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.

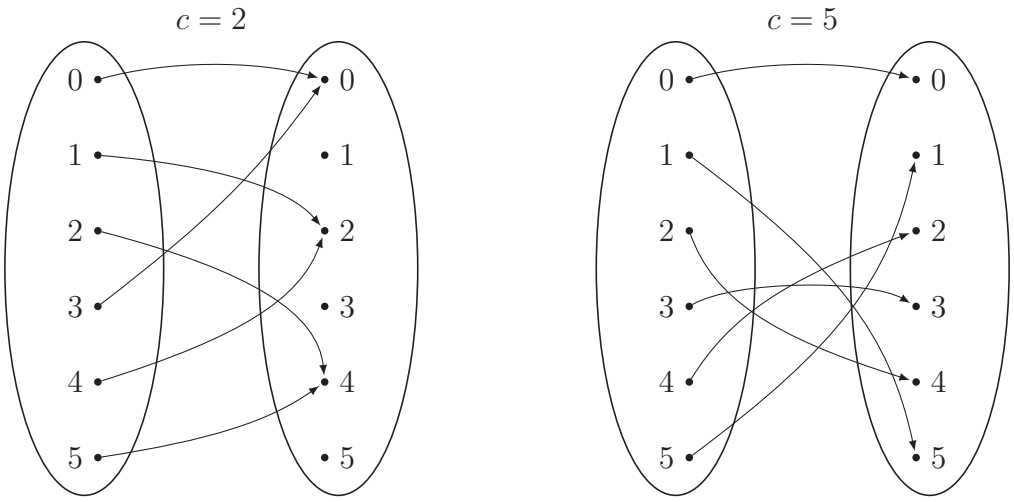
Merk echter op dat de schrappingswet voor de vermenigvuldiging in $\mathbb{Z}/m\mathbb{Z}$ niet geldt. Zo is bijvoorbeeld in $\mathbb{Z}/6\mathbb{Z}$,

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

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 $\mathbb{Z}/6\mathbb{Z}$,

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



Figuur 4.1: De afbeelding f voor $c = 2$ en $c = 5$

Men zegt daarom dat de klassen $[a]_m$ met a een echte deler van m, *nuldelers* zijn in $\mathbb{Z}/m\mathbb{Z}$. Indien $m = p$ een priemgetal is, dan bezit $\mathbb{Z}/p\mathbb{Z}$ dus geen nuldelers door Lemma 4.23.

Indien er geen verwarring mogelijk is, zullen we in het vervolg de klassen $[r]_m$ meestal voorstellen door een representant $r+tm$ en zullen we voor de optelling van twee klassen in plaats van $[a]_m \oplus [b]_m$, de notatie $a+b \pmod m$ gebruiken. Analoog zal voor de vermenigvuldiging van twee klassen $[a]_m \otimes [b]_m$ de notatie $a \times b \pmod m$ of kortweg $ab \pmod m$ of $a \cdot b \pmod m$gebruikt worden.

Een geheel getal r ($r \neq \pm 1$) bezit geen invers element in $\mathbb{Z}$ voor de vermenigvuldiging. In $\mathbb{Z}/m\mathbb{Z}$ is de situatie enigszins anders. We gaan na wanneer een element van $\mathbb{Z}/m\mathbb{Z}$ een invers element in $\mathbb{Z}/m\mathbb{Z}$ bezit.

Definitie 4.34

Een element $r \in \mathbb{Z}/m\mathbb{Z}$ wordt *inverteerbaar* genoemd als er een element x in $\mathbb{Z}/m\mathbb{Z}$ bestaat, zodanig dat $rx = 1$ in $\mathbb{Z}/m\mathbb{Z}$, met andere woorden indien $rx \equiv 1 \pmod m$. We noteren het *invers element* x van r als r^{-1}.

Stelling 4.35

Een element r in $\mathbb{Z}/m\mathbb{Z}$ is inverteerbaar dan en slechts dan als r en m onderling ondeelbaar zijn. In het bijzonder is in $\mathbb{Z}/p\mathbb{Z}$, p een priemgetal, elk element verschillend van 0 inverteerbaar.

Bewijs. Veronderstel dat r inverteerbaar is, dan bestaat er een geheel getal x, zodanig dat $rx \equiv 1 \pmod{m}$. Bijgevolg bestaat er een $k \in \mathbb{Z}$ zodanig dat $rx - 1 = km$, of

$$rx - km = 1.$$

Uit Gevolg 4.14 volgt dat $\text{ggd}(r, m) = 1$.

