Examen Discrete Wiskunde

Auteur: Daan Pape

1 Hoofdstuk I

Een groepering in de wiskunde is:

- een *verzameling*: als alle elementen verschillend zijn
- een $familie$ of *mulitverzameling*: als er elementen hetzelfde mogen zijn

Twee speciale verzamelingen zijn de *ledige verzameling* ($\emptyset$) en het *universum* of de *universele verzameling*. Voor deze laatste is geen algemene notatie maar vaak wordt deze als Ω genoteerd. Als A, B en C verzamelingen zijn dan gelden volgende eigenschappen:

(1) **Commutatieve eigenschap**

(a) $A \cap B = B \cap A$

(b) $A \cup B = B \cup A$

(2) **Associatieve eigenschap**

(a) $A \cap (B \cap C) = (A \cap B) \cap C$

(b) $A \cup (B \cup C) = (A \cup B) \cap C$

(3) **Distributieve eigenschap**

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(4) **Wetten van De Morgan**

(a) $(A \cup B)^c = A^c \cap B^c$

(b) $(A \cap B)^c = A^c \cup B^c$

Het *cartesisch product* of de *productverzameling* van k verzamelingen wordt gedefinieerd zoals hieronder. De elementen van deze verzamelingen worden *geordende* $k-tallen$ genoemd.

$$A_1 \times A_2 \times ... \times A_k = \{(a_1, a_2, ..., a_k) | a_i \in A_i, i = 1, 2, ..., k\}$$

Een relatie $\mathcal{R}$ tussen twee verzamelingen A en B is een deelverzameling van de *productverzameling* van deze twee verzamelingen. Als $\mathcal{R} \subseteq A \times B$ een relatie is, dan is de *omgekeerde* of *inverse relatie* $\mathcal{R}^{-1}$ de verzameling van de omgekeerde koppels: $\mathcal{R}^{-1} = \{(b, a) | (a, b) \in \mathcal{R}\}$. Koppels gevormd door een relatie kunnen als volgt ingedeeld worden:

- *opeenvolgende koppels*: (a, b) en (b, c)
- *samenstelling* van opeenvolgende koppels: (a, c) als samenstelling van (a, b) en (b, c)

Men kan ook relaties samenstellen wat genoteerd wordt als $\mathcal{R}_2 \circ \mathcal{R}_1$. Hierbij geldt dat dit samenstellen associatief is maar niet commutatief. De omgekeerde van een samengestelde relalatie is het volgende: $(\mathcal{R}_2 \circ \mathcal{R}_1)^{-1} = \mathcal{R}_1^{-1} \circ \mathcal{R}_2^{-1}$. We onderscheiden volgende speciale relaties:

relatie	**vertrekkende pijlen**	**toekomende pijlen**
functie	≤ 1	-
afbeelding	1	-
bijectie	1	1
injectie	≤ 1	≤ 1
surjectie	1	≥ 1

Relaties kan men ook op een andere manier gaan indelen:

- $reflexief$: elk identiek koppel $(x, x) \in \mathcal{R}$
- $antireflexief$: elk identiek koppel $(x, x) \notin \mathcal{R}$
- $niet - reflexief$: noch $reflexief$ noch $antireflexief$
- $symmetrisch$: uit $(x, y) \in \mathcal{R}$ volgt dat $(y, x) \in \mathcal{R}$
- $antisymmetrisch$: als $(x, y) \in \mathcal{R}$ en $(y, x) \in \mathcal{R}$ dan $(x = y)$
- $niet - symmetrisch$: noch $symmetrisch$ noch $antisymmetrisch$
- $reflexief$: als $(x, y) \in \mathcal{R}$ en $(y, z) \in \mathcal{R}$ dan ook $(x, z) \in \mathcal{R}$

Een equivalentierelatie $\mathcal{R} \subseteq A^2$ is een relatie die tegelijkertijd **reflexief**, **symmetrisch** en **transitief** is. Een *equivalentieklasse* van de equivalentierelatie $\mathcal{R}$ is een deelverzameling van alle elementen van A die equivalent zijn met $a \in A$. De equivalentieklasse die het element a bevat wordt als $[a]$ genoteert, a wordt dan een *representant* van deze klasse genoemd.

2 Hoofdstuk II

Hoewel er geen internationale afspraken gemaakt zijn worden in deze cursus volgende notaties gebruikt:

$$\mathbb{N} = \{0, 1, 2, 3, ...\}$$
$$\mathbb{N}^* = \{1, 2, 3, ...\}$$
$$\mathbb{N}[a, b] = \{a, a + 1, ..., b - 1, b\}$$

Een relatie $\mathcal{R}$ wordt een *orderelatie* of *ordening* genoemd als ze **reflexief**, **anti-symmetrisch** en **transitief** is. Indien elke 2 verschillende elementen van een verzameling met elkaar vergeleken kunnen worden door middel van een orderelatie, dan noemt men dit een *totale orderelatie* of *totale ordening*. Een *strikte orderelatie* verkrijgt men als in plaats van $reflexiviteit$ de *anti-reflexiviteit* geldt.
Het is belangrijk om goed onderscheid te maken tussen:

- *benedengrens*: b is een benedengrens voor de verzameling $X \subseteq \mathbb{Z}$ als $b \leq x, \forall x \in X$
- *kleinste element*: b is een kleinste element voor de verzameling $X \subseteq \mathbb{Z}$ als $b \leq x, \forall x \in X$ en $b \in X$

Het **axioma van de goede ordening** zegt dat als X een niet ledige deelverzameling is van $\mathbb{Z}$ d, die een benedengrens heeft, een kleinste element bezit. Dit axioma is zeer belangrijk daar er door dit axioma gebruik kan gemaakt worden van *recurrente betrekkingen* en het *inductieprinciepe*. De bewijzen staan in de cursus. Een bewijs door middel van *inductie* verloopt in 3 stappen:

(1) *inductiebasis*: het resultaat is waar voor een bepaalde waarde van n.

(2) *inductiehypothese*: we veronderstellen dat het klopt voor $n = k$.

(3) *bewijs voor* $k + 1$

Het **ladenprincipe van Dirichlet** stelt dat als men m objecten over n laden wil verdelen waarbij $m > n$ dat er ten minste 1 lade zal zijn die meer dan 1 object bevat. Dit principe stat ook bekend onder het duivenhokprincipe.
Verzamelingen worden als volgt ingedeeld:

- *eindige verzameling*: er is een bijectie met $\mathbb{N}[1, n]$ mogelijk. (bewijs in cursus)
- $aftelbaar\ oneindig$: er is een bijectie met $\mathbb{N}$ mogelijk.
- $overaftelbaar\ oneindig$: er is geen biject met $\mathbb{N}$ mogelijk.

Het **vereenvoudigd somprincipe** luidt als volgt:

Als $A_i (i = 1, ..., k)$ *ktwee aan twee disjuncte, eindige verzamelingen zijn, dan is*

$$|A_1 \cup A_2 \cup ... \cup A_k| = \sum_{i=1}^{k} |A_i|$$

Met behulp van deze stelling wordt het ladenprincipe uitgebreid. Als men m objecten over n laden moet verdelen waarbij $m > nr$, dan is er ten minste één lade die meer dan r objecten bevat.

Het **productprincipe** stelt dat er bij een relate $\mathcal{R}$ er evenveel pijlen vertrekken uit de beginverzameling als dat er toekomen bij de eindverzameling. Dit leidt tot volgende stellingen:

(1) Het principe van de dubbele telling: de orde van S wordt gegeven door:

$$|S| = \sum_{x \in X} r_x(S) = \sum_{y \in Y} k_y(S)$$

(2) Indien $r_x(S)$ een constatne r is, onafhankelijk van de keuze van $x \in Y$, en indien $k_y(S)$ een constante k is, onafhankelijk van de keuze van $y \in Y$, dan is:

$$r|X| = k|Y|$$

(3) Het productprincipe: de orde van $X \times Y$ wordt gegeven door

$$|X \times Y| = |X| \cdot |Y|$$

Het **eenvoudig inclusie-exclusie principe** stelt dat als A en B twee eindig verzamelingen zijn, dan geldt:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

- **variatie**: een geordende keuze van k elementen uit een totaal van n elementen:

$$V_n^k = \frac{n!}{(n-k)!}$$

- **permutatie**: een variatie waarbij $k = n$, alle permutaties worden S_n of $\mathsf{Sym}(n)$:

$$P(n,n) = n!$$

- **combinatie**: een niet gerdende keuze van k elementen uit n elementen waarbij ieder element hoogstens 1 keer gekozen wordt. Deze getallen worden ook *binomiaalgetallen* of *binomiaalcoëfficiënten* genoemd:

$$\binom{n}{k} = C_n^k = C(n,k) = \frac{V_n^k}{k!} = \frac{n!}{(n-k)!k!}$$

Enkele eigenschappen kunnen worden geformuleerd:

(1) Voor alle $n, k \in \mathbb{N}$ met $k \leq n$ geldt: $\binom{n}{k} = \binom{n}{n-k}$

(2) Voor alle $n, k \in \mathbb{N}$ met $k \leq n$ geldt: $\binom{n}{k+1} = \binom{n}{k} \cdot \frac{n-k}{k+1}$

(3) Voor alle $n, k \in \mathbb{N}^*$ met $k < n$ geldt: $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. Dit is de formule van **Stifel-Pascal**.

