Hoofdstuk

4 Getaltheorie

4.1 Deelbaarheid en grootste gemene deler

Definitie 4.1

Deelbaarheid in $\mathbb{Z}$ is een relatie $\mathcal{D} \subset \mathbb{Z} \setminus \{0\} \times \mathbb{Z}$ gedefinieerd door

$$(a, b) \in \mathcal{D} \iff \exists q \in \mathbb{Z} : b = a \cdot q.$$

We noemen $\mathcal{D}$ ook de *deelbaarheidsrelatie* en we zeggen dat a *een deler is van* b of dat b *een* a*-voud* is, of b *is deelbaar door* a of nog dat a *een factor is van* b. Indien $(a, b) \in \mathcal{D}$, dan noteren we dit kort als $a \mid b$, terwijl $a \nmid b$ een verkorte notatie is voor $(a, b) \notin \mathcal{D}$.

Enkele eigenschappen liggen voor de hand. We formuleren ze in opeenvolgende lemma's.

Lemma 4.2

Voor $a, b, c, m, n \in \mathbb{Z}$ geldt

(i) $a \mid b$ en $a \mid c \implies a \mid (b + c)$.

(ii) $a \mid b \implies a \mid bc$.

(iii) $a \mid m$ en $b \mid n \implies ab \mid mn$.

Bewijs. (i) Uit de veronderstelling volgt dat er gehele getallen d, e bestaan waarvoor $a \cdot d = b$ en $a \cdot e = c$. Dus $a(d + e) = b + c$, dus $a \mid (b + c)$.

(ii) Uit $a \mid b$ volgt dat $a \cdot d = b$ voor een zekere $d \in \mathbb{Z}$. Dus $a \cdot d \cdot c = b \cdot c$, dus $a \mid bc$.

(iii) Analoog aan (ii). □

Gevolg 4.3

Veronderstel $a \mid b$ en $a \mid c$. Dan zal voor alle gehele getallen x en y gelden dat $a \mid (bx + cy)$

Lemma 4.4

De deelbaarheidsrelatie beperkt tot $\mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\}$ is reflexief en transitief.

Lemma 4.4 formuleert welgekende eigenschappen van deelbaarheid in $\mathbb{Z}$ en het bewijs laten we over als oefening. De deelbaarheidsrelatie $\mathcal{D}$ is niet antisymmetrisch, $(x, -x)$ en $(-x, x)$ zijn steeds twee koppels in $\mathcal{D}$ voor alle $x \neq 0$. Haar beperking tot $\mathbb{N} \setminus \{0\} \times \mathbb{N} \setminus \{0\}$ is dat echter wel.

Elk geheel getal $b \neq 0$ is uiteraard deelbaar door $1, -1, b$ en $-b$. We noemen deze soms de *onechte delers* van het getal. Al de andere delers worden de *echte delers* van het getal genoemd. Dus 1 is een deler is van elk geheel getal, en elk geheel getal verschillend van 0 is een deler van 0. Het getal b is *even* als $2 \mid b$ en *oneven* als $2 \nmid b$.

Voor twee gegeven gehele getallen a en $b \neq 0$, kunnen we steeds nagaan *hoeveel keer b in a past*. Indien dit een geheel aantal keer is, dan is $b \mid a$. Indien $b \nmid a$, dan zal deze deling een *rest* opleveren. De *staartdeling* of *Euclidische deling* om dit uit te voeren, is een welbekend algoritme. Beschouwen we bijvoorbeeld de getallen 126 en 35, dan vinden we dat $126 = 35 \cdot 3 + 21$. Uiteraard geldt ook dat $126 = 35 \cdot 4 - 14$. Bekijken we -126 en 35, dan zien we dat $-126 = -3 \cdot 35 - 21$, en ook $-126 = -4 \cdot 35 + 14$. Zo kunnen we ook nog 126 en -35 en -126 en -35 bekijken. Telkens zien we twee mogelijkheden, maar telkens zien we ook dat de *absolute waarde* van de rest kleiner is dan de absolute waarde van de deler.

Definitie 4.5

De *absolute waarde* van een geheel getal $a \in \mathbb{Z}$ is a zelf als $a \in \mathbb{N}$ en $-a$ als $a \in \mathbb{Z} \setminus \mathbb{N}$.

De absolute waarde van a wordt genoteerd als $|a|$. De volgende stelling verschaft duidelijkheid.

Stelling 4.6

Voor elke 2 getallen $a \in \mathbb{Z} \setminus \{0\}$ en $b \in \mathbb{Z}$ bestaan er unieke gehele getallen q (quotiënt) en r (rest) zodanig dat

$$b = a \cdot q + r \text{ en } 0 \leq r < |a|$$

Bewijs. (a) We tonen eerst aan dat er dergelijke getallen q en r bestaan. We passen het welordeningsprincipe toe op de volgende verzameling R:

$$R = \{x \in \mathbb{N} || b = a \cdot y + x \text{ voor een } y \in \mathbb{Z}\}.$$

We bewijzen eerst dat R niet ledig is. Als $b \geq 0$, dan volgt uit $b = a \cdot 0 + b$ dat $b \in R$. Als $b < 0$, dan geldt $b = |a| \cdot b + (1 - |a|) \cdot b$. Aangezien $(1 - |a|) \cdot b \geq 0$ zal $(1 - |a|) \cdot b \in R$. De verzameling R is dus niet ledig en bezit bijgevolg een kleinste element r. We hebben $b = a \cdot q + r$ voor een zekere $q \in \mathbb{Z}$. Als $0 < a \leq r$, dan hebben we eveneens dat $b = a \cdot (q + 1) + (r - a)$ met $r > r - a \geq 0$, in tegenstrijd met de definitie van r. Als $-r \leq a < 0$, dan hebben we eveneens dat $b = a \cdot (q - 1) + (r + a)$, met $r > r + a \geq 0$, in tegenstrijd met de definitie van r. Bijgevolg geldt $r \in \mathbb{N}_{<|a|}$.

