Oefeningen Cursus Discrete Wiskunde

26 mei 2003

Hoofdstuk 1

Getallen tellen

1.1 Gehele getallen

1.1.1 Inleiding

1.1.2 De optelling en de vermeningvuldiging

Oefening 1.1.1 *Zoals gebruikelijk noteren wij xx met x^2. Bewijs op basis van de gegeven axioma's, dat voor elke 2 gegeven gehele getallen a en b er een geheel getal c bestaat zodanig dat $(a+b)c = a^2 - b^2$.*

Oplossing. We berekenen $(a+b)(a-b)$, voor alle a, $b \in \mathbb{Z}$.

$$\begin{array}{rcll} (a+b)(a-b) & = & (a+b)a - (a+b)b & \text{wegens (A5)} \\ & = & aa + ba - ab - bb & \text{wegens (A5)} \\ & = & aa - bb & \text{wegens } -(ab) = -(ba) \end{array}$$

want $-(ab) + ba = -(ab) + ab = 0$. Stel nu $c = a - b$.

Oefening 1.1.2 *Bewijs op basis van de gegeven axioma's dat het getal 0 het enige neutraal element is voor de optelling en dat elk geheel getal een uniek invers geheel getal bezit.*

Oplossing. Veronderstel dat $0'$ een neutraal element is voor de optelling in $\mathbb{Z}$. We bewijzen $0' = 0$. Uit de definitie van het neutraal element volgt $0 + 0' = 0$ en $0' + 0 = 0'$, het is duidelijk dat de commutativiteit van de optelling impliceert dat $0' = 0$. Dit bewijst deel 1.

Stel $a \in \mathbb{Z}$ en b, $b' \in \mathbb{Z}$, waarvoor $a + b = 0 = a + b'$. We bewijzen $b = b'$. Aangezien 0 het neutraal element is voor de optelling in $\mathbb{Z}$, geldt dat $b'+0 = b'$ en dus ook $b' + (a + b) = b'$. Gebruikmakend van de commutativiteits- en associativiteitsregels, kunnen we dit herschikken tot $(a+b')+b = b'$, waaruit onmiddellijk $b = b'$ volgt.

1.1.3 De ordening van de gehele getallen

Oefening 1.1.3 *Veronderstel dat $a \leq b$. Gebruik de bovenstaande axioma's om te bewijzen dat $-b \leq -a$, of algemeen, bewijs dat uit $a \leq b$ en $c \leq 0$ volgt dat $bc \leq ac$.*

Oplossing. We zullen beide bewijzen. Veronderstel $a \leq b$, dan volgt uit (A11) dat $0 \leq b + (-a)$. Passen we (A11) nogmaals toe, dan krijgen we $-b \leq -a$.
Het algemene geval kan bewezen worden door middel van dit resultaat. Stel dus $a \leq b$ en $c \leq 0$. Deel 1 impliceert nu dat $0 \leq -c$. We kunnen nu axioma (A12) gebruiken om $a(-c) \leq b(-c)$ te verkrijgen. Aangezien $a(-c) + ac = a(-c + c) = 0$ is ook $a(-c) = -ac$, en analoog $b(-c) = -bc$. Hieruit volgt dus dat $bc \leq ac$ volgens deel 1.

Oefening 1.1.4 *Bewijs dat $0 \leq x^2$ voor elk geheel getal x, bewijs hieruit dat $0 \leq 1$.*

Oplossing. Als $0 \leq x$, dan zegt (A12) dat $0 \cdot x \leq x \cdot x = x^2$. Zij nu $x \leq 0$, dan volgt uit de voorgaande oefening dat $0 \cdot x \leq x \cdot x$, waaruit opnieuw $0 \leq x^2$.

Nu geldt de formule ook voor $x = 1$ en dan krijgen we $0 \leq 1$.

Oefening 1.1.5 *Bewijs dat $n \leq n + 1$ voor elk geheel getal n.*

Oplossing. Dit volgt onmiddellijk uit $0 \leq 1$ en axioma (A11).

1.1.4 Het axioma van de goede ordening

1.2 Recursieve definities

Oefening 1.2.1 *Geef een recursieve definitie van $u_n = 2^n$ voor alle $n \geq 1$.*

Oplossing. Het is duidelijk dat $u_1 = 2$ en $u_n = 2^n = 2 \cdot 2^{n-1} = 2 \cdot u_{n-1}$, wat een recursieve definitie $u_1 = 2$, $u_n = 2u_{n-1}$ van $u_n = 2^n$ oplevert.

Oefening 1.2.2 *Schrijf een expliciete formule voor de uitdrukkingen u_n die als volgt recursief gedefinieerd worden.*

$$\begin{array}{lll} a) & u_1 = 1, \quad u_n = u_{n-1} + 3 & (n \geq 2) \\ b) & u_1 = 1, \quad u_n = n^2 u_{n-1} & (n \geq 2) \end{array}$$

Oplossing.

$$\begin{array}{lrcl} a) & u_n & = & 3(n-1)+1 \\ b) & u_n & = & (n!)^2 \end{array}$$

1.3 Het induktieprincipe

Oefening 1.3.1 *Gebruik het induktieprincipe om te bewijzen dat*

$$\sum_{i=1}^{n} i^2 = \frac{1}{6} n(n+1)(2n+1). \tag{1.1}$$

Oplossing. Neem als induktiebasis 1. Het is snel geverifieerd dat de formule geldig is voor $n = 1$. Neem nu $k \in \mathbb{N}_0$, en veronderstel dat (1.1) geldig is voor $n = k$, deze veronderstelling wordt induktiehypothese (IH) genoemd. Dan is

$$\begin{array}{rcl} \displaystyle\sum_{i=0}^{i=k+1} i^2 & = & \displaystyle\sum_{i=0}^{k} i^2 + (k+1)^2 \\ & \overset{\text{IH}}{=} & \dfrac{k}{6}(k+1)(2k+1) + (k+1)^2 \\ & = & \dfrac{(k+1)(k+2)(2k+3)}{6}, \end{array}$$

waaruit onmiddellijk volgt dat (1.1) geldig is voor $n = k + 1$. Wegens het induktieprincipe volgt het gestelde.

Oefening 1.3.2 *Gebruik het induktieprincipe om te bewijzen dat*

$$\sum_{i=0}^{n} 3^i = \frac{1}{2}(3^{n+1} - 1). \tag{1.2}$$

Oplossing. We nemen als induktiebasis 0. Het is duidelijk dat de formule geldig is voor $n = 0$. Neem nu $k \in \mathbb{N}$ willekeurig, en veronderstel dat (1.2) geldig is voor $n = k$ (IH). Dan is

$$\begin{aligned} \sum_{i=0}^{k+1} 3^i &= \sum_{i=0}^{k} 3^i + 3^{k+1} \\ &\overset{\text{IH}}{=} \frac{1}{2}(3^{k+1} - 1) + 3^{k+1} \\ &= \frac{1}{2}(3^{k+2} - 1) \end{aligned}$$

waaruit volgt dat (1.2) geldig is voor $n = k + 1$. Dus wegens het induktieprincipe is (1.2) geldig voor alle $n \in \mathbb{N}$.

Oefening 1.3.3 *Maak een tabel van de waarden*

$$s_n = \sum_{i=1}^{n} i^3,$$

voor $1 \leq n \leq 6$. *Zoek op basis van deze tabel een formule voor* s_n. *Bewijs met behulp van het induktieprincipe dat deze formule correct is voor alle* $n \geq 1$.

Oplossing.

n	1	2	3	4	5	6	7	8	9	10
n^3	1	8	27	64	125	216	343	512	729	1000
s_n	1	9	36	100	225	441	784	1296	2025	3025

Het valt op dat voor $1 \leq n \leq 10$, s_n steeds een kwadraat is. Nader onderzoek toont aan dat voor $1 \leq n \leq 10$,

$$\sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2.$$

We bewijzen dit nu voor alle $n \in \mathbb{N}_0$. Neem als induktiebasis 1. We hebben reeds aangetoond dat voor $n = 1$ deze formule geldig is. Neem nu $k \in \mathbb{N}_0$ willekeurig, en veronderstel dat de formule geldig is voor $n = k$. Dan is

$$\begin{aligned}
\sum_{i=0}^{k+1} i^3 &= \sum_{i=0}^{k} i^3 + (k+1)^3 \\
&\overset{\text{IH}}{=} \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 \\
&= \left[\frac{(k+1)(k+2)}{2}\right]^2
\end{aligned}$$

waaruit het gestelde volgt voor $n = k + 1$. Wegens het induktieprincipe is het gestelde weerom bewezen voor alle $n \in \mathbb{N}_0$.

Oefening 1.3.4 *Gebruik het sterk induktieprincipe om aan te tonen dat u_n recursief gedefinieerd als*

$$u_1 = 3,\ u_2 = 5,\ u_n = 3u_{n-1} - 2u_{n-2}\ (n \geq 3),$$

gelijk is aan $2^n + 1$ voor elke $n \in \mathbb{N}_0$.

Oplossing. Neem 1 als induktiebasis. Men verifieert eenvoudig dat $u_1 = 2^1 + 1$, m.a.w. het gestelde geldt voor $n = 1$. Neem nu een willekeurige $k \in \mathbb{N}_0$ en veronderstel dat voor alle $l \in \mathbb{N}_0 : l \leq k$ geldt dat $u_l = 2^l + 1$. Dan volgt

$$\begin{aligned}
u_{k+1} &= 3u_k - 2u_{k-1} \\
&\overset{\text{IH}}{=} 3(2^k + 1) - 2(2^{k-1} + 1) \\
&= 2^{k+1} + 1
\end{aligned}$$

waaruit, wegens het induktieprincipe, het gestelde volgt.

Oefening 1.3.5 *Zoek het kleinste positieve natuurlijk getal n_0 waarvoor geldt dat $n! \geq 2^n$. Indien $n = n_0$ als induktiebasis genomen wordt, bewijs dan het resultaat voor alle $n \geq n_0$.*

Oplossing. Berekening voor $n \in \{1, 2, 3\}$ toont dat $n! < 2^n$ en $4! \geq 2^4$, dus het kleinste positieve natuurlijke getal n_0 dat aan de gestelde voorwaarde voldoet is 4. Nu moeten we bewijzen dat $n! \geq 2^n$ voor alle $n \geq 4$. Neem daartoe induktiebasis 4 en veronderstel dat $k \geq 4$ met $k! \geq 2^k$. Dan is $(k+1)! = (k+1)k! \geq 2k! \geq 2 \cdot 2^k \geq 2^{k+1}$, waaruit wegens het induktieprincipe volgt dat $n! \geq 2^n$ voor alle $n \geq 4$.

Oefening 1.3.6 *Bewijs door middel van induktie dat*

$$\sum_{i=1}^{2^n} \frac{1}{i} \geq 1 + \frac{n}{2}. \tag{1.3}$$

Oplossing. Neem als induktiebasis 0, dan ziet men onmiddellijk dat (1.3) geldt voor $n = 0$. Kiezen we nu $k \in \mathbb{N}$ willekeurig en veronderstellen we dat de formule geldig is voor $n = k$, dan is

$$\begin{aligned}
\sum_{i=1}^{2^{k+1}} \frac{1}{i} &= \sum_{i=1}^{2^k} \frac{1}{i} + \sum_{i=1+2^k}^{2^{k+1}} \frac{1}{i} \\
&\overset{\text{IH}}{\geq} 1 + \frac{k}{2} + \sum_{j=1}^{2^k} \frac{1}{j + 2^k} \\
&\geq 1 + \frac{k}{2} + \sum_{j=1}^{2^k} \frac{1}{2^{k+1}} \\
&\geq 1 + \frac{k}{2} + \frac{2^k}{2^{k+1}} = 1 + \frac{k+1}{2}
\end{aligned}$$

waaruit, wegens het induktieprincipe, (1.3) geldig is voor alle $n \in \mathbb{N}$. Dit bewijst het gestelde.

Oefening 1.3.7 *Gebruik het induktieprincipe om te bewijzen dat voor elk natuurlijk getal n, $2^{n+2} + 3^{2n+1}$ deelbaar is door 7.*

Oplossing. Neem als induktiebasis 0. Het is eenvoudig na te gaan dat $7 \mid 2^{n+2} + 3^{2n+1}$ geldig is voor de induktiebasis. Kies nu $k \in \mathbb{N}$ willekeurig en veronderstel dat het gestelde geldig is voor $n = k$. Dan hebben we dat

$$\begin{array}{rcl} 7 & \mid & 2^{k+2} + 3^{2k+1} \\ & \Downarrow & \\ 7 & \mid & 2 \cdot (2^{k+2} + 3^{2k+1}) + 7 \cdot (3^{2k+1}) \\ & \Downarrow & \\ 7 & \mid & 2^{(k+1)+2} + 3^{2(k+1)+1} \end{array}$$

waaruit volgt dat het gestelde ook geldig is voor $n = k + 1$, en dus wegens het induktieprincipe geldig voor alle $n \in \mathbb{N}$.

Examen oefening 1 (1ste zit, 1998-1999) *Een palindromisch getal is een getal dat van achter naar voren gelezen hetzelfde getal oplevert (bvb. 1239321 en 2002 zijn palindromische getallen). Bewijs dat een palindromisch getal dat bestaat uit een even aantal cijfers steeds deelbaar is door 11.*

Oplossing. Het inductieve bewijs steunt op het feit dat wanneer je het eerste en het laatste cijfer van een palindromisch getal weg doet, je opnieuw een palindromisch getal bekomt. Stel dat P een palindromisch getal is dat bestaat uit $2k$ cijfers. Wanneer $k = 1$ dan is de bewering correct. Wanneer $k \geq 2$, dan is

$$\begin{array}{rcl} N & = & a_{2k-1}10^{2k-1} + a_{2k-2}10^{2k-2} + \cdots + a_k 10^k + \cdots + a_{2k-2}10^1 + a_{2k-1}10^0 \\ & = & a_{2k-1}(10^{2k-1} + 10^0) + (a_{2k-2}10^{2k-2} + \cdots + a_{2k-2}10^1), \end{array}$$

waarbij de a_i bepaalde getallen zijn $(i = k, \ldots, 2k-1)$.
Nu is $10^{2k-1} + 10^0 = \underbrace{100\cdots001}_{2k} = 11 \times \underbrace{9090\cdots9091}_{2k-2}$,
en ook $a_{2k-2}10^{2k-2} + \cdots + a_{2k-2}10^1$ is een veelvoud van 11 wegens de induktiehypothese.

Extra Oefening 2 *Voor $n \geq 1$, zij*

$$S_n = 1^2 + 3^2 + \ldots + (2n-1)^2,$$

som van de kwadraten van de eerste n oneven getallen.

(a) Bewijs dat $S_n = n(2n-1)(2n+1)/3$.

(b) Bepaal het laatste cijfer van S_n *met* n *een veelvoud van 5.*

Oplossing.

(a) Het bewijs is door inductie. Voor $n = 1$ geldt de formule. Stel nu dat de formule geldig is voor n, dan moet ze ook gelden voor $n+1$. Neem

$$\begin{aligned} S_{n+1} &= S_n + (2n+1)^2 \\ &\quad \text{(inductiehypothese)} \\ &= \frac{n(2n-1)(2n+1)}{3} + (2n+1)^2 \\ &= (2n+1)\left(\frac{n(2n-1)}{3} + (2n+1)\right) \\ &= (2n+1)\cdot\frac{(n+1)(2n+3)}{3} \\ &= \frac{(n+1)(2(n+1)-1)(2(n+1)+1)}{3}. \end{aligned}$$

De formule geldt inderdaad ook voor $n+1$.

(b) Stel $n = 5k$, dan is

$$\begin{aligned} S_{5k} &\equiv \frac{5k(10k-1)(10k+1)}{3} \pmod{10} \\ &\Updownarrow \quad (3^{-1} \equiv 7 \pmod{10}) \\ &\equiv 35k(10k-1)(10k+1) \pmod{10} \\ &\Updownarrow \quad \text{(alle veelvouden van 10 mogen weggelaten worden)} \\ &\equiv 5k(-1)(+1) \pmod{10} \\ &\Updownarrow \\ &\equiv -5k \pmod{10}. \end{aligned}$$

Als k oneven is, dan is $S_{5k} \equiv 5 \pmod{10}$ en als k even is, dan is $S_{5k} \equiv 0 \pmod{10}$.

1.4 Het ladenprincipe van Dirichlet

Oefening 1.4.1 *Bewijs dat een willekeurige verzameling van 12 gehele getallen ten minste 2 elementen bezit waarvan het verschil deelbaar is door 11.*

Oplossing. Zij $S = \{a_1, a_2, \ldots, a_{12}\}$ een verzameling van 12 gehele getallen. Beschouw de afbeelding $\sigma : S \to \mathbb{N}[1, 11]$, bepaald door elke a_i af te beelden op zijn positieve rest na deling door 11. Wegens het ladenprincipe is er minstens 1 beeld, waarvoor er 2 originelen, a_i en a_j $(i \neq j)$, in S bestaan. Dus $11 \mid a_i - a_j$, wat we moesten aantonen.

Oefening 1.4.2 *Hoeveel elementen moet een deelverzameling M van $\mathbb{N}[1, 999]$ minstens hebben om alleszins twee elementen met som 1000 te bevatten?*

Oplossing. Beschouw de afbeelding $\sigma : M \to \mathbb{N}[1, 500]$ bepaald door $m \in M$ af te beelden op $\min\{m, 1000 - m\}$. Het is duidelijk dat voor elementen m_1, $m_2 \in M : m_1 + m_2 = 1000$ als en slechts als $m_1^\sigma = m_2^\sigma$. Dus een deelverzameling M van $\mathbb{N}[1, 999]$ moet minstens 501 elementen bevatten zodat we er zeker van kunnen zijn dat ze twee elementen bevat waarvan de som 1000 is.

Oefening 1.4.3 *Zij gegeven een rij van m gehele getallen a_1, a_2, a_3, $\cdots$, a_m. Toon aan dat er een aantal a_i's kunnen gevonden worden zodanig dat ze in de rij mekaar opvolgen en waarvan de som deelbaar is door m.*

Oplossing. Stel $A_k = \bigcup_{i=0}^{k} \{a_i\}$ en beschouw de afbeelding $\sigma : \{A_k \parallel k \in \mathbb{N}[1, m]\} \to \mathbb{N}[0, m-1]$ waarbij A_k afgebeeld wordt op de positieve rest van de som van zijn elementen na deling door m. Indien 0 bereikt wordt dan geldt het gestelde. Indien 0 niet bereikt wordt, dan bestaat er een beeld dat minstens 2 originelen heeft (wegens het ladenprincipe), nl A_l en A_k (stel $l > k$). Maar dan is $m \mid \sum_{i=0}^{l} a_i - \sum_{j=0}^{k} a_j = \sum_{i=k+1}^{l} a_i$, wat het gestelde bewijst.

Oefening 1.4.4 *Veronderstel dat X een deelverzameling is van $\mathbb{N}[1, 2n]$. Bewijs dat, in de veronderstelling dat X $(n+1)$ elementen bevat, steeds één van de elementen van X een deler is van een ander element van X zodanig dat het quotient even is.*

Oplossing. Beschouw de afbeelding die elk element van X afbeeldt op zijn unieke priemontbinding waarbij de machten van 2 weggelaten zijn, dan zien we onmiddellijk in dat elk beeld oneven is en kleiner dan $2n$. Dus er zijn maximaal n beelden. Aangezien $|X| = n+1$, zullen twee beelden samenvallen. Stel $x_1,\ x_2 \in X : x_1 \neq x_2$ en $x_1^\sigma = x_2^\sigma$. Dus als $x_1 > x_2$ dan zal x_1/x_2 een macht zijn van 2. Hieruit volgt het gestelde.

Oefening 1.4.5 *In het eenheidsvierkant liggen 51 punten. Bewijs dat er een cirkelschijf met straal* $1/7$ *bestaat die minstens 3 van de 5 punten bedekt.*

Oplossing. Wegens het ladenprincipe van Dirichlet is het voldoende aan te tonen dat we het eenheidsvierkant kunnen bedekken met 25 schijfjes met straal kleiner dan of gelijk aan $\frac{1}{7}$. Daartoe verdelen we het vierkant in 25 gelijke vierkantjes geschikt volgens 5 rijen en 5 kolommen waarvan we de 25 omschrijvende cirkelschijfjes beschouwen. Elk vierkantje heeft diagonaal $\sqrt{\frac{2}{25}}$, waardoor zijn omschrijvende cirkelschijf straal $\sqrt{\frac{1}{50}}$ heeft. Het gestelde volgt nu uit het feit dat $\sqrt{\frac{1}{50}} < \sqrt{\frac{1}{49}} = \frac{1}{7}$.

Examen oefening 3 (1ste zit, 1994-1995) *Hoeveel personen moet men minimaal samenbrengen om zeker te zijn dat er zich onder hen minstens twee personen bevinden die geboren zijn op dezelfde dag van de week en in dezelfde maand?*

Oplossing. Het aantal paren (M, D) met $M \in \{\text{januari}, \ldots, \text{december}\}$ en $D \in \{\text{maandag}, \ldots, \text{zondag}\}$ is gelijk aan $\sum_M |\{D \parallel D \text{ dag van } M\}| = 12 \cdot 7$. Dus als we er zeker van willen zijn dat er 2 personen in dezelfde maand en op dezelfde dag van de week geboren zijn, moet het aantal personen strict groter zijn dan $7 \cdot 12$.

Examen oefening 4 (2de zit, 1998-1999) *Zij* $X = \{1, 2, 3, \ldots, 2n\}$ *en stel dat* D *een deelverzameling is van* X *met* $n+1$ *elementen. Toon aan dat* D *twee getallen bevat zodanig dat het ene deelbaar is door het andere.*

Oplossing. Definieer O als de verzameling van oneven getallen in X, en E de verzameling van even getallen in X. Definieer eveneens d als het aantal elementen in $D \cap O$.

We bewijzen dat er twee getallen k, l bestaan in D zodat $l = 2k$. Indien dit niet het geval zou zijn, dan zou $|D| = |D \cap O| + |D \cap E| \leq d + (n - d) = n$, duidelijk een tegenstrijdigheid.

Examen oefening 5 (1ste zit, 1999-2000) *Toon aan dat elke verzameling van drie verschillende positieve getallen twee elementen x en y bevat zodanig dat $x^3y - xy^3$ deelbaar is door 10.*

Oplossing. Stel $f(x, y) = x^3y - xy^3$. Er geldt dat $f(x, y) = xy(x - y)(x + y)$ zodat voor elke keuze van de getallen x en y, $f(x, y)$ een even getal is. Daarom is het voldoende om te bewijzen dat $f(x, y)$ deelbaar is door 5. Dit is het geval als en slechts als x of y deelbaar is door 5, of wanneer de som of het verschil van twee van hen deelbaar is door 5. Veronderstel dat noch x noch y deelbaar is door 5. Het laatste cijfer van elk getal dat niet deelbaar is door 5 behoort tot de verzameling $A = \{1, 2, 3, 4, 6, 7, 8, 9\}$. Beschouw nu de twee verzamelingen $B = \{1, 4, 6, 9\}$ en $C = \{2, 3, 7, 8\}$. Van de drie elementen in onze verzameling, zijn er dus minstens twee waarvan het laatste cijfer tot B behoort of minstens twee waarvan het laatste cijfer tot C behoort. Dit betekent dat in elk van beide gevallen, de som of het verschil van die twee getallen deelbaar is door 5. Dit bewijst het gestelde.

Examen oefening 6 (2de zit, 1999-2000) *Tien punten worden willekeurig gekozen binnen een gelijkzijdige driehoek. De lengte van 1 zijde bedraagt 3 eenheden. Toon aan dat er twee punten bestaan die op een afstand liggen van elkaar van minder dan één eenheid.*

Oplossing. Verdeel de gelijkzijdige driehoek in 9 gelijkzijdige deeldriehoeken met zijde 1. Dan moet wegens het ladenprincipe er minstens 1 driehoek bestaan die 2 punten x en y bevat. Beschouw nu de cirkel met straal 1 en middelpunt x, dan zal deze alle hoekpunten van onze deeldriehoek bevatten en daardoor dus ook de ganse deeldriehoek. Hieruit volgt dat de afstand tussen x en y kleiner is of gelijk aan 1.

Extra Oefening 7 *Op een kermisrad staan de nummers 1, 2, ..., 36 in een willekeurige volgorde geschreven. Toon aan dat, wat die volgorde ook is, er steeds 3 opeenvolgende nummers op het rad gevonden kunnen worden met som groter dan 54.*

Oplossing. Zij x_1 een nummer op het rad. Duid daarna, in wijzerzin tellend, de andere nummers op het rad aan met $x_2, \ldots, x_{36}$. Stel nu dat welke drie opeenvolgende nummers ook genomen worden, de som van de getallen steeds kleiner is dan 55. Dus $x_1+x_2+x_3 \leq 54, x_2+x_3+x_4 \leq 54, \ldots, x_{34}+x_{35}+x_{36} \leq 54, x_{35}+x_{36}+x_1 \leq 54$ en $x_{36}+x_1+x_2 \leq 54$. Dan is

$$\begin{array}{rcl} (x_1+x_2+x_3)+\cdots+(x_{36}+x_1+x_2) & \leq & 36 \cdot 54 \\ & \Updownarrow & \\ 3\displaystyle\sum_{i=1}^{36} x_i & \leq & 36 \cdot 54 \\ & \Updownarrow & \\ 3 \cdot \dfrac{36 \cdot 37}{2} & \leq & 36 \cdot 54 \\ & \Updownarrow & \\ 1998 & \leq & 1944. \end{array}$$

Dit is vals.

Extra Oefening 8 *In een maand bestaande uit 30 dagen speelt een team ten minste één wedstrijd per dag, maar niet meer dan 45 wedstrijden. Toon aan dat er een periode is bestaande uit een aantal opeenvolgende dagen waarin het team precies 14 wedstrijden speelt.*

Oplossing. Zij a_j het aantal wedstrijden die gespeeld zijn tot en met de $j$de dag. Dan is $a_1,\ a_2,\ \ldots,\ a_{30}$ een strikt stijgende rij getallenm met $1 \leq a_j \leq 45$. Verder is $a_1+14,\ a_2+14,\ \ldots, a_{30}+14$ ook een strikt stijgende rij met $15 \leq a_j+14 \leq 59$. Hieruit volgt dat $a_1,\ a_2,\ \ldots, a_{30},\ a_1+14,\ a_2+14,\ \ldots, a_{30}+14$ 60 gehele getallen zijn gelegen in $\mathbb{N}[1, 59]$, dus er bestaan twee dergelijke getallen die gelijk zijn, en aangezien de twee afzonderijke rijen strikt stijgen moeten de twee getallen beide tot een andere rij behoren. Dus er bestaan i en j zodat $a_i = a_j + 14$.

Extra Oefening 9 *Tijdens een voetbaltornooi van 15 dagen werden er 20 wedstrijden gespeeld. Elke dag werd er minstens 1 keer gespeeld. Toon aan dat er een periode van opeenvolgende dagen was waarin er precies 9 wedstrijden werden gespeeld.*

Oplossing. De oefening wordt volledig analoog opgelost als de voorgaande. Zij dus a_j het aantal wedstrijden die gespeeld werden na de j-de dag, $j \in \{1, \ldots, 15\}$, dan geldt $1 \leq a_j \leq 20$. Anderzijds zal dus $10 \leq a_j + 9 \leq 29$. Indien er een i en een j bestaat waarvoor $a_i = a_j + 9$, dan werden er op de opeenvolgende dagen $\{\text{dag } j+1, \text{dag } j+2, \ldots, \text{dag } i\}$ net 9 wedstrijden gespeeld. Indien dit dus niet het geval zou zijn, dan zouden we 30 verschillende getallen $a_1, \ldots, a_{15}, a_1 + 9, \ldots, a_{15} + 9$ gevonden hebben die allen in $\{1, \ldots, 29\}$ gelegen zijn, een strijdigheid.

1.5 Eindige en oneindige verzamelingen

1.5.1 Definities

1.5.2 Opmerking

1.5.3 Kardinaaalgetallen

1.6 Het vereenvoudigd somprincipe

1.7 Het produktprincipe

Oefening 1.7.1 *Veronderstel dat we een verzameling M van verschillende deelverzamelingen van $\mathbb{N}[1,8]$ beschouwen zodanig dat elke deelverzameling 4 elementen bevat en dat elk element van $\mathbb{N}[1,8]$ tot 3 dergelijke deelverzamelingen behoort. Hoeveel dergelijke deelverzamelingen zijn er dan?*

Oplossing. Beschouw de deelverzameling $S = \{(n, D) \in \mathbb{N}[1,8] \times M \parallel n \in D\}$ van $\mathbb{N}[1,8] \times M$, dan is $r_n(S) = 3$ voor alle $n \in \mathbb{N}[1,8]$ en $k_D(S) = 4$ voor alle $D \in M$. Wegens het produktprincipe, bekomen we

$$\begin{array}{rcl} \displaystyle\sum_{n \in \mathbb{N}_{[1,8]}} r_n(S) & = & \displaystyle\sum_{D \in M} k_D(S) \\ & \Downarrow & \\ 3 \cdot |\mathbb{N}[1,8]| & = & 4 \cdot |M| \\ & \Downarrow & \\ |M| & = & 6. \end{array}$$

Oefening 1.7.2 *Is het mogelijk om een verzameling M van deelverzamelingen van $\mathbb{N}[1,8]$ te vinden zodanig dat elke deelverzameling 3 elementen bevat, en zodanig dat elk element van $\mathbb{N}[1,8]$ tot 5 deelverzamelingen behoort?*

Oplossing. Dezelfde redenering als hierboven zou impliceren dat

$$|M| \cdot 3 = 8 \cdot 5$$

waaruit zou volgen $3 \mid 8 \cdot 5$, een strijdigheid. Dus een dergelijke verzameling M bestaat niet.

Oefening 1.7.3 *Indien X_1, X_2, X_3, ..., X_n verzamelingen zijn (eventueel gelijk), dan wordt $X_1 \times X_2 \times \cdots \times X_n = \{(x_1, x_2, \ldots, x_n) \parallel x_i \in X_i\}$ de* produktverzameling *van X_1, X_2, ..., X_n genoemd. Bewijs door middel van het induktieprincipe dat*

$$|X_1 \times X_2 \times \cdots \times X_n| = |X_1| \cdot |X_2| \cdot \ldots \cdot |X_n|$$

Oplossing. Neem als induktiebasis 1, dan zien we onmiddellijk dat de oefening voldaan is voor $n = 1$. Zij nu $k \in \mathbb{N}_0$ willekeurig zodat de formule geldt voor alle $n \leq k$ (sterk induktieprincipe toepassen). Dan is

$$\begin{array}{rcl} |X_1 \times X_2 \times \cdots \times X_{k+1}| & = & |X_1 \times (X_2 \times \cdots \times X_{k+1})| \\ & \Downarrow & \text{IH} \\ & = & |X_1| \cdot |X_2 \times X_3 \times \cdots \times X_{k+1}| \\ & \Downarrow & \text{IH} \\ & = & |X_1| \cdot |X_2| \cdot \ldots \cdot |X_{k+1}| \end{array}$$

waaruit, wegens het induktieprincipe, het gestelde volgt.

Examen oefening 10 (1ste zit, 1995-1996) *Een bedrijf dat steekproeven organiseert bezit een databank met gegevens van n personen. De databank bezit deelverzamelingen van grootte k ($k < n$), blokken genoemd, zodat als t willekeurige personen genomen worden, er precies λ blokken zijn die deze t*

personen bevatten ($t < k$). Zij $t' < t$ en beschouw t' verschillende personen. Bewijs dat er precies

$$\lambda \binom{v-t'}{t-t'} / \binom{k-t'}{t-t'}$$

blokken zijn die deze t' personen bevatten.

Oplossing. Gegeven een groepje G' van t' personen, dan kan je deze op $\binom{n-t'}{t-t'}$ manieren uitbreiden tot een groep G van t personen. Door elk zo'n uitgebreide groep G bestaan er juist λ blokken. Als we nu $\mathcal{B}'$ definiëren als de verzameling van blokken door G' en $\mathcal{T}'$ als de verzameling van uitgebreide groepjes G, dan vinden we wegens het productprincipe (tel de paren $(B, T) \in \mathcal{B}' \times \mathcal{T}'$ zodat $T \subseteq B$) dat

$$\begin{aligned} \sum_{b \in \mathcal{B}'} |\{T \in \mathcal{T}' \parallel T \subseteq B\}| &= \sum_{T \in \mathcal{T}'} |\{B \in \mathcal{B}' \parallel T \subseteq B\}| \\ |\mathcal{B}'| \cdot \binom{k-t'}{t-t'} &= \binom{n-t'}{t-t'} \cdot \lambda. \end{aligned}$$

Examen oefening 11 (2de zit, 1995-1996) *Veronderstel dat X een verzameling is met cardinaliteit n en dat $\mathcal{U}$ de verzameling van deelverzamelingen van X met cardinaliteit d ($d \leq n$) is. De elementen van $\mathcal{U}$ zijn zodanig gekozen dat elke deelverzameling van kardinaliteit t (t een vast gekozen getal, waarvoor $d \leq t \leq n$) precies 1 element van $\mathcal{U}$ als deelverzameling bevat. Veronderstel nu dat S een deelverzameling is van X met $|S| = i$, $t \leq i \leq n$. Bereken dan het aantal elementen van $\mathcal{U}$ die bevat zijn in S.*

Oplossing. Zij S een deelverzameling van grootte i. Het is mogelijk om op $\binom{i}{t}$ manieren t elementen te kiezen uit dit groepje S van i elementen. Elk groepje van t elementen bevat één element uit $\mathcal{U}$; dit zijn allemaal deelverzamelingen A van grootte d die bevat zijn in S. Een dergelijk element A uit $\mathcal{U}$ is echter verschillende keren geteld. Namelijk, elk element A van $\mathcal{U}$ dat in S bevat is, wordt precies $\binom{i-d}{t-d}$ keer geteld, want de d elementen van A kunnen op $\binom{i-d}{t-d}$ manieren uitgebreid worden tot een verzameling van t elementen volledig bestaande uit elementen van S.

Dit toont aan dat er precies $\binom{i}{t} / \binom{i-d}{t-d}$ elementen van $\mathcal{U}$ zijn die bevat zijn in S.

1.8 Het eenvoudig inclusie-exclusie principe

1.9 Kombinatieleer

1.9.1 Variaties

1.9.2 Permutaties

1.9.3 Kombinaties

1.9.4 Herhalingsvariaties

1.9.5 Herhalingskombinaties

Examen oefening 12 (1ste zit, 1991-1992) *De programmeertaal van Pastran aanvaardt variabelen van ten hoogste 6 karakters. Het eerste karakter moet een klinker zijn, terwijl elk ander eventueel karakter ofwel een klinker ofwel een oneven cijfer moet zijn. Hoeveel variabelen kunnen er in Pastran gebruikt worden?*

Oplossing. Er zijn 5 mogelijkheden voor de klinkers, namelijk a, e, i, o, u. Dus zijn er 5 mogelijkheden voor het eerste karakter.

Voor de volgende karakters kiezen we steeds uit de verzameling $\{a, e, i, o, u, 1, 3, 5, 7, 9\}$. Dus zijn er hier 10 mogelijkheden.

Dit geeft dan de volgende tabel voor het aantal variabelen van lengte 1 tot 6:

variabele van 1 letter	5 mogelijkheden
variabele van 2 letters	$5 \cdot 10$ mogelijkheden
variabele van 3 letters	$5 \cdot 10^2$ mogelijkheden
variabele van 4 letters	$5 \cdot 10^3$ mogelijkheden
variabele van 5 letters	$5 \cdot 10^4$ mogelijkheden
variabele van 6 letters	$5 \cdot 10^5$ mogelijkheden

In totaal zijn er dus $5 \cdot (1 + 10 + 10^2 + \cdots + 10^5) = 555555$ mogelijke variabelen.

Examen oefening 13 (2de zit, 1991-1992) *Hoeveel geordende 5-tallen $(x_1, x_2, \ldots, x_5)$ bestaande uit 5 oneven natuurlijke getallen x_1, x_2, …, x_5 bestaan er waarvoor $x_1 + x_2 + x_3 + x_4 + x_5 = 25$?*

Oplossing. Daar alle getallen $x_i, i = 1, \ldots, 5$, oneven zijn, kunnen ze geschreven worden als $x_i = 2y_i + 1$.

Nu is

$$(2y_1 + 1) + \cdots + (2y_5 + 1) = 25$$

equivalent met

$$y_1 + \cdots + y_5 = 10.$$

Het aantal oplossingen hiervoor is $\overline{\left(\begin{array}{c} 5 \\ 10 \end{array} \right)} = \left(\begin{array}{c} 14 \\ 10 \end{array} \right) = 1001.$

Examen oefening 14 (2de zit, 1992-1993) *Hoeveel oplossingen natuurlijke getallen* $(x_1, \ldots, x_6)$ *zijn er voor de vergelijking* $x_1 + \ldots + x_6 = 31$ *met* $x_1, \ldots, x_4 \equiv 1 \pmod 3$ *en* $x_5 \equiv x_6 \equiv 0 \pmod 3$*?*

Oplossing. Daar $x_1, \ldots, x_4 \equiv 1 \pmod 3$ en $x_5, x_6 \equiv 0 \pmod 3$, stel $x_1 = 3y_1 + 1, x_2 = 3y_2 + 1, x_3 = 3y_3 + 1, x_4 = 3y_4 + 1$ en $x_5 = 3y_5, x_6 = 3y_6$.

Dit geeft

$$\begin{array}{rcl} x_1 + \cdots + x_6 & = & 31 \\ & \Updownarrow & \\ (3y_1 + 1) + \cdots + (3y_4 + 1) + 3y_5 + 3y_6 & = & 31 \\ & \Updownarrow & \\ y_1 + \cdots + y_6 & = & 9. \end{array}$$

Het aantal oplossingen hiervoor is

$$\overline{\left(\begin{array}{c} 6 \\ 9 \end{array} \right)} = \left(\begin{array}{c} 14 \\ 9 \end{array} \right) = 2002.$$

Examen oefening 15 (1ste zit, 1993-1994) *Hoeveel natuurlijke getallen met hoogstens 4 cijfers bestaan er zodanig dat de cijfers van links naar rechts stijgen (strikt stijgen of gelijk blijven) met betrekking tot de natuurlijke orderelatie?*

Oplossing. Schrijf elk getal met hoogstens 4 cijfers als $a_0a_1a_2a_3$ met eventueel de voorste getallen gelijk aan nul.

Dan bepalen a_0, a_1, a_2, a_3 een ongeordend 4-tal, met eventueel herhaling, uit $\mathbb{N}[0, 9]$.

Omgekeerd bepaalt elk ongeordend 4-tal a_0, a_1, a_2, a_3, waarin herhaling toegelaten is, uit $\mathbb{N}[0, 9]$ één getal met hoogstens 4 cijfers zodat de cijfers van links naar rechts stijgen.

Bijgevolg zijn er precies $\overline{\binom{10}{4}} = 715$ dergelijke getallen.

Examen oefening 16 (2de zit, 1993-1994) *(a) Hoeveel woorden (zonder betekenis) van 26 letters kan men vormen als elke letter uit het alfabet tot 26 keer gebruikt mag worden?*

(b) Als een letter uit het alfabet hoogstens 25 keer mag voorkomen, hoeveel woorden (zonder betekenis) met 26 letters kunnen er dan gevormd worden?

Oplossing.

(a) Dit aantal is 26^{26}.

(b) Als een letter hoogstens 25 keer gebruikt mag worden, dan moeten enkel de woorden bestaande uit 26 keer dezelfde letter weggelaten worden.

Dus zijn er nog $26^{26} - 26$ woorden over.

Examen oefening 17 (1ste zit, 1994-1995) *Hoeveel permutaties van de 26 letters van het alfabet bevatten geen enkele van de drie woorden: hond, poes, muis?*

Oplossing. Het is onmiddellijk duidelijk dat als 'poes' voorkomt, dan niet 'hond' en 'muis'. Het gevraagde aantal is dus het verschil van het totale aantal permutaties en de permutaties die ofwel 'poes' bevatten, ofwel 'hond' of 'muis' bevatten.

We tellen het aantal permutaties die 'poes' bevatten. Beschouw daarom 'poes' als 1 letter van het alfabet. Dan is het aantal permutaties van dit nieuwe alfabet gelijk aan 23!.

We tellen het aantal permutaties die 'hond' of 'muis' bevatten. Zij die 'hond' bevatten zijn met 23!, net als zij die 'muis' bevatten. Maar dan hebben

we de permutaties die 'hond' en 'muis' bevatten dubbel geteld, en dit aantal bedraagt 20!. Het aantal permutaties die 'hond' of 'muis' bevatten is dus $2 \cdot 23! - 22!$.

Het antwoord is:

$$26! - [23! + (2 \cdot 23! - 20!)].$$

Examen oefening 18 (1ste zit, 1995-1996) *Bij het pokerspel krijgt iedere speler bij de aanvang van het spel vijf kaarten. Er wordt gepeeld met 52 kaarten en er zijn 13 soorten kaarten, namelijk de nummers 1 tot en met 10, boer, dame en heer, en binnen elke soort zijn er 4 kaarten, namelijk harten, klaveren, ruiten en schoppen.*

(a) Hoeveel mogelijke vijftallen kaarten kan een speler toebedeeld krijgen?

(b) Op hoeveel manieren kan een speler elk van de volgende combinaties toebedeeld krijgen bij de aanvang van het spel:

(b.1) Four of a kind: vier van eenzelfde soort + een vijfde van een andere soort;

(b.2) Full house: drie van eenzelfde soort + twee van eenzelfde soort verschillend van de eerste soort;

(b.3) Three of a kind: drie van eenzelfde soort + vierde van een andere soort + vijfde van nog een andere soort;

(b.4) Two pair: twee van eenzelfde soort + twee van eenzelfde andere soort + vijfde van nog een andere soort;

(b.5) One pair: slechts twee van dezelfde soort, alle andere van verschillende soort niet gelijk aan de eerste soort.

Oplossing.

Als de volgorde niet belangrijk is:

(a) $\binom{52}{5}$

(b.1) Eerst kiezen we 1 soort uit 13: $\binom{13}{1}$; gevolgd door de keuze van 4 kaarten van deze soort: $\binom{4}{4}$.
Dan kiezen we nog 1 soort maar nu slechts uit 12: $\binom{12}{1}$; gevolgd door de keuze van 1 kaart van deze soort: $\binom{4}{1}$.
Het aantal combinaties die 'Four of a kind' opleveren is $(\binom{13}{1} \cdot \binom{4}{4}) \cdot (\binom{12}{1} \cdot \binom{4}{1})$.