- **herhalingsvariatie**: een geordende keuze van k elementen uit een totaal van n elementen met herhaling:

$$\overline{V_n^k} = n^k$$

- **herhalingscombinatie**: een niet gerdende keuze van k elementen uit n elementen met herhaling:

$$\overline{\binom{n}{k}} = \overline{C_n^k} = \overline{C(n,k)} = \binom{n+k-1}{k}$$

Er zijn verschillende toepassingen op combinatieleer. In deze samenvatting worden de bewijzen ervan weggelaten. Volgende zijn de toepassingen:

- Een verzameling X van n elementen bezit 2^n deelverzamelingen.

- **Binomium van Newton**: veronderstel dat $n \in \mathbb{N}*$, dna geldt voor elke twee reële getallen a en b dat:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Het veralgemeend inclusie-exclusie principe of **zeefprincipe** is de uitbreiding van het vereenvoudigd model die 2 verzamelingen behandeld. Als $A_1, A_2, ..., A_n$ eindige verzamelingen zijn, dan is

$$|A_1 \cup A_2 \cup ... \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{n-1}\alpha_n$$

waarbij α_i de notatie voor de somv an de kardinaalgetallen van al de mogelijke doorsneden die men kan vormen met i dergelijke verzamelingen A_i:

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{S \subseteq \{1,...,n\}} (-1)^{|S|-1} \left| \bigcap_{j \in S} A_j \right|$$

Permuaties zonder fixelementen: wanorde is een permutatie waarbij alle elementen van plaats veranderd zijn. Volgens het incluse-exclusie principe is het totaal aantal wanordes d_n van $\mathbb{N}[1, n]$ gelijk aan:

$$d_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right) = (n-1)(d_{n-1} + d_{n-2})$$

De Stirling getallen (van de tweede soort). Een Stirling getal $S(n, k)$ is het aantal mogelijkheden waarop men een verzameling X met n elementen kan schrijven als een disjuncte unie van k niet-ledige deelverzamelingen. Het Stirling getal $S(n, k)$ met $1 \leq k \leq n$ wordt recursief gedefinieerd door:

$S(n, 1) = 1$
$S(n, k) = S(n-1, k-1) + kS(n-1, k)(2 \leq k \leq n-1)$
$S(n, n) = 1$

De multinomiaalgetallen: als $n, n_1, n_2, ..., n_k$ positieve natuurlijke getallen zijn waarvoor $\sum_{i=1}^{k} = n$, dan is

$$\binom{n}{n, n_1, n_2, ..., n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}$$

De multinomiaalgetallen zijn een veralgemening van de binomiaalgetallen, er bestaat dus ook een veralgemening vna het binomium van Newton, de minomiaalstelling: voor elke 2 positive natuurlijke getallen n en k geldt dat:

$$\left(\sum_{i=1}^{k} a_i\right)^n = \sum \binom{n}{n_1, n_2, ..., n_k} a_2^{n_1} a_1^{n_2} \cdots a_k^{n_k}$$

Hierbij wordt de som in het rechterlid genomen over al de mogelijke k-tallen van natuurlijke getallen $(n_1, n_2, ..., n_k)$ waarvoor $\sum_{i=1}^{k} n_i = n$.

3 Hoofdstuk III

Een **hashtabel** is een tabel met m genummerde *buckets* of *slots*. Elk daarvan bevat een unieke identifier, de *key*. Als men een nieuw item in de tabel wil opslaan berekent men de $hashfunctie\ h$ van de *key* die als resultaat weergeeft in welke bucket dit item thuishoort. Een goede hashfunctie moet alle data dus gelijkmatig over de *buckets* verdelen. Dit is een belangrijke toepassing van statistiek.

Volgende zijn belangrijke basisbegrippen:

- *uitkomstenruimte*: alle mogelijke uitkomsten van een element
- *gebeurtenis*: deelverzameling van de uitkomstenruimte
- *disjunctiegebeurtenissen*: ze kunnen niet beide voorkomen
- *probabiliteitsgewicht* $P(x)$: een kans voor elk element x van de uitkomstenruimte
- *probabiliteitsfunctie*: de som van de probabiliteitsgewichten van een gebeurtenis
- *probabiliteitsdistributie* of *probabiliteitsmaat*: een probabiliteitsfunctie die voldoet aan:
  - $P(A) \geq 0$ voor elke $A \subseteq S$
  - $P(S) = 1$
  - $P(A \cup B) = P(A) + P(B)$ voor elke twee *disjuncte* gebeurtenissen A en B

Twee gebeurtenissen worden complementair genoemd als hun doorsnede ledig is en als hun unie de uitkomstenruimte vormt.
Uniforme probabiliteitsmaten: P wordt een *uniforme probabiliteitsmaat* of een *uniforme probabiliteitsdistributie* genoemd als elk element van de uitkomstenruimte een gelijk probabiliteitsgewicht heeft. Als dit zo is dan geldt voor elke gebeurtenis $E \subseteq S$ dat:

$$P(E) = \frac{|E|}{|S|}$$

Het inclusie-exclusie principe kan doorgetrokken worden naar pobabiliteiten om de probabiliteit van niet-disjuncte unie's te berekenen. Zij S een uitkomstenruimte met een probabiliteitsmaat P. Dan geldt, voor elk stel gebeurtenissen $E_1, ..., E_n$, dat:

$$P\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{i_1, i_2, ..., i_k \\ 1 \leq i_1 < i_2 < \cdots i_k \leq n}} P(E_{i_1} \cap E_{i_2} \cap \cdots E_{i_k})$$

Een **voorwaardelijke kans** $P(A|B)$ is de kans op gebeurtenis A onder bijkomende voorwaarde dat B zich voordoet. Dit wordt gegeven door:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

De **vermenigvuldigingsregel** is een omvorming van de formule voor voorwaardelijke kans. Zij $A_1, ..., A_n$ gebeurtenissen, dan geldt:

$$P\left(\bigcap_{i=1}^{n} A_i\right) = P(A_1)P(A_2|A_1)P(A_3|A_1 \cap A_2) \cdots P(A_n| \cap_{i=1}^{n-1} A_i)$$

De totalekansformule: veronderstel dat $A_1, ..., A_n$ gebeurtenissen zijn die een partitie vormen voor de uitkomstenruimte S. Dan geldt voor een willekeurige gebeurtenis $B \subseteq S$ dat:

$$P(B) = P(A_1)P(B|A_1) + \cdots + P(A_n)(B|A_n)$$

De **regel van Bayes** legt een verband tussen voorwaardelijke kansen van de vorm $P(A|B)$ en $P(B|A)$. Veronderstel dat $A_1, ..., A_n$ gebeurtenissen zijn die een partitie vormen voor de uitkomstenruimte S. Dan geldt voor een willekeurige gebeurtenis $B \subseteq S$ dat:

$$P(A_i|B) = \frac{P(A_i)P(B|A_i)}{P(B)} = \frac{P(A_i)P(B|A_i)}{P(A_1)P(B|A_1) + \cdots + P(A_n)P(B|A_n)}$$

Deze regel wordt vaak gebruikt voor $inferentie$ of $(inference)$, dit is het statistisch conclusies trekken over een oorzaak van een effect.