(b) We tonen de uniciteit van q en r aan. Onderstel dat $b = a \cdot q_1 + r_1 = a \cdot q_2 + r_2$ voor zekere $q_1, q_2 \in \mathbb{Z}$ en zekere $r_1, r_2 \in \mathbb{N}_{<|a|}$. Als $q_1 \neq q_2$, dan mogen we zonder verlies van algemeenheid veronderstellen dat $a \cdot (q_1 - q_2) > 0$. Dan geldt $r_2 = a \cdot (q_1 - q_2) + r_1 \geq |a| + r_1 \geq |a|$, een tegenstrijdigheid. Bijgevolg geldt $q_1 = q_2$ en daaruit volgt dan ook dat $r_1 = r_2$. □

Opmerking

Een belangrijk gevolg van deze stelling is, dat voor elk gegeven natuurlijk getal $t \geq 2$, een willekeurig positief geheel getal geschreven kan worden als een lineaire combinatie van machten van t waarbij de coëfficiënten tot de verzameling $\mathbb{N}_{<t}$ behoren. Indien we immers de voorgaande stelling herhaalde

malen toepassen, dan verkrijgen we:

$$\begin{aligned} x &= tq_0 + r_0 \\ q_0 &= tq_1 + r_1 \\ \dots &\quad \dots \\ q_{n-2} &= tq_{n-1} + r_{n-1} \\ q_{n-1} &= tq_n + r_n. \end{aligned}$$

Hierbij zal elke rest r_i tot $\mathbb{N}_{<t}$ behoren en zal dit proces stoppen van zodra $q_n = 0$. Indien we nu de quotiënten q_i elimineren, dan verkrijgen we

$$x = r_n t^n + r_{n-1} t^{n-1} + \cdots + r_1 t + r_0.$$

We schrijven verkort $x = (r_n r_{n-1} \dots r_0)_t$ en we noemen dit de *ontwikkeling van x in basis t*. De meest gebruikte basissen zijn $t = 10$ (tiendelig getallenstelsel, $r_i \in \mathbb{N}_{<10}$) en $t = 2$ (binair getallenstelsel, $r_i \in \{0, 1\}$). Men kan bv. eenvoudig narekenen dat $(1992)_{10} = (11111001000)_2$.

Voor elke 2 gehele getallen a, b noemen we een geheel getal d dat zowel a als b deelt, een *gemene deler* van a en b.

Definitie 4.7

Stel $a, b \in \mathbb{Z}$ niet beide nul. Een gemene deler c van a en b is een *grootste gemene deler* van a en b als en slechts als elke gemene deler van a en b een deler is van c.

De terminologie *grootste* is dus niet gerelateerd aan de natuurlijke orderelatie op $\mathbb{Z}$, maar aan de pre-orderelatie $\mathcal{D}$. We bekijken een voorbeeld. Stel $a = 30$ en $b = 75$. De gemene delers van a en b zijn $\{-15, -5, -3, -1, 1, 3, 5, 15\}$. Elke gemene deler deelt -15 en 15. Dus -15 en 15 zijn twee verschillende grootste gemene delers van a en b. Men kan zich afvragen of er meer dan twee grootste gemene delers zijn in $\mathbb{Z}$. Het antwoord volgt uit het volgende lemma.

Lemma 4.8

Als a en b twee grootste gemene delers zijn van twee gehele getallen, dan geldt $a = b$ of $a = -b$.

Bewijs. Uit het feit dat a en b twee grootste gemene delers zijn, volgt $a \mid b$ en $b \mid a$. Er bestaan dus getallen $c, d \in \mathbb{Z}$ zodat $a \cdot c = b$ en $b \cdot d = a$. Dus $a \cdot c \cdot d = a$, dus er geldt noodzakelijk dat $c \cdot d = 1$. Met andere woorden, c en d zijn elkaars inverse in $\mathbb{Z}$, dus $c = d = 1$ of $c = d = -1$, waaruit het lemma volgt. □

Stelling 4.9

Stel $a, b \in \mathbb{Z}$ niet beide nul, dan bezitten a en b een grootste gemene deler in $\mathbb{Z}$.

Bewijs. Stel dat er getallen a en b, niet beide nul, in $\mathbb{Z}$ bestaan zonder een grootste gemene deler in $\mathbb{Z}$. Beschouw dan twee getallen $a, b \in \mathbb{Z}$, niet beide nul, zonder een grootste gemene deler in $\mathbb{Z}$, en met $\max(|a|, |b|)$ minimaal.

Voor het bewijs kunnen verschillende onderstellingen gemaakt worden over a en b.

Merk op dat $a, b \neq 0$ kan ondersteld worden, want als, bijvoorbeeld, $a = 0$, dan is b een grootste gemene deler van a en b. Analoog, merk op dat $|a| \neq |b|$ kan ondersteld worden, want als $|a| = |b|$, dan is a een grootste gemene deler van a en b. Analoog kan ook $a, b > 0$ ondersteld worden, want de gemene delers van a en b zijn gelijk aan de gemene delers van $-a$ en b.

Onderstel, zonder verlies aan algemeenheid, dat $b > a$.

Beschouw de verzameling G van de gemene delers van a en b. Deze verzameling G is zeker niet-ledig, daar $1 \in G$.

Deze verzameling G is ook de verzameling van de gemene delers van de getallen a en $b-a$, en dan hebben de twee getallen a en $b-a$ ook geen grootste gemene deler. Maar dit kan niet, want $\max(|a|, |b-a|) < \max(|a|, |b|)$, wat in tegenstrijd is met de specifieke keuze voor de getallen a en b.

Dit toont aan dat elke twee getallen a en b in $\mathbb{Z}$, niet beide nul, een grootste gemene deler hebben in $\mathbb{Z}$. □

De voorgaande twee stellingen verzekeren in $\mathbb{Z}$ dat er steeds twee grootste gemene delers zijn voor twee gehele getallen a en b, niet beide nul, een positieve en een negatieve. We maken de keuze om de positieve gemene deler te kiezen als *de* grootste gemene deler.

Definitie 4.10

Stel $a, b \in \mathbb{Z}$ niet beide nul. *De grootste gemene deler* van a en b is de unieke positieve onder de grootste gemene delers van a en b.

