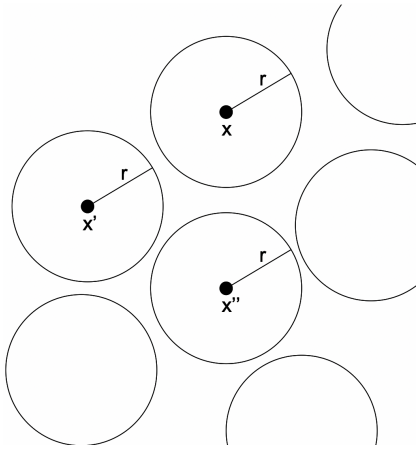
4.5.2 BCH-codes

Een $(n, M = 2^m, d)$-code is een binaire code, waarbij de codewoorden n bits lang zijn, en waarvan er $M = 2^m$ effectief gebruikt worden. Er zijn dus m "nuttige" bits en $n - m \geq 0$ controlebits. De grootheid d stelt de minimale Hammingafstand tussen twee verschillende codewoorden voor. De Hammingafstand is het minimaal aantal bits dat verschillend is tussen twee codewoorden, en dit voor alle mogelijke codewoorden.

Bij het versturen van een codewoord x zijn er verschillende mogelijkheden:

- Geval 1: er treedt geen fout op bij het versturen van het codewoord. Het ontvangen bericht is dus ook x en wordt door de ontvanger ook als x geïnterpreteerd.
- Geval 2: er treden minder dan $\frac{d}{2}$ fouten op bij het versturen van het codewoord. Het ontvangen bericht is nu geen codewoord (m.a.w. er wordt een fout 'gedetecteerd'), maar de onvanger van dit bericht kan het bericht wel 'corrigeren' tot het meest waarschijnlijke codewoord, nl. x.
- Geval 3: er treden minstens $\frac{d}{2}$ fouten op bij het versturen van het codewoord. Het ontvangen bericht is in de meeste gevallen geen codewoord (in die gevallen zal er dus een fout gedetecteerd worden). Het kan echter zijn dat het ontvangen codewoord nu dichter bij een ander codewoord x' ligt, en dan zal de ontvanger het bericht verkeerd corrigeren (naar x' i.p.v. x).

In vele praktische gevallen is de kans op het optreden van fouten in een bericht (door transmissie of opslag) relatief klein (bv. 1 foute bit per miljard verstuurde bits) en kunnen deze bitfouten als statistisch onafhankelijke gebeurtenissen aanzien worden (d.w.z. optreden van fout op een bepaalde bit heeft geen invloed op kans op fout in de daarop volgende bit). De onderstaande figuur illustreert het belang van de Hamming distance in dergelijke situaties. Op de figuur hieronder zijn 3 van de codewoorden afgebeeld: x, x' en x''. De afstanden tussen deze codewoorden onderling bedraagt dus minstens d. Men kan dus rond elk codewoord een cirkel met straal $r < \frac{d}{2}$ tekenen. Dit leidt tot disjuncte schijven.



Een BCH-code is nu zo een foutcorrigerende code uit de jaren '50 van de vorige eeuw, genoemd naar diens uitvinders: Bose, Chaudhuri en Hocquenghem. Hoe gaat het toepassen van zo'n BCH-code nu in zijn werk?

- Construeer een eindig veld $\mathbf{GF}(2^4)$, dus van orde 16. Als voortbrengende veelterm kan de irreduciebele veelterm $h(x) = x^4 + x + 1$ genomen worden.
- Neem nu een codewoord van 11 bits lang, dan hebben we in dit hoofdstuk gezien dat we dit codewoord kunnen voorstellen a.d.h.v. een veelterm $f(x)$ van graad 10 met coëfficiënten in $\mathbb{Z}_2$.
- Vermenigvuldigen we nu dit codewoord met onze voortbrengende veelterm $h(x)$, bekomen we een nieuwe veelterm $f(x) \cdot h(x)$ van graad 14 met coëfficiënten in $\mathbb{Z}_2$.

Voor dit voorbeeld kan men aantonen (maar dat is buiten het bestek van deze cursus) dat de vermeningvuldigingsoperatie $\cdot h(x)$ in $\mathbb{Z}_2$ precies overeenkomt met een encoderingsoperatie voor een binaire $(15, 2^{11}, 3)$-code.

Elke oorspronkelijke bitsequentie $f_{10}f_9f_8 \dots f_1f_0$ van 11 bits wordt dus omgezet naar een codewoord $a_{14}a_{13} \dots a_1a_0$ van 15 bits. De Hammingafstand bedraagt 3, m.a.w. deze code laat ons toe om enkelvoudige bitfouten te corrigeren, ofwel enkelvoudige en dubbele bitfouten te detecteren. De decoderingsoperatie zelf (incl. correctie) valt buiten het bestek van deze cursus.

Het speciale geval van een BCH-code met $n = q - 1$ wordt ook wel een Reed-Solomon-code genoemd. Deze wordt o.a. gebruikt bij de codering van informatie op CD's, DVD's, barcodes en bij *deep space* satellietcommunicatie.