Een gebeurtenis A is *stochastisch onafhankelijk* van een gebeurtenis B als $P(A|B) = P(A)$ of nog, als $P(A \cap B) = P(A)P(B)$. Als A en B onafhankelijk zijn, dan zijn ook A en B^c dat ook, evenals A^c en B^c. Dit kan alsvolgt veralgemeend worden voor meerdere gebeurtenissen: $A_1, ..., A_n$ zijn onderling onafhankelijk als

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i) \text{ voor alle } I \subseteq \{1, ..., n\}$$

Dit is sterker dan paarsgewijze onafhankelijkheid van deze gebeurtenissen.

Een **toevalsvariabele (random variable)** X over een uitkomstenverzameling S met probabiliteitsmaat P is een reëel waardige functie van de uitkomsten in S, $X : S \to \mathbb{R}$. Een toevalsveranderlijke X is een **discrete toevalsveranderlijke** als de waardenverzameling $X(S)$ eindig of aftelbaar oneindig is.
Een discrete toevalsveranderlijke X bezit een **kansmassafunctie** p_X, die de kansen weergeeft van de waarden die X kan aannemen:

$$p_X : X(S) \to [0, 1] : x \mapsto P(X = x) := P(\{s \in S | X(s) = x\})$$

Met andere woorden, $p_X(x) = P(X = x)$ is de kans dat de toevalsveranderlijke X de waarde x aanneemt. Zij X een discrete toevalsveranderlijke op een uitkomstenverzameling S, dan geldt:

$$\sum_{x \in X(S)} p_X(x) = 1$$

Meer algemeen geldt dat als $T \subseteq X(S)$ een bepaalde deelverzameling van de waardenverzameling $X(S)$ is, dan geldt:

$$P(X \in T) = \sum_{x \in T} p_X(x)$$

In de cursus staan speciale verdelingen vermeldt op pagina 72-74.

De **verwachtingswaarde** is een getal dat uitdrukt wat de gemiddelde uitkomst zal zijn van een bepaald experiment naarmate het aantal uitvoeringen van het experiment toeneemt.De *verwachtingswaarde* of *verwachting* (expected value) van een discrete toevalsveranderlijke X met kansmassafunctie p_X is gedefinieerd als:

$$E[X] = \sum_{x \in X(S)} p_X(x)x$$

Als X een binomiaal verdeelde toevalsveranderlijke is met parameters n en p, dan is de verwachtingswaarde: $E[X] = np$.

Uit een discrete toevalsveranderlijke X kan een andere discrete toevalsveranderlijke gegenereerd worden door middel van een functie. Stel bv. $Y = g(X)$ voor een zekere functie $g : \mathbb{R} \to \mathbb{R}$. Y is nu opnieuw een discrete toevalsveranderlijke, en de kansmassafunctie van Y is gegeven door:

$$p_Y(y) = \sum_{x \in X(S) | g(x) = y} P_X(x)$$

De **verwachtingswaarderegel voor functies van een discrete toevalsveranderlijke**. Zij X een discrete toevalsveranderlijke met waardengebied W en kansmassafunctie p_X, en zij $g(X)$ een functie van X. De verwachtingswaarde van de toevalsveranderlijke $g(X)$ is dan gelijk aan:

$$E[g(X)] = \sum_{x \in W} p_X(x) g(x)$$

Het **moment van de k-de orde** of het **k-de moment** $\mu_k(X)$ van een toevalsveranderlijke X is de verwachtingswaarde van de toevalsveranderlijke X^k:

$$\mu_k(X) = E[X^k]$$

De verwachtingswaarde is dus het moment van de eerste orde. een toevalsveranderlijke X heeft ook een **variantie** $(var(X))$:

$$var(X) = E[(X - E[X])^2]$$

De **standaardafwijking** σ_X wordt gedefinieerd als de vierkantswortel van de variantie van X. De variantie is een maat voor de spreiding van X ten opzichte van de verwachtingswaarde van X. De standaardafwijking drukt het zelfde uit, maar is eenvoudiger te interpreteren omdat hij in dezelfde eenheden als X wordt uitgedrukt. Er geldt:

$$var(X) = E[X^2] - E[X]^2$$

4 Hoofdstuk IV

Als de afspraak maken dat $\binom{n}{k}$ voor $k > n$ gelijk is aan nul, dan kan het binomium als volgt herschreven worden:

$$(1 + x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k$$

In het rechterlid staat nu een oneindige veelterm in x welke een **machtreeks in de onbepaalde variabele x** wordt genoemd. x wordt hierbij als symbool geïnterpreteerd en niet als getal, er wordt dan ook niet naar de convergentie van de reeks gekeken. Daarom wordt een reeks:

$$\sum_{k=0}^{\infty} a_k x^k$$

een **formele machtreeks** genoemd. De coëfficiënten $a_k (k \in \mathbb{N})$ behoren tot een bepaalde getallenverzameling, meestal tot $\mathbb{Z}$ of een deelverzameling van $\mathbb{Z}$. Op deze manier zal bij elke rij $(a_k)_{k \in \mathbb{N}}$ een formele machtreeks behoren. Omgekeerd bepalen de coëfficiënten van een formele machtreeks een rij getallen $(a_k)_{k \in \mathbb{N}}$. Elke veelterm $p(x) = \sum_{k=0}^{n} a_k x^k$ kan dus als formele machtreeks geschreven worden, mits de afspraak dat $a_m = 0$ voor $m > n$. Een

Het verschil tussen een *formele machtreeks* en een *veeltermfunctie* is dat de functie door haar waarden wordt vastgelegd en een formele machtreeks door een rij getallen. De som en het product worden zoals verwacht gedefinieerd en ook distributiviteitseigenschappen gelden voor de optelling en vermenigvuldiging. Op deze manier vormt een formele machtreeks een ring.

Een formele machtreeks heeft veel inverteerbare elementen. Als $f(x) = \sum_{k=0}^{\infty} a_k x^k$ en $g(x) = \sum_{k=0}^{\infty} b_k x^k$ twee formele machtreeksen zijn met $b_0 \neq 0$, dan bestaat er een unieke formele machtreeks $h(x) = \sum_{k=0}^{\infty} c_k x^k$ zodat $f(x) = g(x) \cdot h(x)$. We noteren $h(x) = \frac{f(x)}{g(x)}$ en noemen $h(x)$ het quotiënt van $f(x)$ en $g(x)$. Meer bepaald is

$$h(x) = \frac{1}{b_0} \sum_{k=0}^{\infty} c_k x^k,$$

waarbij de coëfficiënten c_k recursief gedefinieerd worden als $c_0 = a_0$ en

$$c_k = a_k - \frac{1}{b_0} \sum_{i=1}^{k} b_i c_{k-i} \quad \textit{voor alle } k \geq 1.$$

Indien $g(x) = \sum_{k=0}^{\infty} a_k x^k$, dan wordt de formele machtreeks $\sum_{k=0}^{\infty} a_k x^k$ de *ontwikkeling* van $g(x)$ genoemd.

Veronderstel dat een rij $(a_k)_{k\in\mathbb{N}}$ gegeven wordt. Elke uitdrukking $g(x)$ waarvan de ontwikkeling gelijk is aan de formele machtreeks $\sum_{k=0}^{\infty}$, behorend bij de rij $(a_k)_{k\in\mathbb{N}}$, wordt een *(gewone) voortbrengende functie* (ook al is het niet altijd functie) genoemd.
Voortbrengende functies worden in de praktijk gebruikt om *telproblemen* op te lossen:

- Dit zijn combinatorische problemen met uitkomstenverzameling $\mathbb{N} = \{0, 1, 2, 3, ...\}$ (waarbij toegelaten wordt dat bepaalde uitkomsten niet kunnen voorkomen), en men geïnteresseerd is in het *aantal* keer dat een uitkomst voorkomt.
- De *voortbrengende functie van een telprobleem* is de voortbrengende functie van de rij $(a_0, a_1, a_2, ...)$, waarbij elke a_i gelijk is aan het aantal keer dat uitkomst i voorkomt; het is dus de formele machtreeks $\sum_{k=0}^{\infty} a_k x^k$.
- De *som van twee telproblemen* is het telprobleem dat beide gegeven problemen naast elkaar uitvoert en dat als resultaat de som neemt van deze twee telproblemen.

Volgende stelling toont de kracht van voortbrengende functies aan. Beschouw twee telproblemen, met corresponderende voortbrengende functies gelijk aan $f(x) = \sum_{k=0}^{\infty} a_k x^k$ en $g(x) = \sum_{k=0}^{\infty} b_k x^k$. Dan is de voortbrengende functie van de som van deze twee telproblemen gelijk aan $h(x) = f(x)g(x)$.