Vanaf nu slaat *de grootste gemene deler* dus steeds op de unieke positieve grootste gemene deler. We noteren de grootste gemene deler van a en b als $\text{ggd}(a, b)$.

Alhoewel de *Elementen* van Euclides hoofdzakelijk over meetkunde gaan, worden in Boeken 7, 8 en 9 aritmetische problemen beschreven. Propositie 2 in Boek 7 beschrijft een algoritme om de grootste gemene deler van 2 gehele getallen te berekenen. Dit algoritme is zeer efficiënt, en staat algemeen bekend als het **algoritme van Euclides**. Het algoritme steunt op het volgende lemma.

Lemma 4.11

Stel $a, b, q, r \in \mathbb{Z}$, met $a = bq + r$. Dan geldt $\text{ggd}(a, b) = \text{ggd}(b, r)$.

Bewijs. Stel $c = \text{ggd}(a, b)$. Dan is $c \mid a - bq = r$ door Gevolg 4.3. Dus c is een gemene deler van b en r, en bijgevolg geldt $\text{ggd}(a, b) \mid \text{ggd}(b, r)$. Stel $d = \text{ggd}(b, r)$. Dan is $d \mid bq + r = a$, opnieuw door Gevolg 4.3. Dus d is een gemene deler van a en b, en bijgevolg geldt $\text{ggd}(b, r) \mid \text{ggd}(a, b)$. Omdat beide positief zijn, besluiten we dat $\text{ggd}(a, b) = \text{ggd}(b, r)$. □

Voorbeeld 4.12. We passen het lemma toe om een grootste gemene deler van 126 en 35 te bepalen. Omdat $\text{ggd}(a, 0) = |a|$ voor alle $a \in \mathbb{Z} \setminus \{0\}$, kennen we een grootste gemene deler van zodra de deling opgaat.

$$\begin{aligned} 126 &= 3 \cdot 35 + 21 \\ 35 &= 1 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 \end{aligned}$$

Dus $\text{ggd}(126, 35) = 7$. De keuze van de quotiënten en resten bepaalt uiteraard niet het eindresultaat, maar wel de uitvoering van het algoritme:

$$\begin{aligned} 126 &= 4 \cdot 35 - 14 \\ 35 &= -3 \cdot (-14) - 7 \\ -14 &= -2 \cdot 7 \end{aligned}$$

Het is duidelijk dat de laatste niet-nul rest *een* grootste gemene deler is. Zijn absolute waarde is steeds de grootste gemene deler. Omdat we zeker weten dat de resten in absolute waarde steeds kleiner worden, zal dit algoritme eindigen. We noteren de unieke positieve rest (Stelling 4.6) bij deling van a door b als $\text{rem}(a, b)$.

Algoritme 4.1 Algoritme van Euclides

input: $a, b \in \mathbb{Z} \setminus \{0\}$.
output: de grootste gemene deler van a en b.
1 $r_0 \leftarrow a$, $r_1 \leftarrow b$
2 $i \leftarrow 1$
3 **while** $r_i \neq 0$
4 **do** $r_{i+1} \leftarrow \text{rem}(r_{i-1}, r_i)$
5 $i \leftarrow i + 1$
6 **return** r_{i-1}

Voorbeeld 4.12 toont aan dat de bekomen grootste gemene deler kan geschreven worden als een lineaire combinatie van de elementen 126 en 35:

$$7 = 21 - 1 \cdot 14 = 21 - (35 - 1 \cdot 21) = 2 \cdot (126 - 3 \cdot 35) - 35 = 2 \cdot 126 - 7 \cdot 35$$

Dit principe kunnen we onmiddellijk vertalen naar een aanpassing van het algoritme van Euclides. Voor $a, b \in \mathbb{Z}$ noteren we het uniek quotiënt horend bij $\text{rem}(a, b)$ als $\text{quo}(a, b)$. Er geldt dus steeds dat $a = \text{quo}(a, b)b + \text{rem}(a, b)$.

Algoritme 4.2 Uitgebreid algoritme van Euclides

input: $a, b \in \mathbb{Z} \setminus \{0\}$.
output: r, s, t, met $r = \gcd(a, b) = sa + tb$.
1 $r_0 \leftarrow a$, $s_0 \leftarrow 1$, $t_0 \leftarrow 0$.
2 $r_1 \leftarrow b$, $s_1 \leftarrow 0$, $t_1 \leftarrow 1$.
3 $i \leftarrow 1$.
4 **while** $r_i \neq 0$
5 **do** $q_i \leftarrow \text{quo}(r_{i-1}, r_i)$
6 $r_{i+1} \leftarrow (r_{i-1} - q_i r_i)$
7 $s_{i+1} \leftarrow (s_{i-1} - q_i s_i)$
8 $t_{i+1} \leftarrow (t_{i-1} - q_i t_i)$
9 $i \leftarrow i + 1$
10 $l \leftarrow i - 1$
11 **return** r_l, s_l, t_l

De volgende stelling toont de correctheid van het uitgebreid algoritme van Euclides aan.

Stelling 4.13

Veronderstel dat a en b gehele getallen zijn (niet beide nul), en dat $d = \text{ggd}(a, b)$, dan bepaalt Algoritme 4.2 gehele getallen m, n zodanig dat $am + bn = d$, tenzij $b \mid a$.

Bewijs. Als $b \mid a$, dan geeft het algoritme b terug. Indien $b < 0$, dan is $-b = \text{ggd}(a, b)$. Het is duidelijk dat $b \mid a \iff r_2 = 0$.

