Hoofdstuk 1: Inleidende begrippen

We frissen enkele basisbegrippen op en we maken notationele afspraken.

1.1 Logica:

De wiskunde is opgebouwd uit logische redeneringen. Deze redeneringen worden in het algemeen bestudeerd in de wiskundige discipline die logica heet. Logica komt uitgebreid aan bod in de cursus Logica en Formele Systemen" (Prof. Dr. De Troyer). Wij zullen de taal en notatie van de zogenaamde predikatenlogica gebruiken om redeneringen neer te schrijven. We herhalen hier enkele notaties en begrippen:

- **Propositie:** een bewering p die ofwel waar, ofwel onwaar is
- **Conjunctie:** $p \wedge q$ ("p en q") en **disjunctie:** $p \vee q$ ("p of q")
- **implicatie:** $p \Rightarrow q$ ("Als p dan q)
  - "x is deelbaar door $10 \Rightarrow x$ is even"
- **equivalentie**: $p \Leftrightarrow q$ ("p is equivalent met q") betekent $(p \Rightarrow q) \wedge (q \Rightarrow p)$
  - n^2 even $\Leftrightarrow$ n even"
- **negatie:** $\neg p$
  - "Het regent niet."

Opmerking.
De negatie van de implicatie is niet hetzelfde als contrapositie!

- **Negatie van de implicatie:** $\neg(p \Rightarrow q)$ is equivalent met $p \wedge \neg q$
- **Contrapositie van de implicatie:** $p \Rightarrow q$ is equivalent met $\neg q \Rightarrow \neg p$

Voorbeeld. Om te bewijzen dat "$n^2\ even \Leftrightarrow n\ even$" is het gemakkelijker te bewijzen dat

$$n\ oneven \Rightarrow n^2 oneven$$

1.2 Verzamelingen

Een fundamenteel begrip in de wiskunde is **verzameling**. Het is echter moeilijk dit begrip precies te definiëren. Verzamelingen laten toe alle (wiskundige) objecten met dezelfde kenmerken te groeperen of te verzamelen.
Voorbeeld. De verzameling priemgetallen groepeert alle positieve gehele getallen die juist twee verschillende delers bezitten.

Een object uit een gegeven verzameling heet een **element**. We noteren verzamelingen meestal met Latijnse hoofdletters: $A, B, C, \dots, X, Y, Z$. Sommige verzamelingen verdienen een speciaal symbool:

- $\mathbb{N} = \{0,1,2, \dots\}$: de natuurlijke getallen
- $\mathbb{Z} = \{\dots, -3, -2, -1,0,1,2, \dots\}$: de gehele getallen
- $\mathbb{Q} = \left\{\frac{a}{b} \middle| a, b \in \mathbb{Z} \wedge b \neq 0\right\}$: de rationale getallen
- $\mathbb{R}$: de reële getallen
- $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$: de complexe getallen

Merk op:
Een verzameling kan gedefinieerd worden door haar elementen op te sommen tussen accolades. We kunnen ook een algemene beschrijving geven van haar elementen zoals in het voorbeeld van $\mathbb{Q}$. Hierbij moet je het verticale streepje "|" lezen als "waarvoor geldt". Het symbool ∈ betekent "is element van" of "behoort tot". Meer voorbeelden:

Als A **eindig** is (d.w.z. A bevat een eindig aantal elementen) noteren we het aantal elementen in A met $|A|$ of $\#A$. De **lege verzameling** $\emptyset$ bevat geen elementen. De uitspraak $\neg(x \in A)$ korten we af tot $x \notin A$, "x behoort niet tot A".

1.3 Kwantoren

Sommige uitspraken of eigenschappen zijn geldig voor alle objecten in een gegeven verzameling. Om dit te noteren gebruiken we de **kwantor** "voor alle": $\forall$

Voorbeeld. $\forall x \in \mathbb{R}: x^2 \geq 0$
Het dubbelpunt ":" betekent in een logische uitspraak "geldt". Er is ook een kwantor "er bestaat" indien men wil zeggen dat een eigenschap geldt voor minstens één element in een gegeven verzameling

Voorbeeld. $\exists x \in \mathbb{R}: x^2 = x$
Soms wil men benadrukken dat er slechts één element bestaat met de gegeven eigenschap.

Voorbeeld. $\exists! x \in \mathbb{R}_0^+: x^2 = x$

1.4 Meerdere kwantoren en negaties

De volgorde van kwantoren heeft belang! Bijvoorbeeld

$$\forall x \in \mathbb{R}: \exists \mathrm{y} \in \mathbb{R}^+: x^2 = y$$

is waar, terwijl

$$\exists \mathrm{y} \in \mathbb{R}^+: \forall x \in \mathbb{R}: \mathrm{x}^2 = y$$

onwaar is.

Negaties van uitspraken zijn zeer belangrijk. Denk bijvoorbeeld aan het bewijs door contrapositie.
De negatie van:

$$\forall x \in X: p(x) \text{ is } : \exists \mathrm{x} \in X: \neg p(x)$$

en de negatie van:

$$\exists \mathrm{x} \in X: p(x) \text{ is } \forall x \in X: \neg p(x)$$

1.5 Deelverzamelingen en gelijke verzamelingen

Indien elk element van een verzameling A ook behoort tot een verzameling B, zeggen we dat A een **deelverzameling** is van B of dat B de verzameling A omvat.

Symbolisch:

$$A \subset B \Leftrightarrow \forall a \in A: a \in B$$

Voor $A \subset B$ schrijven we ook $B \supset A$. We hebben steeds $B \subset B$ en $\emptyset \subset B$. Alle andere deelverzamelingen heten **echte deelverzamelingen** van B.

Twee verzamelingen A en B zijn **gelijk** indien ze dezelfde elementen hebben.
Dit is het geval als en slechts als $(A \subset B) \wedge (B \subset A)$. We noteren (uiteraard) $A = B$.

Gevolg: $A \neq B$ indien $(A \not\subset B) \vee (B \not\subset A)$, d.w.z.$(\exists \mathrm{a} \in \mathrm{A}: \mathrm{a} \notin \mathrm{B}) \vee (\exists \mathrm{b} \in \mathrm{B}: \mathrm{b} \notin \mathrm{A})$

De verzameling van alle deelverzamelingen van een gegeven verzameling X noteren we $P(X)$.
Er geldt dus:

$$P(x) = \{S \text{ verzameling} \mid S \subset X\}$$

1.6 Bewerkingen met verzamelingen

De **doorsnede** van A en B is de verzameling $A \cap B = \{x \in A | x \in B\}$. Twee verzamelingen A en B heten **disjunct** indien $A \cap B = \emptyset$, d.w.z. ze hebben geen elementen gemeenschappelijk.

De unie van A en B is $A \cup B = \{x \mid (x \in A) \vee (x \notin B)\}$.
Het **verschil** van A en B is de verzameling $A \backslash B = \{x \mid (x \in A) \wedge (x \notin B)\}$.

Voorbeeld. Stel $A = \{1,2,3\}$ en $B = \{2,3,4,5\}$. Dan geldt: $A \cap B = \{2,3\}$, $A \cup B = \{1,2,3,4,5\}$, $A \backslash B = \{1\}$ en $B \backslash A = \{4,5\}$

Als $A \subset B$, dan heet $B \backslash A$ het **complement** van A t.o.v. B. Soms speelt een wiskundige theorie zich volledig af in een gegeven verzameling U. In dat geval worden alle complementen berekend t.o.v. U (tenzij anders vermeld natuurlijk). Voor $A \subset U$ noteert men dan kort A^c, $\bar{A}$ voor het complement $U \backslash A$. De verzameling U noemt men het **universum** van de theorie.

1.7 Oneindige unies en doorsneden

Zij I een verzameling. Onderstel dat voor elke $i \in I$ een verzameling A_i gegeven is. Zo bekomen we een verzameling $A = \{A_i \mid i \in I\}$ van verzamelingen **geïndexeerd** door I.

Voorbeeld. Stel $I = \{3,4,5,6,7\}$ en $A_i = \{1,2,3,\dots,i\}$. Dan is $A_3 = \{1,2,3\}$, $A_4 = \{1,2,3,4\}$ enz. Stel $J = \mathbb{N}_0$, $B_j = \left[0, \frac{1}{j}\right]$, een gesloten interval in $\mathbb{R}$. Dan is $B_1 = [0,1]$, $B_2 = \left[0, \frac{1}{2}\right]$ enz.

De doorsnede van alle verzamelingen geïndexeerd door I definiëren we als

$$\bigcap A = \bigcap_{i \in I} A_i = \{x \mid \forall i \in I : x \in A_i\}$$

en analoog definiëren we de unie

$$\bigcup A = \bigcup_{i \in I} A_i = \{x \mid \exists i \in I : x \in A_i\}$$

1.8 Cartesisch product

Zijn A, B twee verzamelingen. Het cartesisch product van A en B is de verzameling

$$A \times B = \{(a,b) | a \in A, b \in B\}$$

De elementen van $A \times B$ heten **koppels**. Als $(a,b), (c,d) \in A \times B$ dan geldt $(a,b) = (c,d) \Leftrightarrow (a = c) \wedge (b = d)$. Als $a \neq b$ geldt $(a,b) \neq (b,a)$.
In het algemeen zijn dus $A \times B$ en $B \times A$ verschillend. Als $A, B \subset U$ dan geldt $A \times B \subset U \times U$ en niet $A \times B \subset U$!

Als A en B eindig zijn geldt $|A \times B| = |A| \times |B|$.

Notatie. $A \times A$ noteren we kort A^2. Ook het Cartesisch product $A \times A \times \dots \times A$ van n keer dezelfde verzameling schrijven we A^n.

1.9 Relaties

Een relatie van een verzameling A naar een verzameling B is per definitie een deelverzameling R van het cartesisch product $A \times B$.

Notatie. Als $(a, b) \in R$, schrijven we aRb.

Voorbeeld. Beschouw de verzameling $A = \{1,2,3,4\}$ en de relatie "is kleiner dan of gelijk aan" op A. Dan is:

$$R = \{(a, b) \in A \times A | a \leq b\}$$
$$= \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$$

De inverse relatie R^{-1} van R is per definitie

$$R^{-1} \coloneqq \{(b, a) | (a, b) \in R\}$$

Dit is een relatie van B naar A.

1.10 Functies

Zijn A, B verzamelingen. Een functie van A naar B is een relatie van A naar B waarbij elk element van A precies één keer voorkomt als eerste component van een koppel in de relatie. De verzameling A heet het **domein** van de functie en B is het **codomein**.

Meestal noteren we functies met kleine letters en vermelden we duidelijk domein en codomein. Als $f \subset A \times B$ een functie is, noteren we $f: A \to B$.

Het woord **afbeelding** is een synoniem voor functie.
Zij $f: A \to B$ een functie. Indien $(a, b) \in f$ noteren we $f(a) = b$. Het element $b \in B$ heet beeld van a door f en a heet een origineel van b voor f.
We zeggen ook dat f het element a op het element b stuurt, notatie:

$$a \to b.$$

Merk op:
Niet alle elementen van het codomein hebben een origineel, maar elk element van het domein heeft wel een beeld.
Voor vele functies bestaat er een formule om het beeld van een willekeurig element van het domein te berekenen. Dit heet het **functievoorschrift**. De volledige notatie voor een functie wordt dan:

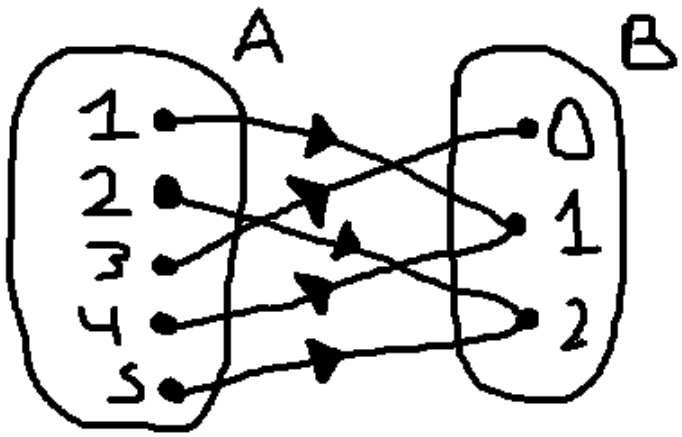
$$f: A \to B: a \to f(a)$$

waarbij $f(a)$ het functievoorschrift voorstelt.

Opmerking. Een functie wordt dus gedefinieerd door drie gegevens: domein, codomein en functievoorschrift, allen even belangrijk!

Voorbeeld.

$$f: A \to B: a \to \text{De rest na deling door } 3$$



In dit voorbeeld is $A = \text{domein}$ en $B = \text{Codomein}$, indien $(a, b) \in f$ dan heet a het origineel van b.
Opmerking:
het beeld van f is een deel van het codomein

$$f: \mathbb{R} \to \mathbb{R}: \text{x} \to \underbrace{\text{x}^2}_{\mathbb{R}^+ = \text{beeld}}$$

Dan:

$$f([-1,2]) = \underbrace{[0,4]}_{\text{Codomein}}$$

1.11 Beeld en invers beeld

Voor een functie $f: A \to B$ en $S \subset A$ definiëren we het **beeld van** S door f als

$$f(S) \coloneqq \{f(s) |\, s \in S\}$$
$$\coloneqq \{b \in B \mid \exists s \in S, f(s) = b\}$$

Dus geldt zeker $f(S) \subset B$.
De verzameling $f(A)$, het beeld van het hele domein van f, noemen we het **beeld van** f en noteren we ook als $Im\ f$. Het beeld van f is dus een deel van het codomein.

Voorbeeld. Zij $f: \mathbb{R} \to \mathbb{R}: x \to x^2$. Dan is $f([-1; 2]) = [0, 4]$ en $Im\ f = R^+$. Uit dit voorbeeld leren we dat $Im\ f$ dus in het algemeen niet gelijk is aan het codomein van f. Verwar dus niet beeld en codomein!

Nog steeds voor $f: A \to B$ maar nu $T \subset B$, definiëren we het **invers beeld** van T onder f als

$$f^{-1}(T) \coloneqq \{a \in A \mid f(x) \in T\}$$

Merk op dat $f^{-1}(T)$ een notatie is en niet impliceert dat er voor f een inverse functie bestaat.
Als T een **singleton** $\{b\}$ is, schrijven we $f^{-1}(b)$ i.p.v. $f^{-1}(\{b\})$.

Voorbeeld. Met f zoals in het vorige voorbeeld hebben we: $f^{-1}(4) = \{-2, 2\}, f^{-1}\ (-1) = \emptyset$ en $f^{-1}\big(f([0, 1])\big) = f^{-1}([0,1]) = [-1, 1]$.

In het algemeen geldt: $\forall S \subset A$: $f^{-1}\big(f(S)\big) \supset S$ en, zoals het voorbeeld toont, niet $f^{-1}\big(f(S)\big) = S$.
We bewijzen dit even.

Bewijs. Zij $f: A \to B$ een functie en $S \subset A$. We moeten bewijzen:

$$\forall s \in S: s \in f^{-1}\big(f(S)\big)$$

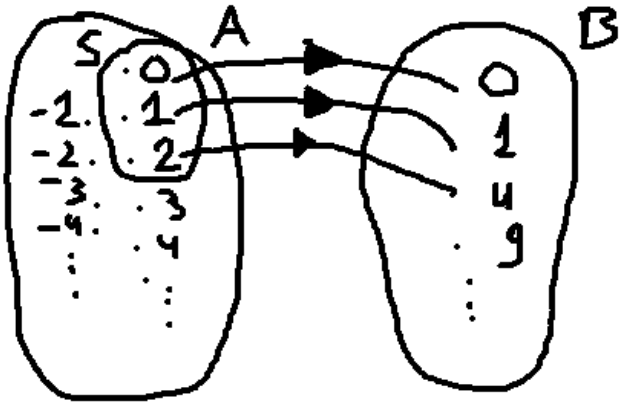
Dit is equivalent met

$$\forall s \in S: f(s) \in f(S) = \{f(t) |\, t \in S\}$$

wat duidelijk voldaan is. Je zal andere gelijkaardige eigenschappen in de oefeningen bewijzen.

Voorbeeld:

$$S = \{0,1,2\}, \qquad A \in \mathbb{Z}, \qquad B \in \mathbb{Z}$$



$$f^{-1}\big(f(\{0,1,2\})\big)$$
$$\Leftrightarrow f^{-1}(\{0,1,4\})$$
$$\Leftrightarrow \{0,1,-1,-2,2\} \supset S$$

1.12 Geïnduceerde functies, restrictie en corestrictie

Wanneer een functie $f: A \to B$ gegeven is, kan je gemakkelijk een functie van $A \times A$ naar $B \times B$ definiëren: we beelden (a, a') gewoon af op $\big(f(a), f(a')\big)$. Algemeen kan je functies $A^n \to B^n$ maken voor alle machten n. Je kan ook een functie maken op de delenverzameling $P(A)$ van A. Door $P(A) \to P(B): S \to f(S)$.

We noteren al deze functies afgeleid uit f meestal nog altijd met f en noemen ze de functies door f **geïnduceerd** op $A \times A$ (of op A^n of op $P(A)$). We kunnen ook beslissen om de functie $f: A \to B$ te bekijken op een deelverzameling X van A. Dan spreken we van de **restrictie** of **beperking** van f tot X. We noteren deze functie met $f|_X$. Er geldt dus

$$f|_X: X \to B: x \to f(x)$$

Voorbeeld.

$$A = \{1,2,3\}, B = \{4,5\}, D = \{1,2\} \text{ en } \mathrm{D} \subset \mathrm{A}$$
$$f = \{(1,4), (2,5), (3,4)\} \text{ en } f|_{\mathrm{D}} = \{(1,4), (2,5)\}$$

We kunnen ook het codomein van de functie f beperken. Zij $Y \subset B$ zo dat $\forall a \in A: f(a) \in Y$. Dan is de **corestrictie** van f tot Y de functie

$$f|^Y: A \to Y: x \to f(x)$$

We kunnen natuurlijk ook domein en codomein tegelijk beperken zodat we een functie $f|_X^Y: X \to Y$ bekomen met voor elke $x \in X: f|_X^Y(x) = f(x)$

1.13 Injecties en surjecties

Definitie 1. Een functie $f: A \to B$ heet **injectief** indien elk element van B hoogstens één keer voorkomt als tweede component van een koppel in f.

Anders gezegd: elk element van B heeft hoogstens één origineel. Nog anders gezegd: indien twee elementen van A hetzelfde beeld hebben, moeten ze gelijk zijn. In symbolen: $f: A \to B$ is injectief $\forall a, b \in A: \big(f(a) = f(b)\big) \Rightarrow (a = b)$

We zien dat we een functie injectief kunnen maken door punten uit het domein weg te laten. De functie g uit het voorbeeld is gewoon de restrictie van f tot R^+, of $f|_{R^+}$

Definitie 2. Een functie $f: A \to B$ is surjectief indien $Im\ f = B$.

Anders gezegd: elk element van het codomein heeft minstens één origineel. Symbolisch:

$$\forall b \in B: \exists a \in A: f(a) = b$$

Door het codomein te beperken kan je een functie dus surjectief maken.

Een functie die tegelijk surjectief en injectief is, heet **bijectief**. Een functie is bijectief ⇔

$$\forall b \in B: \exists! a \in A: f(x) = b$$

Een bijectie van een verzameling naar zichzelf heet een **permutatie**. Een zeer belangrijke permutatie is de **identieke permutatie** of de **identiteit**. Deze beeldt elk element af op zichzelf. We noteren de identieke permutatie van een verzameling X als 1_X. Er geldt dus $\forall x \in X: 1_X(x) = x$ o

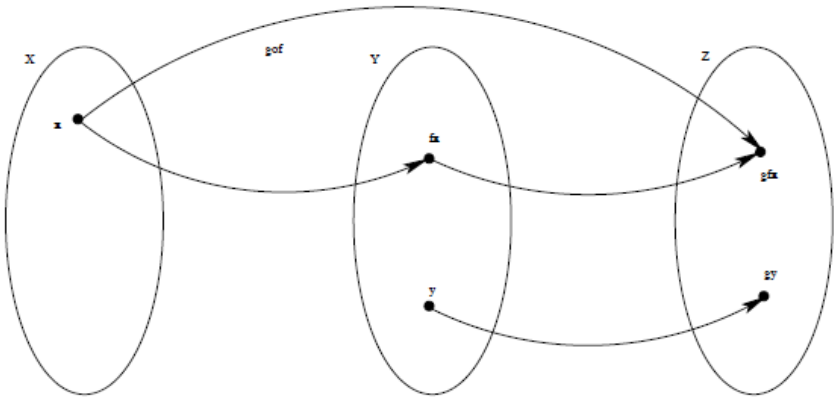
$$1_X; X \to X: x \to x$$

Opmerking. Andere notaties voor de identieke permutatie op X zijn i_X, Id_X of id_X.

1.14 De samenstelling van functies

Beschouw twee functies $f: A \to B$ en $g: B \to C$, waarbij het domein van g het codomein van f is. Dan kunnen we op elk beeld $f(a)$ de functie g toepassen. Zo definiëren we een nieuwe functie van A naar C die we $g \circ f$ noteren (lees "g na f" omdat we eerst f toepassen en dan g). Dus:

$$g \circ f: A \to C: a \to g\big(f(a)\big)$$



We merken op dat $f \circ g \neq g \circ f$ dus de volgorde heeft belang.

Eigenschap 1. De samenstelling van functies is associatief: voor elke drie functies

$$A \underset{\rightarrow}{f} B \underset{\rightarrow}{g} C \underset{\rightarrow}{h} D$$

Geldt

$$h \circ (f \circ g) = (h \circ f) \circ g$$

Bewijs. Domeinen en codomeinen zijn duidelijk gelijk. Zij $a \in A$, dan

$$\begin{aligned} &\big(h \circ (f \circ g)\big)(a) = h\big((f \circ g)(a)\big) \\ &= h\Big(g\big(f(a)\big)\Big) \\ &= (h \circ g)\big(f(a)\big) \\ &= \big((h \circ g) \circ f\big)(a) \end{aligned}$$

1.15 Inverse functies

Definitie 3. Zij $f\colon A \to B$ een functie. Indien een functie $g\colon B \to A$ voldoet aan

$$f \circ g = 1_B \text{ en } g \circ f = 1_A$$

dan heet g een **invers** voor f. We zeggen dan ook dat f **inverteerbaar** is.

Niet alle functies hebben een invers. Een inverse g van $f\colon A \to B$ moet een functie zijn van B naar A. Dus moet voor elke $b \in B$ precies één beeld $g(b) \in A$ voorzien worden. Bovendien moet gelden:

$$(f \circ g)(b) = 1_B(b) = b.$$

Bijgevolg moet $g(b) \in f^{-1}(b)$. Opdat $g\colon B \to A$ een functie zou zijn is dus nodig dat $\forall b \in B\colon f^{-1}(b) \neq \emptyset$ Dit komt erop neer dat f surjectief moet zijn.

Als $f\colon A \to B$ surjectief is, zouden we als volgt een inverse $g\colon B \to A$ kunnen construeren: voor elke $b \in B$ kiezen we een beeld $g(b)$ in $f^{-1}(b)$. Maar is zulke g dan een invers van f?

De voorwaarde $g \circ f = 1_A$ dwingt de injectiviteit van f. Inderdaad: als f niet injectief is, bestaan er $a \neq a' \in A$ met $f(a) = f(a')$. Stel $b := f(a)$, dan geldt $a, a' \in f^{-1}(b)$. Kiezen we dan als beeld van b door g het element a, dan hebben we $g(b) = a$, maar ook

$$g(b) = g(f(a')) = (g \circ f)(a') = 1_A(a') = a'.$$

Dus $a = a'$, wat in tegenspraak is met $a \neq a'$.

Als f een bijectie is, is $\forall b \in B; f^{-1}(b)$ een singleton. Er is dus geen keuze voor het construeren van de inverse g. De functie $g\colon B \to A$ is dan wel degelijk een inverse van f.

We hebben bewezen:
Stelling 1. Enkel bijectieve functies hebben een invers.

Eigenschap 2. Een functie heeft hoogstens één invers.

Bewijs. Zij $f: A \to B$ en zijn $g: B \to A$ en $g': B \to A$ twee inversen. Dan geldt, $\forall b \in B$

$$\begin{aligned} g(b) &= g\big(1_B(b)\big) \\ &= g\big((f \circ g')(b)\big) \\ &= (g \circ f \circ g')(b) \\ &= (g \circ f)\big(g'(b)\big) \\ &= 1_A\big(g'(b)\big) \\ &= g'(b) \end{aligned}$$

Vermits de domeinen en codomeinen van g en g' gelijk zijn, hebben we $g = g'$.

Nu we weten dat elke inverteerbare functie juist één invers heeft, kunnen we spreken over het invers van een functie f in plaats van over een invers. We noteren de inverse functie f^{-1}. Verwar dit niet met inverse beelden die voor alle functies gedefinieerd zijn, niet enkel voor bijecties.

Hoofdstuk 2: Eenvoudige principes van discrete wiskunde

2.1 De duiventil

We weten allemaal zeer goed dat als we 25 duiven in 20 hokjes moeten verdelen, er minstens 1 hokje zal zijn met meer dan 1 duif.

Stelling 2 (Principe van de duiventil). Als we n identieke objecten verdelen over k dozen met $n > k$, **dan** is er $\underbrace{\text{minstens } 1}_{\geq 1}$ doos met $\underbrace{\text{minstens } 2}_{\geq 2}$ objecten.

Bewijs. Uit het ongerijmde (U.H.O.) $1 \Rightarrow 2 \Leftrightarrow \neg 2 \Rightarrow \neg 1$
Veronderstel van niet. Als we niet hebben dat er $\underbrace{\text{minstens } 1}_{\geq 1}$ doos is met $\underbrace{\text{minstens } 2}_{\geq 2}$ objecten,
Dan is er in elke[1] doos $\underbrace{\text{hoogstens } 1}_{< 2}$ [2] object. Zij m het aantal lege dozen (met nul objecten dus).
Dan zijn er in totaal $k - m$ dozen met elk juist 1 object. Vermits alle objecten verdeeld werden, geldt:

$$n = k - m$$

We hebben ze allemaal in die $k - m$ dozen gestoken, m kan 0 zijn dus dat kunnen we boven afschatten door k

$$n = k - m \leq k$$
$$n \leq k$$

Maar er was gegeven dat $n > k$:

$$n \leq k < n$$
$$n < n$$

en dat is een tegenspraak. □

Toepassing. Bekijk de rij $7, 77, 777, 7777, \ldots$ van natuurlijke getallen die enkel het cijfer 7 bevatten. Is 1 van die getallen deelbaar door 2013? We gaan bewijzen dat het antwoord ja is. Sterker zelfs:

Gevolg 1. In de eerste 2013 elementen van bovenstaande rij $7, 77, 777, 7777, \ldots$ zit minstens 1 veelvoud van 2013.

Bewijs. We noteren de eerste elementen van de rij $a_1, a_2, .., a_{2013}$.
Voor twee getallen a en b kunnen we steeds quotiënt q en rest r bepalen zodat $a = qb + r$ met $0 \leq r < b$. Doe dit nu voor alle getallen in de rij. Dus $\forall i \in \{1, \ldots, 2013\}$ bepalen we q_i en r_i zodat $a_i = 2013q_i + r_i$.

Als er een i bestaat met $r_i = 0$, dan is a_i deelbaar door 2013 en is er niets meer te bewijzen. Veronderstel nu, uit het ongerijmde, dat geen enkele r_i 0 is. Dan is $\{r_1, r_2, \ldots, r_{2013}\}$ een deelverzameling van$\{1,2, \ldots, 2012\}$, de mogelijke niet-nulle resten bij deling door 2013.

De duiventil leert ons dat minstens twee resten gelijk zijn. Dus $\exists i \neq j \in \{1, \ldots, 2013\}$ met $r_i = r_j$.
We mogen, zonder de algemeenheid te schaden, aannemen dat $a_i > a_j$.

Bekijk nu het verschil $a_i - a_j$: enerzijds is:

---

[1] $\neg \geq 1 = 0$
[2] $\neg \geq 2 = < 2$ (0 of 1)

$$\begin{array}{rcrcl} & & a_i & = & 77\ldots7777\ldots77 \\ & - & a_j & = & 77\ldots77 \\ \hline a_i & - & a_j & = & \underbrace{77\ldots77}_{a_{i-j}}00\ldots00 \end{array}$$

Of dus $a_i - a_j = \underbrace{77\ldots77}_{a_{i-j}} x10^j$

Anderzijds is $a_i - a_j = (2013q_i + r_i) - \left(2013q_j + r_j\right) = 2013\left(q_i - q_j\right) + 0$, aangezien $r_i = r_j$. Dus $a_i - a_j = a_{i-j} \times 10^j$ is een veelvoud van 2013.

Dit wil zeggen dat $a_{i-j} \times 10^j$ deelbaar is door 2013, maar vermits 10^j geen enkele deler gemeenschappelijk heeft met 2013, moet a_{i-j} een veelvoud zijn van 2013. We bekomen een tegenspraak en dus is het gestelde bewezen. □

Voorbeeld. In een groep van 100 mensen zijn er minstens 9 die hun verjaardag vieren in dezelfde maand. Inderdaad; onderstel dat er geen 9 hun verjaardag in dezelfde maand hebben, dan zijn er hoogstens $8 \times 12 = 96$ mensen. Strijdig!

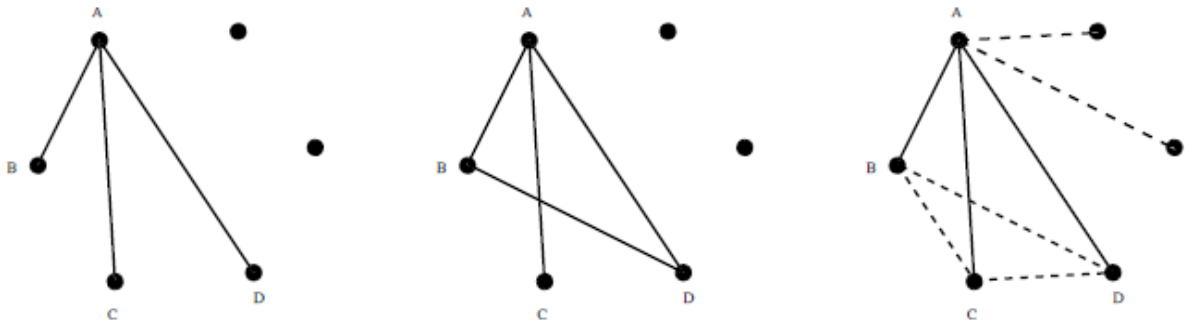
Notatie. Zij $x \in \mathbb{R}$. Dan noteren we:

$$\lceil x \rceil = \text{kleinste geheel getal} \geq x$$
$$\lfloor x \rfloor = \text{kleinste geheel getal} \leq x$$

Het voorbeeld illustreert de **veralgemeende duiventil**. Als je n identieke objecten verdeelt over k dozen, dan is er minstens 1 doos met minstens $\left\lceil \frac{n}{k} \right\rceil$ objecten. Het bewijs is analoog met dat van de "gewone" duiventil.

Voorbeeld. In een groepje van 6 mensen zijn elke twee individu's ofwel vrienden ofwel vijanden. Men kan met zekerheid zeggen dat er in deze groep drie mensen zijn die ofwel 2 aan 2 vijanden zijn, ofwel 2 aan 2 vrienden.

Bewijs. Zij A één van die personen. De overblijvende 5 personen vallen uiteen in 2 groepen, de vrienden van A en de vijanden van A. Door het veralgemeend principe van de duiventil bevat 1 van die twee groepen minstens $\left\lceil \frac{5}{2} \right\rceil = 3$ personen.
Onderstel dat we dus minstens 3 vrienden hebben (het geval dat er minstens 3 vijanden zijn verloopt analoog). We noemen B, C, D drie van die vrienden (zie figuur 2.1). Als twee van de drie bevriend zijn is het bewijs gedaan. Als geen twee van de drie bevriend zijn, hebben we drie personen gevonden die 2 aan 2 vijanden zijn. □



Figuur 2.1: Illustratie van het bewijs. In de derde tekening zijn voor de duidelijkheid de vijanden verbonden met streepjeslijnen.

Opmerking. In dit bewijs gebruikten we een voorstelling van het probleem met punten en verbindingen. Zulks heet een graf (of graaf). We zullen dit concept nauwkeurig definiëren en bestuderen in Hoofdstuk 4.

2.2 Eenvoudige teltechnieken

Laat ons terugdenken aan het bewijs van het veralgemeende principe van de duiventil. We tellen de objecten in de verschillende dozen op en komen zo tot een contradictie omdat het totaal aantal objecten niet bereikt is. Als we objecten tellen in dozen komt het er eigenlijk op neer dat we elementen tellen in disjuncte verzamelingen.

2.2.1 Tellen

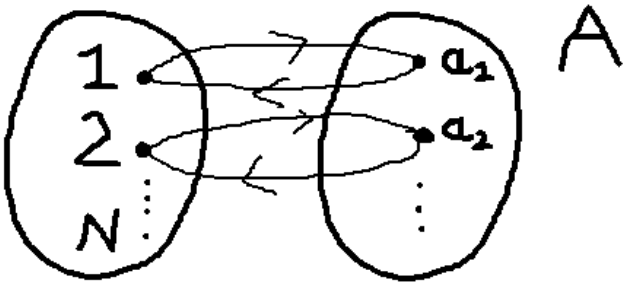
Twee eindige verzamelingen A en B evenveel elementen hebben $\Leftrightarrow$ er een bijectie $A \leftrightarrow B$ bestaat. We gaan nu meer formeel definiëren wat we bedoelen met aantal elementen in een eindige verzameling. Als we elementen van een verzameling A tellen, gaan we ze eigenlijk nummeren: je neemt een eerste element weg uit de verzameling, dan een tweede enz. tot er geen meer zijn.

Dit resulteert in een bijectie f tussen de verzameling $\{1, 2, \dots, n\}$ en A met $f(i) = i$-de element van A in onze selectie.

Notatie. $[n] \coloneqq \{1,2, \dots, n\}$. Meer algemeen is $[1..n] = [n]$, maar ook $[0..n] = \{0,1, \dots, n\}$ en $[-k..l] = \{-k, -k+1, \dots, l-1, l\}$.

Definitie 4. Een verzameling A heeft $n \in \mathbb{N}$ elementen indien er een bijectie bestaat van $[n]$ naar A. We noteren $|A| = n$. Zulk bijectie bepaalt een **ordening** of **nummering** van A.

Notatie. Als $|A| = n$ en $f: [n] \to A$ een nummering is, dan schrijven we dikwijls a_i i.p.v. $f(i)$.



$$|A| = [n]$$

De twee verzameling hebben evenveel elementen omdat er een bijectie bestaat tussen te twee.

Hoeveel deelverzamelingen heeft een eindige verzameling X? We kunnen de elementen van X nummeren:

$$x = \{x_1, x_2, \dots, x_n\}$$

We stellen ons dus eigenlijk de vraag op hoeveel manieren we een aantal elementen uit X kunnen kiezen om een deelverzameling te vormen. Het eerste element x_1 kan geselecteerd worden of niet. Er zijn dus twee keuzes. Ook x_2 kan wel of niet tot de deelverzameling behoren. We zien dus dat er voor elk element apart kan beslist worden om het in de deelverzameling te stoppen of niet.
We moeten dus n keer kiezen tussen twee mogelijkheden. In totaal zijn er dus 2^n deelverzamelingen van X.

Stelling 3. Voor elke eindige verzameling X geldt:

$$|P(X)| = 2^{|x|}$$

2.2.2 Somprincipe

Stelling 4 (Somprincipe).
Zijn $A_1, A_2, \dots, A_k$ twee aan twee disjuncte eindige verzamelingen. Dan geldt:

$$|A_1 \cup A_2 \cup \dots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|$$

Niet op examen:
Bewijs. Dit is intuïtief weer zeer vanzelfsprekend. We hebben bijecties $f_i: [n_i] \to A_i$ voor $i \in [k]$.
Merk op dat:

$$\left[\sum_{i=1}^{k} n_i\right] = [1..n_1] \cup [(n_1+1)..(n_1+n_2)] \cup \dots \cup \left[\left(\sum_{i=1}^{k-1} n_i\right) + 1..\sum_{i=1}^{k} n_i\right]$$

Definieer:

$$f: \left[\sum_{i=1}^{k} n_i\right] \to A_1 \cup A_2 \cup \dots \cup A_k$$

Door:

$$f(i) = f_j\left(i - \sum_{l=1}^{j-1} n_l\right) \; als \; i \in \left[\left(\sum_{l=1}^{j-1} n_l\right) + 1..\sum_{l=1}^{j} n_l\right]$$

Verifieer zelf dat f een bijectie is. Vergeet hierbij niet dat alle verzamelingen disjunct zijn.

Voorbeeld.

$$A_1 = \{1,2,3\}, \qquad A_2\{6\}, \qquad A_3 = \{7,8\}$$

Met $k = 3$,

$$f_1: \overbrace{[n_1]}^{\{1,2,3\}^3} \to A_1$$
$$f_2: [n_2] \to A_2$$
$$f_3: [n_3] \to A_3$$

Dus:

$$\left[\sum_{i=1}^{3} n_i\right] = [1..n_1] \cup [(n_1+1)..(n_1+n_2)] \cup [(n_1+n_2+1)..(n_1+n_2+n_3)]$$
$$= \{1,2,3\} \cup \{4\} \cup \{5,6\}$$
$$= 6 \text{ elementen} = |A_1| + |A_2| + |A_3|$$

[3] Dit leiden we af door een bijectie

2.3 Teltechnieken met producten

2.3.1 Dubbeltellen

Je gaat met vrienden iets drinken. Iedereen trakteert een rondje. Op het einde van de avond willen jullie weten hoeveel glazen water er in totaal gedronken zijn. Dit kan je enerzijds te weten komen door aan iedereen te vragen hoeveel glazen water hij gedronken heeft die avond en dan alles op te tellen. Of je kan aan iedereen vragen hoeveel watertjes hij betaalde in zijn ronde en dan alles optellen.