$(1+x)^n$ is dus de gewone voortbrengede functie voor de combinaties zonder herhaling van n elementen. De volgende stelling geeft de voortbrengende functie van de combinaties met herhaling. $(1-x)^{-n}$ is de voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ met

$$a_k = \overline{\binom{n}{k}} = \binom{n+k-1}{k}$$

Met andere woorden:

$$\left(\sum_{k=0}^{\infty} x^k\right)^n = \left(\frac{1}{1-x}\right)^n = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k.$$

Het aantal *partities* p_n van een natuurlijk getal $\mathbb{N}$ is het aantal manieren waarop je een getal in kleinere getallen verschillend van 0 kan opdelen. Zij p_n het aantal partities van het getal n. Dan geldt:

$$\begin{aligned}\sum_{k=0}^{\infty} p_k x^k &= \prod_{i=1}^{\infty} \frac{1}{1-x^i} \\ &= (1+x+x^2+\cdots)(1+x^2+x^4+\cdots)(1+x^3+x^6+\cdots)\cdots\end{aligned}$$

Het binomium van Newton leidt dus tot de gewone voortbrengende functie voor de rij van de combinaties (zowel met als zonder herhaling). Echter valt op te merken dat:

$$\begin{aligned}(1+x)^n &= \sum_{k=0}^{\infty} \binom{n}{k} x^k \\ &= \sum_{k=0}^{\infty} \frac{V_n^k}{k!} x^k.\end{aligned}$$

In plaats van nu de formele machtreeksen met coëfficiënten a_k te gebruiken als voortbrengende functie van een rij $(a_k)_{k\in\mathbb{N}}$, kunnen we nu ook de formele machtreeksen met coëfficiënten $a_k/k!$ gebruiken. We spreken in dit geval van de *exponentieel voortbrengende functie*.
Met andere woorden, $g(x)$ is de exponentieel voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ dan en slechts dan als

$$g(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!}.$$

Bijgevolg is $(1+x)^n$ de exponentieel voortbrengende functie van de variaties van n elementen in groepen van k. De exponentieel voortbrengende functie van de rij $(a_k)_{k\in\mathbb{N}}$ gegeven door $a_k = 1$ voor alle $k \in \mathbb{N}$, is:

$$\frac{1}{0!} + \frac{1}{1!}x^1 + \cdots + \frac{1}{k!}x^k + \cdots = \sum_{k=0}^{\infty} \frac{1}{k!} x^k.$$

Dit is een zeer bekende reeks daar, indien het als functie over $\mathbb{R}$ wordt opgevat, het niets anders is dan de reeksontwikkeling van de exponentiële functie e^x. De *formele exponentiële functie* e^x wordt op volgende manier gedefinieerd:

$$e^x = \sum_{k=0}^{\infty} \frac{1}{k!} x^k.$$

Deze exponentieel voortbrengende functies bewijzen hun nut bij het beschouwen van de som van telproblemen, met name bij het samenvoegen van *geordende telproblemen*:

1. Een geordend telprobleem is een combinatorisch probleem met als uitkomstenverzameling geordende rijen, waarbij men geïnteresseerd is in het aantal geordende rijen ven elke lengte i.

2. De *exponentieel voortbrengende functie van een geordend telprobleem* is de exponentieel voortbrengende functie van de rij $(a_0, a_1, a_2, \ldots)$, waarbij elke a_i gelijk is aan het aantal geordende rijen van lengte i; het is dus de formele machtreeks $\sum_{k=0}^{\infty} a_k \frac{x^k}{k!}$.

3. het *samenvoegen van twee geordende telproblemen* is het geordend telprobleem waarbij we beide gegeven problemen naast elkaar uitvoeren, en vervolgens ïn elkaar schuivenöp een willekeurige manier, d.w.z. dat de nieuwe rijen ontstaan door de rijen van beide problemen samen te voegen, zonder echter de onderlinge volgorde van de elementen van elk van de rijen te wijzigen.

Vogende stelling is van gelijkaardige rol als de vorige. Beschouw twee geordende telproblemen, met corresponderende exponentieel voortbrengende functies gelijk aan

$$f(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!} \quad en \quad g(x) = \sum_{k=0}^{\infty} b_k \frac{x^k}{k!}$$

Dan is de exponentieel voortbrengende functie van het samenvoegen van deze twee telproblemen gelijk aan $h(x) = f(x)g(x)$.

5 Hoofdstuk V

Een rij $(a_n)_{n\in\mathbb{N}}$ wordt vaak op een *recursieve manier* gedefinieerd, m.a.w. door het opgeven van enkele spcifieke waarden van $a_i (i = 0, \ldots, k-1)$ voor een zekere k en een vormingswet

$$a_n = f(a_{n-1}, a_{n-2}, \ldots, a_{n-k}), \quad n \geq k.$$

welke een *recurrente betrekking* voor de rij $(a_n)_{n\in\mathbb{N}}$ wordt genoemd. Elke functie $g(n)$ zodanig dat de rij $a_n = g(n)$ voldoet aan bovenstaande vormingswet wordt een *oplossing* van de betrekking genoemd. Elke oplossing zal nog afhangen van de termen $a_0, a_1, \ldots, a_{k-1}$, die we de *vrijheidsgraden* van de recurrente betrekking noemen. Indien we geen specifieke waarden aan deze vrijheidsgraden geven dan spreken we over een *algemene oplossing*, als daartegenover aan alle vrijheidsgraden een specifieke waarde wordt toegekend spreken we van een *particuliere oplossing*.

Er is geen algemene oplosmethode, we zullen ons beperken tot de zogenaamde lineaire recurrente betrekkingen met constante coëfficiënten. Een *lineaire betrekking van de orde k met constante coëfficiënten* is een recurrente betrekking van de vorm

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \ldots + \lambda_k a_{n-k} + f(n), \quad n \geq k,$$

met $\lambda_1, \ldots, \lambda_k$ constanten. We veronderstellen bovendien dat $\lambda_k \neq 0$. Deze recurrente betrekking bezit k vrijheidsgraden $a_0, a_1, \ldots, a_{k-1}$. De recurrente betrekking wordt *homogeen* genoemd als $f(n) = 0$ voor alle $n \geq k$.

Een stelling zegt dat indien $g_i(n) (i = 1, 2, \ldots, m)$ oplossing zijn van

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + f(n), \quad n \geq k,$$

dan is elke lineaire combinatie $\sum_{i=1}^{m} \alpha_i g_i(n) (\alpha_i \in \mathbb{R})$ van deze oplossingen een oplossing van de recurrente betrekking

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + \sum_{i=1}^{m} \alpha_i f_i(n), \quad n \geq k.$$

In het bijzonder is elke lineaire combinatie van oplossingen van een homogene recurrente betrekking terug een oplossing van deze betrekking.

Voor lineaire homogene recurrente betrekkingen bestaat er een vaste techniek om ze op te lossen. Op te merken is dat $a_n = r^n$ een oplossing is van de recurrente betrekking:

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k}, \quad n \geq k,$$

dan en slechts dan als

$$r^n = \lambda_1 r^{n-1} + \lambda_2 r^{n-2} + \cdots + \lambda_k r^{n-k}, \quad n \geq k,$$

met andere woorden dan en slechts dan als ofwel $r = 0$ (maar dit leidt tot de triviale oplossing) ofwel r oplossing is van

$$x^k - \lambda_1 x^{k-1} - \lambda_2 x^{k-2} - \cdots - \lambda_{k-1} x - \lambda_k = 0.$$

Bijgevolg is de rij $(a_n)_{n\in\mathbb{N}}$ met $a_n = r^n$ een oplossing van de eerste recurrente betrekking dan en slechts dan als r een oplossing is van de laatste vergelijking welke de *karakteristieke vergelijking* van de eerste recurrente betrekking wordt genoemd. De oplossingen worden de *karakteristieke oplossingen* genoemd van de eerste recurrente betrekking genoemd. Deze *karakteristieke oplossingen* worden gebruikt om een expliciete formule voor de oplossingen van de recurrente betrekking op te stellen. Voor iedere soort lineaire betrekking is dit anders:

Homogene lineaire recurrente betrekkingen van de eerste orde

De oplossing van een recurrente betrekking van volgende vorm wordt gezocht:

$$a_n = ca_{n-1}, \quad \geq 1.$$

De karakteristieke vergelijking is dus $(x - c) = 0$. Bijgevolg is de algemene oplossing van de vorm $a_n = \alpha c^n$. Merk op dat $a_0 = \alpha c^0 = \alpha$ zodat de rij volledig bepaald is indien de waarde van a_0 gekend is. De algemene oplossing is dus gelijk aan $a_n = c^n a_0$. Een rij $(a_n)_{n\in\mathbb{N}}$ met $a_n = c^n a_0$ wordt een *meetkundige rij met reden c* genoemd.