Noem $k > 2$ de kleinste natuurlijke k waarvoor $r_k = 0$. Dan is $r_{k-1} = \text{ggd}(a, b) =: d$. Dus kan de voorlaatste vergelijking herschreven worden als

$$\text{ggd}(a, b) = r_{k-1} = r_{k-3} - r_{k-2} q_{k-2}.$$

Bijgevolg kan d geschreven worden in de vorm

$$m' r_{k-2} + n' r_{k-3},$$

waarbij $m' = -q_{k-2}$ en $n' = 1$. Indien we nu r_{k-2} substitueren als een lineaire combinatie van r_{k-3} en r_{k-4} dan verkrijgen we

$$d = m'(r_{k-4} - r_{k-3} q_{k-2}) + n' r_{k-3},$$

hetgeen in de vorm $m''r_{k-3} + n''r_{k-4}$ gebracht kan worden met $m'' = n' - m'q_{k-3}$ en $n'' = m'$. Op die manier zal na opeenvolgende substituties uiteindelijk d in de gewenste vorm gebracht worden. □

De getallen m en n worden ook wel de *Bézout-coëfficiënten* genoemd. Stelling 4.13 is vooral belangrijk in het geval $\text{ggd}(a, b) = 1$, aangezien er dan gehele getallen m en n gevonden kunnen worden zodat $ma + nb = 1$. Merk wel op dat de getallen m en n niet noodzakelijk uniek bepaald zijn, immers

$$ma + nb = (m - kb)a + (n + ka)b, \quad \forall k \in \mathbb{Z}.$$

Het (uitgebreid) algoritme van Euclides is wel degelijk efficiënt in de computationele zin. Men kan aantonen dat de complexiteit voor $\mathbb{Z}$ kwadratisch is in de woordlengte van de getallen, hetgeen goed genoeg is om als basisalgoritme te dienen. Het uitgebreid algoritme van Euclides maakt daarenboven efficiënte modulaire berekeningen mogelijk, hetgeen de hoeksteen is van vele belangrijke algoritmen in de computeralgebra. Elk computeralgebrasysteem bevat dan ook een implementatie van dit algoritme[1]. Meer informatie vindt men in [17, pp. 22–24].

Een aantal elementaire eigenschappen van de grootste gemene deler zijn nuttig in de verdere opbouw. Het bewijs steunt al dan niet op Stelling 4.13.

Gevolg 4.14

Er geldt dat $\text{ggd}(a, b) \mid ax + by$ voor alle $x, y \in \mathbb{Z}$.

Bewijs. Dit volgt onmiddellijk uit Gevolg 4.3 □

Gevolg 4.15

Veronderstel dat $a, b, c \in \mathbb{Z}$, en $\text{ggd}(a, b) = 1$. Dan geldt $a \mid b \cdot c \Longrightarrow a \mid c$.

Bewijs. Uit $a \mid bc$ volgt dat $a \cdot z = bc$, voor een $z \in \mathbb{Z}$. Door Stelling 4.13 en de veronderstelling dat $\text{ggd}(a, b) = 1$ volgt het bestaan van gehele getallen x, y met $ax + by = \text{ggd}(a, b) = 1$. Vermenigvuldigen we beide leden met c, dan zien we onmiddellijk dat $c = cax + cby = a(cx + zy)$, dus $a \mid c$. □

[1] Dit algoritme is het oudste niet-triviale algoritme dat nog steeds onvervangbaar is, [11, §4.5.2]

Gevolg 4.16

Veronderstel dat $a \mid m$, $b \mid m$ en $\text{ggd}(a, b) = 1$. Dan geldt $a \cdot b \mid m$.

Bewijs. Uit Stelling 4.13 volgt het bestaan van $x, y \in \mathbb{Z}$ met $ax + by = 1$, dus $max + mby = m$. Uit de veronderstellingen $a \mid m$ en $b \mid m$ volgt ook dat $ab \mid max$ en $ab \mid mby$, dus $ab \mid m$. □

Getallen a en b met $\text{ggd}(a, b) = 1$ noemen we *onderling ondeelbaar*.

Lemma 4.17

Veronderstel dat de gehele getallen a en b onderling ondeelbaar zijn. Dan geldt voor alle $c \in \mathbb{Z}$ dat $\text{ggd}(\text{ggd}(a, c), \text{ggd}(b, c)) = 1$.

Bewijs. Noem $g = \text{ggd}(a, c)$ en $h = \text{ggd}(b, c)$. Dan geldt $g \mid a$, $g \mid c$ en $h \mid b$, $h \mid c$, dus $\text{ggd}(g, h)$ is een deler van a, b en c. Maar $\text{ggd}(a, b) = 1$, dus $\text{ggd}(g, h) = 1$. □

Lemma 4.18

Als a, b en c natuurlijke getallen zijn, en ac en bc niet beide nul zijn, dan is $\text{ggd}(ca, cb) = c\,\text{ggd}(a, b)$.

Bewijs. Stel $h = \text{ggd}(ca, cb)$ en $g = \text{ggd}(a, b)$. Er geldt dat $g \mid a$ en $g \mid b$, dus $cg \mid ca$ en $cg \mid cb$, dus $cg \mid \text{ggd}(ca, cb)$. Er geldt ook dat $h \mid ca$ en $h \mid cb$, dus $h \mid xca + ycb$ voor willekeurige gehele getallen x en y. Er bestaan welbepaalde gehele getallen m en n waarvoor $\text{ggd}(a, b) = ma + nb$ (Stelling 4.13), dus $h \mid c(ma + nb) = c\,\text{ggd}(a, b)$. We besluiten dat $\text{ggd}(ca, cb) = c\,\text{ggd}(a, b)$. □

Lemma 4.19

Als a, b en c gehele getallen zijn met hetzij a en b, hetzij a en c, hetzij b en c onderling ondeelbaar, dan geldt $\text{ggd}(a, c) \cdot \text{ggd}(b, c) = \text{ggd}(ab, c)$. Bijgevolg zijn ab en c onderling ondeelbaar als en slechts als zowel a en c als b en c onderling ondeelbaar zijn.

Bewijs. (i) We tonen eerst aan dat $\text{ggd}(ab, c) \mid \text{ggd}(a, c)\,\text{ggd}(b, c)$. Wegens Stelling 4.13 bestaan er gehele getallen r, s, t en u zodat $\text{ggd}(a, c) = ra + sc$ en $\text{ggd}(b, c) = tb + uc$. Dus $\text{ggd}(a, c)\,\text{ggd}(b, c) = rtab + c(stb + rua + suc)$, een lineaire combinatie van ab en c. Door Gevolg 4.14 geldt nu dat $\text{ggd}(ab, c) \mid \text{ggd}(a, c)\,\text{ggd}(b, c)$.