(b.2) Analoog. $(\binom{13}{1} \cdot \binom{4}{3}) \cdot (\binom{12}{1} \cdot \binom{4}{2})$

(b.3) Analoog. $(\binom{13}{1} \cdot \binom{4}{3}) \cdot (\binom{12}{1} \cdot \binom{4}{1}) \cdot (\binom{11}{1} \cdot \binom{4}{1})$

(b.4) Analoog. $(\binom{13}{1} \cdot \binom{4}{2}) \cdot (\binom{12}{1} \cdot \binom{4}{2}) \cdot (\binom{11}{1} \cdot \binom{4}{1})$

(b.5) Analoog. $(\binom{13}{1} \cdot \binom{4}{2}) \cdot (\binom{12}{1} \cdot \binom{4}{1}) \cdot (\binom{11}{1} \cdot \binom{4}{1}) \cdot (\binom{10}{1} \cdot \binom{4}{1})$

Als de volgorde belangrijk is:

(a) $52 \cdot 51 \cdot 50 \cdot 49 \cdot 48$

(b.1) Dit zijn dan alle permutaties van de eerder gevonden combinaties in (b.1), meer concreet kan je elke 'Four of a kind' op 5! manieren toebedeeld krijgen, wat oplevert dat het gezochte aantal gelijk is aan $5! \cdot (4 \cdot \binom{13}{4}) \cdot (3 \cdot 13)$.

(b.2) $5! \cdot (\binom{13}{1} \cdot \binom{4}{3}) \cdot (\binom{12}{1} \cdot \binom{4}{2})$

(b.3) $5! \cdot (\binom{13}{1} \cdot \binom{4}{3}) \cdot (\binom{12}{1} \cdot \binom{4}{1}) \cdot (\binom{11}{1} \cdot \binom{4}{1})$

(b.4) $5! \cdot (\binom{13}{1} \cdot \binom{4}{2}) \cdot (\binom{12}{1} \cdot \binom{4}{2}) \cdot (\binom{11}{1} \cdot \binom{4}{1})$

(b.5) $5! \cdot (\binom{13}{1} \cdot \binom{4}{2}) \cdot (\binom{12}{1} \cdot \binom{4}{1}) \cdot (\binom{11}{1} \cdot \binom{4}{1}) \cdot (\binom{10}{1} \cdot \binom{4}{1})$

Examen oefening 19 (2de zit, 1995-1996) *Hoeveel woorden (met of zonder betekenis) van 26 letters kan men vormen zodanig dat elke letter uit het alfabet een onbeperkt aantal keren mag voorkomen en zodanig dat de letters in het woord van links naar rechts alfabetisch zijn gerangschikt?*

Oplossing. Men ziet in dat dit gelijk is aan het aantal oplossingen $(n_a, n_b, n_c, \ldots, n_x, n_y, n_z) \in \mathbb{N}[0, 26]^{26}$ waarvoor geldt dat $n_a + n_b + n_c + \cdots + n_x + n_y + n_z = 26$. Dit aantal wordt bepaald door

$$\overline{\binom{26}{26}} = \binom{26 + 26 - 1}{26}.$$

Examen oefening 20 (1ste zit, 1996-1997) *Een boodschap die bestaat uit 12 verschillende symbolen moet worden doorgeseind. Naast de 12 symbolen, zal de transmittor 45 blanco ruimten tussen de symbolen doorzenden, met tussen elke 2 verschillende symbolen minstens 3 blanco ruimten. Op hoeveel manieren kan de boodschap doorgeseind worden?*

Oplossing. Als de boodschap vast ligt, moeten we enkel het aantal mogelijkheden tellen waarop we de blanco ruimten kunnen tussen voegen, zodat tussen elke twee symbolen minstens 3 blanco ruimten zitten. We zien in dat dit gelijk is aan het aantal oplossingen $(r_1, r_2, \ldots, r_{11}) \in \mathbb{N}$, waarvoor

$$r_1 + r_2 + \cdots + r_{11} = 45$$

waarbij $r_i \geq 3$, voor alle $i \in \{1, \ldots, 11\}$. En dit is gelijk aan het aantal oplossingen $(v_1, v_2, \ldots, v_{11}) \in \mathbb{N}$ die voldoen aan $v_1 + v_2 + \cdots + v_{11} = 12$ (definiëer v_i als $r_i - 3$), wat gegeven wordt door $\overline{\binom{12}{11}} = \binom{12+11-1}{11} = \binom{22}{11}$.

Indien de boodschap nog moet gevormd worden (dit kan op 12! manieren), dan vinden we dus

$$12! \cdot \binom{22}{11}$$

als antwoord.

Examen oefening 21 (1ste zit, 1997-1998) *Je beschikt over een gewoon kaartspel van 52 kaarten. Je trek hieruit 5 kaarten, de volgorde is van geen belang.*

(a) Hoeveel mogelijke kaartenvijftallen zijn er die juist één paar gelijkwaardige kaarten bevatten, dus bijvoorbeeld 2 Azen of 2 drieën of 2 Dames? (Let op: drie of vier gelijkwaardige kaarten of twee dergelijke paren worden uitgesloten.)

(b) Hoeveel mogelijkheden zijn er die minstens één paar van dezelfde waarde bevatten? (Eén paar, twee paren, drie of vier kaarten van dezelfde soort zijn nu allemaal wel toegelaten.)

Oplossing.

(a) Als we de kaarten verdelen per waarde, dan krijgen we 13 stapeltjes van 4 kaarten. We kiezen het stapeltje waaruit we 2 kaarten willen trekken (dit kan op 13 manieren), dan kiezen we uit dit stapeltje 2 kaarten (dit kan op $\binom{4}{2} = 6$ manieren). Deze keuze combineren we dan met de keuze van 3 andere stapeltjes waaruit we elk 1 kaart trekken (dit kan op $(12 \cdot 4)(11 \cdot 4)(10 \cdot 4)$ manieren). Het totale aantal combinaties die net 1 paar van gelijkwaardige kaarten oplevert is dus $(13{\cdot}6)(12{\cdot}4)(11{\cdot}4)(10{\cdot}4)$.

(b) We tellen eerst de combinaties waarbij het maximale aantal gelijkwaardige kaarten gelijk is aan 2. In (a) telden we de combinaties met net 1 paar gelijkwaardige kaarten. Tellen we nu de combinaties met 2 paren, van verschillende waarde, op een analoge wijze, dan krijgen we $(\binom{13}{2}\binom{4}{2}\binom{4}{2})(11 \cdot 1)$.

Laat ons nu de combinaties tellen die juist 3 kaarten van eenzelfde waarde bevatten. Voor elke dergelijk combinaties vormen de 2 overblijvende kaarten een gelijkwaardig paar of net niet. In het eerste geval hebben we $(13 \cdot \binom{4}{3})(12 \cdot \binom{4}{2})$ mogelijkheden. In het tweede geval hebben we $(13 \cdot \binom{4}{3})(12 \cdot 1)(11 \cdot 1)$ mogelijkheden.

De resterende combinaties zijn die met 4 gelijkwaardige kaarten, en dit zijn er $(13 \cdot \binom{4}{4})(12 \cdot 1)$.

Het antwoord is dus de som van alle mogelijkheden:

$$(13 \cdot 6)(12 \cdot 4)(11 \cdot 4)(10 \cdot 4) + (\binom{13}{2}\binom{4}{2}\binom{4}{2})(11 \cdot 1)$$
$$+ (13 \cdot \binom{4}{3})(12 \cdot 1)(11 \cdot 1) + (13 \cdot \binom{4}{3})(12 \cdot \binom{4}{2})$$
$$+ (13 \cdot \binom{4}{4})(12 \cdot 1).$$

Examen oefening 22 (1ste zit, 1999-2000) *(a) Op hoeveel manieren kan men 24 mensen aan 4 ronde tafels van 6 personen schikken. Twee plaatsingen aan eenzelfde tafel noemen we gelijk als er een rotatie bestaat die de ene plaatsing afbeeldt op de andere.*

(b) Veronderstel nu dat er twaalf mannen en twaalf vrouwen zijn. Hoeveel mogelijke schikkingen zijn er als we elke man tussen twee vrouwen willen zetten en omgekeerd?

Oplossing.

(a) Eerst en vooral moeten we de 24 mensen verdelen in 4 groepjes van 6 personen, dit kan op

$$\frac{\binom{24}{6}\binom{18}{6}\binom{12}{6}\binom{6}{6}}{4!}$$

manieren. Nu moeten we voor elke groepje het aantal permutaties tellen die niet cyclisch verbonden zijn. We doen dit als volgt. Elke permutatie van 6 elementen is cyclisch verbonden met 6 permutaties (waaronder zichzelf!) en deze relatie is transitief. Met andere woorden, de verzameling van alle permutaties wordt onderverdeeld in disjuncte verzamelingen van cyclisch verbonden permutaties. Als we het aantal permutaties die niet cyclisch verbonden zijn voorstellen als n, dan krijgen we dus

$$6! = \sum_{i=1}^{n} 6$$

waaruit volgt dat $n = 5!$. Dit geldt nu voor elke tafel, zodat het gevraagde aantal schikkingen gelijk is aan dus

$$\frac{\binom{24}{6}\binom{18}{6}\binom{12}{6}\binom{6}{6}}{4!} \cdot 5!^4.$$

(b) Het is duidelijk dat het totale aantal mogelijkheden waarop we 3 mannen en 3 vrouwen aan een ronde tafel kunnen plaatsen, zodat personen van hetzelfde geslacht nooit naast elkaar mogen zitten, gelijk is aan $3 \cdot 3 \cdot 2 \cdot 2 \cdot 1 \cdot 1$. Daar nu elk dergelijke combinatie 6 cyclisch verbonden combinaties heeft, hebben we die ook 6 keer geteld. Dus het aantal mogelijkheden om 3 mannen en 3 vrouwen rond een tafel te plaatsen waarbij geen twee mogelijkheden verbonden zijn door rotatie, is gelijk aan 6.

Vooralleer we de personen aan de tafel schikken, verdelen we eerst de 12 mannen en de 12 vrouwen beide in 4 groepjes van 3. Dit kan op $(\binom{12}{3}\binom{9}{3}\binom{6}{3}/4!)^2$ manieren. Natuurlijk moeten we ook nog elk groepje van 3 mannen combineren met een groepje van 3 vrouwen, dit kan op 4! manieren.

Het totale aantal is dus $\left(\frac{\binom{12}{3}\binom{9}{3}\binom{6}{3}}{4!}\right)^2 \cdot 4! \cdot 6^4$.

Examen oefening 23 (1ste zit, 2001-2002) *Een vrouw wil de kluis van haar man kraken, en er met het geld vandoor gaan vooralleer hij thuis komt. De code $a_1a_2a_3a_4a_5$ bestaat uit 5 cijfers, allen bevat in $\mathbb{N}[0, 9]$, en ze weet dat het eerste en het laatste cijfer hun huisnummer vormt (huisnummer $= a_1a_5$). Het drukken van een code x vraagt 2 seconden. Bovendien heeft de kluis s_x seconden nodig om te verifiëren of de code x correct is, waarbij s_x gelijk is aan het aantal verschillende cijfers optredend in x. In welk tijdsbestek kan de vrouw de klus klaren als je weet dat*

(a) het eerste en het laatste cijfer gelijk zijn?

(b) het eerste en het laatste cijfer verschillend zijn?

Oplossing. Aangezien de vrouw het eerste en het laatste cijfer kent, resten er 10^3 mogelijkheden $x = x_1x_2x_3x_4x_5$. Stokkeer ze in een verzameling X. In het slechtste geval moet ze alle codes drukken ($2 \cdot 10^3$ seconden) en moet de kluis ze ook allemaal verifiëren ($\sum_{x \in X} s_x$ seconden). Het komt er dus op neer de laatste som te bepalen. We doen dit door X op te delen in vijf verzamelingen X_1, X_2, X_3, X_4, X_5 waarbij X_i gelijk is aan de verzameling van mogelijkheden bestaande uit i verschillende cijfers, en elke $|X_i|$ te tellen.

Het maximale aantal seconden wordt dan gegeven door

$$2 \cdot 10^3 + \sum_{x \in X} s_x = 2 \cdot 10^3 + \sum_{i=1}^{5} |X_i| \cdot i.$$

(a) Als het eerste en het laatste cijfer gelijk zijn, dan kunnen er geen 5 verschillende cijfers optreden, dus $|X_5| = 0$. Anderzijds is $X_1 = 1$ en $|X_4| = 9 \cdot 8 \cdot 7$.

Als $x \in X_2$, dan komt het eerste cijfer van x twee, drie of vier keer voor in x. Het aantal elementen van X_2 waarin het eerste cijfer 2 keer voorkomt is 9, het aantal elementen waarin het eerste cijfer 3 keer voorkomt is $\binom{3}{1} \cdot 9$, het aantal elementen waarin het eerste cijfer 4 keer voorkomt is $\binom{3}{2} \cdot 9$.

Als $x \in X_3$, dan zijn de 3 middelste cijfers van x ofwel verschillend van het eerste cijfer (en dan zijn er noodzakelijk twee gelijk), ofwel bestaat er een uniek cijfer onder hen dat gelijk is aan het eerste cijfer (waardoor de middelste cijfers zeker verschillend zijn). Het aantal cijfers in het eerste geval is $\binom{3}{2} \cdot 9 \cdot 8$, en het aantal in het tweede geval is $\binom{3}{1} \cdot 9 \cdot 8$.

De oplossing van (a) wordt dus gegeven door $2 \cdot 10^3 + 1 \cdot 1 + 9 \cdot (1 + \binom{3}{1} + \binom{3}{2}) \cdot 2 + 9 \cdot 8 \cdot (\binom{3}{2} + \binom{3}{1}) \cdot 3 + (9 \cdot 8 \cdot 7) \cdot 4$ seconden.

(b) Hier is $|X_1| = 0$ en $|X_5| = 8 \cdot 7 \cdot 6$.

Als $x \in X_2$, dan hebben we $2 \cdot 2 \cdot 2 \cdot$ mogelijkheden om de drie middelste cijfers te kiezen.

Als $x \in X_3$, dan komt er in x en cijfer c voor dat verschillend is aan het eerst en het tweede cijfer. We hebben nu drie mogelijkheden, namelijk, c komt 1,2 of 3 keer voor. In het eerste geval tellen we $(3 \cdot 8) \cdot 3 \cdot 3$ mogelijkheden, in het tweede geval tellen we $(3 \cdot 8) \cdot 3$ en tenslotte in het derde geval tellen we slechts 1 mogelijkheid.

Als $x \in X_4$, dan hebben we de volgende mogelijkheden voor x. Het eerste cijfer komt 2 keer voor, het laatste cijfer komt twee keer voor, of de drie middelste cijfers zijn verschillend van het eerste en het laatste (maar dan moeten er wel twee gelijk zijn). In het eerste geval tellen we $3 \cdot 8 \cdot 7$. In het tweede geval tellen we er eveneens $3 \cdot 8 \cdot 7$. En in het derde geval tellen we er nogmaals $3 \cdot 8 \cdot 7$.

De oplossing van (b) wordt dus gegeven door $2 \cdot 10^3 + 2^3 \cdot 2 + [(3 \cdot 8) \cdot 3 \cdot (3 + 1) + 1] \cdot 3 + (3 \cdot 8 \cdot 7)^3 \cdot 4 + (8 \cdot 7 \cdot 6) \cdot 5$ seconden.

Extra Oefening 24 *(a) Hoeveel natuurlijke getallen kleiner dan 100000 zijn er die bestaan uit verschillende cijfers?*

(b) Hoeveel natuurlijke getallen kleiner dan 1000000 zijn er die het cijfer 9 bevatten en waarvan de som van de cijfers gelijk is aan 13?

Oplossing.

(a) We beginnen met het tellen van het aantal getallen kleiner dan 100000 die bestaan uit 5 verschillende cijfers. Dan zien we dat er precies $\binom{9}{5} \cdot 5!$ dergelijke getallen zijn die 0 niet bevatten en precies $\binom{9}{4} \cdot 5! - \binom{9}{4} \cdot 4!$ dergelijke getallen met 0. Dit aantal is dus $9 \cdot \binom{9}{4} \cdot 4!$.

Ten tweede tellen we het aantal getallen kleiner dan 100000 die bestaan uit 4 verschillende cijfers (en dus ook maar bestaan uit 4 cijfers). Het aantal dergelijke getallen die 0 niet bevatten is $\binom{9}{4} \cdot 4!$, terwijl het aantal dergelijke getallen die 0 wel bevatten gelijk is aan $\binom{9}{3} \cdot 4! - \binom{9}{3} \cdot 3!$. Dit aantal is dus $9 \cdot \binom{9}{3} \cdot 3!$.

Ten derde tellen we het aantal getallen kleiner dan 100000 die bestaan uit 3 verschillende cijfers (en dus ook maar bestaan uit 3 cijfers). Het aantal dergelijke getallen die 0 niet bevatten is dus $\binom{9}{3} \cdot 3!$ en het aantal dergelijke getallen die 0 wel bevatten is dus $\binom{9}{2} \cdot 3! - \binom{9}{2} \cdot 2!$. Dit aantal is dus $9 \cdot \binom{9}{2} \cdot 2!$.

Ten laatste tellen we het aantal getallen kleiner dan 100000 die bestaan uit 2 verschillende cijfers (en dus ook maar uit 2 cijfers bestaan). Het aantal zonder 0 bedraagt $\binom{9}{2} \cdot 2!$ en het aantal met 0 bedraagt $\binom{9}{1} \cdot 2! - \binom{9}{1}$. Dit aantal is dus $9 \cdot \binom{9}{1} \cdot 1!$.

Hieruit volgt dat het totale aantal natuurlijke getallen kleiner dan 100000 bestaande uit verschillende getallen gelijk is aan

$$9 \cdot \sum_{i=1}^{4} \binom{9}{i} \cdot i! + 10 = 32491.$$

(b) Vervolledig elk dergelijk natuurlijk getal tot een zestal door vooraan nullen toe te voegen indien nodig. Nu kan elk zestal verkregen worden op de volgende manier:

Neem een willekeurige oplossing $(a_1, a_2, a_3, a_4, a_5)$ van $a_1 + a_2 + a_3 + a_4 + a_5 = 4$, dan hebben we nog zes mogelijkheden om 9 toe te voegen zodat we een natuurlijk getal krijgen dat aan de voorwaarden van de oefening voldoet.

Het gevraagde aantal natuurlijke getallen is dus $6 \cdot \binom{8}{4} = 420$.

Extra Oefening 25 *Een groep van 24 personen gaat dineren aan een ronde tafel. Er kan gekozen worden tussen een vlees- en visgerecht. Om technische redenen wordt een visgerecht enkel klaargemaakt voor 2 personen die naast elkaar zitten. Stel er zijn 5 paren die het visgerecht nemen. Bereken het aantal manieren waarop de 24 personen het diner kunnen gebruiken. Tafelschikkingen die door rotatie uit elkaar ontstaan, worden als gelijk gesteld, maar tafelschikkingen waarbij tenminste één persoon iets anders bestelt, als verschillend.*

Oplossing. Stel de 5 paren zijn bepaald. Stel ze voor als $\{P_1, \ldots, P_5\}$ en stel de personen die vlees eten voor als $\{p_1, \ldots, p_{14}\}$. Het aantal mogelijkheden om deze rond de tafel te schikken is gelijk aan het aantal permutaties van $(P_1, \ldots, P_5, p_1, \ldots, p_{14})$ vermenigvuldigd met aantal mogelijkheden om de personen van elk paar te schikken op de twee stoelen die nu voor het paar gereserveerd zijn. Dus het totale aantal schikkingen zodat de paren niet gescheiden worden, is

$$19! \cdot 2^5,$$

zodat het aantal dergelijke schikkingen die niet verbonden zijn door rotatie gegeven wordt door

$$\frac{19! \cdot 2^5}{24}$$

daar elke permutatie cyclisch equivalent is met 24 permutaties waaronder zichzelf (zie ook Extra Oefening 22).

Extra Oefening 26 *Hoeveel elementen van* $\mathbb{N}[1, 6000]$ *zijn er waarin geen enkel cijfer herhaald wordt en alle cijfers even zijn?*

Oplossing. Het aantal geldige getallen bestaande uit vier cijfers is gelijk aan $2 \cdot 4 \cdot 3 \cdot 2$, daar we 2 keuzes hebben voor het eerste cijfer ($\in \{2, 4\}$), 4 keuzes voor het tweede cijfer ($\in \{0, 2, 4, 6, 8\} \setminus \{\text{eerste cijfer}\}$), enzovoort.
Het aantal bestaande uit 3 cijfers is $4 \cdot 4 \cdot 3$ daar het eerste cijfer verschillend is van nul, het tweede cijfer verschillend is van het eerste cijfer, en het derde cijfer verschillen is van het eerste en het tweede cijfer.
Het aantal bestaande uit 2 cijfers is dus $4 \cdot 4$, en het aantal bestaande uit 1 cijfer is 5. Het aantal elementen bedraagt dus $48 + 48 + 16 + 5 = 117$.

1.10 Toepassing op de kombinatieleer

1.10.1 De binomiale kansverdeling

1.10.2 Het aantal deelverzamelingen

1.10.3 Het Binomium van Newton

Oefening 1.10.1 *Bewijs het binomium van Newton door gebruik te maken van induktie.*

Oplossing. Neem als induktiebasis 1, dan volgt duidelijkerwijze dat het binomium geldig is voor $n = 1$. Kies eveneens $k \in \mathbb{N}_0$ waarvoor het binomium voldaan is. Dan

$$\begin{aligned}
(a+b)^{k+1} &= (a+b)^k(a+b) \\
&\overset{\text{IH}}{=} (a+b)\sum_{i=0}^{k}\binom{k}{i}a^i b^{k-i} \\
&= \binom{k}{k}a^{k+1} + \sum_{i=0}^{k-1}\binom{k}{i}a^{i+1}b^{k-i} + \sum_{i=1}^{k}\binom{k}{i}a^i b^{k-i+1} + \binom{k}{0}b^{k+1} \\
&= a^{k+1} + b^{k+1} + \sum_{j=1}^{k}\left[\binom{k}{j-1} + \binom{k}{j}\right]a^j b^{(k+1)-j} \\
&= \sum_{i=0}^{k+1}\binom{k+1}{i}a^i b^{(k+1)-i}
\end{aligned}$$

waaruit, wegens het induktieprincipe, volgt dat het binomium van Newton geldig is voor alle $n \in \mathbb{N}_0$.

Oefening 1.10.2 *Bewijs de volgende formules:*

$$\begin{aligned} \sum_{k=0}^{n} \binom{n}{k} &= 2^n \\ \sum_{k=0}^{n} (-1)^k \binom{n}{k} &= 0 \end{aligned}$$

Oplossing. We hebben reeds gezien dat het aantal deelverzamelingen van $\mathbb{N}[1,n]$ gelijk is aan 2^n. We tellen nu dit aantal op een andere wijze

$$\begin{aligned} |\{M \parallel M \subseteq \mathbb{N}[1,n]\}| &= \sum_{i=0}^{n} |\{M \subseteq \mathbb{N}[1,n] \parallel |M| = i\}| \\ &= \sum_{i=0}^{n} \binom{n}{i} \end{aligned}$$

waaruit de eerste formule.

Om de tweede formule te bewijzen gebruiken we het induktieprincipe, gecombineerd met de formule $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. Kies als induktiebasis 1, dan is het duidelijk dat de gevraagde formule geldt voor de induktiebasis. Zij nu $l \in \mathbb{N}_0$ willekeurig zodat het gestelde geldt voor $n = l$. Dan is

$$\begin{aligned} \sum_{k=0}^{l+1} (-1)^k \binom{l+1}{k} &= \sum_{k=0}^{l+1} (-1)^k \left[\binom{l}{k} + \binom{l}{k-1} \right] \\ &= \sum_{k=0}^{l} (-1)^k \binom{l}{k} + \sum_{k=1}^{l+1} (-1)^k \binom{l}{k-1} \\ &\overset{\text{IH}}{=} 0 - \sum_{i=0}^{l} (-1)^i \binom{l}{i} \\ &\overset{\text{IH}}{=} 0 \end{aligned}$$

waaruit de tweede formule.

Oefening 1.10.3 *Bewijs de volgende formule*

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \ldots + \binom{n}{n-1}^2 + \binom{n}{n}^2 = \binom{2n}{n}.$$

Oplossing. Beschouw $M = \mathbb{N}[1, 2n]$, dan is $M = M_1 \cup M_2$ waarbij de unie disjunct is en $M_1 = \mathbb{N}[1, n]$, $M_2 = \mathbb{N}[n+1, 2n]$. Elke deelverzameling van M met cardinaliteit n kan verkregen worden door eerst in M_1 i getallen te kiezen ($i \leq n$) en daarna nog $(n-i)$ getallen in M_2, en elke dergelijke verkregen verzameling is uniek. Dus

$$\begin{aligned}
|\{D \subseteq M \parallel |D| = n\}| &= |\{(D_1, D_2) \in 2^{M_1} \times 2^{M_2} \parallel |D_1 \cup D_2| = n\}| \\
&= \sum_{D_1 \in 2^{M_1}} |\{D_2 \in 2^{M_2} \parallel |D_1 \cup D_2| = n\}| \\
&= \sum_{i=0}^{n} \sum_{D_1 \in 2^{M_1} : |D_1| = i} |\{D_2 \in 2^{M_2} \parallel |D_2| = n - i\}| \\
&= \sum_{i=0}^{n} \sum_{D_1 \subseteq M_1 : |D_1| = i} \binom{n}{n-i} \\
&= \sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i} \\
&= \sum_{i=0}^{n} \binom{n}{i}^2
\end{aligned}$$

wat het gestelde bewijst.

Oefening 1.10.4 *Bewijs dat het binomiaalgetal $\binom{p}{k}$ met p een priemgetal, deelbaar is door p voor alle waarde van k, $1 \leq k \leq p-1$. Leid hieruit af dat $(a+b)^p - a^p - b^p$ steeds deelbaar is door p voor elke 2 gehele getallen a en b.*

Oplossing. aangezien $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ volgt dat $p! = \binom{p}{k} k!(p-k)!$. Omdat nu p het linkerlid deelt, moet het ook het rechterlid delen. Aangzien $k, p-k < p$ is $k!(p-k)!$ niet deelbaar door p want p is priem. Dus $p \mid \binom{p}{k}$ voor alle k met $1 \leq k \leq p-1$.

Nu is $(a+b)^p - a^p - b^p = \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}$ waaruit onmiddellijk volgt dat $p \mid (a+b)^p - a^p - b^p$.

1.10.4 Het veralgemeend inclusie-exlusie principe

1.10.5 Permutaties zonder fixelementen: wanorde

1.11 Stirling getallen

Oefening 1.11.1 *Bewijs de volgende identiteiten voor de Stirling getallen.*

$$\begin{aligned} S(n,2) &= 2^{n-1}-1 \\ S(n,n-1) &= \binom{n}{2} \\ S(n,k) &= \sum_{i=0}^{n-1} \binom{n-1}{i} S(i,k-1) \end{aligned}$$

Oplossing. Zij $\mathcal{P}$ de verzameling van alle mogelijke partities van $\mathbb{N}[1,n]$ met exact 2 niet-ledige komponenten. Beschouw de volgende afbeelding $\sigma : 2^{\mathbb{N}[1,n]} \setminus \{\emptyset, \mathbb{N}[1,n]\} \to \mathcal{P}$, gedefinieerd door $D^\sigma = \{D, \mathbb{N}[1,n] \setminus D\}$. Dan is het duidelijk dat deze afbeelding surjectief is, en dat elk beeld 2 maal bereikt wordt. Uit toepassing van het produktprincipe volgt dan dat $|2^{\mathbb{N}[1,n]} \setminus \{\emptyset, \mathbb{N}[1,n]\}| = 2^n - 2 = 2 \cdot |\mathcal{P}| = 2 \cdot S(n,2)$. Waaruit de eerste formule volgt.

Zij nu $\mathcal{P}$ de verzameling van alle mogelijke partities van $\mathbb{N}[1,n]$ met exact $(n-1)$ niet-ledige komponenten. Het is eenvoudig in te zien dat elk zo'n partitie uit $(n-1)$ punten en 1 paar bestaat. En met elk paar correspondeert een unieke partitie met de gestelde eigenschappen. Dus $S(n,n-1)$ is gelijk aan het aantal paren in $\mathbb{N}[1,n]$, wat gegeven wordt door $\binom{n}{2}$.

We bewijzen nu de laatste formule. Indien $k = 1$ dan is het duidelijk dat de formule geldig is. Zij dus $k \geq 2$, dan tellen we de partities van $\mathbb{N}[1,n]$ met exact k niet-ledige komponenten op een bijzondere wijze. Neem een willekeurige deelverzameling D van $\mathbb{N}[1,n]$ die 1 bevat en daarbij een partitie van $\mathbb{N}[1,n] \setminus D$ bestaande uit $(k-1)$ niet-ledige komponenten. Het is duidelijk dat we, bij vaste D, telkens een andere partitie van $\mathbb{N}[1,n]$ bekomen, bestaande uit k niet-ledige komponenten. Laten we nu D variëren, dan bekomen we weer andere partities. Zij P een willekeurige partitie van $\mathbb{N}[1,n]$ die exact k niet-ledige elementen bevat. Dan is er dus steeds een unieke $D \in P$, die 1 bevat, m.a.w. elke gezochte partitie wordt juist 1 keer geconstrueerd volgens de gegeven constructie. Dus

$$S(n,k) = \sum_{D \subseteq \mathbb{N}[1,n] : 1 \in D \neq \mathbb{N}[1,n]} |\mathcal{P}(D)|$$

met $\mathcal{P}(D)$ de verzameling van alle partities van $\mathbb{N}[1,n] \setminus D$ met exact $(k-1)$ niet-ledige komponenten. Dus

$$S(n,k) = \sum_{i=0}^{n-1} \binom{n-1}{i} \cdot S(n-i-1,k-1)$$

waaruit het gestelde volgt.

1.12 Multinomiaalgetallen

Oefening 1.12.1 *Hoeveel woorden (eventueel zonder betekenis) van 11 letters kunnen we maken met de letters uit het woord MISSISSIPPI?*

Oplossing. Stel $X = \mathbb{N}[1,11]$ and $Y = \{m,i,s,p\}$, dan correspondeert met elk woord $x_1x_2\ldots x_{11}$, bestaande uit de 11 letters van MISSISSIPPI, net 1 afbeelding $\sigma : X \to Y$, gegeven door $i^\sigma = x_i$ waarbij $|m^{\sigma^{-1}}| = 1$, $|i^{\sigma^{-1}}| = |s^{\sigma^{-1}}| = 4$ en $|p^{\sigma^{-1}}| = 2$, en omgekeerd. Dus het aantal woorden is gelijk aan het aantal dergelijke functies, wat net de definitie van het multinomiaalgetal

$$\binom{11}{1,4,4,2} = \frac{11!}{4!4!2!} = 34650$$

is.

Oefening 1.12.2 *Indien $a+b+c=n$, bewijs dan dat*

$$\binom{n}{a,b,c} = \binom{n-1}{a-1,b,c} + \binom{n-1}{a,b-1,c} + \binom{n-1}{a,b,c-1}.$$

Oplossing.

$$\begin{aligned}
\binom{n}{a,b,c} &= \frac{n!}{a!b!c!} \\
&= (a+b+c)\frac{(n-1)!}{a!b!c!} \\
&= \frac{(n-1)!}{(a-1)!b!c!} + \frac{(n-1)!}{a!(b-1)!c!} + \frac{(n-1)!}{a!b!(c-1)!} \\
&= \binom{n-1}{a-1,b,c} + \binom{n-1}{a,b-1,c} + \binom{n-1}{a,b,c-1}
\end{aligned}$$

wat het gestelde bewijst.

Oefening 1.12.3 *Veronderstel dat p een priemgetal is. Bewijs dat het multinomiaalgetal*

$$\binom{p}{n_1, n_2, \ldots, n_k}$$

deelbaar is door p, tenzij één van de getallen n_i gelijk is aan p.

Oplossing. Aangezien p priem is, zal p $(p-1)!$ niet delen. Dus $p \mid p!$ en p^2 deelt $p!$ niet. Deze vaststellingen impliceren dat $p \mid \frac{p!}{n_1!n_2!\ldots n_k!}$ als en slechts als $n_1!n_2!\ldots n_k!$ niet deelbaar is door p, of dus als en slechts als $n_i < p$, voor alle $i \in \mathbb{N}[1,k]$.

Oefening 1.12.4 *Bewijs dat*

$$S(n,k) = \frac{1}{k!} \sum \binom{n}{n_1, n_2, \ldots, n_k}$$

waarbij de som genomen wordt over al de mogelijke k-tallen $(n_1, n_2, \ldots, n_k)$ van positieve natuurlijke getallen zodanig dat hun som n is.

Oplossing. Stel $k \leq n$ en definieer

$$\begin{aligned} \Sigma &= \{\gamma : \mathbb{N}[1,n] \to \mathbb{N}[1,k] \parallel \gamma \text{ surjectief}\} \\ \mathcal{P} &= \{P \text{ partitie van } \mathbb{N}[1,n] \parallel |P| = k,\ \emptyset \notin P\} \end{aligned}$$

Zij $\gamma \in \Sigma$, dan is $\{i^{\gamma^{-1}} \parallel i \in \mathbb{N}[1,k]\}$ een partitie van $\mathbb{N}[1,n]$ die we noteren met $P(\gamma)$. Laat ons nu de koppels $(P,\gamma) \in \mathcal{P} \times \Sigma : P = P(\gamma)$ tellen, dan levert het somprincipe volgende gelijkheid.

$$\sum_{P \in \mathcal{P}} |\{\gamma \in \Sigma \parallel P(\gamma) = P\}| = \sum_{\gamma \in \Sigma} |\{P \in \mathcal{P} \parallel P = P(\gamma)\}|$$

waaruit $k!|\mathcal{P}| = |\Sigma|$. Omdat $|\mathcal{P}| = S(n,k)$ en $|\Sigma| = \sum \binom{n}{n_1, n_2, \ldots, n_k}$, met het bereik van de som net als in de opgave, volgt het gestelde.

Oefening 1.12.5 *Op hoeveel manieren kan men mn voorwerpen verdelen over m dozen zodanig dat elke doos juist n elementen bevat?*

Oplossing. Het is duidelijk dat dit net het aantal surjectieve afbeeldingen γ van $\mathbb{N}[1, nm]$ naar $\mathbb{N}[1, m]$ is, waarbij voor alle $i \in \mathbb{N}[1, m] : |i^{\gamma^{-1}}| = n$. Per definitie is dit het multinomiaal getal $\binom{nm}{n_1, n_2, \ldots, n_m}$ met alle n_i gelijk aan n.

Oefening 1.12.6 *Bewijs door gebruik te maken van de multinomiaalgetallen, dat*

(a) 2^n *een deler is van* $(2n)!$ *en dat het quotient even is als* $n \geq 2$.

(b) $(n!)^{2n+1}$ *een deler is van* $(n^2!)!$.

Oplossing. Aangezien het multinomiaalgetal $\binom{2n}{n_1, n_2, \ldots, n_n}$ waarbij alle n_i gelijk zijn aan 2, goed gedefinieerd is en dus per definitie een natuurlijk getal is, zal $2^n = (2!)^n \mid (2n)!$. (Men kan (a) ook eenvoudig inzien door op te merken dat $(2n)!$ zeker n even factoren bevat, waardoor $2^n \mid (2n)!$. Als $n \geq 2$ dan zit ook $4 = 2^2$ onder deze factoren, zodat $2^{n+1} \mid (2n)!$. Dit betekent dat $\frac{(2n)!}{2^n}$ even is.)

Om (b) te bewijzen volstaat het aan te tonen dat $(2n+1)n \leq n^2!$, omdat dan het multinomiaalgetal $\binom{n^2!}{n_1, n_2, \ldots, n_{2n+1}, c}$ met alle n_i gelijk aan n en $c = n^2! - (2n+1)n$, gedefinieerd is. Als $n \geq 3$ dan is het duidelijk dat $(2n+1) \leq n^2$, waaruit $(2n+1)n \leq n^2 n \leq n^2!$. Als $n = 2$ dan is het duidelijk dat $(2n+1)n \leq n^2!$ en als $n \in \{0, 1\}$ dan is $(n!)^{2n+1} \mid (n^2!)!$ triviaal.

Examen oefening 27 (2de zit, 1994-1995) *Hoeveel woorden (zonder betekenis) kunnen er gevormd worden met al de letters uit het woord OPEENVOLGEND waarbij twee klinkers elkaar nooit mogen opvolgen?*

Oplossing. Om dit aantal te vinden, beschouw eerst de medeklinkers $PNNVLGD$ van *opeenvolgend*. Die kunnen op $\frac{7!}{2!1!1!1!1!1!} = \frac{7!}{2!}$ manieren geordend worden.

Plaats nu de klinkers $OOEEE$ ertussen. Beschouw bijvoorbeeld de reeks $PNNVLGD$. Er zijn precies 8 posities waar een klinker geplaatst kan worden: namelijk voor P, tussen twee medeklinkers, en na de laatste medeklinker G.

Om de twee klinkers O te plaatsen, zijn er dus $\binom{8}{2}$ mogelijkheden. Daarna blijven voor de drie klinkers E nog $\binom{6}{3}$ mogelijkheden over om deze bij te voegen.

In totaal zijn er dus

$$\frac{7!}{2!}\cdot\binom{8}{2}\binom{6}{3} = 1411200$$

mogelijke oplossingen.

Examen oefening 28 (2de zit, 1996-1997) *Beschouw het woord 'ONGEWOON'.*

(a) Hoeveel verschillende woorden (eventueel zonder betekenis) kunnen worden gevormd als we alle letters gebruiken?

(b) Hoeveel van deze woorden hebben drie O's na elkaar?

(c) In hoeveel woorden staan er twee maar geen drie O's na elkaar?

Oplossing.

(a) Dit is niks anders dan de definitie van het multinomiaal getal $\binom{8}{3,2,1,1,1}$.

(b) Vat '000' op als 1 karakter, dan is dit het multinomiaal getal $\binom{6}{1,2,1,1,1}$.

(c) De woorden waarbij alle O's naast elkaar staan is berekend in (b). De woorden waarbij geen twee O's naast elkaar voorkomen is gelijk aan het aantal combinaties van de niet-O letters (dit zijn er $\binom{5}{2,1,1,1}$) vermenigvuldigd met het aantal combinaties om de O's tussen te voegen (dit zijn er $6 \cdot 5 \cdot 4/3!$). Het antwoord is dus

$$\binom{8}{3,2,1,1,1} - \left[\binom{6}{1,2,1,1,1} + \binom{5}{2,1,1,1} \cdot 6 \cdot 5 \cdot 4/3!\right].$$

Examen oefening 29 (2de zit, 1997-1998) *Hoeveel verschillende mogelijkheden zijn er om de letters van het woord 'BINNENKORT' te rangschikken zodanig dat alle klinkers gegroepeerd blijven? Dezelfde vraag voor het woord 'TREINKAART'.*

Oplossing. Vat de klinkers van $BINNENKORT$, op als een karakter dan kunnen we met de gegeven letters $\binom{8}{1,1,3,1,1,1}$ woorden maken. Nu hebben we nog de vrijheid de klinkers te verwisselen naar hartelust. Hierdoor wordt het aantal woorden gemaakt met alle letters van het woord BINNENKORT waarbij de klinkers gegroepeerd staan, gegeven door

$$\binom{8}{1,1,3,1,1,1} \cdot 3!.$$

Voor TREINKAART moeten we opletten dat er permutaties van de klinkers zijn die dezelfde combinaties opleveren daar er gelijke klinkers zijn. Stel $K = eiaa$. We vermenigvuldigen het aantal woorden gemaakt met de medeklinkers en K ($\binom{7}{1,2,2,1,1}$), met het aantal woorden gemaakt met de klinkers uit K ($\binom{4}{1,1,2}$). Dus het aantal mogelijke woorden bestaande uit de letters van TREINKAART waarbij de klinkers naast elkaar voorkomen, is gelijk aan

$$\binom{7}{1,2,2,1,1} \cdot \binom{4}{1,1,2}.$$

Extra Oefening 30 *Hoeveel woorden kunnen er gevormd worden met de letters uit TALLAHASSEE, zodat geen 2 letters A naast elkaar staan?*

Oplossing. We merken op dat met elk zo'n woord een uniek woord bestaande uit de letters uit TLLHSSEE correspondeert, en met elk woord gevormd uit de letters van TLLHSSEE kan je $9 \cdot 8 \cdot 7/3!$ woorden vormen zodat geen twee A's naast elkaar staan (beschouw de ruimte tussen twee opeenvolgende letters als een bakje, dan krijg je zo 9 bakjes als je vooraan en achteraan ook een bakje plaatst, dit aantal is dan gewoon het aantal manieren om drie A's in drie verschillende bakjes te leggen). Dus het gevraagde aantal is dus

$$\binom{8}{1,2,1,2,2} \cdot \frac{9 \cdot 8 \cdot 7}{3!}.$$

Hoofdstuk 2

Voortbrengende functies

2.1 Formele machtreeksen

2.1.1 Inleiding

2.1.2 Som en product van machtreeksen

2.1.3 Een andere kijk op het binomium van Newton

2.2 Gewone voortbrengende functies

2.2.1 Definities

2.2.2 De voortbrengende funktie voor de herhalingskombinaties

Oefening 2.2.1 *Bepaal $g(x)$ zodanig dat $g(x)(1+2x+3x^2+4x^3+\ldots)=1$.*

Oplossing. We herschrijven $p(x)=(1+2x+3x^2+4x^3+\ldots)$ als volgt

$$\begin{aligned} p(x) &= (1+2x+3x^2+4x^3+\ldots) \\ &= (1+x+x^2+x^3+\ldots)+x(1+x+x^2+x^3+\ldots)+ \\ &\quad +x^2(1+x+x^2+x^3+\ldots)+\ldots \\ &= (1+x+x^2+x^3+\ldots)(1+x+x^2+x^3+\ldots) \\ &= (1-x)^{-1}(1-x)^{-1}. \end{aligned}$$

Hieruit volgt onmiddelijk $g(x) = (1-x)^2$.

Oefening 2.2.2 *Bepaal de coëfficiënt van x^7 in de ontwikkeling van $(1+x+x^2)^{-1}$.*

Oplossing. We zullen de oefening in zijn algemeenheid oplossen, d.w.z. we bepalen de coëfficiënt van alle x^i. We zoeken de formele machtreeks $\sum_{i=0}^{\infty} a_i x^i$ (indien ze bestaat!) van $(1+x+x^2)^{-1}$ of dus de coëfficiënten a_i zodanig dat

$$\begin{aligned}
(1+x+x^2)\sum_{i=0}^{\infty} a_i x^i &= 1 \\
&\Updownarrow \\
\sum_{i=0}^{\infty} a_i x^i + x\sum_{i=0}^{\infty} a_i x^i + x^2\sum_{i=0}^{\infty} a_i x^i &= 1 \\
&\Updownarrow \\
a_0 + (a_0+a_1)x + \sum_{i=2}^{\infty}(a_{i-2}+a_{i-1}+a_i)x^i &= 1.
\end{aligned}$$

Vergelijk van de coëfficiënten van linker- en rechterlid, geeft ons de volgende recursieve definitie van a_i voor alle $i \in \mathbb{N}$.

$$\begin{aligned}
a_0 &= 1 \\
a_1 &= -1 \\
a_i &= -(a_{i-2}+a_{i-1}). \qquad (2.1)
\end{aligned}$$

Met behulp van deze recursieve definitie kunnen we een algemene gedaante voor a_n opstellen, we bewijzen dat $a_{3i} = 1$, $a_{3i+1} = -1$ en $a_{3i+2} = 0$ voor alle $i \in \mathbb{N}$. Neem als induktiebasis 0, dan is eenvoudig nagegaan dat dit voldaan is voor de induktiebasis. Zij k dus willekeurig zodat aan het gestelde voldaan is voor k. Dan is

$$\begin{aligned}
a_{3(k+1)} &\overset{(2.1)}{=} -(a_{3k+1}+a_{3k+2}) \\
&\overset{\text{IH}}{=} -(-1+0) = 1 \\
a_{3(k+1)+1} &\overset{(2.1)}{=} -(a_{3k+2}+a_{3(k+1)})
\end{aligned}$$

$$\begin{aligned} & \overset{\text{IH}}{=} && -(0 + a_{3(k+1)}) \\ & = && -1 \\ a_{3(k+1)+2} & \overset{(2.1)}{=} && -(a_{3(k+1)} + a_{3(k+1)+1}) \\ & = && -(1 + (-1)) = 0 \end{aligned}$$

waaruit, wegens het induktieprincipe, het gestelde volgt. Dit impliceert in het bijzonder dat de coëfficiënt van x^7 gelijk is aan $a_7 = -1$.