We kunnen dus hetzelfde op twee manieren tellen.

Stelling 5 (Principe van dubbeltelling). Zij A en B twee (eindige) verzamelingen. Zij $S \subset A \times B$. Stel voor elke $a \in A$:

$$k_a \coloneqq |\{(a,b) \mid b \in B \text{ en } (a,b) \in S\}|^4$$

En voor elke $ab \in B$:

$$r_b \coloneqq |\{(a,b) \mid a \in A \text{ en } (a,b) \in S\}|$$

Dan geldt:

$$\sum_{a \in A} k_a = |S| = \sum_{b \in B} r_b$$

Bewijs.
Stel $K_a \coloneqq \{(a,b) \mid b \in B \text{ en } (a,b) \in S\}$. De verzamelingen $(K_a)_{a \in A}$ zijn disjunct omdat we altijd een andere a vastnemen dus:

$$|S| = \left|\bigcup_{a \in A} K_a\right| = \sum_{a \in A} K_a$$

Analoog:
Stel $R_b \coloneqq \{(a,b) \mid a \in A \text{ en } (a,b) \in S\}$. De verzamelingen $(R_b)_{b \in B}$ zijn disjunct omdat we altijd een andere b vastnemen dus:

$$|S| = \left|\bigcup_{b \in B} R_b\right| = \sum_{b \in B} R_b$$

□

Gevolg 2. Als alle k_a gelijk zijn aan een zekere constante k en alle r_b gelijk zijn aan r dan geldt $k|A| = r|B|$.

Toepassing. De dodecaëder heeft 30 ribben want er zijn 12 zijvlakken met elk 5 ribben en elke ribbe ligt op 2 zijvlakken. We tellen de koppels (ribbe, zijvlak) op twee manieren:

$$\#ribben \times 2 = 12 \times 5.$$

[4] Is het aantal elementen in de verzameling van de koppels (a,b) met b in B waarvoor we dus hebben dat de koppel (a,b) is S zitten (we nemen dus een a vast)

Voorbeeld.

$$A = \{1,2\}, \qquad B = \{a, b\}, \qquad S = \{(1, a), (1, b), (2, a)\}$$
$$\sum_{a \in A} k_a = k_1 + k_2$$
$$\Leftrightarrow |(1, a), (1, b)| + |(2, a)| + |\emptyset|$$
$$= 3 = |S|$$

2.3.2 Tel probleem 1: Woorden (H en V)

Zij $f: [m] \to Y$ een functie. Deze bepaalt m elementen van Y, namelijk $f(1), f(2), \dots, f(m)$.
Ook elk m-tupel in Y^m bepaalt een functie $[m] \to Y$.
Als je bijvoorbeeld het m-tupel $(y_1, y_2, \dots, y_m)$ neemt, stel dan gewoon $f(i) \coloneqq y_i$.

Een **woord** van **lengte** m over het alfabet Y is gewoon een m-tupel elementen uit Y.
Elk woord bepaalt dus een functie en omgekeerd.

Stelling 6 (Woorden). Zijn X, Y eindige verzamelingen, met $|X| = m$ en $|Y| = n$.
Dan geldt:

$$\#\{\text{functies } f: X \to Y\} = n^m.$$

Bewijs. Elke functie komt overeen met een m-tupel van Y en we weten:

$$|Y^m| = \underbrace{|Y \times Y \times \dots \times Y|}_{m \text{ keer}} = |Y|^m$$

□

Voorbeeld. $y = \{1,2,3,4\}$ met $m = 2$

$$\{(1,1), (1,2), (1,3), (1,4),$$
$$(2,1), (2,2), (2,3), (2,4),$$
$$(3,1), (3,2), (3,3), (3,4),$$
$$(4,1), (4,2), (4,3), (4,4)\}$$

Een m-tupel is bijvoorbeeld: $(1,2)$ en $|Y|^m = 4^2 = 16$

Voorbeeld. Het aantal woorden van lengte 3 in ons alfabet is 26^3.

Opmerking. Een woord maken komt erop neer dat we uit ons alfabet achtereenvolgend een letter kiezen. Herhalingen zijn toegestaan. Je kan je ook inbeelden dat de letters van het alfabet gedrukt staan op 26 bollen in een bokaal. Je neemt dan telkens een bol, kijkt naar de letter die erop staat en legt hem dan terug.

Voorbeeld. Het aantal deelverzamelingen van een verzameling met n elementen is 2^n.

2.3.3 Tel probleem 2: Injecties tellen (~~H~~ en V)

Als we geen herhaling toelaten, bekijken we woorden waarin de functie $[m] \to Y$ injectief is.
We tellen met injectieve functie omdat als we een element gekozen hebben uit ons Codomein, mogen we niet meer dart element opnieuw kiezen elke $b \in B$ mag hoogstens één origineel hebben.

Hoe tellen we het aantal injectieve functies?

Stelling 7. Het aantal geordende keuzes van m objecten uit n zonder herhaling is

$$n(n-1)(n-2)\ldots(n-m+1)$$

Bewijs. Om zo een woord te vormen moeten we achtereenvolgend m verschillende elementen van Y kiezen. Voor de eerste letter zijn er n keuzes, voor de tweede $n-1$ (want we mogen om het even welke letter nemen behalve die die we als eerste kozen). Voor de derde letter $n-2$ keuzes enz. tot we de laatste letter kiezen uit de $n-m+1$ die overblijven. □

Notatie. De faculteit (Engels: "factorial", Frans: "factorielle") van een natuurlijk getal $n \in \mathbb{N}$ is het getal:

$$n! = n \times (n-1) \times \ldots \times 3 \times 2 \times 1$$

Per definitie stellen we $0! = 1$ (we zullen dit later motiveren).[5]
Het aantal keuzes in stelling 7 is bijgevolg kort te noteren als

$$\frac{n!}{(n-m)!}$$

Voorbeeld. Op hoeveel manieren kan ik 6 studenten uit de klas kiezen en in een rij tegen het bord zetten? (720)

2.3.4 Bijecties tellen

Wat als in vorige stelling $n = m$?
Het aantal keuzen is gelijk aan het aantal objecten in de verzameling. Elk object kiezen zonder herhaling. Dan staat er: we kunnen op $n!$ Verschillende manieren n objecten kiezen waarbij de volgorde van belang is.

$$\frac{n!}{(n-n)!} = \frac{n!}{0!} = \frac{n!}{1} = n!$$

En dat noemen we ook een **permutatie**. $n!$ Heeft het aantal manier om n objecten te ordenen en elke ordening een ander resultaat is.

Dit betekent dat we de bijecties $[n] \leftrightarrow Y$ tellen,
want als $f: [n] \to Y$ injectief is met $|Y| = n$, dan is f een bijectie (oefening).
Een selectie van n objecten uit n kunnen we zien als een **(her)ordening** van die objecten.

Een bijectie $f: Y \leftrightarrow Y$ van een verzameling naar zichzelf noemt men een permutatie.
Een **permutatie** $f: Y \leftrightarrow Y$ is een (her)ordening van Y. Vermits $|Y| = n$, hebben we een bijectie (of ordening) $g: [n] \to Y$. . We kunnen dus ook spreken van een **permutatie** van n objecten.

[5] Wordt vaak vergeten bij definities op examens.

Als we twee ordeningen hebben, kunnen we die samensmelten in de context van samenstellingen van functies. Het Codomein is het domein van het ander enz. en dan krijgen we opnieuw een permutatie.

De samenstelling $f \circ g: [n] \to Y$ is ook een ordening van Y. Twee ordeningen $f, g: [n] \leftrightarrow Y$ geven ook aanleiding tot een permutatie $Y \leftrightarrow Y$. Inderdaad: vermits f en g bijecties zijn, zijn ze inverteerbaar. $g \circ f^{-1}: Y \leftrightarrow Y$ is dan een permutatie.

2.3.5 Tel probleem 3: Deelverzamelingen tellen (~~↮~~ en ~~∀~~)[6]

Zij A een verzameling en $k \in \mathbb{N}$. Een k-deelverzameling van A is een deelverzameling met k elementen. Gegeven is $|A| = n$. Hoeveel k-deelverzamelingen heeft A?[7]

We gaan daarvoor eerst de volgorde wel laten meetellen en dan kunnen naar de volgorde van geen belang gaan door een aantal mogelijkheden te gaan weg delen:
Kiezen we k elementen uit A met volgorde, dan zullen we eenzelfde deelverzameling meerdere keren kiezen.

Hoeveel keren hebben we de deelverzameling dubbel geteld ?
We kunnen dit aantonen a.d.h.v. het principe van de dubbeltelling, Beschouw de verzameling:

$$S = \{(B, f) \mid B \subset A, |B| = k \text{ en } f \text{ een ordening op } B\}^{8}$$

Dan kunnen we $|S|$ op 2 manieren tellen:

1:

$$|S| = x \times k!$$

Met x het aantal k-deelverzamelingen van A en $k!$ Het aantal ordeningen van een gegeven k-deelverzamelingen. We zijn opzoek naar x maar enerzijds bestaat $|S| = x \times k!$.

2:

$$|S| = 1 \times \frac{n!}{(n-k)!}$$

Want we kunnen op $\frac{n!}{(n-k)!}$ Manieren k elementen kiezen uit A met volgorde.

Als we 1 en 2 aan elkaar gaan gelijkstellen:

$$x \times k! = 1 \times \frac{n!}{(n-k)!}$$
$$x = \frac{n!}{(n-k)!\,k!}$$

Voor $n \geq k$ noteren we:

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$$

[6] Het aantal mogelijke keuze om k objecten uit een verzameling van n objecten te gaan kiezen, waar de herhaling van objecten niet is toegestaan, en volgorde niet van belang is.
[7] Hoeveel keuzes van k objecten ka ik maken waar de volgorde niet uitmaakt. $(aab = baa = aba)$
[8] Een verzameling S met k deelverzamelingen

Stelling 8. Het aantal keuzes van k elementen uit een verzameling van n elementen, zonder volgorde en zonder herhaling, bedraagt

$$\binom{n}{k}$$

We merken ook nog op dat:

$$\binom{n}{n-k} = \binom{n}{k}$$

Voorbeeld.

$$A = \{1,2,3\}, \qquad n = 3, \qquad k = 2$$

Met

$$S = \{(B, f) \mid B \subset A, |B| = k \text{ en } f \text{ een } \textbf{ordening} \text{ op } B\}$$

Om $|S|$ te kunnen berekenen kijken we eerst hoeveel manieren k elementen kiezen uit A **met volgorde:**

$$\frac{n!}{(n-k)!} = \frac{3!}{(3-2)!} = \frac{6}{1} = 6$$

Maar we hebben nu bepaalde deelverzamelingen dubbel geteld want $\{1,2\} = \{2,1\}$ dus die moeten we nog er aftrekken. Dit kunnen we doen door Het aantal ordeningen van een gegeven k-deelverzamelingen te delen door onze tussenuitkomst:

$$k! = 2! = 2$$

Dus:

$$\frac{6}{2} = 3$$

Deelverzamelingen:

Dus 2-deelverzamelingen uit A:

$$\{1,2\}, \{1,3\}, \{2,3\}$$

Eigenschap 3. (Identiteit van Pascal). Zij $n, k \in \mathbb{N}$ met $k \leq n$. Dan geldt:

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

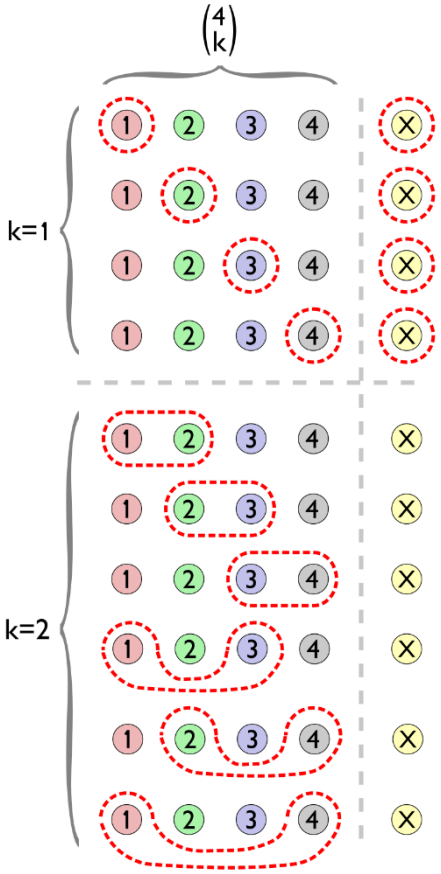
Wat ons de identiteit van pascal ons zegt is op een recursieve manier het aantal mogelijkheden van k uit n te gaan berekenen uit de keuzes van verzamelingen met 1 element minder.

Bewijs.
Algebraïsch:

$$\binom{n-1}{k-1}+\binom{n-1}{k}=\frac{(n-1)!}{(k-1)!\,(n-k)!}+\frac{(n-1)!}{k!\,(n-1-k)!}$$
$$=(n-1)!\left[\frac{n-k}{k!\,(n-k)!}+\frac{k}{k!\,(n-k)!}\right]$$
$$=(n-1)!\frac{n}{k!\,(n-k)!}$$
$$=\frac{n!}{k!\,(n-k)!}=\binom{n}{k}$$

Combinatorisch:

Onthoud dat $\binom{n}{k}$ gelijk is aan het aantal deelverzamelingen met k elementen uit een verzameling met n elementen. Stel dat één bepaald element uniek gelabeld is met X in een verzameling met n elementen.



Om een deelverzameling van k elementen te construeren die ***X* bevat**, neem je X op en kies je $k-1$ elementen uit de resterende $n-1$ elementen in de verzameling.
Er zijn $\binom{n-1}{k-1}$ dergelijke deelverzamelingen.

Om een deelverzameling van k elementen te construeren die ***X* niet bevat**, kies je k elementen uit de resterende $n-1$ elementen in de verzameling. Er zijn $\binom{n-1}{k}$dergelijke deelverzamelingen.

Elke deelverzameling van k elementen bevat X of niet.
Het totaal aantal deelverzamelingen met k elementen in een verzameling van n elementen is de som van het aantal deelverzamelingen dat ***X* bevat** en het aantal deelverzamelingen dat **X niet bevat**:

$$\binom{n-1}{k-1}+\binom{n-1}{k}$$

Dit is gelijk aan: $\binom{n}{k}$

Voorbeeld.

$$n=\{1,2,\overset{x}{\overset{\sim}{3}}\},\qquad |N|=3,\qquad k=2$$

1. $|\{(3,1),(3,2)\}|=2=\binom{n-1}{k-1}=\binom{2}{1}=2$
2. $|\{(1,2)\}|=1=\binom{2}{2}=1$
3. $\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k}=2+1=\binom{3}{2}=3$

Deze stelling geeft aanleiding tot de beroemde driehoek van Pascal:

$$\begin{array}{ccccccccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & & & & & & & \\
 & & & & & \binom{1}{0} & & & \binom{1}{1} & & & & & & & & & \\
 & & & & \binom{2}{0} & & & \binom{2}{1} & & & \binom{2}{2} & & & & & & & \\
 & & & \binom{3}{0} & & & \binom{3}{1} & & & \binom{3}{2} & & & \binom{3}{3} & & & & & \\
 & & \cdots & & & \cdots & & & \cdots & & & \cdots & & & \cdots & & & \\
 & & & & & & & & 1 & & & & & & & & & & \\
 & & & & & & & 1 & & & 1 & & & & & & & & \\
 & & & & & & 1 & & & 2 & & & 1 & & & & & & \\
 & & & & & 1 & & & 3 & & & 3 & & & 1 & & & & \\
 & & & & 1 & & & 4 & & & 6 & & & 4 & & & 1 & & \\
 & & & 1 & & & 5 & & & 10 & & & 10 & & & 5 & & & 1 \\
 & & 1 & & & 6 & & & 15 & & & 20 & & & 15 & & & 6 & & & 1 \\
 & \cdots & & & \cdots & & & \cdots & & & \cdots & & & \cdots & & & \cdots & & & \cdots & & & \cdots
\end{array}$$

waarbij de getallen op de zijkant altijd 1 zijn, en de andere getallen telkens de som zijn van de twee getallen die op de rij erboven links en rechts ervan staan.

2.3.6 Tel probleem 4: Herhalingscombinaties (H en ~~V~~)

Stel $A = \{a, b, c, d\}$. De keuze $bcadabd$ is equivalent met de keuze $aabbcdd$ wanneer de volgorde geen rol speelt. Hoeveel mogelijkheden zijn er zo?
We moeten hier dus de woorden tellen die bestaan uit een aantal a's, gevolgd door een aantal b's, dan een aantal c's enz. zodat er in totaal 7 letters zijn. Let wel, het aantal in kwestie kan soms nul zijn: $bbbbbbb$ is ook een woord van zeven letters met herhaling!

Een voorstelling van $aabbcdd$ is $**\,|\,**\,|\,*\,|\,**$. In totaal hebben we dus 10 tekens waarvan elk een $*$ of een | is. We zetten een $*$ voor elke letter en een | als de letter verandert.
Dus | $**$ || $******$ stelt het woord $bbddddd$ voor: er zijn geen a's omdat er voor de eerste | geen $*$ staat, en geen c's omdat er tussen de tweede en de derde | geen $*$ staan.

In het algemeen hebben we n objecten waarin we k keer kiezen met terugleggen en geen rekening houden met de volgorde. Het aantal manieren om dat te doen is het aantal manieren om $n-1$ streepjes te plaatsen als er $n+k-1$ plaatsen beschikbaar zijn. Dit is dus $\binom{n+k-1}{n-k}$. We weten $\binom{n+k-1}{n-k} = \binom{n+k-1}{k}$ zodat het aantal **herhalingscombinaties** van k objecten uit n gelijk is aan:

$$\binom{n+k-1}{k}$$

We tonen nog even een interessante eigenschap van de getallen $\binom{n}{k}$.

Eigenschap 4. Voor $n \in \mathbb{N}$ geldt

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0$$

Bewijs. We weten dat $\binom{n}{0} = \binom{n-1}{0} = \binom{n}{n} = \binom{n-1}{n-1} = 1$ zodat het linkerlid via de Pascal-identiteit kan herschreven worden als:

$$1 - \left[1 + \binom{n-1}{1}\right] + \left[\binom{n-1}{1} + \binom{n-1}{2}\right] - \cdots + (-1)^{n-1}\left[\binom{n-1}{n-2} + 1\right] + (-1)^n \times 1$$

De tweede term tussen de eerste vierkante haken valt weg tegen de eerste term tussen de tweede vierkante haken. Analoog valt de tweede term tussen de tweede haken weg tegen de eerste term tussen de derde haken, enz. Uiteindelijk blijft er over

$$1 - 1 + (-1)^{n-1} \times 1 + (-1)^n \times 1 = 0$$

□

2.4 Het binomium van Newton

We kennen reeds zeer lang volgende formules: $(a + b)^2 = a^2 + 2ab + b^2$ en $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$. Algemeen geldt:

Stelling 9 (Binomium van Newton).

$$(a+b)^n = \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \cdots + \binom{n}{n} a^0 b^n$$
$$= \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Bewijs.
De macht

$$(a+b)^n = \underbrace{(a+b)(a+b)\ldots(a+b)}_{n \text{ keer}}$$

werken we uit aan de hand van de distributiviteit. De term met $a^{n-i}b^i$ ontstaat door in i factoren $(a + b)$ de b te kiezen (en in de overige natuurlijk de a). De coëfficiënt die hoort bij $a^{n-i}b^i$ is bijgevolg gelijk aan het aantal keuzes van i objecten uit n. Dat is $\binom{n}{i}$. □

Je kan dus de driehoek van Pascal gebruiken om de coëfficiënten van elke macht te vinden in $(a + b)^n$.

De naam binomium komt van binoom, een geleerd woord voor tweeterm (een ander woord voor veelterm is trouwens polynoom). Daarom heten de getallen $\binom{n}{k}$. ook binomiaalcoëfficiënten.

Voorbeeld. De letters a en b in het binomium kunnen om het even wat zijn. Bijvoorbeeld:

$$(1-x)^7 = 1 - 7x + 21x^3 - 35x^3 + 35x^4 - 21x^5 + 7x^6 - x^7$$

Het binomium kan ook gebruikt worden om andere eigenschappen van binomiaalcoëfficiënten aan te tonen

Stelling 10. Voor alle $n \in \mathbb{N}$ geldt:

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

Bewijs.
We weten dat $(1+x)^n(1+x)^n = (1+x)^{2n}$. We passen nu op het rechterlid het binomium toe:

$$(1+x)^n(1+x)^n = \binom{2n}{0} + \binom{2n}{1}x + \cdots + \binom{2n}{n}x^n + \cdots + \binom{2n}{2n}x^{2n}$$

De coëfficiënten van de term in het midden van het rechterlid is het rechterlid van wat we willen bewijzen.

Nu zijn twee veeltermen gelijk als en slechts als de coëfficiënten van de overeenkomstige machten van x gelijk zijn. We gaan dus de coëfficiënt zoeken van x^n in $(1+x)^n(1+x)^n$. We krijgen een bijdrage tot de coëfficiënt van x^n telkens wanneer we in de eerste factor de term met x^k vermenigvuldigen met de term met x^{n-k} in de tweede factor. Hierbij is $0 \leq k \leq n$.

Het binomium leert ons dat

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

zodat de bijdrage tot de coëfficiënten van x^n die komt van $x^k x^{n-k}$ gelijk moet zijn aan

$$\binom{n}{k} \times \binom{n}{n-k} = \binom{n}{k}^2$$

We krijgen in totaal als coëfficiënt voor x^n dus $\sum_{k=0}^{n} \binom{n}{k}^2$ □

2.5 Inclusie en exclusie

We weten dat $|A \cup B| = |A| + |B|$ als $A \cap B = \emptyset$. Als $A \cap B = \emptyset$, dan worden de elementen van $A \cap B$ dubbel geteld in $|A| + |B|$ terwijl ze maar 1 keer in $A \cup B$ zitten. Dit kunnen we goedmaken door $|A \cap B|$ af te trekken:

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

Voor drie verzamelingen geldt:

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

Algemeen geldt de volgende:

Stelling 11 (Principe van inclusie en exclusie). Zijn $A_1, A_2, \ldots, A_n$ eindige verzamelingen en stel $A = \{A_1, A_2, \ldots, A_n\}$. Dan hebben we:

$$\left|\bigcup A\right| = |A_1 \cup A_2 \cup \ldots \cup A_n| = \alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{n-1}\alpha_n$$

Met

$$\alpha_i = \sum_{B \in \binom{A}{i}} \left|\bigcap B\right|$$

Bewijs. Zij $x \in \bigcup A$, dan $\exists k \in \mathbb{N}_0$ zodat x behoort tot juist k van de n verzamelingen in A. Dus

levert x een bijdrage	
	k in $\alpha_1 = \lvert A_1 \rvert + \lvert A_2 \rvert + \cdots + \lvert A_n \rvert$
	$\binom{k}{2}$ in α_2
	$\binom{k}{3}$ in α_3
	…
	$\binom{k}{k}$ in α_k
	0 in α_{k+1}
	…
	0 in α_n

In totaal hebben we een bijdrage:

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \cdots + (-1)^{k-1}\binom{k}{k} = 1$$

□

Voorbeeld. In de klas zijn er 73 studenten. 52 spelen piano, 25 viool en 20 uit. 17 spelen piano en viool, 12 spelen piano en uit, 7 viool en uit en 1 enkele speelt alle drie de instrumenten. Hoeveel studenten spelen geen van de 3 instrumenten?

$$\begin{aligned} &73 - \left|A_p \cup A_V \cup A_F\right| = 73 - (53 + 25 + 20 - 17 - 12 - 7 + 1) \\ &= 73 - 62 \\ &= 11. \end{aligned}$$

Hoofdstuk 3: Gehele getallen

Een ring is een abstracte structuur die we op een verzameling leggen, We kunnen dus op die verzameling een bewerking zetten.

Zij R een verzameling voorzien van twee bewerkingen

$$+: R \times R \to R$$
$$\cdot : R \times R \to R$$

die voldoen aan volgende eigenschappen:

- $(R, +)$ is een **abelse** of **commutatieve** groep:
  - De optelling is **associatief**

$$\forall a, b, c \in R: (a + b) + c = a + (b + c)$$

  - De optelling heeft een **neutraal element**

$$\exists n \in R: \forall a \in R: a + n = a = n + a$$

  - Elk element a heeft een **invers** of **symmetrisch element** t.o.v. de optelling (dat we noteren als $-a$)

$$\forall a \in R: \exists b \in R: a + b = n = b + a$$

  - De optelling is **commutatief**

$$\forall a, b \in R: a + b = b + a$$

- $(R, \cdot)$ is een **monoide**:
  - De vermenigvuldiging is associatief

$$\forall a, b, c \in R: (a.b).c = a.(b.c)$$

  - De vermenigvuldiging heeft een neutraal element

$$\exists e \in R: \forall a \in R: a.e = a = e.a$$

- De vermenigvuldiging is **distributief** t.o.v. de optelling

$$\forall a, b, c \in R: \quad a.(b + c) = a.b + a.c$$
$$(a + b).c = a.c + b.c$$

We hebben in de gehele getallen geen inverse voor de vermenigvuldiging, we moeten met breuken kunnen werken om dit te kunnen doen.

We zeggen dat $(R, +, \cdot)$ **een ring met eenheid** is. Wanneer ook de vermenigvuldiging commutatief is, spreken we van **een commutatieve ring met eenheid.**

Notatie. We schrijven $a - b$ voor $a + (-b)$.
$a - b$ is dus kort voor "a plus het symmetrisch element van b".

Eigenschap 5. De symmetrische en neutrale elementen zijn uniek.

Bewijs. Het neutrale element is uniek:
Stel: n_1 en n_2 zijn beide een neutraal element van $(R, +)$

$$\begin{aligned}
&\Rightarrow n_1 = n_1 + n_2 \text{ (want } n_2 \text{ is neutraal element)}\\
&n_1 = n_2 \text{ (want } n_1 \text{ is neutraal element)}\\
&\Rightarrow n_1 \; en \; n_2 \text{ (zijn gelijk)}
\end{aligned}$$

Bewijs. De symmetrische elementen zijn uniek:
Stel: b_1 en b_2 zijn beiden een symmetrische element van a

$$\begin{aligned}
&\Rightarrow a \in R: \exists b_1, b_2 \in R: a + b_1 = n = a + b_2\\
&b_1 = b_1 + n && (n \text{ is neutraal element})\\
&= b_1 + (a + b_2) && (b_2 \text{ is een symmetrisch element van } a)\\
&= (b_1 + a) + b_2 && (+ \text{ is associatief})\\
&= n + b_2 && (b_1 \text{ is en symmetrisch element van } a)\\
&= b_2 && (n \text{ is neutraal element})\\
&\Rightarrow b_1 \text{ en } b_2 \text{ zijn gel ijk}
\end{aligned}$$

Eigenschap 6. $\forall m, n \in R: m - (-n) = m + n$

Bewijs.
Als we bewijzen dat $-(-n) = n$ is het in orde, want $m - (-n) = m + (-(-n))$.
Maar vermits symmetrische elementen uniek zijn is dit duidelijk want $n + (-n) = 0$.

3.1.1 De ring van gehele getallen

De verzameling van alle gehele getallen uitgerust met $+$ en $\cdot$ is een ring met 0 als neutraal element voor de optelling en 1 als neutraal element voor de vermenigvuldiging die we noteren als $(\mathbb{Z}, +, \cdot)$.

3.1.2 Andere voorbeelden van ringen

Veeltermen
De verzameling van veeltermen met reële coëfficiënten en onbekende X is

$$\mathbb{R}[X] := \left\{ \sum_{i=0}^{n} a_1 X^i \mid n \in \mathbb{N}, \forall i \in [0..n]: a_i \in \mathbb{R} \right\}.$$

Op deze verzameling definiëren we een optelling door:

$$\left(\sum_{i=0}^{n} a_i X^i \right) + \left(\sum_{j=0}^{m} b_j X^j \right) = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) X^k$$

waarbij we veronderstellen dat $a_k = 0$ voor $k > n$ en $b_k = 0$ voor $k > m$.
We definiëren ook een vermenigvuldiging door

$$\left(\sum_{i=0}^{n} a_i X^i \right) \cdot \left(\sum_{j=0}^{m} b_j X^j \right) = \sum_{k=0}^{m+n} c_k X^k$$

Waarbij

$$c_k = \sum_{\substack{i\in[0..n]\\ j\in[0...m]\\ i+j=k}} a_i b_j$$

De formule voor c_k drukt gewoon uit dat je de som neemt van alle producten van termen uit de eerste en de tweede veelterm die X^k opleveren.

Met deze definities is $(\mathbb{R}[X], +, \cdot)$ een ring. Analoog zijn ook $(\mathbb{Z}[X], +, \cdot)$ en $(\mathbb{Q}[X], +, \cdot)$ ringen. Verifieer dit zelf als oefening.

Matrices
Een voorbeeld van een niet-commutatieve ring is de verzameling van alle reële $(n \times n)$-matrices, voor een gegeven $n \in \mathbb{N}_0$, met de optelling en de vermenigvuldiging die we gewoon zijn. Verifieer eveneens zelf.

3.2 Welorde

De elementen van $\mathbb{Z}$ zijn ook **geordend** door de relatie ≤. Deze heeft ook enkele goed gekende eigenschappen:

- ≤ **reflexief**

$$\forall a \in \mathbb{Z}: a \leq a$$

- ≤ **antisymmetrisch**

$$\forall a, b \in \mathbb{Z}: (a \leq b) \wedge (b \leq a) \Rightarrow (a = b)$$

- ≤ **transitief**

$$\forall a, b, c \in \mathbb{Z}: (a \leq b) \wedge (b \leq c) \Rightarrow (a \leq c)$$

- Bovendien geldt:

$$\forall a, b, c \in \mathbb{Z}: a \leq b \Rightarrow a + c \leq b + c$$

En

$$\forall a, b \in \mathbb{Z}, \forall c \in \mathbb{N}: a \leq b \Rightarrow a.c \leq b.c$$

Eigenschap 7. Als $a \leq b$, dan $-b \leq -a$.

Bewijs. Trek van beide leden a af. Je krijgt: $0 \leq b - a$. Trek vervolgens van beide leden b af: $-b \leq -a$

Definitie 5. Zij $S \subset \mathbb{Z}$. $x \in \mathbb{Z}$ heet een **ondergrens** van S indien $\forall s \in S: x \leq s.$.
Het infimum van S is de grootste ondergrens van S.

Voorbeeld.

$$s = \{-5, 3, 10, 20\}$$

heeft vele ondergrenzen, bijvoorbeeld $-6, -200, -5, \ldots$ Het infimum is -5.
Merk op dat in dit voorbeeld het infimum van S zelf tot S behoort.

Definitie 6. Indien het infimum van een verzameling S zelf tot S behoort, dan noemen we het een **minimum**.

De volgende bijzondere eigenschap van $\mathbb{Z}$ is in feite een axioma.

Principe van de Welgeordendheid.
Elke niet-lege deelverzameling van $\mathbb{Z}$ die een ondergrens heeft, heeft ook een minimum.

3.3 Bewijs per inductie

Voorbeeld.
Hoe bewijzen we dat $\forall n \in \mathbb{N}_0$ geldt dat

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2?$$

We merken eerst op dat voor $n = 1$, het kleinste element van $\mathbb{N}_0$, de eigenschap waar is:

$$1 = 1^2$$

Dan gaan we ervan uit dat de eigenschap geldt voor $n = k$ en we bewijzen hieruit dat de eigenschap dan ook moet waar zijn voor $n = k + 1$.
Dus nemen we aan dat $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ en dan tonen we aan dat
$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k\ +\ 1)^2$. Gebruikmakend van de aanname, wordt het linkerlid $k^2 + (2k + 1) = k^2 + 2k + 1 = (k + 1)^2$.
Kunnen we uit deze algemene redenering afleiden dat de eigenschap geldt voor alle $n \in \mathbb{N}$?

Principe van Bewijs per Inductie
Zij $P(n)$ een eigenschap die we willen bewijzen voor alle $n \in \mathbb{N}$.

1. **Basis van de inductie.** Zij $P(0)$ waar (of $P(1)$ of $P(n_0)$, met n_0 het kleinste natuurlijke getal waarvoor P zin heeft).
2. Onderstel dat de **inductiehypothese** geldt, i.e. wanneer $P(k)$ waar is voor een willekeurige $k \in \mathbb{N}$, dan is $P(k + 1)$ dat ook (deze stap heet de **inductiestap**).

Dan is $P(n)$ waar voor alle $n \in \mathbb{N}$

Bewijs. Buit het principe van de Welgeordendheid uit.
We moeten tonen dat dit waar is voor alle elementen dat het waar is. We gaan veronderstellen dat het niet zo is en dan willen we tot een contradictie komen en dan weten dat het moet gelden voor allemaal.

Stel dat er een aantal element $n \in \mathbb{N}$ waarvoor $P(n)$ niet waar is:

$$S = \{n \in \mathbb{N} | \neg P(n) \text{ waar}\}$$

Die verzameling is niet leeg, aangezien dat we verondersteld hebben niet voor alle n geldt.

We hebben nu een verzameling S die een deelverzameling is van $\mathbb{N}$ en dit heeft een ondergrens, door het principe van de welgeordendheid die zegt dat die S een minimum m heeft.

We zijn nagegaan met de basis van de inductie $P(0)$ wel waar is, dus 0 kan niet in S zitten, want voor 0 is het waar:

$$0 \notin S$$

En dus moet dat minimum $m \geq 1$.
We weten dat m een minimum is en als we daar 1 van aftrekken, zit het niet meer in S:

$$(m - 1) \notin S$$

Want voor $m-1$ is p waar, uit de inductiestap weten we dat P(m) waar zal zijn, want als we het veronderstellen voor een k kunnen we het veronderstellen voor $k+1$. Dus de $P(m-1)$ is waar, maar de inductiestap verzekert dan dat $P(m)$ ook waar is.
En dat is een tegenspraak met dat de verzameling S niet leeg is, ze is daadwerkelijk leeg en dus moet het voor alle gelden.

Voor een bewijs per inductie, moet je dus de basis en de inductiehypothese verifiëren.

3.4 Quotiënt en rest

Als we 46 delen door 6, weten we dat de deling 'niet opgaat' en dat er een **rest** is van 4 met quotiënt 7. We kunnen dit samenvatten als $46 = 6 \times 7 + 4$ of `46 is een veelvoud van 6 plus 4'. In het algemeen geldt:

Stelling 12. Gegeven $a \in \mathbb{Z}$ en $b \in \mathbb{N}_0$, dan $\exists q, r \in \mathbb{Z}: a = bq + r$ met $0 \leq r < b$.

Bewijs.
Stel:

$$R \coloneqq \{x \in \mathbb{N} \mid \exists y \in \mathbb{Z} : a = by + x\}$$

R is zeker niet leeg, want als a positief is[9] kunnen we als x gewoon a zelf nemen,
dan is $a \in R$ want $a = b \times 0 + a$.

Wat als a negatief is?
Als a negatief is[10] kunnen we als y gewoon a zelf nemen. Dan hebben we $a = ba + (1-b)a$.
Nu moeten we enkel controleren of $(1-b)a$ positief is:

We weten dat $a < 0$ en we weten dat $b \geq 1$ ($b \in \mathbb{N}_0$) dus:

$$1 - b \leq 0$$

$a \times (1-b)$ is dus $\in \mathbb{N}$

Dus als a zowel negatief of positief is vinden we een x, dus de verzameling is niet leeg.
$R \subset \mathbb{N}$ en zo we kunnen als ondergrens 0 nemen, hierdoor weten we dat er een minimum bestaat.
We kunnen dus een kleinste x vinden waarvoor $\exists y \in \mathbb{Z} : a = by + x$ geldt.

Uit het welordeningsprincipe kunnen we besluiten dat R een kleinste element r heeft. Dan geldt:

$$\exists y \in \mathbb{Z} : a = by + r$$

Zodat we $q \coloneqq y$ kunnen nemen.

Nu moeten we aantonen dat dat kleinste element r voldoet aan $0 \leq r < b$.
Door de definitie van R we weten dat r positief is, dus we moeten enkel nog aantonend dat $r < b$.
Dit gaan we aantonen via contradictie, stel dat r niet kleiner is dan b, dus $r \geq b$, dan gaan we werken naar een tegenspraak.

[9] $a \geq 0$
[10] $a < 0$

We veronderstellen dat $r \geq b$, dan is $r - b \geq 0$ en uit:

$$\begin{aligned} & a = by + r \\ \Leftrightarrow\ & a = by + b + (r - b) \\ \Leftrightarrow\ & a = b(y + 1) + (r - b) \end{aligned}$$

$r - b \in R,\ r - b < r$ want b is niet 0, en dat is een contradictie want r was het kleinste element. We hebben een contradictie gemaakt met de veronderstelling $r \geq b$

Stelling 13. r en q in de vorige stelling zijn uniek.

Bewijs. Bewijs uit het ongerijmde. Onderstel dat

$$\exists q \neq q' \in \mathbb{Z}, \exists r \neq r' \in [0..b-1] : bq + r = a = bq' + r'$$

Uit de ordening mogen we onderstellen dat $q' < q$, dus dan is $q - q' \geq 1$.
Dan krijgen we:

$$r' = a - bq'$$

Nu willen we die $q - q' \geq 1$ daar in krijgen, we tellen bq' daar bij op en trekken het weer af.

$$\begin{aligned} r' &= a + bq - bq' \\ r' &= a + b(q - q') \\ r' &= a + b(q - q') - bq \\ r' &= (a - bq) + b(q - q') \end{aligned}$$

$(a - bq) = r$

Dus dan staat er eigenlijk:

$$r' = r + b(q - q')$$

Maar $q - q' \geq 1$, dus we kunnen dat gaan afschatten door te zeggen als we $(q - q')$ vermenigvuldigen met b dan maken we de b gelijk of vergroter.

$$r + b(q - q') \geq r + b$$

Maar $r \geq 0$ dus als we r weglaten krijgen we

$$r' \geq b$$

En dat is een tegenspraak want $r' < b$, onze fout is gekomen door te veronderstellen dat $q' < q$. Als we hadden veronderstel dat $q' > q$ dan zou we op dezelfde manier weer een contradictie. Uiteindelijk moet dus $q' = q$ en dan ook $r = r'$

Een belangrijke toepassing van de vorige stellingen is onze (decimale) schrijfwijze voor getallen. Gegeven een natuurlijk getal x en een `basis' $t \geq 2$, dan kunnen we herhaaldelijk de stelling toepassen:

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

Met elke $r_i \in [0..t-1]$ en $q_n = 0$.