5.0.1 Homogene lineaire recurrente betrekkingen van de tweede orde

De karakteristieke vergelijking die hoort bij een homogene lineaire betrekking van de tweede orde $a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2}, \quad n \geq 2$, is

$$x^2 - \lambda_1 x - \lambda_2 = 0$$

Waarmee het oplossen wordt herleid tot het oplossen van een kwadratische vergelijking. Veronderstel eerst dat er twee verschillende (eventueel complexe) oplossingen r_1, r_2 zijn. Dan zijn zowel $a_n = r_1^n$ als $a_n = r_2^n$ oplossingen en er volgt uit voorgaande stelling dat

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

een oplossing is van de recurrente betrekking voor elke mogelijke waarde van α_1 en α_2. Elke oplossing van de recurrente betrekking is echte van deze vorm, verzonderstel namelijk dat de beginvoorwaarden $a_0 = k_0$ en $a_1 = k_1$ gegeven zijn en beschouw het stelsel:

$$\begin{cases} k_0 = \alpha_1 + \alpha_2 \\ k_1 = \alpha_1 r_1 + \alpha_2 r_2 \end{cases}$$

De determinant van dit stelsel is $r_2 - r_1 \neq 0$ waardoor er juist één oplossing α_1 en α_2 kan gevonden worden. Voor deze waarden van α_1 en α_2 geeft $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ de unieke

particuliere oplossing van de recurrente betrekking die aan de gegeven beginvoorwaarden voldoet. De *algemene* oplossing van de recurrente betrekking wordt dus gegeven door $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$.

Veronderstellen we echter dat $x^2 - \lambda_1 x - \lambda_2 = 0$ een unieke oplossing heeft, dus als de discriminant van $x^2 - \lambda_1 x - \lambda_2 = 0$ gelijk is aan nul. Dan is voorgaande vergelijking gelijkwaardig met:

$$\left(x - \frac{\lambda_1}{2}\right)^2 = 0$$

zodat de unieke oplossing $r = \frac{\lambda_1}{2}$ wordt. ($r \neq 0$ omdat anders $c_1 = c_2 = 0$). Bijgevolg is $a_n = \left(\frac{\lambda_1}{2}\right)^2$ een oplossing van de recurrente betrekking. In dit geval is echter $a_n = nr^n = n\left(\frac{\lambda_1}{2}\right)^2$ eveneens oplossing van de recurrente betrekking. Uit voorgaande stelling volgt nu opnieuw dat

$$a_n = (\alpha_1 + \alpha_2 n) r^n$$

een oplossing is van de recurrente betrekking, voor elke mogelijke waarde van α_1 en α_2. Ook hier beweren we dat elke oplossing van de recurrente betrekking van deze vorm is door de beginwaarden $a_0 = k_0$ en $a_1 = k_1$ te veronderstellen en het volgend stelsel te beschouwen:

$$\begin{cases} k_0 = \alpha_1 \\ k_1 = (\alpha_1 + \alpha_2) r \end{cases}$$

Dit stelsel heeft een unieke oplossing (α_1, α_2). Voor deze waarden van α_1 en α_2 geeft $a_n = (\alpha_1 + \alpha_2 n) r^n$ de unieke perticuliere oplossing van de recurrente betrekking die aan de gegeven beginvoorwaarden voldoet. We besluiten dat de *algemene oplossing* van de recurrente betrekking gegeven wordt door $a_n = (\alpha_1 + \alpha_2 n) r^n$

Homogene lineaire recurrente betrekkingen van een hogere orde

De techniek gebruikt voor recurrente betrekkingen van de eerste en tweede orde kan zomaar tot hogere ordes worden uitgebreid. Dit wordt in volgende stelling gezegt: Als de wortels $r_1, r_2, \ldots, r_k$ van de karakteristieke vergelijking behorend bij de recurrente betrekking

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k}$$

allemaal verschillend zijn, dan is de algemene oplossing

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$$

met $\alpha_1, \ldots, \alpha_k$ willekeurige getallen. Als r een wortel is met de karakteristieke vergelijking met multipliciteit m, dan is

$$(\alpha_0 + \alpha_1 n + \alpha_2 n^2 + \cdots + \alpha_{m-1} n^{m-1}) r^n$$

een oplossing van de recurrente betrekking, voor willekeurige waarden van $\alpha_0, \ldots, \alpha_{m-1}$.

Niet-homogene lineaire recurrente betrekkingen met constante coëfficiënten

We zullen enkel de oplossingsmethode voor eenvoudige gevallen van niet-homogene lineaire betrekkingen met constante coëfficiënten

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + f(n), \quad n \geq k,$$

waarbij $f \neq 0$ (dit betekent: er bestaat een $n \geq k$ waarvoor $f(n) \neq 0$) bespreken. Zoals bij de homogene betrekkingen is de algemene oplossing van dergelijke vergelijking van de orde k afhankelijk van de k vrijheidsgraden $a_0, a_1, \ldots, a_{k-1}$. Elke particuliere oplossing wordt gegeven door specifieke waarden toe te kennen aan deze vrijheidsgraden. Veronderstel dat we een particuliere oplossing $a_n^{(p)}$ kennen die correspondeert met de waarden $a_0^{(p)}, a_1^{(p)}, \ldots, a_{k-1}^{(p)}$ van de vrijheidsgraden, zodat dus

$$a_n^{(p)} = \lambda_1 a_{n-1}^{(p)} + \lambda_2 a_{n-2}^{(p)} + \cdots + \lambda_k a_{n-k}^{(p)} + f(n)$$

Beschouw anderzijds de corresponderende *homogene* lineaire recurrente betrekking

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k}$$

en veronderstel dat we de algemene oplossing $a_n^{(h)}$ van deze homogene betrekking gevonden hebben. Dan volgt uit voorgaande stelling dat de algemene oplossing van de recurrente betrekking gegeven wordt door:

$$a_n = a_n^{(h)} + a_n^{(p)}$$

De algemene oplossing van een niet-homogene lineaire recurrente betrekking met constante coëfficiënten is bijgevolg de som van een particuliere oplossing van deze vergelijking en de algemene oplossing van de bijbehorende lineaire betrekking.

Een algemene oplossingsmethode om een particuliere oplossing te vinden is moeilijk aan te geven. In volgende stelling wordt uitgelegt dat er soms wel een methode te vinden is: Veronderstel dat de volgende lineaire recurrente betrekking met constante coëfficiënten gegeven is:

$$a_n = \lambda_1 a_{n-1} + \lambda_2 a_{n-2} + \cdots + \lambda_k a_{n-k} + f(n)$$

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

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

Hierbij is $t (0 \leq t \leq k)$ de multipliciteit 1 als oplossing van de karakteristieke vergelijking van de bijbehorende homogene recurrente betrekking. De coëfficiënten $\alpha_0, \alpha_1, \ldots, \alpha_l$ worden bepaald door substitutie in de recurrente betrekking.

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

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

een particuliere oplossing. Hierbij is $t (0 \leq t \leq k)$ de multipliciteit van q in de karakteristieke vergelijking van de bijhorende homogene betrekking. De waarde van α kan bepaald worden door substitutie van de particuliere oplossing in de recurrente betrekking.

In de cursus staan twee sorteer algoritmen uitgelegd, *bubble-sort* en *merge-sort*. Lees dat eens door.

6 Hoofdstuk VI

Als de relatie $\mathcal{D} \subseteq (\mathbb{Z} \setminus \{0\}) \times \mathbb{Z}$ gedefinieerd door

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

wordt beschouwd. Dan noemen we $\mathcal{D}$ de *deelbaarheidsrelatie*. Naast de gebuikelijke termen wordt ook gezegt dat *a een factor is van b*. Dit wordt genoteerd als $a|b$. Daar elk getal $b \neq 0$ deelbaar is door $1, -1, b$ en $-b$, worden deze soms de *onechte* delers van het getal genoemd. Als geldt dat $a|b$ en $a|c$ dan geldt voor alle gehele getallen x en y dat $a|(bx + cy)$. In het bijzonder is a dan een deler van $b + c$ en van $b - c$.