Oefening 2.2.3 *Bewijs dat voor allle natuurlijke getallen $k > 0$ geldt dat:*

$$(-4)^{-k}\binom{2k}{k} = \binom{-\frac{1}{2}}{k}.$$

Oplossing. Vooreerst vermelden we de volgende makkelijk te bewijzen formules

$$\binom{n}{k+1} = \binom{n}{k}\frac{n-k}{k+1} \tag{2.2}$$

$$\binom{n}{k} = \binom{n+2}{k+1}\frac{(k+1)(n-k+1)}{(n+1)(n+2)}. \tag{2.3}$$

We bewijzen de oefening door middel van induktie. Kies als induktiebasis 1, dan is het eenvoudig nagegaan dat het gestelde geldt voor $k = 1$. Zij $l \geq 1$ zodanig dat het gestelde geldt voor $k = l$. Dan is

$$\begin{aligned} \binom{-\frac{1}{2}}{l+1} & \overset{(2.2)}{=} \binom{-\frac{1}{2}}{l}\frac{-1/2-l}{l+1} \\ & \overset{\text{IH}}{=} (-4)^{-l}\binom{2l}{l}\frac{-1/2-l}{l+1} \\ & \overset{(2.3)}{=} (-4)^{-l}\binom{2(l+1)}{l+1}\frac{(l+1)(-1/2-l)}{(2l+1)(2l+2)} \\ & = (-4)^{-(l+1)}\binom{2(l+1)}{l+1}. \end{aligned}$$

Met behulp van het induktieprincipe geldt dus

$$(-4)^{-n}\binom{2n}{n} = \binom{-\frac{1}{2}}{n}, \forall n \in \mathbb{N}_0.$$

Examen oefening 31 (2de zit, 1991-1992) *Op hoeveel manieren kan men 7 verschillende knikkers verdelen over 5 bakjes, zodanig dat er in ieder bakje ten minste 1 knikker ligt?*

Oplossing. Dit kan op 2 manieren opgelost worden.

(a) Dit is een toepassing op de Stirling getallen.

Er is namelijk een verzameling X van 7 knikkers die geschreven wordt als een disjuncte unie van 5 niet-ledige verzamelingen.

De oplossing is dus $S(7,5) = 140$.

Bij de Stirling getallen speelt de volgorde van de 5 niet-ledige verzamelingen geen rol. Als de volgorde van de 5 bakjes wel van belang is, dan is het aantal mogelijkheden $5! \cdot S(7,5) = 16800$.

(b) Stel we plaatsen n_1 knikkers in het eerste bakje, n_2 in het 2de,..., n_5 in het 5de bakje. Uit de betekenis van de multinomiaalgetallen volgt dat dit op

$$\frac{7!}{n_1! \cdots n_5!}$$

manieren kan gebeuren.

Het totale aantal oplossingen is dus

$$\sum \frac{7!}{n_1! \cdots n_5!} \text{ met } n_i \in \mathbb{N}[1,3] \text{ en } n_1 + \cdots + n_5 = 7. \tag{2.4}$$

Dit getal wordt berekend met behulp van de exponentieel voortbrengende functies. Associeer met elk bakje de polynoom $x + \frac{x^2}{2!} + \frac{x^3}{3!}$, dan is de gevraagde som (2.4) de coëfficient van $\frac{x^7}{7!}$ in $(x + \frac{x^2}{2!} + \frac{x^3}{3!})^5$.

Dit is ook de coëfficient van $\frac{x^7}{7!}$ in

$$\begin{aligned} \left(\sum_{k=1}^{+\infty} \frac{x^k}{k!}\right)^5 &= (e^x - 1)^5 \\ &= e^{5x} - 5e^{4x} + 10e^{3x} - 10e^{2x} + 5e^x - 1. \end{aligned}$$

Deze coëfficient is $5^7 - 5 \cdot 4^7 + 10 \cdot 3^7 - 10 \cdot 2^7 + 5 = 16800$.

Examen oefening 32 (2de zit, 1994-1995) *Gegeven zijn drie dozen die respectievelijk gevuld zijn met 6 rode, zes blauwe en zes gele ballen. Op hoeveel manieren kan men 11 ballen uit deze dozen nemen, als uit elke doos minstens 1 bal genomen moet worden?*

Oplossing. Dit is de coëfficient van x^{11} in $(x+x^2+x^3+x^4+x^5+x^6)^3$. Dus de coëfficient van x^8 in

$$\begin{aligned}(1+x+x^2+x^3+x^4+x^5)^3 &= (1-x^6)^3(1+x+x^2+\cdots)^3\\ &= \tfrac{(1-x^6)^3}{(1-x)^3}\\ &= (1-3x^6+\cdots)\sum_{k=0}^{+\infty}\overline{\tbinom{3}{k}}x^k.\end{aligned}$$

De oplossing is bijgevolg $\overline{\binom{3}{8}}-3\overline{\binom{3}{2}}=\binom{10}{8}-3\binom{4}{2}=27$.

Examen oefening 33 (1ste zit, 1997-1998) *Op hoeveel verschillende manieren kan men 25 identieke ballen in 7 verschillende bakjes leggen, als er hoogstens 10 in het eerste bakje kunnen? Er is geen beperking op het aantal ballen in de overige 6 bakjes.*

Oplossing. De voortbrengende functie van het eerste bakje is $(1+x+\cdots+x^{10})$. De voortbrengende functies die corresponderen met de 6 andere bakjes zijn $(1+x+x^2\cdots)$. De voortbrengende functie van dit probleem is dus $(1+x+\cdots+x^{10})(1+x+x^2\cdots)^6$.
We zoeken de coëfficiënt van x^{25} in deze uitdrukking. Daarvoor herschrijven we de factoren als volgt:
$(1+x+\cdots+x^{10})=\frac{1-x^{11}}{1-x}$, en
$\sum_{i=0}^{\infty}x^i=\frac{1}{1-x}$.
De voortbrengende functie is dus $(1-x^{11})(\frac{1}{1-x})^7$. Nu geldt:

$$(\frac{1}{1-x})^7=\sum_{k=0}^{\infty}\left(\begin{array}{c}7+k-1\\ k\end{array}\right)x^k=\sum_{k=0}^{\infty}\left(\begin{array}{c}6+k\\ k\end{array}\right)x^k\ .$$

De term in x^{25} is dan $\left(\begin{array}{c}6+25\\ 25\end{array}\right)x^{25}+(-1)x^{11}\left(\begin{array}{c}6+14\\ 14\end{array}\right)x^{14}$. Het gevraagde aantal mogelijkheden is de coëfficiënt van deze term, dus er zijn $\left(\begin{array}{c}31\\ 25\end{array}\right)-$

$\begin{pmatrix} 20 \\ 14 \end{pmatrix}$ mogelijkheden om de 7 bakjes te vullen met 25 ballen.

Examen oefening 34 (2de zit, 1998-1999) *Zoek het aantal manieren om een briefje van honderd Belgische franken te wisselen in* $(1BF, 5BF, 20BF, 50BF)$ *waarbij je hoogstens* 10 *1-frankstukken mag gebruiken.*

Oplossing. Omdat we maar 0, 5 of 10 1-frankstukken mogen gebruiken krijgen we de volgende voortbrengende functie:

$$g(x) = (1 + x^5 + x^{10})h(x)(1 + x^{50} + x^{100}),$$

met

$$h(x) = (1 + x^5 + x^{10} + x^{15} + \cdots + x^{100})(1 + x^{20} + x^{40} + x^{60} + x^{80} + x^{100}).$$

We zoeken nu de coëfficient van x^{100} in $g(x)$. De coëfficient van x^{100} in $h(x)$ is 6 en deze van x^{95} en x^{90} is 5. Dus bedraagt de coëfficient van x^{100} in $(1 + x^5 + x^{10})h(x)$, 16. De coëfficient van x^{50}, x^{45} en x^{40} in $h(x)$ is 3. Dus bedraagt de coëfficient van x^{50} in $(1 + x^5 + x^{10})h(x)$, 9. Tenslotte bedraagt de coëfficient van x^0 in $(1 + x^5 + x^{10})h(x)$, 1. Vandaar dat de coëfficient van x^{100} in $g(x)$ gelijk is aan 26.

2.3 Exponentieel voortbrengende functies

Oefening 2.3.1 *Bewijs dat* $k! \cdot S(n, k)$ *de coëfficient is van* $x^n/n!$ *in* $(e^x - 1)^k$. *Hierbij is* $S(n, k)$ *het Stirling getal van de tweede soort.*

Oplossing. Uit voorgaande voorbeelden volgt dat de coëfficiënt van $x^n/n!$ in $(e^x - 1)^k$ gelijk is aan het aantal manieren om met de cijfers uit $\mathbb{N}[1, k]$, een getal van n cijfers te maken, zodanig dat elk cijfer (uit $\mathbb{N}[1, k]$) minstens 1 keer optreedt. Het is duidelijk dat elk dergelijk getal $x_1 x_2 \ldots x_n$ een partitie bestaande uit k niet-ledige komponenten van $\mathbb{N}[1, n]$ definieert, die de indices, drager zijnde van hetzelfde element uit $\mathbb{N}[1, k]$, groepeert (we zeggen dat $i \in \mathbb{N}[1, n]$ het cijfer $j \in \mathbb{N}[1, k]$ draagt, indien $x_i = j$). Analoog zal elk dergelijke partitie juist $k!$ getallen definiëren (met elk getal correspondeert een unieke keuze van de te dragen elementen, en zo zijn er $k!$ keuzen). Deze beschouwingen bewijzen de oefening.

Oefening 2.3.2 *Bepaal de exponentieel voortbrengende functie die behoort bij het bepalen van het aantal woorden (zonder betekenis) die men kan maken met de letters van het woord MISSISSIPPI, waarbij elke letter ten hoogste zoveel keer mag voorkomen in de gemaakte woorden als in het woord MISSISSIPPI zelf.*

Oplossing. We zoeken dus een formule in x, nl. $g(x)$, zodat $g(x) = \sum_{i=0}^{\infty} a_i \frac{x^i}{i!}$ waarbij a_i gelijk is aan het aantal woorden van lengte i die aan de voorwaarden van de oefening voldoen. Nu verschijn M niet of 1 keer in het woord, P maximaal 2 keer, I en S maximaal 4 keer. Dus

$$g(x) = (1+x)(1+x+\frac{x^2}{2!})(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!})^2.$$

Oefening 2.3.3 *Op hoeveel manieren kan men 9 personen plaatsen in 4 kamers, zodanig dat geen enkle kamer onbezet is?*

Oplossing. Zij (n_1, n_2, n_3, n_4) een 4-tal van positieve natuurlijke getallen met som 9. Dan zijn er net $\binom{9}{n_1,n_2,n_3,n_4}$ mogelijke verdelingen zodat kamer1 n_1 personen bevat, kamer2 n_2 personen bevat, kamer3 n_3 personen bevat en kamer4 n_4 personen bevat. Dus het gevraagde aantal is

$$\sum \binom{9}{n_1, n_2, n_3, n_4}$$

waarbij de sommatie gebeurt over alle mogelijke 4-tallen van positieve natuurlijke getallen met som 9.

Examen oefening 35 (1ste zit, 1998-1999) *(a) Op hoeveel manieren kunnen we 19 identiek uitziende stoelen in vier verschillende kamers stoppen met in elke kamer minstens 1 stoel?*

(b) Zelfde vraag maar nu voor 19 stoelen met verschillende kleur.

Oplossing.

(a) De voortbrengende functie die bij dit probleem hoort is $g(x) = (x + x^2 + \cdots)^4 = x^4(1-x)^{-4}$. Wij zoeken de coëfficient van x^{19} in $g(x)$ of de coëfficient van x^{15} in $(1-x)^{-4}$. Deze is $\binom{4+15-1}{15} = 816$.

(b) Omdat we nu werken met verschillende objecten gebruiken we nu de exponentieel voortbrengende functie $g(x)$. Bij dit probleem is $g(x) = (\frac{x}{1!} + \frac{x^2}{2!} + \cdots)^4 = (e^x - 1)^4 = e^{4x} - 4e^{3x} + 6e^{2x} - 4e^x + 1$
$= \sum_{k=0}^{\infty} 4^k \frac{x^k}{k!} - 4\sum_{k=0}^{\infty} 3^k \frac{x^k}{k!} + 6\sum_{k=0}^{\infty} 2^k \frac{x^k}{k!} - 4\sum_{k=0}^{\infty} \frac{x^k}{k!}$. Wij zoeken de coëfficient van $\frac{x^{19}}{19!}$ in $g(x)$.
Deze is $4^{19} - 4 \times 3^{19} + 6 \times 2^{19} - 4$.

Examen oefening 36 (2de zit, 1999-2000) *Bepaal het aantal woorden van n letters die kunnen gevormd worden met behulp van de letters van het woord EURO zodanig dat er in elk woord er een oneven aantal E's voorkomen en een even aantal U's. Doe dit op twee manieren:*

(i) combinatorisch;

(ii) met behulp van genererende functies.
[Hint: merk op dat volgorde van belang is.]

Oplossing.

(i) Combinatorisch. Laat a_n het aantal woorden van lengte n zijn van letters uit het alfabet {E,U,R,O} en met een even aantal E's en een oneven aantal U's. Laat nu b_n het aantal woorden van lengte n zijn van letters uit het alfabet {E,U,R,O} en met een even aantal E's en een even aantal U's. Laat c_n het aantal woorden van lengte n zijn van letters uit het alfabet {E,U,R,O} en met een oneven aantal E's en een even aantal U's. En laat d_n het aantal woorden van lengte n zijn van letters uit het alfabet {E,U,R,O} en met een oneven aantal E's en een oneven aantal U's. Dan is $d_n = 4^n - a_n - b_n - c_n$. Merk op dat $a_1 = 1$, namelijk U; $b_1 = 2$, namelijk R en O; en $c_1 = 1$, namelijk E, en $d_1 = 0$.

Wanneer een woord van n letters begint met een E, dan moet het overblijvende gedeelte een woord zijn van $n-1$ letters met een oneven aantal E's en een oneven aantal U's opdat het totale woord een even aantal E's en een oneven aantal U's zou hebben. Wanneer het woord met n letters begint met een U, dan moet het overblijvende gedeelte een even aantal E's en een even aantal U's hebben. Wanneer het woord met n letters begint met een R, dan moet het overblijvende gedeelte een even aantal E's en een oneven aantal U's hebben. Ten slotte, wanneer

een woord met n letters begint met een O, dan moet het overblijvende gedeelte een even aantal E's en een oneven aantal U's hebben. Dit geeft

$$a_n = d_{n-1} + b_{n-1} + 2a_{n-1} = 4^{n-1} + a_{n-1} - c_{n-1}.$$

Analoog bekomen we

$$c_n = b_{n-1} + d_{n-1} + 2c_{n-1} = 4^{n-1} - a_{n-1} + c_{n-1}.$$

Nu beweren we dat $a_n = c_n$. Dit is zo voor $n = 1$. Stel dat $a_k = c_k$ voor een zekere k, dan is $a_{k+1} = 4^k + a_k - c_k = 4^k$ en $c_{k+1} = 4^k - a_k + c_k = 4^k$. Dus $a_{k+1} = c_{k+1} = 4^k$. Dit levert $a_n = 4^{n-1}$.

(ii) Met behulp van genererende functies. Het antwoord is de coëfficient van $\frac{x^n}{n!}$ in

$$\begin{aligned}(x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots)(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots)(e^x)(e^x) \\ = \frac{e^x - e^{-x}}{2}\frac{e^x + e^{-x}}{2}e^{2x} = \frac{e^{4x} - 1}{4}.\end{aligned}$$

Deze coëfficient bedraagt 4^{n-1}.

Extra Oefening 37 *Op hoeveel manieren kan men zes verschillende taken verdelen over 3 bedienden als de moeilijkste taak aan de meest ervaren en de gemakkelijkste taak aan de minst ervaren bediende gegeven wordt?*

Oplossing. Aangezien de moeilijkste en de gemakkelijkste taak steeds voor de meest ervaren en minst ervaren bediende zijn, moeten er maar 4 taken verdeeld worden over 3 bedienden. Stel de eerste bediende krijgt n_1, de tweede n_2 en de derde n_3 taken, $0 \leq n_1, n_2, n_3 \leq 4, n_1 + n_2 + n_3 = 4$, dan kan dit op

$$\frac{4!}{n_1!n_2!n_3!}$$

manieren. Dus het totale aantal mogelijkheden is

$$\sum \frac{4!}{n_1!n_2!n_3!} \text{ met } n_1 + n_2 + n_3 = 4, n_i \in \mathbb{N}[0, 4]. \tag{2.5}$$

Om dit getal (2.5) te vinden, associeer met elke bediende de functie $1 + \frac{x}{1!} + \cdots + \frac{x^4}{4!}$, dan is (2.5) de coëfficient van $\frac{x^4}{4!}$ in $(1 + \frac{x}{1!} + \cdots + \frac{x^4}{4!})^3$. Dit is ook de coëfficient bij $\frac{x^4}{4!}$ in de reeksontwikkeling van $(e^x)^3 = x^{3x} = \sum_{k=0}^{+\infty} \frac{3^k x^k}{k!}$ en deze coëfficient is $3^4 = 81$.

2.4 De differentiaaloperator

Oefening 2.4.1 *Bewijs dat*

(a) $D(e^x) = e^x$.

(b) $D(\ln 1 + x) = (1 + x)^{-1}$.

Oplossing. We bewijzen eerst (a)

$$\begin{aligned} D(e^x) &= D(\sum_{i=0}^{\infty} \frac{x^i}{i!}) \\ &\stackrel{\text{def}}{=} \sum_{i=1}^{\infty} i \frac{x^{i-1}}{i!} \\ &= \sum_{j=0}^{\infty} \frac{x^j}{j!} \\ &= e^x. \end{aligned}$$

Nu (b)

$$\begin{aligned} D(\ln(1+x)) &= D(\sum_{i=1}^{\infty} (-1)^{i+1} \frac{x^i}{i}) \\ &\stackrel{\text{def}}{=} \sum_{i=1}^{\infty} i(-1)^{i+1} \frac{x^{i-1}}{i} \\ &= \sum_{j=0}^{\infty} (-1)^j x^j \\ &= \sum_{j=0}^{\infty} (-x)^j \\ &= (1+x)^{-1}. \end{aligned}$$

Oefening 2.4.2 *Bereken $D((1+x)^n)$. Leidt hieruit af dat*

$$\sum_{k=0}^{n} k\binom{n}{k} \;=\; n \cdot 2^{n-1}$$

Oplossing.

$$\begin{aligned} D((1+x)^n) &= D(\sum_{k=0}^{\infty} \binom{n}{k} x^k) \\ &\overset{\text{def}}{=} \sum_{k=1}^{\infty} k\binom{n}{k} x^{k-1} \\ &= \sum_{k=1}^{n} k\binom{n}{k} x^{k-1}. \end{aligned} \tag{2.6}$$

We bewijzen nu $D((1+x)^n) = n(1+x)^{n-1}$ voor alle $n \in \mathbb{N}_0$ met behulp van induktie. Kies dus als induktiebasis 0. Dan is het gevraagde triviaal voldaan voor $n = 0$. Zij $k \in \mathbb{N}$ waarvoor $D((1+x)^k) = k(1+x)^{k-1}$, dan is

$$\begin{aligned} D((1+x)^{k+1}) &= D((1+x)(1+x)^k) \\ &= D(1+x) \cdot (1+x)^k + (1+x) \cdot k(1+x)^{k-1} \\ &= (1+x)^k + k(1+x)^k \\ &= (k+1)(1+x)^k. \end{aligned}$$

Met behulp van het induktieprincipe vinden we het gestelde.

We bekomen dus

$$\sum_{k=1}^{n} k\binom{n}{k} x^{k-1} = n(1+x)^{n-1}.$$

Aangezien het linker lid convergeert voor $x = 1$, is dus $\sum_{k=0}^{n} k\binom{n}{k} = 2^{n-1}n$, wat we nog moesten aantonen.

2.5 Constructie van voortbrengende functies

Extra Oefening 38 *Stel de voortbrengende functie op behorend bij de rij* $(2^{n-1}(2^n-1))_n$.

Oplossing. Herschrijf de rij als een som, dus $a_n = 2^{2n-1} - 2^{n-1}$, dus de voortbrengende functie is het verschil van de voortbrengende functies van $b_n = 2^{2n-1}$ en van $c_n = 2^{n-1}$. Nu is

$$\sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} \frac{(4x)^n}{2} = \frac{1}{2}\frac{1}{1-4x}.$$

Analoog vind je

$$\sum_{n=0}^{\infty} c_n x^n = \frac{1}{2}\frac{1}{1-2x}.$$

Het antwoord is dus $\frac{1}{2}\left[\frac{1}{1-4x} - \frac{1}{1-2x}\right]$.

Extra Oefening 39 *Geef de voortbrengende functie voor de rij* $(\frac{3^{n+1}}{5}(4^n - 1))$.

Oplossing. Herschrijf de gegeven rij $(a_n)_n$ als $(b_n - c_n)_n$ met $b_n = \frac{3 \cdot 12^n}{5}$ en $c_n = \frac{3\cdot(-3)^n}{5}$. De voortbrengende functie voor a_n, $a_n \geq 1$, is dan gelijk aan

$$\begin{aligned}
\sum_{n=1}^{+\infty} a_n X^n &= \sum_{n=1}^{+\infty} b_n X^n - \sum_{n=1}^{+\infty} c_n X^n \\
&= \frac{3}{5}(\sum_{n=1}^{+\infty}(12X)^n - \sum_{n=1}^{+\infty}(-3X)^n) \\
&= \frac{3}{5}(\sum_{n=0}^{+\infty}(12X)^n - \sum_{n=0}^{+\infty}(-3X)^n) \\
&= \frac{3}{5}(\frac{1}{1-12X} - \frac{1}{1+3X}) = \frac{9X}{1-9X-36X^2}.
\end{aligned}$$

Extra Oefening 40 *Stel de voortbrengende functie op behorend bij de rij* $(2^{n-1}(1+2^{n-1}))_n$.

Oplossing. De genererende functie van de rij $(a_n)_n$ is

$$\begin{aligned}\sum_{n=0}^{+\infty} a_n X^n &= \frac{1}{2}\sum_{n=0}^{+\infty} 2^n X^n + \frac{1}{4}\sum_{n=0}^{+\infty} 4^n X^n \\ &= \frac{1}{2}\frac{1}{1-2X} + \frac{1}{4}\frac{1}{1-4X} \\ &= \frac{3-10X}{4(1-2X)(1-4X)}.\end{aligned}$$

Hoofdstuk 3

Recurrente betrekkingen

3.1 Definitie

3.2 Lineaire recurrente betrekkingen met constante coëfficiënten

3.2.1 Definitie

3.2.2 Homogene lineaire recurrente betrekkingen met constante coëfficiënten

Homogene lineaire recurrente betrekkingen van eerste orde

$$a_n = ca_{n-1}$$

Is x oplossing van de karakteristieke vergelijking $x - c = 0$, dan is de algemene oplossing geven door

$$a_n = \alpha x^n.$$

Homogene lineaire recurrente betrekkingen van tweede orde

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

Zijn x_1 en x_2 de oplossingen van de karakteristieke vergelijking $x^2 - c_1 x - c_2 = 0$, dan is de algemene oplossing gegeven door

$$a_n = \begin{cases} \alpha_1 x_1^n + \alpha_2 x_2^n & \text{als } x_1 \neq x_2 \\ \alpha_1 x_1^n + \alpha_2 n x_1^n = (\alpha_1 + \alpha_2 n) x_1^n & \text{als } x_1 = x_2 \end{cases}$$

Homogene lineaire recurrente betrekkingen van hogere orde

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$$

Zijn $x_1, \ldots, x_l$ de oplossingen van de karakteristieke vergelijking met respectivelijke multipliciteiten $m_1, \ldots, m_l$, dan is de algemene oplossing gegeven door

$$a_n = \sum_{i=1}^{l} x_i^n \sum_{j=0}^{m_i - 1} \alpha_{ij} n^j.$$

Oefening 3.2.1 *Los volgende recurrente betrekkingen op:*

(i) $2a_n - 3a_{n-1} - 2a_{n-2} = 0$, $n \geq 2$, $a_0 = 0$, $a_1 = -5$.

(ii) $4a_n - 12a_{n-1} + 9a_{n-2} = 0$, $n \geq 2$, $a_0 = 2$, $a_1 = 3/2$.

(iii) $a_n = 8(a_{n-1} - 2a_{n-2})$, $n \geq 2$, $a_0 = 1$, $a_1 = 5$.

(iv) $a_n - 2a_{n-2} + a_{n-4} = 0$, $n \geq 4$, $a_0 = 2$, $a_1 = a_3 = 0$, $a_2 = 6$.

Oplossing.

(i) De karakteristieke vergelijking $2x^2 - 3x - 2 = 0$ heeft oplossingen $-1/2$ en 2, beide met multipliciteit 1. Dus de algemene oplossing is

$$a_n = \alpha_1 \left(\frac{-1}{2}\right)^n + \alpha_2 2^n.$$

Houden we rekening met de waarden a_0 en a_1, dan vinden we $\alpha_1 = 2$ en $\alpha_2 = -2$.

(ii) De karakteristieke vergelijking $4x^2 - 12x + 9 = 0$ heeft unieke oplossing $3/2$ (dus multipliciteit 2). Dus de algemene oplossing is

$$a_n = \alpha_1 \left(\frac{3}{2}\right)^n + \alpha_2 n \left(\frac{3}{2}\right)^n.$$

Houden we rekening met $a_0 = 2$ en $a_1 = 3/2$, dan vinden we $\alpha_1 = 2$ en $\alpha_2 = -1$.

(iii) De karakteristieke vergelijking $x^2 - 8x + 16 = 0$ heeft unieke oplossing 4 (dus multipliciteit 2), waardoor de algemene oplossing gegeven wordt door

$$a_n = \alpha_1 4^n + \alpha_2 n 4^n.$$

Rekening houdend met $a_0 = 1$ en $a_1 = 5$, vinden we $\alpha_1 = 1$ en $\alpha_2 = 1/4$.

(iv) De karakteristieke vergelijking $x^4 - 2x^2 + 1 = 0$ heeft oplossingen 1 en -1 beide met multipliciteit 2, dus de algemene oplossing is

$$a_n = (\alpha_{00} + \alpha_{01} n) + (\alpha_{10} + \alpha_{11} n)(-1)^n.$$

Nu volgt uit $a_1 = 0$ dat $\alpha_{00} - \alpha_{10} = 0$. Wegens voorgaande en $a_0 = 2$ volgt $\alpha_{00} = \alpha_{10} = 1$.
Eveneens geeft $a_3 = 0$ dat $3\alpha_{01} - 3\alpha_{11} = 0$. Wegens voorgaande en $a_2 = 6$ volgt dan $\alpha_{01} = \alpha_{11} = 1$.

Examen oefening 41 (2ste zit, 1991-1992) *Laat a_n het aantal* woorden *zijn van n letters uit het alfabet $\{x, y\}$, die de lettercombinatie yy niet bevatten. Stel een recurrente betrekking op van a_n en los ze op. Bepaal a_7.*

Oplossing.

Deel 1: De recurrente betrekking.

De beginvoorwaarden voor de recurrente betrekking zijn $a_1 = 2$, want er zijn twee oplossingen x en y van lengte 1, en $a_2 = 3$, want er zijn drie oplossingen xx, yx en xy van lengte 2.

Zij $z = z_1 \cdots z_n$ een oplossing van lengte n. Als $z_n = x$, dan is $z_1 \cdots z_{n-1}$ een oplossing van lengte $n-1$, dus zijn er precies a_{n-1} oplossingen van lengte n die eindigen op x.

Als $z_n = y$, dan moet $z_{n-1} = x$, want yy mag niet optreden in z. Dan volgt uit het vorige geval dat $z_1 \cdots z_{n-2}$ een oplossing is van lengte $n-2$. Bijgevolg zijn er precies a_{n-2} oplossingen van lengte n die eindigen op y.

Het totaal aantal oplossingen van lengte n is dus $a_n = a_{n-1} + a_{n-2}$.

Deel 2: De oplossing van de recurrente betrekking.

Uit de studie van de recurrente betrekking van de Fibonacci getallen volgt dat een algemene oplossing voor de recurrente betrekking gegeven wordt door

$$a_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Invullen van de beginvoorwaarden $a_1 = 2$ en $a_2 = 3$ geeft het volgende stelsel

$$\begin{cases} 2 &= \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right) \\ 3 &= \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^2 + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^2 \end{cases}$$

en dit heeft als oplossingen

$$\alpha_1 = \frac{6+2\sqrt{5}}{4\sqrt{5}} \text{ en } \alpha_2 = \frac{-6+2\sqrt{5}}{4\sqrt{5}}.$$

Bijgevolg

$$a_n = \left(\frac{6+2\sqrt{5}}{4\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{-6+2\sqrt{5}}{4\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Hieruit volgt $a_7 = 34$.

Examen oefening 42 (1ste zit, 1995-1996) *In een programmeertaal worden enkel correcte wiskundige uitdrukkingen (zonder haakjes) aanvaard die gevormd worden met de cijfers* $1, \ldots, 9$ *en de binaire bewerkingssymbolen* $+, *, /, -$ *(Bijvoorbeeld:* $1221, 3 + 4, 2 + 3 * 5, 23 * 59 + 1124$ *zijn correcte wiskundige uitdrukkingen, maar* $+2, 8 + *9, 9 + 3-$ *zijn dit niet).*

Zij a_n *het aantal correcte wiskundige uitdrukkingen van lengte* n*.*
(1) Bewijs dat a_n *voldoet aan de recurrente betrekking:*

$$a_n = 9a_{n-1} + 36a_{n-2}, \qquad n \geq 3, \qquad a_1 = 9, a_2 = 81;$$

(2) Los deze recurrente betrekking op;
(3) Geef de voortbrengende functie voor a_n*.*

Oplossing. (1) Zij x een correcte wiskundige uitdrukking van lengte n. Dan moet het laatste symbool in x een cijfer zijn. Voor dit laatste cijfer staat ofwel een cijfer, of een binair bewerkingssymbool.

Als voor het laatste cijfer een cijfer staat, dan vormen de $n-1$ eerste symbolen van x een correcte wiskundige uitdrukking. Hiervan zijn er precies a_{n-1} en dit toont aan dat er $9a_{n-1}$ correcte wiskundige uitdrukkingen zijn van lengte n die eindigen op twee cijfers.

Als echter voor het laatste cijfer een binair bewerkingssymbool staat, dan moet voor dit bewerkingssymbool een cijfer staan; dus vormen de eerste $n-2$ symbolen in x een correcte wiskundige uitdrukking. Hiervan zijn er precies a_{n-2}. Daar er vier mogelijkheden voor de bewerkingssymbolen zijn (en die staan op de voorlaatste positie in x), en 9 mogelijkheden voor het cijfer op de laatste positie, zijn er $36a_{n-2}$ correcte wiskundige uitdrukkingen van lengte n die op de voorlaatste positie een bewerkingssymbool staan hebben.

Dit toont aan dat $a_n = 9a_{n-1} + 36a_{n-2}$, $n \geq 3$. De beginvoorwaarden zijn $a_1 = 9$ en $a_2 = 81$ daar een correcte wiskundige uitdrukking van lengte 1 of 2 enkel uit cijfers kan bestaan.

(2) De karakteristieke vergelijking $R^2 - 9R - 36 = 0$ heeft als oplossingen $R = 12$ en $R = -3$. Dit impliceert dat een willekeurige oplossing voor a_n gelijk is aan $a_n = \alpha_1 12^n + \alpha_2(-3)^n$. Substitutie van de beginvoorwaarden $a_1 = 9$ en $a_2 = 81$ impliceert dat $\alpha_1 = 3/5$ en dat $\alpha_2 = -3/5$.

Dus $a_n = 3(12^n - (-3)^n)/5$.

(3) zie Extra Oefening 39.

Examen oefening 43 (2de zit, 1997-1998) *Onderstel dat een codetaal enkel gebruik maakt van de strings 'a', 'ab' en 'bc' die in willekeurige volgorde na elkaar kunnen worden geplaatst. Stel de recurrente betrekking op die voor elk natuurlijk getal n het aantal mogelijke codewoorden geeft van lengte n (dus: noem a_n het aantal codewoorden van lengte n). Los de recurrente betrekking op.*

Oplossing. We schrijven eerst de mogelijkheden uit voor woorden van beperkte lengte:

n	mogelijke codewoorden van lengte n
1	a
2	aa, ab, bc
3	aaa, aab, abc, aba, bca

Het is triviaal dat $a_1 = 1$ en $a_2 = 3$, de codewoorden zijn hier de twee basisstrings 'ab' 'bc' en de combinatie 'aa', waarin tweemaal de basisstring 'a' wordt gecombineerd. Ook voor $n = 3$ ligt de telling voor de hand.

Hoe bepalen we nu het aantal woorden van lengte 4? Er zijn drie mogelijkheden:
(1) een string 'a' gevolgd door een codewoord van lengte 3: 5 mogelijkheden.
(2) een string 'ab' gevolgd door een codewoord van lengte 2: 3 mogelijkheden.
(3) een string 'bc' gevolgd door een codewoord van lengte 2: 3 mogelijkheden.
Dit geeft ons in totaal 11 mogelijke codewoorden van lengte 4.
Merk op dat we geen codewoorden dubbelgeteld hebben: de woorden gevormd in (1) (aaaa, aaab, aabc, aaba en abca) kunnen niet gelijk zijn aan woorden gevormd in (2) (abab, abbc, abaa). Dit komt omdat de combinatie 'a-bc' nooit anders kan worden opgesplitst omdat er geen basisstrings zijn die beginnen met een c: 'ab-c' kan dus nooit voorkomen. Op dezelfde manier kan er ook geen probleem van dubbele tellingen optreden indien de combinatie 'aba' voorkomt: daar de basisstring 'ba' niet bestaat, moet dit noodzakelijk afkomstig zijn van een na elkaar plaatsen van 'ab-a'.
We veralgemenen nu deze redenering. Een codewoord van lengte n wordt gevormd door de string a voor een woord van lengte $n-1$ te plaatsen, de string ab voor een woord van lengte $n-2$ of de string bc voor een woord van lengte $n-2$. Dit levert ons voor $n \geq 3$ de volgende recurrente betrekking op:

$$a_n = a_{n-1} + 2a_{n-2}.$$

De karakteristieke vergelijking $X^2 - X - 2 = 0$ heeft twee enkelvoudige wortels: $X = 2$ en $X = -1$. De algemene oplossing is van de vorm $a_n = \alpha 2^n + \beta(-1)^n$. Met de beginvoorwaarden $a_3 = 5$ en $a_4 = 11$ bepalen we α en β:

$$\begin{cases} 5 &= 8\alpha - \beta \\ 11 &= 16\alpha + \beta. \end{cases}$$

Als we dit stelsel oplossen bekomen we $\alpha = \frac{2}{3}$ en $\beta = \frac{1}{3}$. De oplossing van de recurrente betrekking is dus $a_n = \frac{2}{3}2^n + \frac{1}{3}(-1)^n$.

De matrixmethode voor homogene lineaire betrekkingen van hogere orde

3.2.3 Niet-homogene lineaire recurrente betrekkingen met constante coëfficiënten

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} + f(n)$$

De oplossing van deze recurrente betrekking is volledig bepaald door een particuliere oplossing en de oplossing van het homogene gedeelte.

Indien $f(n)$ veelterm is van graad l, dan is een particuliere oplossing van de vorm

$$a_n^{(p)} = \alpha_0 n^t + \alpha_1 n^{t+1} + \ldots + \alpha_l n^{t+l},$$

waarbij t de multipliciteit van 1 als oplossing van de karakteristieke vergelijking van de bijhorende homogene betrekking. De coëfficiënten α_j worden berekend door de particuliere oplossing te substitueren in de recurrente betrekking.

Indien $f(n) = cq^n$, met c een constante, dan is

$$a_n^{(p)} = \alpha n^t q^n$$

een particuliere oplossing. Hierbij is t de multipliciteit van q in de karakteristieke vergelijking van de bijhorende homogene recurrente betrekking. Ook hier vindt men α door de particuliere oplossing te substitueren in de recurrente betrekking.

Oefening 3.2.2 *Los volgende recurrente betrekkingen op.*

(a) $a_n = 2a_{n-1} + n + 1$, $n \geq 1$, $a_0 = 1$.

(b) $a_n = 9a_{n-2} + 8n$, $n \geq 2$, $4a_0 = 9$, $4a_1 = 1$.

(c) $a_n = 4a_{n-2} + 2^n$, $n \geq 2$, $a_0 = 2$, $a_1 = 1$.

Oplossing.

(a) We berekenen eerst de oplossing van de homogene recurrente betrekking met karakteristieke vergelijking $x - 2 = 0$. Deze is duidelijkerwijze

$$a_n^{(h)} = \alpha 2^n.$$

Om de particuliere oplossing te bepalen merken we op dat $f(n) = n+1$ en dus is de particuliere oplossing $a_n^{(p)}$ van de vorm

$$a_n^{(p)} = \beta_0 n^0 + \beta_1 n^1.$$

Substitutie in de niet-homogene recurrente betrekking levert

$$\beta_0 + \beta_1 n = 2\beta_0 + 2\beta_1(n-1) + n + 1$$

waardoor $\beta_0 = 2\beta_0 - 2\beta_1 + 1$ en $\beta_1 = 2\beta_1 + 1$ en dus $\beta_1 = -1$, $\beta_0 = -3$. De algemene oplossing bedraagt dus

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha 2^n - 3 - n.$$

Wegens $a_0 = 1$ vinden we $\alpha = 4 + n$.

(b) We berekenen eerst de oplossing van de homogene recurrente betrekking met karakteristieke vergelijking $x^2 - 9 = 0$, namelijk

$$a_n^{(h)} = \alpha_0 3^n + \alpha_1(-3)^n.$$

Om de particuliere oplossing te bepalen merken we op dat $f(n) = 8n$ en dus is de particuliere oplossing $a_n^{(p)}$ van de vorm

$$a_n^{(p)} = \beta_0 + \beta_1 n.$$

Substitutie in de niet-homogene recurrente betrekking levert

$$\beta_0 + \beta_1 n = 9\beta_0 + 9\beta_1(n-2) + 8n$$

waardoor $\beta_0 = 9\beta_0 - 18\beta_1$ en $\beta_1 = 9\beta_1 + 8$, dus $\beta_1 = -1$ en $\beta_0 = -9/4$. De algemene oplossing bedraagt dus

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha_0 3^n + \alpha_1(-3)^n - 9/4 - n.$$

Bovendien geldt wegens $4a_0 = 9$ dat $4\alpha_0 + 4\alpha_1 = 18$ en wegens $4a_1 = 1$ dat $12\alpha_0 - 12\alpha_1 = 14$, waardoor $\alpha_0 = 17/3$ en $\alpha = 9/2$.

(c) We starten met de oplossing van het homogeen vraagstuk. De karakteristieke vergelijking is $x^2 - 4 = 0$ en heeft dus twee oplossingen, namelijk 2 en -2. De homogene oplossing is dus van de vorm

$$a_n^{(h)} = \alpha_1 2^n + \alpha_2(-2)^n.$$

De term in de recurrente betrekking verantwoordelijk voor het niet-homogeen zijn is van de vorm cq^n ($c = 1$ en $q = 2$), waardoor de particuliere oplossing van de vorm

$$a_n^{(p)} = \beta n 2^n$$

want q is een oplossing van multipliciteit 1 van de karakteristieke vergelijking. Substitutie van de particuliere oplossing in de recurrente betrekking levert $\beta = 1/2$.

De algemene oplossing is dus van de vorm

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha_1 2^n + \alpha_2(-2)^n + n2^{n-1}.$$

Houden we rekening met $a_0 = 2$ en $a_1 = 1$, vinden we $\alpha_1 = \alpha_2 = 1$.

Oefening 3.2.3 *Iemand leent geld van een bank en betaalt hiervoor jaarlijks een vast bedrag s aan de bank. Een gedeelte van de jaarlijkse betaling is de rente over de schuld volgens een vast percentage r, de rest van de betaling wordt gebruikt om de schuld te verminderen.*

(a) Als a_{n-1} de schuld is van $n-1$ jaar, wat is dan de schuld na n jaar?

(b) Geef de algemene oplossing van de recurrente betrekking die bij het probleem behoort.

(c) Bereken de jaarlijkse betaling s aan de bank, als de persoon een bedrag K leende en zijn schuld in p jaar moet aflossen.

Oplossing.

(a) $a_n = a_{n-1} - s(1-r)$, waarbij we r als een $\frac{\cdot}{100}$ breuk voorstellen.

(b) De algemene oplossing van de bijbehorende homogene recurrente betrekking bedraagt

$$a_n^{(h)} = \alpha.$$

Aangezien $f(n) = (1-r)s$ gezien kan worden als een veelterm van graad nul, zien we dat de particuliere oplossing van de volgende vorm is

$$a_n^{(p)} = \beta n.$$

Substitutie in de recurrente betrekking levert, $\beta = -s(1-r)$. De algemene oplossing bedraagt dus

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha - s(1-r)n.$$

(c) De persoon leende het bedraag K, dus $a_0 = K$. Dit impliceert onmiddellijk dat $\alpha = K$. Tevens eisen we dat $a_p = 0$, waaruit $0 = K - s(1-r)p$ of $s = K/(1-r)p$.