Substitutie van de laatste vergelijking in de voorlaatste enz. geeft:

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

zodat de schrijfwijze voor x in basis t gelijk is aan

$$r_n r_{n-1} \ldots r_1 r_0$$

Notatie. We noteren de schrijfwijze van een getal x in basis t als $(x)_t$.

Voorbeeld. In de informatica werkt men dikwijls in basis 2. Hoe berekenen we $(386)_2$?

386	$=$	193×2	$+$	0
193	$=$	96×2	$+$	1
96	$=$	48×2	$+$	0
48	$=$	24×2	$+$	0
24	$=$	12×2	$+$	0
12	$=$	6×2	$+$	0
6	$=$	3×2	$+$	0
3	$=$	1×2	$+$	1
1	$=$	0×2	$+$	1

Dus $(386)_2 = 110000010$

Definitie 7.
We zeggen dat een geheel getal b een veelvoud is van $a \in \mathbb{Z}$ indien $\exists k \in \mathbb{Z}: b = k \times a$.
We zeggen in dat geval ook dat a het getal b **deelt** en schrijven $a|b$.
Ook zeggen we dat a een **factor** of een **deler** is van b of dat b deelbaar is door a.
Als $a \neq 0$, noteren we het getal $k \in \mathbb{Z}$ waarvoor $b = k \times a$ met $\frac{b}{a}$. Natuurlijk bestaat $\frac{b}{a}$ voor elke keuze $b \in \mathbb{Z}, a \in \mathbb{Z}_0$ maar in het algemeen behoort $\frac{b}{a}$ tot $\mathbb{Q}$ en niet tot $\mathbb{Z}$. Enkel als $a|b$ hebben we $\frac{b}{a} \in \mathbb{Z}$

Eigenschap 8.
Zij $n, d, c \in \mathbb{Z}$ met $c \neq 0 \neq d$. Er geldt:

$$d \mid n \wedge c \mid \frac{n}{d} \Rightarrow c \mid n \wedge d \mid \frac{n}{c}$$ [11]

Bewijs.

$$\begin{aligned} & d \mid n \\ \Leftrightarrow\ & \exists k \in \mathbb{Z}: n = k \times d \\ \Leftrightarrow\ & \exists k \in \mathbb{Z}: k = \frac{n}{d} \end{aligned}$$

En

$$\begin{aligned} & c \mid \frac{n}{d} \\ \Leftrightarrow\ & c \mid k \\ \Leftrightarrow\ & \exists l \in \mathbb{Z}: k = l \times c \end{aligned}$$

[11] Als d een deler is van n en c is een deler van $\frac{n}{d}$, $\frac{n}{d}$ zit in $\mathbb{Z}$ want d is een deler van n, dus dan kunnen we zeggen dat c ook een deler is van n en dat d op zijn beurt ook een deler moet zijn van c

Bijgevolg is:

$$n = l \times c \times d$$

en dus volgt:

$$c \mid n$$

En aangezien:

$$\frac{n}{c} = l \times d$$

volgt ook:

$$d \mid \frac{n}{c}$$

3.5 Grootste gemene deler

Definitie 8. Stel $a, b \in \mathbb{Z}$. Een geheel getal d heet een **grootste gemene deler (ggd)** van a en b indien $d|a$ en $d|b$ (gemene deler) en $\forall c \in \mathbb{Z}: c \mid a \ \wedge \ c \mid b \Rightarrow c \mid d$ (grootste).

Voorbeeld. 6

$$6 \mid 60 \text{ en } 6 \mid 84$$

maar toch is 6 geen ggd van 60 en 84, want $12 \mid 60$ en $12 \mid 84$ maar $12 \nmid 6$.

Opmerking. Als d een ggd is, is ook $-d$ een ggd. We hebben:

Eigenschap 9. Zijn $d \neq d'$ grootste gemene delers van a en b. Dan geldt:

$$d = -d'$$

Bewijs. Dit volgt uit $d \mid d'$ en $d' \mid d$.

Definitie 9. De grootste gemene deler van a en b is de **unieke positieve grootste gemene deler** van a en b. We noteren hem $ggd(a, b)$.

Hoe berekenen we nu $ggd(a, b)$? Hiervoor hebben we nog volgende eigenschap nodig:

Eigenschap 10. Stel $a = bq + r$. Dan is $ggd(a, b) = ggd(b, r)$.

Bewijs.
We moeten aantonen dat de grootste gemene deler van a en b ook dezelfde is als die van b en r:

Stel:

$$d \mid a \text{ en } d \mid b$$

Dan zal ook:

$$d \mid (a - bq)$$

Want

$$a = bq + r$$
$$\Leftrightarrow a - bq = r$$

Waardoor dus d ook een deler zal zijn van r. Dit betekend enkel dat d gemene deler is!
Dus $d \mid b$ en $d \mid r$.

Omgekeerd als:

$$d \mid b \; en \; d \mid r$$

Dan volgt:

$$d \mid (bq + r)$$

Zodat

$$d \mid ggd(a, d)$$

Voorbeeld. We bepalen $ggd(2406, 654)$. We passen hiervoor de voorgaande eigenschap herhaaldelijk toe:

$$\begin{array}{ccccccc} 2406 & = & 654 \times 3 + 444 & \Rightarrow & ggd(2406{,}654) & = & ggd(654, 444) \\ 654 & = & 444 \times 1 \; + 210 & \Rightarrow & ggd(654{,}444) & = & ggd(400, 210) \\ 444 & = & 210 \times 2 + 24 & \Rightarrow & ggd(444{,}210) & = & ggd(210, 24) \\ 210 & = & 24 \times 8 + 18 & \Rightarrow & ggd(210{,}24) & = & ggd(24, 18) \\ 24 & = & 18 \times 1 + 6 & \Rightarrow & ggd(24{,}18) & = & ggd(18, 6) \\ 18 & = & 6 \times 3 + 0 & \Rightarrow & ggd(18{,}6) & = & 0 \end{array}$$

Algemeen: als we hebben

$$\begin{array}{ccccc} a & = & Bq_1 + r_1 & met & 0 \leq r_1 < b \\ b & = & r_1 q_2 + r_2 & met & 0 \leq r_2 < r_1 \\ r_1 & = & r_2 q_3 + r_3 & met & 0 \leq r_3 < r_2 \\ & \ldots & & \ldots & \\ r_{k-4} & = & r_{k-3} q_{k-2} + r_{k-2} & met & 0 \leq r_{k-2} < r_{k-3} \\ r_{k-3} & = & r_{k-2} q_{k-1} + r_{k-1} & met & 0 \leq r_{k-1} < r_{k-2} \\ r_{k-2} & = & r_{k-1} q_k + 0 & met & \end{array}$$

dan is

$$\begin{aligned} & ggd(a, b) = ggd(r_{k-2}, r_{k-1}) \\ & = r_{k-1} \\ & = \text{de laatste niet-nulle rest} \end{aligned}$$

Dit algoritme heet het **Euclidisch algoritme.**

Stelling 14 (Bézout). Stel $a, b \in \mathbb{Z}, b \geq 0$ met $d = ggd(a, b)$, dan
$\exists m, n \in \mathbb{Z}: d = ma + nb$. Ook is d het kleinste natuurlijk getal waarvoor dit kan.

Voorbeeld.

$$d = 6, \qquad a = 2046, \qquad b = 654$$

$$\begin{aligned} & ggd(2046{,}654) = 6 \\ & 6 = 28 \times 2406 - 103 \times 654 \end{aligned}$$

Bewijs.
Voor $b = 0$ is de stelling triviaal.

Als $b \neq 0$ dan lezen we het resultaat van het euclidisch algoritme van achter naar voor:

$$d = r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$$

Dus $d = m'r_{k-2} + n'r_{k-3}$, met $m' = -q_{k-1}$ en $n' = 1$.
Nu substitueren we $r_{k-2} = r_{k-4} - r_{k-3}q_{k-2}$ zodat

$$\begin{aligned} d &= m'(r_{k-4} - r_{k-3}q_{k-2}) + n'r_{k-3} \\ &= (-m'q_{k-2} + n')r_{k-3} + m'r_{k-4} \\ &= m''r_{k-3} + n''r_{k-4} \end{aligned}$$

Daarin substitueren we $r_{k-3} = r_{k-5} - r_{k-5}q_{k-3}$ enz. Uiteindelijk vinden we

$$d = m^{(k-3)}r_2 + n^{(k-3)}r_1$$

Waaruit, via substituties $r_2 = b - r_1q_2$ en $r_1 = a - bq_1$:

$$\begin{aligned} d &= m^{(k-3)}(b - r_1q_2) + n^{(k-3)}r_1 \\ &= \left(-m^{(k-3)}q_2 + n^{(k-3)}\right)r_1 + m^{(k-3)}b \\ &= m^{(k-2)}r_1 + n^{(k-2)}b \\ &= m^{(k-2)}(a - bq_1) + n^{(k-2)}b \\ &= \left(-m^{(k-2)}q_1 + n^{(k-2)}\right)b + m^{(k-2)}a \\ &= mb + na \end{aligned}$$

Bewijs als oefening dat er geen kleiner getal $d' > 0$ bestaat waarvoor $\exists n', m' \in \mathbb{Z}$: $d' = m'a + n'b$.

Voorbeeld. We passen de stelling van Bézout toe op het vorige voorbeeld:

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (210 - 8 \times 24) = 9 \times 24 - 210 \\ &= 9 \times (444 - 2 \times 210) - 210 = 9 \times 444 - 19 \times 210 \\ &= 9 \times 444 - 19 \times (654 - 444) = 28 \times 444 - 19 \times 654 \\ &= 28 \times (2406 - 3 \times 654) - 19 \times 654 = 28 \times 2406 - 103 \times 654 \end{aligned}$$

Uit vorige stelling volgt onmiddellijk dat alle veelvouden van $ggd(a, b)$ te schrijven zijn als $ma + nb$ voor zekere $m, n \in \mathbb{Z}$.

Gevolg 3. Zij a en b gehele getallen. Enkel veelvouden van $ggd(a,b)$ zijn te schrijven als $ma+nb$.

Bewijs.
Schrijf $d = ggd(a,b) = ma+nb$, uit vorige stelling, en veronderstel even dat een ander geheel getal x met $d \nmid x$ kan geschreven worden als $m'a+n'b$.

Vermits x geen veelvoud is van d, hebben we $x = kd+q$, met $0 < q < d$.

Maar dan is

$$\begin{aligned} q &= x - kd \\ q &= m'a + n'b - kd \\ q &= m'a + n'b - k(ma+nb) \\ q &= m'a + n'b - kma - knb \\ q &= (m' - km)a + (n' - kn)b \end{aligned}$$

Een getal kleiner dan d dat te schrijven is als $ra+sb$, tegenspraak.

Definitie 10. $a, b \in \mathbb{Z}$ heten **relatief priem** indien $ggd(a,b) = 1$.

Eigenschap 11. $ggd(a,b) = 1 \Rightarrow \exists m,n \in \mathbb{Z}: ma+nb = 1$.

Het belangrijkste gevolg van Bézout:
Gevolg 4. Als a en b relatief priem zijn, kan elk geheel getal geschreven worden als $ma+nb$.

Bewijs. Vermits alle getallen veelvouden zijn van $1 = ggd(a,b)$, volgt dit uit voorgaande eigenschap.

Eigenschap 12. Een positief rationaal getal heeft een unieke schrijfwijze als $\frac{a}{b}$ met a en b relatief priem en positief.

Bewijs.
Stel dat we twee verschillende schrijfwijzen hebben:

$$\frac{a}{b} \; en \frac{a'}{b'} \; met \; ggd(a,b) = 1 = \; ggd(a',b')$$

Dan is:

$$ab' = a'b$$

Maar

$$\begin{aligned} b' &= 1 \times b' \\ b' &= (ma+nb)b' \\ b' &= (mab' + nbb'' \\ b' &= ma'b + nb'b \\ b' &= (ma' + nb')b \end{aligned}$$

Dus $b \mid b'$. analoog geldt $b' \mid b$ zodat $b = b'$ en $a = a'$

3.6 Priemgetallen

De definitie kennen we allemaal: een priemgetal is een natuurlijk getal met juist twee verschillende positieve delers. Dus een getal $m \geq 2$ is niet priem als en slechts als we $m = m_1 m_2$ kunnen schrijven met $1 < m_1, m_2 < m$.

Opmerking. 1 is geen priemgetal.

Priemgetallen hebben zeer veel toepassingen. Een van de meest gebruikte is het `ontbinden in priemfactoren' om een getal beter te leren kennen, b.v. $825 = 3 \times 52 \times 11$. Als gevolg van de welordeningseigenschap van $\mathbb{Z}$, hebben we volgend gekend resultaat.

Stelling 15. Elk natuurlijk getal groter dan 1 een ontbinding heeft in priemfactoren.

Bewijs.
Veronderstel even dat er minstens 1 getal is zonder factorisatie in priemgetallen.
Dan is de verzameling A van alle getallen zonder factorisatie een niet-leeg deel van $\mathbb{N}$.

Bijgevolg heeft A een minimum m. Indien m een priemgetal is, heeft m een triviale priemontbinding. Dus moet $m = m_1 m_2 \; met \; m_1, m_2 \in [2..m-1]$. Maar vermits m het kleinste element is van A, zullen m_1 en m_2 niet tot A behoren.

Bijgevolg zijn deze getallen ontbindbaar. Maar als we deze twee ontbindingen naast elkaar schrijven, hebben we een ontbinding van m. Dit is in tegenspraak met $m \in A$.

Opmerking. Hoewel we eenvoudig kunnen aantonen dat elk getal ontbindbaar is in priemfactoren, is het vinden van zulke ontbinding helemaal niet voor de hand liggend. Er bestaan momenteel geen efficiënte algoritmen voor het vinden van priemfactorisaties.

We zullen nu aantonen dat de ontbinding van een gegeven getal uniek is (op de volgorde van de priemfactoren na). Eerst een hulpstelling:

Stelling 16. Zij p een priemgetal. Indien p een product $x_1 x_2 \ldots x_n$ deelt, moet p één van de factoren delen.

Bewijs. Door inductie op het aantal factoren van $x_1 x_2 \ldots x_n$ (deze factoren hoeven natuurlijk niet priem te zijn).

- $n = 1$ OK, triviaal
- $n = k \Rightarrow n = k + 1$

Onderstel dat $p \mid x_1 x_2 \ \ldots \ x_k x_{k+1}$ en stel $x := x_1 x_2 \ldots x_k$. Dan hebben we $p \mid x \times x_{k+1}$

Indien $p \mid x$, hebben we door de inductiehypothese dat $\exists i \in [k]: p \mid x_i$
Indien $p \nmid x$, weten we dat $ggd(p, \ x) = 1$ omdat p priem is en dus maar twee delers heeft en p niet de ggd kan zijn.
De stelling van Bézout levert $m, \ n \in Z$ zodat $1 = mp \ + \ nx$. Dan geldt:

$$\begin{aligned} x_{k+1} &= 1 \times x_{k+1} \\ &= (mp + nx) x_{k+1} \\ &= mpx_{k+1} + nxx_{k+1} \end{aligned}$$

Vermits $p \mid mpx_{k+1}$ en $p \mid nxx_{k+1}$ (omdat $p \mid xx_{k+1}$), moet $p \mid x_{k+1}$

Stelling 17. Een natuurlijk getal $n \geq 2$ heeft een unieke ontbinding in priemfactoren (op de volgorde van de factoren na).

Bewijs.
Als de stelling niet waar zou zijn, is er door de welordeningseigenschap, een kleinste getal n met 2 verschillende ontbindingen[12]:

$$p_1 p_2 \dots p_k = n = p_1' p_2' \dots p_l'$$

Met p_i en p_j' (niet noodzakelijk verschillende) priemgetallen voor $i \in [k]$ en $j \in [l]$.

Uit $n = p_1 p_2 \dots p_k$ leiden we af dat $p_1 \mid n$ en dus $p_1 \mid p_1' p_2' \dots p_l'$.
De vorige stelling zegt dan dat $\exists j \in [l]: p_1 \mid p_j'$.

Maar vermits p_1 en p_j' beide priemgetallen zijn (en 1 geen priemgetal is) wil dit zeggen dat $p_j' = p_1$
Voor de eenvoud hernummeren we de priemfactoren $p_1', p_2', \dots, p_l'$ zodanig dat de nieuwe $p_1' = p_1$.

Dan hebben we

$$\cancel{p_1} p_2 \dots p_k = \cancel{p_1} p_2' \dots p_l'$$

zodat

$$p_2 \dots p_k = p_2' \dots p_l'$$

Het geen een tegen spraak is, want dan zou $p_2 \dots p_k$ een getal kleiner zijn dan n met twee verschillende ontbindingen.

Notatie. Meestal groeperen we gelijke factoren in de priemontbinding van een getal $n \in \mathbb{N}$.
In het algemeen noteren we dus een priemontbinding als

$$n = p_1^{l_1} p_2^{l_1} \dots p_k^{l_k}$$

Met $p_1, p_2, \dots, p_k$ verschillende priemgetallen en $l_1, l_2, \dots, l_k \in \mathbb{N}_0$

[12] We maken opnieuw een verzameling van al die getallen die niet een unieke priemontbinding hebben, als we veronderstellen dat de stellen niet waar is, dan is die verzameling niet leeg, door de welorde krijgen we een kleinste getal waarvoor we twee verschillende priemontbindingen hebben.

Toepassing. Zijn m, n niet-nulle natuurlijke getallen, dan geldt $m^2 \neq 2n^2$.

Bewijs.
Als $m = 1$ of $n = 1$ is de stelling duidelijk.
We nemen dus $m, n \geq 2$.
Bekijken we de priemontbinding van m en n:

$$m = 2^x h \text{ en } n = 2^y k \text{ met } x, y \in \mathbb{N} \text{ en } h, k \text{ oneven}$$

(het zijn de producten van de priemfactoren $\neq 2$).

Dan is de priemontbinding:

$$m^2 = 2^{2x} h^2$$

en

$$2n^2 = 2 \times (2^y \times k)^2 = 2 \times (2^{2y} \times k^2) = 2 \times 2^{2y} \times k^2 = 2^{2y+1} k^2$$

Als deze ontbindingen gelijk zouden zijn, krijgen we dus als die 2 getallen gelijk zijn, de twee priemontbindingen ook gelijk moeten zijn. Maar alle factoren 2 zitten in:

$$m^2 = 2^{2x} h^2$$

En

$$2n^2 = 2^{2y+1} k^2$$

En die twee kunnen nooit gelijk zijn, een even exponenten zal nooit gelijk zijn aan het oneven exponent.

Een gevolg is dat $\forall m, n \in \mathbb{N}_0 : \left(\frac{m}{n}\right)^2 \neq 2$, nog een bewijs dat $\sqrt{2} \notin \mathbb{Q}$

Soms lezen we in de krant dat het `grootste priemgetal' is ontdekt. Dit is fout geformuleerd. Eigenlijk bedoelt men `het grootste getal waarvan men tot nu toe zeker is dat het een priemgetal is'. Immers:

Stelling 18. Er zijn oneindig veel priemgetallen.

Bewijs. Veronderstel dat er maar $n \in \mathbb{N}$ priemgetallen $p_1, p_2, \ldots, p_n$ zijn.
Beschouw het getal:

$$m = p_1 p_2 \ldots p_n + 1$$

Voor elke priemgetallen $p_i (i \in [n])$ is $m - 1$ een veelvoud van p_i dus $\forall i \in [n] : p_i \nmid m$.
maar m is een natuurlijk getal en heeft unieke een priemontbinding, maar geen enkele van de zo gezegde allemaal bestaande priemgetallen is een priemfactor , dan moeten er nog andere priemgetallen bestaan om die priemontbinding van m te garanderen en dat is een contradictie met dat er maar n priemgetallen zouden bestaan.

Definitie 11. Voor twee niet-nulle natuurlijke getallen m en n definiëren we het **kleinste gemeen veelvoud** van m en n als het kleinste niet-nul natuurlijk getal dat een veelvoud is van zowel m als n. We noteren dit getal $kgv(m, n)$. We hebben dus dat elk gemeen veelvoud van m en n deelbaar is door $kgv(m, n)$.

Lemma 1. Zij m en n niet-nulle natuurlijke getallen en zij $P = \{p_1, p_2, \dots, p_k\}$ de verzameling van alle priemgetallen die m of n delen. Dan hebben we

$$m = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} \quad \text{en} \quad n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$

Voor een zekere natuurlijke getallen $m_1, m_2, \dots, m_k$ en $n_1, n_2, \dots, n_k$

Er geldt:

$$ggd(m,n) = \prod_{i=1}^{k} p_i^{\min\{m_i, n_i\}}$$

En

$$kgv(m,n) = \prod_{i=1}^{k} p_i^{\max\{m_i, n_i\}}$$

Voorbeeld.

$$m = 10, \qquad n = 49, \qquad p = \{2,5,7\}$$

Er geldt:

$$ggd(m,n) = \prod_{i=1}^{k} p_i^{\min\{m_i, n_i\}}$$

$$ggd(10,49) = 2^0 \times 5^0 \times 7^0 = 1 \times 1 \times 1 = 1$$

$$\text{want} \Rightarrow \begin{matrix} 10 = 2^1 \times 5^1 \times 7^0 \\ 49 = 2^0 \times 5^0 \times 7^2 \end{matrix}$$

Er geldt:

$$kgv(m,n) = \prod_{i=1}^{k} p_i^{\max\{m_i, n_i\}}$$

$$kvg(10,49) = 2^1 \times 5^1 \times 7^2 = 490$$

$$\text{want} \Rightarrow \begin{matrix} 10 = 2^1 \times 5^1 \times 7^0 \\ 49 = 2^0 \times 5^0 \times 7^2 \end{matrix}$$

Bewijs.

Zij c een gemeenschappelijke deler van m en n. Dan moet elk priemgetal dat c deelt zeker behoren tot P. Dus geldt

$$c = \prod_{i=1}^{k} p_i^{c_i}$$

Met voor elke $i \in [k], c_i \leq m_i$ en $c_i \leq n_i$ Bovendien levert elke keuze van $c_i \in \mathbb{N}$ binnen deze beperkingen een gemeenschappelijke deler van m en n. Hieruit volgt nu gemakkelijk dat de grootste gemeenschappelijke deler moet gelijk zijn aan $\prod_{i=1}^{k} p_i^{\min\{m_i, n_i\}}$.

Het is ook duidelijk dat elk gemeenschappelijk veelvoud van m en n deelbaar moet zijn door $p_i^{\max\{m_i, n_i\}}$ voor elke $i \in [k]$. Het kleinste zulk veelvoud is juist $\prod_{i=1}^{k} p_i^{\max\{m_i, n_i\}}$

Gevolg 5. Voor niet-nulle natuurlijke getallen n en m geldt steeds:

$$ggd(m,n) \times kgv(m,n) = m \times n$$

Voorbeeld.
Als:

$$m = 10, n = 49 \text{ dan is } P = \{2,5,7\}$$

$$10 \times 49 = 490$$

$$\begin{matrix} ggd(10,49) = 1 \\ kgv(10,49) = 490 \end{matrix} = 490$$

En:

$$\begin{matrix} \prod_{i=1}^{k} p_i^{\min\{m_i,n_i\}} = 2^0 \times 5^0 \times 7^0 = 1 \\ \prod_{i=1}^{k} p_i^{\max\{m_i,n_i\}} = 2^1 \times 5^1 \times 7^2 = 490 \end{matrix} = 490$$

En

$$\prod_{i=1}^{k} p_i^{m_i+n_i} = 2^{1+0} \times 5^{1+0} \times 7^{2+0} = 490 = 1 \times 490$$

Bewijs. Merk op dat $min\{m_i, n_i\} = m_i$ impliceert dat $max\{m_i, n_i\} = n_i$ en omgekeerd.
Dus volgt uit vorig lemma dat:

$$ggd(m,n) \times kgv(m,n) = \prod_{i=1}^{k} p_i^{\min\{m_i,n_i\}} \times \prod_{i=1}^{k} p_i^{\max\{m_i,n_i\}} = \prod_{i=1}^{k} p_i^{m_i+n_i} = m \times n$$

Gevolg 6. Voor niet-nulle natuurlijke getallen n en m zijn $\frac{m}{ggd(m,n)}$ en $\frac{n}{ggd(m,n)}$ steeds relatief priem.

Voorbeeld.

$$m = 10, n = 49 \text{ dan is } P = \{2,5,7\}$$

$$\frac{m}{ggd(m,n)} = \prod_{i=1}^{k} p_i^{m_i - \min\{m_i,n_i\}}$$

$$\Leftrightarrow \frac{10}{1} = 2^{1-0} \times 5^{1-0} \times 7^{0-0} \text{ want} \Rightarrow \begin{matrix} 10 = 2^1 \times 5^1 \times 7^0 \\ 49 = 2^0 \times 5^0 \times 7^2 \end{matrix}$$

$$\Leftrightarrow 10 = 10$$

En:

$$\frac{n}{ggd(m,n)} = \prod_{i=1}^{k} p_i^{n_i - \min\{m_i,n_i\}}$$

$$\Leftrightarrow \frac{49}{1} = 2^{0-0} \times 5^{0-0} \times 7^{2-0} \text{ want} \Rightarrow \begin{matrix} 10 = 2^1 \times 5^1 \times 7^0 \\ 49 = 2^0 \times 5^0 \times 7^2 \end{matrix}$$

$$\Leftrightarrow 49 = 49$$

Bewijs.

Rekening houdend met $ggd(m,n) = \prod_{i=1}^{k} p_i^{\min\{m_i,n_i\}}$, zien we dat:

$$\frac{m}{ggd(m,n)} = \prod_{i=1}^{k} p_i^{\mathrm{m_i}-\min\{m_i,n_i\}}$$

En dat:

$$\frac{n}{ggd(m,n)} = \prod_{i=1}^{k} p_i^{\mathrm{n_i}-\min\{m_i,n_i\}}$$

Bovendien is voor elke $i \in [k]$ het minimum van $\{m_i, n_i\}$ gelijk aan m_i of n_i zodat voor elke $i \in [k]$ minstens één van de exponenten $\mathrm{m_i} - \min\{m_i, n_i\}$ of $\mathrm{n_i} - \min\{m_i, n_i\}$ moet gelijk zijn aan nul. Dit betekent dat de priemfactor p_i niet voorkomt in de ontbinding van respectievelijk $\frac{m}{ggd(m,n)}$ of $\frac{n}{ggd(m,n)}$ Hierdoor hebben deze twee getallen geen enkele priemfactor gemeenschappelijk.

3.7 De φ-functie van Euler

Definitie 12. Voor een $n \in \mathbb{N}_0$ definiëren we $\varphi(n)$ als het aantal getallen in $[n]$ die relatief priem zijn met n

Laten we een kleine tabel maken voor de eerste 8 positieve natuurlijke getallen.

n	1	2	3	4	5	6	7	8
$\varphi(n)$	1	1	2	2	4	2	6	4

We merken op: voor p priem is $\varphi(p) = p - 1$. Laten we $\varphi(12)$ berekenen. We krijgen $\varphi(12) = 4$. Als we de som nemen van $\varphi(d)$ voor alle delers d van 12 krijgen we:

$$\begin{aligned}&\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = \\ &1 \quad + \quad 1 \quad + \quad 2 \quad + \quad 2 \quad + \quad 2 \quad + \quad 4 \quad = 12\end{aligned}$$

Dus als we bijvoorbeeld $\varphi(12)$ willen berekenen en we weten alle φ van 1 tot 6:

$$\begin{aligned}&12 - \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) = \varphi(12)\\ &12 - 8 = 4\end{aligned}$$

Dus als we bijvoorbeeld $\varphi(6)$ willen berekenen en we weten alle φ van 1 tot 4:

$$\begin{aligned}&6 - \varphi(1) + \varphi(2) + \varphi(3) = \varphi(6)\\ &6 - 4 = 2\end{aligned}$$

Algemeen hebben we

Stelling 19.

$$\forall n \in \mathbb{N}_0 : \sum_{d \mid n} \varphi(d) = n$$

Bewijs.
Stel

$$S \coloneqq \{(d, f) |\ d \mid n, f \in [d], ggd(d, f) = 1\}^{13}$$

We sommen dus alle delers op, en bij elke delers zetten we de getallen die relatief priem zijn met die deler.

Hoeveel koppels hebben we dan?
We kunnen sommeren over alle delers d van n, en dan moet we nog alle f-en gaan tellen die relatief priem zijn met d.

Formeel:

$$|S| = \sum_{d|n} |\{f|(d, f) \in S\}|$$
$$= \sum_{d|n} \varphi(d).$$

We bewijzen nu $|S| = n$ door een bijectie $\beta : S \to [n]$ te construeren. Stel

$$\beta(d, f) \coloneqq f \times \frac{n}{d},$$

Wat altijd een getal uit $[n]$ is (zie definitie van S). Nu is β injectief omdat

$$\beta(d, f) = \beta(d', f')$$
$$\Leftrightarrow f \times \frac{n}{d} = f' \times \frac{n}{d'}$$
$$\Leftrightarrow \frac{f}{d} = \frac{f'}{d'}$$

met $ggd(f, d) = ggd(f', d') = 1$. Uit Eigenschap 12[14] volgt dan $f' = f$ en $d' = d$.

β is ook surjectief. Zij immers $x \in [n]$ en stel

$$d_x = \frac{n}{ggd(n,x)} \in \mathbb{N} \text{ en } f_x = \frac{x}{ggd(n,x)} \in \mathbb{N}$$

Dan is $f_x \leq d_x$ (omdat $x \leq n$) en $ggd(d_x, f_x) = 1$ (wegens Gevolg 6). Nu geldt ook

$$\beta(d_x, f_x) = f_x \times \frac{n}{d_x} = \frac{x}{ggd(x,n)} \times n \times \frac{ggd(x,n)}{n} = x$$

We kunnen ook een expliciete formule bekomen voor $\varphi(n)$, indien we de priemontbinding van n kennen. Laat ons bijvoorbeeld $\varphi(60)$ berekenen. We weten dat $60 = 2^2 \times 3 \times 5$.

[13] Verzameling koppels (d, f), waarbij d steeds een deler is van n en f een element is van de verzameling $[1 \ldots d]$ en relatief priem is met d

[14] Als we twee rationale getallen hebben die gelijk zijn maar waar de tellen er noemer relatief priem zijn, dan zijn die gelijk.

We zoeken de getallen $f \in [60]$ met $ggd(f, 60) = 1$. Dit zijn juist alle getallen in $[60]$ die geen (priem)factor gemeenschappelijk hebben met 60.

De getallen die wegvallen zijn dus alle veelvouden van 2, van 3 en van 5 tussen 1 en 60.
Maar er zijn natuurlijk getallen die tegelijk een veelvoud zijn van 2 en van 3.
We hebben hier een typisch probleem van inclusie en exclusie.

Noteer $A_d \coloneqq \{x \in [60] |\ d\ |x\}$ Dan is

$$\begin{aligned}
&\varphi(60) = 60 - |A_2 \cup A_3 \cup A_5| \\
&= 60 - (|\mathrm{A}_2| + |\mathrm{A}_3| + |\mathrm{A}_5| - |\mathrm{A}_2 \cap \mathrm{A}_3| - |\mathrm{A}_2 \cap \mathrm{A}_5| - |\mathrm{A}_3 \cap \mathrm{A}_5| + |\mathrm{A}_2 \cap \mathrm{A}_3 \cap \mathrm{A}_5|) \\
&= 60 - (|\mathrm{A}_2| + |\mathrm{A}_3| + |\mathrm{A}_5| - |A_6| - |A_{10}| - |A_{15}| + |A_{30}|) \\
&= 60 - (30 + 20 + 12 - 10 - 6 + 2) \\
&= 16
\end{aligned}$$

Algemeen bewijzen we:

Stelling 20. Zij $n \geq 2$ met als ontbinding in priemfactoren $n = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$, dan geldt:

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_1}\right) \times \dots \times \left(1 - \frac{1}{p_k}\right)$$

Bewijs.
We stellen weer voor $d \mid n$:
$A_d \coloneqq \{x \in [n] |\ d \mid x\} = \left\{kd \mid k \in \left[\frac{n}{d}\right]\right\}$ zodat $|A_d| = \frac{n}{d}$

$$\begin{aligned}
\varphi(n) &= n - \left|A_{p_1} \cup A_{p_2} \cup \dots \cup A_{p_k}\right| \\
&= n - \left(\alpha_1 - \alpha_2 + \alpha_3 - \dots + (-1)^{k-1} \alpha_k\right)
\end{aligned}$$

Met

$$\alpha_i = \sum_{\substack{\{j_1, j_2, \dots, j_i\} \\ \in \binom{[k]}{i}}} \left|A_{p_{j_1}} \cup A_{p_{j_2}} \cup \dots \cup A_{p_{j_i}}\right|$$

De som van de cardinaliteiten van elle doorsnedes van i van de k verzamelingen.

Dit kunnen we nog schrijven als:

$$\begin{aligned}
\alpha_i &= \sum_{\substack{\{j_1, j_2, \dots, j_i\} \\ \in \binom{[k]}{i}}} \left|A_{p_{j_1} p_{j_2} \dots p_{j_i}}\right| \\
&= \sum_{\substack{\{j_1, j_2, \dots, j_i\} \\ \in \binom{[k]}{i}}} \frac{n}{p_{j_1} p_{j_2} \dots p_{j_i}} \\
&= n \times \sum_{\substack{\{j_1, j_2, \dots, j_i\} \\ \in \binom{[k]}{i}}} \frac{1}{p_{j_1} p_{j_2} \dots p_{j_i}}
\end{aligned}$$

Dus

$$\varphi(n) = n - \left(n\left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k}\right) - n\left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdots\right) + \cdots + (-1)^{k-1} n\left(\frac{1}{p_1 p_2 \ldots p_k}\right)\right)$$
$$= n\left(1 - \frac{1}{p_1}\right) \times \left(1 - \frac{1}{p_2}\right) \times \ldots \times \left(1 - \frac{1}{p_k}\right)$$

3.8 Equivalentierelaties en partities

Definitie 13. Een relatie $R \subset X \times X$ is een **equivalentierelatie** als ze

1. Reflexief is:

$$\forall x \in X: xRx$$

2. Symmetrisch is:

$$\forall x, y \in X: xRy \Leftrightarrow yRx$$

3. Transitief is:

$$\forall x, y, z \in X: xRy \wedge yRz \Rightarrow xRz$$

Voorbeeld:
Zij R de relatie op de verzameling reëel getallen zodat $aRb \Leftrightarrow a - b$ een geheel getal is.

Is R een equivalentierelatie?

1. Reflexief?

$$aRa \Rightarrow a - a \in \mathbb{Z}, \text{want } a - a = 0 \in \mathbb{Z}$$

2. Symmetrisch?

$$aRb \Rightarrow bRa$$

Is $a - b \in \mathbb{Z} \Rightarrow b - a \in \mathbb{Z}$?
laten we zeggen dat $a - b = c \in \mathbb{Z}$, twee gehele getallen aftrekken is weer een geheel getal.
Dan is $b - a = -c$ het tegengestelde van een $\in \mathbb{Z}$ is ook $\in \mathbb{Z}$.

3. Transitief is:

$$\underbrace{(aRb)}_{a-b} \wedge \underbrace{(bRc)}_{b-c} \Rightarrow aRc$$

$$a - c = (a - b) + (b - x)$$
$$a - c = a - c$$

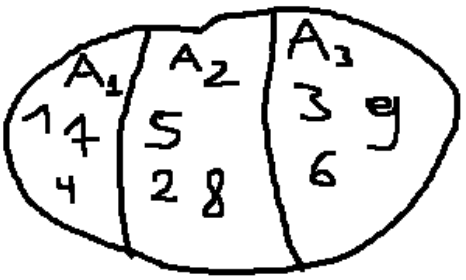
Is dit een geheel getal?
Ja, want een geheel getal optellen met een andere geheel getal is een geheel getal.