Omgekeerd, veronderstel dat r en m onderling ondeelbaar zijn, dan bestaan er gehele getallen x en y, zodanig dat $rx + my = 1$ (Stelling 4.13), hetgeen gelijkwaardig is met $xr \equiv 1 \pmod{m}$. □

Stelling 4.36 — Stelling van Wilson

Als p een priemgetal is, dan geldt

$$(p-1)! \equiv -1 \pmod{p}.$$

Bewijs. We merken vooreerst op dat de stelling triviaal voldaan is voor $p = 2$. Veronderstel daarom nu dat p een oneven priemgetal is. We beschouwen de verzameling $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. Aangezien p een priemgetal is, zal elk element a van deze verzameling inverteerbaar zijn en het invers element a^{-1} behoort eveneens tot deze verzameling. Bijgevolg kunnen we bij de berekening van $(p-1)!$ modulo p telkens een element a samennemen met zijn invers element a^{-1}, (en $aa^{-1} \equiv 1 \pmod{p}$) op voorwaarde dat $a \not\equiv a^{-1} \pmod{p}$. Maar $a \equiv a^{-1} \pmod{p}$ dan en slechts dan als $(a^2 - 1) \equiv 0 \pmod{p}$, zodat dus p een deler is van $a^2 - 1 = (a+1)(a-1)$. Aangezien p een priemgetal is, volgt hieruit dat p ofwel een deler is van $a - 1$ of van $a + 1$. Aangezien $a \in \{1, \ldots, p-1\}$, volgt hieruit dat ofwel $a = 1$ ofwel $a = p - 1$. Bijgevolg is

$$(p-1)! \equiv 1 \cdot (p-1) \cdot (1)^{\frac{p-3}{2}} \equiv -1 \pmod{p}.$$ □

4.5 Lineaire congruenties

We beschikken over de bewerkingen + en $\cdot$ in $\mathbb{Z}/m\mathbb{Z}$. Het is dus vanzelfsprekend dat we proberen om vergelijkingen op te lossen in $\mathbb{Z}/m\mathbb{Z}$. We zullen ons beperken tot de lineaire en de kwadratische vergelijkingen.

Een vergelijking van de vorm $ax \equiv b \pmod{m}$ met a en b gegeven gehele getallen, en x een onbekende in $\mathbb{Z}/m\mathbb{Z}$, wordt een **lineaire congruentie** genoemd. Het oplossen van een dergelijke lineaire congruentie is gelijkwaardig met het zoeken naar een koppel $(x,t), x \in \mathbb{N}_{<m}, t \in \mathbb{Z}$, zodanig dat $ax = b + mt$.

Merk op dat $ax \equiv b \pmod{m}$ in feite een verkorte schrijfwijze is voor $[a]_m \otimes [x]_m = [b]_m$. Een oplossing van deze vergelijking tussen congruentieklassen modulo m is dus zelf een congruentieklasse modulo m. We zullen echter ook nu weer spreken van de oplossing r i.p.v. $[r]_m$. Met deze afspraken zijn twee oplossingen r_1 en r_2 van eenzelfde lineaire congruentie verschillend dan en slechts dan als $[r_1]_m \neq [r_2]_m$.

Stelling 4.37

1. Als $d = \text{ggd}(a,m) \nmid b$, dan bezit $ax \equiv b \pmod{m}$ geen oplossing.
2. Als $d = \text{ggd}(a,m) \mid b$, dan bezit $ax \equiv b \pmod{m}$ juist d oplossingen r waarbij $r \in \mathbb{N}_{<m}$.

Bewijs.

1. Veronderstel dat $\text{ggd}(a,m) = d > 1$ geen deler is van b. Indien $r \in \mathbb{N}_{<m}$ een oplossing is van de lineaire congruentie $ax \equiv b \pmod{m}$, dan bestaat er een geheel getal k zodanig dat $ar - b = km$ of dus zodanig dat $ar - km = b$. Hieruit zou volgen dat d een deler is van b. Een tegenstrijdigheid.

2. Veronderstel dat $\text{ggd}(a,m) = 1$, dan is, wegens stelling 4.35, a inverteerbaar in $\mathbb{Z}/m\mathbb{Z}$. Bijgevolg bestaat er een element $a^{-1} \in \mathbb{Z}/m\mathbb{Z}$ zodanig dat $aa^{-1} \equiv 1 \pmod{m}$, zodat $a^{-1}(ax) \equiv (a^{-1}b) \pmod{m}$ of dus $x \equiv (a^{-1}b) \pmod{m}$. Bovendien kan men eenvoudig bewijzen dat elke oplossing van deze vorm is (oefening). Veronderstel nu dat $\text{ggd}(a,m) = d > 1$ en dat $d|b$. We kunnen dan de beide leden van de lineaire congruentie delen door d en we bekomen dan

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}, \quad \text{ggd}(\frac{a}{d}, \frac{m}{d}) = 1.$$

Deze laatste lineaire congruentie bezit juist één oplossing r in $\mathbb{N}_{<\frac{m}{d}}$. Alle oplossingen van $ax \equiv b \pmod{m}$ zijn bijgevolg van de gedaante $r + t\frac{m}{d}, t \in \mathbb{N}_{<d}$. Er zijn dus juist d oplossingen. □

Opmerkingen

1. Veronderstel dat $\text{ggd}(a, m) = 1$, dan bezit $ax \equiv b \pmod{m}$ juist één oplossing. Wegens het algoritme van Euclides (zie stelling 4.13), weten we dat er gehele getallen r en s bestaan zodanig dat $ar + ms = 1$, en bijgevolg is dan $a(rb) + m(sb) = b$ of $a(rb) \equiv b \pmod{m}$. Hieruit volgt dat $rb \pmod{m}$ een oplossing is van de gegeven lineaire congruentie.