Oefening 3.2.4 *Een verzameling rechten noemt men willekeurig gelegen in het vlak als geen twee van die rechten evenwijdig zijn en geen drie ervan door een zelfde punt gaan. Bepaal het aantal gebieden waarin het vlak door n willekeurig gelegen rechten verdeeld wordt.*

Oplossing. Duidelijkerwijze $a_1 = 2$. Om een recurrente betrekking voor het aantal gebieden op te stellen merken we op dat als we vertrekken van $n-1$ willekeurig gelegen rechten en een $n$de rechte L toevoegen, dat dan het aantal gebieden dat niet meer voorkomt in de nieuwe verdeling juist gelijk is aan het aantal lijnstukken waarin L verdeeld wordt ($= n$). Nu levert elk zo'n gebied juist twee nieuwe gebieden. Dus het aantal gebieden a_n is gelijk aan $a_{n-1} + n$. Nu lossen we deze recurrente betrekking op. De oplossing voor het homogene vraagstuk is een constante, stel α. Een particuliere oplossing wordt gegeven door $\beta_0 n + \beta_1 n^2$, substitutie in de recurrente betrekking geeft ons $\beta_0 n + \beta_1 n^2 = \beta_0(n-1) + \beta_1(n-1)^2 + n$ of $0 = -\beta_0 + \beta_1$, $0 = -2\beta_1 + 1$. Hieruit volgt dan dat

$$a_n^{(p)} = \frac{n(n+1)}{2}$$

en dat de algemene oplossing gegeven wordt door

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha + \frac{n(n+1)}{2}.$$

Omdat $a_1 = 2$ volgt dat $\alpha = 1$.

Examen oefening 44 (1ste zit, 1991-1992) *Laat a_n het aantal* woorden *van lengte n zijn met letters uit het alfabet $\{0,1,2,3\}$ waarin een oneven aantal nullen voorkomen.*

(a) Bewijs dat $a_{n+1} = 2a_n + 4^n, \forall n \in \mathbb{N}$.

(b) Zoek de waarde van een algemene term uit de rij $(a_k)_{k\in\mathbb{N}}$.

(c) Stel de voortbrengende functie op die bij dit probleem behoort.

Oplossing.

(a) De beginvoorwaarden voor het probleem zijn $a_1 = 1$ en $a_2 = 6$ want er is maar één oplossing, namelijk 0, van lengte 1 en er zijn 6 oplossingen, namelijk $01, 02, 03, 10, 20, 30$, van lengte 2.

Om de recursieve betrekking te vinden, beschouw alle 4^n geordende n-tallen over $\{0, 1, 2, 3\}$. Precies a_n hiervan hebben een oneven aantal keer nul, terwijl $4^n - a_n$ van deze n-tallen een even aantal keer nul hebben.

Als er in zo'n n-tal een even aantal keer nul staat, dan moet er nul bijgevoegd worden om een $(n+1)$-tal te bekomen met een oneven aantal keer nul. Dit geeft al $4^n - a_n$ oplossingen van lengte $n + 1$.

Als er echter een oneven aantal keer nul staat in het n-tal, dan moet er $1, 2$ of 3 toegevoegd worden om een $(n + 1)$-tal te verkrijgen met een oneven aantal keer nul. Op deze manier bekomen we $3a_n$ andere oplossingen van lengte $n + 1$.

Dus $a_{n+1} = 4^n - a_n + 3a_n = 2a_n + 4^n$. Om deze recurrente betrekking te doen gelden vanaf $n = 0$, stel $a_0 = 0$.

(b) De karakteristieke vergelijking van de corresponderende homogene recurrente betrekking $a_{n+1} = 2a_n$ is $R - 2 = 0$. Bijgevolg is een algemene oplossing van de homogene recurrente betrekking $a_n^{(h)} = \alpha_1 2^n, n \geq 0$.

Een particuliere oplossing van de niet-homogene recurrente betrekking is $a_n^{(p)} = \alpha n^t 4^n$ waarbij t de multipliciteit is van 4 als oplossing van $R - 2 = 0$. Dus $t = 0$ en $a_n^{(p)} = \alpha 4^n$.

De precieze waarde van α kan enkel gevonden worden door substitutie van $a_n^{(p)}$ in de niet-homogene recurrente betrekking. Dit geeft

$$\begin{array}{rcl} \alpha 4^{n+1} & = & 2\alpha 4^n + 4^n \\ & \Updownarrow & \\ 4\alpha & = & 2\alpha + 1 \end{array}$$

en deze laatste vergelijking impliceert dat $\alpha = 1/2$. Dus is

$$a_n^{(p)} = \frac{1}{2} 4^n$$

en

$$a_n = a_n^{(p)} + a_n^{(h)} = \frac{1}{2} 4^n + \alpha_1 2^n. \tag{3.1}$$

De beginvoorwaarde $a_1 = 1$ levert de precieze waarde van de vrijheidsgraad α_1. Substitutie van $n = 1$ en $a_1 = 1$ in (3.1) impliceert dat $1 = 2\alpha_1 + 2$, m.a.w. $\alpha_1 = -1/2$.

Dit toont aan dat

$$a_n = \frac{1}{2}4^n - \frac{1}{2}2^n, \qquad n \geq 0.$$

(c) Zie Extra Oefening 38.

Examen oefening 45 (1ste zit, 1992-1993) *Een computer aanvaardt als paswoord elke rij cijfers die een even aantal maal het cijfer 0 bevat. Noem a_n het aantal paswoorden van lengte n.*

(a) Bereken a_1 en a_2.

(b) Bewijs dat de recurrente betrekking van a_n gegeven wordt door:

$$a_n = 8a_{n-1} + 10^{n-1}.$$

(c) Los de recurrente betrekking op.

Oplossing.

(a) Er zijn precies $a_1 = 9$ paswoorden van lengte 1. Zo'n paswoord van lengte 1 bestaat uit een cijfer verschillend van nul. Het aantal paswoorden van lengte 2 is $a_2 = 100 - 18 = 82$ daar er 18 rijen cijfers van de vorm $x0$ of $0x$, met $x \in \{1, \ldots, 9\}$, zijn die niet aanvaard kunnen worden als paswoord.

(b) Neem een paswoord bestaande uit n cijfers. Als dit paswoord eindigt op 0, dan bevatten de $n-1$ eerste cijfers een oneven aantal keer 0. Dit is dus een slecht paswoord van lengte $n-1$ en hiervan zijn er precies $10^{n-1} - a_{n-1}$.

Eindigt dit paswoord niet op 0, dan vormen de $n-1$ eerste cijfers een goed paswoord van lengte $n-1$. Een goed paswoord van lengte $n-1$ kan op 9 manieren uitgebreid worden tot een paswoord van lengte n door

er de cijfers $1, \ldots, 9$ aan toe te voegen. Zo zijn er $9a_{n-1}$ paswoorden van lengte n die niet op 0 eindigen.

Het totale aantal paswoorden van lengte n is dus

$$a_n = 9a_{n-1} + 10^{n-1} - a_{n-1} = 8a_{n-1} + 10^{n-1}.$$

(c) De homogene recurrente betrekking is $a_n = 8a_{n-1}$ en die heeft als karakteristieke vergelijking $R - 8 = 0$, dus een algemene oplossing voor het homogeen probleem is $a_n^{(h)} = \alpha_1 8^n$.

Een particuliere oplossing is $a_n^{(p)} = \alpha_2 n^t 10^n$ waarbij t de multipliciteit is van 10 als oplossing van $R-8 = 0$. Dit betekent $t = 0$, dus $a_n^{(p)} = \alpha_2 10^n$.

De waarde van α_2 wordt gevonden door substitutie in de niet-homogene recurrente betrekking. Dit geeft

$$\begin{array}{rcl} \alpha_2 10^n & = & 8\alpha_2 10^{n-1} + 10^{n-1} \\ & \Updownarrow & \\ 10\alpha_2 & = & 8\alpha_2 + 1 \end{array}$$

en dit impliceert dat $\alpha_2 = 1/2$.

Dus

$$a_n^{(p)} = \frac{1}{2} 10^n$$

en

$$a_n = a_n^{(p)} + a_n^{(h)} = \frac{1}{2} 10^n + \alpha_1 8^n. \tag{3.2}$$

De beginvoorwaarde $a_1 = 9$ levert de precieze waarde van de vrijheidsgraad α_1. Substitutie van $n = 1$ en $a_1 = 9$ in (3.2) impliceert dat $9 = 8\alpha_1 + 5$, m.a.w. $\alpha_1 = 1/2$.

Dit betekent dat

$$a_n = \frac{1}{2} 10^n + \frac{1}{2} 8^n, \qquad n \geq 1.$$

Examen oefening 46 (1ste zit, 1993-1994) *Men beschouwt n ($n \geq 1$) cirkels in het vlak zodat*

(a) elke cirkel alle andere cirkels in 2 verschillende punten snijdt;

(b) geen 3 cirkels een punt gemeen hebben.

Zij a_n het aantal gebieden waarin het vlak verdeeld wordt door deze cirkels. Bepaal een recurrente betrekking voor a_n en los deze recurrente betrekking op.

Oplossing. De eerste waarden zijn $a_1 = 2; a_2 = 4$ en $a_2 = 8$.

Algemeen geldt

$$a_n = a_{n-1} + 2(n-1)$$

want de $n$de cirkel snijdt de $n-1$ andere cirkels in $2n-2$ punten $d_1, \ldots, d_{2n-2}$. Elk lijnstuk $d_1d_2, d_2d_3, \ldots, d_{2n-3}d_{2n-2}, d_{2n-2}d_1$ verdeelt, bij het bijvoegen van de n^{de} cirkel, een gebied in twee delen. Er zijn dus $2n-2$ nieuwe gebieden bijgekomen waardoor $a_n = a_{n-1} + 2(n-1)$.

Om de oplossingen voor $a_n = a_{n-1} + 2(n-1)$ te vinden, zoeken we eerst de oplossingen voor het homogeen deel

$$a_n = a_{n-1}.$$

Dit heeft $R-1 = 0$ als karakteristieke vergelijking waardoor de homogene oplossingen $a_n^{(h)} = \alpha$ zijn.

Een particuliere oplossing voor het niet-homogeen deel is

$$a_n^{(p)} = \alpha_0 n + \alpha_1 n^2$$

daar $a_n = a_{n-1} + f(n)$ met $f(n) = 2n-2$, graad$(f) = 1$, en daar $R = 1$ een nulpunt is van de karakteristieke vergelijking.

Substitutie in de niet-homogene vergelijking geeft

$$\begin{array}{rcl} \alpha_0 n + \alpha_1 n^2 & = & \alpha_0(n-1) + \alpha_1(n-1)^2 + 2(n-1) \\ & \Updownarrow & \\ 0 & = & -\alpha_0 + \alpha_1(-2n+1) + 2n - 2 \end{array}$$

$$\Updownarrow$$

$$\left\{ \begin{array}{l} -\alpha_0 + \alpha_1 - 2 = 0 \\ -2\alpha_1 + 2 = 0 \end{array} \right. \iff \left\{ \begin{array}{l} \alpha_0 = -1 \\ \alpha_1 = 1. \end{array} \right.$$

Dus $a_n^{(p)} = -n + n^2$ waardoor alle oplossingen $a_n = a_n^{(h)} + a_n^{(p)} = \alpha - n + n^2$ zijn.

Daar $a_1 = 2$ moet $2 = \alpha - 1 + 1$, waardoor $\alpha = 2$.

Het besluit is:

$a_n = 2 - n + n^2$.

Examen oefening 47 (1ste zit, 1994-1995) *Beschouw de driehoekige getallentabel met* $0, 1, 2, 3, \ldots$, *langs de buitenzijden en waarbij een getal "binnenin" verkregen wordt door de som te nemen van de twee aanliggende getallen in de vorige rij en het getal dat 2 rijen erboven staat.*

Het begin van de tabel ziet er dus als volgt uit:

$$\begin{array}{ccccccccccc} & & & & 0 & & & & & & \\ & & & 1 & & & 1 & & & & \\ & & 2 & & & 2 & & & 2 & & \\ & 3 & & & 5 & & & 5 & & & 3 \\ 4 & & & 10 & & & 12 & & & 10 & & & 4 \end{array}$$

Noem a_n *de som van de getallen in rij* n*, dus* $a_0 = 0$, $a_4 = 40$.

(a) Bewijs dat a_n *voldoet aan de recurrente betrekking*

$$a_n = 2a_{n-1} + a_{n-2} + 2, \qquad n \geq 2, \qquad a_0 = 0, a_1 = 2.$$

(b) Los de recurrente betrekking op.

(c) Stel de voortbrengende functie op die bij dit probleem hoort.

Oplossing.

(a) Er geldt dat

$$a_n = 2n + (2a_{n-1} - 2(n-1)) + a_{n-2}$$

daar de som van de getallen op rij n gelijk is aan de som van de buitenste getallen (dit verklaart de term $2n$), twee keer de som van de getallen op de voorgaande rij min $2(n-1)$ daar de buitenste getallen op rij $n-1$ maar één keer meegeteld worden (dit verklaart de term $2a_{n-1} - 2(n-1)$), plus de som van de getallen op rij $n-2$ (dit verklaart de term a_{n-2}).

Bijgevolg $a_n = 2a_{n-1} + a_{n-2} + 2$.

(b) We lossen eerst het homogeen gedeelte $a_n = 2a_{n-1} + a_{n-2}$ op. De karakteristieke vergelijking is $R^2 - 2R - 1$ wat $R = 1 \pm \sqrt{2}$ als nulpunten heeft. Dus zijn de oplossingen voor het homogeen gedeelte gelijk aan

$$a_n^{(h)} = \alpha_1(1 + \sqrt{2})^n + \alpha_2(1 - \sqrt{2})^n.$$

De particuliere oplossing is $a_n^{(p)} = \alpha_3$ want het niet-homogeen gedeelte is gelijk aan de constante $f(n) = 2$, en $R = 1$ is geen nulpunt van de karakteristieke vergelijking.

Substitutie in de niet-homogene recurrente betrekking geeft

$$\alpha_3 = 2\alpha_3 + \alpha_3 + 2$$

waardoor $\alpha_3 = -1$.

Dus

$$a_n = \alpha_1(1+\sqrt{2})^n + \alpha_2(1-\sqrt{2})^n - 1.$$

Invullen van de beginvoorwaarden $a_0 = 0$ en $a_1 = 2$ levert

$$\begin{cases} \alpha_1 + \alpha_2 = 1 \\ \alpha_1(1+\sqrt{2}) + \alpha_2(1-\sqrt{2}) = 3 \end{cases} \iff \begin{cases} \alpha_1 = \frac{1+\sqrt{2}}{2} \\ \alpha_2 = \frac{1-\sqrt{2}}{2}. \end{cases}$$

Dit impliceert dat

$$a_n = \frac{(1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}}{2} - 1.$$

(c) De genererende functie is

$$\begin{aligned} g(x) &= \sum_{n=0}^{+\infty} a_n x^n \\ &= \tfrac{(1+\sqrt{2})}{2} \sum_{n=0}^{+\infty} ((1+\sqrt{2})x)^n + \tfrac{(1-\sqrt{2})}{2} \sum_{n=0}^{+\infty} ((1-\sqrt{2})x)^n - \sum_{n=0}^{+\infty} x^n \\ &= \tfrac{1+\sqrt{2}}{2(1-(1+\sqrt{2})x)} + \tfrac{1-\sqrt{2}}{2(1-(1-\sqrt{2})x)} - \tfrac{1}{1-x} \\ &= \tfrac{2x}{x^3+x^2-3x+1}. \end{aligned}$$

Examen oefening 48 (2de zit, 1995-1996) *Bereken* $s_n = 1 \cdot 2 + 3 \cdot 4 + 5 \cdot 6 + \cdots + (2n-1) \cdot (2n)$, $n \geq 1$. *(Hulp: Stel de recurrente betrekking op voor* s_n *en los deze op.)*

Oplossing. Stel $a_n = 1 \cdot 2 + 3 \cdot 4 + 5 \cdot 6 + \cdots + (2n-1) \cdot (2n)$, dan is $a_n = a_{n-1} + 4n^2 - 2n$.

De algemene oplossing voor de homogene recurrente betrekking is $a_n^{(h)} = \alpha$ daar in de homogene recurrente betrekking $a_n = a_{n-1}$.

De karakteristieke vergelijking voor deze homogene recurrente betrekking is $R - 1 = 0$. Daar $R = 1$ een enkelvoudig nulpunt is van de karakteristieke vergelijking, is een particuliere oplossing gelijk aan $a_n^{(p)} = \alpha_0 n + \alpha_1 n^2 + \alpha_2 n^3$ waarbij de waarden van $\alpha_0, \alpha_1, \alpha_2$ gevonden worden door $a_n^{(p)}$ te substitueren in de niet-homogene recurrente betrekking.

Substitutie levert

$$\alpha_0 n + \alpha_1 n^2 + \alpha_2 n^3 = \alpha_0(n-1) + \alpha_1(n-1)^2 + \alpha_2(n-1)^3 + 4n^2 - 2n.$$

Door de coëfficienten van n, n^2, n^3 rechts en links gelijk te stellen, bekomen we het stelsel

$$\left\{ \begin{array}{rcl} -\alpha_0 + \alpha_1 - \alpha_2 & = & 0 \\ -2\alpha_1 + 3\alpha_2 & = & 2 \\ 3\alpha_2 & = & 4 \end{array} \right. \Longleftrightarrow \left\{ \begin{array}{rcl} \alpha_0 & = & -1/3 \\ \alpha_1 & = & 1 \\ \alpha_2 & = & 4/3. \end{array} \right.$$

Dit betekent dat $a_n^{(p)} = -n/3 + n^2 + 4n^3/3$ en dus $a_n = \alpha - n/3 + n^2 + 4n^3/3$.

De exacte waarde van α volgt uit de beginvoorwaarde $a_1 = 2$. Substitutie van $n = 1$ impliceert $2 = \alpha + 2$, en dus $\alpha = 0$.

Het besluit is dat $a_n = -n/3 + n^2 + 4n^3/3$.

Examen oefening 49 (2de zit, 1996-1997) *Onderstel dat er n personen ($n \geq 2$) op een receptie zijn. Elke persoon zal juist éénmaal een hand geven aan alle andere aanwezigen (en dus niet aan zichzelf).*

(a) Bewijs dat de recurrente betrekking voor het bepalen van het totale aantal keer dat handen werden geschud, gegeven wordt door:

$$a_{n+1} = a_n + n \ .$$

(b) Vind de nodige beginvoorwaarde(n).

(c) Los de recurrente betrekking op.

Oplossing.

(a)+(b) Voor $n = 2$ wordt er juist eenmaal een hand gegeven, dus $a_n = 1$. Voor drie personen wordt dat driemaal, dus $a_3 = 3 = 1 + 2$. Onderstel dat a_n het aantal keer handen schudden telt bij n aanwezigen. Als daar een nieuwe persoon bijkomt, geeft deze aan iedereen die al aanwezig was een hand, zodat het aantal keer dat handen werden geschud inderdaad gegeven wordt door $a_{n+1} = a_n + n$.

(c) De homogene betrekking is $a_{n+1} = a_n$, dus de karakteristieke vergelijking is $r - 1 = 0$, dus $r = 1$. Hieruit volgt dat $a_n^{(h)} = \alpha \cdot 1^n = \alpha$. Het niet homogeen deel van de betrekking is n, een veelterm in n van de graad 1. Daar de multipliciteit van 1 als oplossing van de karakteristieke vergelijking van de homogene recurrente betrekking 1 is, is de particuliere oplossing van de vorm: ${a_n}^{(p)} = \beta \cdot n + \gamma \cdot n^2$. Als we ${a_n}^{(p)}$ substitueren in de recurrente betrekking, dan bekomen we:

$$\beta(n+1) + \gamma(n+1)^2 = \beta n + \gamma n^2 + n,$$

wat het volgende stelsel oplevert:

$$\begin{cases} 2\gamma & = & 1 \\ \beta + \gamma & = & 0. \end{cases}$$

Dus als oplossing vinden we dat $\beta = -1/2$ en $\gamma = 1/2$. Dit geeft ons ${a_n}^{(p)} = -\frac{1}{2}n + \frac{1}{2}n^2$. De algemene oplossing is dus van de vorm $a_n = \alpha - \frac{1}{2}n + \frac{1}{2}n^2$. Uit de beginvoorwaarde $a_2 = 2$ halen we tenslotte dat $1 = \alpha + 2 - 1$ dus $\alpha = 0$. We vinden als algemene term:

$$a_n = \frac{1}{2}n(n-1).$$

Examen oefening 50 (1ste zit, 1997-1998) *Je beschikt over 4 symbolen* $\{0, 1, 2, 3\}$ *waarmee rijen moeten gevormd worden van lengte* n*. In deze rijen moet minstens één 1 voorkomen. Bovendien mag de eerste 0 niet vóór de eerste 1 voorkomen (er moet geen 0 voorkomen in de rij). Zij* a_n *het aantal dergelijke rijen van lengte* n*.*

(1) Toon aan dat de recurrente betrekking voor dit probleem $a_n = 4a_{n-1} + 2^{n-1}$ *is, voor* $n \geq 1$*.*

(2) Bereken a_n, recursief gedefinieerd door deze betrekking en in de veronderstelling dat $a_0 = 0$.

Oplossing. (1) We bekijken een aantal korte rijtjes om een idee te krijgen van de recurrente betrekking. De enige rij van lengte 1 is '1', dus $a_1 = 1$. Er zijn 6 mogelijke rijen van twee symbolen: '10', '11', '12', '13', '21' en '31', dus $a_2 = 6$. Uitschrijven van alle mogelijkheden levert ons 28 rijen van lengte 3 die voldoen aan alle voorwaarden.
Om de algemene betrekking voor rijen van lengte n te vinden, tellen we de het aantal van die rijen als volgt. Er zijn a_{n-1} rijen van lengte $n-1$, die allemaal aan de voorwaarden voldoen: ze bevatten minstens een 1 en er komt geen 0 voor vóór de eerste 1. Al deze rijen kunnen we uitbreiden tot een rij van lengte n door achteraan één van de vier symbolen toe te voegen, wat ons de term $4a_{n-1}$ oplevert. Er bestaan echter ook rijen waarin slechts één 1 voorkomt. Indien dit niet op de laatste (n-de) plaats is, zijn deze rijen reeds geteld in a_{n-1}. We moeten dus nog het aantal rijen tellen van lengte n met een 1 op de laatste plaats. Dit zijn er 2^{n-1}, omdat op elke plaats vóór de 1 enkel een 2 of een 3 kan staan. We vinden inderdaad dat $a_n = 4a_{n-1} + 2^{n-1}$.
(2) De recurrente betrekking $a_n = 4a_{n-1} + 2^{n-1}$ is niet-homogeen. De karakteristieke vergelijking van de corresponderende homogene betrekking is $r - 4 = 0$. De oplossing voor de homogene recurrente betrekking is dus ${a_n}^h = \alpha 4^n$.
Het niet-homogene deel van de betrekking is $f(n) = 2^{n-1} = \frac{1}{2}2^n$. Daar 2 geen oplossing is van de karakteristieke vergelijking is de multipliciteit t gelijk aan 0, en dus weten we dat een particuliere oplossing van de recurrente betrekking in dit geval gegeven wordt door ${a_n}^p = \beta 2^n$ (stelling 3.3 in de cursus).
Om β te bepalen substitueren we ${a_n}^p$ in de recurrente betrekking. Dit levert ons het volgende op:

$$\begin{aligned} \beta 2^n &= 4\beta 2^{n-1} + 2^{n-1}, \text{ of} \\ 2\beta &= 4\beta + 1, \text{ of} \\ \beta &= -\frac{1}{2}. \end{aligned}$$

De algemene oplossing wordt gegeven door $a_n = {a_n}^h + {a_n}^p = \alpha 4^n - 2^{n-1}$. Met behulp van de beginvoorwaarde $a_0 = 0$ bepalen we α:

$$a_0 = 0 = \alpha 1 - 2^{-1} = \alpha - \frac{1}{2} \Longrightarrow \alpha = \frac{1}{2}.$$

We vinden als oplossing van de recurrente betrekking: $a_n = \frac{1}{2}4^n - 2^{n-1}$.

Examen oefening 51 (2de zit, 1998-1999) *Los de volgende recurrente betrekkingen op:*

(a) $a_n = 3a_{n-1} - 4n$;

(b) $b_n = 3b_{n-1} + 3(2^n)$;

(c) $c_n = 3c_{n-1} - 4n + 3(2^n)$.

Oplossing.

(a) De homogene recurrente betrekking is $a_n = 3a_{n-1}$, en die heeft als karakteristieke vergelijking $R - 3 = 0$. Dus een algemene oplossing voor het homogeen probleem is $a_n^{(h)} = \alpha 3^n$. Een particuliere oplossing is $a_n^{(p)} = \beta + \gamma n$. De waarden van β en γ worden gevonden door substitutie in de niet-homogene recurrente betrekking. Dit geeft $\beta + \gamma n = 3(\beta + \gamma(n-1)) - 4n$. Dus is $\beta = 3\beta - 3\gamma$ en $\gamma = 3\gamma - 4$. Dus is $\beta = 3$ en $\gamma = 2$. We krijgen dus $a_n^{(p)} = 3 + 2n$ en $a_n = a_n^{(h)} + a_n^{(p)} = \alpha 3^n + 2n + 3$.

(b) De homogene recurrente betrekking is $b_n = 3b_{n-1}$ en die heeft als oplossing $b_n^{(h)} = \alpha 3^n$. Een particuliere oplossing is $b_n^{(p)} = \delta 2^n$. De waarde van δ wordt gevonden door substitutie in de niet-homogene recurrente betrekking. Dit geeft $\delta 2^n = 3\delta 2^{n-1} + 3(2^n)$. Dus is $\delta = -6$. We krijgen dus $b_n = b_n^{(h)} + b_n^{(p)} = \alpha 3^n - 6(2^n)$.

(c) De homogene recurrente betrekking is $c_n = 3c_{n-1}$ en die heeft als oplossing $c_n^{(h)} = \alpha 3^n$. Een particuliere oplossing is $c_n^{(p)} = a_n^{(p)} + b_n^{(p)}$. Dit verifieren we door substitutie van $c_n^{(p)}$ in de niet-homogene recurrente betrekking.
Dus is $c_n = \alpha 3^n + 2n + 3(1 - 2^{n+1})$.

Examen oefening 52 (1ste zit, 1999-2000) *Op een blad papier tekenen we n willekeurige driehoeken zodat elke driehoek elke andere driehoek snijdt in precies twee punten. Een snijpunt is nooit bevat in drie driehoeken. Zoek de recurrente betrekking voor het aantal gebieden waarin het blad verdeeld wordt door deze driehoeken, en los deze recurrente betrekking op.*

Oplossing. Zij a_n het aantal gebieden waarin het vlak verdeeld wordt door deze driehoeken. De eerste waarden zijn $a_1 = 2; a_2 = 4$ en $a_2 = 8$. Algemeen geldt $a_n = a_{n-1} + 2(n-1)$ want de n^{de} driehoek snijdt de $n-1$ andere driehoeken in $2n-2$ punten $d_1, \ldots, d_{2n-2}$. De omtrek van de n^{de} driehoek wordt dus verdeeld in $2n-2$ delen. Er zijn dus $2n-2$ nieuwe gebieden bijgekomen waardoor $a_n = a_{n-1} + 2(n-1)$.

Om de oplossingen voor $a_n = a_{n-1} + 2(n-1)$ te vinden, zoeken we eerst de oplossingen voor het homogeen deel $a_n = a_{n-1}$. Dit heeft $x - 1 = 0$ als karakteristieke vergelijking waardoor de homogene oplossingen $a_n^{(h)} = \alpha$ zijn. Een particuliere oplossing voor het niet-homogeen deel is $a_n^{(p)} = \alpha_0 n + \alpha_1 n^2$ daar $a_n = a_{n-1} + f(n)$ met $f(n) = 2n - 2$, graad$(f) = 1$, en daar $x = 1$ een nulpunt is van de karakteristieke vergelijking. Substitutie in de niet-homogene vergelijking geeft

$$\begin{array}{rcl} \alpha_0 n + \alpha_1 n^2 & = & \alpha_0(n-1) + \alpha_1(n-1)^2 + 2(n-1) \\ & \Updownarrow & \\ 0 & = & -\alpha_0 + \alpha_1(-2n+1) + 2n - 2 \end{array}$$

$$\Updownarrow$$

$$\left\{ \begin{array}{l} -\alpha_0 + \alpha_1 - 2 = 0 \\ -2\alpha_1 + 2 = 0 \end{array} \right. \iff \left\{ \begin{array}{l} \alpha_0 = -1 \\ \alpha_1 = 1. \end{array} \right.$$

Dus $a_n^{(p)} = -n + n^2$ waardoor alle oplossingen $a_n = a_n^{(h)} + a_n^{(p)} = \alpha - n + n^2$ zijn. Daar $a_1 = 2$ moet $2 = \alpha - 1 + 1$, waardoor $\alpha = 2$. Het besluit is: $a_n = 2 - n + n^2$.

Extra Oefening 53 *Zij a_n het aantal rijen van lengte n, enkel bestaande uit 0,1,2 en 3 zodat de som van 2 opeenvolgende getallen nooit deelbaar is door 3. Bepaal een recurrente betrekking voor a_n en los ze op. (Merk op: 2 keer 0 achter elkaar is niet toegelaten.)*

Oplossing. Vooreerst stellen we de recurrente betrekking op. Beschouw alle oplossingen van lengte $n-1$. Veronderstel dat er b_{n-1} eindigen op 1, c_{n-1} op 2, en d_{n-1} op 0 of 3. Dan is $a_n = b_{n-1} + c_{n-1} + d_{n-1}$. Ook $b_n = b_{n-1} + d_{n-1}$ want voor 1 mag 1,0 of 3 staan, $c_n = d_{n-1} + c_{n-1}$ want voor 2 mag 0, 2 of 3 staan, en $d_n = 2(b_{n-1} + c_{n-1})$ want na 1 of 2 mag 0 of 3 toegevoegd worden.

Dit betekent

$$\begin{aligned} a_n &= b_n + c_n + d_n \\ &= 3b_{n-1} + 3c_{n-1} + 2d_{n-1} \\ &= a_{n-1} + 2b_{n-1} + 2c_{n-1} + d_{n-1} \\ &= a_{n-1} + 2(b_{n-2} + d_{n-2}) + 2(c_{n-2} + d_{n-2}) + 2(b_{n-2} + c_{n-2}) \\ &= a_{n-1} + 4(b_{n-2} + d_{n-2} + c + n - 2) \\ &= a_{n-1} + 4a_{n-2} \end{aligned}$$

Nu lossen we deze homogene recurrente betrekking op. De karakteristieke vergelijking $x^2 - x - 4 = 0$ heeft als oplossingen $(1+\sqrt{17})/2$ en $(1-\sqrt{17})/2$. Dus de algemene oplossing is van de vorm

$$a_n = \alpha_1 \left(\frac{1+\sqrt{17}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{17}}{2}\right)^n .$$

Invullen van de beginvoorwaarden geeft

$$\alpha_1 = \frac{13 + 3\sqrt{17}}{4\sqrt{17}}$$

en

$$\alpha_2 = \frac{-13 + 3\sqrt{17}}{4\sqrt{17}}.$$

Examen oefening 54 (1ste zit, 1998-1999) *Laat a_n het aantal woorden van lengte n zijn van letters uit het alfabet $\{A,B,C,D\}$ en met een even aantal A's en een even aantal B's.*

(a) *Bewijs dat $a_n = 2a_{n-1} + \frac{1}{2}4^{n-1}, \forall n \in \mathbb{N}$.*

(b) *Los deze recurrente betrekking op.*

(c) *Stel de voortbrengende functie op die behoort bij dit probleem.*

Oplossing.

(*a*) Laat nu b_n het aantal woorden van lengte n zijn van letters uit het alfabet {A,B,C,D} en met een even aantal A's en een oneven aantal B's. Laat c_n het aantal woorden van lengte n zijn van letters uit het alfabet {A,B,C,D} en met een oneven aantal A's en een even aantal B's. En laat d_n het aantal woorden van lengte n zijn van letters uit het alfabet {A,B,C,D} en met een oneven aantal A's en een oneven aantal B's. Dan is $d_n = 4^n - a_n - b_n - c_n$.

De beginvoorwaarden voor het probleem zijn $a_1 = 2$, namelijk C en D; $b_1 = 1$, namelijk B; en $c_1 = 1$, namelijk A.

Wanneer een woord van n letters begint met een A, dan moet het overblijvende gedeelte een woord zijn van $n-1$ letters met een oneven aantal A's en een even aantal B's opdat het totale woord een even aantal A's en een even aantal B's zou hebben. Wanneer het woord met n letters begint met een B, dan moet het overblijvende gedeelte een even aantal A's en een oneven aantal B's hebben. Wanneer het woord met n letters begint met een C, dan moet het overblijvende gedeelte een even aantal A's en een even aantal B's hebben. Tenslotte, wanneer een woord met n letters begint met een D, dan moet het overblijvende gedeelte een even aantal A's en een even aantal B's hebben. Dit geeft

$$a_n = c_{n-1} + b_{n-1} + 2a_{n-1}.$$

Analoog bekomen we

$$\begin{aligned} b_n &= (4^{n-1} - a_{n-1} - b_{n-1} - c_{n-1}) + a_{n-1} + 2b_{n-1} \\ &= 4^{n-1} + b_{n-1} - c_{n-1}, \end{aligned}$$

en

$$\begin{aligned} c_n &= a_{n-1} + (4^{n-1} - a_{n-1} - b_{n-1} - c_{n-1}) + 2c_{n-1} \\ &= 4^{n-1} - b_{n-1} + c_{n-1}. \end{aligned}$$

Nu beweren we dat $b_n = c_n$. Dit is zo voor $n = 1$. Stel dat $b_k = c_k$ voor een zekere k, dan is $b_{k+1} = 4^k + b_k - c_k = 4^k$ en $c_{k+1} = 4^k - b_k + c_k = 4^k$. Dus $b_{k+1} = c_{k+1} = 4^k$.

Dit levert $a_n = 2a_{n-1} + 4^{n-2} + 4^{n-2} = 2a_{n-1} + \frac{1}{2}4^{n-1}$.

(b) De karakteristieke vergelijking van de corresponderende homogene recurrente betrekking $a_n = 2a_{n-1}$ is $X - 2 = 0$. Bijgevolg is een algemene oplossing van de homogene recurrente betrekking $a_n^{(h)} = \alpha 2^n, n \geq 0$. Een particuliere oplossing van de niet-homogene recurrente betrekking is $a_n^{(p)} = \beta n^t 4^n$, waarbij t de multipliciteit is van 4 als oplossing van $X - 2 = 0$. Dus $t = 0$ en $a_n^{(h)} = \beta 4^n$. Substitutie in de niet-homogene recurrente betrekking levert $\beta 4^n = 2\beta 4^{n-1} + \frac{1}{2}4^{n-1}$, dus $4\beta 4^{n-1} = 4^{n-1}$ of $\beta = \frac{1}{4}$. Bijgevolg is $a_n^{(h)} = 4^{n-1}$.

De algemene oplossing is $a_n = a_n^{(p)} + a_n^{(h)} = \alpha 2^n + 4^{n-1}$. Substitutie van $n = 1$ en $a_1 = 2$ levert $2 = \alpha 2 + 1$, dus $\alpha = \frac{1}{2}$.

Dit toont aan dat $a_n = 2^{n-1} + 4^{n-1}$.

(c) Zie Extra Oefening 40.

3.3 Recurrente betrekkingen en voortbrengende functies

3.4 Zuinig en onzuinig sorteren

3.5 Differentierijen

Examen oefening 55 (2de zit, 1994-1995) *Los het volgend stelsel recurrente betrekkingen op:*

$$\begin{cases} a_n &= 3a_{n-1} + 2b_{n-1}, & n \geq 1 \\ b_n &= a_{n-1} + 2b_{n-1}, & n \geq 1 \end{cases}$$

met $a_0 = 1$ en $b_0 = 2$. (Herleid hiertoe het stelsel tot een lineaire recurrente betrekking voor b_{n+1}, met $n \geq 1$)

Oplossing. We herschrijven de tweede vergelijking als $a_{n-1} = b_n - 2b_{n-1}$ en substitueren dit in de eerste vergelijking. Dit geeft

$$a_n = 3(b_n - 2b_{n-1}) + 2b_{n-1} = 3b_n - 4b_{n-1}.$$

Als nu in $a_{n-1} = b_n - 2b_{n-1}$ de index n vervangen wordt door $n+1$, dan bekomen we $a_n = b_{n+1} - 2b_n$.

Uit

$$a_n = b_{n+1} - 2b_n = 3b_n - 4b_{n-1}$$

volgt

$$b_{n+1} = 5b_n - 4b_{n-1}.$$

De karakteristieke vergelijking van deze homogene lineaire recurrente betrekking is $R^2 - 5R + 4$ met nulpunten $R = 4$ en $R = 1$ waardoor

$$b_n = \alpha_1 \cdot 4^n + \alpha_2 \cdot 1^n = \alpha_1 \cdot 4^n + \alpha_2.$$

De beginvoorwaarden zijn $a_0 = 1; a_1 = 7; a_2 = 31$ en $b_0 = 2; b_1 = 5; b_2 = 17$ waardoor voor $n = 0$ en $n = 1$

$$\begin{cases} \alpha_1 + \alpha_2 = 2 \\ 4\alpha_1 + \alpha_2 = 5 \end{cases} \iff \begin{cases} \alpha_1 = 1 \\ \alpha_2 = 1. \end{cases}$$

Dus $b_n = 4^n + 1$.

Daar $a_n = 3b_n - 4b_{n-1} = 3(4^n + 1) - 4(4^{n-1} + 1)$, bekomen we

$$a_n = 2 \cdot 4^n - 1.$$

Examen oefening 56 (2de zit, 1998-1999) *De Fibonacci rij wordt gedefinieerd door de recursieve betrekking $f_n = f_{n-1} + f_{n-2}$, met als beginvoorwaarden $f_0 = f_1 = 1$.*

(*a*) *Bewijs dat het Fibonacci getal f_n even is als en slechts als $n = 3k + 2$, waarbij $k \in \mathbb{N}$ (hint: beschouw f_{3k}, f_{3k+1} en f_{3k+2}).*

(*b*) *Bewijs dat elk vijfde Fibonacci getal een veelvoud is van 5.*

Oplossing.

(*a*) De verzameling van de niet-negatieve gehele getallen kunnen als volgt verdeeld worden in drie disjuncte verzamelingen:

$$\begin{aligned} A &= \{1, 4, 7, 10, 13 \ldots\} = \{3k + 1 | k = 0, 1, 2, \ldots\} \\ B &= \{2, 5, 8, 11, 14 \ldots\} = \{3k + 2 | k = 0, 1, 2, \ldots\} \\ C &= \{0, 3, 6, 9, 12 \ldots\} = \{3k | k = 0, 1, 2, \ldots\}. \end{aligned}$$

Via inductie bewijzen we dat f_n even is wanneer $n \in B$ en oneven wanneer $n \in A$ of $n \in C$. De bewering is geldig voor $k = 0$. Stel dat dit ook geldig is voor een waarde k, i.e. f_{3k+1} en f_{3k} zijn oneven en f_{3k+2} is even. Dan geldt

$$\begin{aligned} f_{3(k+1)+1} &= f_{3k+4} = f_{3k+3} + f_{3k+2} \\ &= f_{3k+1} + 2f_{3k+2} = \text{ oneven } + \text{ even } = \text{ oneven} \\ f_{3(k+1)} &= f_{3k+2} + f_{3k+1} = \text{ even } + \text{ oneven } = \text{ oneven} \\ f_{3(k+1)+2} &= f_{3k+5} = f_{3k+4} + f_{3k+3} \\ &= f_{3k} + f_{3k+1} + 2f_{3k+3} \\ &= \text{ oneven } + \text{ oneven } + \text{ even } = \text{ even }. \end{aligned}$$

De bewering is dus ook correct voor $k + 1$.

(b) Merk op dat f_{n-1} het n-de Fibonacci getal is. We moeten dus aantonen dat f_{5k-1} ($k = 1, 2, 3, \ldots$) deelbaar is door vijf. Nu is $f_4 = 5$ en

$$f_{5(k+1)-1} = f_{5k+4} = f_{5k+3} - f_{5k+2} = 3f_{5k+1} + 2f_{5k} = 5f_{5k} + 3f_{5k-1}.$$

Inductie levert het gewenste resultaat.

Examen oefening 57 (2de zit, 1992-1993) *Gegeven is de rij* $(a_i)_{i \in N}$ *die recursief gedefinieerd wordt door*

$$a_0 = 0, \qquad ia_i = (i-1)(a_{i-1} + 1), i \geq 1.$$

Bereken $\sum_{i=1}^{n} a_i$ *in functie van* n.

Oplossing. De beginvoorwaarden zijn

$$a_0 = 0, a_1 = 0, a_2 = \frac{1}{2}, a_3 = 1, a_4 = \frac{3}{2}, a_5 = 2, ...$$

en hieruit zou blijken dat $a_n = (n-1)/2$, $n \geq 1$.

Dit wordt bewezen door inductie. De formule is correct voor $n = 1$. Stel dat ze geldig is voor n, dan volgt uit de recurrente betrekking dat

$$(n+1)a_{n+1} = n(a_n + 1)$$

$$\begin{aligned} & \Updownarrow & (a_n = \frac{n-1}{2}) \\ &= n(\frac{n-1}{2}+1) \\ &= \frac{n(n+1)}{2} \\ & \Updownarrow \\ a_{n+1} &= \frac{n}{2} \end{aligned}$$

en dit toont aan dat inderdaad $a_n = (n-1)/2$ voor alle $n \geq 1$.

Bijgevolg is

$$\begin{aligned} \sum_{i=1}^{n} a_i &= \sum_{i=1}^{n} \frac{i-1}{2} \\ &= \frac{1}{2}\sum_{i=1}^{n} i - \sum_{i=1}^{n} \frac{1}{2} \\ &= \frac{1}{4}n(n+1) - \frac{n}{2} \\ &= \frac{n^2-n}{4}. \end{aligned}$$

Examen oefening 58 (2de zit, 1993-1994) *Los de volgende recurrente betrekking op:*

$$a_{n+2} = a_{n+1}a_n, \quad n \geq 2, \quad a_0 = 1, a_1 = 2.$$

Oplossing. De eerste waarden zijn $a_0 = 1; a_1 = 2; a_2 = 2; a_3 = 4 = 2^2; a_4 = 8 = 2^3$. Deze waarden zijn allemaal machten van 2. We bewijzen nu door inductie dat dit geldig is voor alle a_n.

Het is geldig voor $a_0 = 1 = 2^0$ en $a_1 = 2 = 2^1$. Als $a_{n-2} = 2^{b_{n-2}}$ en $a_{n-1} = 2^{b_{n-1}}$, dan is $a_n = a_{n-1}a_{n-2} = 2^{b_{n-2}+b_{n-1}}$ nog steeds een macht van 2.

We zien ook dat er een lineaire recurrente betrekking is voor de macht b_n met $a_n = 2^{b_n}$. Namelijk $b_n = b_{n-2} + b_{n-1}$ met $b_0 = 0$ en $b_1 = 1$.