Definitie 14. Gegeven een verzameling V, definiëren we een **partitie** van V als een verzameling A van deelverzamelingen van V die voldoen aan volgende twee voorwaarden:

- **(P1)** $\forall A \neq B \in A: A \cap B = \emptyset$
- **(P2)** $\bigcup A = V$

Voorbeeld. $mod\ 3$
$S = \{1,2,3,4,5,6,7,8,9\}$ als $x, y \in S$ dan:

1. $x_i \neq \emptyset$
2. $x \cap y = \neq \emptyset$
3. $\bigcup x_i = S$



Want $mod3 =$

$0 = \{3,6,9\}$
$1 = \{1,4,7\}$
$2 = \{2,5,8\}$

Stelling 21. Een equivalentierelatie geeft steeds aanleiding tot een partitie.
Bewijs.
Stel voor $x \in X$

$$E_x \coloneqq \{y \in X \mid yRx\}$$

E_x heet de **equivalentieklasse** van x en x zelf heet **representant**.
Dan is $\varepsilon = \{E_x \mid x \in X\}$ een partitie. Inderdaad,

- **(P2)** is voldaan omdat $\forall x \in X: E_x \subset X$, zodat $\varepsilon \subset X$ maar bovendien geeft de reflexiviteit van R dat $\forall x \in X: x \in E_x$ zodat $X \subset \varepsilon$.
- **(P1)** is ook voldaan. We bewijzen dat $E_x \cap E_y \neq \emptyset \Rightarrow E_x = E_y$ zij namelijk $z \in E_x \cap E_y$ Dan xRz en yRz en bijgevolg xRy zodat $x \in E_y$. De transitiviteit toont aan dat $E_x \subset E_y$. Ook $y \in E_x$ zodat $E_y \subset E_x$

Stelling 22. elke partitie van een verzameling X aanleiding tot een equivalentierelatie.
Bewijs.
Zij A een partitie van X. Definieer, voor $x, y \in X$:

$$xRy \Leftrightarrow \exists A \in\ A: x, y \in\ A$$

1. R is reflexief:

$$\forall x \in X: \exists A \in A: x \in A$$
$$\Rightarrow \forall x \in X = xRx$$

2. R is symmetrisch

$$\forall x, y \in X: \exists A \in A: x, y \in A$$
$$\Rightarrow \forall x, y \in X: \exists A \in A: y, x \in A$$
$$\Rightarrow\Rightarrow \forall x, y \in X: xRy \Rightarrow yRx$$

3. R is transitief

$$\forall x, y, z \in X: \exists A_1 \in A: x, y \in A \wedge: \exists A_2 \in A: y, z \in A$$

Aangezien de doorsnede van " $\neq$ " partities $\emptyset$ moet zijn is $A_1 = A_2$ (want $A_1 \cap A_2 = y$)

$$\Rightarrow \exists A \in A: x(y)z \in A$$
$$\Rightarrow xRz$$

3.9 Congruenties

Definitie 15. Zij $x_1, x_2 \in \mathbb{Z}, m \in \mathbb{N}_0$. x_1 en x_2 heten **congruent modulo** m indien $m \mid x_2 - x_1$. Het natuurlijk getal m heet de **modulus**. We schrijven:

$$x_1 \equiv_m x_2 \text{ of } x_1 \equiv x_2 \ (mod\ m).$$

Eigenschap 13. $\equiv_m$ is een equivalentierelatie.

Bewijs. $\equiv_m$ is

- Reflexief $x \equiv_m \mathrm{x}$ want $x - x = 0$ is een veelvoud van m
- Symmetrisch: $x \equiv_m \mathrm{y} \Rightarrow \mathrm{y} - \mathrm{x} = \mathrm{km} \Rightarrow \mathrm{x} - \mathrm{y} = (-\mathrm{k})\mathrm{m} \Rightarrow \mathrm{y} \equiv_m \mathrm{x}$
- Transitief: $x \equiv_m \mathrm{y}$ en $y \equiv_m \mathrm{z} \Rightarrow \mathrm{y} - \mathrm{x} = \mathrm{km}$ en $z - y = lm$
  $\Rightarrow z - x = (z - y) + (y - x) = (k + l)m$

Stelling 23.
$\equiv_m$ is "compatibel" met "+" en "×" in $\mathbb{Z}$, $\forall x_1, x_2, y_1, y_2 \in \mathbb{Z}$ met $x_1 \equiv_m \mathrm{x}_2$ en $y_1 \equiv_m \mathrm{y}_2$:

$$x_1 + y_1 \equiv_m x_2 + y_2$$

En

$$x_1 y_1 \equiv_m x_2 y_2$$

Bewijs.

$$x_2 - x_1 = km \ en \ y_2 - y_1 = lm$$

Dan geldt:

$$(x_2 + y_2) - (x_1 + y_1) = (x_2 - x_1) + (y_2 - y_1) = km + lm = (k + l)m$$

En

$$\begin{aligned} x_1y_2 - x_1y_1 &= x_2y_2 - x_1y_2 + x_1y_2 - x_1y_1 \\ x_1y_2 - x_1y_1 &= (x_2 - x_1)y_2 + (y_2 - y_1)x_1 \\ x_1y_2 - x_1y_1 &= kmy_2 + lmx_1 \\ x_1y_2 - x_1y_1 &= (ky_2 + lx_1)m \end{aligned}$$

Toepassing.(De 9-proef):
Als een getal in basis 10 geschreven wordt als $x_n, x_{n-1}, \ldots, x_0$ dan hebben we

$$x \equiv x_0 + x_1 + \cdots + x_n \text{ (mod 9)}$$

Bewijs.

$$\begin{aligned} x - (x_0 + x_1 + \cdots + x_n) &= x_0 + x_1 \times 10 + \cdots + x_n \times 10^n - x_0 - x_1 - \cdots - x_n \\ x - (x_0 + x_1 + \cdots + x_n) &= 9x_1 + 99x_2 + 999x_3 + \cdots + (10^n - 1)x_n \end{aligned}$$

Maar er geldt duidelijk dat $9 \mid 10^i - 1 = \underbrace{99 \ldots 99}_{i \text{ keer}}$. Als we dan $p(x)$ schrijven voor:

$$x_0 + x_1 + \cdots + x_n$$

dan hebben we aangetoond:

$$\forall x \in \mathbb{Z}: x \equiv p(x) \ (mod\ 9)$$

Dit wordt in de lagere school gebruikt om berekeningen na te kijken.
Inderdaad, we weten dat $x \equiv p(x)\ (mod\ 9)$ en $y = p(y)\ (mod\ 9)$.

Als $xy = z$ moet dus

$$p(z) \equiv z \equiv xy \equiv p(x)p(y)\ (mod\ 9)$$

Opgelet: het omgekeerde geldt niet noodzakelijk. Als de 9-proef klopt ben je dus nog niet zeker van je resultaat.

Voorbeeld.

$54321 \times 98765 = 5363013565$ kan onmogelijk juist zijn, want $p(54321) = 15$, $p(98765) = 35$ en $p(5363013565) = 37$. Wil de berekening kloppen, dan moet dus ook
$15 \times 35 \equiv 37\ (\text{mod}\ 9)$. Maar we mogen elk van deze getallen nog reduceren mod 9 om de berekeningen te vereenvoudigen. Dus

$$15 \times 35 \equiv 37\ (\text{mod}\ 9)$$
$$6 \times 8 \equiv 1\ (\text{mod}\ 9)$$
$$48 \equiv 1\ (\text{mod}\ 9)$$
$$3 \equiv 1\ (\text{mod}\ 9)$$

Wat dus fout is.

3.10 Modulair rekenen

Vermits congruentie modulo m een equivalentierelatie is, kunnen we kijken naar de partitie die ontstaat. Bijvoorbeeld:

$$E_0 = \{0, m, 2m, -5m, \dots\}$$
$$E_0 = \{km \mid k \in \mathbb{Z}\}$$
$$E_0 = \{\text{veelvouden van } m\}$$
$$E_1 = \{1, m+1, -3m+1, \dots\}$$
$$E_1 = \{km + 1 \mid k \in \mathbb{Z}\}$$
$$E_1 = \{\text{gehele getallen waarvoor de rest bij deling door } m \text{ gelijk is aan } 1\}$$
$$E_2 = \{km + 2 \mid k \in \mathbb{Z}\}$$
$$\dots$$
$$E_{m-1} = \{km + (m-1) \mid k \in \mathbb{Z}\}$$
$$E_m = E_0$$

Stelling 23 zorgt er nu voor dat we kunnen gaan rekenen met die equivalentieklassen.
We hebben m congruentieklassen. Ze vormen een partitie van $\mathbb{Z}$. De bewerkingen van Z induceren bewerkingen op deze m congruentieklassen:

$$E_k + E_l \coloneqq E_{k+l}, \qquad E_k \times E_l \coloneqq E_{k \times l}$$

Natuurlijk moeten we nagaan dat deze bewerkingen niet afhangen van de keuze van de representanten in E_k en E_l.

Zij $E_k = E_{k'}$ en $E_l = E_{l'}$ We moeten bewijzen dat $E_{k+l} = E_{k'+l'}$ Maar dat is gewoon een gevolg van Stelling 23 omdat $k \equiv_m k'$ en $l \equiv_m l'$ en dus $k + l \equiv_m k' + l'$. Voor de vermenigvuldiging werken we volledig analoog.

Notatie. De verzameling $\{E_0, E_1, \dots, E_{m-1}\}$ noteren we $\mathbb{Z}_m$

We zien nu een nieuwe soort verzameling van getallen waarmee we kunnen rekenen, $\mathbb{Z}_m$ is verzameling van m objecten waarmee we kunnen rekenen, $\mathbb{Z}_2$ kennen we al binair rekenen.

Stelling 24. $(\mathbb{Z}_m, +, \cdot)$ is een commutatieve ring met eenheid.[15]

Bewijs.
De bewerkingen zijn inwendig: $E_k + E_l \in \mathbb{Z}_m$ en $E_k \times E_l \in \mathbb{Z}_m$.
Want als we twee equivalentieklassen optellen of vermenigvuldigen krijgen we opnieuw een equivalentieklasse die $\in \mathbb{Z}_m$
De commutativiteit komt neer op $E_k + E_l = E_l + E_k$ en $E_k \times E_l = E_l \times E_k$,
Dat leiden we af door de commutativiteit die we hebben van $+$ en $\cdot$ in $\mathbb{Z}$.

Verder moeten we nog aantonen dat:

$$(E_k + E_l) + E_n = E_k + (E_l + E_n)$$
$$(E_k \times E_l) \times E_n = E_k \times (E_l \times E_n)$$
$$E_k + E_0 = E_K = E_0 + E_k$$
$$E_k \times E_1 = E_k = E_1 \times E_k$$
$$E_K \times (E_l + E_n) = E_k \times E_l + E_k \times E_n$$
$$(E_k + E_l) \times E_n = E_k \times E_n + E_l \times E_n$$
$$\forall E_k \in \mathbb{Z}_m : \exists - E_k = E_{-k} \in \mathbb{Z}_m : E_k + (-E_k) = E_0 = (-E_k) + E_k$$

Vereenvoudiging van notatie
Vermits de rekenregels in $(\mathbb{Z}_m, +, \times)$ dezelfde zijn als in $(\mathbb{Z}, +, \times)$, kunnen we zonder gevaar k noteren in plaats van E_k voor de restklasse van k modulo m. De context moet dan uitwijzen of we modulo m tellen of gewoon in $\mathbb{Z}$.

$5 + 3$ zal dus een verkorte notatie zijn voor $E_5 + E_3$ in $\mathbb{Z}_6$ bijvoorbeeld.
We zullen dan ook hebben $5 + 3 = 2$.

Toch even wijzen op een belangrijk verschil tussen $\mathbb{Z}$ en $\mathbb{Z}_m$. In $\mathbb{Z}$ geldt voor elke $a \neq 0$ dat $ab = ac \Rightarrow b = c$. Dit is niet langer waar in $\mathbb{Z}_m$. In $\mathbb{Z}_6$ bijvoorbeeld hebben we $3 \times 1 = 3 \times 5$, maar $1 \neq 5$.

Inverteerbare elementen in $\mathbb{Z}_m$
We hebben gezien dat $(\mathbb{Z}_m, +, \times)$ een commutatieve ring is met eenheid.
Het verschil met veelgebruikte ringen zoals $(\mathbb{Q}, +, \times)$ of $(\mathbb{R}, +, \times)$ is dat sommige elementen niet inverteerbaar zijn.

[15] *Commutatief* slaat op het feit dat we voor de vermenigvuldiging elementen van plaats mogen veranderen, *eenheid* slaat er op dat we voor de vermenigvuldiging een neutraal element hebben

Definitie 16.
$x \in \mathbb{Z}_m$ heet **inverteerbaar** indien er een $y \in \mathbb{Z}_m$ bestaat met $x \times y = 1$ (dus $x \times y \equiv_m 1$).

Voorbeeld.
In $\mathbb{Z}_6$ is 1 inverteerbaar, want $1 \times 1 = 1$.
2 is niet inverteerbaar want:

$$\begin{aligned} &2 \times 0 = 0, \\ &2 \times 1 = 2, \\ &2 \times 2 = 4, \\ &2 \times 3 = 6\ (mod\ 6) \Rightarrow\ 0, \\ &2 \times 4 = 8\ (mod\ 6) \Rightarrow\ 2, \\ &2 \times 5 = 10\ (mod\ 6) \Rightarrow 4. \end{aligned}$$

Dus $\nexists y \in \mathbb{Z}_6 : 2 \times y = 1$, 2 in niet inverteerbaar in $\mathbb{Z}_6$.

Lemma 2. Zij $x \in \mathbb{Z}_m$ inverteerbaar. Dan is het invers van x uniek.

Bewijs.
Veronderstel dat y en z twee inversen zijn. Dus:

$$x \times y = x \times z = 1$$

Dan:

$$\begin{aligned} y &= y \times 1 \\ y &= y \times (x \times z) \\ y &= (y \times x) \times z \\ y &= 1 \times z \\ y &= z \end{aligned}$$

Bijgevolg kunnen we een notatie invoeren voor het uniek invers van $x \in \mathbb{Z}_m$, namelijk x^{-1}.
Noteer ook

$$U_m = \{x \in \mathbb{Z}_m |\ x \text{ inverteerbaar}\}^{16}$$

[16] Staat voor unit

Stelling 25.

$$\forall x \in \mathbb{Z}_m : x \in U_m \Leftrightarrow ggd(x,m) = 1$$

Bewijs.

⇒

$$x \in U_m \Leftrightarrow \exists y \in \mathbb{Z}_m : \overbrace{x \times y = 1}^{\equiv_m}$$
$$x \in U_m \Leftrightarrow \exists y \in \mathbb{Z}, \exists k \in \mathbb{Z} : x \times y - 1 = k \times m$$
$$x \in U_m \Leftrightarrow \exists y \in \mathbb{Z}, \exists k \in \mathbb{Z} : x \times y - k \times m = 1$$

Een gemene deler van x en m is ook een deler van $xy - km$. Bijgevolg is $ggd(x,m) = 1$.

⇐

$$ggd(x,m) = 1 \Rightarrow \exists y, k \in \mathbb{Z} : xy + km = 1$$

Of

$$xy - 1 = -km$$

Of nog:

$$m | xy - 1$$

Zodat:

$$xy = 1 \text{ in } \mathbb{Z}_m$$

Gevolg 7. $|U_m| = \varphi(m)$

Definitie 17. Een ring met eenheid waarin elk niet-nul element inverteerbaar is, heet een **lichaam**. Indien de vermenigvuldiging bovendien commutatief is, spreekt men van een **veld**.

Gevolg 8. Voor p priem is elk van nul verschillend element in $\mathbb{Z}_p$ inverteerbaar. $(\mathbb{Z}_p, +, \times)$ is dus een veld.

Lemma 3. Als $x, y \in U_m$, dan $xy \in U_m$ en $(xy)^{-1} = y^{-1}x^{-1}$

Bewijs.

$$xy \times y^{-1}x^{-1} = xx^{-1} = 1$$

en inversen zijn uniek.

Stelling 26.

$$\forall y \in U_m : yU_m = U_m$$

Bewijs.
Uit Lemma 3 volgt $yU_m \subset U_m$[17]

Stel nu $x \in U_m$.
Dan is $x = y(y^{-1}x)$ en $y^{-1} \in U_m$ want $y^{-1}y = 1$, zodat $y^{-1}x \in U_m$

[17] Als we een inverteerbaar element y nemen en we vermenigvuldigen alle inverteerbare elementen met uit de verzameling U_m, veranderd de verzameling U_m niet

Stelling 27. Zij $y \in U_m$. Dan geldt: $y^{\varphi(m)} = 1$ in $\mathbb{Z}_m$.

Dus in het bijzonder:

$$y \times y^{\varphi(m)-1} = 1 \text{ in } \mathbb{Z}_m$$

$y^{\varphi(m)-1}$ is dus het inverse van y.

Bewijs.
Nummer de elementen van U_m. Dus:

$$U_m = \{u_1, u_2, \dots, u_{\varphi(m)}\}$$

Stel:

$$u \coloneqq u_1 u_2 \dots u_{\varphi(m)}$$

Dan is u een element van U_m, want het is een product van elementen van U_m.
Vermits $yU_m = U_m$ zijn de elementen $yu_1, yu_2, \dots, yu_{\varphi(m)}$ niets anders dan:

$$u_1, u_2, \dots, u_{\varphi(m)}$$

eventueel in een andere volgorde geschreven. Bijgevolg geldt ook:

$$yu_1 \times yu_2 \times \dots \times yu_{\varphi(m)} = u$$

Of nog:

$$y^{\varphi(m)} u_1 u_2 \dots u_{\varphi(m)} = u$$

Of

$$\begin{aligned} y^{\varphi(m)} u &= u \\ y^{\varphi(m)} u u^{-1} &= u u^{-1} \\ y^{\varphi(m)} &= 1 \end{aligned}$$

Andere formuleren van dezelfde stelling:

$$\forall y \in \mathbb{Z}, \forall m \in \mathbb{N}_0 : \underbrace{ggd(y,m) = 1}_{y \in U_m} \Rightarrow y^{\varphi(m)} \equiv_m 1$$

Dit resultaat heet de Stelling van Euler. Een speciaal geval is de Kleine stelling van Fermat:

Stelling 28. Voor p priem hebben we

$$\forall n \in \mathbb{N} : n^p \equiv_p n$$

Bewijs.
Als $p \nmid n$ in n inverteerbaar modulo p zodat $n^{\varphi(m)} \equiv_p 1$, of nog $n^{p-1} \equiv_p 1$, zodat $n^p \equiv_p n$
Als $p \mid n$ is het duidelijk dat $n^p \equiv_p 0 \equiv_p n$

3.11 De Chinese reststelling

In de eerste eeuw stelde de Chinese wiskundige Sun-Tsu het volgende vraagstuk:

"Van een getal weet men dat de rest bij deling door 3 gelijk is aan 2; wanneer men deelt door 5, vindt men als rest 3 en bij deling door 7 bedraagt de rest 2. Over welk getal gaat het?"

Het gaat hier eigenlijk om een stelsel van verschillende vergelijkingen waaraan het onbekende getal x moet voldoen:

$$x \equiv 2 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 5)$$
$$x \equiv 1 \ (mod\ 7)$$

Dit probleem kan gemakkelijk opgelost worden aan de hand van de zogenaamde Chinese reststelling.

Stelling 29 (Chinese reststelling). Zij $m_1, m_2, \dots, m_n$ paarsgewijs relatief prieme natuurlijke getallen en $a_1, a_2, \dots, a_n$ willekeurige gehele getallen. Dan heeft het stelsel

$$x \equiv \mathrm{a}_1 \ (mod\ m_1)$$
$$x \equiv \mathrm{a}_2 \ (mod\ m_2)$$
$$\dots$$
$$x \equiv \mathrm{a}_\mathrm{n} \ (mod\ m_n)$$

een oplossing die uniek is modulo $m = m_1 m_2 \dots m_n$.
D.w.z. een unieke oplossing x met $0 \leq x < m$ en alle andere oplossingen congruent modulo m met deze x.

Bewijs.
We geven een constructief bewijs. We gaan dus een algoritme geven om de oplossing werkelijk te construeren.

We gaan een variabele $M_k = \frac{m}{m^k}$, dat is het product van alle moduli, behalve m_k.
Omdat alle moduli relatief priem hebben we $ggd(m_k, M_k) = 1$[18],
we weten dus als we gaan rekenen in $\mathbb{Z}_{m_k}$, M_k inverteerbaar is en dat betekend dat we een getal y_k kunnen vinden voor M_k zodat:

$$M_k y_k \equiv 1 \ (mod\ m_k)$$

Stel nu:

$$x \coloneqq a_1 \overset{mod\ m_1}{\widetilde{M_1}} y_1 + a_2 \overset{mod\ m_2}{\widetilde{M_2}} y_2 + \dots + a_n \overset{mod\ m_n}{\widetilde{M_n}} y_n \in \mathbb{Z}$$

We tonen nu dat deze x een oplossing is van het stelsel.
Merk eerst op dat:

$$M_j \equiv 0 \ (mod\ m_i)$$

van zodra $i \neq j$. Als we dus x reduceren modulo m_k, blijft er alleen maar:

$$x \equiv a_k M_k y_k \equiv a_k \ (mod\ m_k)$$

[18] $m_k$zit er zelf al niet meer in want we hebben hem weg gedeeld, maar we weten dat die m_k geen gemeenschappelijke deler had met alle die andere m_i'tjes. Dus als we naar de $ggd(m_k, M_k)$ dan zijn die relatief priem.

over.

Onderstel nu dat y een andere oplossing is van het stelsel. Dan geldt voor elke $k \in [n]$ dat:

$$m_k | x - y$$

Vermits alle m_k relatief priem zijn, volgt hieruit $m \mid x - y$.

Voorbeeld. We kunnen nu de vraag van Sun-Tsu oplossen.
We berekenen

$$m = 3 \times 5 \times 7 = 105,\ M_1 = \frac{m}{3} = 35,\ M_2 = \frac{m}{5} = 21\ en\ M_3 = \frac{m}{7} = 15.$$

De inversen van M_k modulo m_k berekenen is ook niet moeilijk. We vinden:

$$y_1 = 2, y_2 = 1\ en\ y_3 = 1.$$

Hieruit vinden we:

$$\begin{aligned} x &\equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \\ &= 233 \\ &\equiv 23\ (mod\ 105). \end{aligned}$$

3.12 Public key cryptografie

Als je geheime berichten wil versturen moet je een techniek afspreken om te coderen. Deze techniek noemen we een cryptosysteem. Een bekend eenvoudig cryptosysteem bestaat erin om de letters te “verschuiven" in het alfabet. Als je bijvoorbeeld het bericht “IK HEB EEN KOEKJE" wil versturen, kan je elke letter drie plaatsen opschuiven in het alfabet. Je stuurt dus “LN KHE HHQ NRHNMH".
Indien je als antwoord “LN ZLO HHQ VWXN" krijgt, kan je door de inverse operatie het bericht ontcijferen. Je krijgt “IK WIL EEN STUK".

Zulk eenvoudig systeem is doeltreffend indien men er zeker van is dat het bericht nooit zal onderschept worden door iemand die iets weet over de frequentie waarmee letters voorkomen in de Nederlandse taal. In onze berichten zie je bijvoorbeeld twee keer “HHQ". Er is veel kans dat dit “EEN" voorstelt.

Een ander nadeel van dit systeem is dat de twee personen die willen communiceren, op voorhand moeten afspreken hoeveel plaatsen zij elke letter opschuiven. Dit is wat men de sleutel van het cryptosysteem noemt. Deze sleutel moet geheim blijven. De sleutel uitwisselen tussen de twee personen die willen communiceren is dus een probleem bij dit soort cryptosysteem. Voor betalingen over internet moeten vele gebruikers communiceren met één bedrijf. Het is onbegonnen werk om voor elke gebruiker een sleutel mee te delen zonder dat hij kan onderschept worden. Gelukkig werd er in de jaren '70 door Rivest, Shamir en Adleman een systeem bedacht waarbij de sleutels niet meer geheim hoeven te zijn. Men spreekt van Public Key Cryptografie.

Het systeem is gebaseerd op priemgetallen en modulair rekenen. Persoon A wil een geheim bericht naar persoon B sturen. Hiervoor gaat hij eerst zijn bericht (dat in letters geschreven is) vertalen naar getallen zodat er kan gerekend worden. Dit gebeurt via een standaard tabel die niet geheim hoeft te zijn. We kunnen bijvoorbeeld afspreken dat “A" wordt voorgesteld door het getal 1, “B" door 2, enz. De spatie is 0. Het bericht “LUISTER GOED" wordt dan bijvoorbeeld “12 21 09 19 20 05 18 00 07 15 05 04”.

We gaan nu elke letter coderen door het te verheffen tot een vaste macht en dan het resultaat te reduceren modulo 33 (omdat er bijvoorbeeld 33 tekens zijn in ons eenvoudig systeem: letters plus wat leestekens). Laat ons bijvoorbeeld telkens de derde macht nemen. Dan is het gecodeerd bericht “12 21 3 28 14 26 24 0 13 9 26 31".

Dit was een voorbeeld met kleine getallen om te illustreren wat er gebeurt. In de praktijk gaan we te werk met veel grotere getallen. We moeten ook nog zien hoe deze machtsverheffing kan geïnverteerd worden om te decoderen.

één van de voornaamste eigenschappen waarop de veiligheid van het RSA cryptosysteem steunt, is de moeilijkheid om een willekeurig getal te ontbinden in priemfactoren. Het is bijvoorbeeld zeer gemakkelijk om de twee priemgetallen 71 en 59 met elkaar te vermenigvuldigen. We krijgen 4189. Probeer nu het omgekeerde: neem een vergelijkbaar getal, 4161, en probeer dat eens te ontbinden in priemfactoren.

Laat ons de methode van de machtsverheffing nu eens proberen met grotere getallen: we verheffen tot de macht 101 en reduceren modulo 1189. Vermits resten modulo 1189 groter kunnen worden dan 27 hebben we de mogelijkheid om meer symbolen te gebruiken of meerdere letters ineens te coderen. In ons bericht “12 21 09 19 20 05 18 00 07 15 05 04" van hoger kunnen we de cijfers per drie groeperen zodat we “122 109 192 005 180 007 150 504" verkrijgen. Indien het aantal cijfers geen veelvoud is van drie, voegen we op het einde nullen toe om overal groepjes van drie cijfers te hebben.

We moeten nu dus 122^{101} berekenen. Dat is een ander paar mouwen… Zelfs met een rekenmachine zal dat niet lukken, tenzij we het slim aanpakken. We hebben hier immers te maken met een getal van 211 cijfers. Een eerste idee zou zijn om die macht stap voor stap te berekenen en steeds te reduceren modulo 1189. Op die manier krijgen we geen al te grote getallen. Hier gaan we dan:

$$122^2 = 122 \times 122 = 14884 \equiv 616 \ (mod\ 1189)$$
$$122^3 = 122^2 \times 122 \equiv 616 \times 122 = 75152 \equiv 245 \ (mod\ 1189)$$
$$122^4 = 122^3 \times 122 \equiv 245 \times 122 = 29890 \equiv 165 \ (mod\ 1189)$$
$$\dots$$

Maar dat is ook nogal veel werk. Veel slimmer is om steeds te kwadrateren.

$$122^2 = \cdots = 14884 \equiv 616 \ (mod\ 1189)$$
$$122^4 = 616^2 = 379456 \equiv 165 \ (mod\ 1189)$$
$$122^8 = 165^2 = 27225 \equiv 1067 \ (mod\ 1189)$$
$$122^{16} = 1067^2 = 1138489 \equiv 616 \ (mod\ 1189)$$
$$122^{32} = 616^2 = 379456 \equiv 165 \ (mod\ 1189)$$
$$122^{64} = 165^2 = 27225 \equiv 1067 \ (mod\ 1189)$$

Nu geldt $101 = 1 + 4 + 32 + 64$ zodat:

$$122^{101} = 122^1 \times 122^4 \times 122^{32} \times 122^{64}$$
$$\equiv 122 \times 165 \times 165 \times 1067 = 3543987150 \equiv 245 \ (mod\ 1189).$$

Dus met vijf kwadrateringen, een paar vermenigvuldigingen en reducties modulo 1189 hebben we het resultaat. Dit is veel efficiënter dan de honderd vermenigvuldigingen en reducties die we eerst gingen uitvoeren! Deze methode werkt steeds omdat we elke mogelijke exponent steeds kunnen schrijven als som van machten van 2. Dit komt er immers op neer dat we de exponent uitschrijven in basis 2 (zie blz. 46).

We beschrijven nu het RSA algoritme in het algemeen. Persoon B die berichten wil ontvangen kiest twee (grote) priemgetallen p en q en berekent hun product $n:=pq$. Hij bepaalt ook $b:=(p-1)(q-1)$ en zoekt e met $ggd(e,b) = 1$. De informatie die publiek wordt gemaakt is n en e.

Indien persoon A een gecodeerd bericht wil sturen naar B zal hij eerst zijn bericht omzetten in getallen. Elk van die getallen m gaat hij dan coderen als volgt

$$c \coloneqq m^e \ (mod\ n)$$

Het symbool c wordt dan verstuurd.
Wanneer B het bericht c ontvangt, moet hij dat decoderen. Hij maakt hiervoor gebruik van het feit dat $ggd(e,b) = 1$. Er is dus een invers d van e modulo b.
Er bestaat dus een k met $ed = 1 + k(p-1)(q-1)$ zodat

$$c^d \equiv (m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)}\ (mod\ n)$$

We veronderstellen nu even dat $ggd(m,p) = ggd(m,q) = 1$, wat geen grote beperking is. Dan kunnen we de uit de Stelling van Euler (Stelling 27) halen dat :

$$m^{p-1} \equiv 1\ (mod\ q)$$

En

$$m^{q-1} \equiv 1\ (mod\ q)$$

Bijgevolg geldt:

$$c^d \equiv m \times (m^{p-1})^{k(q-1)} \equiv m \times 1 \equiv m\ (mod\ p)$$

Alsook

$$c^d \equiv m \times (m^{q-1})^{k(p-1)} \equiv m \times 1 \equiv m\ (mod\ q)$$

Merk op dat indien m een veelvoud is van p of q, bovenstaande equivalenties geldig blijven.
De onderstelling $ggd(m,\ p) = ggd(m,q) = 1$ was dus slechts tijdelijk nodig.

Uit de Chinese reststelling volgt nu dat:

$$c^d \equiv m\ (mod\ pq)$$

Dus kan B decoderen door gewoon c^d te reduceren modulo n.
Merk op dat je ook gemakkelijk “met de hand" kan bewijzen dat:

$$c^d \ \equiv m\ (mod\ pq).$$

In de praktijk worden priemgetallen van ongeveer tweehonderd cijfers gebruikt. Dan heeft n ongeveer vierhonderd cijfers en duurt de ontbinding in priemfactoren, met de beste algoritmen die tot nu toe bekend zijn, nog duizenden jaren. Men mag dus zeggen dat RSA cryptosystemen voorlopig veilig zijn. Bovendien bieden zij het grote voordeel dat de sleutel die dient voor het coderen publiek mag gemaakt worden zonder het systeem in gevaar te brengen.

Hoofdstuk 4: Inleiding tot de grafentheorie:

In Hoofdstuk 2 losten we reeds een probleem op door een grafische voorstelling met verbonden punten, welke ook nuttig is voor vele andere problemen. Daarom wijden we er nu een heel hoofdstuk aan.

4.1 Definities en terminologie

Definitie 18. Een **graf** bestaat uit een verzameling V wiens elementen we **toppen** noemen en een relatie $\rightarrow$ op V die we **adjacentierelatie** noemen.
Een koppel (u, v) dat behoort tot de relatie $\rightarrow$ (d.w.z. $u \rightarrow v$) heet een pijl. De verzameling van pijlen noteren we met E.

Meestal noteren we graffen met kalligrafische letters $G, H, \ldots$ Bij ons zal de toppenverzameling van een graf G meestal eindig zijn. De orde van G is dan $|V(G)|$, het aantal toppen in G.

Nu kunnen we naargelang de eigenschappen van de adjacentierelatie verschillende soorten graffen onderscheiden.

Definitie 19. Zij $G = (V, \rightarrow)$ een graf.
Indien de relatie $\rightarrow$ symmetrisch is, zegt men dat de graf **ongericht** is. In dat geval schrijven we dikwijls $\sim$ in plaats van $\rightarrow$.
Indien we willen benadrukken dat de graf niet ongericht is, spreken we van een **gerichte graf**.
Indien $v \rightarrow v$ zeggen we dat de graf een **lus** heeft in v. Een graf zonder lussen noemen we **simpel of enkelvoudig**.

Als er meerdere zulke graffen in het spel zijn, noteren we $V(G)$ om de toppenverzameling van G aan te duiden en $E(G)$ voor de pijlen. De letters V en E komen van het Engels: een top is een “vertex” (meervoud “vertices") en een pijl een “edge".

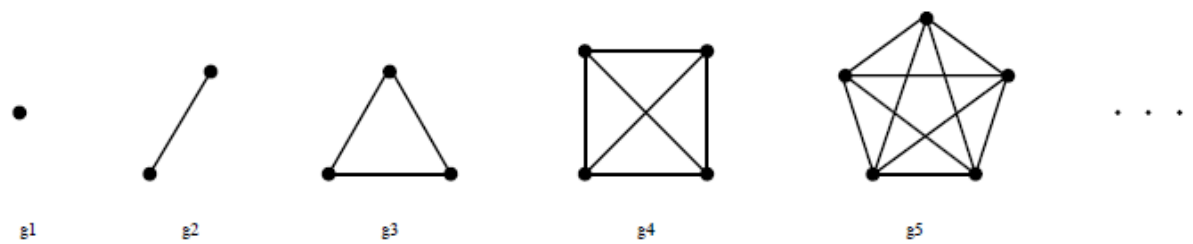
Een ongerichte simpele graf kunnen we ook zien als een koppel verzamelingen (V, E) waarbij V gestructureerd wordt door een verzameling E van 2-verzamelingen van V.
We hebben dus $E \subset \binom{V}{2}$ en de elementen van E noemen we dan **bogen**. Twee toppen u, v van zulk een graf (V, E) zijn dus adjacent indien $\{u, v\} \in E$. We zeggen dan ook dat u en v **buren** zijn.
De **buurt** van een top v van een ongerichte simpele graf G is de verzameling G_v van alle buren van v.
We hebben dus:

$$G_v = \{x \in V(G) | x \sim v\}$$

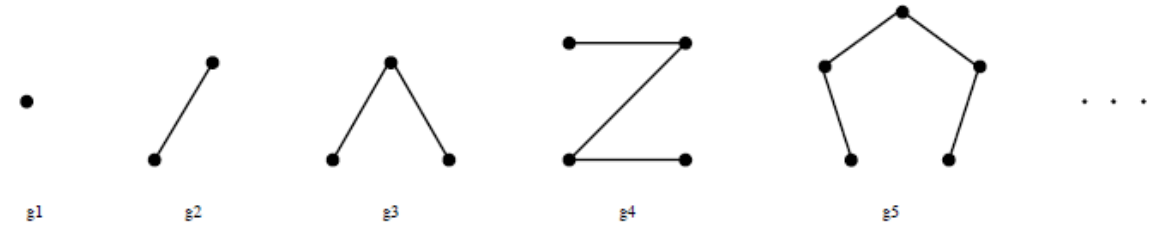
Een top zonder buren heet geïsoleerd.
Opmerking. In de literatuur gebruikt men het woord “graf” vaak voor deze specifieke soort van ongerichte simpele graffen.

4.2 Belangrijke voorbeelden van ongerichte simpele graffen

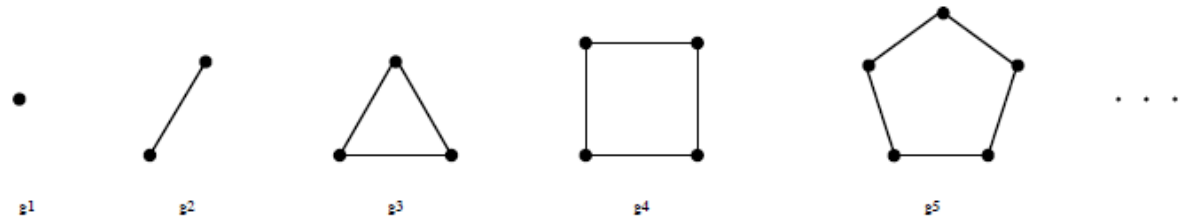
Complete graffen De complete graf K_n heeft n toppen. Alle toppen zijn verbonden met alle overige toppen



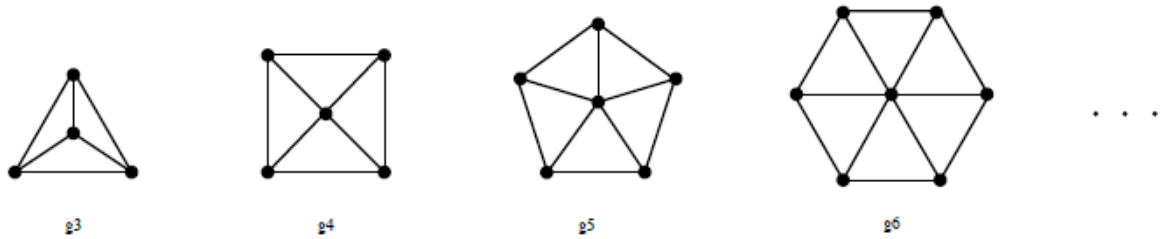
Paden Het pad P_n heeft n toppen $t_1, t_2, \dots, t_n$ die zo verbonden zijn dat $t_i \sim t_{i+1}$ voor $i \in [n-1]$.



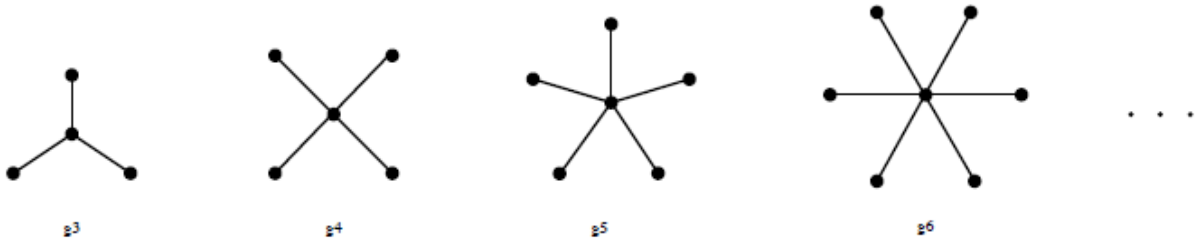
Cycli Een cyclus (of cykel) van lengte n is een graf C_n met n toppen $t_0, t_1, \dots, t_{n-1}$ die z0 verbonden zijn dat $t_i \sim t_{i+1}$ voor $i \in \mathbb{Z}_n$, waarbij we de indices modulo n nemen.



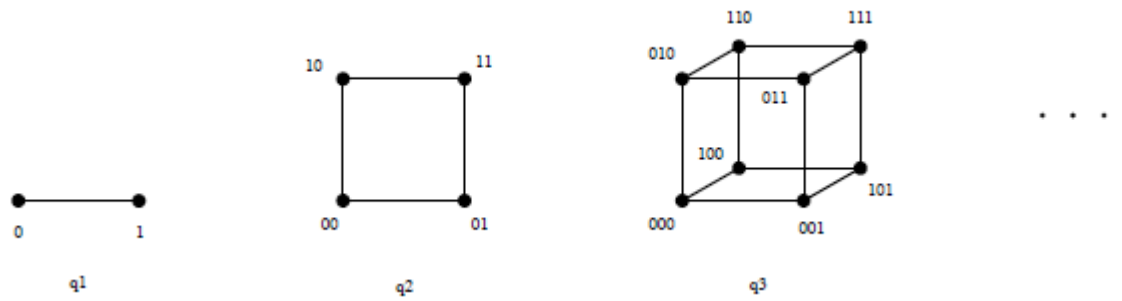
Wielen Het wiel W_n van orde n is een cyclus C_n met in het midden een top toegevoegd die verbonden is met alle toppen van de cyclus.