(ii) We veronderstellen nu dat $\text{ggd}(a, b) = 1$. Er geldt dat $\text{ggd}(a, c) \mid \text{ggd}(ab, c)$ en $\text{ggd}(b, c) \mid \text{ggd}(ab, c)$, en $\text{ggd}(\text{ggd}(a, c), \text{ggd}(b, c)) = 1$ door Lemma 4.17. Door Gevolg 4.16 geldt dat $\text{ggd}(a, c)\,\text{ggd}(b, c) \mid \text{ggd}(ab, c)$. Door (i) mogen we nu besluiten dat $\text{ggd}(ab, c) = \text{ggd}(a, c)\,\text{ggd}(b, c)$.

(iii) We veronderstellen nu dat $\text{ggd}(a, c) = 1$. Samen met (i) geldt nu dat $\text{ggd}(ab, c) \mid \text{ggd}(b, c)$. Omdat $\text{ggd}(b, c) \mid \text{ggd}(ab, c)$ volgt nu dat $\text{ggd}(ab, c) = \text{ggd}(b, c)$.

(iv) Volledig analoog als in (iii) leidt de veronderstelling $\text{ggd}(b, c) = 1$ tot $\text{ggd}(ab, c) = \text{ggd}(a, c)$. □

Voor elke 2 gehele getallen a, b noemen we een geheel getal v waarvoor zowel $a \mid v$ als $b \mid v$ een *gemeen veelvoud* van a en b. Volkomen analoog aan de definitie van grootste gemene deler, komen we tot de volgende definitie van kleinste gemeen veelvoud.

Definitie 4.20

Stel $a, b \in \mathbb{Z}$ beide niet nul. Een getal $c \in \mathbb{Z}$ is een *kleinste gemeen veelvoud* van a en b als en slechts als elk gemeen veelvoud van a en b een veelvoud is van c. *Het kleinste gemeen veelvoud* van a en b is het unieke positieve onder de kleinste gemene veelvouden van a en b.

Op vergelijkbare wijze zoals voor de grootste gemene deler, kunnen heel wat eigenschappen van het kleinste gemeen veelvoud bewezen worden.

4.2 Priemgetallen

Definitie 4.21

Een positief geheel getal p wordt een *priemgetal* genoemd als p juist 2 verschillende positieve delers bezit (1 en zichzelf).

Met deze definitie is dus 1 geen priemgetal. Elk getal $m \in \mathbb{N} \setminus \{0, 1\}$ dat geen priemgetal is, kan dus geschreven worden als een product $m_1 m_2$ met $m_i \in \{2, \ldots, m-1\}$ (m_1 kan gelijk zijn aan m_2). We noemen daarom elk dergelijk getal m een *samengesteld getal*.

De priemgetallen kleiner dan 50 zijn:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

Nochtans is het voor grotere getallen niet altijd zo eenvoudig om snel te bepalen of een getal een priemgetal is. Het probleem om al de priemgetallen kleiner dan een gegeven positief geheel getal op te sommen is een ander probleem.

Merk vooreerst op dat er oneindig veel priemgetallen bestaan. Dit is een stelling die toegeschreven is aan Euclides.

Stelling 4.22 — Euclides

Er zijn oneindig veel priemgetallen.

Bewijs. Veronderstel dat de verzameling van de priemgetallen een eindige verzameling $\{p_1, p_2, \ldots, p_n\}$ zou zijn. Stel $m = \prod_{i=1}^{n} p_i$, dan is $m + 1$ dus geen priemgetal en dus bezit $m + 1$ eigenlijke delers. Noem q de kleinste eigenlijke positieve deler van $m + 1$. Dan is q een priemgetal en dus ook een deler van m. Bijgevolg is q een deler van $(m + 1) - m = 1$. Dit is een tegenstrijdigheid. Bijgevolg is de verzameling van de priemgetallen een oneindige verzameling. □

Priemgetallen spelen een fundamentele rol in de algebraïsche structuur van de gehele getallen. Wij zijn vertrouwd met de idee dat elk natuurlijk getal (verschillend van 0 en 1) geschreven kan worden als een product van priemfactoren, of m.a.w. ontbonden kan worden in priemfactoren, en dat die ontbinding uniek is, op de volgorde van de factoren na. Om de uniciteit van de ontbinding aan te tonen, zullen we gebruik maken van het volgende lemma (en zijn gevolg).

Lemma 4.23

Stel dat p een priemgetal is en dat $p \mid ab$ voor twee gehele getallen $a, b \in \mathbb{Z}$. Dan geldt $p \mid a$ of $p \mid b$.

Bewijs. Veronderstel dat $p \nmid a$. Dan is $\text{ggd}(a, p) = 1$. Uit Gevolg 4.15 volgt dat $p \mid b$. □

Gevolg 4.24

Indien p een priemgetal is en indien $x_1, x_2, \ldots, x_n$ gehele getallen zijn zodanig dat

$$p \Big| \prod_{i=1}^{n} x_i,$$

dan is p een deler van ten minste één x_i ($i \in \{1, \ldots, n\}$).

Bewijs. Door volledige inductie, en met behulp van Lemma 4.23. □

Het *bestaan* van een ontbinding steunt in het bewijs dat we hier geven op het welordeningsprincipe. Het is niet verwonderlijk dat dit ook kan aangetoond worden door volledige inductie.

Stelling 4.25 — Hoofdstelling van de rekenkunde (Euclides)

Elk getal $n \in \mathbb{N} \setminus \{0, 1\}$ is te schrijven als een product van priemfactoren. Op de volgorde na is deze ontbinding uniek.