Een stelling zegt dat voor elke 2 getallen $a \in \mathbb{N}^*$ en $b \in \mathbb{Z}$ er unieke gehele getallen q (quotiënt) en r (rest) bestaan zodanig dat

$$b = a \cdot q + r \quad r \in \mathbb{N}[0, a-1].$$

Een belangrijk gevolg van deze stelling i,s dat voor elk gegeven natuurlijk getal $t \geq 2$, een willekeurig positief geheel getal geschreven kan worden als een lineaire combinatie van machten van t waarbij de coëfficiënten tot de verzameling $\mathbb{N}[0, t-1]$ behoren. Indien we immers de voorgaande stelling meerdere keren toepassen, dan verkrijgen we:

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

Elke rest r_i zal hierbij tot $\mathbb{N}[0, t-1]$ behoren en de deling zal stoppen van zodra $q_n = 0$. Als de quotiënten q_i geëlimineerd worden dan verkrijgen we:

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

Dit wordt verkort opgeschreven als $x = (r_n r_{n-1} \ldots r_0)_t$ en wordt de *ontwikkeling van x in basis t* genoemd.

Elk getal dat geen *priemgetal* is kan geschreven worden als een product $m_1 m_2$ met $m_i \in \mathbb{N}[2, m-1]$ (m_1 kan gelijk zijn aan m_2), daarom wordt het een *samengesteld getal* genoemd. Euclides heeft bewezen dat er oneindig veel priemgetallen bestaan. Als gevolg van het axioma van de goede ordening kan bewezen wordt dat elk getal $n \in \mathbb{N} \setminus \{0, 1\}$ te schrijven is als een product van priemfactoren. Men kan verder bewijzen dat deze ontbinding uniek is.

Belangrijk is om volgende begrippen goed uit elkaar te houden:

- Grootste gemene deler: het grootste getal $m \in \mathbb{N}$ waarvoor geldt $m|a$ en $m|b$.
- Kleinste gemeen veelvoud: het kleinste getal $m \in \mathbb{N}$ waarvoor geldt $m = ax$ en $m = bx$ met $x \in \mathbb{N}$.

Getallen met $\gcd(a, b) = 1$ noemen we *onderling ondeelbaar*. Men kan ook zeggen dat $\gcd(a, b) = 1$ betekent dat a en b geen priemfactoren gemeen hebben waardoor ze *relatief priem* of *compriem* genoemd worden.

De stelling van Bézout zegt dat als a en b gehele getallen zijn (niet beide nul), en als $d = \gcd(a, b)$ er dan gehele getallen m en n bestaan zodat $am + bn = d$. Met deze stelling kunnen een heel pak afgeleide stellingen bewezen worden:

(1) Als voor drie gehele getallen a, b en c geldt dat $c|ab$ en dat $\gcd(b, c) = 1$, dan is $c|a$.

(2) Als a, b en c natuurlijke getallen zijn, en ab en ac niet beide nul zijn, dan is $\gcd(ab, ac) = a \gcd(b, c)$.

(3) Als a, b, c getallen zijn (a en b niet beide nul), zodanig dat c deelbaar is door a en b, dan is c deelbaar door $\dfrac{ab}{\gcd(a, b)}$.

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

(5) Als a, b en c getallen zijn met hetzij a en b, hetzij a en c, hetzij b en c relatief priem, dan geldt $\gcd(a, c) \cdot \gcd(b, c) = \gcd(ab, c)$. Bijgevolg zijn ab en c relatief priem dan en slechts dan als zowel a en c als b en c relatief priem zijn.

Een andere stelling zegt dat indien p een priemgetal is en indien $x_1, x_2, \ldots, x_n$ gehele getallen zijn zodanig dat

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

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

Het feit dat een priemontbinding uniek is heeft enkele gevolgen:

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

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

  Elke deler d van n is dan van de vorm

  $$d = p_1^{x_1} p_2^{x_2} \ldots p_k^{x_k}, \quad x_i \in \mathbb{N}[0, e_i], i = 1, \ldots, k$$

  Het aantal delers van n is bijgevolg gelijk aan het aantal k-tallen $(x_1, x_2, \ldots, x_k)$ met $x_i \in \mathbb{N}[0, e_i]$ en is bijgevolg gelijk aan $\displaystyle\prod_{i=1}^{k} (e_i + 1)$.

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

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

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

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

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

De *Euler functie* of *Indicator van Euler* is belangrijk. Stel dat n een positief natuurlijk getal is, dan noteren we met $\Phi(n)$ het aantal natuurlijke getallen uit $\mathbb{N}[1, n]$ die compriem zijn met n. Indien $n = p$ een priemgetal is, dan is duidelijk

$$\Phi(p) = p - 1$$

In het algemeen geval is de functie als volgt. Veronderstel dat $n \geq 2$ een natuurlijk getal is met priemfactorontbinding $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Dan is

$$\Phi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

We kunnen de formule ook herschrijven voor de functie $\Phi(n)$ met $n = n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$:

$$\Phi(n) = p_1^{e_1 - 1}(p_1 - 1) p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1) = \prod_{i=1}^{k} \left(p_i^{e_i - 1}(p_i - 1)\right)$$

7 Hoofdstuk 7

Twee gehele getallen x_1 en x_2 zijn *congruent modulo* m dan en slechts dan als $x_1 - x_2$ deelbaar is door m. Dit wordt genoteerd als:

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

Voor vaste m vormt dit een equivalentierelatie die $\mathbb{Z}$ indeelt in partities. De equivalentieklassen worden de *congruentieklassen modulo* m genoemd. Er wordt soms gezegt dat x_1 en x_2 *equivalent zijn modulo* m. Twee gehele getallen zijn congruent modulo m dan en slechts dan als ze de zelfde rest opleveren na deling door m. Met andere woorden x_1 en x_2 zijn congruent modulo m dan en slechts dan als er een geheel getal t bestaat zodanig dat

$$x_1 = x_2 + mt$$

De congruentieklassen modulo m worden daarom ook nog de *restklassen modulo* m genoemd en de klasse met representant r wordt soms genoteerd door $[r]_m$ of kortweg door $[r]$ indien er geen verwarring mogelijk is. De verzameling van de restklassen modulo m (met andere woorden de quotiëntverzameling van $\mathbb{Z}$ met betrekking tot de equivalentierelatie congruent modulo m) wordt genoteerd door $\mathbb{Z}/m$. Indien uit elke restklasse de kleinste natuurlijke representant wordt gekozen, dan ontstaat de verzameling $\mathbb{N}[0, m-1]$. Er bestaat m.a.w. een bijectie tussen de verzamelingen $\mathbb{Z}/m$ en $\mathbb{N}[0, m-1]$.

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

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

Dan gelden volgende eigenschappen:

(1) $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$,

(2) $x_1 y_1 \equiv x_2 y_2 \pmod{m}$.

De optelling en vermenigvuldiging worden in $\mathbb{Z}/m$ anders opgeschreven en gedefinierd:

- $[x]_m \oplus [y]_m = [x + y]_m$
- $[x]_m \otimes [y]_m = [x \cdot y]_m$

Er wordt hier dus met restklasen modulo m gewerkt en het maakt niet uit welke representant men uit deze klasse neemt om de bewerkingen uit te voeren. De resulterende klasse zal steeds gelijk zijn.
De eigenschappen volgen uit de eigenschappen voor dezelfde bewerkingen van gehele getallen. Voor alle $[a]_m, [b]_m, [c]_m \in \mathbb{Z}/m$ geldt:

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

(A2) $[a]_m \oplus [b]_m = [b]_m \oplus [a]_m$ en $[a]_m \otimes [b]_m = [b]_m \otimes [a]_m$

(A3) $([a]_m \oplus [b]_m) \oplus [c]_m = [a]_m \oplus ([b]_m \oplus [c]_m)$ en
$([a]_m \otimes [b]_m) \otimes [c]_m = [a]_m \otimes ([b]_m \otimes [c]_m)$

(A4) $[a]_m \oplus [0]_m = [a]_m$ en $[a]_m \otimes [1]_m = [a]_m$

(A5) $[a]_m \otimes ([b]_m \oplus [c]_m) = ([a]_m \otimes [b]_m) \oplus ([a]_m \otimes [c]_m)$

(A6) Er bestaat een $-[a]_m = [-a]_m \in \mathbb{Z}/m : [a]_m \oplus (-[a]_m) = [0]_m$

Niet alle eigenschappen kunnen worden overgenomen:

- De schrappingswet geldt niet. Zo is $[3]_6 \otimes [1]_6 = [3]_6 \otimes [5]_6$
- Het kan voorkomen dat $[a]_m \otimes [b]_m = [0]_m$ terwijl $[a]_m \neq [0]_m$ en $[b]_m \neq [0]_m$. Dit is als a en b echte delers zijn van m en m een deler is van $a \cdot b$. Men zegt daarom dat de klassen $[a]_m$ met a een echte deler van m, *nuldelers* zijn in $\mathbb{Z}/m$.