Sterren De ster S_n van orde n bekom je door in het wiel W_n de bogen van de cyclus weg te laten.



Kubussen Neem $\{0,1\}^n$ als toppenverzameling en maak twee toppen adjacent als ze verschillen in juist één coördinaat. We noteren de kubus in dimensie n met Q_n.



4.3 Verdere definities en eigenschappen

Definitie 20.
De **graad** van een top v in een ongerichte graf G is het aantal bogen die v bevatten. Een lus tellen we twee keer. We noteren dit met $deg(v)$ zodat geldt:

$$\deg(v) = |G_v|$$

Eigenschap 14 (Handshake). In een eindige ongerichte graf G geldt steeds

$$\sum_{v \in V(G)} \deg(c) = 2|E(G)|$$

Bewijs.
Dubbeltelling: $deg(v)$ is het aantal bogen die v bevatten en elke boog bevat juist twee toppen.

Gevolg 9. Een eindige ongerichte graf heeft steeds een even aantal toppen van oneven graad.

Bewijs. Omdat, wegens de vorige eigenschap, de som van alle graden even moet zijn.

Een ander woord voor graad is **valentie**. Indien alle toppen van een ongerichte graf dezelfde graad hebben, zeggen we dat de graf **regulier** is. Een k-reguliere graf is een ongerichte graf waarin elke top graad k heeft.

Definitie 21. In een gerichte graf G definiëren we voor elke top v de **ingraad** en de **uitgraad** als het aantal pijlen dat in v respectievelijk aankomt en vertrekt. We noteren deze graden respectievelijk $\deg^+(v)$ en $\deg^-(v)$. Een gerichte graf heet **gebalanceerd** indien voor elke top v geldt dat:

$$\deg^+(v) = \deg^-(v).$$

Een **deelgraf** van een graf G is een graf H met $V(H) \subset V(G)$ en $E(H) \subset E(G)$. We spreken van een **opspannende deelgraf** indien $V(H) = V(G)$. Zij $S \subset V(G)$. De **deelgraf door G geïnduceerd op S** is de graf met toppenverzameling S en de hierbij behorende pijlen (voor een ongerichte graf hebben we dus de bogenverzameling $E(G) \cap \binom{S}{2}$.

Een **wandeling** in een ongerichte graf G is een rij van toppen:

$$t_0, t_1, \dots, t_k$$

zodanig dat $t_{i-1} \sim t_i$ voor elke $i \in [k]$. We spreken van een **gerichte wandeling** als $t_{i-1} \to t_i$

De **lengte** van de wandeling is k, één minder dan het aantal toppen.
De top t_0 heet **beginpunt** (of vertrekpunt) van de wandeling en t_k heet het **eindpunt** (of aankomstpunt).

In een wandeling $t_0 \sim t_1 \sim \dots \sim t_k$ zijn er dus k bogen van de vorm $\{t_{i-1}, t_i\}$ met $i \in [k]$.
Als al die bogen verschillend zijn, wordt de wandeling een **pad** genoemd.

Als $t_0 = t_k$ heet het pad **gesloten**. Een **simpel of enkelvoudig pad** is een pad waarin geen twee toppen gelijk zijn. Een gesloten pad dat na verwijderen van de top $t_0 = t_k$ een simpel pad wordt, heet een **cyclus**.

Een ongerichte graf heet **samenhangend** indien er voor elk paar toppen $u, v \in V(G)$ een pad van u naar v bestaat. Een graf die niet samenhangend is bestaat uit verschillende **samenhangscomponenten** waartussen geen bogen bestaan.

Een gerichte graf G heet **samenhangend** indien de onderliggende graf (verwijder alle pijlen op de bogen) samenhangend is. We zeggen dat G sterk samenhangend is indien er tussen elke twee toppen u en v een gericht pad bestaat.

Dit wil natuurlijk zeggen dat er een opeenvolging van toppen en bogen $u = t_0, b_1, t_1, b_2, t_2, \dots, b_k, t_k = v$ bestaat zodanig dat de boog b_i gericht is van t_{i-1} naar t_i en al zulke pijlen verschillend zijn.

Op een ongerichte graf kunnen we ook een **afstand** definiëren. Voor $u, v \in V(G)$ stellen we $d(u, v)$ gelijk aan de lengte van de kortste wandeling van u naar v. Als er tussen u en v geen wandeling bestaat, schrijven we $d(u, v) = \infty$. We stellen ook voor elke top v dat $d(v, v) = 0$.

Eigenschap 15. Voor een ongerichte graf G geldt dat

$$d: V(G) \times V(G) \to \mathbb{N} \cup \{\infty\}: (u, v) \to d(u, v)$$

Een metriek is.

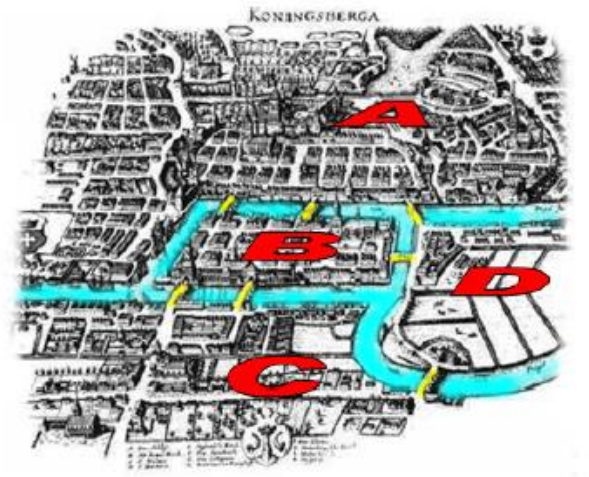
Bewijs.
Het is duidelijk dat $d(u, v) = 0$, $u = v$ en dat $d(u, v) = d(v, u)$ voor elk paar toppen $u, v \in V(G)$.

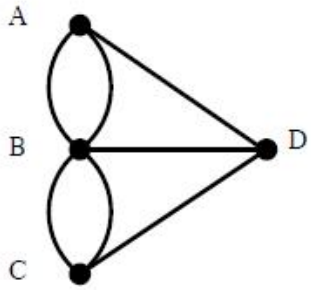
Transitiviteit nagaan:
Zij nu $u, v, w \in V(G)$. drie toppen met $d(u, v) = k$ en $d(v, w) = l$.
Dit geeft een wandeling van u naar v en één van v naar w.
Door deze na elkaar te volgen, krijgen we een wandeling van v naar w die lengte $k + l$ heeft.
De afstand $d(u, w)$ zal dus ten hoogste $k + l$ bedragen.

4.4 Bijzondere paden

4.4.1 Eulerpaden

Graffen werden uitgevonden door Leonhard Euler (1707{1783). Hij leefde op dat moment in Königsberg (nu Kaliningrad, Rusland) in Pruisen. De stad wordt in vier stukken verdeeld door de Pregel-rivier.





Zijn ook zeven bruggen over de rivier om de verschillende stadsgedeelten te verbinden. Op een dag was er een stoet die door de hele stad ging en Euler vroeg zich af of er een wandeling bestond voor de stoet zodanig dat elke brug juist één maal overgestoken werd en bovendien de wandeling terug zou komen naar het startpunt.

Euler stelde het probleem grafisch voor (zie Figuur 4.1) met zeven bogen en vier toppen, welke overeenkomen met de zeven bruggen en de vier stadsgedeelten. Het resultaat is geen graf aangezien er dubbele bogen zijn en in een relatie komen de koppels immers hoogstens één keer voor.

Definitie 22. Een multigraf is een graf $G = (V, \rightarrow)$ uitgebreid door middel van een functie μ: $V \times V \rightarrow \mathbb{N}$ die een **multipliciteit** toekent aan elke pijl. We interpreteren de functie μ als volgt:

- $\mu(u, v) = 0$ betekend dat u en v niet adjacent zijn
- $\mu(u, v) = k > 0$ betekent dat er k pijlen zijn van u naar v.

Pijlen die hetzelfde begin- en eindpunt hebben worden **parallel** genoemd.

Een multigraf zonder parallelle pijlen is een graf.

Definitie 23.
Een pad in een ongerichte multigraf G heet een **Eulerpad** indien het elke boog van G precies één maal bevat.
Een gesloten Eulerpad is een **Eulercyclus.**
Een multigraf die een Eulercyclus bevat heet een **Eulergraf.**

Stelling 30 (Euler, 1736). Zij G een ongerichte multigraf zonder geïsoleerde toppen. Dan geldt dat G een Eulergraf is ⇔ G samenhangend is en alle toppen van G even graaf hebben.

⇒

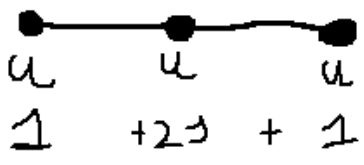
1. Omdat G een Eulergraf is, moet hij een Eulercyclus bevatten (def. 23), die bevat alle bogen van G waardoor $\forall a, b \in V$ een pad van a naar b bestaat, dus G is samenhangend
2. Een cyclus C begint en eindigt op dezelfde knoop u, neem $v \in C$ met $v \neq u$

Als we v tegenkomen in de cyclus C, worden altijd 2 bogen meegerekend (in, uit), we kunnen v ook meerdere keren tegenkomen:

Als v, k keer wordt aangetroffen in C dan hebben $2k$ bogen aangetroffen ⇒ even graad

Wat met u?

Neem $u \in C$:
Dus als we beginnen in u zien we hem 1 keer, als we eindigen in u zien we heb ook 1 keer, Dan kunnen we u nog j keer aantreffen in de cyclus (in uit) net zoals bij de v



En:

$$1 + 2j + 1 = 2(1 + j) \Rightarrow \text{even} \Rightarrow \text{even graad}$$

⇒ elke top die onze cyclus passeert heeft een even graad en sinds C een Eulercyclus is, passeert het door alle bogen & toppen van de graf.

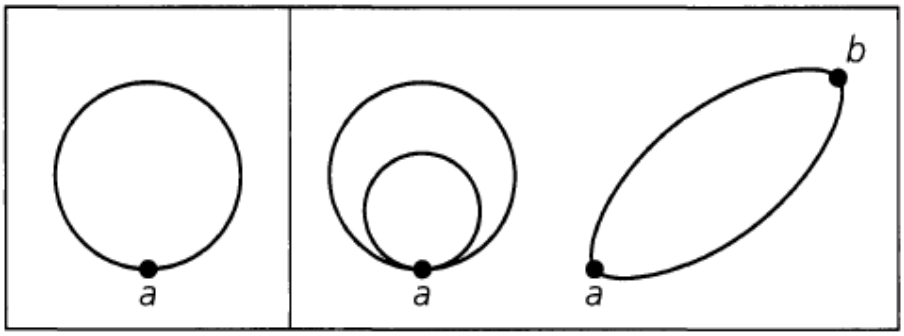
⇐

Omgekeerd moeten we nu een Eulercyclus maken vertrekkende uit:

- Samenhang
- Alle toppen even graad.

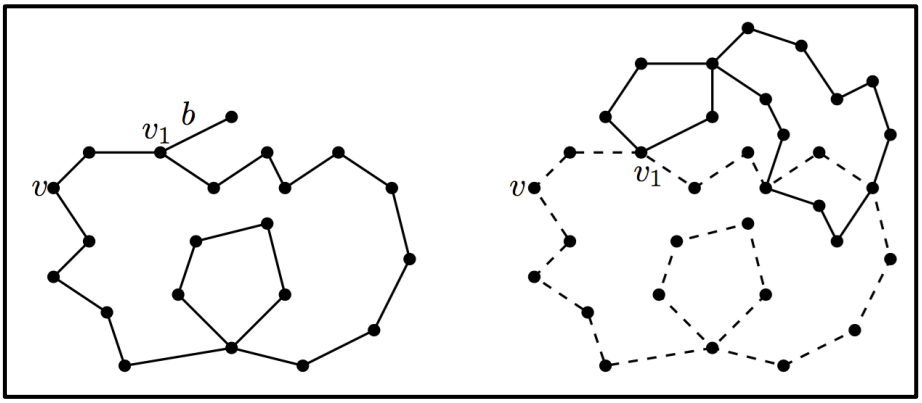
We gaan de Eulercyclus construeren met sterke inductie op het aantal bogen:

Stel dat ons aantal bogen in de graf 1 of 2 is, dan ziet onze graf er al volgt uit:



We gaan veronderstellen dat het resultaat waar is wanneer er minder dan n bogen zijn.
Wanneer de graf n bogen heeft, nemen we een willekeurige top v, We moeten nu een Eulercyclus construeren, maar we willen daar onze inductie hypothese gebruiken.

We kiezen een willekeurige boog die v bevat, die heeft een ander uiteinde u.
Vanuit u kunnen we weer vertrekken, maar we kunnen alleen maar vertrekken door een andere boog te gebruiken die we net hadden gebruikt. Dit kan want u heeft een even graad. Zo blijven we dus bogen toevoegen zonder tweemaal dezelfde boog te gebruiken tot we terug in ons startpunt komen. We hebben nu een gesloten pad gemaakt.



We hebben dus een gesloten pad gemaakt dat vertrekt en aankomt in v en geen enkele boog tweemaal heeft gebruikt, als dat alle bogen van onze graf waren dan hebben we een Eulercyclus.

Stel dat we de boog b nog niet bewandeld hebben, hoe kunnen we het pad toch nog gaan vergroten of veranderen zodanig dat we over de boog b stappen?

Wat weten we over die boog b?
Door de samenhang moet die boog b dus net aan een top van ons pad hangen, anders hebben we een zwevende top en dat kan niet wegens de samenhang. (We hebben dus een boog b die niet tot het pad bestaat maar wel een top v_1 van het pad bevat.)

Nu gaan we alle bogen van ons gemaakt pad P weggooien, de graf die we overhouden noemen we G'. Alle toppen van G' hebben nog even graad want we hebben per top maar een even aantal bogen wegegelaten.

We hebben nu wel dat G' niet noodzakelijk meer samenhangend is, als dat zo is, dan beschouwen we de samenhangcomponent die v_1 bevat en deze moet wegens onze inductiehypothese een Eulercyclus P_1 bevatten.

Hetzelfde geldt voor alle resterende samenhangscomponenten, omdat we maar een eindig aantal toppen hebben, gaan we maar een eindig aantal extra cyclussen gaan vinden.

Hoe gaan we door die cycli stappen? (hoe gaan we ze allemaal aan elkaar hangen?)
We krijgen verschillende paden P_i die allemaal een boog gemeenschappelijk gaan hebben met P op de top v_i. We gaan die allemaal combineren door in v door het pad P te wandelen tot we zo een speciale top v_1 aantreffen, dan bewandelen we het pad P_1 tot als we weer in v_1 toekomen en gaan we weer door in P. Wanneer er nog andere toppen v_i doen we dit weer op dezelfde manier tot we terug in aan de start zijn, dit proces zal stoppen omdat G eindig is. □

Definitie 24. Een simpel pad dat alle toppen van een multigraf G bevat heet een **Hamiltonpad.**
Een **Hamiltoncyclus** is een gesloten Hamiltonpad.
Een multigraf die een Hamiltoncyclus bevat heet een **Hamiltongraf.**

Lemma 4. Als je k toppen uit een Hamiltongraf G weglaat, samen met de aangrenzende bogen, dan valt G uiteen in hoogstens k samenhangscomponenten.

Bewijs:
We hebben een Hamiltongraf G dus per definitie bestaat er een Hamiltoncyclus H (die gaat door alle toppen, maar gebruikt niet noodzakelijk alle bogen). We noemen de graffen die uit G en H ontstaan door het weglaten van k toppen G' en H' met $k > 0$.

Als we naar onze Hamiltoncyclus H gaan kijken en we laten daar de k toppen en bijhorende toppen weg, dan gaat die uiteenvallen in $\leq k$ samenhangscomponenten want het is een cyclus.
(Als in een cyclus knippen dan hebben we $\leq k$ samenhangscomponenten)

VOORBEELD 1

Als we naar onze graf G' gaan kijken waar we ook k toppen en bogen hebben weg gegooid dan heeft die mogelijks meer bogen dan H', dus als die meer bogen heeft dan kan die hebben dat er wel van die samenhangscomponenten der nog meer aan elkaar gangen.
Dus het aantal samenhangscomponenten kan alleen maar zakken (en dus niet groter worden).
Het aantal samenhangscomponenten van G' zal niet groter zijn dan dat van H' en weten we dus ook dat die uiteenvalt uit $\leq k$ samenhangscomponenten.

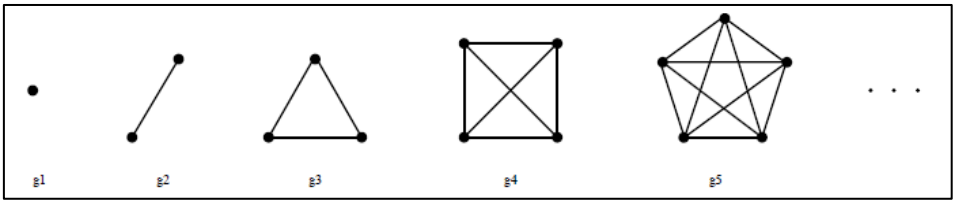
VOORBEELD 2

Stelling 31. Zij G multigraf waarbij het verwijderen van n toppen leidt tot $m > n$ samenhangscomponenten, $\Rightarrow$ is G geen Hamiltongraf.

Dit is logisch door het toepassen van lemma 4.

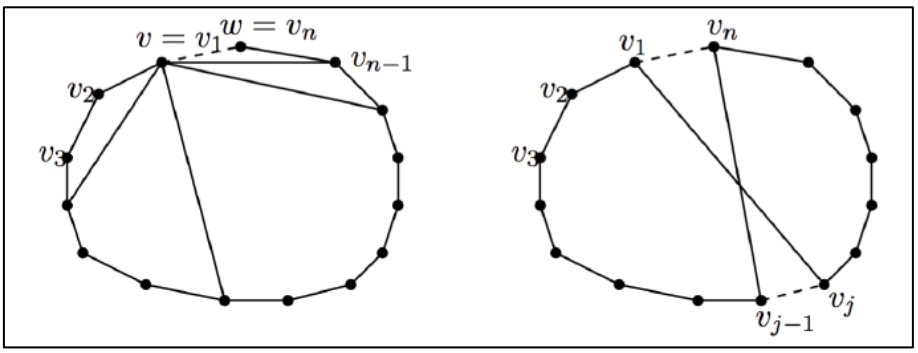
Stelling 32 (Dirac, 1952). Zij G een ongerichte simpele graf met $n \geq 3$ toppen. Als alle toppen van G minstens graad $\frac{n}{2}$ hebben, dan heeft G een Hamiltoncyclus.

Bewijs. Uit het ongerijmde.
Dus als de stelling niet waar zou zijn, dan moet er minstens 1 tegenvoorbeeld bestaan.
Laat G' zo een tegenvoorbeeld zijn met n toppen. Dan hebben we dat elke top van G' minstens graad $\geq \frac{n}{2}$ heeft, maar toch zou er geen Hamiltoncyclus bestaan. We gaan in de graf G' maximaal bogen toevoegen (toppen verbinden die niet verbonden waren in G') zonder een Hamiltoncyclus te vormen. Die nieuwe graf noemen we G.
In G is er geen Hamiltoncyclus, dus G kan niet de complete graf zijn. Moest dat zo zijn dan kunnen we natuurlijk gaan stappen zodanig dat we alle toppen passeren.

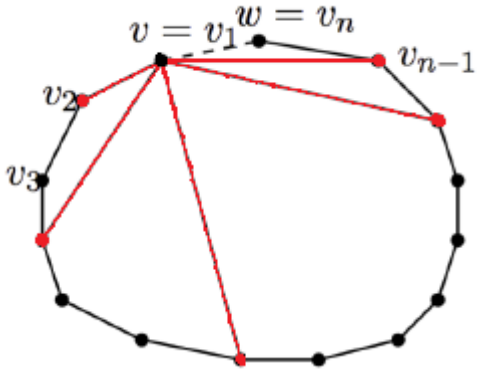


Er zijn dan dus zeker 2 toppen v en w die niet verbonden zijn in G, want als we die verbinden dan hebben we een complete graf en hebben we een Hamiltoncyclus. Dus bevat G een Hamiltonpad:

$$v = v_1 \sim v_2 \sim \ldots \sim v_n = w.$$

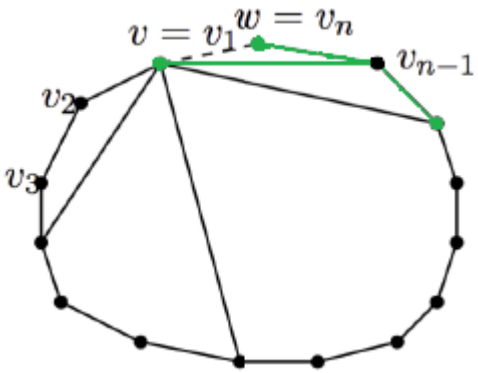


We gaan naar alle buren (verzameling toppen) van v gaan kijken, die verzameling noemen we G_v, door de veronderstelling van de graad weten we die verzameling buren van v minstens $\frac{n}{2}$ toppen bevat.



Dan bekijken we de verzameling van de opvolgers van de buren van w op het Hamiltonpad (w zit daar zelf ook in). (w heeft maar 1 opvolger en dat is v_{n-1})

$$S' \coloneqq \{v_{i+1} | v_i \in G_w\}.$$



$w \in S'$ maar dat is niet interessant dus we gaan w daaruit halen:

$$S \coloneqq S' \backslash \{w\}$$

Er geldt dan $|S| \geq \frac{n}{2} - 1$.

Nu gaan we naar het duiventil gaan:
Als we kijken naar de buurtverzameling van v, G_v en naar S, die maken natuurlijk gebruik van de toppen van onze graf die op dat Hamiltonpad liggen en dus de deelverzameling van:

$$\{v_2, v_3, \dots, v_{n-1}\}$$

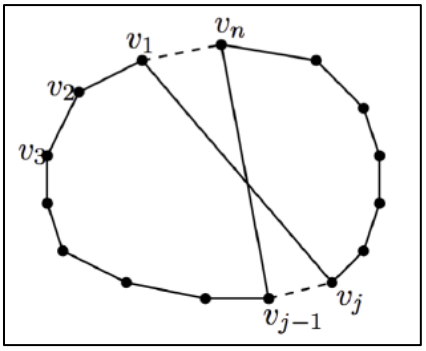
v_1 en v_n zitten daar niet in omdat ze aangrenzend zijn. Dus G_v en S zijn deelverzamelingen van $\{v_2, v_3, \dots, v_{n-1}\}$. De verzameling bevat $n - 2$ elementen,
dus het duiventil leert ons dat $|S \cap G_v| \geq 1$ (in de doorsnede moet er 1 element zitten)
Want:

$$|S| + G_v = \frac{n}{2} - 1 + \frac{n}{2}$$
$$= n - 1$$

Dus moet er 2 toppen in eenzelfde hok zitten.

Dus er bestaat een top v_j met $v_j \sim v$ en $v_j \in S$, wat betekend dat $w = v_n \sim v_{j-1} \sim v_j$. Neem nu het pad

$$v = v_1 \sim v_j \sim v_{j+1} \sim \ldots \sim v_n \sim v_{j-1} \sim v_{j-2} \sim \ldots \sim v_1$$



Dit is een Hamiltoncyclus, tegenspraak. Want we gingen er vanuit dat die niet bestond. □

Definitie 25. Een gerichte (multi)graf heet een **gerichte Eulergraf** indien er een gesloten gericht pad is dat elke pijl juist één keer gebruikt.

Stelling 33. Een samenhangende gerichte (multi)graf G is een gerichte Eulergraf ⇔
G sterk samenhangend[19] en gebalanceerd[20] is.

Bewijs:

⇒

We vertrekken van een gerichte Eulergraf dus bestaat er een Eulercyclus in G, moet die wel gebalanceerd zijn want met zo'n cyclus gaan we wanneer we door toppen gaan, telkens we binnen komen ook weer buiten gaan en dus zal de ingraad gelijk zijn aan de uitgraad. Die Eulercyclus zorgt er ook voor dat er tussen elke twee toppen een gericht pad bestaat, dus zijn we sterksamenhangend. □

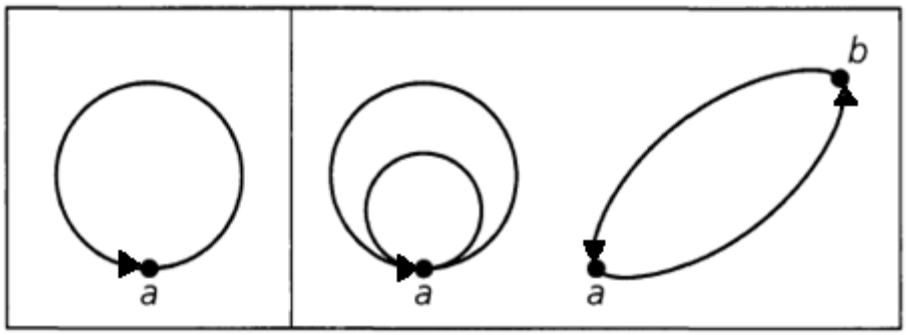
⇐

Omgekeerd moeten we nu een Eulercyclus maken vertrekkende uit:

- Sterk samenhangend
- Gebalanceerd

We gaan de Eulercyclus construeren met sterke inductie op het aantal bogen.

Stel dat ons aantal bogen in de graf 1 of 2 is, dan ziet onze graf er al volgt uit:

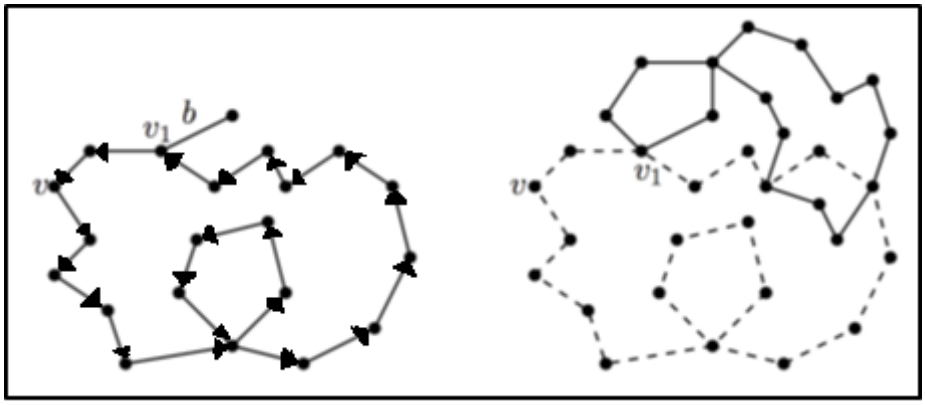


[19] We zeggen dat G sterk samenhangend is indien er tussen elke twee toppen u en v een gericht pad bestaat.

[20] Een gerichte graf heet gebalanceerd indien voor elke top v geldt dat $\deg^+(v) = \deg^-(v)$.

We gaan veronderstellen dat het resultaat waar is wanneer er minder dan n bogen zijn.
Wanneer de graf n bogen heeft, nemen we een willekeurige top v, We moeten nu een gerichte Eulercyclus construeren, maar we willen daar onze inductie hypothese gebruiken.

We kiezen een willekeurige boog die v bevat, die heeft een ander uiteinde u.
Vanuit u kunnen we weer vertrekken, maar we kunnen alleen maar vertrekken door een andere boog te gebruiken die we net hadden gebruikt. Dit kan want u is gebalanceerd. Zo blijven we dus bogen toevoegen zonder tweemaal dezelfde boog te gebruiken tot we terug in ons startpunt komen.
We hebben nu een gesloten gericht pad gemaakt.



We hebben dus een gesloten gericht pad gemaakt dat vertrekt en aankomt in v en geen enkele boog tweemaal heeft gebruikt, als dat alle bogen van onze graf waren dan hebben we een gerichte Eulercyclus.

Stel dat we de boog b nog niet bewandeld hebben, hoe kunnen we het pad toch nog gaan vergroten of veranderen zodanig dat we over de boog b stappen?

Wat weten we over die boog b?
Door de sterk samenhangend moet die boog b dus net aan een top van ons gericht pad hangen, anders hebben we een zwevende top en dat kan niet wegens de sterke samenhang. (We hebben dus een boog b die niet tot het gericht pad bestaat maar wel een top v_1 van het gericht pad bevat.)

Nu gaan we alle bogen van ons gemaakt gericht pad P weggooien, de graf die we overhouden noemen we G'. Alle toppen van G' zijn nog gebalanceerd want we hebben per top maar een even aantal in- en uit bogen wegegelaten.

We hebben nu wel dat G' niet noodzakelijk meer sterk samenhangend is, als dat zo is, dan beschouwen we de samenhangcomponent die v_1 bevat en deze moet wegens onze inductiehypothese een Eulercyclus P_1 bevatten.

Hetzelfde geldt voor alle resterende samenhangscomponenten, omdat we maar een eindig aantal toppen hebben, gaan we maar een eindig aantal extra cyclussen gaan vinden.

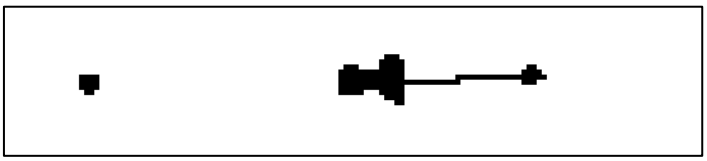
Hoe gaan we door die cycli stappen? (hoe gaan we ze allemaal aan elkaar hangen?)
We krijgen verschillende gerichte paden P_i die allemaal een boog gemeenschappelijk gaan hebben met P op de top v_i. We gaan die allemaal combineren door in v door het gericht pad P te wandelen tot we zo een speciale top v_1 aantreffen, dan bewandelen we het gericht pad P_1 tot als we weer in v_1 toekomen en gaan we weer door in P. Wanneer er nog andere toppen v_i doen we dit weer op dezelfde manier tot we terug in aan de start zijn, dit proces zal stoppen omdat G eindig is. □

Een toernooi (bijvoorbeeld een schaaktoernooi, voetbaltoernooi, …) kan aan de hand van een gerichte graf gemodelleerd worden. We trekken een pijl van speler (of ploeg) u naar speler v indien u gewonnen heeft van v. Als iedereen tegen iedereen speelt, hebben we dus een complete graf waar elke boog een oriëntatie krijgt.

Definitie 26. Een toernooi is een gerichte simpele graf die ontstaat door alle bogen van een complete graf te oriënteren.

Stelling 34. Elk toernooi heeft een gericht Hamiltonpad.

Bewijs. Bij inductie op n, het aantal toppen in het toernooi T.
Als $n = 1$ of $n = 2$ is de stelling duidelijk waar:



We kunnen veronderstellen dat de stelling geldt voor alle toernooien met $n - 1$ toppen. Nu moeten we tonen voor een toernooi met n toppen gebruikmakende van de inductie hypothese. □

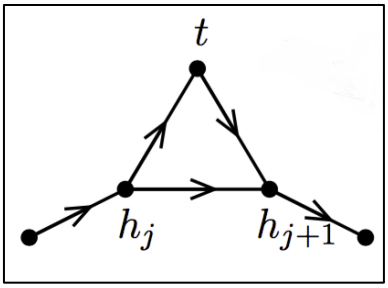
Opmerking:
Soms proberen studenten van $n - 1$ toppen naar n te gaan door een top toe te voegen, zo werkt inductie niet, we vertrekken van een toernooi T met n toppen en we gaan proberen herleiden naar een toernooi met $n - 1$ toppen.

Dus in T gaan we een top t kiezen en we noemen T' die graf die onstaat door door die top t weg te doen en alle bogen waar die op zat. Wat overblijft in nog altijd een toernooi want ze waren allemaal verbonden. Onze inductie hypothese geeft ons een Hamiltonpad in T', die gaat door die $n - 1$ toppen wandelen $h_1 \to h_2 \to \cdots \to h_{n-1}$.

De t die we hebben weggegooid die is verbonden met al de toppen $h_1 \to h_2 \to \cdots \to h_{n-1}$, want het was een complete graf. We kunnen nu makkelijk op een tekening gaan zien hoe die verbinding kon geweest zijn:

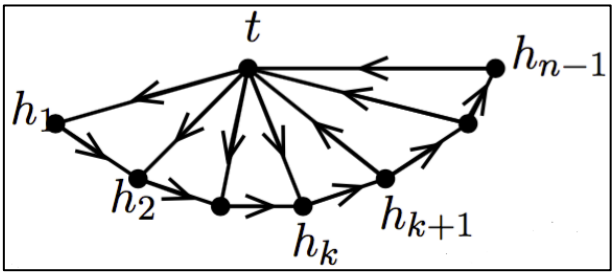
<u>Geval 1:</u>
Stel dat t verbonden was met een h_j een opvolger van h_j.
Dan kunnen we natuurlijk het pad gewoon gaan vergroten door de top t te nemen en de boog tussen $\{h_j, h_{j+1}\}$ te gaan verwijderen.

Dus ons pad is dan $\to \cdots \to h_j \to t \to h_{j+1} \to \cdots$

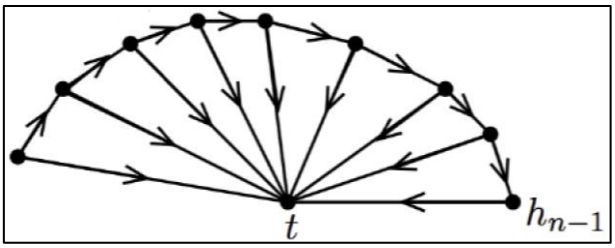


<u>Geval 2:</u>
Stel dat geval 1 zich niet voordoet, dan hebben we eigenlijk dat wanneer we door ons pad lopen tot een bepaalde j er geen uitgaande boog is van dat pad naar t, maar allemaal inkomend zijn en dan pas uitgaand.

We kunnen dan gewoon ons pad verleggen door t in het begin te zetten en dan door te lopen.



Geval 3:
Stel dat ze allemaal van de h_1 en de h_{n-1} naar t gaan. Ook dan kunnen we een Hamiltonpad maken want dan gaan we gewoon door heel ons pad en via h_{n-1} naar t stappen.



Formeel:
We hebben ons Hamiltonpad $h_1 \to h_2 \to \cdots \to h_{n-1}$ en als er dus een index **($\boldsymbol{j} \in [\boldsymbol{n-2}]$)** bestaat zodat de h_j naar t wijst en t naar de opvolger van h_j **($\boldsymbol{h_j \to t \to h_{j+1}}$)** dan hebben we het volgend Hamiltonpad:

$$h_1 \to h_2 \to \cdots \to h_j \to t \to h_{j+1} \to \cdots \to h_{n-1}$$

Als er zo geen j bestaat dan hebben we dat $\forall j \leq k: t \to h_j$ en $\forall j > k: t \leftarrow h_j$ en dan kunnen we hem aan het begin hangen:

$$t \to h_1 (\text{indien } k \neq 0)$$

Maar stel dat we dat niet hebben, hangen we t gewoon aan het einde:

$$h_1 \to h_2 \to \cdots \to h_{n-1} \to t$$

□

Stelling 35. Een toernooi T heeft een gerichte Hamiltoncyclus ⇔ T sterk samenhangend is.

⇒

Als we een Hamiltoncyclus hebben, dan hebben we een gericht pad voor elk twee toppen, want die cyclus passeert overal, dus als we twee toppen kiezen dan stappen we gewoon langs die cyclus van de ene top naar de andere. □

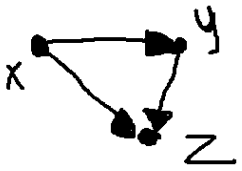
⇐

Als ons toernooi T sterk samenhangend is dan gaan we eerst tonen dat we een gerichte cyclus hebben en dan gaan we zien dat dat een Hamiltoncyclus is. Die gaan we doen uit het ongerijmde.

Als we veronderstellen dat ons toernooi T geen cyclus bevat dan:

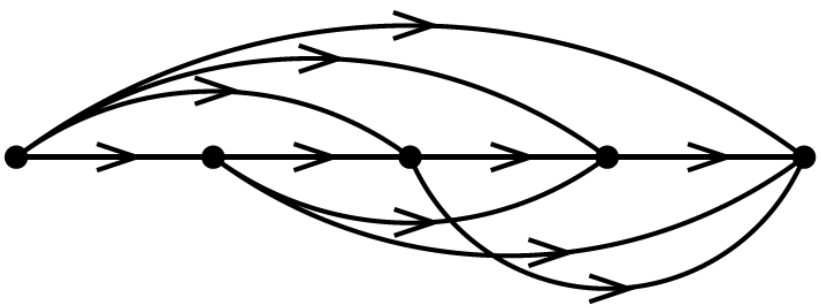
$$\forall x, y, z \in T: (x \to y \text{ en } y \to z) \Rightarrow x \to z$$

Voor elke 3 toppen die we in ons toernooi T pakken dat als x wijst naar y en y wijst naar z dat x dan naar z moet wijzen. Als dat niet zo is dan zouden we een cyclus hebben.



Het niet hebben van een cyclus herleidt zich eigenlijk dat we tot 3 punten ons kunnen concentreren dat heten we transitiviteit.

Als we een transitief toernooi hebben dan kunnen we eigenlijk onze toppen allemaal gaan rangschikken van links naar rechts zodat alle pijlen naar rechts wijzen:



Dan krijgen we een tegenspraak met de sterke samenhang die verondersteld was want we kunnen nooit van meest rechts top naar de meest linkse top stappen. En dat is een tegenspraak.