Bewijs. Noem B de verzameling van de natuurlijke getallen $n \geq 2$ die niet te schrijven zijn als een product van priemfactoren. Veronderstel dat $B \neq \emptyset$, dan bezit B als gevolg van het axioma van de goede ordening een kleinste element m. Aangezien m dan geen priemgetal kan zijn, moet m samengesteld zijn: stel $m = m_1 m_2,\ m_i \in \{2, \ldots, m-1\}$. Aangezien echter m als kleinste element uit B gekozen was, bezitten zowel m_1 als m_2 een ontbinding in priemfactoren. Het product $m = m_1 m_2$ bezit dan echter eveneens een ontbinding in priemfactoren, en dit is tegen de onderstelling dat m tot B behoort. Bijgevolg is B de ledige verzameling.

Beschouw het kleinste natuurlijk getal $n \in \mathbb{N} \setminus \{0, 1\}$ waarvoor er twee ontbindingen gevonden kunnen worden

$$\begin{aligned} n &= p_1 \cdot p_2 \cdot \cdots \cdot p_k \\ &= q_1 \cdot q_2 \cdot \cdots \cdot q_r. \end{aligned}$$

Alle getallen p_i en q_i zijn priemgetallen. Door Gevolg 4.23 geldt $p_1 \mid q_j$ voor een zekere j. We mogen $j = 1$ stellen. Omdat q_1 en p_1 priemgetallen zijn, geldt $p_1 = q_1$. na wegdelen van $p_1 = q_1$ in beide zijden van de vergelijking, blijft er de gelijkheid

$$p_2 \cdots p_k = q_2 \cdots q_r$$

over.

Daar $n > p_2 \cdots p_k$ en daar n het kleinste natuurlijk getal is dat op minstens 2 verschillende manieren ontbonden kan worden als een product van priemfactoren, dient te gelden, op een eventuele wijziging van de volgorde van de priemfactoren na, dat $r = k$, $p_i = q_i$, $i = 2, \ldots, k$. Samen met $p_1 = q_1$ leidt dit tot het besluit dat n toch een unieke ontbinding in priemfactoren bezit.

Hiermee is de uniciteit van de ontbinding in priemfactoren voor elk getal $n \in \mathbb{N} \setminus \{0, 1\}$ aangetoond. □

Zoals gezegd is het ook mogelijk om het bestaan van een ontbinding in priemfactoren te bewijzen door volledige inductie. Daartoe gebruiken we als inductiehypothese de volgende uitspraak:

> $A(n)$: elk natuurlijk getal $m \in \mathbb{N}_{<n+1}$ is ofwel een priemgetal ofwel het product van priemgetallen.

Het is nu een eenvoudige oefening om een alternatief bewijs op te stellen.

De zeef van Eratosthenes

Een elementaire manier om alle priemgetallen te vinden die kleiner zijn dan een gegeven getal n staat bekend als de *Zeef van Eratosthenes*. Deze methode gaat als volgt. Het getal 2 is een priemgetal, en al de andere even getallen zijn uiteraard geen priemgetallen. We kunnen ons dus beperken tot de oneven getallen, kleiner dan n. We rangschikken deze getallen van klein naar groot. Het eerste getal in de rij is 3, een priemgetal, maar alle 3-vouden mogen we schrappen. Het volgende getal is het priemgetal 5, de 5-vouden worden geschrapt, daarna komt 7 en worden al de 7-vouden geschrapt. Merk op dat 9 reeds geschrapt was als 3-voud, zodat het volgende priemgetal 11 zal zijn, ... Telkens we een getal tegenkomen dat nog niet geschrapt is, weten we dat het geen eigenlijke delers bezit en dus een priemgetal is. We schrappen telkens de veelvouden van dit getal (sommige van deze getallen kunnen al eerder geschrapt zijn).

Priemelenten in $\mathbb{Z}$

Priemgetallen spelen een essentiële rol in de algebra van de gehele getallen. Desondanks hebben we priemgetallen als natuurlijke getallen gedefinieerd.

Definitie 4.26

Een getal $x \in \mathbb{Z}$ is een *priemelement* als $|x| \in \mathbb{N}$ een priemgetal is.

In Hoofdstuk 5 zullen we zien dat de getallen -1 en 1 een bijzondere rol spelen in $\mathbb{Z}$. De formulering van de hoofdstelling van de rekenkunde in $\mathbb{Z}$ is de volgende stelling.

Stelling 4.27

Elk getal $z \in \mathbb{Z} \setminus \{-1, 0, 1\}$ is te schrijven als het product van priemelementen. Op de volgorde en het teken van deze priemelementen na, is deze ontbinding uniek.

In een cursus algebra zal bovenstaande stelling in nog een abstracter kader herhaald worden.

Aangezien we afgesproken hebben om 1 niet als priemgetal te beschouwen, kunnen we ook zeggen dat $\text{ggd}(a, b) = 1$ betekent dat a en b geen priemfactoren gemeen hebben. Daarom worden in dit geval a en b *relatief priem*, en soms ook *copriem* genoemd.

Gevolg 4.28

1. Het aantal positieve delers van een natuurlijk getal n kan op de volgende manier berekend worden. Veronderstel dat de ontbinding van n in priemfactoren er als volgt uitziet:

   $$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}.$$

   Elke deler d van n is dan van de vorm

   $$d = p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}, \quad x_i \in \mathbb{N}_{<e_i+1}, i = 1, \dots, k.$$

   Het aantal delers van n is bijgevolg gelijk aan het aantal k-tallen $(x_1, x_2, \dots, x_k)$ met $x_i \in \mathbb{N}_{<e_i+1}$ en is bijgevolg gelijk aan $\prod_{i=1}^{k}(e_i + 1)$.

2. De grootste gemene deler van twee natuurlijke getallen a en b verschillend van 0, heeft een ontbinding in priemfactoren van de vorm $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, waarbij elk van de priemgetallen p_i een gemene deler is van a en van b, en waarbij e_i het minimum is van de exponent van p_i in de priemfactorontbindingen van a en b.

3. Het kleinste gemeen veelvoud van 2 natuurlijke getallen a en b verschillend van 0, heeft een ontbinding in priemfactoren van de vorm $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, waarbij elk van de priemgetallen p_i ten minste één maal voorkomt in de priemfactorontbinding van a of van b, en waarbij e_i het maximum is van de exponent van p_i in deze priemfactorontbindingen van a en b.