Bijlage A

Groepen, ringen, velden

Een **groep** is een niet-ledige verzameling $\mathcal{G}$ van elementen waarop een binaire operator $\star$ is gedefinieerd, zó dat volgende eigenschappen gelden:

(1)	$\mathcal{G}$ is gesloten onder $\star$	$\forall a, b \in \mathcal{G} : a \star b \in \mathcal{G}$
(2)	$\star$ is associatief	$\forall a, b, c \in \mathcal{G} : (a \star b) \star c = a \star (b \star c)$
(4)	er is een uniek eenheidselement voor $\star$	$\exists e \in \mathcal{G} : \forall a \in \mathcal{G} : a \star e = a = e \star a$
(5)	elk element heeft een invers voor $\star$	$\forall a \in \mathcal{G} : \exists b \in \mathcal{G} : a \star b = e = b \star a$

Een groep wordt meestal genoteerd aan de hand van verzameling én operator, dus $< \mathcal{G}, \star >$ of $(\mathcal{G}, \star)$. Als de bewerking duidelijk blijkt uit de context, durft men de operator soms weg te laten uit de naamgeving.

Een **commutatieve groep** (of **Abelse groep**) is een groep $(\mathcal{G}, \star)$ waarvoor bovendien commutativiteit van de bewerking $\star$ geldt.

(3)	$\star$ is commutatief	$\forall a, b \in \mathcal{G} : a \star b = b \star a$

Een **eindige** (al dan niet Abelse) **groep** is een (Abelse) groep $(\mathcal{G}, \star)$ waarbij $\mathcal{G}$ eindig is. Het aantal elementen van $\mathcal{G}$ wordt de orde van de groep $(\mathcal{G}, \star)$ genoemd, en noteren we als $|\mathcal{G}|$ of $\sharp(\mathcal{G})$.

Een **ring** is een verzameling $\mathcal{R}$ van minimum twee elementen waarop twee binaire operatoren $\oplus$ en $\odot$ gedefinieerd zijn, zó dat volgende eigenschappen gelden:

(1)	$\mathcal{R}$ is gesloten onder $\oplus$	$\forall a, b \in \mathcal{R} : a \oplus b \in \mathcal{R}$
(2)	de bewerking $\oplus$ is associatief	$\forall a, b, c \in \mathcal{R} : (a \oplus b) \oplus c = a \oplus (b \oplus c)$
(3)	de bewerking $\oplus$ is commutatief	$\forall a, b \in \mathcal{R} : a \oplus b = b \oplus a$
(4)	er is een uniek eenheidselement voor $\oplus$ dit elt. wordt het additief eenheidselt. genoemd, doorgaans genoteerd met 0	$\exists e \in \mathcal{R} : \forall a \in \mathcal{R} : a \oplus e = a = e \oplus a$
(5)	elk element heeft een invers voor $\oplus$ dit elt. wordt het additief invers van a genoemd, doorgaans genoteerd als $-a$	$\forall a \in \mathcal{R} : \exists b \in \mathcal{R} : a \oplus b = e = b \oplus a$
(1')	$\mathcal{R}$ is gesloten onder $\odot$	$\forall a, b \in \mathcal{R} : a \odot b \in \mathcal{R}$
(2')	de bewerking $\odot$ is associatief	$\forall a, b, c \in \mathcal{R} : (a \odot b) \odot c = a \odot (b \odot c)$
(6')	de bewerking $\odot$ is distributief tov $\oplus$	$\forall a, b, c \in \mathcal{R} : a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$

Een **commutatieve ring** is een ring $(\mathcal{R}, \oplus, \odot)$ met bijkomende eigenschap

(3')	de bewerking $\odot$ is commutatief	$\forall a, b \in \mathcal{R} : a \odot b = b \odot a$

Een **ring met eenheidselement** is een ring $(\mathcal{R}, \oplus, \odot)$ met bijkomende eigenschap

(4')	er is een uniek eenheidselement voor $\odot$ dit elt. wordt het multiplicatief eenheidselt. genoemd, doorgaans genoteerd met 1	$\exists \mathbf{1} \in \mathcal{R} : \forall a \in \mathcal{R} : a \odot \mathbf{1} = a = \mathbf{1} \odot a$

Een **veld** is een commutatieve ring met eenheidselement met bijkomende eigenschap

(5')	elk element ($\neq 0$) heeft een invers voor $\odot$ dit elt. wordt het multiplicatief invers van a genoemd, doorgaans genoteerd als a^{-1}.	$\forall a \in \mathcal{G} : \exists b \in \mathcal{G} : a \odot b = e = b \odot a$

Een **eindig veld** is een veld waarvan de verzameling een eindig aantal elementen bezit.

Stelling A.1. *Er bestaat een veld van de orde q als en slechts als q een priemmacht is ($q = p^r$, p priem en $r \in \mathbb{N}$). Bovendien bestaat er slechts één veld van die orde (eventueel door herschikken van elementen te bekomen). Zulk eindig veld wordt dikwijls een* **Galoisveld** *genoemd, en noteren we met* $\mathbf{GF}(q)$ *of* $\mathbb{F}(q)$.

Voorbeeld De verzamelingen $\mathbb{Q}$, $\mathbb{R}$ en $\mathbb{C}$ (met bewerkingen) zijn oneindige velden; $\mathbb{Z}$ is een ring; en $\mathbf{GF}(5) = \{0, 1, 2, 3, 4\} = \mathbb{Z}_5$ is een eindig veld.