Hier uit leiden we af dat er een gerichte cyclus moeten hebben. Dus we hebben een cyclus die door alle toppen gaat en terug naar het begin gaat:

$$C = y_1 \to y_2 \to \cdots \to y_k \to y_1$$

We veronderstellen dat C maximale lengte heeft in T en toch geen Hamiltoncyclus is. (er zouden toch nog toppen ontbreken).

Maar omdat ons toernooi T sterk samenhangend is en er toppen zouden ontbreken dan is er zo'n top buiten die cyclus die verbonden is met een top van de cyclus want we hebben samenhang.

Dus de top die niet op die cyclus ligt is wel verbonden met die cyclus, nu mogen we er vanuit gaan dat bijvoorbeeld de y_1 verbonden is met t

$$y_1 \to t$$

Moest $t \to y_2$ dan hebben we een probleem met de maximale lengte die we hadden verondersteld want we zouden dan kunnen stappen van $y_1 \to t \to y_2 \to y_3 \to \cdots$ en dit is een langere cyclus

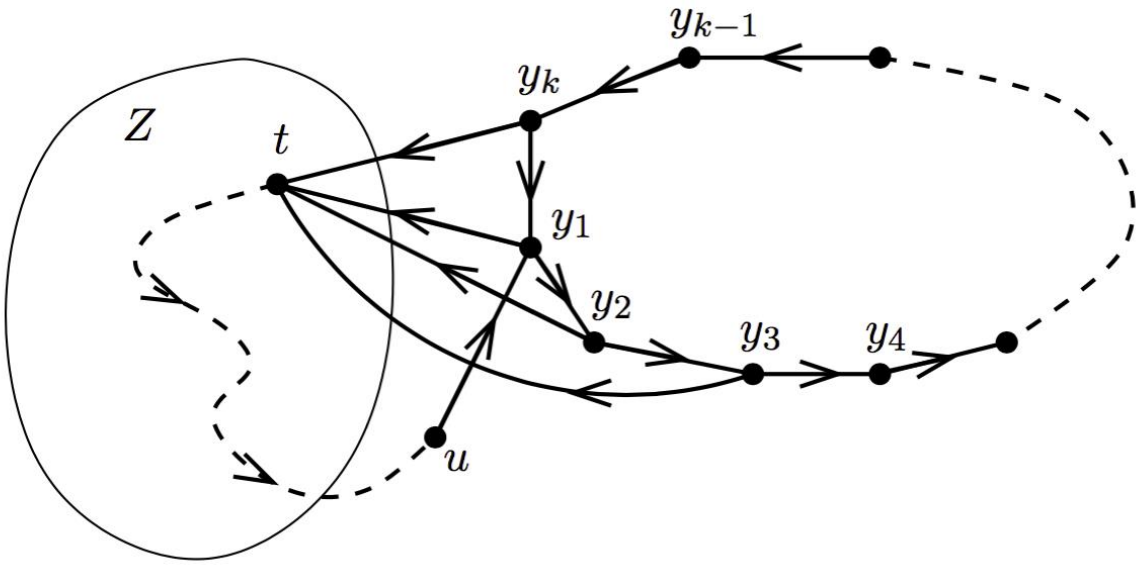
Dus de boog van $t \to y_2$ (die is er want we hebben een complete graf) die moet dus $y_2 \to t$ gericht zijn.

Diezelfde redenering kunnen we nu doen voor alle andere toppen op die cyclus, die moeten dus allemaal gericht zijn naar t:

$$\forall i \in [k]: y_i \to t$$

Nu gaan we die toppen nemen zonder de y_2 waar dat de y_1 naar wijst:

$$Z \coloneqq \{z \in V(T) \backslash \{y_2\} | y_1 \to z\}$$



We kijken nu naar de verzameling Z dat zijn die toppen zonder de y_2, waar de y_1 naar toe wijst. In het bijzonder zit die t in die verzameling Z. (Alle toppen waar y_1 naar wijst zitten in Z, maar we nemen niet de y_2 want daar wijst hij ook naar)

Als we nu naar alle toppen binnen die Z gaan kijken dan moeten natuurlijk voor alle andere y_i wijzen naar die Z anders zouden we terug het pad kunnen verlengen. Door de sterke samenhang moet er een pad zijn van t naar de y_1, maar doordat alle y_i naar alle toppen uit onze verzameling Z moeten wijzen gaan we nooit in y_i komen. We moeten in de Z kunnen stappen naar een top die buiten de verzameling Z ligt want alleen die kan verbonden zij met y_1 in de juiste richting.

Maar een top buiten de verzameling Z door de definitie van Z en toernooi moet die onmiddellijk verbonden zijn met y_1 en dus krijgen we een cyclus vanuit $t \to u \to y_1 \to y_2 \to \cdots \to y_k \to t$ en die is veel langer (≥ 2 toppen meer) en dit is een tegenspraak.

Dus dit is een tegenspraak met "er bestaat geen cyclus". We hadden verondersteld dat C een maximale cyclus was maar niet Hamilton, maar die moet een Hamiltoncyclus zijn. Want als hij niet overal passeerde kregen we terug een tegenspraak. □

Isomorfismen tussen graffen

Definitie 27. Zij (V, μ) en (W, φ) twee multigraffen. Een afbeelding $f: V \to W$ heet een **morfisme** indien zij voldoet aan $\forall (u, v) \in V \times V$ geldt dat $\varphi\big(f(u), f(v)\big) = \mu(u, v)$

Definitie 28. Twee multigraffen (V, μ) en (W, φ) zijn **isomorf** als er een bijectief morfisme $V \to W$ bestaat. Zulk een morfisme heet dan ook een **isomorfisme** tussen (V, μ) en (W, φ).

Voor twee ongerichte simpele graffen $G = (V, \sim_G)$ en $H = (W, \sim_H)$ hebben we dus dat een isomorfisme een bijectie f is tussen de toppenverzamelingen V en W zodanig dat voor elk paar toppen $u, v \in V$ geldt $u \sim_G v \Leftrightarrow f(u) \sim_H f(v)$

Notatie. Als twee graffen G en H isomorf zijn, noteren we $G \cong H$.

Bomen en bossen

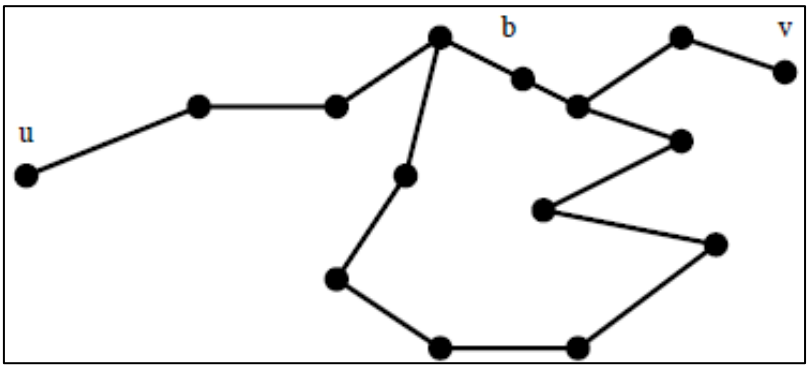
Stelling 36. Zij G een samenhangende simpele graf. Dan zijn volgende twee eigenschappen equivalent:

1) G is **minimaal samenhangend** (d.w.z. dat als je een boog weglaat, G niet meer samenhangend is)
2) G heeft geen cyclus.

Bewijs.

$\boxed{1 \Rightarrow 2}$

Als G minimaal samenhangend en hij zou toch een cyclus hebben, dan kan je een boog van die cyclus weg laten zonder de samenhang te verliezen. Inderdaad: Als we de toppen u en v nemen van G, ofwel was u met v verbonden via een pad dat de boog b niet bevatte en dan blijven u en v verbonden. Indien het pad wel in de boog b bevatte dan kunnen we gewoon een nieuwe paden maken door de rest van die cyclus te volgen, en dat is een tegenspraak met minimaal samenhangend want we kunnen nog steeds van overal naar overal stappen.



□

$2 \Rightarrow 1$

Bij contrapositie: $\neg 1 \Rightarrow \neg 2$.

We veronderstellen dat G niet minimaal samenhangend is, dus er is een boog $b = \{u, v\}$ die we niet nodig hebben voor de samenhang. Als we de boog b weglaten van G, krijgen we een nieuwe graf G'. in G'hebben we een pad van u naar v en als we de boog b daar weer aan toevoegen dan hebben we weer een cyclus en dat is een tegenspraak. □

Definitie 29. Een samenhangende ongerichte simpele graf zonder cyclus noemen we een **boom**.

Gevolg 11. Een samenhangende ongerichte graf is een boom ⇔ elke twee toppen verbonden zijn door juist één pad.

Bewijs.

⇐

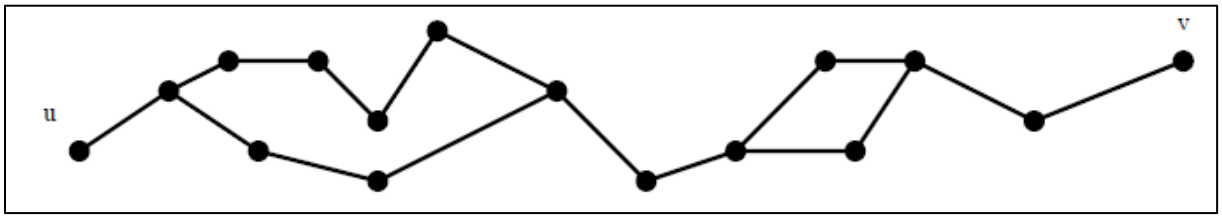
Als er voor elke paar toppen juist 1 pad is, is de graf minimaal samenhangend en dat is equivalent met geen cyclus, dus per definitie 29 een boom.

Waarom is dat zo?

Als je na het verwijderen van een boog $b = \{u, v\}$ nog een samenhangende graf zou hebben, dan is er buiten de boog b nog steeds een pad van u naar v en dit is een tegenspraak met dat er juist 1 pad zou zijn. □

⇒

Als we een boom hebben en toch veronderstellen dat er twee paden zouden zijn van u naar v.
Dan nemen we de stukken van de paden die niet samenvallen en dan hebben we op die manier een cyclus en dat is een tegenspraak met de definitie van een boom.



□

Definitie 30. Een top van graad 1 in een boom heet een **blad**.

Lemma 5. Een boom met $n \geq 2$ toppen heeft minstens twee bladeren.

Bewijs. Neem een top t van de boom. Dan zijn er twee mogelijkheden:

- Ofwel is het **een** blad
- Ofwel is het **geen** blad

t is geen blad

Als het t geen blad is, dan is het dus niet van graad 1, (graad moet ≥ 2). We kunnen dan wandelen vanuit t naar een buur, enzo verder. Zonder ooit een top tweemaal te bezoeken. Omdat de boom eindig is gaan we dus wel op een bepaald moment gaan stoppen in een top s. s moet een blad zijn, als het proces was gestopt omdat s meerdere buren zou hebben die reeds bezocht werden, dan betekend het dat er meerdere paden zijn van t naar s en dat is tegenspraak.

We hebben nu 1 blad 1 s, hoe vinden we het ander?
We kunnen nog een wandeling doen vanuit t want graad moet ≥ 2 op zoek naar een ander blad. En dat moet weeral stoppen want als er meerdere buren zouden zijn die we reeds bezocht hebben dan zouden er meerdere paden zijn.

t is een blad

Als het t zelf een blad is , heeft t graad 1. Vanuit die enige buur kunnen we weer wandelen en die top heeft graad ≥ 2 want anders zou het ook een blad zijn en zou de boom maar uit 2 toppen bestaan. Anders stappen we dus verder tot we het ander blad tegenkomen. □

Belangrijk

Stelling 37. Een boom met n toppen heeft $n - 1$ bogen.

Bewijs. Per inductie op n.
Voor $n = 1$ is de stelling duidelijk voldaan. (1 top en 0 bogen)

Als we veronderstellen dat de stellen waar is voor n toppen en we nemen nu een boom T met $n + 1$ toppen. Dan moeten we herleiden naar n toppen.

We hebben een boom met $n + 1$ toppen lemma 5 verzekert ons het bestaan van een blad. Nu gaan we uit onze boom met $n + 1$ toppen dat blad verwijderen. Hierdoor verwijderen we 1 top en 1 boog, nu hebben we een graf T' die heeft n toppen en 1 boog minder dan T.

Wegens de inductie hypothese (stelling was waar dat alle bomen met n toppen $n - 1$ bogen hebben) heeft dit $n - 1$ bogen, maar dan wil dat zeggen dat onze oorspronkelijk boom T (die 1 boog meer had) n bogen heeft.

Dus onze oorspronkelijk boom T heeft $n + 1$ toppen en n bogen. □

Definitie 31. Wanneer G een gerichte graf is, dan wordt G een **gerichte boom** genoemd als de ongerichte graf geassocieerd met G een boom is.

Een gerichte boom noemen we een **gewortelde boom** als er een unieke top t is waarvoor de ingraad nul is en alle andere toppen ingraad één hebben. We noteren (G, t).

We kunnen elke ongerichte boom wortelen door een willekeurige top als wortel te kiezen waardoor alle bogen een natuurlijke oriëntatie krijgen weg van die wortel.

Definitie 32. Een **bos** is een ongerichte simpele graf zonder cyclus.
Een **geworteld bos** is een bos waarin elke samenhangscomponent geworteld is[21].

Opmerking. De samenhangscomponenten van een bos zijn dus bomen.

Eigenschap 16. Zij F een bos met n toppen en k samenhangscomponenten. Dan heeft F juist $n - k$ bogen.
Bewijs.
We kijken naar alle bomen van het bos. We hebben k bomen met respectievelijk $n_1, n_2, \ldots, n_k$ toppen. Al die bomen hebben dus elk $n_i - 1$ bogen (*stelling 37*). Als we alles optellen hebben we dus:

[21] Verschil met definitie boom: samenhang.

$$n_1 - 1 + n_2 - 1 + \cdots + n_k - 1 = \left(\sum_{i=1}^{k} n_i\right) - k = n - k.$$

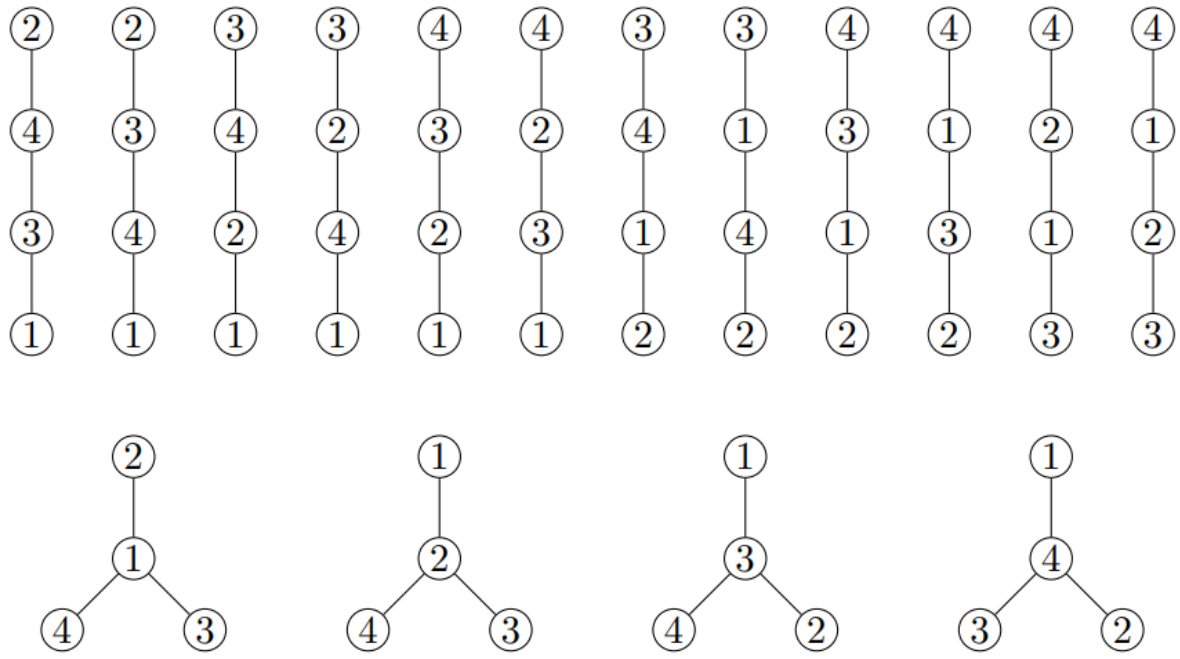
Isomorfe graffen zijn belangrijk in de studie van abstractie van problemen, we kunnen een probleem gaan voorstellen met een graf en waar we dan ons gaan afvragen "wat zijn de eigenschappen van die graf". In plaats van die graf iedere keer opnieuw te gaan bestuderen is het vaak sneller om te kijken of het niet al lijkt een graf die we al kennen en de eigenschappen al van bewijzen hebben.

Het aantal niet-isomorfe bomen tellen op n toppen is nogal moeilijk. Het aantal genummerde bomen tellen daarentegen is niet zo moeilijk. □

Definitie 33. Een genummerde (of gelabelde) boom is een boom met als toppenverzameling $[n]$ voor $n \in \mathbb{N}\backslash\{0,1\}$[22].

Stelling 38 (Cayley).
Voor elke $n \in \mathbb{N}\backslash\{0,1\}$ is het aantal genummerde bomen met n toppen gelijk aan n^{n-2}.

Bewijs: Joyal's bewijs van Cayley's formule:
Er zijn 16 bomen met toppen verzameling $4 = \{1, 2, 3, 4\}$:



We zullen Joyal's bewijs van deze stelling geven. Laat T_n staan voor het aantal bomen op n toppen. Dan kan de formule van Cayley geherformuleerd worden als:

$$n^2 T_n = n^n$$

Om de formule van Cayley te bewijzen, creëert Joyal een bijectie tussen twee verzamelingen, de ene van grootte $n^2 T_n$, en de andere van grootte n^n. Deze laatste verzameling is gemakkelijk te beschrijven: het is n^n, de verzameling van alle functies van $\{1, 2, \ldots, n\}$ naar zichzelf.
(Onthoud dat n^n n^n elementen heeft omdat er voor elk van de n elementen in het domein n keuzes

[22] We kijken naar bomen met minstens 2 toppen, anders hebben we geen boog.

zijn voor een toegewezen waarde in het codomein).
De eerste verzameling -die met n^2T_n elementen- bestaat uit wat Joyal gewervelde dieren noemde.

Een gewerveld dier op n toppen is een boom T met toppenverzameling n en een keuze van een geordend paar(t, h) bestaande uit toppen t en h van T (waarbij $t = h$ is toegestaan).
Het top t wordt de staart van het gewerveld dier genoemd en h is het hoofd. Het aantal gewervelde dieren op n toppen is n^2T_n aangezien er T_n keuzes zijn voor T, en voor elk van deze zijn er n mogelijkheden voor elk van t en h. Zij V_n de verzameling van alle gewervelde dieren op n toppen.
Om de geldigheid van Cayley's formule te bewijzen, volstaat het om een bijectie te maken:

$$J: V_n \to n^n$$

Waarom het woord gewerveld? Gegeven de boom T met staart t en hoofd h, is er een uniek pad van t naar h, dat we ons voorstellen als de ruggengraat van een of ander wezen. De bogen die niet op dit pad liggen zijn de aanhangsels van het wezen. Wanneer we een gewerveld dier tekenen, markeren we zijn ruggengraat, die gebruikt zal worden in de constructie van onze bijectie. Zie figuur 1.

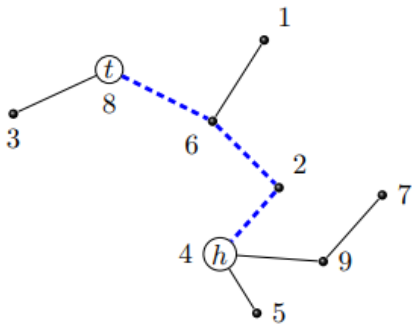


FIGURE 1. Vertebrate on 9 vertices with tail vertex 8 and head vertex 4.

Bijectie.
We beschrijven eerst de afbeelding $J: V_n \to n^n$ aan de hand van het voorbeeld van het gewervelde dier T van figuur 1 met staart $t = 8$ en kop $h = 4$. Om de overeenkomstige afbeelding $f: 9 \to 9$ te vinden, begin je met de waarden van f langs de ruggengraat.
De hoekpunten van de wervelkolom, in de volgorde van staart tot hoofd langs de wervelkolom, zijn:

$$8, 6, 2, 4,$$

Zet deze getallen in twee rijen. De bovenste rij is de natuurlijke ordening van deze getallen en de onderste is hun "ruggengraat-ordening":

i	2	4	6	8
$f(i)$	8	6	2	4

.

*

Begin dan met het definiëren van f door elk getal in de bovenste rij naar het overeenkomstige getal eronder te sturen, zoals weergegeven in de tabel. Nu moeten nog waarden worden toegekend aan de toppen langs de aanhangsels. Om dit te doen, richt je de bogen die invallen op de aanhangseltoppen zodat ze naar de ruggengraat wijzen, zoals getoond in Figuur 2.

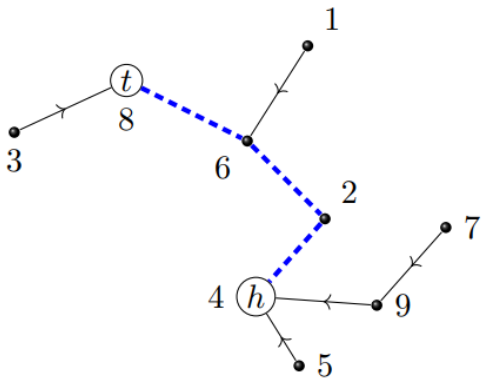


FIGURE 2. Directing addendage edges towards the spine.

Als het gehele getal i een aanhangsel-top is, laat dan $f(i)$ de top zijn dat aan i grenst op het pad dat naar de ruggengraat leidt. Dus bijvoorbeeld $f(7) = 9$ en $f(9) = 4$. Het invullen van deze waarden definieert f op de rest van zijn domein:

i	1	2	3	4	5	6	7	8	9
$f(i)$	6	8	8	6	4	2	9	4	4

We laten nu $J\big(T,(t,h)\big) = f \in 9^9$:

Definitie van de afbeelding $J: V_n \to n^n$

Laat $T,(t,h)$ een gewerveld dier zijn. Onze taak is om $f := J(T,(t,h)) \in n^n$

1. Definieer eerst f voor de toppen langs de ruggengraat. Stel dat de hoekpunten langs de ruggengraat $v_1,\dots,v_k$, in volgorde langs de wervelkolom van staart naar hoofd.
   Zij $a_1 < \cdots < a_k$ de permutatie van deze toppen in de ruggengraat in hun natuurlijke volgorde als gehele getallen. Definieer dan $f(a_i) = v_i$ voor $i = 1,\dots,k$. Dus, f permuteert de toppen van de ruggengraat.
2. Richt vervolgens alle bogen die voorkomen op aanhangsel (niet spinale) toppen zodat ze naar de wervelkolom wijzen. Als i een aanhangselhoekpunt is, definieer $f(i) = j$ als j het hoekpunt is dat aan i grenst langs het gerichte pad van i naar de wervelkolom.

i	1	2	3	4	5	6	7	8	9
$f(i)$	3	5	8	7	5	1	4	1	2

FIGURE 4. A function $f: \underline{9} \to \underline{9}$.

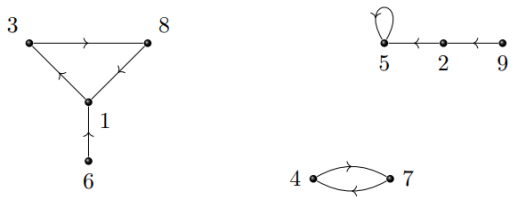


FIGURE 5. Directed graph associated with the function in Figure 4.

De inverse afbeelding.

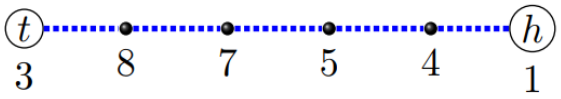
We beschrijven nu de inverse van de afbeelding $J: V_n \to n^n$ met een voorbeeld.
Beschouw de functie gegeven door de tabel in Figuur 4. We zijn op zoek naar een gewerveld dier.
Om te beginnen, associeer een gerichte graf met f met toppenverzameling 9 en met bogen $(i, f(i))$

voor $i \in 9$. Deze graf is afgebeeld in figuur 5. Elk van de componenten van de resulterende graf heeft een unieke cyclus.

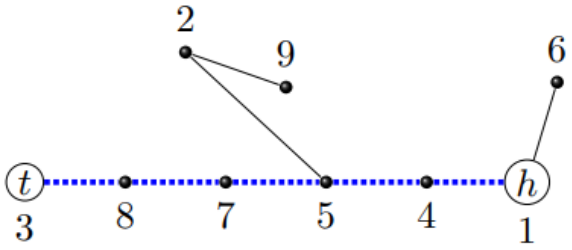
De cycli zijn $1 \to 3 \to 8 \to 1$, en $5 \to 5$, en $4 \to 7 \to 4$. Beschouw de functie beperkt tot de toppen in deze cycli:

i	1	3	4	5	7	8
$f(i)$	3	8	7	5	4	1

De lijst met toppen in de onderste rij van de tabel definieert de ruggengraat, van staart tot kop, van het gewervelde dier dat we zoeken:



Tot slot verbinden we aan elk aanhangseltop i de boog $\{i, f(i)\}$. Dit zijn ongerichte versies van de bogen in figuur 5:



PROBLEEM 3. Pas de afbeelding $J: V_n \to n^n$ toe op de bovenstaande wervel om te zien dat je de oorspronkelijke functie f terugkrijgt.

De inverse afbeelding: $J^{-1}: n^n \to V_n$

Zij $f: n \to n$. Onze taak is het vinden van een gewervelde $T, (t, h)$ zodat $J\big(T, (t, h)\big) = f$.

1. Maak een gerichte grafiek G met toppenverzameling set n en gerichte bogen $(i, f(i))$ voor $i \in n$.
2. Zij $i_1 < i_2 < \cdots < i_k$ (met de natuurlijke volgorde als gehele getallen) de toppen die voorkomen in cycli in G. Definieer de wervelkolom van het gewervelde dier $T, (t, h)$ dat we construeren als de pad graf met toppen $f(i_1), \ldots, f(i_k)$. Dus $t := f(i_1)$ en $h := f(i_k)$.
3. Voeg ten slotte voor elk top i van G dat zich niet in een cyclus bevindt, de (ongerichte) boog $\{i, f(i)\}$ toe aan T.

Voorbeeld.

Hier is een laatste voorbeeld dat het speciale geval illustreert waarbij $t = h$.

Begin met het gewervelde dier $T, (t, h)$ in figuur 6

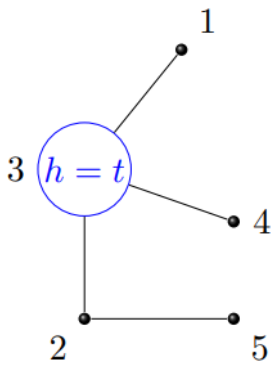


FIGURE 6. Vertebrate in for which $t = h$

Om de bijbehorende functie $f := J(T, (t, h))$ te definiëren, definiëren we f eerst langs de ruggengraat zoals in de tabel $(*)$. Hieruit volgt dat $f(3) = 3$. Vervolgens richten we de bogen van het aanhangsel (in dit geval alle bogen) naar de ruggengraat en lezen we de rest van de functie af:

i	1	2	3	4	5
$f(i)$	3	3	3	3	2

Om het proces om te keren, teken je eerst de gerichte graf G die overeenkomt met f zoals in Figuur 7.

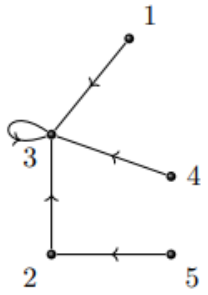


FIGURE 7. Graph for the function corresponding to the vertebrate in Figure 6.

Er is maar één verbonden component met G, en die heeft één cyclus: een lus op 3. Dit betekent dat het corresponderende gewervelde dier een wervelkolom heeft met $t = h = 3$. Door de aanhangselbogen $\{i, f(i)\}$ voor $i \neq 3$ toe te voegen, krijgen we het oorspronkelijke gewerveld dier terug.

Gevolg 12. Het aantal gewortelde genummerde bomen op n toppen is n^{n-1}.

Gevolg 13. Het aantal gewortelde genummerde bossen op n toppen is $(n+1)^{n-1}$.

Bewijs. Voeg een top toe aan het bos en verbind die met alle wortels van de resp. bomen. Nu hebben we een genummerde boom op $n+1$ toppen.
Dit gaat ook omgekeerd: vertrek van een genummerde boom met $n+1$ toppen en neem top nummer 1 weg. Alle buren van deze top maak je wortel van de samenhangscomponenten die overblijven. Dus is het aantal gewortelde genummerde bossen juist

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

□

Definitie 34. Zij G een graf en $w: E(G) \to \mathbb{R}^+$ een functie die aan elke pijl een **prijs** of **gewicht** toekent en welke we een gewichtsfunctie noemen. Een graf samen met een gewichtsfunctie heet een gewogen graf.

Wat we meestal zoeken, is een opspannende deelgraf met minimaal gewicht in een ongerichte graf G. Dit betekent dat de som van de gewichten van de pijlen van de opspannende deelgraf minimaal is. Deze is zeker een boom omdat hij minimaal samenhangend moet zijn. We geven een algoritme.

Gierigheidsalgoritme (Kruskal).
Om een opspannende boom T van minimaal gewicht te vinden in een gewogen samenhangende ongerichte simpele graf (G, w):

1. Neem een boog met kleinste gewicht om T te starten;
2. Neem een boog met kleinste gewicht in G die nog niet tot T behoort en geen cyclus creëert als je hem aan T toevoegt.
3. Ga naar (2) tot T een opspannende boom is.

Geeft dit algoritme nu de opspannende boom met het kleinste gewicht? Om hierop te antwoorden geven we eerst een lemma.

Lemma 6. Zij F en F' twee bossen op dezelfde toppenverzameling en onderstel dat F minder bogen heeft dan F'. Dan heeft F' een boog b die we kunnen toevoegen aan F zodanig dat $F \cup \{b\}$ nog steeds een bos is.

Bewijs. Uit het ongerijmde:
Stel dat er niet zo'n boog b is, dus om het even welke boog b die we uit F' nemen en aan F toevoegen zorgt ervoor dat we geen bos meer krijgen, dus dat betekend dat er een cyclus is.

Dus uit het ongerijmde:
Als er zo geen boog is, hebben we dus dat om het even welke boog die we kiezen uit F' een cyclus zal krijgen.

Alle bogen van F' toppen gaan verbinden uit een zelfde samenhangscomponent van F, want als we een boog verbinden met toppen uit twee verschillende samenhangscomponenten krijgen we gewoon een grotere boom en geen cyclus. Dus als de bogen die we toevoegen telkens voor cyclussen zorgen dan zitten we binnen die samenhangscomponenten te werken.

Dus dan weten we dat alle bogen van F' toppen gaan verbinden binnen dezelfde samenhangscomponent/boom van F. Maar dan hebben we dat de F' minstens evenveel componenten moet hebben als F en dus is het aantal samenhangscomponenten van $F = k$.

Dan weten we dat F juist $m-k$ bogen heeft, maar onze F' heeft meer bogen dan F en dat is een tegenspraak. □

We hebben afgeleid:
Als ik twee bossen heb waarvan 1 minder bogen heeft dan de andere dan kan ik altijd uit die andere met meer bogen nog een boog uitnemen en toevoegen zonder een cyclus te maken.

Stelling 39. Het gierigheidsalgoritme vindt steeds een opspannende boom met minimaal gewicht.

Bewijs.
We nemen de resulterende boom van het gierigheidsalgoritme T en we veronderstellen in onze graf G toch nog een lichtere opspannende boom H zou bestaan. het gierigheidsalgoritme heeft dus niet boom gekozen. We gaan de bogen van H zodanig gaan ordenen dat het gewicht stijgt:

$$w(h_1) \leq w(h_2) \leq \cdots \leq w(h_{n-1})^{23}$$

We doen hetzelfde voor T

$$w(t_1) \leq w(t_2) \leq \cdots \leq w(t_{n-1})$$

In het maken van keuzes in het gierigheidsalgoritme het niet anders kan zijn het lichts uitkomen, als we veronderstellen dat er nog een lichtere is zouden we nu een tegenspraak gaan maken.
Vermits het gierigheidsalgoritme begint met de alle lichtste boog, moet gelden:

$$w(t_1) \leq w(h_1)$$

Nu kijken we naar de eerste index i van H waar die lichter wordt dan T, dus i is het kleinste getal zodanig dat als we de som van de gewichten nemen tot i dat we dan vallen onder de som van de gewichten van de eerste i bogen van T.

$$\sum_{j=1}^{i} w(h_j) < \sum_{j=1}^{i} w(t_j)$$

Dus doordat er een lichtere boom bestaat uit onze veronderstelling, moet $i > 1$
i is de eerste index waar H lichter wordt dan T dus:

$$w(h_i) < w(t_i)$$

En ook:

$$\sum_{j=1}^{i-1} w(h_j) \geq \sum_{j=1}^{i-1} w(t_j)$$

Want i is de eerste index waar de som van H het lichter wordt!

We gaan het bos[24] T_{i-1} nemen dat geleverd wordt door het gierigheidsalgoritme na $i-1$ stappen.
We nemen dan ook H_i[25]

[23] $\leq$ omdat we bogen kunnen hebben met hetzelfde gewicht. $n-1$: omdat we een graf hebben met n toppen, onze opspannende boom moet dus n toppen hebben dus we weten dat die $n-1$ bogen heeft.
[24] Op dit moment hebben we nog niets iets samenhangend.
[25] H_i is het bos bestaat uit de bogen $\{h_1, h_2, \ldots, h_i\}$ tot en met de h_i

Nu hebben we 2 bossen op dezelfde toppen gemaakt, uit *lemma 6* kunnen we uit H_i[26] een boog gaan toevoegen aan de T_{i-1} zodanig dat het nog steeds een bos blijft, die boog is een zekere h_j maar die index moet kleiner zijn dan i $(j \leq i)$. En:

$$w(h_j) \leq w(h_i) < w(t_i)$$

Dan was er eigenlijk een boog in onze graf met gewicht kleiner $w(t_i)$, maar dan zou dat algoritme nooit t_i gekozen hebben in de i-de stap maar de h_j die lichter is, en dat is een tegenspraak. □

Gerelateerd hiermee is het zeer gekende **handelsreizigersprobleem** (traveling salesman problem) binnen de computerwetenschappen en operationeel onderzoek, nl. als er n steden gegeven zijn die een handelsreiziger moet bezoeken, samen met de afstand tussen ieder paar van deze steden, vind dan de kortste weg die kan worden gebruikt, waarbij iedere stad juist één keer wordt bezocht en die eindigt bij het beginpunt. Hier zoeken we dan eigenlijk een Hamiltoncyclus met minimaal gewicht.

Het tellen van opspannende bomen

De incidentiematrix

Zij G een gerichte multigraf zonder lussen[27]. Zij $V(G) = \{v_1, v_2, \dots, v_n\}$ en $E(G) = \{b_1, b_2, \dots, b_m\}$ nummeringen van de toppen en pijlen van G. De **incidentiematrix** van G is de $(n \times m)$-matrix B_G met

$$\begin{cases} b_{ij} \coloneqq 1 & \text{als } v_i \text{ het eindpunt is van } b_j \\ b_{ij} \coloneqq -1 & \text{als } v_i \text{ het beginpunt is van } b_j \\ b_{ij} \coloneqq 0 & \text{in alle andere gevallen} \end{cases}$$

Stelling 40 (Kirchhoff). Zij G een gerichte multigraf zonder lussen en zij B de incidentiematrix van G. Stel B_0 gelijk aan de matrix die ontstaat na verwijdering van om het even welke rij van B.
Het aantal opspannende bomen in G is dan gelijk aan $detB_0B_0^T$.

Bewijs.
We mogen om en even welke rij verwijderen, in het bewijs gaan we zeggen: "eigenlijk is het om het even welke rij weg laten hetzelfde de toppen te gaan hernummeren en der voor zorgen dat de rij die we hebben weg gelaten in het maken van de B_0 de laatste is.

- n = aantal toppen
- m = aantal bogen

Als $m < n - 1$ dan kunnen we geen samenhangende graf hebben[28]. Als dit zich voordoet kunnen we zeker geen opspannende boom vinden. Dus als we toch opspannende bomen willen vinden moet $m \geq n - 1$. In de $(n \times m)$-matrix gaan we dus zeker een deelmatrix C kunnen nemen van B_0 die $(n - 1 \times m - 1)$ is.

We beweren dat:
$|\det C| = 1$
$\Leftrightarrow$ De deelgraf G_c bepaald door is door de kolommen van C[29] een opspannende boom is,
anders is $\det C = 0$.

---

[26] H_i heeft meer bogen dan de T_{i-1}
[27] Dus gerichte simpele graf wanneer er geen parallelle pijlen zijn.
[28] Stelling 37. Een boom met n toppen heeft $n - 1$ bogen. We hebben nu een graf maar we willen een boom maken, we vertrekken niet noodzakelijk van een boom.
[29] Dit zijn juist $n - 1$ pijlen van G.

We gaan dit bewijzen per inductie op n:
De basisstap van de inductie is voor $\boldsymbol{n = 2}$.
We hebben dus 2 toppen en is de stelling duidelijk waar.

Inductie hypothese:
We veronderstellen in de G_C een top v_i is met graad 1[30], dit wil zeggen als we in de i-de rij van de incidentiematrix gaan kijken dat daar maar 1 niet 0 element zal staan. Want hij is ofwel de top of het eindpunt van één pijl.

We kiezen deze top v_i omdat we dan gemakkelijk determinant van C kunnen ontwikkelen volgens die i-de rij, We hebben in die rij enkel ($+1$ of -1) en dan moeten we naar de rest gaan kijken a.d.h.v. de cofactor. Voor die cofactor kunnen we de inductiehypothese gebruiken, want die cofactor die zal dan de determinant van de matrix zijn die overeenkomt met de graf G_c waaruit we de v_i uit hebben weggelaten. We noteren dit als $G_C - v_i$.