4. Als a en b natuurlijke getallen zijn, niet beide nul, dan is $\text{kgv}(a, b) \cdot \text{ggd}(a, b) = ab$.

Stelling 4.29

Laat n een positief natuurlijk getal zijn, en $a_0, \ldots, a_n$ gehele getallen, met $a_0 \neq 0$ en $a_n \neq 0$. Dan geldt voor elke rationale oplossing x_0 van de vergelijking

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

dat $x_0 = p/q$, voor een zekere p die deler is van a_n, en voor een zekere q die deler is van a_0. In het bijzonder, als $a_0 = 1$, dan zijn de rationale oplossingen ook geheel.

Bewijs. Laten we een rationale oplossing x_0 schrijven als een onvereenvoudigbare breuk, dus $x_0 = p/q,\ \text{ggd}(p, q) = 1$. Dan geldt

$$a_0(p/q)^n + a_1(p/q)^{n-1} + \cdots + a_{n-1}(p/q) + a_n = 0.$$

Vermenigvuldiging met q^n levert

$$a_0 p^n + a_1 p^{n-1} q + \cdots + a_{n-1} p q^{n-1} + a_n q^n = 0.$$

Hieruit volgt dat

$$p(a_0 p^{n-1} + a_1 p^{n-2} q + \cdots + a_{n-1} q^{n-1}) = -a_n q^n,$$

zodat p een deler is van $a_n q^n$. Aangezien echter p en q relatief priem zijn, moet p een deler zijn van a_n. Op dezelfde manier bewijzen we dat q een deler is van a_0. □

4.3 Congruenties

Definitie 4.30

Veronderstel dat x_1 en x_2 gehele getallen zijn en dat m een positief natuurlijk getal is. We noemen dan x_1 en x_2 *congruent modulo* m dan en slechts dan als $x_1 - x_2$ deelbaar is door m. We noteren dit als

$$x_1 \equiv x_2 \pmod{m}.$$

Twee gehele getallen zijn congruent modulo m dan en slechts dan als ze dezelfde rest opleveren na deling door m. Met andere woorden x_1 en x_2 zijn

congruent modulo m dan en slechts dan als er een geheel getal t bestaat zodanig dat

$$x_1 = x_2 + mt.$$

Het volgende lemma is eenvoudig te bewijzen.

Lemma 4.31

De relatie congruent modulo m is een equivalentierelatie op $\mathbb{Z}$.

Bewijs. Oefening. □

De equivalentieklassen worden *congruentieklassen modulo m* genoemd. We zeggen ook soms dat x_1 en x_2 *equivalent zijn modulo m*. De congruentieklassen modulo m worden daarom ook nog *de restklassen modulo m* genoemd, en de klasse met representant r, wordt soms genoteerd door $[r]_m$ of kortweg door $[r]$ indien er geen verwarring mogelijk is. De verzameling van de restklassen modulo m (met andere woorden de quotiëntverzameling van $\mathbb{Z}$ met betrekking tot de equivalentierelatie congruent modulo m) wordt genoteerd door $\mathbb{Z}/m\mathbb{Z}$. Indien we uit elke restklasse de kleinste natuurlijke representant kiezen, dan ontstaat de verzameling $\mathbb{N}_{<m}$. Er bestaat m.a.w. een bijectie tussen de verzamelingen $\mathbb{Z}/m\mathbb{Z}$ en $\mathbb{N}_{<m}$.

Stelling 4.32

Veronderstel dat m een positief natuurlijk getal is en dat x_1, x_2, y_1, y_2 gehele getallen zijn zodanig dat

$$x_1 \equiv x_2 \pmod{m}, \quad y_1 \equiv y_2 \pmod{m}.$$

Dan gelden volgende eigenschappen

1. $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$,
2. $x_1 y_1 \equiv x_2 y_2 \pmod{m}$.

Bewijs. 1. Uit het gegeven volgt dat er gehele getallen t en t' bestaan zodanig dat

$$x_1 - x_2 = mt, \qquad y_1 - y_2 = mt'.$$

Bijgevolg geldt

$$\begin{aligned}(x_1 + y_1) - (x_2 + y_2) &= (x_1 - x_2) + (y_1 - y_2) \\ &= mt + mt' \\ &= m(t + t').\end{aligned}$$

Bijgevolg zijn $x_1 + y_1$ en $x_2 + y_2$ congruent modulo m.

2. Merk op dat

$$\begin{aligned}x_1y_1 - x_2y_2 &= (x_1 - x_2)y_1 + x_2(y_1 - y_2) \\ &= mty_1 + x_2mt' \\ &= m(y_1t + x_2t').\end{aligned}$$

Bijgevolg zijn x_1y_1 en x_2y_2 congruent modulo m. □

Bovenstaande stelling toont in feite aan dat we over een goed gedefinieerde *optelling en vermenigvuldiging* beschikken in de verzameling $\mathbb{Z}/m\mathbb{Z}$. Merk op dat we optelling en vermenigvuldiging hier zien als een abstracte binaire operatie die aan bepaalde vereisten voldoet. In Hoofdstuk 5 zullen we dieper ingaan op deze vereisten.

We bespreken eerst een kleine toepassing. De *negenproef* is een werkwijze die in de lagere school aangeleerd wordt om na te gaan of een gemaakte vermenigvuldiging al dan niet fout is. Deze werkwijze is gebaseerd op het volgende eenvoudige lemma.