Uit de cursus volgt

$$b_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

De beginvoorwaarden $b_0 = 0$ en $b_1 = 1$ impliceren

$$\begin{cases} \alpha_1 + \alpha_2 = 0 \\ \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right) = 1 \end{cases} \Longrightarrow \begin{cases} \alpha_1 = \frac{\sqrt{5}}{5} \\ \alpha_2 = -\frac{\sqrt{5}}{5}. \end{cases}$$

Dit betekent dat $a_n = 2^{b_n}$ met

$$b_n = \frac{\sqrt{5}}{5}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{\sqrt{5}}{5}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Hoofdstuk 4

Getaltheorie

4.1 Basisbegrippen

4.1.1 Deelbaarheid

4.1.2 Priemgetallen

4.1.3 Ontbinden in faktoren

4.2 Grootste gemene deler en kleinste gemeen veelvoud

Stelling 4.5

1. *Als* $a,\ b,\ c \in \mathbb{Z} : c \mid ab$ *en* $ggd(b,c) = 1$, *dan* $c \mid a$.
2. *Als* $a,\ b,\ c \in \mathbb{N} : (ac, bc) \neq (0,0)$, *dan is* $ggd(ca, cb) = c \cdot ggd(a,b)$.
3. *Als* $a,\ b,\ c \in \mathbb{Z} = (a,b) \neq (0,0)$ *en* $a,\ b \mid c$, *dan* $\frac{ab}{ggd(a,b)} \mid c$.
4. *Als* a *en* $b \in \mathbb{N} : (a,b) \neq (0,0)$, *dan is* $kgv(a,b) \cdot ggd(a,b) = ab$.
5. *Als* $a,\ b,\ c \in \mathbb{Z} : ggd(a,b) = 1$ *of* $ggd(a,c) = 1$ *of* $ggd(b,c) = 1$, *dan* $ggd(a,c) \cdot ggd(b,c) = ggd(ab,c)$. *Bijgevolg zijn* ab *en* c *relatief priem, als en slechts als zowel* a *en* c *als* b *en* c *relatief priem zijn.*

Bewijs

1. Uit het gegeven volgt dat er een koppel $(x, y) \in \mathbb{Z}^2$ bestaat waarvoor $bx+cy = 1$. Dus voor deze x en y geldt eveneens $abx+acy = a$. Omdat $c \mid abx$ en $c \mid acy$ zal ook $c \mid abx + acy = a$.

2. Beschouw de drie priemontbindingen van a, b en c:

$$\begin{aligned} a &= {p_1}^{a_1}{p_2}^{a_2}\cdots{p_k}^{a_k} \\ b &= {p_1}^{b_1}{p_2}^{b_2}\cdots{p_k}^{b_k} \\ c &= {p_1}^{c_1}{p_2}^{c_2}\cdots{p_k}^{c_k} \end{aligned}$$

   waarbij de exponenten 0 kunnen zijn. Dan hebben we

$$\begin{aligned} ca &= {p_1}^{c_1+a_1}{p_2}^{c_2+a_2}\cdots{p_k}^{c_k+a_k} \\ cb &= {p_1}^{c_1+b_1}{p_2}^{c_2+b_2}\cdots{p_k}^{c_k+b_k} \end{aligned}$$

   zodat $\text{ggd}(ca, cb) = {p_1}^{c_1+m_1}{p_2}^{c_2+m_2}\cdots{p_k}^{c_k+m_k}$, met $m_i = \min(a_i, b_i)$, $\forall i \in \mathbb{N}[1, k]$. Wat gelijk is aan $c\text{ggd}(a, b)$.

3. $a \mid c$ impliceert dat $a/\text{ggd}(a, b) \mid c$, eveneens geldt $b \mid c$ en $\text{ggd}(a/\text{ggd}(a, b), b) = 1$ waaruit volgt dat $b \cdot \frac{a}{\text{ggd}(a,b)} \mid c$.

4. Wegens het voorgaande, weten we dat

$$\frac{ab}{\text{ggd}(a, b)} \mid \text{kgv}(a, b).$$

   Omdat nu $ab/\text{ggd}(a, b)$ een veelvoud is van zowel a als b ($\text{ggd}(a, b) \mid a, b$) zal $\text{kgv}(a, b) \leq \frac{ab}{\text{ggd}(a,b)}$. We beschikken nu over twee ongelijkheden die de gevraagde gelijkheid oplevert.

5. Veronderstel eerst dat a en b relatief priem zijn, dan zijn $\text{ggd}(a, c)$ en $\text{ggd}(b, c)$ copriem die beide $\text{ggd}(ab, c)$ delen. Dus $\text{ggd}(a, c) \cdot \text{ggd}(b, c) \leq \text{ggd}(ab, c)$. Aangezien $\text{ggd}(ab, c)$ een deler is van ab, met a en b copriem, dan kunnen we stellen dat $\text{ggd}(ab, c) = d_1 \cdot d_2$ met $d_1 \mid a$ en $d_2 \mid b$. Duidelijkerwijze moet ook $d_1, d_2 \mid c$, zodat $\text{ggd}(ab, c) = d_1 \cdot d_2 \leq \text{ggd}(a, c) \cdot \text{ggd}(b, c)$. Dit geeft ons de gezochte gelijkheid.

□

Oefening 4.2.1 *1. Bewijs dat $4^{2n} - 1$ ($n \geq 1$) steeds deelbaar is door 15.*

2. *Zoek de grootste gemene deler d van 1320 en 714 en zoek de gehele getallen x en y zodanig dat $d = 1320x + 714y$.*

3. *Zoek een koppel $(x, y) \in \mathbb{Z}^2$ waarvoor geldt dat $325x + 26y = 91$.*

4. *Is 65537 een priemgetal?*

5. *Bewijs dat in de veronderstelling dat $ggd(a, b) = 1$, dan de $ggd(a+b, a-b)$ gelijk is aan 1 of 2.*

6. *Bewijs dat $\sqrt{2}$ een irrationaal getal is.*

7. *Bewijs dat er geen gehele getallen x, y, z en u, met $(x, y, z, u) \neq (0, 0, 0, 0)$, bestaan waarvoor $x^2 + y^2 - 3z^2 - 3u^2 = 0$.*

Oplossing.

1. We gebruiken induktie. Duidelijkerwijze is dit voldaan voor $n = 1$ (induktiebasis) en stel dit is voldaan voor $n = k$ (induktiehypothese). Dan is eveneens $16(4^{2k} - 1) + 15 = 4^{2(k+1)} - 1$ deelbaar door vijftien. Wegens het induktieprincipe is dit dus voldaan voor alle $n \geq 1$.

2. We passen het algoritme toe, besproken aan het begin van deze sectie. Dus

$$\begin{aligned} 1320 &= 1 \cdot 714 + 606 \\ 714 &= 1 \cdot 606 + 108 \\ 606 &= 5 \cdot 108 + 66 \\ 108 &= 1 \cdot 66 + 42 \\ 66 &= 1 \cdot 42 + 24 \\ 42 &= 1 \cdot 24 + 18 \\ 24 &= 1 \cdot 18 + 6 \\ 18 &= 3 \cdot 6 \end{aligned}$$

waaruit volgt dat $\text{ggd}(1320, 714) = 6$. De getallen x en y worden eveneens bepaald door dit algoritme, want hieruit volgt

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (42 - 24) \end{aligned}$$

$$\begin{aligned} &= 2 \cdot (66 - 42) - 42 \\ &= 2 \cdot 66 - 3 \cdot (108 - 66) \\ &= 5 \cdot (606 - 5 \cdot 108) - 3 \cdot 108 \\ &= 5 \cdot 606 - 28 \cdot (714 - 606) \\ &= 33 \cdot (1320 - 714) - 28 \cdot 714 = 1320 \cdot 33 - 714 \cdot 61. \end{aligned}$$

Dus $(x, y) = (33, -61)$.

3. Als we de grootste gemene deler van 325 en 26 berekenen, bekomen we 13. Dus er bestaat een kombinatie $325v + 26u = 13$. Met de methode gebruikt in de vorige oefening krijgen we $(v, u) = (1, -12)$, en dus $(x, y) = (7, -7 \cdot 12)$.

4. Schrijf alle natuurlijke getallen tussen 2 en $\sqrt{65537} \leq 257$ op, en pas de methode van Eratosthenes toe (zeef van Eratosthenes).

5. Stel $\text{ggd}(a + b, a - b) = d$. Dan $d \mid a + b, a - b$ en dus $d \mid 2a, 2b$. Nu is $\text{ggd}(2a, 2b) = 2 \cdot \text{ggd}(a, b) = 2$, waaruit $d \mid 2$.

6. Stel $\sqrt{2}$ is rationaal, dan $\sqrt{2} = \frac{a}{b}$ $(a, b \in \mathbb{Z})$ en dus $a^2 = 2b^2$. We bewijzen $2^n \mid a, \forall n \in \mathbb{N}$, duidelijk een tegenstrijdigheid. Neem als induktiebasis $n = 1$, dan $2 \mid a$ is triviaal wegens bovenstaande vergelijking en het feit dat 2 priem is. Stel $2^k \mid a$, dan volgt daaruit dat $2^{2k} \mid 2b^2$ waarop op zijn beurt weer $2^{2k+1} \mid 2b^2$. Dus $2^{2k+1} \mid a^2$ en weer $2^{2k+2} = 2^{2(k+1)} \mid a^2$. Hieruit volgt uiteindelijk $2^{k+1} \mid a$. Het induktieprincipe leidt ons dan naar de eerder gestelde tegenstrijdigheid.

7. Vooreerst bewijzen we dat 3 nooit een deler is van $a^2 + 1$ voor alle $a \in \mathbb{Z}$. Er kunnen zich drie gevallen voordoen, namelijk:

   (i) $a = 3q + 0$, dan volgt eenvoudig het gestelde.

   (ii) $a = 3q + 1$, zodat $a^2 + 1 = (a-1)^2 + 2(a-1) + 2$, waaruit eveneens het gestelde volgt.

   (iii) $a = 3q + 2$, analoog vinden we $a^2 + 1 = (a - 2)^2 + 2(a - 2) + 4$ zodat ook hier 3 geen deler is van $a^2 + 1$.

   Stel er bestaat zo'n stel (x, y, z, u) van gehele getallen. Dan $3 \mid x^2 + y^2$. Opnieuw kunnen zich drie gevallen voordoen:

(i) $3 \mid x^2, y^2$.

(ii) $3 \mid x^2 - 1, y^2 + 1$.

(iii) $3 \mid x^2 + 1, y^2 - 1$.

Wegens het voorgaande is dan noodzakelijk (i) voldaan, zodat $x^2 = x'^2 \cdot 3^2$ en $y^2 = y'^2 \cdot 3^2$. Substitueren we dit in onze vergelijking dan verkrijgen we $3x'^2 + 3y'^2 - z^2 - u^2 = 0$ waaruit we op dezelfde wijze kunnen aantonen dat $3 \mid z, u$, en dan weer dat $3 \mid x', y'$, enz.... Dit betekent dat $3^n \mid x$, $\forall n \in \mathbb{N}$, een strijdigheid.

4.3 De Euler funktie

Veronderstel dat n een positief natuurlijk getal is, dan noteren we met $\Phi(n)$ het aantal natuurlijke getallen uit $\mathbb{N}[1, n]$ die copriem zijn met n. De funktie Φ wordt de *Euler funktie* of *indikator van Euler* genoemd naar Leonhard Euler (1707 - 1783).

4.4 De Möbius funktie

4.4.1 Definitie

De *Möbius funktie* μ naar A. Möbius (1790-1868), is een funktie van $\mathbb{N}_0$ naar de verzameling $\{0, 1, -1\}$ die als volgt gedefinieerd wordt:

$$\mu(d) = \begin{cases} 1 & \text{als } d = 1 \\ (-1)^r & \text{als } d \text{ is een produkt van } r \text{ verschillende priemgetallen} \\ 0 & \text{als } d \text{ een meervoudige priemfaktor bezit.} \end{cases}$$

4.4.2 Een eerste eigenschap

4.4.3 De Möbius inversieformule

Oefening 4.4.1 *1. Bepaal* $\Phi(1992)$.

2. Bewijs dat voor elke twee natuurlijke getallen geldt:

$$\Phi(n^m) = n^{m-1}\Phi(n).$$

3. *Bewijs dat voor een gegeven natuurlijk getal n de som van al de natuurlijke getallen $x \in \mathbb{N}[1,n]$ die copriem zijn met n gelijk is aan $\frac{1}{2}n\Phi(n)$.*

4. *Voor een natuurlijk getal definiëren we*

$$\sigma(n) := \sum_{d|n} d.$$

   (a) *Geef een formule voor $\sigma(n)$ als $n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k}$.*

   (b) *Vereenvoudig*

$$\sum_{d|n} \mu(d)\sigma(n/d).$$

Oplossing.

1. We hoeven enkel Stelling 4.9 toe te passen. Hiervoor hebben we de priemontbinding van 1992 nodig: $1992 = 2^3 \cdot 3 \cdot 83$. Dus $\Phi(1992) = 2^2 \cdot 1 \cdot 3^0 \cdot 2 \cdot 83^0 \cdot 82 = 8 \cdot 82 = 656$.

2. Beschouw de priemontbinding ${p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k}$ van n, dan is ${p_1}^{me_1}{p_2}^{me_2}\cdots{p_k}^{me_k}$ de priemontbinding van n^m. Wegens Stelling 4.9 is

$$\begin{aligned}\Phi(n) &= n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})\\ \Phi(n^m) &= n^m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})\end{aligned}$$

   waaruit onmiddellijk de oplossing van de oefening volgt.

3.

$$\begin{aligned}\sum_{\substack{x\in\mathbb{N}[1,n-1]:\\ \gcd(x,n)=1}} x &= \sum_{\substack{x\in\mathbb{N}[1,n-1]:\\ \gcd(n-x,n)=1}} x\\ &= \sum_{\substack{n-l\in\mathbb{N}[1,n-1]:\\ \gcd(l,n)=1}} (n-l)\\ &= \sum_{\substack{l\in\mathbb{N}[1,n-1]:\\ \gcd(l,n)=1}} n - \sum_{\substack{l\in\mathbb{N}[1,n-1]:\\ \gcd(l,n)=1}} l\end{aligned}$$

waaruit volgt dat

$$\begin{aligned} 2 \cdot \sum_{\substack{x \in \mathbb{N}[1,n-1]: \\ \gcd(x,n)=1}} x &= \sum_{\substack{l \in \mathbb{N}[1,n-1]: \\ \gcd(l,n)=1}} n \\ &= n \cdot \Phi(n). \end{aligned}$$

4. Duidelijkerwijze is heeft elke deler d van n een unieke voorstelling ${p_1}^{a_1}{p_2}^{a_2}\cdots{p_k}^{a_k}$ met $a_i \leq e_i, \forall 1 \leq i \leq k$. En elke dergelijke voorstelling is een deler van n. Dus

$$\begin{aligned} \sum_{d|n} d &= \sum_{\substack{1 \leq a_1 \leq e_1 \\ 1 \leq a_2 \leq e_2 \\ \vdots \\ 1 \leq a_k \leq e_k}} {p_1}^{a_1}{p_2}^{a_2}\cdots{p_k}^{a_k} \\ &= (1 + p_1 + \ldots + p_1^{e_1})(1 + p_2 + \ldots + p_2^{e_2})\cdots(1 + p_k + \ldots + p_k^{e_k}) \\ &= \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p_i - 1}. \end{aligned}$$

Dit geeft (a). Nu lossen we (b) op. Beschouw de funktie $g(d) = d$. Als we $f(n)$ definiëren als $\sum_{d|n} g(d) = \sum_{d|n} d$, dan kunnen we de funktie $g(d)$ hieruit bekomen door middel van de inversieformule van Möbius, namelijk, $d = g(d) = \sum_{d|n} \mu(d) f(n/d)$. Hier is $\sigma(n) = f(n)$, zodat we verkrijgen dat $n = \sum_{d|n} \mu(d)\sigma(n/d)$, wat de gezochte vereenvoudiging oplevert.

Examen oefening 59 (2de zit, 1995-1996) *Bewijs dat* $ggd(2^a - 1, 2^b - 1) = 2^{ggd(a,b)} - 1$.

Oplossing. Het is duidelijk dat $2^{ggd(a,b)} - 1 \mid 2^a - 1$, omdat

$$(2^{ggd(a,b)} - 1)(2^{q_a} + 2^{q_a - 1} + \cdots + 2 + 1) = 2^a - 1,$$

met $a = q_a \cdot ggd(a,b)$. We vinden het zelfde resultaat voor b, maar nu met $b = q_b \cdot ggd(a,b)$. Er rest ons dus nog enkel aan te tonen dat elke gemene

deler m van $2^a - 1$ en $2^b - 1$ een deler is van $2^{ggd(a,b)} - 1$. Maar dan is m oneven en is m een deler van het verschil $(2^b-1)-(2^a-1) = 2^a(2^{b-a}-1)$ (we veronderstellen dat $a \leq b$). We besluiten dus dat $m \mid 2^{b-a} - 1$. Veranderen we nu de rol van a en b door die van a en $b-a$, dan vinden we $m \mid 2^{b-2a} - 1$, en uiteindelijk $m \mid 2^{b-q_1 a} - 1 = 2^{r_1} - 1$ (met $r_1 = ggd(a, b)$, voor de notaties verwijzen we naar het algoritme van Euclides).

Examen oefening 60 (2de zit, 1998-1999) *Bewijs dat de Möbiusfunctie multiplicatief is, d.w.z. toon aan dat $\mu(mn) = \mu(m)\mu(n)$ als m en n copriem zijn.*

Oplossing. Als $mn = 0$, dan is deze oefening triviaal.
Als $mn \neq 0$ en een meervoudige priemfactor bevat, stel $p^2 \mid mn$, dan eveneens $p^2 \mid m$ of $p^2 \mid n$ en is de gelijkheid ook hier triviaal.
Er rest ons dus nog enkel het geval waar mn geen meervoudige priemfactoren bevat, dan geldt dit eveneens voor m en n. Dus als r, r_m, r_n het aantal priemfactoren van mn respectievelijk m, n voorstelt dan is $r = r_m + r_n$ en dus $\mu(mn) = (-1)^r = (-1)^{r_m}(-1)^{r_n} = \mu(m)\mu(n)$.

Extra Oefening 61 *Definieer $ggd(x_1, x_2, \ldots, x_n)$ op analoge wijze, met $n \in \mathbb{N} : n > 2$. Toon aan dat $ggd(x_1, \ldots, x_n) = ggd(x_1,\ ggd(x_2, \ldots, x_n))$.*

Oplossing. We bewijzen

$$m \mid ggd(x_1, x_2, \ldots, x_n) \Leftrightarrow m \mid ggd(x_1, ggd(x_2, \ldots, x_n)),$$

voor alle $n \in \mathbb{N} : n > 2$.

Stel eerst dat $m \mid ggd(x_1, x_2, \ldots, x_n)$ dan $m \mid x_1$ en $m \mid ggd(x_2, \ldots, x_n)$. Daarom $m \mid ggd(x_1, ggd(x_2, \ldots, x_n))$.

Anderzijds als $m \mid ggd(x_1, ggd(x_2, \ldots, x_n))$, dan $m \mid x_1$, x_2, …, x_n. Dus ook $m \mid ggd(x_1, x_2 \ldots, x_n)$. Dit bewijst het gestelde.

Hoofdstuk 5

Modulo rekenen

5.1 Congruenties

5.1.1 Definitie

De negenproef

5.2 Optelling en vermenigvuldiging in $\mathbb{Z}_m$

De optelling $\oplus$ en de vermenigvuldiging $\otimes$ worden als volgt gedefinieerd

$$[x]_m \oplus [y]_m = [x+y]_m \text{ en } [x]_m \otimes [y]_m = [xy]_m.$$

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

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

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

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

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

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

Examen oefening 62 (1ste zit, 1991-1992) *Zoek de oplossingen* (x, y) *van volgende stelsel over* $\mathbb{Z}_7$ ***en*** *over* $\mathbb{Z}_5$*.*

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

Oplossing. Eliminatie van x levert: $5y = 12$. Over $\mathbb{Z}_7$ reduceert dit tot

$$\begin{array}{rcl} [5 \cdot y]_7 &=& [5]_7 \\ &\Updownarrow& \text{(A6)} \\ [5 \cdot y]_7 \oplus [-5]_7 &=& [0]_7 \\ &\Updownarrow& \text{definitie van } \oplus \\ [5 \cdot y - 5]_7 &=& [0]_7 \\ &\Updownarrow& \text{definitie van } \otimes \\ [5]_7 \otimes [y - 1]_7 &=& [0]_7 \end{array}$$

waaruit onmiddellijk $[y]_7 = 1$ en dus ook $[x]_7 = 2$. Als we de twee vergelijkingen van ons stelsel lid per lid optellen, dan krijgen we $5x + 5y = 8$. Dus als ons stelsel een oplossing $([x]_5, [y]_5)$ zou hebben over $\mathbb{Z}_5$, dan zou

$$\begin{array}{rcl} [5]_5 \otimes [x + y]_5 &=& [3]_5 \\ &\Updownarrow& [5]_5 = [0]_5 \\ [0]_5 \otimes [x + y]_5 &=& [3]_5 \end{array}$$

maar dan zou wegens de definitie van $\otimes$, $[3]_5 = [0]_5$, duidelijk een tegenstrijdigheid.

Examen oefening 63 (2de zit, 1993-1994) *Bewijs dat* $(3^{9999} - 1)/2$ *oneven en niet priem is.*

Oplossing. Dit is het geval als $3^{9999} - 1 \neq 0 \pmod 4$. Nu is $3^{9999} - 1 = (-1)^{9999} - 1 \pmod 4 \neq 0 \pmod 4$. Dus $(3^{9999} - 1)/2$ is oneven, en dit getal is niet priem want het is deelbaar door $(3^{3333} - 1)/2$.

Examen oefening 64 (2de zit, 1993-1994) *Bewijs dat voor elk natuurlijk getal* x*,* x^{73} *en* x *op hetzelfde cijfer eindigen.*

Oplossing. We splitsen het probleem op in 4 gevalletjes. Als

$$\begin{array}{lll} x \equiv 1 \pmod 2 & \Rightarrow & x^{73} \equiv 1 \pmod 2 \equiv x \pmod 2 \\ x \equiv 0 \pmod 2 & \Rightarrow & x^{73} \equiv 0 \pmod 2 \equiv x \pmod 2 \\ x \equiv 0 \pmod 5 & \Rightarrow & x^{73} \equiv 0 \pmod 5 \equiv x \pmod 5 \end{array}$$

Als tenslotte $z \equiv a \pmod 5$ met $a \in \{1, 2, 3, 4\}$, dan is $x^4 \equiv 1 \pmod 5$, waardoor $x^{73} \equiv (x^4)^{18} \cdot x \pmod 5 \equiv x \pmod 5$.
In alle gevallen is $x^{73} \equiv x \pmod 2$ en $x^{73} \equiv x \pmod 5$, waardoor $x^{73} \equiv x \pmod{10}$.

5.3 Inverteerbare elementen in $\mathbb{Z}_m$

5.3.1 Definitie

Examen oefening 65 (2de zit, 1991-1992) *Bereken de rest na deling van* 3^{47} *door 23.*

Oplossing. Aangezien $ggd(3, 23) = 1$, kunnen we de Stelling van Euler toepassen waaruit volgt dat $3^{22} = 1 \pmod{23}$. Dus $3^{47} \equiv 3^{22 \cdot 2 + 3} \equiv 3^3 \pmod{23}$. Dus de rest van 3^{47} na deling door 23 is gelijk aan de rest van 3^3 na deling door 23, wat niks anders is dan 4.

Examen oefening 66 (2de zit, 1994-1995) *Bereken de kleinste positieve macht n zodat voor elke* $a \in \mathbb{Z}$*, met* $ggd(a, 1020) = 1$*,*

$$a^n = 1 \pmod{15} = 1 \pmod{20} = 1 \pmod{17}.$$

Oplossing. We kunnen de vraag herformuleren als volgt: zoek het kleinste gemeen veelvoud van k_1, k_2 en k_3 waarbij k_1, k_2 en k_3 de kleinste positieve natuurlijke getallen zijn waarvoor $a^{k_1} = 1 \pmod{15}$, $a^{k_2} = 1 \pmod{20}$ en $a^{k_3} = 1 \pmod{17}$. Gebruikmakend van de stelling van Euler vind je gemakkelijk $k_1 = k_2 = 8$ en $k_3 = 16$. Het antwoord op de vraag is dus $n = 16$.

Examen oefening 67 (1ste zit, 1992-1993) *Bereken* $7^{28483} \pmod{1320}$.

Oplossing. Uit de stelling van Euler volgt, $7^{320} = 1 \pmod{1320}$. Waardoor $7^{28483} \pmod{1320} = 7^{320 \cdot 89+3} \pmod{1320} = 7^3 \pmod{1320} = 343 \pmod{1320}$.

Examen oefening 68 (2de zit, 1997-1998) *Bewijs dat 37 geen deler is van* 9^{6561}.

Oplossing. Met andere woorden: $9^{6561} = 0 \pmod{37}$? Wegens Euler vinden we $9^{36} = 1 \pmod{37}$, waardoor $9^{6561} \pmod{37} = 9^9 \pmod{37} \neq 0$.

5.4 Lineaire congruenties

5.4.1 Definities

5.5 De stelling van Wilson en toepassingen

5.6 Stelsel lineaire congruenties

Examen oefening 69 (1ste zit, 1991-1992) *Stel dat een jaar een schrikkeljaar is, m.a.w. 366 dagen bevat, als en slechts als het jaartal een veelvoud is van 4. Veronderstel ook dat een maancyclus bestaat uit 29 dagen.*
Op zaterdag 1 juni 1991 was het volle maan. In welk jaar, volgend op een schrikkeljaar, zal het voor het eerst volle maan zijn op een dinsdag 2 juni?

Oplossing.
Deel 1: Het stelsel congruentievergelijkingen.

Zij x het aantal dagen na 1 juni 1991 waarop het voor de eerste maal volle maan is op een dinsdag 2 juni, in een jaar volgend op een schrikkeljaar. Dan voldoet x aan

$$\begin{cases} x \equiv 0 \pmod{29} \\ x \equiv 3 \pmod{7} \\ x \equiv 732 \pmod{1461} \end{cases}$$

want een maancyclus bestaat uit 29 dagen, wat de eerste vergelijking geeft, de volle maan moet op een dinsdag zijn, dus 3 dagen na een zaterdag, waaruit de tweede vergelijking volgt.

De derde vergelijking wordt als volgt bekomen: De eerstvolgende 2 juni volgend op een schrikkeljaar is 2 juni 1993 en dit is 732 dagen na 1 juni 1991. De volgende kandidaat-oplossingen zijn 2 juni 1997, 2 juni 2001,... Tussen twee mogelijke oplossingen liggen er dus 4 jaar en 4 jaar bestaat uit $3 \cdot 365 + 366 = 1461$ dagen. Dus $x \equiv 732 \pmod{1461}$.

Deel 2: De oplossing van het stelsel.

Een oplossing voor x is $3 \cdot 29 \cdot 1461 \cdot y_1 + 732 \cdot 7 \cdot 29 \cdot y_2$. Dus

$$\begin{array}{rcl} x \equiv 3 \pmod 7 & \equiv & 3 \cdot 29 \cdot 1461 \cdot y_1 \pmod 7 \\ & \Updownarrow & \\ 1 & \equiv & 5 \cdot y_1 \pmod 7 \end{array}$$

zodat $y_1 = 3$. Analoog vinden we

$$\begin{array}{rcl} x \equiv 732 \pmod{1461} & \equiv & 732 \cdot 7 \cdot 29 \cdot y_2 \pmod{1461} \\ & \Updownarrow & \\ 1 & \equiv & 203 \cdot y_2 \pmod{1461} \end{array}$$

zodat hier $y_2 = 203^{-1}$.

De inverse van $203 \pmod{1461}$ volgt uit het algoritme van Euclides. Namelijk

$$\begin{array}{rcl} 1461 & = & 7 \cdot 203 + 40 \\ 203 & = & 5 \cdot 40 + 3 \\ 40 & = & 13 \cdot 3 + 1 \\ 3 & = & 3 \cdot 1. \end{array}$$

Bijgevolg

$$\begin{array}{rcl} 1 & = & 40 - 13 \cdot (203 - 5 \cdot 40) \\ & = & 66 \cdot 40 - 13 \cdot 203 \\ & = & 66 \cdot (1461 - 7 \cdot 203) - 13 \cdot 203 \\ & = & 66 \cdot 1461 - 475 \cdot 203. \end{array}$$

Uit de laatste gelijkheid volgt $1 \equiv -475 \cdot 203 \pmod{1461}$, waardoor $y_2 \equiv 986 \equiv -475 \pmod{1461}$.

Dus

$$\begin{array}{rcl} x & \equiv & 3 \cdot 29 \cdot 1461 \cdot 3 + 732 \cdot 7 \cdot 29 \cdot 986 \pmod{7 \cdot 29 \cdot 1461} \\ & \equiv & 88392 \pmod{296583}. \end{array}$$

Daar $88392 = 60 \cdot 1461 + 732$, is het voor de eerste keer volle maan op dinsdag 2 juni, in een jaar volgend op een schrikkeljaar, in het jaar $1991 + 60 \cdot 4 + 2 = 2233$.

Examen oefening 70 (1ste zit, 1994-1995) *Zoek het kleinste natuurlijk getal x dat aan het volgend stelsel voldoet.*

$$\begin{cases} 2x &= 3 \pmod 5 \\ 7x &= 11 \pmod{13} \\ 6x &= 8 \pmod{14} \end{cases}$$

Oplossing.

$$\begin{cases} 2x \equiv 3 \pmod 5 \\ 7x \equiv 11 \pmod{13} \\ 6x \equiv 8 \pmod{14} \end{cases} \iff \begin{cases} 2x \equiv 3 \pmod 5 \\ 7x \equiv 11 \pmod{13} \\ 3x \equiv 4 \pmod 7 \end{cases} \iff \begin{cases} x \equiv 9 \equiv 4 \pmod 5 \\ x \equiv 22 \equiv 9 \pmod{13} \\ x \equiv 20 \equiv 6 \pmod 7. \end{cases}$$

Dus $x = 4 \cdot y_1 \cdot 13 \cdot 7 + 9 \cdot y_2 \cdot 5 \cdot 7 + 6 \cdot y_3 \cdot 5 \cdot 13$ met

$$\begin{array}{lll} 4 \cdot y_1 \cdot 13 \cdot 7 \equiv 4 \pmod 5 & \iff y_1 \equiv 1 \pmod 5 \\ 9 \cdot y_2 \cdot 5 \cdot 7 \equiv 9 \pmod{13} & \iff y_2 \equiv 3 \pmod{13} \\ 6 \cdot y_3 \cdot 5 \cdot 13 \equiv 6 \pmod 7 & \iff y_3 \equiv 4 \pmod 7. \end{array}$$

Dus

$$\begin{aligned} x &\equiv 4 \cdot 13 \cdot 7 + 9 \cdot 3 \cdot 5 \cdot 7 + 6 \cdot 4 \cdot 5 \cdot 13 \pmod{5 \cdot 13 \cdot 7} \\ &\equiv 2869 \pmod{455} \equiv 139 \pmod{455}. \end{aligned}$$

Examen oefening 71 (2de zit, 1997-1998)

1. *Ga na welke van de volgende congruenties oplosbaar zijn:*

$$\begin{aligned} 18x &= 6 \pmod{12} \\ x &= 8 \pmod{13} \\ 35x &= 25 \pmod{14} \\ 25x &= -5 \pmod{15} \\ 28x &= 13 \pmod{16} \end{aligned}$$

2. Los het stelsel, gevormd door de oplosbare congruenties, op.

Oplossing. (1) We weten dat $ax \equiv b \pmod{m}$ oplosbaar is als $\text{ggd}(a,m)|b$. We gaan na in welke congruenties deze voorwaarde is voldaan.

$$\begin{array}{rcrlrcrcl} 18x & \equiv & 6 & \pmod{12} & : \text{ggd}(18,12) & = & 6 & \text{en} & 6|6 \\ x & \equiv & 8 & \pmod{13} & : \text{ggd}(1,13) & = & 1 & \text{en} & 1|8 \\ 35x & \equiv & 25 & \pmod{14} & : \text{ggd}(35,14) & = & 7 & \text{en} & 7 \not| 25 \\ 25x & \equiv & -5 & \pmod{15} & : \text{ggd}(25,15) & = & 5 & \text{en} & 5|-5 \\ 28x & \equiv & 13 & \pmod{16} & : \text{ggd}(28,16) & = & 4 & \text{en} & 4 \not| 13. \end{array}$$

Dit betekent dat de derde en de vijfde congruentie niet oplosbaar zijn.
(2) We lossen het volgende stelsel op:

$$\left\{\begin{array}{rcrl} 18x & \equiv & 6 & \pmod{12} \\ x & \equiv & 8 & \pmod{13} \\ 25x & \equiv & -5 & \pmod{15} \end{array}\right. \iff \left\{\begin{array}{rcrl} 3x & \equiv & 1 & \pmod{2} \\ x & \equiv & 8 & \pmod{13} \\ 5x & \equiv & -1 & \pmod{3} \end{array}\right.$$

$$\iff \left\{\begin{array}{rcrl} x & \equiv & 1 & \pmod{2} \\ x & \equiv & 8 & \pmod{13} \\ 2x & \equiv & 2 & \pmod{3} \end{array}\right. \iff \left\{\begin{array}{rcrl} x & \equiv & 1 & \pmod{2} \\ x & \equiv & 8 & \pmod{13} \\ x & \equiv & 1 & \pmod{3}. \end{array}\right.$$

Aangezien 2, 13 en 3 onderling priem zijn, kunnen we de Chinese reststelling toepassen. De oplossing van het stelsel wordt gegeven door:

$$x \equiv 1.y_1.13.3 + 8.y_2.2.3 + 1.y_3.2.13 \pmod{2.3.13}.(*)$$

Reduceren modulo 2 geeft ons het volgende resultaat: er geldt $x \equiv 1 \pmod{2}$, en dus volgt uit (*) dat $39.y_1 \equiv 1 \pmod{2}$ of dus $y_1 \equiv 1 \pmod{2}$. We vinden dat $y_1 = 1$.
Vervolgens reduceren we (*) modulo 13. Dit geeft ons $48.y_2 \equiv 8 \pmod{13}$ of dus $9.y_2 \equiv 8 \pmod{13}$. We zoeken nu de inverse van $9 \pmod{13}$. We vinden (eventueel m.b.v. het algoritme van Euclides) hiervoor 3: $9.3 = 27 \equiv 1 \pmod{13}$, dus $y_2 = 3$.
Tenslotte geeft reductie van (*) modulo 3 ons $26.y_3 \equiv 1 \pmod{3}$ of $2.y_3 \equiv 1 \pmod{3}$, waaruit we vinden dat $y_3 = 2$.
We vullen nu de gevonden waarden voor de y_i in in (*), en we krijgen:

$$x \equiv 39 + 8.11.6 + 2.26 \equiv 619 \equiv 73 \pmod{78}.$$

Examen oefening 72 (2de zit, 1996-1997) *Zoek het kleinste natuurlijk getal dat oplossing is van:*

$$\begin{cases} 5x &= 13 \pmod{17} \\ -2x &= 3 \pmod{17} \\ 8x &= 12 \pmod{14} \end{cases}.$$

Oplossing. Dit is een oefening op de Chinese reststelling. We reduceren het stelsel achtereenvolgens tot:

$$\begin{cases} 5x \equiv 13 \pmod{17} \\ 3x \equiv 3 \pmod{5} \\ 4x \equiv 6 \pmod{7} \end{cases} \iff \begin{cases} 5x \equiv 30 \pmod{17} \\ x \equiv 1 \pmod{5} \\ 4x \equiv 20 \pmod{7} \end{cases} \iff \begin{cases} x \equiv 6 \pmod{17} \\ x \equiv 1 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$$

Hieruit volgt dan dat $x \equiv 6 \cdot y_1 \cdot 5 \cdot 7 + 1 \cdot y_2 \cdot 17 \cdot 7 + 5 \cdot y_3 \cdot 17 \cdot 5 \pmod{17 \cdot 5 \cdot 7}$, waarbij

$$\begin{cases} 6 \cdot y_1 \cdot 5 \cdot 7 \equiv 6 \pmod{17} \\ y_2 \cdot 17 \cdot 7 \equiv 1 \pmod{5} \\ 5 \cdot y_3 \cdot 17 \cdot 5 \equiv 5 \pmod{7} \end{cases} \iff \begin{cases} y_1 \equiv 1 \pmod{17} \\ y_2 \equiv 4 \pmod{5} \\ y_3 \equiv 1 \pmod{7} \end{cases}$$

Hieruit volgt dat

$$\begin{aligned} x &\equiv 6 \cdot 1 \cdot 5 \cdot 7 + 1 \cdot 4 \cdot 17 \cdot 7 + 5 \cdot 1 \cdot 17 \cdot 5 \pmod{17 \cdot 5 \cdot 7} \\ &\equiv 210 + 476 + 425 \pmod{595} \\ &\equiv 1111 \pmod{595} \\ &\equiv 516 \pmod{595}. \end{aligned}$$

Examen oefening 73 (2de zit, 1998-1999) *Toon aan dat het berekenen van* $5^{6791} \pmod{391}$ *te herleiden valt tot het oplossen van het stelsel*

$$\begin{cases} X &= 10 \pmod{17} \\ X &= 19 \pmod{23}. \end{cases}$$

Oplossing. We willen gebruik maken van de stelling van Euler. Nu is $\text{ggd}(5, 391) = 1$ en aangezien $391 = 17 \times 23$ is $\Phi(391) = 16 \times 22 = 352$. Dus $5^{352} \equiv 1 \pmod{391}$. Nu is $6791 = 103 + 19 \times 352$. Dus

$$5^{6791} \pmod{391} \equiv 5^{103} 5^{19 \times 352} \pmod{391} \equiv 5^{103} \pmod{391}.$$

Het berekenen van $5^{103} \pmod{391}$ is equivalent met het zoeken naar een oplossing van het stelsel

$$\begin{cases} X \equiv 5^{103} \pmod{17} \\ X \equiv 5^{103} \pmod{23} \end{cases}$$

Omdat $\Phi(17) = 16$ en $\Phi(23) = 22$ en rekening houdende met het feit dat $103 = 16 \times 6 + 7 = 22 \times 4 + 15$, is het stelsel equivalent met

$$\begin{cases} X \equiv 5^{7} \pmod{17} \\ X \equiv 5^{15} \pmod{23} \end{cases}$$

Nu is $5^2 \equiv 8 \pmod{17}$ en $5^4 \equiv 13 \pmod{17}$, dus wordt
$5^7 \equiv 5 \times 8 \times 13 \pmod{17} \equiv 10 \pmod{17}$. En $5^2 \equiv 2 \pmod{23}$, $5^4 \equiv 4 \pmod{23}$, en $5^8 \equiv 16 \pmod{23}$, dus wordt
$5^{15} \equiv 5 \times 2 \times 4 \times 16 \pmod{23} \equiv 19 \pmod{23}$. Het stelsel is dus equivalent met

$$\begin{cases} X \equiv 10 \pmod{17} \\ X \equiv 19 \pmod{23} \end{cases}$$

We zoeken een oplossing hiervan met behulp van de Chinese reststelling. Stel $X = 10y_1 23 + 19y_2 17$ dan is

$$\begin{aligned} 1 \pmod{17} \equiv 23y_1 \pmod{17} \equiv 6y_1 \pmod{17} &\Rightarrow y_1 \equiv 3 \pmod{17} \\ 1 \pmod{23} \equiv 17y_2 \pmod{23} \equiv (-6)y_2 \pmod{23} &\Rightarrow y_2 \equiv -4 \pmod{23} \end{aligned}$$

Na substitutie van y_1 en y_2 wordt $X \equiv -620 \equiv 180 \pmod{391}$ is de oplossing van het stelsel.

Examen oefening 74 (1ste zit, 1997-1998) *Bereken* $7^{1998} \pmod{143}$.

Oplossing. We gebruiken voor de oplossing de stelling van Euler:

$$y^{\phi(m)} \equiv 1 \pmod{m} \text{ als } \text{ggd}(y, m) = 1.$$

Dit kan, want $\text{ggd}(7, 143) = 1$. We berekenen nu $\phi(m) = \phi(143) = \phi(11 \times 13) = 10 \times 12 = 120$. Uit de stelling van Euler leiden we dus af: $7^{120} \equiv 1 \pmod{143}$.
$1998 = 16 \times 120 + 78$, dus $7^{1998} \equiv 7^{16 \times 120 + 78} \equiv 7^{16 \times 120}.7^{78} \equiv 1^{16}.7^{78} \equiv 7^{78}$

(mod 143). Noem $7^{78} \pmod{143} = x$.
We zoeken x aan de hand van het volgende stelsel lineaire congruenties:

$$\begin{cases} x & \equiv & 7^{78} \pmod{11} \\ x & \equiv & 7^{78} \pmod{13}. \end{cases}$$

Voor beide congruenties passen we nu dezelfde techniek toe als daarnet: met behulp van de stelling van Euler (mag worden toegepast want ggd$(7, 11)$ =ggd$(7, 13) = 1$) trachten we de exponent van 7 te verkleinen.
$\phi(11) = 10$, dus $7^{10} \equiv 1 \pmod{11}$ en $\phi(13) = 12$, dus $7^{12} \equiv 1 \pmod{13}$.
Verder is $78 = 7 \times 10 + 8 = 6 \times 12 + 6$, dus:

$$\begin{cases} x & \equiv & 7^{10\times 7+8} \equiv 7^8 \pmod{11} \\ x & \equiv & 7^{6\times 12+6} \equiv 7^6 \pmod{13}. \end{cases}$$

Nu is $7^2 \equiv 49 \equiv 5 \pmod{11}$, en dus $7^4 \equiv 25 \equiv 3 \pmod{11}$. Dus $7^8 \equiv 7^4.7^4 \equiv 3.3 \equiv 9 \pmod{11}$. Analoog vinden we $7^2 \equiv 49 \equiv 10 \pmod{13}$, en dus $7^4 \equiv 100 \equiv 9 \pmod{13}$. Dus $7^6 \equiv 7^4.7^2 \equiv 9.10 \equiv 12 \pmod{13}$. Het stelsel is herleid tot:

$$\begin{cases} x & \equiv & 9 \pmod{11} \\ x & \equiv & 12 \pmod{13}. \end{cases}$$

De oplossing hiervan wordt gegeven door $x = 9.y_1.13 + 12.y_2.11$. Door respectievelijk de rest na deling door 11 en door 13 te bepalen, vinden we dat

$$\begin{cases} 2.y_1 & \equiv & 1 \pmod{11} \\ 11.y_2 & \equiv & 1 \pmod{13}, \end{cases}$$

waaruit we vinden dat $y_1 = y_2 = 6$. Dus $x \equiv 9.6.13 + 12.6.11 \equiv 64 \pmod{143}$.