Wegens onze inductiehypothese krijgen we dus een opspannende boom $G_C - v_i$ van onze originele $G - v_i \Leftrightarrow G_c$ een opspannende boom was van G.

Stel dat er nu toch geen enkele top was van graad 1 in de G_C[31], dan gaat de G_C geen boom zijn want een boom moet altijd top met een blad hebben, als hij geen boom is kan hij zeker geen opspannende boom zijn.

Maar onze G_C doordat die overeenkomt met een $(n-1 \times m-1)$-matrix heeft hij wel $n-1$ pijlen en $n-1$ toppen. Maar dan moet G_C een top van graad 0 hebben. Als dit niet v_n, de top van de weggelaten rij is, dan heeft C een nulle rij zodat $\det C = 0$.

Als v_n de geïsoleerde top was, dan bevat elke kolom van C een $+1$ en een -1. Alle overig toppen zitten dus ofwel als begin al eindpunt, maar als we dan de som gaan nemen van alle rijen dan kunnen we eigenlijk de 0-rij maken, maar dan wil dat zeggen de rijen van onze C lineair afhankelijk waren en dan is de $\det C = 0$

Nu gebruiken we de formule van Cauchy-Binet (zie Appendix A) die zegt dat:

$$\det B_0 B_0^T = \sum_{\text{C een } (n-1 \times n-1)-\text{deelmatrix van } B_0} (detC)^2$$

Maar we weten dat $(\det C)^2 = 1$ of 0, naargelang de kolommen van C een opspannende boom bepalen of niet. □

We hebben het aantal opspannende bomen in $G = \det B_0 B_0^T$, we hebben dat bewezen door te gaan linken C vanwaar we aantonen de $\det C = 1$ is $\Leftrightarrow$ we een opspannende boom 0 hebben anders 0

Als de graf ongericht is, hebben we een analoge stelling. We definiëren hiervoor eerst een andere matrix. Zij G een ongerichte simpele graf met genummerde toppen en bogen $\{v_1, v_2, \dots, v_n\}$ en $\{b_1, b_2, \dots, b_m\}$ respectievelijk. **De Laplaciaanse matrix** L_G is e $(n \times n)$-matrix met:

$$\begin{cases} l_{ij} \coloneqq \deg(v_i) & als\ i = j \\ l_{ij} \coloneqq -1 & als\ i \neq j\ en\ v_i \sim v_j \\ l_{ij} \coloneqq 0 & in\ alle\ andere\ gevalen \end{cases}$$

[30] Als we kijken naar gerichte graffen met pijlen dan betekend de graad van een top dat de $ingraad + uitgraad = 1$ is
[31] Behalve misschien v_n, de top die we weglieten in B_0

Stelling 41. Het aantal opspannende bomen in een ongerichte simpele graf is gelijk aan elke cofactor van L_G.

Bewijs.
We kennen al de oplossing van het probleem van in een gerichte graf. We maken van G gerichte graf H. We gaan elke boog die we hebben tussen top u en top v vervangen door twee pijlen $u \to v$ en $u \leftarrow v$.

We kijken nu naar de incidentiematrix van B_0 van H, met daarin de laatste rij weglaten. We weten dat de $\det B_0 B_0^T$ het aantal opspannende bomen in de gerichte graf we gaan nu beweren dat we die $B_0 B_0^T$ in verband kunnen brengen met die Laplaciaanse matrix, we gaan van onze Laplaciaanse matrix de laatste rij en kolom weglaten. En we beweren:

$$B_0 B_0^T = 2L_{0G}{}^{32}$$

Wat zit er op plaats (i, j) van $B_0 B_0^T$ staat het scalair product van de i-de en de j-de rij van b_0:

$$\sum_{k=1}^{m} b_{ik} b_{jk}$$

Als $i = j$ zal elke pijl die in v_i vertrekt of aankomt een bijdrage 1 hebben in dit product. In totaal hebben we dus $2deg(v_i)$ op plaats (i, i). Voor $i \neq j$ zal elke pijl $v_i \to v_j$ en elke pijl $v_i \leftarrow v_j$ een bijdrage -1 hebben. Dit geeft dus -2 of 0 op plaats (i, j), naargelang v_i en v_j adjacent zijn of niet.

Nu geldt dus dat $B_0 B_0^T = \det 2L_{0G} = 2^{n-1} \det L_{0G}$. Maar elke opspannende boom van G geeft aanleiding tot 2^{n-1} opspannende bomen in H omdat er 2^{n-1} manieren zijn om de bogen te oriënteren. □

Toepassing. Het aantal opspannende bomen in een complete graf K_n met genummerde toppen is n^{n-2}.

Dit volgt uit:

$$L_{k_n} = \begin{pmatrix} n-1 & -1 & -1 & \cdots & -1 \\ -1 & n-1 & -1 & & -1 \\ & \vdots & & \ddots & \vdots \\ -1 & -1 & -1 & \cdots & n-1 \end{pmatrix}$$

Dit geeft ons een alternatief bewijs van de stelling van Cayley.

Samenhang van een graf bestuderen

Definitie 35 Adjacentiematrix.
Zij G een multigraf van orde n met genummerde toppen. Definieer de adjacentiematrix A_G van G als de $(n \times n)$-matrix met a_{ij} gelijk aan het aantal pijlen van de i-de naar de j-de top. Een lus wordt tweemaal geteld in een ongerichte graf en éénmaal in een gerichte. De adjacentiematrix bevat veel informatie over de graf G.

Stelling 42. Zij $k > 0$. Het element op plaats (i, j) in de k-de macht A_G^k geeft het aantal (gerichte) wandelingen van lengte k van top i naar top j.

[32] $2L_{0G}$= 2 maal de Laplaciaanse matrix met de laatste rij en laatste kolom weggelaten.

Bewijs. Per inductie op k
Als $k = 1$ tellen we wandelingen van lengte 1, dus bogen. De adjacentiematrix die we dan tot de eerste macht nemen kijkt juist naar die bogen die we tussen toppen hebben. Dus dat geeft al onze wandelingen (Definitie van A_G).

Onderstel dat de stelling waar is voor de k-de macht. Zij l een top van G. Als er b_{il} wandelingen zijn van lengte k van i tot l en a_{lj} wandelingen van lengte 1 (t.t.z. pijlen) van l naar j, dan zijn er:

$$b_{il}a_{lj}$$

wandelingen van lengte $k + 1$ van i tot j die langs l gaan. Dus is het aantal wandelingen van lengte $k + 1$ tussen i en j in totaal gelijk aan:

$$\sum_{l \in V(G)} b_{il}a_{lj} =: c_{ij}$$

De inductiehypothese levert dat b_{il} het element is op plaats (i, l) in A_G^k zodat c_{ij} juist het element is op plaats (i, j) van het matrixproduct:

$$A_G^k A_G = A_G^{k+1}$$

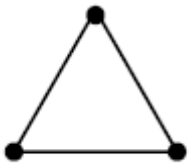
Stelling 43.
Zij een G een ongerichte multigraf op n toppen met adjacentiematrix A_G. Dan is G samenhangend ⇔ $(I_n + A_G)^{n-1}$ enkel strikt positieve elementen heeft.

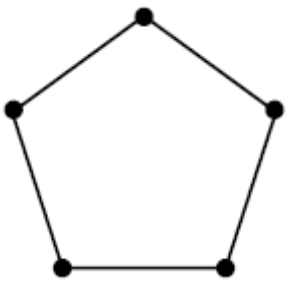
Bewijs.
Als we een pad gaan nemen tussen twee toppen van G dan gaat ten hoogste $n - 1$ bogen hebben.
G samenhangend ⇔ voor elke twee toppen i, j er een k bestaat die begrenst is door die $n - 1$.
een $k \leq n - 1$ is een pad van lengte k van de i-de naar de j-de top.
Dus $\forall i, j \in V(G): \exists k < n: \left(A_G^k\right)_{ij} > 0$. Vermits $(I_n + A_G)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} A_G^k$ □

4.7 Bipartiete graffen

Definitie 36. Een multigraf heet **bipartiet** indien zijn toppenverzameling kan gepartitioneerd worden in twee delen zodat er geen enkele pijl is die toppen verbindt in hetzelfde deel.

We kunnen de toppen van de graf kleuren met twee kleuren zodat geen aangrenzende toppen dezelfde kleur hebben.
Het is eenvoudig na te gaan dat de driehoeksgraf C_3 niet bipartiet is. Ook het pentagon C_5 niet.
In het algemeen is een cyclus van oneven lengte niet bipartiet. Als een graf een cyclus van oneven lengte omvat, is hij zeker niet bipartiet. Omgekeerd ook.





Stelling 44. Een ongerichte multigraf G is bipartiet $\Leftrightarrow$ G geen cyclus bevat van oneven lengte.
Bewijs.

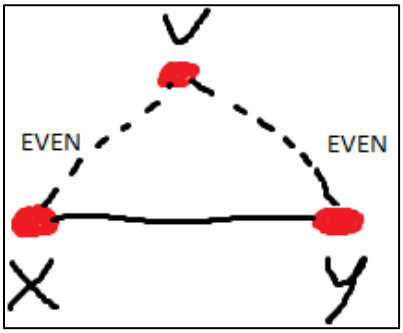
$\Rightarrow$
We veronderstellen dat we een ongerichte bipartiete multigraf G hebben en een cyclus van oneven lengte:

$$v_1 \sim v_2 \sim \ldots \sim v_{2m+1}$$

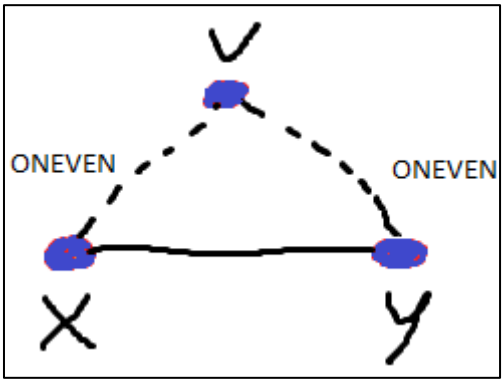
Als we v_1 rood kleuren dan moet v_2 blauw zijn, …, v_{2m+1} rood, maar het probleem is nu dat v_1 niet aangrenzend mag zijn met v_{2m+1} maar door de cyclus is dat wel zo dus tegenspraak.

$\Leftarrow$
Als we geen cyclus hebben van oneven lengte, kunnen we dan tonen dat hij bipartiet is?
We veronderstellen een graf G zonder oneven cyclus en we gaan onze toppen proberen te verdelen in twee kleurenverzamelingen.
We nemen een willekeurige top v en die kleuren we rood, we kleuren alle buren van v blauw.
Als we dan verder gaan op die manier, vanuit die blauwe toppen zullen al die buren rood zijn.
In het algemeen krijgen we dat een top t rood zal zijn als de afstand tot v even is en anders blauw is.
We blijven dit herhalen, als G niet samenhangend is, herhalen we dit desnoods in elke samenhangscomponent.

We tonen nu aan dat deze kleuring de graf bipartiet maakt:
Stel dat we toch twee aangrenzende toppen x en y rood zijn, dan zou er een pad van even lengte zijn van x tot v en een pad van even lengte van y tot v.



Dit levert minstens een cyclus van oneven lengte en dat is een tegenspraak. Dezelfde redenering gaat ook voor blauw:



Het pad van $x \sim v \sim y \sim x$ is oneven omdat het pad $x \sim v \sim y$ even is. □

Stelling 45. Zij G een bipartiete ongerichte graf met n toppen. Dan heeft G ten hoogste $\frac{n^2}{4}$ bogen als n even is en ten hoogste $\frac{n^2-1}{4}$ als n oneven is.

Deze stelling geeft een bovengrens voor bipartiete graffen. Hebben we meer dan $\frac{n^2}{4}$ bogen in een graf met een even aantal toppen, dan weten we dat er bogen gaan zijn tussen zelfde gekleurde toppen. Als een graf meer bogen heeft, is hij niet bipartiet en bevat hij dus een cyclus van oneven lengte.

Bewijs.
Zij G een bipartiete ongerichte graf met n toppen. We kiezen G zodanig dat er geen andere bipartiete graf met n toppen bestaat die meer bogen heeft.[33] We stellen de variabele:

- r = het aantal rode toppen.
- b = het aantal blauwe toppen.

Doordat de graf G maximaal is, zal elke rode top verbinden zijn met elke blauwe, Dus heeft G juist rb bogen.

$$n = r + b$$

Dus kunnen we b uitdrukken als volgt:

$$b = n - r$$

Dus:

$$rb = r(n - r)$$

We hebben $r(n - r)$ bogen.

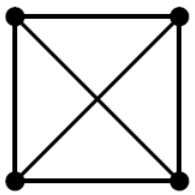
r is een parameter en we zoeken nu waar r maximaal is, we moeten een $r \in [1; n]$ zodanig dat de functie:

$$f(r) = r(n - r)$$

een maximum bereikt. □

Stelling 46. Zij H een ongerichte simpele graf met $2m$ toppen[34] $(m \geq 2)$ en minstens $m^2 + 1$ bogen. Dan bevat H een driehoeksgraf[35].

Bewijs. Per inductie op m.
Als $m = 2$ dan hebben we een graf H met 4 toppen. H moet een deelgraf zijn van de K_4 met minstens 5 bogen. (Stelling 45) zegt ons als we een even aantal toppen hebben we ten hoogste $\frac{n^2}{4} = \frac{4^2}{4} = 4$ bogen mogen hebben om bipartiet te zijn. We hebben minstens 5 bogen dus H is niet bipartiet en heeft dus een cyclus van oneven lengte. Dit moet een driehoekgraf zijn omdat H maar vier toppen heeft.



We kunnen nu veronderstellen dat de stelling waar is voor alle graffen met minder dan $2m$ toppen. De graf waarvan we gaan vertrekken heeft dus $2m$ toppen en we moeten gaan aantonen dat we daarin een driehoeksgraf hebben.

[33] Maximaal voorbeeld.
[34] Even aantal toppen.
[35] Cyclus van oneven lengte.

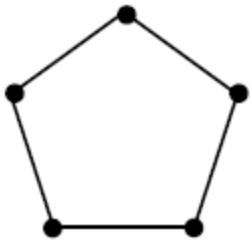
In een graf h met $2m$ toppen nemen we twee aangrenzende toppen u en v.
Als $\deg(u) + \deg(v) > 2m$, dan hebben deze topen een gemeenschappelijke buur die een driehoek zal vormen. Als $\deg(u) + \deg(v) \leq 2m$, dan verwijderen u en v uit H en ook alle bogen van u en v.

Maar als $\deg(u) + \deg(v) \leq 2m$ en die u en v waren aangrenzend, en we verwijderen u en v en alle bogen waar ze op zitten uit H, dan gaat het aantal bogen afnemen in H met ten hoogste $2m - 1$.

Het resultaat is dus een graf met $2m - 2$ toppen en minstens:

$$m^2 + 1 - (2m - 1) = m^2 - 2m + 2 = (m - 1)^2 + 1$$

Bogen. Deze graf H wegens de inductiehypothese een driehoek. □



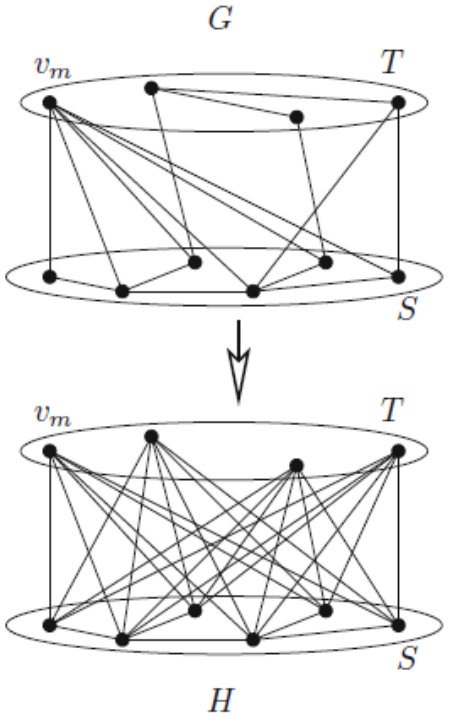
We kunnen zonder teveel moeite Stelling 45 veralgemenen tot een iets grotere klasse van graffen. We weten dat een bipartiete graf nooit een driehoeksgraf kan bevatten. Een driehoeksgraf komt voor in elke complete graf K_r voor $r > 2$ zodat een bipartiete graf geen deelgraf K_r kan hebben voor $r > 2$. Er bestaan wel graffen zonder K_r die niet bipartiet zijn (denk aan C_5)

Een r-kliek in G is een volledige subgraaf van G op r toppen, aangeduid met K_r.
Paul Turán stelde de volgende vraag:

Stel dat G een eenvoudige grafiek is die geen K_r bevat. Wat is het grootste aantal bogen dat G kan hebben?

Stelling 47 (Turán). Zij G een ongerichte simpele graf met n toppen die geen deelgraf K_r omvat voor een zekere $r \geq 2$. Dan is het aantal bogen in G ten hoogste $\frac{(r-2)n^2}{2r-2}$.

Bewijs. Per inductie op r.
Voor $r = 2$ is G een graf zonder bogen. De bovengrens $\frac{(r-2)n^2}{2r-2}$ is in dit geval ook gelijk aan 0.
In het eerste interessante geval $p = 3$
Dit bewijs maakt gebruik van de structuur van de Turán-graffen.
Zij $v_m \in V$ een top van maximale graad $d_m = max_{1 \leq j \leq n}\, d_j$.
Noem S de verzameling buren van v_m, $|S| = d_m$,
en stel $T := V \setminus S$. Aangezien G geen p-kliek bevat, en v_m aan alle toppen van S grenst, merken we op dat S geen $(p-1)$-kliek bevat.



We construeren nu de volgende grafiek H op V (zie de figuur). H komt overeen met G op S en bevat alle bogen tussen S en T, maar geen bogen binnen T. Met andere woorden, T is een onafhankelijke verzameling in H, en we concluderen dat H weer geen p-klieren heeft.

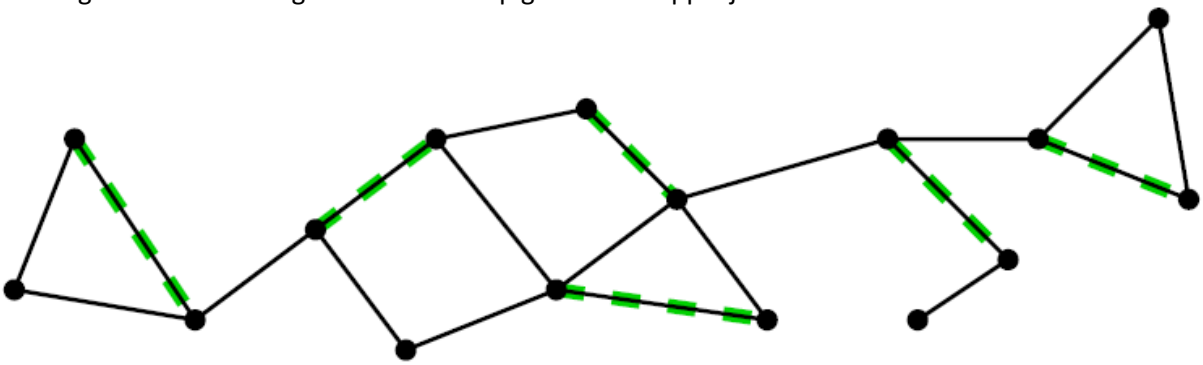
Zij d'_j de graad van v_j in H. Als $v_j \in S$, dan hebben we zeker $d'_j \geq d_j$ door de constructie van H, en voor $v_j \in T$ zien we $d'_j = |S| = d_m \geq d_j$ door de keuze van v_m.

We leiden $|E(H)| \geq |E|$ af en vinden dat er onder alle grafen met een maximaal aantal bogen er één moet zijn met de vorm van H. Door inductie heeft de door S geïnduceerde graf hooguit evenveel bogen als een geschikte graf $K_{n_1,\ldots,n_{p-2}}$ op S.

Dus $|E| \leq |E(H)| \leq E\left(K_{n_1,\ldots,n_{p-1}}\right)$ met $n_{p-1} = |T|$, wat (1) impliceert.

4.8 Koppelingen

Definitie 37. Een **koppeling** (Engels: "matching") in een ongerichte (multi) graf G is een verzameling van bogen van G waarin geen twee een top gemeenschappelijk hebben.



In het algemeen kan je in een gegeven graf vele verschillende koppelingen vinden. Eén enkele boog bijvoorbeeld vormt reeds een koppeling op zich.

Definitie 38. Een koppeling heet **maximaal** indien we ze niet kunnen uitbreiden tot een koppeling met meer bogen. Een **maximumkoppeling** in een graf G is een koppeling van maximale grootte. Dit wil zeggen dat er in G geen koppeling met meer bogen bestaat.

Zij K een koppeling in G. Een top van G heet ***K*-verzadigd** indien hij bevat is in een boog van K. Anders heet hij K-onverzadigd. Als het duidelijk is over welke koppeling K het gaat, spreken we gewoon van verzadigd en onverzadigd.

Een koppeling die alle toppen van een graf verzadigt wordt een **volledige koppeling** genoemd.

Een volledige koppeling is duidelijk een maximumkoppeling. Ook kan een graf alleen maar een volledige koppeling hebben als zijn aantal toppen even is.

Hoe kunnen we nu koppelingen vinden met zoveel mogelijk bogen in een gegeven graf?

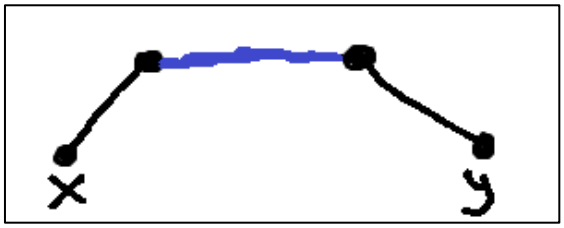
Een strategie zou kunnen zijn om een willekeurige boog te nemen, dan een boog te nemen die daar geen top mee gemeenschappelijk heeft, enz. We krijgen zo zeker een koppeling en van zodra we geen nieuwe boog meer kunnen toevoegen, is de koppeling maximaal. Er is echter geen garantie dat de gevonden koppeling een maximumkoppeling is. We hebben dus een betere manier nodig.

Definitie 39. Zij (V, E) een graf met een koppeling K. Een ***K*-wisselpad** is een pad waarvan de opeenvolgende bogen afwisselend wel en niet tot K behoren.
Een **vergrotend *K*-wisselpad** is een K-wisselpad waarvan de eerste en laatste top K-onverzadigd zijn.[36]

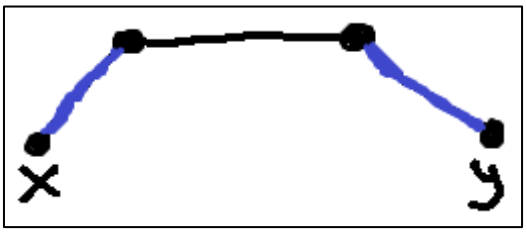
Elke boog vormt een wisselpad. Een boog waarvan beide toppen onverzadigd zijn vormt een vergrotend wisselpad.

[36] Niet op een groene boog liggen.

Als we in een graf een koppeling K hebben en een vergrotend K-wisselpad P, dan kunnen we in K de bogen die op P liggen vervangen door de bogen van P die niet in K zitten. Het resultaat is een koppeling K' die een boog meer heeft dan K. Vandaar de naam *vergrotend* wisselpad.



x en y zijn verzadigd, dus we kunnen een andere kleuren maken:



We kijken nog altijd naar hetzelfde pad en aantal toppen, maar hier hebben meer bogen en dus een groter wisselpad. Dus in de eerste afbeelding was de blauwe boog een vergrotend k-wisselpad.

Dus een vergrotend k-wisselpad, is een k-wisselpad waar de eerste en de laatste niet op mijn gekozen kleuring lagen, we kunnen dan de kleuring omwisselen om een groter k-wisselpad te krijgen.

Willen we nu een maximumkoppeling vinden in een graf G, dan kunnen we als volgt te werk gaan:

Eerst maken we een maximale koppeling volgens de methode van hierboven. We maken nu uit deze koppeling een koppeling met meer bogen door een vergrotend wisselpad te zoeken en bogen uit te wisselen. Dit kunnen we herhalen tot er geen vergrotend wisselpad meer kan gevonden worden. Dat we op deze manier een koppeling van maximale grootte bekomen, wordt door volgende stelling van de Deen Petersen gegarandeerd. Hoewel Petersen zijn stelling reeds in 1891 bewees, geraakte ze in vergetelheid. In 1957 bewees de Fransman Berge de stelling opnieuw. Daarom wordt deze stelling soms de stelling van Berge genoemd.

Stelling 48 (Petersen, 1891). Gegeven een ongerichte graf G. Een koppeling K in G is een maximumkoppeling ⇔ er in G geen vergrotend K-wisselpad bestaat.

Bewijs.

⇒

Als we een maximumkoppeling hebben, dan gaat er geen vergrotend K-wisselpad kunnen bestaan, Anders zouden we de koppeling kunnen vergroten en dan was het geen maximumkoppeling.

⇐

Contrapositie:

Veronderstel dat K een koppeling is die geen maximumkoppeling is, en dan moeten we tonen dat er wel een vergrotend K-wisselpad bestaat.

Omdat die koppeling geen maximumkoppeling is weten we dat we nog een andere koppeling K' zal bestaan die meer bogen heeft dan K.

We kijken vervolgens naar de verzameling:

$$E' = K \backslash K' \cup K' \backslash K$$[37]

Dit is een verzameling bogen, we kunnen dan gaan kijken naar de deelgraf H met E' als bogenverzameling en de toppenverzameling als de uiteinden van de bogen in E'.

Omdat K en K' koppelingen zijn, moet elke samenhangscomponent van H een cyclus of een pad zijn waar de bogen afwisselend is K en K' zitten.

Nu buiten we K geen maximumkoppeling is en K' meer bogen heeft:
Aangezien K' groter is dan K, moet er tenminste één component van H zijn die meer bogen van K' bevat dan K. Deze component zal dan een pad zijn waarvan de eerste en laatste top K-onverzadigd zijn. Dus dat is per definitie een vergrotend K-wisselpad. □

We hebben nu een manier om na te gaan of een koppeling een maximumkoppeling is en hebben ook gezien dat vergrotende wisselpaden helpen bij het vinden van een maximumkoppeling.

Kunnen we ook iets zeggen over de grootte van een maximumkoppeling in een gegeven graf? Algemene uitspraken zijn hierover moeilijk te doen.

Een cyclus van even lengte en een complete graf met een even aantal toppen hebben beide een volledige koppeling. Voor bipartiete graffen kunnen we echter meer zeggen.

4.9 Toewijzingen en het lessenroosterprobleem

Herinner dat de toppenverzameling V van een bipartiete graf de disjuncte unie is van twee verzamelingen V_1 en V_2 waarbij elke boog een top in V_1 en een top in V_2 heeft.

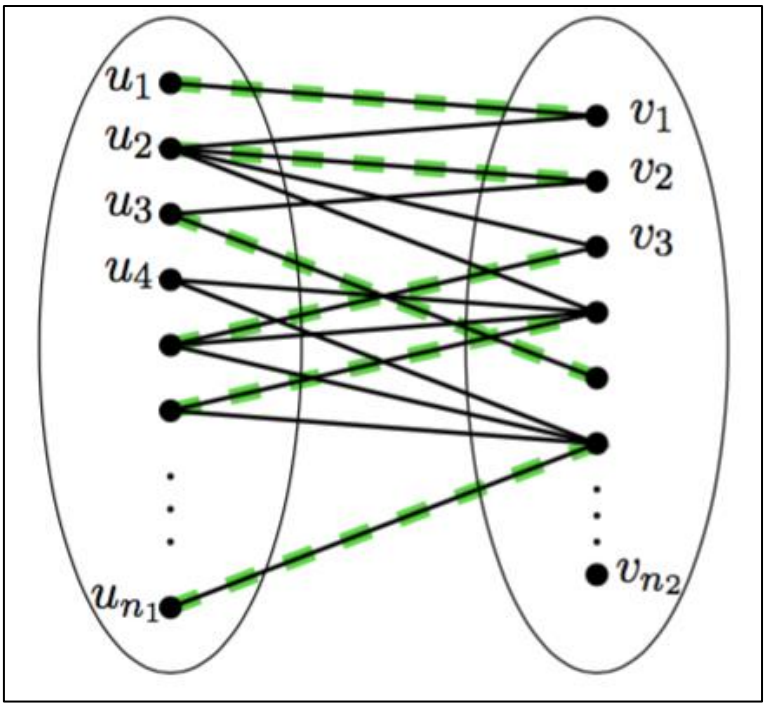
Definitie 40. Zij $G = (V_1 \cup V_2, E)$ een bipartiete ongerichte graf. Indien elke top van V_1 adjacent is met elke top van V_2, spreekt men van een **compleet bipartiete graf.** Als $|V_1| = m$ en $|V_2| = n$ noteren we zulke graf $K_{m,n}$.

Zoals jullie weten is het niet eenvoudig om een lessenrooster op te stellen. Het aantal beschikbare lokalen bijvoorbeeld is een bovengrens op het aantal lessen dat tegelijkertijd kan gegeven worden. Er zijn ook lessen die enkel in een speciaal ingericht lokaal (bijvoorbeeld een labo of een lokaal met dataprojector) kunnen gegeven worden. Men wil meestal twee uur na elkaar doceren in eenzelfde lokaal. Sommige docenten hebben nog andere eigenaardige wensen die het probleem zeker niet vereenvoudigen.

Veronderstel dat we een universiteit hebben met n_1 docenten $u_1, u_2, \dots, u_{n_1}$ en n_2 (disjuncte) studierichtingen die we $v_1, v_2, \dots, v_{n_2}$noteren. We kunnen een bipartiete graf opstellen met als toppen de docenten en de studierichtingen. Twee toppen u_i en v_j zijn adjacent als en slechts als docent u_i lesgeeft in richting v_j.

Indien we een lessenrooster willen opstellen zodanig dat zoveel mogelijk simultaan wordt lesgegeven, kunnen we het probleem formuleren met koppelingen in een bipartiete graf. Elke koppeling komt overeen met een bepaald tijdslot waarin de docenten lesgeven aan een bepaalde groep studenten zodat het probleem herleid wordt tot het bepalen van een maximumkoppeling per tijdslot rekening houdend met de gestelde randvoorwaarden.

[37] We kijken naar de koppeling K en we gooien daar de bogen uit die in K'zitten, anders kijken we ook naar de koppeling K' en we gooien daar de bogen uit die in K zitten. Die steken we samen in een unie.



Wanneer elke docent alvast les zou willen geven in het tijdslot $10-12$, zouden we dus al zeker een koppeling moet vinden bestaande uit n_1 bogen. Het zal duidelijk zijn dat dergelijke voorwaarde niet altijd kan voldaan zijn.

Definitie 41. Stel $G = (V_1 \cup V_2, E)$ bipartiet ongericht en $W \subset V_1$.
Een toewijzing (Engels: assignment) van W in V_2 is een koppeling K tussen toppen van W en V_2 die alle toppen van W verzadigt. Als W' de deelverzameling is van V_2 die door K verzadigd wordt, is K ook een toewijzing van W' in V_1.

Een toewijzing is **maximaal** als de bijhorende koppeling maximaal is. We spreken van een **maximumtoewijzing** (respectievelijk **volledige toewijzing**) wanneer de bijhorende koppeling een maximumkoppeling (resp. volledige koppeling) is.

Wij zijn vooral geïnteresseerd in toewijzingen van de volledige verzameling V_1 in V_2.
We kunnen ons afvragen wanneer zulke toewijzing bestaat. Het antwoord wordt gegeven door een stelling van Philip Hall (1904-1982).

We zullen volgende notatie gebruiken: voor $W \subset V_1$ noteren we met $H(W)$ **de verzameling van buren van toppen** van W. Dit zijn dus toppen van V_2 die verbonden zijn met minstens 1 top in W.

Stelling 49 (P. Hall, 1935). Zij $G = (V_1 \cup V_2, E)$ een bipartiete ongerichte graf. Een toewijzing van V_1 in V_2[38] bestaat ⇔ voor elke deelverzameling W van V_1 geldt dat $|H(W)| \geq |W|$.

Bewijs.
Het is duidelijk dat de voorwaarde nodig is. Inderdaad: elke deelverzameling van V_1 moet genoeg buren hebben, dit wil zeggen ten minste evenveel elementen als het aantal elementen in de verzameling zelf.

We bewijzen nu dat deze voorwaarde ook voldoende is. Neem dus aan dat de voorwaarde van Hall voldaan is (dus $\forall\, W \subset V_1 : |H(W)| \geq |W|$)39.

We bewijzen op inductie op $|V_1|$:
We gaan dus bewijzen per inductie op het aantal elementen in V_1, dat er een toewijzing van V_1 in V_2 bestaat.

Stel dat $|V_1| = 1$, dan is V_1 een singleton $\{u\}$. De voorwaarde van Hall geeft $|H(\{u\})| \geq 1$. De top u heeft dus ten minste 1 buur in V_2. Neem zo een buur en noem hem v. De boog $u{\sim}v$ vormt dan een toewijzing van V_1 in V_2.

Inductiestap:
We nemen aan dat de stelling waar is voor alle bipartiete graffen met $|V_1| \leq k$ toppen.
We gaan nu aannemen dat $|V_1| = k + 1$ toppen heeft. Dan willen we een volledige toewijzing vinden als mijn stelling van Hall waar is.

We onderscheiden twee gevallen voor een bipartiete graf $G = (V_1 \cup V_2, E)$ met $|V_1| = k + 1$.
Het eerste geval is dat elke echte deelverzameling[40] van V_1 meer buren heeft dan de voorwaarde van Hall vereist. Dit is het zogenaamde "niet-kritisch geval".

Niet-kritisch geval
We hebben dus:

$$|H(W)| \geq |W| + 1$$

voor elke echte deelverzameling W van V_1. Als we dan een willekeurige top $u \in V_1$ neem, hebben we minstens 2 buren in V_2.
Noem één van die buren v. We wijzen v alvast toe aan u en bekijken de bipartiete graf G' die ontstaat wanneer we $u{\sim}v$ uit G weglaten. Deze graf heeft k toppen in V_1 en elke deelverzameling W van V_1 heeft tenminste $|W| + 1$ buren in V_2 en bijgevolg tenminste $|W|$ buren in $V_2 \backslash \{v\}$.
Voor de graf G' geldt dus de voorwaarde van Hall zodat we uit de inductiehypothese een toewijzing krijgen van $V_1 \backslash \{u\}$ in $V_2 \backslash \{v\}$. Samen met de boog $u{\sim}v$ vormt deze een toewijzing van V_1 in V_2.

kritisch geval
Nu is er minstens 1 echte deelverzameling W' van V_1 met $|H(W')| = |W'|$. Zulke W' heet een **kritische verzameling**. Voor de deelgraf geïnduceerd op $W' \cup H(W')$ geldt uiteraard de voorwaarde van Hall. Omdat $|W'| \leq k$ kunnen we de inductiehypothese toepassen om een toewijzing van W' in $H(W')$ te vinden.

[38] Al de topjes van V_1 gaan kunnen op een boogje leggen gaande naar V_2
[39] Als we voor elke deelverzameling van V_1 dat mijn aantal elementen in die buren verzameling minstens zoveel elementen heeft als in de verzameling.
[40] $\subseteq \Rightarrow$ Strikt minder dan V_1 elementen

Voor de deelgraf geïnduceerd op $V_1 \backslash W' \cup V_2 \backslash H(W')$ kunnen we de voorwaarde van Hall ook aantonen. Zij W een deelverzameling van $V_1 \backslash W'$. Dan heeft $W' \cup W$ ten minste $|W' \cup W|$ buren in V_2 (door de voorwaarde van Hall). Maar vermits precies $|W'|$ van die buren in $H(W')$ liggen, moeten minstens $|W|$ van hen in $V_2 \backslash H(W')$ liggen. Omdat $|V_1 \backslash W'| \leq k$ is ook hier de inductiehypothese van toepassing zodat we een toewijzing van $V_1 \backslash W'$ in $V_2 \backslash H(W')$ krijgen die samen met de toewijzing van W' in $H(W')$ uiteindelijk een toewijzing van V_1 in V_2 oplevert.

We weten nu wanneer er een (maximum)toewijzing bestaat. Om zulke (maximum)toewijzing te vinden, is deze stelling echter nog niet voldoende. Er bestaan algoritmes om een maximumtoewijzing te vinden. We geven als voorbeeld de Hongaarse methode die ook bruikbaar is om een maximumkoppeling te vinden.

Algoritme voor een maximum toewijzing (Hongaarse methode).
We vertrekken van een (eventueel lege) toewijzing K en proberen die uit te breiden door een vergrotend K-wisselpad te maken met volgend algoritme.

Neem een top w van V_1 die K-onverzadigd is. Bouw een gewortelde **wisselboom** T met wortel w (dit is een boom zodanig dat elk pad in T met beginpunt w een wisselpad is) door steeds bogen van G toe te voegen aan T . Stop met bogen toe te voegen als 1 van volgende voorwaarden voldaan is:

- De boom T heeft een onverzadigd blad $u \in V_2$
- Alle bladeren van T zijn verzadigde toppen van V_1 en T kan niet verder uitgebreid worden.

Indien aan 2 is voldaan, herbegin je met een andere onverzadigde top. In het andere geval hebben we een vergrotend K-wisselpad P en wordt de toewijzing K vervangen door $K \backslash P \cup P \backslash K$.
We kunnen nu het algoritme opnieuw uitvoeren met deze nieuwe toewijzing. Uiteindelijk kunnen we geen wisselpaden meer vinden. We eindigen met een toewijzing K_H waarvan we kunnen bewijzen dat dit een maximumtoewijzing is. Dit zal je in de Oefening 36 doen.