Lemma 4.33

Veronderstel dat $(x_nx_{n-1}\ldots x_2x_1x_0)_{10}$ *de voorstelling is van het getal* x *in basis* 10*. Dan geldt*

$$x \equiv \sum_{i=0}^{n} x_i \pmod 9.$$

Bewijs. Uit de definitie van de voorstelling van een getal in basis 10, volgt dat

$$\begin{aligned}x - \left(\sum_{i=0}^{n} x_i\right) &= \sum_{i=0}^{n} x_i(10)^i - \sum_{i=0}^{n} x_i \\ &= \sum_{i=1}^{n}((10)^i - 1)x_i.\end{aligned}$$

Aangezien $10 \equiv 1 \pmod 9$, geldt nu voor elk natuurlijk getal $i \geq 0$ dat $(10)^i - 1 \equiv 0 \pmod 9$, en dus

$$x - \left(\sum_{i=0}^{n} x_i \right) \equiv 0 \pmod 9.$$

Hieruit volgt de gevraagde congruentie. □

Indien we nu kort $\theta(x)$ schrijven voor $\sum_{i=0}^{n} x_i$, dan hebben we dus aangetoond dat $\theta(x) \equiv x \pmod 9$. Bijgevolg geldt wegens stelling 4.32

$$\theta(x)\theta(y) \equiv xy \pmod 9.$$

We hebben eveneens dat

$$\theta(xy) \equiv xy \pmod 9,$$

zodat

$$\theta(xy) \equiv \theta(x)\theta(y) \pmod 9.$$

Dit is de gekende *negenproef* voor de vermenigvuldiging van gehele getallen. B.v. als $x = 12$ en $y = 17$, is $\theta(x) = 3$, $\theta(y) = 8$, $\theta(x)\theta(y) = 24$, $xy = 204$ en $\theta(xy) = 6$. We hebben nu dat $\theta(xy) \equiv \theta(x)\theta(y) \equiv 6 \pmod 9$.

4.4 Optelling en vermenigvuldiging in $\mathbb{Z}/m\mathbb{Z}$

We zullen nu in de verzameling $\mathbb{Z}/m\mathbb{Z}$ een optelling $\oplus$ en een vermenigvuldiging $\otimes$ definiëren.

$$[x]_m \oplus [y]_m = [x + y]_m$$

$$[x]_m \otimes [y]_m = [x \times y]_m.$$

Merk op dat de bewerkingen $+$ en $\times$ de optelling en de vermenigvuldiging zijn van gehele getallen, terwijl $\oplus$ en $\otimes$ bewerkingen definiëren met deelverzamelingen van gehele getallen. Opdat de definitie zinvol zou zijn, moeten we er ons van vergewissen dat deze definitie onafhankelijk is van de keuze van de representanten x en y uit de klassen $[x]_m$ en $[y]_m$. Met andere woorden, als $[x]_m$ en $[x']_m$ dezelfde klasse voorstellen en als $[y]_m$ en $[y']_m$ dezelfde

klasse voorstellen, dan moeten ook $[x]_m \oplus [y]_m$ en $[x']_m \oplus [y']_m$ dezelfde klasse voorstellen, analoog moet dit ook gelden voor de vermenigvuldiging. Dat dit wel degelijk het geval is, volgt onmiddellijk uit stelling 4.32.

De eigenschappen die voor de optelling en de vermenigvuldiging van restklassen modulo m gelden, zijn dan ook een onmiddellijk gevolg van de eigenschappen voor de optelling en de vermenigvuldiging van de gehele getallen. We geven hier een kort overzicht.

(A1) $\forall [a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$: $[a]_m \oplus [b]_m \in \mathbb{Z}/m\mathbb{Z}$ en $[a]_m \otimes [b]_m \in \mathbb{Z}/m\mathbb{Z}$.

(A2) $\forall [a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}$: $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$ en $[a]_m \otimes [b]_m = [b]_m \otimes [a]_m$.

(A3) $\forall [a]_m, [b]_m, [c]_m \in \mathbb{Z}/m\mathbb{Z}$: $([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$ en $([a]_m \otimes [b]_m) \otimes [c]_m = [a]_m \otimes ([b]_m \otimes [c]_m)$.

(A4) $\forall [a]_m \in \mathbb{Z}/m\mathbb{Z}$: $[a]_m \oplus [0]_m = [a]_m$ en $[a]_m \otimes [1]_m = [a]_m$.

(A5) $\forall [a]_m, [b]_m, [c]_m \in \mathbb{Z}/m\mathbb{Z}$: $[a]_m \otimes ([b]_m \oplus [c]_m) = ([a]_m \otimes [b]_m) \oplus ([a]_m \otimes [c]_m)$.

(A6) $\forall [a]_m \in \mathbb{Z}/m\mathbb{Z}, \exists - [a]_m = [-a]_m \in \mathbb{Z}/m\mathbb{Z} : [a]_m \oplus (-[a]_m) = [0]_m$.

Bekijken we de optelling $\oplus$ afzonderlijk, dan is deze inwendig, commutatief, associatief, en bestaat er steeds een neutraal element. Voor de vermenigvuldiging $\otimes$ gelden dezelfde eigenschappen. De optelling heeft echter als extra eigenschap dat er steeds een invers element bestaat. Ten slotte is er nog de distributiviteit van de vermenigvuldiging ten opzichte van de optelling. Deze eigenschappen maken dat $\mathbb{Z}/m\mathbb{Z}, \oplus, \otimes$ een *ring* is. In Hoofdstuk 5 komen we hierop terug.

Merk echter op dat de schrappingswet voor de vermenigvuldiging in $\mathbb{Z}/m\mathbb{Z}$ niet geldt. Zo is bijvoorbeeld in $\mathbb{Z}/6\mathbb{Z}$,

$$[3]_6 \otimes [1]_6 = [3]_6 \otimes [5]_6,$$

en alhoewel $[3]_6 \neq [0]_6$ mogen we de klasse $[3]_6$ niet schrappen, want $[1]_6 \neq [5]_6$. Het zelfde geldt voor de $[2]_6$, maar niet voor $[5]_6$. Bekijken we de afbeelding $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $x \mapsto c \cdot x$, voor $c = 2$, en $c = 5$, dan wordt onmiddellijk duidelijk waarom.

We observeren eveneens dat het kan voorkomen dat $[a]_m \otimes [b]_m = [0]_m$ terwijl nochtans $[a]_m \neq [0]_m$ en $[b]_m \neq [0]_m$, dergelijk geval doet zich onder andere voor indien m een deler is van ab. Zo is bijvoorbeeld in $\mathbb{Z}/6\mathbb{Z}$,

$$[2]_6 \otimes [3]_6 = [0]_6\,,$$