Het element b is het invers element van a in een verzameling met eenheidselement e als geldt dat:

$$b \cdot a = e = a \cdot b$$

In $\mathbb{Z}$ kan dit enkel als $b = \pm 1$. In $\mathbb{Z}/m$ is dit anders. De definitie: Een element $r \in \mathbb{Z}/m$ wordt *inverteerbaar* genoemd als er een element x in $\mathbb{Z}/m$ bestaat, zodanig dat $rx = 1$ in $\mathbb{Z}/m$, m.a.w. indien $rx \equiv 1 \pmod{m}$. We noteren het *invers element* x van r als r^{-1}.

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

Het invers element kan nu gevonden worden met de stelling van Bézout. Stel dat we het inverse element van 5 (mod 18) willen bepalen. Dan schrijven we 1 als lineaire combinatie van 5 en 18 en vinden $1 = 2 \cdot 18 - 7 \cdot 5$; hieruit halen we dat $(-7) \cdot 5 \equiv 1 \pmod{18}$ of dus $11 \cdot 5 \equiv 1 \pmod{18}$.

Eerder werd $\Phi(m)$ gedefinieerd als het aantal gehele getallen r, met $1 \leq r \leq m$, die copriem (er bestaat geen positief geheel getal groter dan 1 dat beide getallen deelt) zijn met m. Het aantal inverteerbare elementen in $\mathbb{Z}/m$ is hier bijgevolg aan gelijk. De volgende stelling, stelling van Euler, is een klassieker en vermeldt dit: Als $\gcd(y, m) = 1$, dan geldt:

$$y^{\Phi(m)} \equiv 1 (\text{mod } m)$$

De verzameling inverteerbare elementen wordt ook als $(\mathbb{Z}/m)^\times$ genoteerd.Deze verzameling is gesloten. Daarmee wordt bedoelt dat het product van twee elementen opnieuw in de verzameling zit en dat het inverse element weer in de verzameling zit. In het bijzonder geval dat $m = p$ een priemgetal is, en dus $\Phi(p) = p - 1$, wordt de stelling van Euler:

$$\text{Als } p \nmid y, \text{dan is } y^{p-1} \equiv 1 \pmod{p}$$

welke beter gekend is als de *kleine stelling van Fermat.*

Een vergelijking van de vorm $ax \equiv b \pmod{m}$ met a en b gegeven gehele getallen en x een onbekende in $\mathbb{Z}/m$ wordt een *lineaire congruentie* genoemd. Het oplossen ervan komt overeen met het zoeken naar een koppel (x, t) met $x \in \mathbb{N}[0, m-1]$ en $t \in \mathbb{Z}$, zodanig dat $ax = b + mt$. Of er al dan niet een oplossing is kan in 2 gevallen worden opgesplitst:

(1) Als $d = \gcd(a, m) \nmid b$, dan bezit $ax \equiv b \pmod{m}$ geen oplossingen.

(2) Als $d = \gcd(a, m) | b$, dan bezit $ax \equiv b \pmod{m}$ juist d oplossingen r waarbij $r \in \mathbb{N}[0, m-1]$.

In de praktijk worden oplossingen voor lineaire congruenties als volgt gevonden. We controleren eerst of $d = gcd(a, m)$ een deler is van b die groter is dan 1. Indien dit het geval is moeten we eerst d wegdelen in de congruentie. Veronderstel dat dit gebeurt is, dan schrijven we de lineaire congruentie $ax = b \pmod{m}$ in de vorm $ax \equiv (b + tm) \pmod{m}$ met $b + tm$ een veelvoud van a. De oplossing van de lineaire congruentie is dan van de vorm $\dfrac{b + tm}{a} \pmod{m}$

Deze techniek kunnen we ook toepassen om *lineaire diophantische vergelijkingen met 2 onbekenden* op te lossen. Dit zijn vergelijkingen $ax + by = c \in \mathbb{Z}$. Een voorbeeld: zoek de oplossingen $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ van $9x + 16y = 35$:

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

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

We lossen één van de congruenties op en substitueren de oplossing dan in de andere lineaire congruentie, bijvoorbeeld:

$$\begin{aligned} & 16y \equiv 35 && \pmod{9} \\ \Leftrightarrow\ & 7y \equiv 35 && \pmod{9} \\ \Leftrightarrow\ & y = 5 && \pmod{9} \\ \Leftrightarrow\ & y = 5 + 9t, && t \in \mathbb{Z} \end{aligned}$$

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

We kunnen ook stelsels van lineaire congruenties beschouwen. Deze zijn van de gedaante:

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

Het zal echter zo zijn dat elke vergelijking van de vorm $x \equiv b_i \pmod{m_i}$ met $b_i \in \mathbb{N}[0, m_i - 1]$ zal kunnen zijn. Daarom worden enkel stelsels van volgende vorm besproken:

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

Deze stelsels worden makkelijk oplosbaar via de Chinese reststelling: Veronderstel dat $m_1, \ldots, m_k$ natuurlijke getallen zijn die twee aan twee onderling ondeelbaar zijn, m.a.w. voor elke $i \neq j$ geldt $\gcd(m_i, m_j)$=1. Zij $M = \prod_{i=1}^{k} m_i = m_1 \cdots m_k$. Beschouw verder voor elke i een $b_i \in \mathbb{N}[0, m_i - 1]$. Dan heeft het stelsel lineaire congruenties

$$x \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, k$$

juist 1 oplossing modulo M.

In de praktijk lossen we een stelsel dus als volgt op. We leggen het uit aan de hand van het voorbeeld:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

We zoeken een oplossing van de vorm

$$x = y_1 \cdot (5 \cdot 7) + y_2 \cdot (3 \cdot 7) + y_3 \cdot (3 \cdot 5)$$

De getallen tussen de haakjes achter y_i zijn de producten van al de moduli uitgezonderd de modulus m_i uit de i-de congruentie. Indien we nu deze gedaante van x invullen in de achtereenvolgende congruenties, dan ontstaat een stelsel van congruenties in y_i, namelijk:

$$\begin{cases} 35y_1 \equiv 1 \pmod 3 \\ 21y_2 \equiv 2 \pmod 5 \\ 15y_3 \equiv 3 \pmod 7 \end{cases}$$

Deze drie congruenties kunnen nu elk afzonderlijk worden opgelost, hier vinden we:

$$\begin{cases} y_1 \equiv 2 \pmod 3 \\ y_2 \equiv 2 \pmod 5 \\ y_3 \equiv 3 \pmod 7 \end{cases}$$

Als we nu deze waarden in $x = y_1 \cdot (5 \cdot 7) + y_2 \cdot (3 \cdot 7) + y_3 \cdot (3 \cdot 5)$ substitueren bekomen we $x = 157$ hetgeen dan modulo $105 = (3 \cdot 5 \cdot 7)$ congruent is met 52.

De orde van een element modulo m is het volgende: veronderstel dat $a \in \mathbb{Z} \setminus \{0\}, m \in \mathbb{N} \setminus \{0\}$ en dat $\gcd(a, m) = 1$. De verzameling $\{s \in \mathbb{N} | a^s \equiv 1 (\text{mod } m)\}$ is niet ledig, want wegens de stelling van Euler is

$$a^{\Phi(m)} \equiv 1 \pmod{m}$$

Bijgevolg bestaat er een kleinste element t in deze verzameling waarvoor dus geldt dat $a^t \equiv 1 \pmod{m}$. We noemen dit natuurlijk getal t de orde van a modulo m en noteren het als $t = o_m(a)$. Merk op dat 1 dus altijd de orde 1 heeft.