2. In de praktijk kunnen we de oplossing het gemakkelijkst op de volgende manier vinden. We controleren eerst of $d = \text{ggd}(a, m)$ een deler is van b die groter is dan 1. Indien dit het geval is, dan moeten we eerst d wegdelen in de congruentie. Veronderstel dat dit gebeurd is, dan schrijven we de lineaire congruentie $ax \equiv b \pmod{m}$ in de vorm $ax \equiv (b + tm) \pmod{m}$ met $b + tm$ een veelvoud van a. De oplossing van de lineaire congruentie is dan van de vorm $\dfrac{b + tm}{a} \pmod{m}$.

Voorbeelden

Zoek de oplossing(en) van de volgende lineaire congruenties.

1. $4x \equiv 1 \pmod{15}$. Dit is gelijkwaardig met $4x \equiv 16 \pmod{15}$ en bijgevolg is $x \equiv 4 \pmod{15}$.

2. $14x \equiv 27 \pmod{31}$. Dit is gelijkwaardig met $14x \equiv 58 \pmod{31}$ en dus met $7x \equiv 29 \pmod{31}$, hetgeen op zijn beurt gelijkwaardig is met $7x \equiv 91 \pmod{31}$, zodat $x \equiv 13 \pmod{31}$.

3. $6x \equiv 15 \pmod{33}$. Aangezien $\text{ggd}(6, 33) = 3$ en 3 een deler is van 15, zijn er 3 oplossingen in $\mathbb{N}_{<33}$. We delen de congruentie door 3, en we zoeken de oplossing van $2x \equiv 5 \pmod{11}$. Dit is gelijkwaardig met $2x \equiv 16 \pmod{11}$ of met $x \equiv 8 \pmod{11}$. Alle oplossingen modulo 33, zijn dus van de gedaante $8 + 11t,\ t \in \{0, 1, 2\}$. Bijgevolg is x congruent met $8, 19, 30$ modulo 33.

Oefening 4.38. *Zoek de oplossingen* $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ *van* $9x + 16y = 35$.

Oplossing. De vergelijking $9x+16y = 35$ impliceert dat x en y oplossingen zijn van het stelsel lineaire congruenties

$$\begin{cases} 9x & \equiv & 35 \pmod{16} \\ 16y & \equiv & 35 \pmod{9}. \end{cases}$$

We lossen één van de congruenties op en substitueren de oplossing dan in de andere lineaire congruentie.

$$\begin{array}{rrcl} & 16y & \equiv & 35 \pmod{9} \\ \iff & 7y & \equiv & 35 \pmod{9} \\ \iff & y & \equiv & 5 \pmod{9} \\ \iff & y & = & 5 + 9t, \quad t \in \mathbb{Z}. \end{array}$$

Indien we deze oplossing nu substitueren in de gegeven vergelijking, dan bekomen we $9x + 16(5 + 9t) = 35$ hetgeen impliceert dat $x = -5 - 16t$. ■

Opmerkingen

1. In plaats van de oplossing $y = 5+9t$ van de lineaire congruentie $16y \equiv 35 \pmod 9$ te substitueren in $9x + 16y = 35$ en dan op te lossen naar x, hadden we ook de andere lineaire congruentie $9x \equiv 35 \pmod{16}$ onafhankelijk kunnen oplossen. Deze congruentie heeft als oplossing $x \equiv -5 \pmod{16}$, bijgevolg bestaat $t' \in \mathbb{Z}$ zodanig dat $x = -5 + 16t'$. De substitutie van $y = 5+9t$ en $x = -5+16t'$ in de gegeven vergelijking levert dan $t = -t'$. Deze werkwijze heeft als voordeel dat we de twee lineaire congruenties parallel kunnen uitrekenen.

2. Elke vergelijking $ax + by = c$ in $\mathbb{Z}$ (a, b en c gehele getallen), wordt *een lineaire diophantische vergelijking met 2 onbekenden* genoemd.

4.6 Stelsels lineaire congruenties

We beschouwen nu een stelsel van lineaire congruenties, met andere woorden een stelsel van de gedaante

$$a_i x \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, k \quad \gcd(a_i, m_i) | b_i.$$

We kunnen er steeds voor zorgen dat de vergelijkingen in dit stelsel van de vorm $x \equiv b_i \pmod{m_i}$ met $b_i \in \mathbb{N}_{<m_i}$ zijn (zie Paragraaf 4.5). We zullen ons daarom beperken tot de stelsels van de vorm

$$x \equiv b_i \pmod{m_i}, \quad b_i \in \mathbb{N}_{<m_i}, i = 1, \ldots, k.$$