5.7 Primitieve wortels

5.7.1 Definitie

5.7.2 Definitie

5.8 Kwadratische congruenties

5.8.1 Definitie

5.8.2 Definities

5.8.3 De kwadratische resten modulo een oneven priemgetal

5.8.4 Het Legendre symbool

Oefening 5.8.1 *1. Zoek het kleinste getal, deelbaar door 2 en door 3, dat een kwadraat is en eveneens een 5de macht.*

2. Merk op dat $2^5 \cdot 9^2 = 2592$. *Bestaat er een ander getal van de vorm* $25ab$ *dat gelijk is aan* $2^5 \cdot a^b$ *(met* $25ab$ *bedoelen we een getal waarvan* a *het cijfer van de tientallen is en* b *het cijfer van de eenheden).*

3. Zoek m *zodanig dat* $1066 = 1776 \pmod{m}$.

4. Los op

(a) $3x = 6 \pmod{18}$

(b) $40x = 777 \pmod{1777}$

(c)
$$\begin{cases} 2x &= 1 \pmod 5 \\ 3x &= 2 \pmod 7 \\ 4x &= 4x \pmod{11} \end{cases}$$

5. Zoek een positief natuurlijk getal zodanig dat de helft een kwadraat is, een derde een vijfde macht is en een vijfde een vijfde macht.

Oplossing.

1. aangezien het gezochte getal x deelbaar is door 2 en door 3, en aangzien $ggd(2,3) = 1$ zal eveneens $6 \mid x$. Nu is ook $x = y^2 = z^5$ voor zekere y. Als nu 6 niet z deelt, dan zal 6 ook niet z^5 delen, een strijdigheid,

dus $6 \mid y$ waardoor $6^2 \mid y$. Verander je de rol van 6 door 6^2 en de rol van y door z, dan toon je aan dat $(6^2)^5 \mid x$. Nu voldoet 6^{10} aan alle voorwaarden uit de oefening en is tevens de kleinste.

2. Gevraagd wordt: bestaan er een $a,\ b \in \mathbb{N}[0,9]$ waarvoor $32 \cdot a^b = 2500 + 10 \cdot a + b$. Nu zijn alle veelvouden van 32 gelegen tussen 2500 en 2600: $79 \cdot 32 = 2528$, $80 \cdot 32 = 2560$ en $81 \cdot 32 = 2592$. Men controleert nu gemakkelijk dat er geen andere a en b bestaan.

3. We zoeken dus een m waarvoor $1066 + x \cdot m = 1776$, of $x \cdot m = 710$. Dus m moet een deler zijn van 710. Het is nu duidelijk dat dit geldt voor ALLE delers van 710.

4. (a) is equivalent met $x = 2 \pmod{18}$. Dus $x \in \{2 + y \cdot 18 \parallel y \in \mathbb{Z}\}$. (b) heeft een unieke oplossing wegens stelling 5.4. We bepalen de inverse van 40 in $\mathbb{Z}_{1777}$.

$$\begin{aligned} 1777 &= 44 \cdot 40 + 17 \\ 40 &= 2 \cdot 17 + 6 \\ 17 &= 2 \cdot 6 + 1 \end{aligned}$$

waardoor $1 = 17 - 2 \cdot 6 = 5 \cdot 17 - 2 \cdot 40 = 5 \cdot 1777 - 222 \cdot 40$. Dus $40^{-1} = 222$ in $\mathbb{Z}_{1777}$. Nu volgt onmiddellijk dat $x = 222 \cdot 777 \pmod{1777}$. (c) is equivalent met het stelsel:

$$\begin{cases} x &= 3 \pmod 5 \\ x &= 10 \pmod 7 \\ x &= 9 \pmod{11} \end{cases}$$

De oplossing volgt nu eenvoudig door gebruik te maken van de Chinese reststelling.

5. Stel x is een oplossing, dan volgt uit de opgave dat $2, 3, 5$ allen x delen. Stellen we nu $x = 2^a 3^b 5^c$, dan moet $a^{a-1} 3^b 5^c$ een kwadraat zijn, waardoor $a - 1$, b en c even zijn. Wegens de tweede voorwaarde moet $2^a 3^{b-1} 5^c$ een derde macht zijn waardoor a, $b - 1$ en c deelbaar zijn door 3. Volgens de laatste voorwaarde besluiten we analoog dat a, b en $c - 1$ deelbaar zijn door 5. Samengevat is a oplossing van

$$\begin{cases} a &\equiv 1 \pmod 2 \\ a &\equiv 0 \pmod 3 \\ a &\equiv 0 \pmod 5 \end{cases},$$

b is oplossing van

$$\begin{cases} b \equiv 0 \pmod 2 \\ b \equiv 1 \pmod 3 \\ b \equiv 0 \pmod 5 \end{cases}$$

en c is oplossing van

$$\begin{cases} c \equiv 0 \pmod 2 \\ c \equiv 0 \pmod 3 \\ c \equiv 1 \pmod 5 \end{cases}$$

Waarmee individueel een oplossing gevonden kan worden door gebruik te maken van de Chinese reststelling.

Examen oefening 75 (2de zit, 1991-1992) *Zoek alle oplossingen van de vergelijking*

$$y^2 = 2158 \pmod{2479}.$$

Tip: $2479 = 37 \cdot 67$.

Oplossing. Het getal na het moduloteken is te factoriseren als $2479 = 37 \cdot 67$. Uit de Chinese reststelling volgt nu dat deze vergelijking equivalent is met het stelsel

$$\begin{cases} y^2 \equiv 2158 \pmod{37} \equiv 12 \pmod{37} \\ y^2 \equiv 2158 \pmod{67} \equiv 14 \pmod{67}. \end{cases}$$

Deel 1: Reductie van de vergelijkingen tot lineaire congruenties.

We zoeken met behulp van het Legendre symbool of 12 en 14 een kwadraatrest zijn modulo 37 en 67.

$$\left[\begin{array}{c} 12 \\ 37 \end{array}\right] = \left[\begin{array}{c} 4 \\ 37 \end{array}\right] \cdot \left[\begin{array}{c} 3 \\ 37 \end{array}\right] = 1 \cdot \left[\begin{array}{c} 3 \\ 37 \end{array}\right] = \left[\begin{array}{c} 37 \\ 3 \end{array}\right] = \left[\begin{array}{c} 1 \\ 3 \end{array}\right] = 1$$

$$\left[\begin{array}{c} 14 \\ 67 \end{array}\right] = \left[\begin{array}{c} 2 \\ 67 \end{array}\right] \cdot \left[\begin{array}{c} 7 \\ 67 \end{array}\right] = (-1) \cdot \left[\begin{array}{c} 7 \\ 67 \end{array}\right] = (-1) \cdot (-1) \cdot \left[\begin{array}{c} 67 \\ 7 \end{array}\right] = \left[\begin{array}{c} 4 \\ 67 \end{array}\right] = 1.$$

Beide Legendre symbolen zijn 1. Beide vergelijkingen hebben dus oplossingen in y.

Uit de eerste vergelijking volgt dat $y^2 \equiv 12 \pmod{37} \equiv 49 \pmod{37}$, dus $y \equiv \pm 7 \pmod{37}$. De tweede vergelijking $y^2 \equiv 14 \pmod{67} \equiv 81 \pmod{67}$ heeft als oplossingen $y \equiv \pm 9 \pmod{67}$.

Dit geeft dan vier stelsels lineaire congruenties:

$$\left\{\begin{array}{rcl} y & \equiv & 7 \pmod{37} \\ y & \equiv & 9 \pmod{67} \end{array}\right. \vee \left\{\begin{array}{rcl} y & \equiv & -7 \pmod{37} \\ y & \equiv & -9 \pmod{67} \end{array}\right. \vee$$

$$\left\{\begin{array}{rcl} y & \equiv & 7 \pmod{37} \\ y & \equiv & -9 \pmod{67} \end{array}\right. \vee \left\{\begin{array}{rcl} y & \equiv & -7 \pmod{37} \\ y & \equiv & 9 \pmod{67}. \end{array}\right.$$

Deel 2: Oplossing van de stelsels lineaire congruenties.

Het eerste en tweede, net zoals het derde en vierde stelsel, hebben tegengestelde oplossingen die, wegens de Chinese reststelling, uniek zijn modulo $37 \cdot 67 = 2479$.

Een oplossing voor het eerste stelsel is

$$y = 7 \cdot 67 \cdot y_1 + 9 \cdot 37 \cdot y_2.$$

Dus

$$\begin{array}{rcl} y \equiv 7 \pmod{37} & \equiv & 7 \cdot 67 \cdot y_1 \pmod{37} \\ & \Updownarrow & \\ 1 & \equiv & 67 \cdot y_1 \pmod{37}. \end{array}$$

De inverse van $67 \pmod{37}$ volgt uit het algoritme van Euclides. Namelijk

$$\begin{array}{rcl} 67 & = & 1 \cdot 37 + 30 \\ 37 & = & 1 \cdot 30 + 7 \\ 30 & = & 4 \cdot 7 + 2 \\ 7 & = & 3 \cdot 2 + 1. \end{array}$$

Bijgevolg

$$\begin{array}{rcll} 1 & = & 7 - 3 \cdot 2 & \\ & = & 7 - 3 \cdot (30 - 4 \cdot 7) & \\ & = & -3 \cdot 30 + 13 \cdot 7 & \\ & = & -3 \cdot 30 + 13 \cdot (37 - 30) & \\ & = & 13 \cdot 37 - 16 \cdot 30 & \\ & = & 13 \cdot 37 - 16 \cdot (67 - 37) & \\ & = & -16 \cdot 67 + 29 \cdot 37. & (5.1) \end{array}$$

Dus $1 \equiv -16 \cdot 67 \pmod{37}$ wat impliceert dat $y_1 \equiv -16 \pmod{37} \equiv 21 \pmod{37}$.

Verder is

$$\begin{array}{rcl} y \equiv 9 \pmod{67} & \equiv & 9 \cdot 37 \cdot y_2 \pmod{67} \\ & \Updownarrow & \\ 1 & \equiv & 37 \cdot y_2 \pmod{67}. \end{array}$$

Uit (5.1) volgt $1 \equiv 29 \cdot 37 \pmod{67}$, dus $y_2 = 29$.

Beide waarden voor y_1 en y_2 geven

$$\begin{array}{rcl} y & \equiv & 7 \cdot 67 \cdot 21 + 9 \cdot 37 \cdot 29 \pmod{37 \cdot 67} \\ & \equiv & 2153 \pmod{2479}. \end{array}$$

De oplossing voor het tweede stelsel is dan

$$y \equiv -2153 \pmod{2479} \equiv 326 \pmod{2479}.$$

Het derde stelsel heeft als oplossing:

$$y = 7 \cdot 67 \cdot y_1 - 9 \cdot 37 \cdot y_2$$

waarbij

$$y \equiv 7 \pmod{37} \equiv 7 \cdot 67 \cdot y_1 \pmod{37}$$

en

$$y \equiv -9 \pmod{67} \equiv -9 \cdot 37 \cdot y_2 \pmod{67}.$$

Beide vergelijkingen zijn equivalent met

$$1 \equiv 67 \cdot y_1 \pmod{37} \quad \text{en} \quad 1 \equiv 37 \cdot y_2 \pmod{67}.$$

Deze vergelijkingen werden hiervoor opgelost, namelijk $y_1 = 21$ en $y_2 = 29$. Dus

$$\begin{array}{rcl} y & \equiv & 7 \cdot 67 \cdot 21 - 9 \cdot 37 \cdot 29 \pmod{2479} \\ & \equiv & 192 \pmod{2479}. \end{array}$$

De oplossing voor het vierde stelsel is dan

$$y \equiv -192 \pmod{2479} \equiv 2287 \pmod{2479}.$$

Examen oefening 76 (1ste zit 1992-1993) *Los het volgende stelsel op:*

$$\begin{cases} z^2 &= 2 \pmod 7 \\ z^2 &= 81 \pmod{101} \end{cases}$$

Oplossing.
Deel 1: Reductie van de vergelijkingen tot lineaire congruenties.

De eerste vergelijking is equivalent met

$$z^2 \equiv 2 \pmod 7 \Leftrightarrow z \equiv \pm 3 \pmod 7.$$

De tweede vergelijking impliceert

$$z \equiv \pm 9 \pmod{101}.$$

Net zoals in Oefening 82 geeft dit 4 stelsels lineaire congruenties die op te splitsen zijn in twee groepen van twee stelsels die onderling tegengestelde oplossingen hebben.
Deel 2: Oplossing van de stelsels lineaire congruenties.

Beschouw als eerste stelsel

$$\begin{cases} z &\equiv 3 \pmod 7 \\ z &\equiv 9 \pmod{101}. \end{cases}$$

Een oplossing hiervoor is $z = 3 \cdot 101 \cdot y_1 + 9 \cdot 7 \cdot y_2$. Dus

$$\begin{aligned} z \equiv 3 \pmod 7 &\equiv 3 \cdot 101 \cdot y_1 \pmod 7 \\ &\Updownarrow \\ 1 &\equiv 3 \cdot y_1 \pmod 7 \end{aligned}$$

zodat $y_1 = 5$.

Nu berekenen we y_2 op analoge wijze.

$$\begin{aligned} z \equiv 9 \pmod{101} &\equiv 9 \cdot 7 \cdot y_2 \pmod{101} \\ &\Updownarrow \\ 1 &\equiv 7 \cdot y_2 \pmod{101}. \end{aligned}$$

zodat y_2 gelijk is aan de inverse van $7 \pmod{101}$, welke volgt uit het algoritme van Euclides. Namelijk

$$\begin{aligned} 101 &= 14 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \end{aligned}$$

waaruit volgt

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2 \cdot (101 - 14 \cdot 7) \\ &= -2 \cdot 101 + 29 \cdot 7. \end{aligned}$$

Dus $1 \equiv 29 \cdot 7 \pmod{101}$ wat betekent dat $y_2 = 29$.

Na substitutie van y_1 en y_2 geeft dit

$$z \equiv 3 \cdot 101 \cdot 5 + 9 \cdot 7 \cdot 29 \pmod{7 \cdot 101} \equiv 514 \pmod{707}.$$

Analoog is $z \equiv -514 \pmod{707} \equiv 193 \pmod{707}$ de oplossing voor het stelsel

$$\begin{cases} z \equiv -3 \pmod{7} \\ z \equiv -9 \pmod{101}. \end{cases}$$

En het stelsel

$$\begin{cases} z \equiv 3 \pmod{7} \\ z \equiv -9 \pmod{101}. \end{cases}$$

heeft als oplossing

$$z \equiv 3 \cdot 101 \cdot y_1 - 9 \cdot 7 \cdot y_2 \pmod{707}$$

waarbij net als voor het eerste stelsel $y_1 = 5$ en $y_2 = 29$. Substitutie van deze waarden voor y_1 en y_2 geeft $z \equiv 395 \pmod{707}$.
Tenslotte is $z \equiv -395 \pmod{707} \equiv 312 \pmod{707}$ de oplossing voor

$$\begin{cases} z \equiv -3 \pmod{7} \\ z \equiv 9 \pmod{101}. \end{cases}$$

Examen oefening 77 (2de zit, 1992-1993) *Los op:*

$$\begin{cases} x^4 = 17 \pmod{19} \\ x^2 = 5 \pmod{59}. \end{cases}$$

Oplossing.
Deel 1: Reductie van de vergelijkingen tot lineaire congruenties.

De eerste vergelijking is equivalent met

$$\begin{array}{rcl} x^4 & \equiv & 17 \pmod{19} \equiv 36 \pmod{19} \\ & \Updownarrow & \\ x^2 & \equiv & \pm 6 \pmod{19}. \end{array}$$

Dus $x^2 \equiv 6 \pmod{19}$ of $x^2 \equiv -6 \pmod{19} \equiv 13 \pmod{19}$.

We onderzoeken met behulp van het Legendre symbool of 6 en 13 kwadraatresten zijn $\pmod{19}$.

$$\left[\begin{array}{c} 6 \\ 19 \end{array}\right] = \left[\begin{array}{c} 3 \\ 19 \end{array}\right] \cdot \left[\begin{array}{c} 2 \\ 19 \end{array}\right] = (-1) \cdot \left[\begin{array}{c} 19 \\ 3 \end{array}\right] \cdot \left[\begin{array}{c} 2 \\ 19 \end{array}\right] = (-1) \cdot \left[\begin{array}{c} 1 \\ 3 \end{array}\right] \cdot (-1) = 1$$

en

$$\left[\begin{array}{c} 13 \\ 19 \end{array}\right] = \left[\begin{array}{c} 19 \\ 13 \end{array}\right] = \left[\begin{array}{c} 6 \\ 13 \end{array}\right] = \left[\begin{array}{c} 2 \\ 13 \end{array}\right] \cdot \left[\begin{array}{c} 3 \\ 13 \end{array}\right] = \left[\begin{array}{c} 2 \\ 13 \end{array}\right] \cdot \left[\begin{array}{c} 13 \\ 3 \end{array}\right] = (-1) \cdot \left[\begin{array}{c} 1 \\ 3 \end{array}\right] = -1.$$

Hieruit blijkt dat 6 een kwadraatrest is $\pmod{19}$, maar dat 13 geen kwadraatrest is $\pmod{19}$. De vergelijking $x^2 \equiv 13 \pmod{19}$ heeft geen oplossingen.

Het origineel stelsel is herleid tot

$$\left\{\begin{array}{rcl} x^2 & \equiv & 6 \pmod{19} \\ x^2 & \equiv & 5 \pmod{59}. \end{array}\right.$$

De eerste vergelijking is equivalent met $x^2 \equiv 6 \pmod{19} \equiv 25 \pmod{19}$, dus $x \equiv \pm 5 \pmod{19}$, en de tweede vergelijking kan herschreven worden als $x^2 \equiv 5 \pmod{59} \equiv 64 \pmod{59}$ zodat $x \equiv \pm 8 \pmod{59}$.

Volledig analoog aan Oefeningen **??** en **??** geven de vergelijkingen

$$\left\{\begin{array}{rcl} x & \equiv & \pm 5 \pmod{19} \\ x & \equiv & \pm 8 \pmod{59} \end{array}\right.$$

vier stelsels lineaire congruenties.

Deel 2: Oplossing van de stelsels lineaire congruenties.

Beschouw

$$\left\{\begin{array}{rcl} x & \equiv & 5 \pmod{19} \\ x & \equiv & 8 \pmod{59}. \end{array}\right.$$

Een oplossing hiervoor is

$$x = 5 \cdot 59 \cdot y_1 + 8 \cdot 19 \cdot y_2.$$

De onbekenden y_1 en y_2 voldoen aan

$$\begin{array}{rcl} x \equiv 5 \pmod{19} & \equiv & 5 \cdot 59 \cdot y_1 \pmod{19} \\ & \Updownarrow & \\ 1 \pmod{19} & \equiv & 59 \cdot y_1 \pmod{19} \end{array}$$

en

$$\begin{array}{rcl} x \equiv 8 \pmod{59} & \equiv & 8 \cdot 19 \cdot y_2 \pmod{59} \\ & \Updownarrow & \\ 1 \pmod{59} & \equiv & 19 \cdot y_2 \pmod{59}. \end{array}$$

De waarden voor y_1 en y_2 volgen uit het algoritme van Euclides. Toepassing van dit algoritme impliceert

$$\begin{aligned} 59 &= 3 \cdot 19 + 2 \\ 19 &= 9 \cdot 2 + 1. \end{aligned}$$

Bijgevolg

$$\begin{aligned} 1 &= 19 - 9 \cdot 2 \\ &= 19 - 9 \cdot (59 - 3 \cdot 19) \\ &= -9 \cdot 59 + 28 \cdot 19. \end{aligned} \tag{5.2}$$

Zoals in Oefeningen **??** en **??** volgt hieruit dat $y_1 = -9$ en $y_2 = 28$ en substitutie van deze waarden in de uitdrukking van x geeft

$$\begin{aligned} x &\equiv 5 \cdot 59 \cdot (-9) + 8 \cdot 19 \cdot 28 \pmod{19 \cdot 59} \\ &\equiv 480 \pmod{1121}. \end{aligned}$$

Als een onmiddellijk gevolg heeft het stelsel

$$\begin{cases} x \equiv -5 \pmod{19} \\ x \equiv -8 \pmod{59} \end{cases}$$

$x \equiv -480 \pmod{1121} \equiv 641 \pmod{1121}$ als oplossing.

Analoog is een oplossing voor

$$\begin{cases} x \equiv 5 \pmod{19} \\ x \equiv -8 \pmod{59} \end{cases}$$

gelijk aan

$$x \equiv 5 \cdot 59 \cdot y_1 - 8 \cdot 19 \cdot y_2 \pmod{19 \cdot 59}.$$

Substitutie van $y_1 = -9$ en $y_2 = 28$ geeft $x \equiv 936 \pmod{1121}$.

Tenslotte is het tegengestelde van deze oplossing, de oplossing van

$$\begin{cases} x \equiv -5 \pmod{19} \\ x \equiv 8 \pmod{59}. \end{cases}$$

Examen oefening 78 (1ste zit, 1993-1994) *Los op:*

$$\begin{cases} x^3 = 5 \pmod{11} \\ x^4 = 38 \pmod{43}. \end{cases}$$

Oplossing.

$$\begin{array}{lcl} X^3 \equiv 5 \pmod{11} & \Longleftrightarrow & X \equiv 3 \pmod{11} \text{ zie Extra Oefening 83} \\ X^4 \equiv 38 \pmod{43} & \Longleftrightarrow & X^4 \equiv 81 \pmod{43} \\ & \Updownarrow & \\ X^2 \equiv 9 \pmod{43} & \vee & X^2 \equiv 34 \pmod{43}. \end{array}$$

Maar $\left[\frac{34}{43}\right] = \left[\frac{2}{43}\right]\left[\frac{17}{43}\right] = (-1) \cdot \left[\frac{43}{17}\right] = (-1) \cdot \left[\frac{9}{17}\right] = -1$. Dus heeft $X^2 \equiv 34 \pmod{43}$ geen oplossingen.

Bijgevolg moeten enkel de volgende twee stelsels opgelost worden.

$$\begin{cases} X \equiv 3 \pmod{11} \\ X \equiv 3 \pmod{43} \end{cases} \vee \begin{cases} X \equiv 3 \pmod{11} \\ X \equiv 40 \pmod{43}. \end{cases}$$

Voor het eerste stelsel is de oplossing $X \equiv 3 \pmod{11 \cdot 43} \equiv 3 \pmod{473}$. Een oplossing voor het tweede stelsel is $X = 3 \cdot y_1 \cdot 43 + 40 \cdot y_2 \cdot 11$. Substitutie in $X \equiv 3 \pmod{11}$ geeft $3 \cdot y_1 \cdot 43 \pmod{11} \equiv 3 \pmod{11}$, dus $y_1 \cdot 10 \equiv 1 \pmod{11}$, waardoor $y_1 = 10$. De substitutie in $X \equiv 40 \pmod{43}$ geeft $40 \cdot y_2 \cdot 11 \equiv 40 \pmod{43}$, dus $y_2 \cdot 11 \equiv 1 \pmod{43}$, waardoor $y_2 = 4$.

Dit betekent dat $x \equiv 3 \cdot 10 \cdot 43 + 40 \cdot 4 \cdot 11 \pmod{473} \equiv 3050 \pmod{473} \equiv 212 \pmod{473}$.

De oplossingen zijn dus

$$X \equiv 3 \pmod{473} \vee X \equiv 212 \pmod{473}.$$

Examen oefening 79 (1ste zit, 1995-1996) *Los op:* $x^4 = 1 \pmod{143}$.

Oplossing. Daar $143 = 11 \cdot 13$ is dit equivalent met

$$\left\{ \begin{array}{rcl} X^4 & \equiv & 1 \pmod{11} \\ X^4 & \equiv & 1 \pmod{13} \end{array} \right. \iff \left\{ \begin{array}{rcl} X^2 & \equiv & 1, -1 \pmod{11} \\ X^2 & \equiv & 1, -1 \pmod{13} \end{array} \right.$$
$$\iff \left\{ \begin{array}{rcl} X & \equiv & 1, -1 \pmod{11} \\ X & \equiv & 1, -1, 5, -5 \pmod{13}. \end{array} \right.$$

Dit geeft acht stelsels

$$\left\{ \begin{array}{rcl} X & \equiv & a \pmod{11} \\ X & \equiv & b \pmod{13} \end{array} \right.$$

met $a \in \{1, -1\}$ en met $b \in \{1, 5, -5, -1\}$. De respectievelijke oplossingen zijn $X \equiv 1 \pmod{143}$ voor $(a, b) = (1, 1)$, $X \equiv 12 \pmod{143}$ voor $(a, b) = (1, -1)$, $X \equiv 122 \pmod{143}$ voor $(a, b) = (1, 5)$, $X \equiv 34 \pmod{143}$ voor $(a, b) = (1, -5)$, $X \equiv 142 \pmod{143}$ voor $(a, b) = (-1, -1)$, $X \equiv 131 \pmod{143}$ voor $(a, b) = (-1, 1)$, $X \equiv 21 \pmod{143}$ voor $(a, b) = (-1, -5)$, $X \equiv 109 \pmod{143}$ voor $(a, b) = (-1, 5)$.

Examen oefening 80 (1ste zit, 1996-1997) *Geef alle oplossingen van* $x^2 = 1526 \pmod{1829}$. *Tip:* $1829 = 59 \cdot 31$.

Oplossing. Merk op dat $1829 = 59 \times 31$. De opgave kan herleid worden tot het volgende stelsel:

$$\left\{ \begin{array}{rcl} x^2 & \equiv 1526 \pmod{59} & \equiv 51 \pmod{59} \\ x^2 & \equiv 1526 \pmod{31} & \equiv 7 \pmod{31}. \end{array} \right.$$

Deel 1: Reductie van de vergelijkingen tot lineaire congruenties.

We zoeken met behulp van het Legendresymbool of 51 een kwadraatrest is modulo 59 en of 7 een kwadraatrest is modulo 31.

$$\left[\begin{array}{c} 51 \\ 59 \end{array} \right] = \left[\begin{array}{c} 17 \\ 59 \end{array} \right] \cdot \left[\begin{array}{c} 3 \\ 59 \end{array} \right].$$

We bekijken deze twee Legendresymbolen afzonderlijk:

$$\left[\begin{array}{c} 17 \\ 59 \end{array} \right] = \left[\begin{array}{c} 59 \\ 17 \end{array} \right] = \left[\begin{array}{c} 8 \\ 17 \end{array} \right] = \left[\begin{array}{c} 4 \\ 17 \end{array} \right] \cdot \left[\begin{array}{c} 2 \\ 17 \end{array} \right] = 1.$$

$$\left[\begin{array}{c} 3 \\ 59 \end{array}\right] = (-1) \cdot \left[\begin{array}{c} 59 \\ 3 \end{array}\right] = (-1) \cdot \left[\begin{array}{c} 2 \\ 3 \end{array}\right] = (-1) \cdot (-1) = 1.$$

We vinden dat

$$\left[\begin{array}{c} 51 \\ 59 \end{array}\right] = 1.$$

Anderzijds is

$$\left[\begin{array}{c} 7 \\ 31 \end{array}\right] = (-1) \cdot \left[\begin{array}{c} 31 \\ 7 \end{array}\right] = (-1) \cdot \left[\begin{array}{c} 3 \\ 7 \end{array}\right] = \left[\begin{array}{c} 7 \\ 3 \end{array}\right] = \left[\begin{array}{c} 1 \\ 3 \end{array}\right] = 1.$$

Beide vergelijkingen hebben oplossingen in x want de twee Legendresymbolen zijn 1. We vinden voor de eerste vergelijking dat $x^2 \equiv 51 \pmod{59} \equiv 169 \pmod{59}$, dus $x \equiv \pm 13 \pmod{59}$. De tweede vergelijking levert het volgende op: $x^2 \equiv 7 \pmod{31} \equiv 100 \pmod{31}$, dus $x \equiv \pm 10 \pmod{31}$.

We bekomen de volgende vier stelsels lineaire congruenties:

$$\left\{\begin{array}{rcll} x & \equiv & 10 & \pmod{31} \\ x & \equiv & 13 & \pmod{59} \end{array}\right. \vee \left\{\begin{array}{rcll} x & \equiv & -10 & \pmod{31} \\ x & \equiv & -13 & \pmod{59} \end{array}\right. \vee$$

$$\left\{\begin{array}{rcll} x & \equiv & -10 & \pmod{31} \\ x & \equiv & 13 & \pmod{59} \end{array}\right. \vee \left\{\begin{array}{rcll} x & \equiv & 10 & \pmod{31} \\ x & \equiv & -13 & \pmod{59}. \end{array}\right.$$

Deel 2: Oplossing van de stelsels lineaire congruenties.

Het eerste en tweede, net zoals het derde en vierde stelsel, hebben tegengestelde oplossingen die, wegens de Chinese reststelling, uniek zijn modulo $31 \cdot 59 = 1829$.

Een oplossing voor het eerste stelsel is $x = 13 \cdot 31 \cdot x_1 + 10 \cdot 59 \cdot x_2$. Dus

$$\begin{array}{rcll} x \equiv 13 \pmod{59} & \equiv & 13 \cdot 31 \cdot x_1 & \pmod{59} \\ & \Updownarrow & & \\ 1 & \equiv & 31 \cdot x_1 & \pmod{59}. \end{array}$$

De inverse van $31 \pmod{59}$ volgt uit het algoritme van Euclides. Namelijk

$$\begin{array}{rcl} 59 & = & 1 \cdot 31 + 28 \\ 31 & = & 1 \cdot 28 + 3 \\ 28 & = & 9 \cdot 3 + 1. \end{array}$$

Bijgevolg

$$\begin{aligned} 1 &= 28 - 9 \cdot 3 \\ &= 28 - 9 \cdot (31 - 28) \\ &= 10 \cdot 28 - 9 \cdot 31 \\ &= 10 \cdot (59 - 31) - 9 \cdot 31 \\ &= 10 \cdot 59 - 19 \cdot 31 \end{aligned}$$

Dus $1 \equiv -19 \cdot 31 \pmod{59}$, dus $-19 \equiv 40 \pmod{59}$ is de inverse van 31 (mod 59), dus $x_1 \equiv 40 \pmod{59}$.
Er geldt:

$$\begin{aligned} x \equiv 10 \pmod{31} &\equiv 10 \cdot 59 \cdot x_2 \pmod{31} \\ &\Updownarrow \\ 1 &\equiv 59 \cdot x_2 \pmod{31}. \end{aligned}$$

Uit $1 = 10 \cdot 59 - 19 \cdot 31$ volgt dat $1 \equiv 10 \cdot 59 \pmod{31}$ dus $x_2 \equiv 10$ (mod 31).

Beide waarden voor x_1 en x_2 geven

$$\begin{aligned} x &\equiv 13 \cdot 31 \cdot 40 + 10 \cdot 59 \cdot 10 \pmod{59 \cdot 31} \\ &\equiv 72 \pmod{1829}. \end{aligned}$$

De oplossing voor het tweede stelsel is dan

$$x \equiv -72 \pmod{1829} \equiv 1757 \pmod{1829}.$$

Het derde stelsel heeft als oplossing:

$$x = 13 \cdot 31 \cdot x_1 - 10 \cdot 59 \cdot x_2$$

waarbij

$$x \equiv 13 \pmod{59} \equiv 13 \cdot 31 \cdot x_1 \pmod{59}$$

en

$$x \equiv -10 \pmod{31} \equiv -10 \cdot 59 \cdot x_2 \pmod{31}.$$

Beide vergelijkingen zijn equivalent met

$$1 \equiv 31 \cdot x_1 \pmod{59} \quad \text{en} \quad 1 \equiv 59 \cdot x_2 \pmod{31}.$$

Deze vergelijkingen hebben we al opgelost, en we vonden $x_1 = 40$ en $x_2 = 10$.

De oplossing van het stelsel wordt nu:

$$\begin{aligned} x &\equiv 13 \cdot 31 \cdot 40 - 10 \cdot 59 \cdot 10 \pmod{1829} \\ &\equiv 1075 \pmod{1829}. \end{aligned}$$

De oplossing voor het vierde stelsel is dan

$$x \equiv -1075 \pmod{1829} \equiv 754 \pmod{1829}.$$

Examen oefening 81 (1ste zit, 1998-1999) *Herleid de volgende vergelijking tot een systeem van stelsels lineaire congruenties.*

$$x^4 = 53 \pmod{259}.$$

Oplossing. Merk op dat $259 = 37 \times 7$. Deze vergelijking is equivalent is met het stelsel

$$\begin{cases} X^4 \equiv 53 \pmod{37} \\ X^4 \equiv 53 \pmod{7} \end{cases}$$

wat equivalent is met

$$\begin{cases} X^4 \equiv 16 \pmod{37} \\ X^4 \equiv 4 \pmod{7} \end{cases}$$

wat equivalent is met

$$\begin{cases} X^2 \equiv +4 \pmod{37} \ \vee \ -4 \pmod{37} \\ X^2 \equiv +2 \pmod{7} \ \vee \ -2 \pmod{7} \end{cases}$$

wat equivalent is met

$$\begin{cases} X^2 \equiv +4 \pmod{37} \ \vee \ -4 \pmod{37} \\ X^2 \equiv +9 \pmod{7} \ \vee \ -2 \pmod{7} \end{cases}.$$

Nu is het duidelijk dat 4 of 9 een kwadraatrest is modulo 37 of 7, en dat $-4 \pmod{37} = 144 \pmod{37}$. Verder is $\left[\frac{-2}{7}\right] = -1$.

Het bovenstaande stelsel is dus equivalent met

$$\begin{cases} X \equiv +2, -2, 12, -12 \pmod{37} \\ X \equiv +3, -3 \pmod{7} \end{cases}$$

of met de acht stelsels

$$\begin{cases} X & \equiv & a & (\text{mod } 37) \\ X & \equiv & b & (\text{mod } 7) \end{cases}$$

waarbij $a \in \{2, 12, 25, 35\}$ en $b \in \{3, 4\}$.

Examen oefening 82 (2de zit, 1998-1999) *Los op:* $Z^6 = 29 \pmod{35}$.

Oplossing. Merk op dat $35 = 5 \times 7$. De vergelijking is dus equivalent is met het stelsel

$$\begin{cases} Z^6 & \equiv & 29 & (\text{mod } 5) \\ Z^6 & \equiv & 29 & (\text{mod } 7) \end{cases},$$

wat equivalent is met

$$\begin{cases} Z^6 & \equiv & 4 & (\text{mod } 5) \\ Z^6 & \equiv & 1 & (\text{mod } 7) \end{cases},$$

wat equivalent is met

$$\begin{cases} Z^3 & \equiv & +2 & (\text{mod } 5) & \vee & -2 & (\text{mod } 5) \\ Z^3 & \equiv & +1 & (\text{mod } 7) & \vee & -1 & (\text{mod } 7) \end{cases},$$

wat equivalent is met

$$\begin{cases} Z^3 & \equiv & 27 & (\text{mod } 5) & \vee & 8 & (\text{mod } 5) \\ Z^3 & \equiv & 1 & (\text{mod } 7) & \vee & -1 & (\text{mod } 7) \end{cases},$$

wat equivalent is met

$$\begin{cases} Z & \equiv & 3 & (\text{mod } 5) & \vee & 2 & (\text{mod } 5) \\ Z & \equiv & 1 & (\text{mod } 7) & \vee & 6 & (\text{mod } 7) \end{cases}.$$

Dit levert vier stelsels.

Beschouw het eerste stelsel

$$\begin{cases} Z & \equiv & 3 & (\text{mod } 5) \\ Z & \equiv & 1 & (\text{mod } 7) \end{cases}.$$

Een oplossing hiervan is van de vorm $Z = 3 \cdot 7y_1 + 1 \cdot 5y_2$ dus

$$\begin{aligned} Z \equiv 3 \pmod{5} \equiv 21y_1 \pmod{5} \Leftrightarrow 3 \equiv 1y_1 \pmod{5} &\Rightarrow y_1 = 3 \\ Z \equiv 1 \pmod{7} \equiv 5y_2 \pmod{7} &\Rightarrow y_2 = 3. \end{aligned}$$

Na substitutie van y_1 en y_2 geeft dit $Z \equiv 78 \pmod{35} \equiv 8 \pmod{35}$.

Beschouw het tweede stelsel

$$\begin{cases} Z \equiv 3 \pmod 5 \\ Z \equiv 6 \pmod 7 \end{cases}.$$

Een oplossing hiervan is van de vorm $Z = 3 \cdot 7y_1 + 6 \cdot 5y_2$ dus

$$\begin{aligned} Z \equiv 3 \pmod 5 \equiv 21y_1 \pmod 5 &\Rightarrow y_1 = 3 \\ Z \equiv 6 \pmod 7 \equiv 30y_2 \pmod 7 \Leftrightarrow 6 \equiv 2y_2 \pmod 7 &\Rightarrow y_2 = 3. \end{aligned}$$

Na substitutie van y_1 en y_2 geeft dit $Z \equiv 153 \pmod{35} \equiv 13 \pmod{35}$.

Beschouw het derde stelsel

$$\begin{cases} Z \equiv 2 \pmod 5 \\ Z \equiv 1 \pmod 7 \end{cases}.$$

Een oplossing hiervan is van de vorm $Z = 2 \cdot 7y_1 + 1 \cdot 5y_2$ dus $y_1 = 3$ en $y_2 = 3$ zodat $Z \equiv 57 \pmod{35} \equiv 22 \pmod{35}$.

Beschouw tenslotte het stelsel

$$\begin{cases} Z \equiv 2 \pmod 5 \\ Z \equiv 6 \pmod 7 \end{cases}.$$

Een oplossing hiervan is $y = 2 \cdot 7y_1 + 6 \cdot 5y_2$ dus $y_1 = 3$ en $y_2 = 3$ zodat $Z \equiv 132 \pmod{35} \equiv 27 \pmod{35}$.

Examen oefening 83 (2de zit, 1999-2000) *Los op* $X^6 = 113 \pmod{143}$.

Oplossing. Merk op dat $143 = 11 \times 13$. Deze vergelijking is equivalent met het stelsel

$$\begin{cases} X^6 \equiv 113 \pmod{11} \\ X^6 \equiv 113 \pmod{13} \end{cases};$$

wat equivalent is met

$$\begin{cases} X^6 \equiv 3 \pmod{11} \\ X^6 \equiv 9 \pmod{13} \end{cases};$$

wat op zijn beurt equivalent is met

$$\begin{cases} X^3 \equiv 5 \pmod{11} \vee 6 \pmod{11} \\ X^3 \equiv 3 \pmod{13} \vee 8 \pmod{13} \end{cases}.$$

Nu is in $\mathbb{Z}_{11}$: $1^3 = 1$, $2^3 = 8$, $3^3 = 5$, $4^3 = 9$, $5^3 = 4$, $6^3 = 7$, $7^3 = 2$, $8^3 = 6$, $9^3 = 3$, $10^3 = 10$; en in $\mathbb{Z}_{13}$: $1^3 = 1$, $2^3 = 8$, $3^3 = 1$, $4^3 = 12$, $5^3 = 8$, $6^3 = 8$, $7^3 = 5$, $8^3 = 5$, $9^3 = 1$, $10^3 = 12$, $11^3 = 5$, $12^3 = 12$.

Dus is het stelsel equivalent met

$$\begin{cases} X \equiv 3 \pmod{11} \vee 8 \pmod{11} \\ X \equiv 2 \pmod{13} \vee 5 \pmod{13} \vee 6 \pmod{13} \end{cases}$$

We bekomen dus zes stelsels.

Beschouw het eerste stelsel

$$\begin{cases} X \equiv 3 \pmod{11} \\ X \equiv 2 \pmod{13} \end{cases}.$$

We gebruiken de Chinese reststelling en stellen $y = 2 \cdot 11y_1 + 3 \cdot 13y_2$. Dan is

$$1 \pmod{11} \equiv 13y_2 \pmod{11} \equiv 2y_2 \pmod{11} \quad \Rightarrow \quad y_2 \equiv 6 \pmod{11}$$
$$1 \pmod{13} \equiv 66 \pmod{13} \equiv 11y_1 \pmod{13} \Rightarrow y_1 \equiv 6 \pmod{13}$$

Na substitutie van y_1 en y_2 wordt $y = 366$ dus $X \equiv 80 \pmod{143}$.

Beschouw het tweede stelsel

$$\begin{cases} X \equiv 8 \pmod{11} \\ X \equiv 2 \pmod{13} \end{cases}.$$

Stel nu $y = 2 \cdot 11y_1 + 8 \cdot 13y_2$. Dan bekomen we volledig analoog $y_1 \equiv 6 \pmod{13}$ en $y_2 \equiv 6 \pmod{11}$. Na substitutie van y_1 en y_2 wordt $y = 756$ dus $X \equiv 41 \pmod{143}$.

Beschouw het derde stelsel

$$\begin{cases} X \equiv 3 \pmod{11} \\ X \equiv 5 \pmod{13} \end{cases}.$$

Stel nu $y = 5 \cdot 11y_1 + 3 \cdot 13y_2$. Dan bekomen we volledig analoog $y_1 \equiv 6 \pmod{13}$ en $y_2 \equiv 6 \pmod{11}$ en $y = 564$ dus $X \equiv 135 \pmod{143}$.

Beschouw het vierde stelsel

$$\begin{cases} X \equiv 8 \pmod{11} \\ X \equiv 5 \pmod{13} \end{cases}.$$

Stel nu $y = 5 \cdot 11y_1 + 8 \cdot 13y_2$. Dan bekomen we volledig analoog $y_1 \equiv 6 \pmod{13}$ en $y_2 \equiv 6 \pmod{11}$ en $y = 954$ dus $X \equiv 96 \pmod{143}$.

Beschouw het vijfde stelsel

$$\left\{\begin{array}{rcll} X & \equiv & 3 & (\text{mod } 11) \\ X & \equiv & 6 & (\text{mod } 13) \end{array}\right. .$$

Stel nu $y = 6 \cdot 11y_1 + 3 \cdot 13y_2$. Dan bekomen we volledig analoog $y_1 \equiv 6 \pmod{13}$ en $y_2 \equiv 6 \pmod{11}$ en $y = 630$ dus $X \equiv 58 \pmod{143}$.

Beschouw nu ten slotte het zesde stelsel

$$\left\{\begin{array}{rcll} X & \equiv & 8 & (\text{mod } 11) \\ X & \equiv & 6 & (\text{mod } 13) \end{array}\right. .$$

Stel nu $y = 6 \cdot 11y_1 + 8 \cdot 13y_2$. Dan bekomen we volledig analoog $y_1 \equiv 6 \pmod{13}$ en $y_2 \equiv 6 \pmod{11}$ en $y = 1020$ dus $X \equiv 19 \pmod{143}$.

Extra Oefening 84 *Zoek alle oplossingen voor de congruentie*

$$X^2 + 6X - 31 = 0 \pmod{72}.$$

Oplossing. Deze congruentie $\pmod{72}$ is equivalent met het stelsel

$$\left\{\begin{array}{rcll} X^2 + 6X - 31 & \equiv & 0 & (\text{mod } 8) \\ X^2 + 6X - 31 & \equiv & 0 & (\text{mod } 9) \end{array}\right.$$

$$\Updownarrow$$

$$\left\{\begin{array}{rcll} X^2 + 6X + 1 & \equiv & 0 & (\text{mod } 8) \\ X^2 + 6X + 5 & \equiv & 0 & (\text{mod } 9) \end{array}\right.$$

$$\Updownarrow$$

$$\left\{\begin{array}{rcll} X & \equiv & 1,5 & (\text{mod } 8) \\ X & \equiv & 4,8 & (\text{mod } 9). \end{array}\right.$$

Er zijn dus 4 stelsels die opgelost moeten worden:

$$\left\{\begin{array}{rcll} X & \equiv & 1 & (\text{mod } 8) \\ X & \equiv & 4 & (\text{mod } 9) \end{array}\right. \vee \left\{\begin{array}{rcll} X & \equiv & 1 & (\text{mod } 8) \\ X & \equiv & 8 & (\text{mod } 9) \end{array}\right. \vee$$

$$\left\{\begin{array}{rcll} X & \equiv & 5 & (\text{mod } 8) \\ X & \equiv & 4 & (\text{mod } 9) \end{array}\right. \vee \left\{\begin{array}{rcll} X & \equiv & 5 & (\text{mod } 8) \\ X & \equiv & 8 & (\text{mod } 9). \end{array}\right.$$

De oplossingen hiervoor zijn

$$X \equiv 49 \pmod{72} \vee X \equiv 17 \pmod{72} \vee X \equiv 13 \pmod{72} \vee X \equiv 53 \pmod{72}.$$

Extra Oefening 85 *Wanneer bezit de vergelijking*

$$5X^2 + 8X + 1 = 0 \pmod{p},$$

met p priem en $p \geq 13$, een oplossing?