Volgende stelling is belangrijk: veronderstel dat $\gcd(a, m) = 1$ en stel dat $t = o_m(a)$. Voor alle $r, s \in \mathbb{Z}$ geldt:

(i) $a^s \equiv 1 \pmod{m}$ als en slechts als $t | s$

(ii) $t | \Phi(m)$

(iii) $a^r \equiv a^s (\text{mod } m)$ als en slechts als $r \equiv s (\text{mod } t)$

8 Hoofdstuk 8

Een *binaire bewerking* op een verzameling V is een afbeelding van de gedaante

$$f : V \times V \to V : (a, b) \mapsto f(a, b)$$

en wordt steeds als gesloten beschouwd. Vaak wordt foor $f(a, b)$ de additieve $(a + b)$ of mulitplicatieve (ab) notatie gebruikt ook al komen nog veel andere bewerkingen in aanmerking.

Een groep is een koppel (G, f), waarbij G een verzameling is en f een binaire bewerking die aan drie bijkomende voorwaarden voldoet. Vaak wordt het ook als $(G, \cdot)$ of $(G, +)$ of zelfs (als er geen verwarring mogelijk is) als G genoteerd. Volgende zijn de 3 voorwaarden eer dat een koppel een groep is:

1. Voor alle $a, b, c \in G$ geldt $a(bc) = (ab)c$ (associatieve wet).
2. Er bestaat een $e \in G$ zodat voor alle $a \in G$ geldt dat $ae = ea = a$ (identiteitswet).
3. Voor alle $a \in G$ bestaat er een element $a^{-}1 \in G$ zodat $aa^{-1} = a^{-1}a = e$ (inversieve wet).

Het element e noemt men het *neutraal element*, dit wordt vaak als 0 genoteerd bij additive notatie en als 1 bij mulitplicatieve notatie. Het element a^{-1} noemt men het invers element van a en wordt bij additive nodatie als $-a$ genoteerd (welke dan ook wel tegengesteld element wordt genoemd). Als de groep ook de commutativiteitseigenschap bezit zegt men dat deze *commutatief* of *abels* is. De *orde* van een groep is het aantal elementen van de onderliggende verzameling.
Als gevolg van de gegeven axioma's voor een groep kunnen enkele eigenschappen aangetoont worden:

1. De vergelijking $xa = b$ met onbekende x heeft juist één oplossing voor elke a en b, namelijk $x = ba^{-1}$.
2. De linkse en rechtse schrappingswetten gelden, d.w.z. uit $ac = ad$ volgt $c = d$.
3. Er is slechts één enkel neutraal element e en elk element $a \in G$ heeft juist één invers element a^{-1}.

Om echter de interactie tussen twee bewerkingen te beschrijven wordt een *ring* gebruikt. Er wordt vanaf een geordend drietal (R, f, g) vertrokken waarbij R een verzameling is en f en g binaire bewerkingen op R zijn. Meestal wordt voor f de additieve notatie $+$ gebruikt en voor g de multiplicatieve notatie. Dit drietal wordt dan een ring genoemd als aan volgende axioma's voldaan is:

1. $(R, +)$ is een abelse groep met neutraal element 0.
2. Voor alle $a, b, c \in R$ geldt $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associatieve wat voor de vermenigvuldiging).
3. Er bestaat een element $e \in R \setminus \{0\}$ zodat voor alle $a \in R$ geldt: $e \cdot a = a \cdot e = a$ (e is het neutraal element voor de vermenigvuldiging).

4. Voor alle $a, b, c \in R$ geldt:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

men zegt dat de vermenigvuldiging distributief is tegenover de optelling.

Het neutraal element van een ring is uniek bepaald en wordt soms voorgesteld door 1. Als $(R, +, \cdot)$ een ring is zodanig dat voor alle $a, b \in R$ geldt dat $a \cdot b = b \cdot a$ dan zegt men dat het een commutatieve ring is. De orde van een ring is de orde van de onderliggende verzameling. Uit de definitie van een ring kan men het gelden van de linkse en/of rechtste schrappingswet niet besluiten. Het is mogelijk dat er in een ring elementen a en b bestaan, beiden verschillend van 0, met een product gelijk aan 0. Dit zijn zogenaamde *nuldelers*.

Een element x van een ring R wordt *inverteerbaar* genoemd dan en slechts dan als x een invers element bezit voor de vermenigvuldiging. Met andere woorden, dan en slechts dan als er een element $u \in R$ bestaat waarvoor

$$u \cdot x = x \cdot u = 1$$

u is, door de definitie van een ring, uniek bepaald en daarom kunnen we het symbool x^{-1} gebruiken. We stellen de deelverzameling van R die de inverteerbare elementen bevat voor door $R^\times$. De verzameling $R^\times$ van de inverteerbare elementen van een ring R vormen een groep voor de (restrictie van de) vermenigvuldiging. Bijgevolg is $(xy)^{-1} = y^{-1}x^{-1}$ het invers element van xy en is de verzameling $R^\times$ dus gesloten.

Een *lichaam* $\mathbb{F}$ is een ring waarvoor $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$. Bijgevolg is $\mathbb{F} \setminus \{0\}$ een groep voor de vermenigvuldiging. Als deze vermenigvuldiging ook commutatief is dan wordt $\mathbb{F}$ een *veld* genoemd. Hierbij valt op te merken dat elk lichaam met een eindig aantal elementen noodzakelijk een veld is. Er bestaan verschillende *eindige* velden en een belangrijke groep zijn de *Galois-velden*. Het aantal elementen q van een eindig veld is van de gedaante $q = p^h$, met p een priemgetal en $h \in \mathbb{N} \setminus \{0\}$. Voor elke $q = p^h$ bestaat er, op isomorfisme na, juist één veld van die orde q. Dit veld wordt als $\mathbb{F}_q$ genoteerd. Als in het bijzonder $h = 1$, dan is $q = p$ een priemgetal en is het veld $\mathbb{F}_p$ niets anders dan het veld $(\mathbb{Z}/p, +, \cdot)$.

Een *veelterm* of *polynoom* over een ring R is elke uitdrukking van de vorm

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$$

x is hierbij de *onbepaalde variabele* en de elementen $a_i, i \in \mathbb{N}[0, n]$ zijn de *coëfficiënten* van de veelterm. Als $a_n \neq 0$ dan noemen we n de *graad* van de veelterm. Omdat x en zijn macht zelf kan worden ingevuld worden veeltermen ook vaak als volgt voorgesteld:

$$(a_0, a_1, a_2, \ldots, a_n)$$

Er bestaat dus een bijectie van de verzameling van de veeltermen met graad hoogstens n over een ring R op de verzameling R^{n+1}. De verzameling van al de veeltermen met coëfficiënten in de ring R wordt voorgesteld door $R[x]$. De veeltermen van de vorm (a_0) worden *constante veeltermen* genoemd en kunnen geïdentificeerd worden met de elementen van R. De *nulveelterm* is per definitie de constante veelterm (0).

Veeltermen worden soms in dalende volgorde van exponenten van x genoteerd:

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

De coëfficiënt van $a_n(\neq 0)$ wordt de *leidende coëfficiënt* genoemd. Indien $a_n = 1$ wordt de veelterm een *monische veelterm* genoemd. In de rijnotatie zullen de coëfficiënten wel steeds in stijgende volgorde van exponenten geschreven worden. De som en het product van veeltermen worden zoals verwacht gedefinieerd.

Volgende stelling bestaat over de deelbaarheid van veeltermen: veronderstel dat $\mathbb{F}$ een veld is en dat $a(x)$ en $b(x)$ veeltermen zijn in $\mathbb{F}[x]$ waarbij $b(x) \neq 0$. Dan bestaan er unieke veeltermen $g(x)$ en $r(x)$ in $\mathbb{F}[x]$ zodanig dat

$$a(x) = b(x)q(x) + r(x)$$

waarbij de graad van $r(x)$ kleiner is dan de graad van $b(x)$ of waarbij $r(x)$ de nulveelterm is.

Het algoritme van Euclides wordt vaak gebruikt om veeltermen te delen. Een veelterm in $\mathbb{F}[x]$, die geen constante veelterm is, kan steeds ontbonden worden in een product van *irreducibele* veeltermen. Een veelterm $f(x)$ in $\mathbb{F}[x]$ wordt irreducibel genoemd dan en slechts dan als $f(x)$ geen constante veelterm is en als $f(x) = g(x)h(x)$ in $\mathbb{F}[x]$ impliceert dat ofwel $g(x)$ ofwel $h(x)$ constante veeltermen zijn.