Oplossing. De vergelijking bezit een oplossing als de discriminant 44 een kwadraatrest $\pmod{p}$ is, m.a.w. als 11 een kwadraatrest $\pmod{p}$ is. Dus $\left[\begin{array}{c} 11 \\ p \end{array}\right] = 1$. Uit de kwadratische wederkerigheidswet volgt

$$\left[\begin{array}{c} 11 \\ p \end{array}\right] \cdot \left[\begin{array}{c} p \\ 11 \end{array}\right] = (-1)^{5(p-1)/2} = (-1)^{(p-1)/2}$$

en dit impliceert, aangezien $\left[\begin{array}{c} 11 \\ p \end{array}\right] = 1$, dat

$$\left[\begin{array}{c} p \\ 11 \end{array}\right] = (-1)^{(p-1)/2}.$$

Deel 1: $\left[\begin{array}{c} p \\ 11 \end{array}\right] = -1 = (-1)^{(p-1)/2}$. Dan is $(p-1)/2$ oneven en dus $p \equiv 3 \pmod{4}$. Aangezien p geen kwadraatrest is $\pmod{11}$, is $p \equiv 2, 6, 7, 8, 10 \pmod{11}$, dus $p, p \geq 13$, is een priemgetal dat voldoet aan de vergelijkingen

$$\left\{\begin{array}{rcl} p & \equiv & 2, 6, 7, 8, 10 \pmod{11} \\ p & \equiv & 3 \pmod{4} \end{array}\right.$$

en dit impliceert $p \equiv 35, 39, 7, 19, 43 \pmod{44}$.

Deel 2: $\left[\begin{array}{c} p \\ 11 \end{array}\right] = 1 = (-1)^{(p-1)/2}$. Dan is $(p-1)/2$ even en dus $p \equiv 1 \pmod{4}$. Aangezien p een kwadraatrest is $\pmod{11}$, is $p \equiv 1, 3, 4, 5, 9 \pmod{11}$. Dus hier voldoet p aan de vergelijkingen

$$\left\{\begin{array}{rcl} p & \equiv & 1, 3, 4, 5, 9 \pmod{11} \\ p & \equiv & 1 \pmod{4} \end{array}\right.$$

en dit betekent $p \equiv 1, 25, 37, 5, 9 \pmod{44}$.

Hoofdstuk 6

Inleiding tot de groepentheorie

6.1 Definities

Voorbeelden

2. Gebruikmakend van de *voortbrengende relaties* kunnen we onze bewerkingstabel aanvullen tot het volgende:

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

   Laat ons nu de bewerkingstabel vervolledigen. We bewijzen $a \bullet b = c$. Stel $a \bullet b = a$, dan zal $b = e$, een strijdigheid. Analoog bewijs je dat $a \bullet b \neq b$, zodat dus $a \bullet b \in \{e, c\}$. Als $a \bullet b = e$, dan moet $a \bullet a = e = a \bullet b$ waaruit $a = b$, een tegenstrijdigheid. Dus $a \bullet b = c$. Analoog kun je zo de ganse tabel vervolledigen.

3. Men controleert eenvoudig dat de bewerking $\oplus$ een *gesloten* binaire bewerking induceert op $\mathbb{Z}_m$, en de axiomaś **(A3), (A4), (A6)** maken $(\mathbb{Z}_m, \oplus)$ tot een groep die noodzakelijk commutatief of abels is. Als we nu $(\mathbb{Z}_m \setminus \{0\}, \otimes)$ beschouwen voor m niet priem, dan bestaan er getallen b, a in $\mathbb{N}[1, m]$ waarvoor $a \cdot b = m$ en dus zal $[a]_m \otimes [b]_m = [0]_m$ waardoor de bewerking $\otimes$ niet gesloten is en er dus niet over een groep kan worden gesproken. Als m wel priem is dan zal $\otimes$ wel gesloten zijn en **(A2)** en

(A3) vullen al twee van de drie groepsaxiomaś in. Het laatste axioma, dat zegt dat elk element een inverse bezit, wordt bewezen door gebruik te maken van de stelling van Euler. Laat $x \in \mathbb{N}[1, m]$, m priem, dan is $x^{m-1} = 1 \pmod{m}$ waardoor de inverse van x gegeven wordt door x^{m-2}.

Examen oefening 86 (2de zit, 1992-1993) *Definieert de onderstaande bewerkingstabel al dan niet een groep?*

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

Oplossing. Deze bewerkingstabel definieert geen groep. Dit kan op verschillende manieren geverifieerd worden.

(a) Beschouw de deelverzameling $\{e, a\}$. Uit de tabel volgt dat deze deelverzameling een groep vormt.

Als de bewerkingstabel een groep definieert, dan volgt uit de Stelling van Lagrange dat de orde van de deelgroep een deler moet zijn van de orde van de groep. Dus 2 moet 5 delen.

Dit is echter niet het geval.

(b) De bewerkingstabel definieert ook geen groep omdat de associativiteit niet geldig is.

Het product $(a \cdot b) \cdot d = c \cdot d = a$ is verschillend van $a \cdot (b \cdot d) = a \cdot c = d$.

Examen oefening 87 (1ste zit, 1994-1995) *Veronderstel dat u en v twee elementen zijn van de abelse groep $(G, \cdot)$ met respectievelijke ordes r en s. Onderstel dat de cyclische groep voortgebracht door u en de cyclische groep voortgebracht door v enkel het neutraal element e gemeen hebben.*
Als je weet dat $ggd(r, s) = d$, wat is dan de orde van het element $u \cdot v$?

Oplossing. Stel $(u \cdot v)^t = 1$, dan is $u^t \cdot v^t = 1$ (wegens commutativiteit!!) en dus ook $u^t = 1$ en $v^t = 1$ daar de cyclische groepen voortgebracht door respectievelijk u en v enkel het neutrale element gemeen hebben.

Daar u orde r heeft, moet r een deler zijn van t. Analoog moet ook s een deler zijn van t. Dit toont aan dat t een veelvoud is van $\text{kgv}(r, s) = r \cdot s/d$.

Neem nu $t = r \cdot s/d$. Dan is $u^t = (u^r)^{s/d} = 1^{s/d} = 1$ en analoog $(v^s)^{r/d} = 1$. Dit toont aan dat de orde van $u \cdot v$ gelijk is aan $r \cdot s/d$.

Examen oefening 88 (1ste zit, 1996-1997) *Zij C_n een cyclische groep voortgebracht door g, dus $C_n = \langle g \rangle$. Bewijs dat de deelgroep $H \leq C_n$, voortgebracht door g^k ($k \in \mathbf{N}\backslash\{0\}$) de orde $\frac{n}{ggd(n,k)}$ heeft.*

Oplossing. De orde van H is het kleinste positief getal m waarvoor $(g^k)^m = e$. Daar $e = g^n$, is m dus het kleinste positief getal waarvoor $km \equiv 0 \pmod{n}$, dus $km = \text{kgv}(n, k)$. Bovendien volgt uit $\text{kgv}(n, k) \cdot \text{ggd}(n, k) = n \cdot k$ dat $km \cdot \text{ggd}(n, k) = nk$ of dus dat $m = \frac{n}{\text{ggd}(n,k)}$.

Examen oefening 89 (2de zit, 1999-2000) *Zij G de verzameling van alle 2×2 matrices van de vorm $\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$, met m een geheel getal. Toon aan dat G een oneindige cyclische groep is voor de matrixvermenigvuldiging. Zoek ook de generator van deze groep.*

Oplossing. Merk op dat

$$\begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & r+s \\ 0 & 1 \end{bmatrix}.$$

Beschouw nu de 1-1 correspondentie

$$\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \leftrightarrow m,$$

dan is duidelijk dat G isomorf is met de oneindige cyclische groep van de gehele getallen $\mathbb{Z}$ onder de optelling. Omdat $(\mathbb{Z}, +)$ gegenereerd wordt door het element 1, hebben we onmiddellijk dat G wordt gegenereerd door $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

6.2 Enkele eenvoudige eigenschappen

Stelling 6.1 *1. In een groep $(G, \cdot)$ heeft de vergelijking $ax = b$ met onbekende x, juist 1 oplossing voor elke a en b, namelijk $a^{-1}b$.*

2. In een groep $(G, \cdot)$ geldt respectievelijk de linkse en de rechtse schrappingswet, m.a.w. uit $ac = ad$, respectievelijk $ca = da$, volgt $c = d$.

3. Elke groep $(G, \cdot)$ heeft slechts 1 neutraal element e. Elk element a van G heeft een unieke inverse a^{-1}.

Oplossing.

1. Als $ax = b$, dan kunnen we beide leden links vermenigvuldingen met a^{-1} om te verkrijgen dat x noodzakelijk gelijk is aan $a^{-1}b$.

2. Als we $ac = ad$ links vermenigvuldingen met a^{-1} dan verkrijgen we $c = d$. Analoog bewijs je de rechtse schrappingswet.

3. Stel G bevat twee neutrale elementen e, e' voor $\cdot$, dan zal $a \cdot e = a = a \cdot e'$, waardoor gebruikmakend van de linkse schrappingswet $e = e'$. Het neutrale element is uniek. Hieruit volgt dat als $a \in G$ twee inverse elementen b_1 en b_2 zou hebben in G voor $\cdot$, dan is $ab_1 = e = ab_2$, waardoor weer met de linkse schrappingswet $b_1 = b_2$ volgt. Elk element heeft dus een unieke inverse.

6.3 Latijnse vierkanten

6.4 Groepsmorphismen

Stelling 6.2 *Als θ een groepsmorphisme is tussen $(G, \bullet)$ en $(G', \circ)$, dan is het beeld van het neutrale element e van G het neutrale element e' van G'. En als a^{-1} de inverse is van $a \in G$ voor $\bullet$, dan zal $\theta(a^{-1})$ de inverse zijn van $\theta(a)$ voor $\circ$.*

Oplossing. Het is duidelijk dat voor alle $a \in G$, $\theta(a) \circ e' = \theta(a) = \theta(a \bullet e) = \theta(a) \circ \theta(e)$. En dus wegens de linkse schrappingswet $e' = \theta(e)$. Hieruit volgt

dan dat $e' = \theta(e) = \theta(a \bullet a^{-1}) = \theta(a) \circ \theta(a^{-1})$. Zodat inderdaad $\theta(a^{-1})$ de unieke inverse is van $\theta(a)$ in $(G', \circ)$.

6.5 Deelgroepen

Voorbeelden

5. We bewijzen dat elke doorsnede van twee deelgroepen $(G_1, \cdot)$, $(G_2, \cdot)$ van $(G, \cdot)$ terug een deelgroep is.
   Beschouw $(G_1 \cap G_2, \cdot)$, dan is $\cdot$ een gesloten bewerking op $G_1 \cap G_2$, want de bewerking is gesloten over zowel G_1 als G_2. Het is triviaal dat het neutrale element e van $(G, \cdot)$ eveneens het neutrale element is van $(G_1 \cap G_2, \cdot)$ (dit volgt onmiddellijk uit $e \in G_1 \cap G_2$). Als $a \in G_1 \cap G_2$, dan zal $a^{-1} \in G_1$ en $a^{-1} \in G_2$ zodat dus elke inverse van een element in $G_1 \cap G_2$ terug in $G_1 \cap G_2$ zit. Dit is voldoende om te besluiten dat $(G_1 \cap G_2, \cdot)$ een groep is want de groeps axioma's worden overgeërft van G. Als we nu $(G_1 \cup G_2, \cdot)$ zouden beschouwen dat is $\cdot$ niet noodzakelijk gesloten over $G_1 \cup G_2$ zodat we in het algemeen niet over een groep kunnen spreken.

Stelling 6.3 *Veronderstel dat $(G, \cdot)$ een groep is en dat G' een deelverzameling is van G. Dan is $(G'.\cdot)$ een deelgroep van $(G, \cdot)$ als en slechts als*

(i) $G' \neq \emptyset$;

(ii) $a, b \in G' \Rightarrow ab \in G'$;

(iii) $a \in G' \Rightarrow a^{-1} \in G'$.

Oplossing. Als G' een deelgroep is dan is $e \in G'$ (e is het neutrale element van $(G, \cdot)$), zodat $e \in G' \neq \emptyset$. (ii) is het zelfde als zeggen dat $\cdot$ gesloten is over G'. En ook (iii) is triviaal als $(G', \cdot)$ een deelgroep is van $(G, \cdot)$. Analoog als in voorgaand voorbeeld kan je aantonen dat als (i), (ii) en (iii) gelden, dat dan de groepsaxioma's van $(G', \cdot)$ volgen uit die van $(G, \cdot)$.

De volgende stelling kan nu eenvoudig bewezen worden door gebruik te maken van de voorgaande.

Stelling 6.4 *Onderstel dat θ een morphisme is van $(G, \bullet)$ naar $(G', \circ)$. Dan is*

1. *$(\theta(G), \circ)$ een deelgroep van $(G', \circ)$.*
2. *$\theta^{-1}(e') = \{g \in G \parallel \theta(g) = e'\}$, met e' het neutrale element van $(G', \circ)$, is een deelgroep van $(G, \bullet)$ die ook de* kern *van θ genoemd wordt.*

De kern van een groepshomomorphisme θ wordt ook Kerθ genoteerd.

6.6 Nevenklassen van een deelgroep

6.7 Cyclische groepen

Examen oefening 90 (2de zit, 1994-1995) *Beschouw de groep $G = \langle a, b\rangle$ met $a^n = e$ $(n \geq 2)$, $b^2 = e$, en met $bab^{-1} = a^{-1}$.*

Bewijs dat de groep G nooit cyclisch is.

Oplossing. Als deze groep cyclisch zou zijn, dan zou zij abels zijn, en dit zou impliceren dat $bab^{-1} = bb^{-1}a = a$.

Dus $bab^{-1} = a^{-1}$ impliceert $a = a^{-1}$ en dus $a^2 = e$, waardoor $n = 2$.

Maar dan is $a^2 = b^2 = e$, en $ab = ba$ daar de groep abels is als zij cyclisch is.

In feite zijn a, b, e en ab de enige elementen in G. Dus $G = \{e, a, b, ab\}$, maar $a^2 = b^2 = (ab)^2 = e$, waardoor er geen element van de orde 4 is.

Dus G is nooit cyclisch.

6.8 Direct product van groepen

Examen oefening 91 (1ste zit, 1991-1992) *Zoek alle deelgroepen van $\mathcal{C}_2 \times \mathcal{C}_3 \times \mathcal{C}_5$.*

Oplossing. Deze oefening kan op de volgende manieren opgelost worden.

(a) Daar $2, 3$ en 5 onderling relatief priem zijn, is de groep $\mathcal{C}_2 \times \mathcal{C}_3 \times \mathcal{C}_5$ isomorf met de cyclische groep $\mathcal{C}_{30}$.

De deelgroepen van $\mathcal{C}_{30}$ zijn de cyclische groepen $\mathcal{C}_d$ met d een deler van 30. Dit zijn de groepen $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_5, \mathcal{C}_6, \mathcal{C}_{10}, \mathcal{C}_{15}$ en $\mathcal{C}_{30}$.

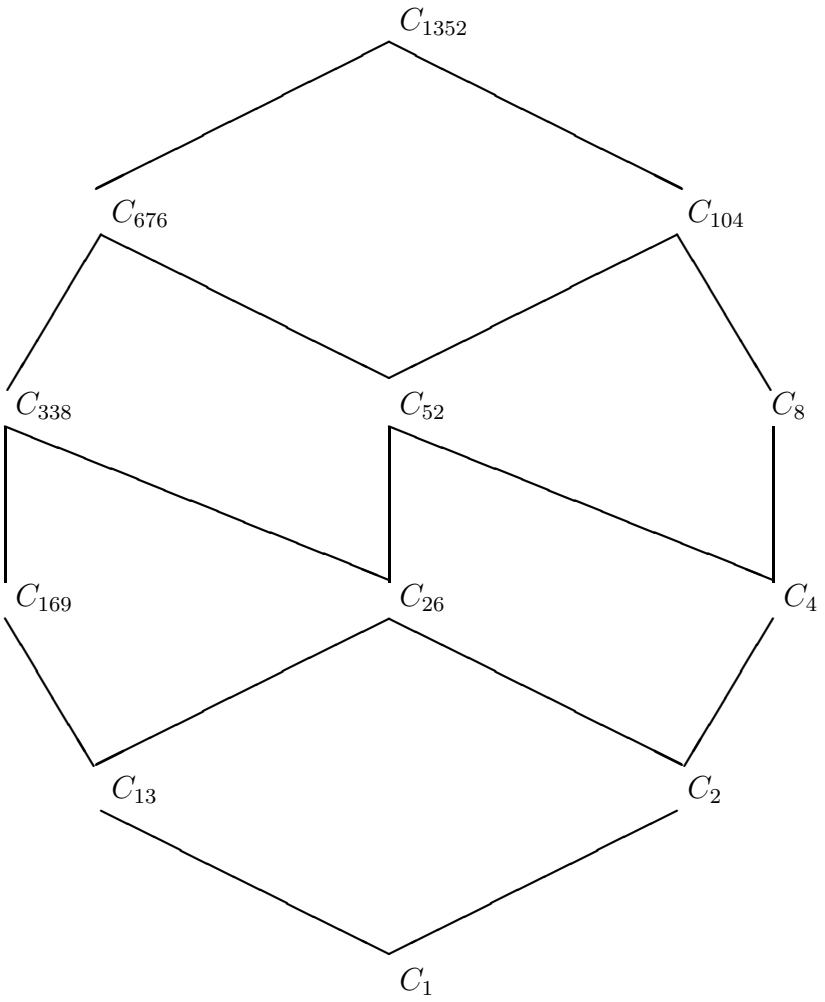
(b) Een deelgroep van $\mathcal{C}_2 \times \mathcal{C}_3 \times \mathcal{C}_5$ bestaat uit het direct product van een deelgroep van $\mathcal{C}_2$, een deelgroep van $\mathcal{C}_3$ en een deelgroep van $\mathcal{C}_5$.

De deelgroepen van $\mathcal{C}_2$ zijn $\mathcal{C}_1$ en $\mathcal{C}_2$, de deelgroepen van $\mathcal{C}_3$ zijn $\mathcal{C}_1$ en $\mathcal{C}_3$, en de deelgroepen van $\mathcal{C}_5$ zijn $\mathcal{C}_1$ en $\mathcal{C}_5$.

Dit geeft de volgende directe producten van deelgroepen $\mathcal{C}_1 \times \mathcal{C}_1 \times \mathcal{C}_1 \cong \mathcal{C}_1, \mathcal{C}_2 \times \mathcal{C}_1 \times \mathcal{C}_1 \cong \mathcal{C}_2, \mathcal{C}_1 \times \mathcal{C}_3 \times \mathcal{C}_1 \cong \mathcal{C}_3, \mathcal{C}_1 \times \mathcal{C}_1 \times \mathcal{C}_5 \cong \mathcal{C}_5, \mathcal{C}_2 \times \mathcal{C}_3 \times \mathcal{C}_1 \cong \mathcal{C}_6, \mathcal{C}_2 \times \mathcal{C}_1 \times \mathcal{C}_5 \cong \mathcal{C}_{10}, \mathcal{C}_1 \times \mathcal{C}_3 \times \mathcal{C}_5 \cong \mathcal{C}_{15}, \mathcal{C}_2 \times \mathcal{C}_3 \times \mathcal{C}_5 \cong \mathcal{C}_{30}$.

Examen oefening 92 (1ste zit, 1993-1994) *Geef de tralie van deelgroepen van de groep* $\mathcal{C}_{169} \times \mathcal{C}_8$.

Oplossing. Daar 169 en 8 copriem zijn, is $C_{169} \times C_8 \cong C_{1352}$. De deelgroepen van C_{1352} zijn C_d met $d|1352$; dus het zijn $C_1, C_2, C_4, C_8, C_{13}, C_{26}, C_{52}, C_{104}, C_{169}, C_{338}, C_{676}, C_{1352}$.
De tralie wordt als volgt opgebouwd.



Examen oefening 93 (2de zit, 1993-1994) *Geef alle cyclische deelgroepen van* $\mathcal{C}_{338} \times \mathcal{C}_{26}$.

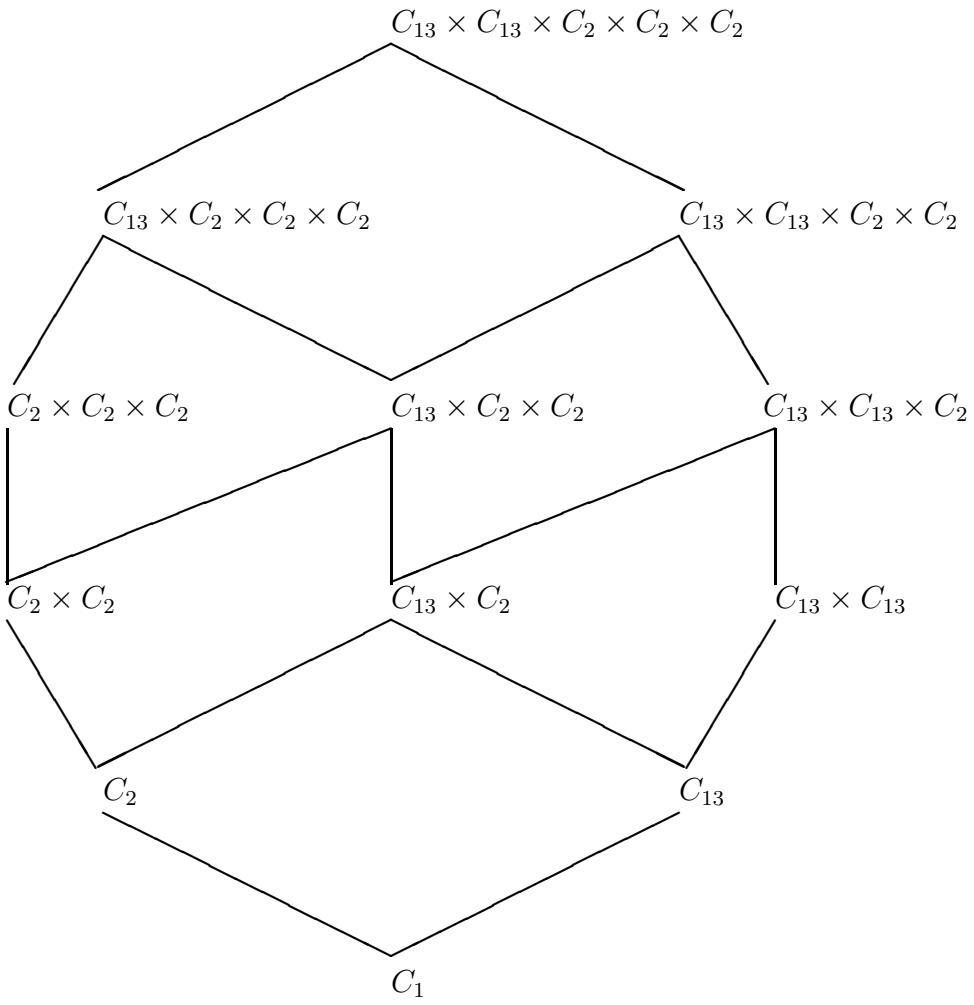
Oplossing. De deelgroepen van $C_{338} \times C_{26}$ zijn de groepen $C_p \times C_q$ met $p|338$ en $q|26$. De groep $C_p \times C_q$ is enkel cyclisch als p en q copriem zijn. Hieruit

volgt dat $C_1 \times C_1, C_1 \times C_2, C_1 \times C_{13}, C_1 \times C_{26}, C_2 \times C_1, C_2 \times C_{13}, C_{13} \times C_1, C_{13} \times C_2, C_{26} \times C_1, C_{169} \times C_1, C_{169} \times C_2,$ en $C_{338} \times C_1$ de cyclische deelgroepen zijn.

Examen oefening 94 (1ste zit, 1994-1995) *Bepaal een groep van de orde 1352 waarin de orde van elk element ten hoogste 26 is. Geef de tralie van deelgroepen van deze groep.*

Oplossing. Daar $1352 = 13^2 \cdot 2^3$ is $C_{13} \times C_{13} \times C_2 \times C_2 \times C_2$ een groep van de orde 1352 met de orde van elk element hoogstens gelijk aan 26.

De tralie is



Examen oefening 95 (2de zit, 1999-2000) *Zoek de cyclische deelgroepen van* $C_2 \times C_5 \times C_{13}$.

Oplossing. Omdat $2, 5$ en 13 copriem zijn is $C_2 \times C_5 \times C_{13} \equiv C_{130}$. De cyclische deelgroepen van C_{130} zijn C_d met $d|130$.
Dus zijn het $C_1, C_2, C_5, C_{13}, C_{10}, C_{26}, C_{65}$ en C_{130}.

6.9 Elementair abelse groepen

6.10 Permutatiegroepen

Extra Oefening 96 *Beschouw een spel kaarten. De 52 kaarten worden geschud zodat als de kaarten oorspronkelijk in de volgorde*

$$1, 2, 3, 4, \ldots, 52$$

lagen, ze nu in de volgorde

$$1, 27, 2, 28, 3, 29, \ldots, 26, 52$$

liggen. Hoeveel keer moeten de kaarten op deze manier geschud worden zodat ze opnieuw in de originele volgorde liggen?

Oplossing. Het schudden van de kaarten betekent de volgende permutatie:

$$\begin{aligned} i &\mapsto 2i - 1 \quad \text{voor} \quad 1 \leq i \leq 26 \\ i &\mapsto 2(i - 26) \quad \text{voor} \quad 27 \leq i \leq 52. \end{aligned}$$

In cykelgedaante is dit de permutatie:

$$(1)(2, 3, 5, 9, 17, 33, 14, 27)(4, 7, 13, 25, 49, 46, 40, 28)(6, 11, 21, 41, 30, 8, 15, 29)$$

$$(10, 19, 37, 22, 43, 34, 16, 31)(12, 23, 45, 38, 24, 47, 42, 32)$$

$$(18, 35)(20, 39, 26, 51, 50, 48, 44, 36)(52).$$

Bijvoorbeeld, de cykel $(2, 3, 5, 9, 17, 33, 14, 27)$ wordt als volgt bekomen: de tweede kaart ligt nu op de derde plaats, de kaart die vroeger op plaats 3 lag, ligt nu op plaats 5, die op plaats 5 lag, bevindt zich nu op plaats $9, \ldots,$ en de kaart die vroeger op plaats 27 lag, ligt nu op plaats 2. De andere cykels worden op analoge wijze gevonden. Alle cykels hebben lengte $1, 2$ of 8. Dus moeten de kaarten precies 8 keer op deze wijze geschud worden om ze opnieuw in hun originele volgorde te bekomen.

Oefening 6.10.1 *1. Stel de Cayley tabel op voor de groep van de symmetrieën van een vierkant. Bewijs dat deze groep de viergroep van Klein bezit als deelgroep van index 2.*

2. *Stel de Cayley tabel op voor de groep* $C_2 \times C_4$.

3. *Stel de Cayley tabel op voor de deelgroep* $(X, \cdot) = (\{1, -1, i, -i\}, \cdot)$ *van de complexe getallen* ($\cdot$ *is de gewone vermenigvuldiging van complexe getallen).*

4. *Bepaal al de deelgroepen van* C_{15} *en* C_{25}.

5. *Hoeveel elementen van* C_{60} *brengen de ganse groep voort?*

6. *Welke van de volgende permutaties zijn even en welke oneven?*

$$\alpha = (1357)(2468); \beta = (127)(356)(48); \gamma = (135)(678)(2)(4).$$

7. *Veronderstel dat* u *en* v *twee elementen zijn van een abelse groep met respectievelijke orde* r *en* s. *Bewijs dat, in de veronderstelling dat* $ggd(r, s) = 1$, *de orde van* uv *gelijk is aan* rs.

8. *Beschouw de groep* $(GL(2, \mathbb{Z}_2), \cdot)$, *van de* 2×2 *matrices met elementen in* $(Z)_2$. *Bewijs dat deze groep isomorf is met* S_3.

9. *Hoeveel groepen van de orde 6 bestaan er op een isomorphisme na?*

Oplossing.

1. De symmetrieën van een vierkant in het Euclidisch vlak, zijn de vier rotaties r_1, r_2, r_3 en $r_4 = e$ om respectievelijk $n \cdot 90°$, $n = 1, 2, 3, 4$, en de spiegelingen d_1, d_2, b_1 en b_2 om respectievelijk de diagonalen en hun bissectrices. Er zijn er dus acht. Men bewijst

$$r_1 \circ r_2 = r_3 = r_2 \circ r_1, r_1 \circ r_3 = r_2 \circ r_2 = e,$$

$$r_1 \circ d_1 = b_1, r_2 \circ d_1 = d_2, r_3 \circ d_1 = b_2, r_1 \circ d_2 = b_1,$$

$$r_2 \circ d_2 = d_1, r_3 \circ d_2 = b_1, r_1 \circ b_1 = d_2, r_2 \circ b_1 = b_2,$$

$$r_3 \circ b_1 = d_1, r_1 \circ b_2 = d_1, r_2 \circ b_2 = b_1, r_3 \circ b_2 = d_2,$$

door aan te tonen dat $x^{l(v)} = x^{r(v)}$ voor alle hoekpunten x van het vierkant en voor alle bovenstaande gelijkheden v, met $l(v)$, $r(v)$ respectievelijk het linker en rechter lid van v. Schrijven we deze gegevens

uit in onze bewerkingstabel, dan komt er:

$\circ$	e	r_1	r_2	r_3	d_1	d_2	b_1	b_2
e	e	r_1	r_2	r_3	d_1	d_2	b_1	b_2
r_1	r_1	r_2	r_3	e	b_1	b_2	d_2	d_2
r_2	r_2	r_3	e	r_1	d_2	d_1	b_2	b_1
r_3	r_3	e	r_1	r_2	b_2	b_1	d_1	d_2
d_1	d_1	b_1	d_2	b_2	e	r_2	r_3	r_1
d_2	d_2	b_2	d_1	b_1	r_2	e	r_1	r_3
b_1	b_1	d_2	b_2	d_1	r_1	r_3	e	r_2
b_2	b_2	d_1	b_1	d_2	r_3	r_1	r_2	e

.

Wegens stelling 6.3 is de verzameling van symmetrieën van een vierkant in het Euclidische vlak een groep onder de samenstelling '$\circ$'. Beschouwen we nu de deeltabel bepaald door de rijen en kolommen waarvoor het eerste element een element is van $K = \{e, r_2, d_1, d_2\}$, dan zien we dat deze tabel dezelfde relaties definieert als de Cayley tabel voor de viergroep van Klein. Dus K is een deelgroep van de groep van symmetrieën die isomorf is met de viergroep van Klein. Duidelijkerwijze heeft K index 2 in de groep van symmetrieën.

2. Stel $C_2 = \{e, b\}$ en $C_4 = \{e, a, a^2, a^3\}$. Dan ziet de bewerkingstabel voor $C_2 \times C_4$ er als volgt uit:

	(e,e)	(e,a)	(e,a^2)	(e,a^3)	(b,e)	(b,a)	(b,a^2)	(b,a^3)
(e,e)	(e,e)	(e,a)	(e,a^2)	(e,a^3)	(b,e)	(b,a)	(b,a^2)	(b,a^3)
(e,a)	(e,a)	(e,a^2)	(e,a^3)	(e,e)	(b,a)	(b,a^2)	(b,a^3)	(b,e)
(e,a^2)	(e,a^2)	(e,a^3)	(e,e)	(e,a)	(b,a^3)	(b,e)	(b,a)	(b,a^2)
(e,a^3)	(e,a^3)	(e,e)	(e,a)	(e,a^2)	(b,a^3)	(b,e)	(b,a)	(b,a^2)
(b,e)	(b,e)	(b,a)	(b,a^2)	(b,a^3)	(e,e)	(e,a)	(e,a^2)	(e,a^3)
(b,a)	(b,a)	(b,a^2)	(b,a^3)	(b,e)	(e,a)	(e,a^2)	(e,a^3)	(e,e)
(b,a^2)	(b,a^2)	(b,a^3)	(b,e)	(b,a)	(e,a^2)	(e,a^3)	(e,e)	(e,a)
(b,a^3)	(b,a^3)	(b,e)	(b,a)	(b,a^2)	(e,a^3)	(e,e)	(e,a)	(e,a^2)

3. Beschouw het vierkant $\{1+i, -1+i, -1-i, 1-i\}$ in het Euclidische vlak. Dan zien we dat na vermenigvuldiging met $x \in X$ het vierkant op het vierkant afgebeeld wordt. Dus elke $x \in X$ induceert een symmetrie s_x van het vierkant. Nu is s_1 de identische summetrie; s_{-1} is de puntspiegeling om de oorsprong; s_i de spiegeling om de rechte door de

punten $-1+i$ en $1-i$; en tenslotte s_{-i} is de spiegeling om de rechte door de punten $1+i$, $-1-i$. De bewerkingstabel van deze groep is dus niks anders dan deze van de viergroep van Klein.

4. Beide groepen zijn cyclisch bij definitie. En dus wegens stelling 6.9 bestaat er voor elke deler d juist 1 deelgroep met orde d, en omgekeerd. Hieruit volgt dat C_{15} slechts 2 eigenlijke deelgroepen heeft met respectievelijke ordes 3, 5; en C_{25} bevat maar 1 eigenlijke deelgroep van de orde 5.

5. We zoeken het aantal elementen van C_{60} met orde 60. Wegens Stelling 6.8 bevat C_{60} juist $\Phi(60) = \Phi(4)\Phi(3)\Phi(5) = 2 \cdot 2 \cdot 5 = 20$.

6. We kunnen (1357) schrijven als (13)(15)(17); analoog geldt (2468) = (24)(26)(28), waardoor α even is. Eveneens is (127) = (12)(17) en (356) = (35)(36), waardoor β oneven is. Voor γ schrijven we (135) als (13)(15) en (678) = (67)(68), zowel (2) als (4) kunnen voorgesteld worden door de ledige transpositie, waardoor γ even is.

7. Stel de orde van uv voor door t, dan is $(uv)^t = u^t v^t = e$. Hieruit volgt dat $v^t in \langle u \rangle$. Als t geen veelvoud is van s, dan is $\langle u \rangle \cap \langle v \rangle \neq \emptyset$, dus hun doorsnede is terug een deelgroep met orde groter dan 1, zodat $ggd(r,s) > 1$ een tegenstrijdigheid. Dus $s \mid t$; en analoog $r \mid t$; waaruit $rs \mid t$. Maar nu is ook $(uv)^{rs} = u^{rs}v^{rs} = (u^r)^s(v^s)^r = e^s e^r = e$, waardoor $t \mid rs$. Hieruit volgt het gestelde.

8. We moeten enkel aantonen dat deze groep ook de groep S is van symmetrieën van een driehoek, omdat de symmetriegroep van een driehoek isomorf is met S_3. Nu zien we dat $(X = \{(0,0),(0,1),(1,0),(1,1)\}, \otimes_2)$ een abelse groep is. Nu kunnen we $\mathrm{GL}(2,\mathbb{Z}_2)$ opvatten als een permutatie groep over X die $(0,0)$ fixeert, die getrouw is op X en dus ook getrouw is op $X \setminus \{(0,0)\}$, waardoor $|\mathrm{GL}(2,\mathbb{Z}_2)| \leq 6$, maar gelijkheid moet gelden! Hieruit volgt dat $\mathrm{GL}(2,\mathbb{Z}_2) \cong S_3$.

9. Teneerste hebben we C_6. Veronderstel dus dat onze groep niet meer cyclisch is, dan heeft elk element, $\neq e$, van onze groep orde 2 of 3. En er bestaan zeker elementen van de orde 2 en 3, want anders zou onze groep, elementair abels zijn en dus van priemacht orde zijn, een strijdigheid. Stel a is een element van de orde 2 en b een element van de orde 3. Dan zijn C_2, C_3 twee deelgroepen van onze groep die dan

noodzakelijk abels is (anders zou onze groep meer dan 6 elementen bevatten), waardoor ook $C_2 \times C_3$ een deelgroep is. Maar $|C_2 \times C_3| = 6$ waardoor $C_2 \times C_3$ gelijk is aan onze groep. Er zijn dus twee groepen van de orde 6 op een isomorphisme na, en ze zijn beide abels.

Hoofdstuk 7

Ringen, lichamen en velden

7.1 Ringen

7.1.1 Definities

Opmerkingen

1. Er wordt gevraagd aan te tonen dat het neutrale element van een ring uniek is. Wel dit wordt op analoge wijze aangetoond als voor groepen: Stel er zijn twee neutrale elementen e, e', dan is $e = e \cdot e' = e'$.

7.2 Inverteerbare elementen van een ring

7.2.1 Definities

Opmerking

Er wordt gevraagd aan te tonen dat $(U(\mathbb{F}_8), \cdot)$ isomorf is met de viergroep van Klein, waarbij $\cdot$ de gewone vermenigvuldiging modulo 8 is. We hebben in Hoofdstuk 5 aangetoond dat de viergroep van Klein de enige groep van de orde vier is waarvoor alle elementen orde 2 hebben. Nu gaan we eenvoudig na dat $(U(\mathbb{F}_8), \cdot)$ hieraan voldoet.

Een andere oplossingsmethode is de volledige bewerkingstabel van $(U(\mathbb{F}_8), \cdot)$ neer te schrijven en deze te vergelijken met die van de viergroep van Klein.

7.3 Lichamen en velden

7.4 Veeltermringen

7.4.1 Definitie

7.4.2 Het delingsalgorithme voor veeltermen

7.4.3 Het algorithme van Euclides voor veeltermen

7.4.4 Ontbinden in factoren

Oefening 7.4.1 *1. Ontbind $x^8 - 1$ in $\mathbb{Z}_3[x]$.*

2. Ontbind $x^3 + 5x^2 + 5$ in $\mathbb{Z}_{11}[x]$.

3. Zoek alle monische polynomen die irreduciebel zijn in $\mathbb{Z}_3$.

4. Bewijs dat $x^2 + 2x + 2$ irreduciebel is in $\mathbb{Z}_3[x]$.

Oplossing.

1. Sinds $a^2-b^2 = (a-b)(a+b)$, kunnen we x^8-1 herleiden tot $(x-1)(x+1)(x^2+1)(x^4+1)$. Nu controleert men eenvoudig dat x^2+1 irreduciebel is in $\mathbb{Z}_3[x]$ omdat deze veelterm van de tweede graad geen wortels heeft over $\mathbb{Z}_3[x]$. Anderzijds wordt de factorisatie van x^4+1 gegeven door het laatste voorbeeld in de cursus, namelijk $x^4+1 = (x^2+x+2)(x^2+2x+2)$. Dus de gezochte factorisatie is $(x-1)(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2)$.

2. Deze veelterm is van de graad 3 en dus irreduciebel over $\mathbb{Z}_{11}$ als ze geen wortels bevat in $\mathbb{Z}_{11}$.

$\alpha \in \mathbb{Z}_{11}$	$\alpha^3 + 5\alpha^2 + 5$
0	5
1	0
$\vdots$	$\vdots$

   Dus $x-1$ is een deler van onze veelterm over $\mathbb{Z}_{11}$. Men verifieert dat $(x^2+6x+6)(x-1)$. Deze factorisatie is compleet als de eerste factor

irreduciebel is.

$\alpha \in \mathbb{Z}_{11}$	$\alpha^2 + 6\alpha + 6$
0	6
1	2
2	0
$\vdots$	$\vdots$

Zodat $x-2 \mid x^2+6x+6$ en men controleert dat $x^2+6x+6 = (x+8)(x-2)$ over $\mathbb{Z}_{11}$. De gezochte factorisatie is dus $(x+8)(x-2)(x-1)$.

3. Er zijn geen irreduciebel veeltermen van de eerste graad, bij definitie. De verzameling V_2 van monische irreduciebele veeltermen $(a_0, a_1, 1)$ van de 2de graad over $\mathbb{Z}_3$, wordt gegeven door

$$V_2 = \{(a_0, a_1, 1) \parallel a_0, a_1 \in \mathbb{Z}_3\} \setminus \{(\alpha\beta, \alpha+\beta, 1) \parallel \alpha, \beta \in \mathbb{Z}_3\}.$$

Nu kunnen we de verzameling V_n van monische irreduciebele veeltermen over $\mathbb{Z}_3$ van de $n$de graad inductief definiëren door

$$\begin{aligned} V_n \;=\; & \{(a_0, \ldots, a_{n-1}, 1) \parallel a_0, \ldots, a_{n-1} \in \mathbb{Z}_3\} \;\setminus \\ & \{(\alpha_0, \ldots, \alpha_{k-1}, 1)(\beta_0, \ldots, \beta_{n-k-1}, 1) \parallel \\ & \forall k \in \mathbb{Z}_n, (\alpha_0, \ldots, \alpha_{k-1}, 1) \in V_k,\; \beta_0, \ldots, \beta_{n-k-1} \in \mathbb{Z}_3\}. \end{aligned}$$

4. Aangezien onze veelterm van de graad ≤ 3 is, is deze irreduciebel als ze geen wortels heeft.

$\alpha \in \mathbb{Z}_3$	$\alpha^2 + 2\alpha + 2$
0	2
1	2
2	1

Uit bovenstaande tabel volgt dat dit inderdaad het geval is, de veelterm $x^2 + 2x + 2$ is dus irreduciebel in $\mathbb{Z}_3[x]$.

7.5 Eindige velden

7.5.1 Inleiding

In deze sectie wordt gevraagd Stelling 7.7 te bewijzen. Wel dit volgt onmiddellijk uit Oefening **??** op pagina **??**.

Oefening 7.5.1 *1. Zoek de primitieve elementen van* $\mathbb{Z}_4 1$.

2. Hoeveel primitieve elementen bezit het veld van de orde 64*?*

Oplossing.

1. De primitieve elementen zijn hier niets anders dan de $\Phi(40) = 16$ voortbrengende elementen van zijn multiplicatieve deelgroep (die cyclisch is!). Als nu α een dergelijk primitief element is dan worden alle primitieve elementen gegeven door $\{\alpha^k \parallel k \in \mathbb{Z}_{41} : (k, q-1) = 1\}$. Het enige wat we dus moeten doen is er een vinden. Nu weten we ook, uit Oefening 7 van sectie 6.10, dat als α orde 8 heeft en β orde 5, dat dan $\alpha\beta$ orde 40 heeft. Nu controleer je gemakkelijk dat 3 orde 8 heeft en 16 orde 5 heeft. Dus 7 is een voortbrengend element van $\mathbb{Z}_{41}$.

2. De primitieve elementen van $\mathbb{Z}_{64}$ zijn niets anders dan de voortbrengende elementen van zijn multiplicatieve groep, die orde 63 heeft. Nu heeft elke cyclische groep van de orde 63, net $\Phi(63) = \Phi(7)\Phi(9) = 18$ voortbrengende elementen. Dus het aantal primitieve elementen van $\mathbb{Z}_{64}$ is gelijk aan 18.

Examen oefening 97 *Hoeveel primitieve elementen bezit het veld* $\mathbb{Z}_{16}$*? Welke orde kan een niet-primitief element van* $\mathbb{F}_{16}$ *hebben en hoeveel elementen van die orde zijn er?*

Oplossing. Alle niet-nul elementen van $\mathbb{Z}_{16}$ voldoen aan $X^{15} = 1$. Een primitief element van $\mathbb{Z}_{16}$ is een element dat precies orde 15 heeft. Het aantal primitieve elementen is dus $\Phi(15)$ met Φ de Euler-functie. Er zijn dus $\Phi(15) = \Phi(3 \cdot 5) = 2 \cdot 4 = 8$ primitieve elementen.

De orde van een niet-primitief element, ongelijk 1, van $\mathbb{Z}_{16}$ is steeds een echte deler van 15, dus een niet-primitief element ongelijk 1 heeft 3 of 5 als orde.

De elementen van de orde 3 zijn de oplossingen in $\mathbb{Z}_{16}$ van $X^3 = 1$, die verschillend zijn van 1. Dus zijn er maximaal twee elementen van de orde 3. Analoog zijn de elementen van de orde 5 de oplossingen in $\mathbb{Z}_{16}$ van $X^5 = 1$, verschillend van 1. Dus hier zijn er maximaal vier elementen van de orde 5. Hieruit krijgen we dat $|\mathbb{Z}_{16} \setminus \{0, 1\}| = 14 \leq 8 + 2 + 4$. Hieruit volgt dat er juist 2 elementen van de orde 3 zijn en 4 elementen van de orde 5.

Examen oefening 98 (2de zit, 1993-1994) *Beschouw de functie*

$$f : \mathbb{F}_{3^5} \to \mathbb{F}_{3^5} : x \mapsto x + x^3 + x^9 + x^{27} + x^{81}.$$

Bewijs dat $f(x) \in \mathbb{F}_3$ *voor alle elementen* x *uit* $\mathbb{F}_{3^5}$.

Oplossing. Daar de karakteristiek 3 is, en in $\mathbb{F}_{3^5}$ voor elk getal x geldt dat $x^{3^5} = x$, bekomen we dat

$$\begin{aligned}(f(x))^3 &= (x + x^3 + x^9 + x^{27} + x^{81})^3 \\ &= x^3 + x^9 + x^{27} + x^{81} + x^{243} \\ &= x^3 + x^9 + x^{27} + x^{81} + x \\ &= f(x).\end{aligned}$$

Er geldt steeds dat $(f(x))^3 = f(x)$ wat impliceert dat $f(x) \in \mathbb{F}_3$.

Examen oefening 99 (1ste zit, 1994-1995) *Beschouw het eindig veld* $\mathbb{F}_{25}$. *Hoeveel oplossingen* $(x, y) \in \mathbb{F}_{25} \times \mathbb{F}_{25}$ *bezit de vergelijking* $x^{12} = y^{24}$*?*

Oplossing. Als $y = 0$, dan moet $x = 0$, dus dit geeft één oplossing.

Als $y \neq 0$, dan is $y^{24} = 1$, waardoor ook $x^{12} = 1$. Daar voor $x \in \mathbb{F}_{25} \backslash \{0\}$ steeds $x^{24} = 1$, moet x een kwadraat zijn. Er zijn hier dus $12 \cdot 24 = 288$ oplossingen. In totaal zijn er dus 289 oplossingen.

Examen oefening 100 (2de zit, 1994-1995) *Hoeveel oplossingen* (x_0, x_1, x_2) *zijn er in* $GF(4) \times GF(4) \times GF(4)$ *voor de vergelijking* $X_0^3 + X_1^3 + X_2^3 = 0$*?*

Oplossing. Als $x_0, x_1, x_2 \neq 0$, dan is $x_0^3 = x_1^3 = x_2^3 = 1$ waardoor $x_0^3 + x_1^3 + x_2^3 = 1 \neq 0$. Voor een oplossing (x_0, x_1, x_2) is dus minstens één van de getallen x_0, x_1, x_2 gelijk aan nul. Als twee van x_0, x_1, x_2 nul zijn, dan is de derde ook nul. Stel slechts één getal x_0, x_1, x_2 is nul. Bijvoorbeeld $x_0 = 0$, dan moet $x_1^3 + x_2^3 = 0$. Daar $x_1, x_2 \neq 0$, is $x_1^3 = x_2^3 = 1$ waardoor $x_1^3 + x_2^3 = 2 = 0$. Er zijn dus 9 oplossingen $(0, x_1, x_2)$ met $x_1, x_2 \neq 0$. Analoog zijn er 9 oplossingen $(x_0, 0, x_2)$ met $x_0, x_2 \neq 0$, en 9 oplossingen $(x_0, x_1, 0)$ met $x_0, x_1 \neq 0$. Samen met $(x_0, x_1, x_2) = (0, 0, 0)$ maakt dit in totaal 28 oplossingen.

Examen oefening 101 (1ste zit, 1995-1996) *Bewijs dat in een eindig veld* $\mathbb{F}_q$ *het product van alle verschillende niet-nul elementen gelijk is aan* -1.

Oplossing. Beschouw het product $\prod_{a\in\mathbb{F}_q\setminus\{0\}} a$.

We kunnen de elementen $a \in \mathbb{F}_q \setminus \{0\}$ groeperen in paren. Namelijk in de paren $\{a, a^{-1}\}$. Dit zijn steeds twee verschillende elementen, tenzij $a = \pm 1$.

Stel $a \neq \pm 1$, dan kunnen we in $\prod_{a\in\mathbb{F}_q\setminus\{0\}} a$, voor een dergelijke a, steeds de twee verschillende factoren a en a^{-1} schrappen daar hun product $a \cdot a^{-1}$ toch gelijk is aan 1.

Dit betekent dat $\prod_{a\in\mathbb{F}_q\setminus\{0\}} a = 1 \cdot (-1) = -1$.

7.5.2 Constructie van eindige velden

Er wordt gevraagd aan te tonen dat K een veld is (zie cursus voor de definitie van K). Het is duidelijk dat K met de gegeven vermenigvuldiging en optelling een ring is. Het is een veld als elk niet-nul element inverteerbaar is. Stel dat $f(x)$ de irreduciebele veelterm is die gebruikt werd bij de definitie van de vermenigvuldiging op K, dan is de grootste gemene deler van eender welke veelterm $k(x)$ uit K en $f(x)$ noodzakelijk 1 (of een constante) waardoor, wegens het algorithme van Euclides voor veeltermen, er veeltermen $\lambda(x)$ en $\mu(x)$ kunnen gevonden worden zodat $\lambda(x)k(x) + \mu(x)f(x) = 1$, zodat er dus een veelterm in K bestaat dat de inverse is van $k(x)$, dus K is een veld.

Examen oefening 102 (1ste zit, 1992-1993) *(a) Stel de tabel van de Zech log-functie op voor het veld*

$$\mathbb{F}_{16} = \{0, \alpha, \ldots, \alpha^{15} || \alpha^4 + \alpha + 1 = 0\}.$$

(b) Hoeveel koppels $(x, y) \in \mathbb{F}_{16}\times\mathbb{F}_{16}$ zijn er die voldoen aan $x^4+y^6+1 = 0$?

Oplossing.

(a) Het veld $\mathbb{F}_{16}$ is de verzameling $\{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 || a_0, a_1, a_2, a_3 \in \mathbb{F}_2\}$ waarbij alle bewerkingen in deze verzameling modulo $\alpha^4 + \alpha + 1$ uitgevoerd worden. Dit betekent dus dat

$$\alpha^4 = \alpha + 1.$$

Dit geeft de volgende tabel voor de elementen van $\mathbb{F}_{16}$. De tweede en vierde kolom geven steeds de ontwikkeling van α^i in functie van $1, \alpha, \alpha^2$ en α^3. Deze tabel wordt inductief opgebouwd. Eénmaal α^i bepaald is,

berekent men $\alpha^{i+1} = \alpha \cdot \alpha^i$ en dit modulo $\alpha^4 + \alpha + 1$. Men vervangt dus steeds α^4 door $\alpha + 1$.

0	0	α^7	$1 + \alpha + \alpha^3$
α^0	1	α^8	$1 + \alpha^2$
α^1	α	α^9	$\alpha + \alpha^3$
α^2	α^2	α^{10}	$1 + \alpha + \alpha^2$
α^3	α^3	α^{11}	$\alpha + \alpha^2 + \alpha^3$
α^4	$1 + \alpha$	α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$
α^5	$\alpha + \alpha^2$	α^{13}	$1 + \alpha^2 + \alpha^3$
α^6	$\alpha^2 + \alpha^3$	α^{14}	$1 + \alpha^3$

De Zech log-functie θ geeft het verband $1 + \alpha^i = \alpha^{\theta(i)}$. Aangezien $\alpha^0 + 1 = 0$ wordt de notatie $\alpha^\infty = 0$ ingevoerd zodat $\theta(0)$ ook gedefinieerd kan worden.

Gebruikmakend van de voorgaande tabel worden de volgende functiewaarden voor de Zech log-functie bekomen.

i	$\theta(i)$	i	$\theta(i)$
∞	0	7	9
0	∞	8	2
1	4	9	7
2	8	10	5
3	14	11	12
4	1	12	11
5	10	13	6
6	13	14	3

(b) Net zoals in Oefening 103 heeft elk element van $\mathbb{F}_{16}$ een unieke vierkantswortel.

Beschouw een vergelijking van de vorm $z^4 = a$ met $a \in \mathbb{F}_{16}$. Stel $z^2 = u$, dan wordt de vergelijking $u^2 = a$ en deze vergelijking heeft een unieke oplossing $u = a'$. Maar ook de vergelijking $z^2 = a'$ heeft een unieke oplossing in z, dus voor elk element $a \in \mathbb{F}_{16}$ heeft de vergelijking $z^4 = a$ een unieke oplossing.

Dit impliceert dat voor elke waarde $y \in \mathbb{F}_{16}$ de vergelijking $X^4 = 1 + y^6$ een unieke oplossing in x heeft.

Er zijn 16 keuzes voor y, dus zijn er 16 koppels (x, y) die voldoen aan $x^4 + y^6 + 1 = 0$.

7.5.3 Voorbeelden van eindige velden

7.5.4 Enkele belangrijke stellingen

Oefeningen

1. Bewijs dat elk element van $\mathbb{F}_q$ steeds de som is van 2 kwadraten.
2. Bepaal de kwadraten verschillend van 0 in $\mathbb{F}_{27}$.

Oplossing.

1. Als q even is, is de oefening triviaal, daar dan elk element een kwadraat is en daar elk element kan geschreven worden als de som van twee elementen. Veronderstel dus dat q oneven is, dan zijn er juist $\frac{q-1}{2}$ kwadraten in de multiplicatieve groep, dus als we het neutraal element voor de optelling ook als een kwadraat rekenen dan bevat $\mathbb{Z}_q$ dus $\frac{q+1}{2}$ kwadraten. Definieer nu de afbeelding

$$\begin{aligned} \alpha_\nu : \text{kwadraten in } \mathbb{F}_q &\rightarrow \mathbb{F}_q{}^* \\ x &\mapsto x - \nu, \end{aligned}$$

voor alle niet kwadraten ν. Nu is het duidelijk dat het aantal beelden van $\alpha_n u$ gelijk is aan het aantal kwadraten in $\mathbb{F}_q$ en dus gelijk is aan $\frac{q+1}{2}$. Wegens het ladenprincipe moet er dus een beeld zijn dat in de kwadraten terecht komt. Daarom bestaat er voor alle niet-kwadraten ν een kwadraat x zodat $\nu - x$ een kwadraat is. Dit bewijst het gestelde.

Examen oefening 103 (1ste zit, 1991-1992) *Zoek het aantal oplossingen* $(x, y) \in \mathbb{F}_{16} \times \mathbb{F}_{16}$ *die voldoen aan* $X^2 + Y^3 = 1$.

Oplossing. Daar $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ een veld is van even karakteristiek, is elk element van dit veld een kwadraat en heeft elk element van dit veld dus een unieke vierkantswortel.

De vergelijking $X^2+Y^3=1$ is equivalent met $X^2=1+Y^3$. Hieruit volgt dat voor elke $y \in \mathbb{F}_{16}$ er een unieke oplossing x in $\mathbb{F}_{16}$ is voor de vergelijking $X^2 = 1 + y^3$.

Dus zijn er in totaal 16 oplossingen (x, y).

7.5.5 Kwadratische vergelijkingen

Oefening 7.5.2 *1. Is $x^4 + x + 1$ een primitieve irreduciebele veelterm in $\mathbb{Z}_2[x]$? Zelfde vraag voor $x^4 + x^3 + 1$.*

2. Construeer het veld $\mathbb{F}_{16}$.

3. Wat is de multipliciteit van de wortel 1 van $x^8 + x^7 + x^6 + x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]$?

4. Bepaal in de volgende gevallen de veeltermen $\lambda(x)$ en $\mu(x)$ zodanig dat $ggd(a(x), b(x)) = \lambda(x)a(x) + \mu(x)b(x)$.

(a) $a(x) = x^4 + 2$ en $b(x) = 5x^2 + 6x + 4$ in $\mathbb{Z}_2[x]$.

(b) $a(x) = x^3 + 2x^2 + 2x + 1$ en $b(x) = 2x^2 + 2$ in $\mathbb{Z}_3[x]$.

(c) $a(x) = x^5 + 1$ en $b(x) = x + 1$ in $\mathbb{Z}_2[x]$.

5. Noem α een primitief element van $\mathbb{F}_9$, noem $f(x)$ een irreduciebele veelterm van $\mathbb{Z}_3[x]$ zodanig dat $f(\alpha^2) = 0$. Bepaal $f(x)$.

6. Bewijs dat $x^{16} + x^4 + x + 1 = 0$ precies 16 verschillende wortels heeft in $\mathbb{Z}_{64}$.

7. Hoeveel koppels $(a, b) \in \mathbb{F}_9 \times \mathbb{F}_9$ zijn er met $a^2 - b^2 = 1$?

Examen oefening 104 (2de zit, 1992-1993) *Beschouw $\mathbb{F}_{16}$ gedefinieerd aan de hand van de primitieve veelterm t^4+t+1. Zoek in $\mathbb{F}_{16}$ alle oplossingen van de vergelijking*

$$t^4X^3 + tX^2 + 1 = 0.$$

Oplossing. De elementen van het veld $\mathbb{F}_{16}$, samen met de Zech log-tabel, werden al berekend in Oefening 102. Deze tabellen, met α vervangen door t, zullen gebruikt worden in de berekeningen.

Daar het veld $\mathbb{F}_{16}$ gedefinieerd is door de polynoom t^4+t+1, veronderstellen we $t^4+t+1=0$ en hieruit volgt dat $X=1$ een oplossing is voor $t^4X^3+tX^2+1=0$.

Na deling vinden we dat

$$t^4X^3+tX^2+1=(X+1)(t^4X^2+X+1).$$

Om te onderzoeken of $t^4X^2+X+1=0$ oplossingen heeft in $\mathbb{F}_{16}$, zullen we eerst de variabele X vervangen door $X=bY/a$ met $b=1$ en $a=t^4$ de coëfficienten bij respectievelijk X en X^2.

Dan gaat de vergelijking t^4X^2+X+1 over in $Y^2+Y+\delta=0$ met $\delta=ac/b^2=t^4=t+1$, waarbij $c=1$ de constante is in de vergelijking in X.

De vergelijking $Y^2+Y+t^4=0$ heeft oplossingen in Y als en slechts als $\mathrm{Tr}(\delta)=0$.

Nu is, gebruikmakend van de log-tabel uit Oefening 102,

$$\begin{aligned}\mathrm{Tr}(\delta) &= t^4+t^8+t+t^2 \qquad (t^{16}=t)\\ &= t^4(1+t^4)+t(1+t)\\ &= t^5+t^5\\ &= 0.\end{aligned}$$

De vergelijking $Y^2+Y+t^4=0$ heeft dus oplossingen in $\mathbb{F}_{16}$. Deze oplossingen zijn s en $s+1$ met

$$s=k\delta^2+(k+k^2)\delta^4+(k+k^2+k^4)\delta^8,$$

waarbij k een element is van $\mathbb{F}_{16}$ met $\mathrm{Tr}(k)=1$.

Neem $k=t^{11}$, want, gebruikmakend van $t^{15}=1$ en de log-tabel uit Oefening 102, $\mathrm{Tr}(t^{11})=t^{11}+t^7+t^{14}+t^{13}=t^7(1+t^4)+t^{13}(1+t)=t^8+t^2=t^2(1+t^6)=t^{15}=1$.

Dus

$$\begin{aligned}s &= k\delta^2+(k+k^2)\delta^4+(k+k^2+k^4)\delta^8\\ &= t^{11}t^8+(t^{11}+t^7)t+(t^{11}+t^7+t^{14})t^2\\ &\quad (t^7+t^{11}=t^7(1+t^4)=t^8)\\ &= t^4+t^9+(t^8+t^{14})t^2\\ &= t^{14}+t^8\\ &= t^6.\end{aligned}$$

Dan zijn $x_1 = bs/a$ en $x_2 = b(s+1)/a$ de oplossingen voor x. Bijgevolg $x_1 = t^6/t^4 = t^2$ en $x_2 = (1+t^6)/t^4 = t^{13}/t^4 = t^9$.

Examen oefening 105 (2de zit, 1992-1993) *Beschouw $\mathbb{F}_{16}$ gedefinieerd aan de hand van de primitieve veelterm $t^4 + t + 1$.*

Geef de log-tabel van $\mathbb{F}_{16}$ en zoek in $\mathbb{F}_{16}$ al de oplossingen van de vergelijking

$$X^8 + X^4 + t^{10} = 0.$$

Oplossing. Voor de log-tabel, zie Oefening 102 op pagina 136.

Om $X^8 + X^4 + t^{10} = 0$ op te lossen, stel $X^4 = Y$. Dan zoeken we de oplossingen voor $Y^2 + Y + t^{10} = aY^2 + bY + c = 0$ met $a = b = 1$ en met $c = t^{10}$.

Hier zoeken we dus de oplossingen voor $Y^2 + Y + \delta = 0$ met $\delta = t^{10}$.

Er zijn twee oplossingen daar

$$\mathrm{Tr}(\delta) = t^{10} + t^{20} + t^{40} + t^{80} = t^{10} + t^5 + t^{10} + t^5 = 2(t^{10} + t^5) = 0.$$

De oplossingen voor Y zijn, met $k = t^{11}$ (zie Oefening 23),

$$\begin{aligned} s &= k\delta^2 + (k + k^2)\delta^4 + (k + k^2 + k^4)\delta^8 \\ &= t^{11}t^5 + (t^{11} + t^7)t^{10} + (t^{11} + t^7 + t^{14})t^5 \\ &= t + t^3 + t^6t^5 = t^9 + t^{11} = t^{17} = t^2 \end{aligned}$$

en

$$s + 1 = t^2 + 1 = t^8.$$

Dus

$$\begin{array}{lcl} X^4 = t^2 & \vee & X^4 = t^8 \\ & \Updownarrow & \\ X^2 = t & \vee & X^2 = t^4 \\ & \Updownarrow & (t = t^{16}) \\ X = t^8 & \vee & X = t^2. \end{array}$$

Examen oefening 106 (2de zit, 1995-1996) *Het eindig veld $\mathbb{F}_{16}$ wordt bepaald aan de hand van het irreduciebel polynoom, over $\mathbb{F}_2$, $f(t) = t^4 + t + 1$, en zij α een nulpunt van f.*

1. *Bewijs dat de volgende vergelijking in X, 3 oplossingen bezit in $\mathbb{F}_{16}$*

$$\alpha^{14}X^3 + \alpha^4X^2 + \alpha^{10}X + \alpha^5 = 0.$$

2. *Ontbind $\alpha^{14}X^3 + \alpha^4X^2 + \alpha^{10}X + \alpha^5$ in lineaire factoren.*

Oplossing. Voor de Log-tabel, zie Oefening 102 op pagina 136. Een eerste oplossing is $X = \alpha$ want, door gebruik te maken van $\alpha^{15} = 1$, substitutie in de vergelijking geeft $\alpha^{17} + \alpha^6 + \alpha^{11} + \alpha^5 = \alpha^2 + \alpha^6 + \alpha^{11} + \alpha^5 = \alpha^3 + \alpha^3 = 0$. De deling van $\alpha^{14}X^3 + \alpha^4X^2 + \alpha^{10}X + \alpha^5$ door $X - \alpha = X + \alpha$ geeft als quotiënt $\alpha^{14}X^2 + \alpha X + \alpha^4$. Om deze kwadratische vergelijking op te lossen, passen we de standaard methode toe. Stel $a = \alpha^{14}, b = \alpha, c = \alpha^4$. Dan is $\delta = ac/b^2 = \alpha$ en $\mathrm{Tr}(\delta) = \mathrm{Tr}(\alpha) = \alpha + \alpha^2 + \alpha^4 + \alpha^8 = \alpha^5 + \alpha^5 = 0$. Daar $\mathrm{Tr}(\delta) = 0$, zijn er twee oplossingen voor de kwadratische vergelijking. Met $k = \alpha^{11}$ zijn de oplossingen voor $Y^2 + Y + \delta = 0$ gelijk aan $s = k\delta^2 + (k + k^2)\delta^4 + (k + k^2 + k^4)\delta^8 = \alpha^{11}\alpha^2 + (\alpha^{11} + \alpha^7)\alpha^4 + (\alpha^{11} + \alpha^7 + \alpha^{14})\alpha^8 = \alpha^{13} + \alpha^8\alpha^4 + \alpha^{21}\alpha^8 = \alpha^{13} + \alpha^{12} + \alpha^{14} = \alpha^{16} + \alpha^{14} = \alpha^{22} = \alpha^7$ en aan $s + 1 = \alpha^9$. De oplossingen voor $\alpha^{14}X^2 + \alpha X + \alpha^4 = 0$ zijn gelijk aan $X_1 = b \cdot s/a = \alpha^7/\alpha^{13} = 1/\alpha^6 = \alpha^9$ en $X_2 = b(s + 1)/a = \alpha^9/\alpha^{13} = \alpha^{11}$. Er zijn dus drie oplossingen $X_1 = \alpha^9, X_2 = \alpha^{11}$ en $X_3 = \alpha$.

De ontbinding in lineaire factoren is dus gelijk aan $\alpha^{14}X^3+\alpha^4X^2+\alpha^{10}X+\alpha^5 = \alpha^{14}(X-\alpha^9)(X-\alpha^{11})(X-\alpha) = \alpha^{14}(X+\alpha^9)(X+\alpha^{11})(X+\alpha)$.

Examen oefening 107 (1ste zit, 1995-1996) *Los over $\mathbb{F}_9$, gedefinieerd door $t^2 + 1$ de volgende vergelijking op:*

$$X^3 + X^2 + (t-1)X - t - 1 = 0$$

Oplossing. Voor de Cayleytabel, zie de collegenota's pagina 131. Het is onmiddellijk duidelijk dat $X = 1$ een oplossing is van de vergelijking. We vinden: $X^3+X^2+(t-1)X-t-1 = (X-1)(X^2-X+t+1)$. De oefening is dus herleid tot het oplossen van de vergelijking $X^2-X+t+1$. De discriminant is $1-4(t-1) = 1-(t-1) = -t$, want we werken over een veld van karakteristiek 3. Bovendien volgt uit de Cayleytabel voor de vermenigvuldiging in $\mathbb{F}_9$ dat $-t = (1+t)^2$, dus de discriminant van de kwadratische vergelijking is $(1+t)^2$.

De oplossingen zijn bijgevolg: $X_1 = \frac{1+1+t}{2} = \frac{t-1}{-1} = 1-t$ en $X_2 = \frac{1-1-t}{2} = \frac{-t}{2} = t$.

Examen oefening 108 (2de zit, 1996-1997) *Beschouw het veld* $\mathbb{F}_{16}$ *bepaald door* $t^4 + t + 1$.

(a) Stel de logtabel op.

(b) Bewijs dat in dit veld, $X = t$ *een oplossing is van de vergelijking*

$$X^3 + t^5X^2 + tX + t^{10} = 0 \ .$$

(c) Ontbind de veelterm $f(X) = X^3 + t^5X^2 + tX + t^{10}$ *in factoren.*

Oplossing.

(a) Deze tabel werd opgesteld in oefening 17 (examenvragen juni 1992-93)

(b) Om te bewijzen dat $X = t$ een oplossing is van de vergelijking, vullen we $X = t$ in in de vergelijking. We krijgen:

$$t^3 + t^7 + t^2 + t^2 = t^3(1 + t^4) + t^2(1 + t^8) = t^4 + t^4 = 0,$$

dus $X = t$ is een oplossing (we maakten gebruik van de logtabel en van het feit dat de karakteristiek 2 is).

(c) Na deling door de factor $(x-t)$ bekomen we de volgende veelterm: $X^2 + t^2X + t^9$. We ontbinden deze veelterm door de oplossingen te zoeken van de vergelijking $X^2 + t^2X + t^9 = 0$. Dit is een kwadratische vergelijking over een veld van karakteristiek 2, met gereduceerde vergelijking: $Y^2 + Y + t^5 = 0$. We zoeken nu $\mathrm{Tr}(\delta) = \mathrm{Tr}(t^5)$. Daar $h = 4$ vinden we:

$$\begin{aligned}
\mathrm{Tr}(t^5) &= t^5 + (t^5)^2 + (t^5)^4 + (t^5)^8 \\
&= t^5(1 + t^5) + t^{20} + t^{40} \\
&= t^5t^{10} + t^5 + t^{10} \\
&= t^{15} + t^5(1 + t^5) \\
&= 2t^{15} \\
&= 0
\end{aligned}$$

We weten dus dat de vergelijking twee oplossingen heeft. We zoeken een element k uit $\mathbb{F}_{16}$, zodanig dat $\mathrm{Tr}(k) = 11$. Het is eenvoudig om

na te gaan dat $\mathrm{Tr}(t^{11}) = 1$. De oplossingen zijn dan gegeven door s en $s+1$, waarbij s als volgt wordt bepaald:

$$\begin{aligned} s &= t^{11}\delta^2 + (t^{11} + t^{22})\delta^4 + (t^{11} + t^{22} + t^{44})\delta^8 \\ &= t^{11}t^{10} + t^8 t^{20} + (t^8 + t^{14})t^{40} \\ &= t^{21} + t^{28} + t^8(1 + t^6)t^{10} \\ &= t^6 + t^{13} + t^8 t^{13} t^{10} \\ &= t^6 + t^{13} + t \\ &= t^6(1 + t^7) + t \\ &= t^{15} + t \\ &= 1 + t \\ &= t^4 \end{aligned}$$

De oplossingen van de gereduceerde vergelijking zijn dus $Y = s = t^4$ en $Y = s+1 = 1+t^4 = t$. De oplossingen van de kwadratische vergelijking in X zijn dan:
$x_1 = t^2 t^4 = t^6$ en $x_2 = t^2 t = t^3$.
Dus $f(X) = X^3 + t^5 X^2 + tX + t^{10} = (X - t)(X - t^6)(X - t^3)$.

Examen oefening 109 (1ste zit, 1997-1998) *(1) Toon aan dat $f(t) = t^2 + t - 1$ gedefinieerd over $\mathbb{Z}_3$ een primitief polynoom is. (0.5 pt)*

(2) Veronderstel dat het veld GF(9) met behulp van dit polynoom wordt gedefinieerd.

(a) Stel de Zech-logtabel op. (1.5 ptn)

(b) Los de vergelijking $t^2X^2 - t^5X + t = 0$ op in dit veld. (2 ptn)

Oplossing. (1) $f(t)$ is irreduciebel over $\mathbb{Z}_3[t]$, want het heeft geen wortels in $\mathbb{Z}_3$: $f(0) = -1$, $f(1) = 1$ en $f(-1) = -1$. Een veelterm van graad 2 is irreduciebel als deze geen wortels heeft.
Is t een primitief element in het veld GF(9)? Een primitief element van $\mathbb{F}_9$ is een element dat precies orde 8 heeft, dus t is primitief in GF(9) als $t^8 = 1$ en $t^k \neq 1$ voor k kleiner dan 8. Met behulp van $t^2 + t - 1 = 0$ vinden we dat

$t^2 = 1 - t$,
$t^3 = -t - 1$,
$t^4 = -1$,
$t^5 = -t$, (*)
$t^6 = t - 1$,
$t^7 = t + 1$ en
$t^8 = 1$,
dus t is inderdaad een primitief element van GF(9).
(2a) Met behulp van $t^2 = 1 - t$ kunnen we de Zech-logtabel opstellen voor $\mathrm{GF}(9) = \{a_0 + a_1 | a_0, a_1 \in \mathbb{Z}_3\}$. In (*) werd reeds de expliciete gedaante van de meeste elementen van GF(9) gegeven, $0 = 0$, $1 = 1$ en $t = t$ maken de lijst compleet. Gebruikmakend van de voorgaande resultaten vinden we de volgende functiewaarden voor de Zech-logfunctie:

i in t^i	i in $1 + t^i$
∞	0
0	4
1	7
2	3
3	5
4	∞
5	2
6	1
7	6

(2b) We lossen nu de vergelijking $t^2X^2 - t^5X + t = 0$ op in GF(9). We berekenen de discriminant: $D = t^{10} - 4t^3 = t^2 - t^3$, want $t^8 = 1$. We vervangen -1 door t^4 en bekomen $D = t^2 + t^4t^3 = t^2 + t^7 = t^2(1 + t^5) = t^2t^2 = t^4 = (t^2)^2$ met behulp van de logtabel. Dus $\sqrt{D} = t^2$.
De twee wortels X_1 en X_2 zijn:
$X_1 = \frac{t^5 + t^2}{2t^2} = \frac{t^2(1+t^3)}{t^4t^2} = \frac{t^2t^5}{t^6} = t$, en
$X_2 = \frac{t^5 - t^2}{2t^2} = \frac{t^5 + t^6}{t^4t^2} = \frac{t^5(1+t)}{t^6} = \frac{t^5t^7}{t^6} = t^6$.

Examen oefening 110 (2de zit, 1997-1998) *Stel de logtabel op voor* $\mathbb{F}_{16} = \{0, \alpha, \alpha^2, \ldots, \alpha^{15} | \alpha^4 + \alpha + 1 = 0\}$*, en los over dit veld de volgende vergelijking op:*

$$X^2 + \alpha^7 X + 1 = 0.$$

Oplossing. Het veld $\mathbb{F}_{16}$ is de verzameling $\{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3||a_0,a_1,a_2,a_3 \in \mathbb{F}_2\}$ waarbij alle bewerkingen in deze verzameling modulo $\alpha^4+\alpha+1$ uitgevoerd worden. Dit betekent dus dat

$$\alpha^4 = \alpha + 1.$$

Dit geeft de volgende tabel voor de elementen van $\mathbb{F}_{16}$. De tweede en vierde kolom geven steeds de ontwikkeling van α^i in functie van $1, \alpha, \alpha^2$ en α^3. Deze tabel wordt inductief opgebouwd. Eénmaal α^i bepaald is, berekent men $\alpha^{i+1} = \alpha \cdot \alpha^i$ en dit modulo $\alpha^4+\alpha+1$. Men vervangt dus steeds α^4 door $\alpha+1$.

0	0	α^7	$1+\alpha+\alpha^3$
α^0	1	α^8	$1+\alpha^2$
α^1	α	α^9	$\alpha+\alpha^3$
α^2	α^2	α^{10}	$1+\alpha+\alpha^2$
α^3	α^3	α^{11}	$\alpha+\alpha^2+\alpha^3$
α^4	$1+\alpha$	α^{12}	$1+\alpha+\alpha^2+\alpha^3$
α^5	$\alpha+\alpha^2$	α^{13}	$1+\alpha^2+\alpha^3$
α^6	$\alpha^2+\alpha^3$	α^{14}	$1+\alpha^3$

De Zech log-functie θ geeft het verband $1+\alpha^i = \alpha^{\theta(i)}$. Aangezien $\alpha^0+1=0$ wordt de notatie $\alpha^\infty = 0$ ingevoerd zodat $\theta(0)$ ook gedefinieerd kan worden. Gebruikmakend van de voorgaande tabel worden de volgende functiewaarden voor de Zech log-functie bekomen.

i	$\theta(i)$	i	$\theta(i)$
∞	0	7	9
0	∞	8	2
1	4	9	7
2	8	10	5
3	14	11	12
4	1	12	11
5	10	13	6
6	13	14	3

Om de vergelijking op te lossen, stellen we eerst de gereduceerde vergelijking op. We zien dat $a=1$, $b=\alpha^7$ en $c=1$. Hiermee vinden we: $Y = \frac{aX}{b} = \frac{X}{\alpha^7} = \frac{\alpha^{15}X}{\alpha^7} = \alpha^8 X$ en
$\delta = \frac{ac}{b} = \frac{1}{\alpha^{14}} = \frac{\alpha^{15}}{\alpha^{14}} = \alpha$.

De gereduceerde vergelijking is $Y^2 + Y + \delta = 0$, dus $Y^2 + Y + \alpha = 0$.
Heeft deze vergelijking oplossingen? Daarvoor moet $\mathrm{Tr}(\delta)$ gelijk zijn aan 0. Daar we werken in $\mathbb{F}_{16}$, is $p = 2$ en $h = 4$, dus $h - 1 = 3$ en $\alpha^{15} = 1$. $\mathrm{Tr}(\delta) = \alpha + \alpha^2 + \alpha^4 + \alpha^8$. Met behulp van de logtabel werken we deze som verder uit:

$$\begin{aligned} \mathrm{Tr}(\delta) &= \alpha + \alpha^2 + \alpha^4 + \alpha^8 \\ &= \alpha(1+\alpha) + \alpha^4(1+\alpha^4) \\ &= \alpha.\alpha^4 + \alpha^4.\alpha = 2\alpha^5 = 0. \end{aligned}$$

De vergelijking heeft dus twee oplossingen. We moeten nu een element van $\mathbb{F}_{16}$ vinden met Trace 1. Dit geldt (bijvoorbeeld) voor het element α^6, want:

$$\begin{aligned} \mathrm{Tr}(\alpha^6) &= \alpha^6 + \alpha^{12} + \alpha^{24} + \alpha^{48} \\ &= \alpha^6(1+\alpha^6) + \alpha^3(1+\alpha^6) \\ &= \alpha^6.\alpha^{13} + \alpha^3.\alpha^1 3 \\ &= \alpha^{19} + \alpha = \alpha^4 + \alpha = 1. \end{aligned}$$

We zoeken nu de oplossingen voor de gereduceerde vergelijking:

$$\begin{aligned} s &= \alpha^6\delta^2 + (\alpha^6 + \alpha^{12})\delta^4 + (\alpha^6 + \alpha^{12} + \alpha^{24})\delta^8 \\ &= \alpha^6\alpha^2 + \alpha^4\alpha^4 + \alpha^4(1+\alpha^5)\alpha^8 \\ &= 2\alpha^8 + \alpha^4\alpha^{10}\alpha^8 = \alpha^{22} = \alpha^7. \end{aligned}$$

De oplossingen van de gereduceerde vergelijking zijn dus $Y_1 = s = \alpha^7$ en $Y_2 = s + 1 = 1 + \alpha^7 = \alpha^9$. De oplossingen van de kwadratische vergelijking in X zijn dan ($X = \frac{bY}{a}$):
$X_1 = \alpha^7\alpha^7 = \alpha^{14}$ en
$X_2 = \alpha^7\alpha^9 = \alpha^{16} = \alpha$.

Examen oefening 111 (1ste zit, 1998-1999) (*a*) *Bewijs dat de veelterm* $f(t) = t^3 - t + 1$ *irreduciebel is over het veld* $\mathbb{F}_3$.

(*b*) *Construeer met behulp van deze veelterm* $f(t)$ *het veld* $\mathbb{F}_{27}$, *bewijs dat* t *primitief element is en stel de Zech-log tabel op.*

(*c*) *Zoek in* $\mathbb{F}_{27}$ *alle oplossingen van de volgende vergelijking in* X*:*

$$(t - t^2)X^2 + (t-1)X - 1 = 0,$$

waarbij t *een primitief element is van* $\mathbb{F}_{27}$.

Oplossing.

(a) Deze veelterm heeft geen wortels in $\mathbb{F}_3$ want $0^3-0+1 \neq 0$ en $1^3-1+1 \neq 0$ en $2^3-2+1 \neq 0$. Bijgevolg is X^3-X+1 irreduciebel is over het veld $\mathbb{F}_3$.

(b) Het veld $\mathbb{F}_{27}$ is de verzameling

$$\{a_0 + a_1 t + a_2 t^2 | a_0, a_1, a_2 \in \mathbb{F}_3\}$$

waarbij alle bewerkingen modulo $t^3 - t + 1$ uitgevoerd worden. Dit betekent dus dat $t^3 = t - 1$. Dit geeft de volgende tabel voor de elementen van $\mathbb{F}_{27}$. De eerste kolom geeft steeds de ontwikkeling van t^i in functie van $1, t$ en t^2. Deze tabel wordt inductief opgebouwd. Eenmaal t^i bepaald is, berekent men $t^{i+1} = tt^i$ en dit modulo $t^3 - t + 1$. Men vervangt dus steeds t^3 door $t - 1$.

0	0
t^0	1
t^1	t
t^2	t^2
t^3	$t-1$
t^4	t^2-t
t^5	$-t^2+t-1$
t^6	t^2+t+1
t^7	t^2-t-1
t^8	$-t^2-1$
t^9	$t+1$
t^{10}	$t+t^2$
t^{11}	t^2+t-1
t^{12}	t^2-1
t^{13}	-1
t^{14}	$-t$
t^{15}	$-t^2$
t^{16}	$-t+1$
t^{17}	$-t^2+t$
t^{18}	t^2-t+1
t^{19}	$-t^2-t-1$
t^{20}	$-t^2+t+1$
t^{21}	t^2+1
t^{22}	$-t-1$
t^{23}	$-t^2-t$
t^{24}	$-t^2-t+1$
t^{25}	$-t^2+1$

Nu is $t^{26}=1$ vandaar dat nu duidelijk is dat t een primitief element is van het veld $\mathbb{F}_{27}$.

De Zech log-functie *theta* geeft het verband $1+t^i=t^{\theta(i)}$.

i	$\theta(i)$	i	$\theta(i)$	i	$\theta(i)$
0	13	9	3	18	7
1	9	10	6	19	23
2	21	11	10	20	5
3	1	12	2	21	12
4	18	13	∞	22	14
5	17	14	16	23	24
6	11	15	25	24	19
7	4	16	22	25	8
8	15	17	20	∞	0

(c) Merk op dat we werken met een veld met oneven karakteristiek. Omdat $-t^2 + t = t^{17}$ en $t - 1 = t^3$ bekomen we dat de discriminant D van de kwadratische vergelijking gelijk is aan $t^6(1 + t^{11})$. Met behulp van de Zeg log-tabel bekomen we dat $D = t^6 t^{10} = t^{16}$. De oplossingen van de kwadratische vergelijking zijn dus

$$X_1 = \frac{1 - t + t^8}{-t^{17}},$$

$$X_2 = \frac{1 - t - t^8}{-t^{17}}.$$

Nu is $t^{-17} = t^{-17}t^{26} = t^9 = t + 1$ en $t^8 = -t^2 - 1$. Bijgevolg is

$$X_1 = (t - 1 + t^2 + 1)(t + 1) = -t^2 - t - 1$$

$$X_2 = (t - 1 - t^2 - 1)(t + 1) = t - 1.$$

Examen oefening 112 (1ste zit, 1999-2000) *Het veld $\mathbb{F}_{16}$ wordt gedefinieerd door de irreduciebele polynoom $f(t) = t^4 + t + 1$. Ontbind het volgend polynoom in de onbepaalde X:*

$$F(X) = X^4 + (t^3 + t^2)X^3 + tX^2 + (t^2 + 1)X + t^3 + t + 1.$$

[Tip: Zoek eerst eenvoudige oplossingen van $F(X) = 0$ om op die manier de graad te verlagen.]

Oplossing. De waarde $X = t$ is een oplossing van de vergelijking $F(X) = 0$ want

$$F(t) = t^4 + (t^3 + t^2)t^3 + tt^2 + (t^2 + 1)t + t^3 + t + 1 = 0.$$

Na deling van $F(X)$ door $(X + t)$ vinden we

$$F(X) = (X+t)(X^3+(t^3+t^2+t)X^2+(t^3+t^2+1)X+t^3+t^2) = (x+t)F_1(X).$$

Opnieuw is de waarde $X = t$ een oplossing van $F_1(X) = 0$ want

$$F_1(t) = t^3 + (t^3 + t^2 + t)t^2 + (t^3 + t^2 + 1)t + t^3 + t^2 = 0.$$

Opnieuw na deling van $F_1(X)$ door $(X + t)$ vinden we

$$F(X) = (X + t)^2(X^2 + (t^3 + t^2)X + t^2 + t) = (X + t)^2F_2(X).$$

Nu is $F_2(X) = (X + t^2)(X + t^3)$ (merkwaardig product). Bijgevolg is

$$F(X) = (X + t)^2(X + t^2)(X + t^3).$$

Merk op dat de ontbinding van $F_2(X)$ ook kan gebeuren via de algemene theorie van kwadratische vergelijkingen van de vorm

$$aX^2 + bX + c = 0.$$

Hier is $a = 1, b = t^2 + t^3, c = t^2 + t$. De kwadratische vergelijking heeft enkel oplossingen als $\mathrm{Tr}(\delta) = \mathrm{Tr}(\frac{ac}{b^2}) = 0$. Nu is

$$\mathrm{Tr}(\frac{ac}{b^2}) = \mathrm{Tr}(\frac{t^5}{t^{12}}) = \mathrm{Tr}(\frac{t^5t^{15}}{t^{12}}) = \mathrm{Tr}(t^8) = t^8 + t + t^2 + t^4 = 0.$$

Beschouw nu een element k van $\mathbb{F}_{16}$ met $\mathrm{Tr}(k) = 1$, bijvoorbeeld $k = t^{11}$, dan levert dit $s = k\delta^2 + (k + k^2)\delta^4 + (k + k^2 + k^4)\delta^8 = t^{12}$. De oplossingen van de kwadratische vergelijking in X zijn dan

$$x_1 = \frac{bs}{a} = t^6t^{12} = t^3 \text{ en } x_2 = \frac{b(s+1)}{a} = t^6t^{11} = t^2.$$