We kunnen ons nu ook afvragen of we de grootte van een maximumtoewijzing kunnen bepalen zonder zo een toewijzing daadwerkelijk te construeren. De stelling van König zegt dat dit inderdaad mogelijk is. We geven geen bewijs.

Stelling 50 (König). Zij $G = (V_1 \cup V_2, E)$ een bipartiete ongerichte graf en stel

$$t := \max_{W \subset V_1} (|W| - |H(W)|)$$

Dan is het aantal bogen van een maximumtoewijzing van V_1 in V_2 gelijk aan $|V_1|$ indien $t \leq 0$ en aan $|V_1| - t$ anders.

Definitie 42. Een **(toppen)overdekking** (Engels: “vertex cover”) van een ongerichte graf G is een deelverzameling U van toppen van G waarbij elke boog van G minstens 1 top van U bevat.

Een **minimale overdekking** is een overdekking die geen echte deelverzameling heeft welke ook een overdekking is. Een **minimumoverdekking** is een overdekking waarnaast geen overdekking bestaat met minder toppen.

Merk op dat voor een bipartiete graf $G = (V_1 \cup V_2, E)$ zowel V_1 als V_2 overdekkingen zijn, welke minimaal zijn als G geen geïsoleerde top heeft. In het algemeen zullen de minimale overdekkingen dus deelverzamelingen hiervan zijn.

Onderstel nu dat we in een (niet noodzakelijk bipartiete) ongerichte graf G een koppeling K en een overdekking U hebben. Dan moet elke boog van K ten minste 1 van zijn uiteinden in U hebben.

Omdat de bogen van K geen toppen gemeenschappelijk hebben, moeten er tenminste zoveel toppen in U liggen als er bogen zijn in K. Dus geldt $|K| \leq |U|$ voor elke koppeling K en elke overdekking U.

We krijgen dus:

$$\max|K| \leq \min\ |U|$$

waarbij K de verzameling van alle koppelingen van G doorloopt en U de verzameling van alle overdekkingen. De vraag is of de gelijkheid geldt. Het antwoord is duidelijk negatief.

In een vijfhoek C_5 bijvoorbeeld zal een maximumkoppeling bestaan uit 2 bogen, terwijl een minimumoverdekking moet bestaan uit 3 toppen. Voor een bipartiete graf geldt de gelijkheid daarentegen wel.

Stelling 51 (König-Egervary, 1931). Voor een bipartiete ongerichte graf $G = (V_1 \cup V_2, E)$ geldt:

$$max|K| = \min|U|$$

waarbij K de verzameling van alle koppelingen van G doorloopt en U de verzameling van alle overdekkingen van G.

Bewijs.
We weten al dat $max|K| \leq \min|U|$ Het is dus voldoende om een koppeling K en een overdekking U te vinden met $|K| = |U|$. Voor K nemen we uiteraard een maximumkoppeling K_{max}.
Volgens de stelling van König hebben we ofwel:

$$|K_{max}| = |V_1|$$

Ofwel

$$|K_{max}| = |V_1| - \max_{W \subset V_1}(|W| - |H(W)|)$$

In het eerste geval kiezen we $U := V_1$. Dit is een overdekking. In het andere geval nemen we W^* gelijk aan een deelverzameling van V_1 waarvoor het "maximum burentekort" van bovenstaande gelijkheid bereikt wordt. Dan volgt

$$|K_{max}| = |V_1| - (|W^*| - |H(W^*)|) = |(V_1 \backslash W^*) \cup H(W^*)|$$

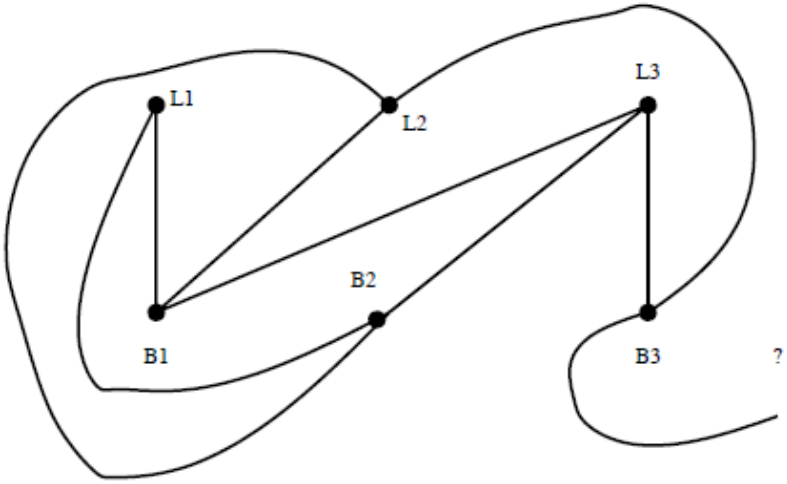
De verzameling:

$$U \coloneqq (V_1 \backslash W^*) \cup H(W^*)$$

heeft het gewenste aantal elementen en is een overdekking. Inderdaad: de verzameling $V_1 \backslash W^*$ overdekt alle bogen met een uiteinde in $V_1 \backslash W^*$ en $H(W^*)$ overdekt alle bogen met een uiteinde in W^*.

4.10 Planaire graffen

Drie professoren willen niet praten met elkaar. Ze moeten regelmatig les geven in drie leslokalen L_1, L_2 en L_3. Is het mogelijk om op de campus wegen te bedenken tussen elk van de drie leslokalen en de drie bureaus B_1, B_2 en B_3 van de proffen zodanig dat die wegen nooit kruisen? Op die manier zouden de proffen elkaar nooit tegenkomen. We proberen op een tekening:

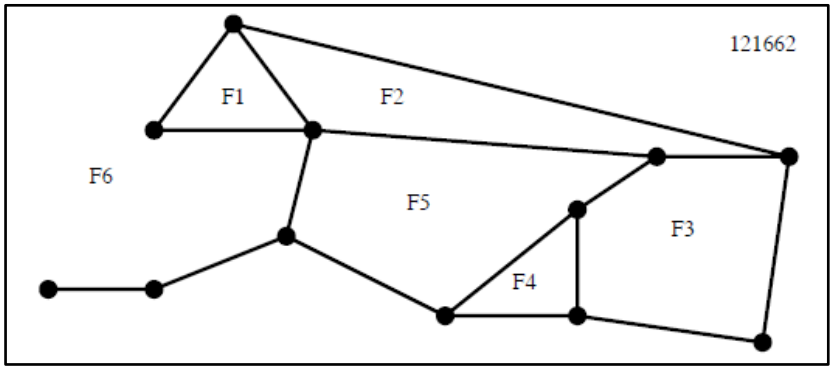


We zien geen mogelijkheid om B_3 met L_1 te verbinden. Misschien moeten we harder proberen? Misschien hangt het af van de ligging van de bureaus en de lokalen?

Wiskundig stelt men zich de vraag of de compleet bipartiete graf $K_{3,3}$ in het vlak (of op een blad papier) kan getekend worden zodanig dat twee bogen elkaar nooit snijden.

Definitie 43. Een multigraf heet **planair** indien hij in een vlak kan getekend worden zonder dat twee bogen elkaar snijden.

Als we een planaire multigraf in het vlak tekenen zodanig dat geen twee bogen snijden, wordt het vlak verdeeld in **gebieden** (Engels: “faces”).
Er bestaat een verband tussen het aantal toppen, bogen en gebieden van een planaire multigraf. We noteren deze aantallen respectievelijk met v, e en f.



$$12 - 16 + 6 = 2$$

Stelling 52 (weeral van Euler). Voor een samenhangende planaire ongerichte multigraf G geldt steeds:

$$v - e + f = 2$$

Bewijs.
We geven een bewijs per inductie op e, het aantal bogen in G.

Als we maar 1 boog hebben en hij is samenhangend hebben we de volgende graffen:

In het eerst geval hebben we $v = 2$ en $f = 1$ en $e = 1$ dus:

$$v - e + f = 2$$
$$2 - 1 + 1 = 2$$

In het tweede geval hebben we $v = 1$ en $f = 2$ en $e = 1$ dus:

$$v - e + f = 2$$
$$1 - 1 + 2 = 2$$

In beide gevallen is de formule van Euler duidelijk voldaan.

Inductiehypothese:
We veronderstellen dat onze formule geldt voor alle planaire graffen met $e - 1$ bogen, nu moeten we het gaan bewijzen voor e bogen.

Als we vertrekken van e bogen willen we het herleiden naar $e - 1$ bogen. Er zij twee gevallen:

1
Als we naar onze graf G kijken en we kunnen een boog b verwijderen zodanig dat de overschot G' nog steeds samenhangend is. Dan weten we dat de boog b een deel was van een cyclus in G. Maar de b die we hebben verwijderd zat dus in een cyclus dus die is eigenlijk de rand van twee gebieden namelijk de binnenkant van die cyclus en de buitenkant.

Als we kijken naar de graf $G' \coloneqq G - b$, is dat een graf met een boog en een gebied minder. Want door de b te verwijderen hebben we 2 gebieden samengevoegd.

De graf G' heeft dan $e - 1$ bogen, $f - 1$ gebieden en v toppen. De inductiehypothese geeft:

$$v - (e - 1) + (f - 1) = 2.$$
$$n - e + 1 + f - 1 = 2.$$
$$n - e + f = 2$$

2

We kunnen geen enkele boog b weglaten zodanig dat de graf G nog samenhangend blijft, dan is G een boom. In een boom hebben we geen cycli dus $f = 1$, en we weten van *Stelling 37.* Dat een boom met v toppen heeft $v - 1$ bogen heeft. Dus:

$$v - (v - 1) + 1 = 2$$

We komen nu terug naar het probleem van de drie proffen. Is $K_{3,3}$ planair? Indien wel, moet $v - e + f = 2$. We weten dat $v = 6$ en $e = 9$. Dus moet $f = 5$. Maar doordat $K_{3,3}$ compleet bipartiet is, moeten de gebieden cyclussen zijn van lengte 4. Om 5 zulke cycli te maken hebben we in principe 20 bogen nodig, maar in een planaire graf ligt elke boog op de grens van 1 of 2 gebieden. De zuinigste manier om planair 5 vierhoeken te maken is dus met 10 bogen. Maar $K_{3,3}$ heeft er maar 9 en kan dus niet planair zijn. Het professorenprobleem heeft bijgevolg geen oplossing.

Stelling 53. Zij G een samenhangende planaire ongerichte simpele graf met minstens 2 bogen. Dan geldt $3f \leq 2e$ en $e \leq 3v - 6$.

Bewijs.
De stelling is duidelijk waar wanneer er maar 1 gebied is. Onderstel $f > 1$. Vermits de graf simpel is, bestaat de rand van elk gebied uit minstens 3 bogen. Elke boog kan hoogstens twee keer optreden als rand van een gebied zodat:

$$2e \geq 3f$$

Samen met $v - e + f = 2$ krijgen we $2 \leq v - e + \frac{2}{3}e = v - \frac{e}{3}$. □

Gevolg 14. Elke samenhangende planaire ongerichte simpele graf G heeft een top van graad ≤ 5.

Bewijs.
We weten $e \leq 3v - 6$. Dus moet

$$\sum_{x \in V(G)} \deg(x) = 2e \leq 6v - 12.$$

Mocht elke x graad ≥ 6 hebben, zou:

$$\sum_{x \in V(G)} \deg(x) \geq 6v.$$

En dat is een tegenspraak □

Uit het feit dat noch $K_{3,3}$ noch K_5 planair zijn, volgt gemakkelijk dat een graf die een deelgraf isomorf met $K_{3,3}$ of met K_5 bevat nooit planair kan zijn.

Als een graf niet planair is, is het duidelijk dat als we een top van graad 2 weglaten en zijn 2 buren verbinden met een boog, de graf niet planair kan worden. Ook mogen we een boog $\{x, y\}$ gerust vervangen door een nieuwe top t en twee bogen $\{x, t\}$ en $\{t, y\}$, zonder de planariteit te veranderen.

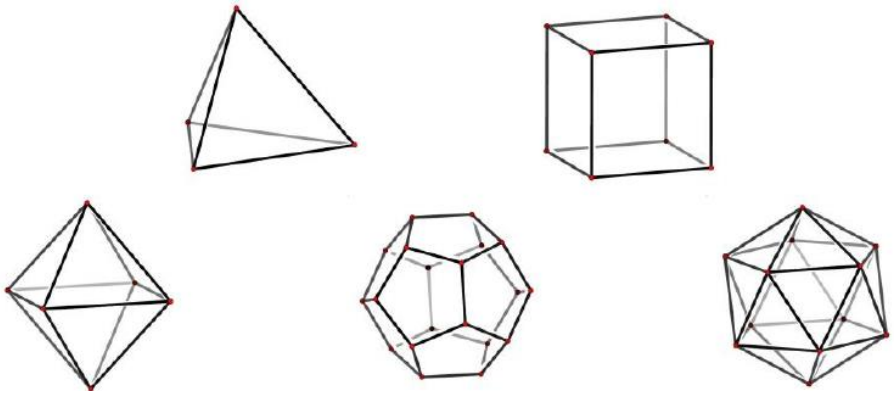
Definitie 44. Een graf H die ontstaat uit een graf G door (eventueel meermaals) toepassen van bovenstaande operaties heet **boogequivalen**t met G.

Volgende belangrijke stelling geven we zonder bewijs.

Stelling 54 (Kuratowski, 1930). Een multigraf is planair ⇔ hij geen deelgraf bevat die boogequivalent is met $K_{3,3}$ of met K_5.

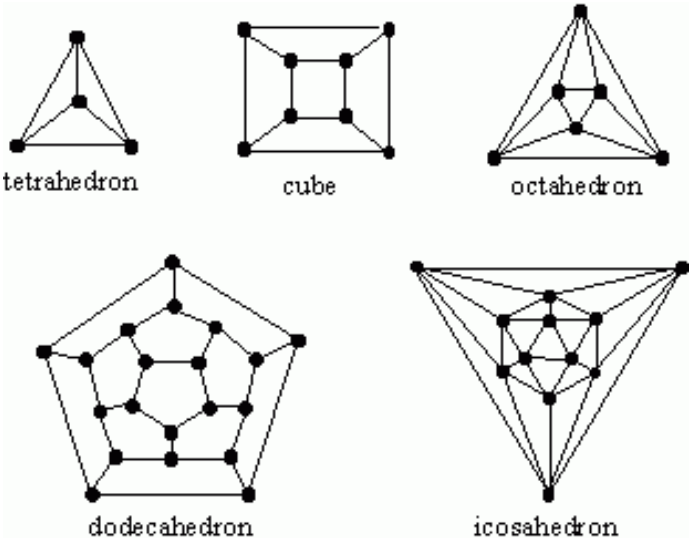
4.10.1 Platonische lichamen

We kennen allemaal de vijf regelmatige veelvlakken die soms ook platonische lichamen worden genoemd: de tetraëder, de kubus, de octaëder, de dodecaëder en de icosaëder. Waarom zijn er maar vijf zulke regelmatige veelvlakken?



Bij de platonische lichamen behoort elke ribbe tot juist twee zijvlakken en alle zijvlakken hebben evenveel ribben op hun rand. Bovendien liggen ook alle hoekpunten op eenzelfde aantal ribben.

Merk op dat de platonische lichamen aanleiding geven tot planaire graffen gevormd door de hoekpunten en ribben:



We bestuderen nu de planaire graffen waarin elke boog in de rand zit van twee gebieden, elke top graad n heeft en alle gebieden m bogen hebben in hun rand. Het is duidelijk dat we ook $n, m \geq 3$ moeten nemen.

Vermits elke boog op twee gebieden ligt, hebben we $2e = mf$. Vermits elke top graad n heeft en elke boog twee toppen verbindt, geldt ook $2e = nv$. De planariteit impliceert:

$$0 < 2 = v - e + f = \frac{2e}{n} - e + \frac{2e}{m} = e\left(\frac{2m - nm + 2n}{nm}\right)$$

Vermits zowel e als m en n strikt positief zijn, moet $2m - nm + 2n > 0$ of $nm - 2n - 2m < 0$.
Dit is equivalent met $nm - 2m - 2n + 4 < 4$ of $(n-2)(m-2) < 4$.
Doordat $m, n \geq 3$, zijn zowel $n-2$ als $m-2$ positief. Er zijn maar vijf koppels (m, n) die voldoen aan alle voorwaarden. Deze geven aanleiding tot de vijf gekende platonische lichamen.

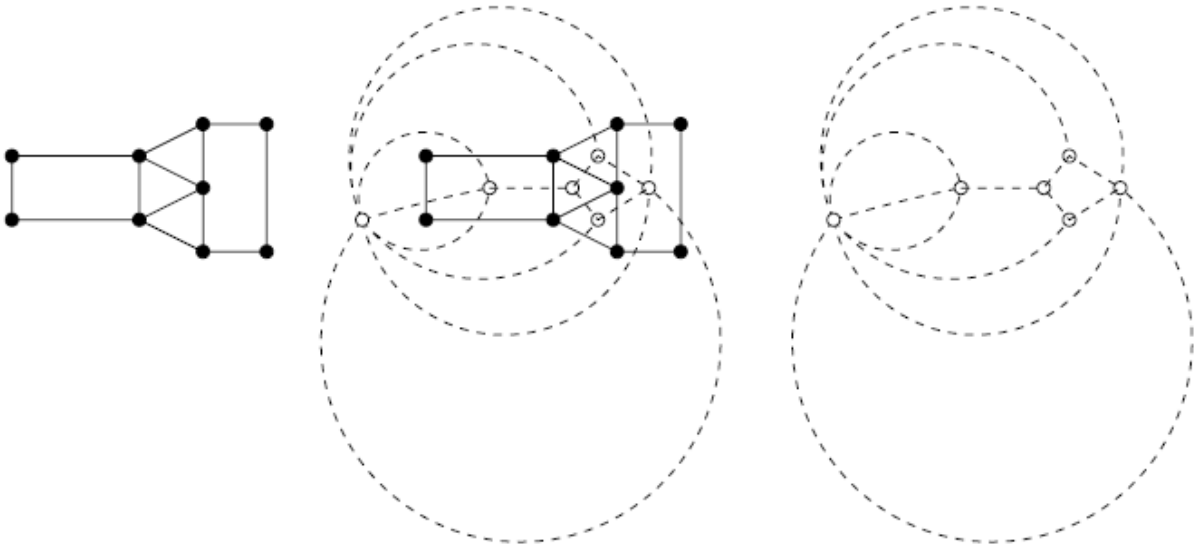
$m-2$	$n-2$	m	n	lichaam
1	1	3	3	tetraëder
2	1	4	3	kubus
1	2	3	4	octaëder
3	1	5	3	dodecaëder
1	3	3	5	icosaëder

4.10.2 Het kleuren van planaire graffen

In een atlas worden de landen meestal ingekleurd met verschillende kleuren zodat twee buurlanden nooit dezelfde kleur krijgen. Zo zie je duidelijk de grens tussen twee landen. Hoeveel kleuren heb je hiervoor minstens nodig? Luxemburg toont dat het antwoord minstens 4 is.

We moeten voor een planaire graf dus bepalen hoeveel kleuren er minstens nodig zijn om de gebieden zo te kleuren dat aangrenzende gebieden nooit dezelfde kleur krijgen. Om dit probleem te vertalen naar een kleuring van toppen in een graf, voeren we het zeer belangrijke begrip dualiteit in.

Definitie 45. Zij G een planaire ongerichte multigraf. De **duale graf** G^* heeft als toppen de gebieden van G en twee toppen zijn adjacent als en slechts als de overeenkomstige gebieden een boog delen. De figuur hieronder toont een voorbeeld van een graf en zijn duale (in streepjeslijn).



Opmerking. De duale van een planaire graf is opnieuw een planaire graf.

Het probleem wordt nu: wat is het minimaal aantal kleuren nodig om de toppen van een planaire graf te kleuren zodanig dat adjacente toppen nooit dezelfde kleur hebben?

Stelling 55. Elke samenhangende planaire ongerichte simpele graf G kan met 6 kleuren gekleurd worden.

Bewijs. We doen dit bij inductie op v, het aantal toppen van de planaire graf G.
Voor $v = 1$ is het duidelijk in orde.

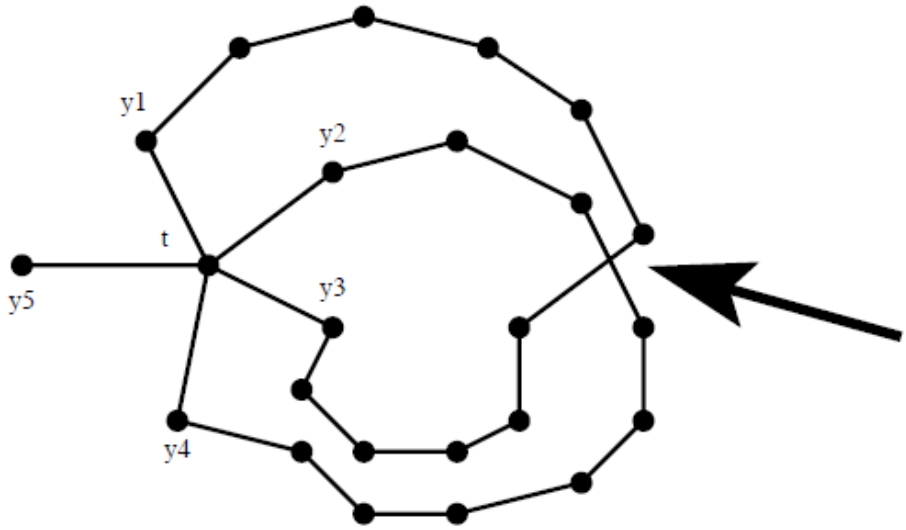
Onderstel nu dat de stelling geldt voor alle planaire graffen met $v - 1$ toppen. Uit Gevolg 14 weten we dat G een top t heeft met $deg(t) \leq 5$.
Als we t weglaten, krijgen we een graf G' met $v - 1$ toppen. Deze kan dus gekleurd worden met 6 kleuren. Vermits t hoogstens 5 buren heeft (die in G' elk een kleur krijgen), is er zeker een kleur over voor t. □

We kunnen dit resultaat nog een beetje verfijnen.

Stelling 56. Elke samenhangende planaire ongerichte simpele graf G kan met 5 kleuren gekleurd worden.

Bewijs. Ook per inductie op v, zoals in het vorige bewijs.

Dat bewijs kan trouwens alleen maar mis gaan voor 5 kleuren als t echt 5 buren heeft, elk van een andere kleur in de kleuring van G'. We bekijken dit geval van nabij.



Noteer de 5 buren van t met y_1, y_2, y_3, y_4 en y_5, genummerd in wijzerzin (zie tekening). Zij G' de graf die uit G ontstaat als je t weglaat, alsook de 5 bogen op t. Als G' kan gekleurd worden met 5 kleuren waarbij y_1 en y_3 dezelfde kleur hebben, is er een kleur over voor t. Anders moet elke kleuring van G_0 met 5 kleuren een pad van y_1 tot y_3 hebben dat alternerend de kleuren van y_1 en y_3 gebruikt.

Op dezelfde manier is er een pad van y_2 naar y_4 dat alleen de kleuren van y_2 en y_4 gebruikt (die verschillend zijn van die van y_1 en y_3). Dus kunnen de twee gevonden paden geen top gemeenschappelijk hebben. Maar door de ligging van y_2 tussen y_1 en y_3, moeten de twee paden kruisen. Dit spreekt de planariteit tegen. □

Hoofdstuk 5: Genererende functies

In dit hoofdstuk nemen we de methode van inclusie en exclusie (zie paragraaf 2.5) nog eens onder de loupe.

5.1 Voorbeelden en definitie

Eerste voorbeeld

Een moeder koopt 12 snoepjes en wil die verdelen onder haar drie kinderen: Piet, Andres en Jan. Wel zo dat Piet er minstens 4 krijgt, Andres en Jan minstens 2 en Jan hoogstens 5.

Noteren we c_P , c_A en c_J voor het aantal snoepjes dat Piet, Andres en Jan respectievelijk krijgen, hebben we $c_P + c_A + c_J = 12$ en $c_P \geq 4, c_A \geq 2$ en $5 \geq c_J \geq 2$.

We kunnen alle oplossingen opschrijven:

c_P	4	4	4	4	5	5	5	5	6	6	6	7	7	8
c_A	3	4	5	6	2	3	4	5	2	3	4	2	3	2
c_J	5	4	3	2	5	4	3	2	4	3	2	3	2	2

We hebben dus 12 op alle mogelijke manieren geschreven als som van drie natuurlijke getallen die voldoen aan de voorwaarden. Dit doen we eigenlijk ook als we de distributiviteit toepassen bij het uitwerken van volgend product van veeltermen:

$$(x^4 + x^5 + x^6 + x^7 + x^8)(x^2 + x^3 + x^4 + x^5 + x^6)(x^2 + x^3 + x^4 + x^5)$$

De eerste factor komt overeen met het feit dat de toegelaten waarden voor c_P enkel $4, 5, 6, 7$ en 8 zijn. De tweede factor ontstaat uit de opmerking dat een oplossing steeds een c_A zal hebben in $\{2,3,4,5,6\}$.
In het product (5.1) komt de coëfficiënt van x^{12} overeen met alle mogelijke manieren om x^{12} te bekomen door een term te nemen in elk van de drie factoren. Dus is de oplossing van het vraagstuk ook de coëfficiënt van x^{12} in het product (5.1) van veeltermen.

Tweede voorbeeld.
We hebben grote hoeveelheden knikkers van vier kleuren : rood, groen, wit en zwart.
Op hoeveel manieren kan je 24 knikkers kiezen zo dat er een even aantal witte is en minstens 6 zwarte.

We maken een veelterm die een factor heeft voor elke kleur. Op de rode of groene knikkers is er geen beperking : er kunnen geen, 1, 2, . . . , 17 of 18 (niet meer want minstens 6 knikkers zijn zwart) knikkers zijn van die kleur. Dit geeft voor beide kleuren een factor $(1 + x + x^2 + \cdots + x^{18})$.
De factor van de witte knikkers bevat enkel even machten : $(1 + x^2 + x^4 + \cdots + x^{18})$. Aangezien er minstens 6 zwarte knikkers zijn, krijgen we een factor $(x^6 + x^7 + \cdots + x^{24})$.

Het antwoord op de vraag is dus gelijk aan de coëfficiënt van x^{24} in het product:

$$(1 + x + x^2 + \cdots + x^{18})^2(1 + x^2 + x^4 + \cdots + x^{18})(x^6 + x^7 + \cdots + x^{24})$$

Definitie 46. Zij $a_0, a_1, a_2, \ldots$ een rij van reële getallen. De genererende functie voor die rij is per definitie

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{i=0}^{\infty} a_i x^i$$

Voorbeeld. De genererende functie van de rij $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}, 0,0, \ldots$ is

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

Voorbeeld. We weten zeer goed dat $(1-x)(1+x+x^2+\cdots+x^n) = 1-x^{n+1}$, waaruit volgt

$$\frac{1-x^{n+1}}{1-x} = 1+x+x^2+\cdots+x^n. \quad (1)$$

Bijgevolg is $\frac{1-x^{n+1}}{1-x}$ een genererende functie voor de rij $\underbrace{1,1,1,\ldots,1}_{n+1 \text{ keer}}, 0,0, \ldots$

Voorbeeld. Ook de rij $1,1,1, \ldots$ kunnen we genereren omdat
$(1-x)(1+x+x^2+\cdots) = 1$ (voor $|x| < 1$) zodat:

$$\frac{1}{1-x} = 1+x+x^2+\cdots \quad (2)$$

Als we beide leden afleiden krijgen we

$$\frac{1}{(1-x)^2} = 0+1+2x+3x^2+\cdots \quad (3)$$

Zodat $\frac{1}{(1-x)^2}$ een genererende functie is voor de rij $1,2,3, \ldots$ Als we nu beide leden van (5.3) vermenigvuldigen met x, krijgen we

$$\frac{x}{(1-x)^2} = x+2x^2+3x^3+\cdots \quad (4)$$

Zodat $\frac{x}{(1-x)^2}$ een genererende functie is voor de rij $0,1,2,3, \ldots$ Nog eens beide leden van (5.4) afleiden geeft:

$$\frac{1+x}{(1-x)^3} = 1+2^2x+3^2x^2+\cdots$$

Zodat deze functie de rij $1^2, 2^2, 3^2, \ldots$ genereert.
We zien nu ook gemakkelijk dat:

$$\frac{x(1+x)}{(1-x)^3} \quad (5)$$

De rij $0^2, 1^2, 2^2, \ldots$ genereert.

Voorbeeld. Willen we nu de rij $1,1,0,1,1,1, \ldots$ genereren, starten we met (5.2) en trekken we gewoon x^2 af. We hebben inderdaad

$$\frac{1}{1-x} - x^2 = 1+x+x^3+x^4+\cdots$$

Analoog genereert $\frac{1}{(1-x)} + 2x^3$ de rij $1,1,1,3,1,1, \ldots$

5.2 Veralgemeende binomiaal coëfficiënten

Wat is het volgende getal in de rij $0, 2, 6, 12, 20, 30, 42, ?$
Merk op dat:

$$a_0 = 0 + 0^2$$
$$a_1 = 1 + 1^2$$
$$a_2 = 2 + 2^2$$
$$a_3 = 3 + 3^2$$
$$\dots$$

De genererende functie van die rij kunnen we nu gemakkelijk opstellen door (5.4) en (5.5) te combineren:

$$\frac{x(1+x)}{(1-x)^3} + \frac{x}{(1-x)^2} = \frac{2x}{(1-x)^3}$$

Het antwoord is dus de coëfficiënt van x^7 in $\frac{2x}{(1-x)^3}$. Hoe bepalen we die coëfficiënt?

We breiden het begrip binomiaal coëfficiënt uit. We weten dat voor $n, r \in \mathbb{N}_0$ geldt:

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!} = \frac{n(n-1)(n-2)\dots(n-r+1)}{r!}$$

Definitie. We stellen nu voor alle niet-nulle natuurlijke getallen n en r:

$$\binom{-n}{r} := \frac{(-n)(-n-1)(-n-2)\dots(-n-r+1)}{r!}$$

Dan geldt:

$$\binom{-n}{r} = (-1)^r \frac{n(n+1)(n+2)\dots(n+r-1)}{r!}$$
$$= (-1)^r \frac{(n+r-1)!}{r!\,(n-r)!}$$
$$= (-1)^r \binom{n+r-1}{r}$$

We stellen ook $\forall n \in \mathbb{Z}$: $\binom{n}{0} := 1$.

Uit de analyse weet je dat de Maclaurin-reeks voor $(1 + x)^{-n}$ gelijk is aan:

$$1 + (-n)x + \frac{(-n)(-n-1)}{2!}x^2 + \frac{(-n)(-n-1)(-n-2)}{3!}x^3 + \cdots$$

Zodat:

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

Dit is een veralgemening van het binomium van Newton. Nog anders gezegd : $(1 + x)^{-n}$ is een genererende functie voor $\binom{-n}{0}, \binom{-n}{1}, \binom{-n}{2}, \dots$

We passen dit nieuw begrip toe:

Voorbeeld. Bepaal de coëfficiënt van x^5 in $(1-2x)^{-7}$
Pas het veralgemeend binomium van Newton toe :

$$\big(1+(-2x)\big)^{-7} = \sum_{r=0}^{\infty} \binom{-7}{r} (-2x)^r$$

Dus is de coëfficiënt die we zoeken gelijk aan:

$$\binom{-7}{5}(-2)^5 = (-32)(-1)^5\binom{11}{5} = 14784$$

Voorbeeld. Op hoeveel manieren kunnen we 24 snoepjes verdelen onder 4 kinderen zodat iedereen minstens 3 snoepjes krijgt en hoogstens 8?
De genererende functie is:

$$f(x) = (x^3+x^4+x^5+x^6+x^7+x^8)^4$$

En we zoeken de coëfficiënt van x^{24}. We hebben:

$$f(x) = x^{12}(1+x+x^2+x^3+x^4+x^5)^4 = x^{12}\left(\frac{1-x^6}{1-x}\right)^4$$

zodat we eigenlijk de coëfficiënt van x^{12} in $\left(\frac{1-x^6}{1-x}\right)^4$ nodig hebben. Dit is niet moeilijk :

$$\left(\frac{1-x^6}{1-x}\right)^4 = (1-x^6)^4(1-x)^{-4}$$
$$= \left[1-\binom{4}{1}x^6+\binom{4}{2}x^{12}-\binom{4}{3}x^{18}+\binom{4}{4}x^{24}\right]\left[\binom{-4}{0}+\binom{-4}{1}(-x)+\binom{-4}{2}(-x)^2+\cdots\right]$$

zodat de coëfficiënt van x^{12} gelijk is aan:

$$\binom{15}{12}-\binom{4}{1}\binom{9}{6}+\binom{4}{2}\times 1 = 125$$

Voorbeeld. Op hoeveel manieren kan je een deelverzameling van $[15]$ met 4 elementen kiezen zodanig dat er geen twee opeenvolgende getallen inzitten?

Zulk een verzameling is bijvoorbeeld $\{1,3,7,10\}$ We merken op dat de verschillen

$$1-1 = 0 =: c_1$$
$$3-1 = 2 =: c_2$$
$$7-3 = 4 =: c_3$$
$$10-7 = 3 =: c_4$$
$$15-10 = 5 =: c_5$$

als som 14 hebben. Dit blijkt algemeen zo te zijn zodat de vraag kan geformuleerd worden als vind alle getallen $c_1, c_2, c_3, c_4, c_5 \in [15]$ met $c_1+c_2+c_3+c_4+c_5 = 14$ en
$0 \leq c_1, c_5$ en $2 \leq c_2, c_3, c_4$." Het volstaat dus om de coëfficiënt van x^{14} te bepalen in

$$f(x) = (1+x^2+x^3+\cdots)^2(x^2+x^3+x^4+\cdots)^3 = x^6(1-x)^{-5}$$

De coëfficiënt van x^8 in $(1-x)^{-5}$ is $\binom{-5}{8}(-1)^8$. Het antwoord is dus 495.

5.3 Partities van natuurlijke getallen

Een bekende waspoederfabrikant wil reclame maken via de televisie. Hij kan bij een bepaalde zender reclamespots kopen van 15, 30 en 60 seconden. Op hoeveel manieren kan hij zendtijd kopen als hij in totaal n minuten reclame wil maken?

Laat ons 15 seconden als tijdseenheid beschouwen. Dan is het antwoord het aantal mogelijke combinaties van natuurlijke getallen a, b en c zodanig dat $a + 2b + 4c = 4n$. De genererende functie die hiermee overeen komt is

$$f(x) \coloneqq (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^4 + x^8 + \cdots)$$
$$= \frac{1}{1-x} \times \frac{1}{1-x^2} \times \frac{1}{1-x^4}$$

Het antwoord vinden we terug als de coëfficiënt van x^{4n} in $f(x)$. We merken ook op dat dit antwoord het aantal manieren is om het natuurlijk getal 4n te schrijven als som van enen, tweeën en vieren.

Definitie 48. Een partitie van een niet-nul natuurlijk getal n is een schrijfwijze van n als som van niet-nulle natuurlijke getallen

Voorbeeld. $11 = 4 + 3 + 3 + 1$

Opmerking. Een partitie (zie Definitie 14 op blz. 57) van een eindige verzameling V geeft aanleiding tot een partitie van het natuurlijk getal $|V|$.

Voorbeeld. Op hoeveel manieren kunnen we 6 schrijven als som van niet-nulle natuurlijke getallen?

Dit komt neer op het tellen van de partities van het getal 6. We schrijven ze eens alle neer:

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

Er zijn in totaal dus 11 manieren.

Notatie. We noteren het aantal partities van een natuurlijk getal n met $p(n)$.

Kunnen we voor $p(n)$ een genererende functie vinden? Het antwoord is JA!

We kunnen bijvoorbeeld $p(10)$ vinden als de coëfficiënt van x^{10} in het product

$$\underbrace{(1+x+x^2+\cdots)}_{\text{voor de enen}}\underbrace{(1+x^2+x^4+\cdots)}_{\text{voor de tweeën}}\ldots\underbrace{(1+x^{10}+x^{20}+\cdots)}_{\text{voor de tienen}}$$

$$\frac{1}{1-x}\times\frac{1}{1-x^2}\times\ldots\times\frac{1}{1-x^{10}}$$
$$=\prod_{i=1}^{10}(1-x^i)^{-1}$$

Hoeveel partities van 6 hebben alle termen verschillend?
Uit het voorbeeld hoger halen we dat dit aantal 4 is. We schrijven $p_{\neq}(6)=4$.
In het algemeen hebben we een genererende functie

$$P_{\neq}(x)=(1+x)(1+x^2)\ldots=\prod_{i=1}^{\infty}(1+x^i)$$

Hoeveel partities van 6 gebruiken enkel oneven termen?
We zien weer uit ons voorbeeld dat dit aantal 4 is. We schrijven $p_0(6)=4$
Dit is juist evenveel als $p_{\neq}(6)$. Is dit toeval?

Stelling 57. Voor elk niet-nul natuurlijk getal n geldt $p_{\neq}(n)=p_o(n)$.

De genererende functie voor $p_o(n)$ is

$$P_0(x)=(1+x+x^2+\cdots)(1+x^3+x^6+\cdots)\ldots$$
$$=\frac{1}{1-x}\times\frac{2}{1-x^3}\times\ldots$$

Merk op dat

$$1+x=\frac{1-x^2}{1-x},1+x^2=\frac{1-x^4}{1-x^2},\ldots$$

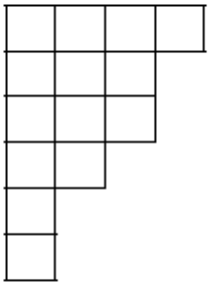
Zodat

$$P_{\neq}(x)=(1+x)(1+x^2)(1+x^3)\ldots$$
$$=\frac{\cancel{1-x^2}}{1-x}\times\frac{\cancel{1-x^4}}{\cancel{1-x^2}}\times\frac{1-x^6}{1-x^3}\times\frac{1-x^8}{\cancel{1-x^4}}\times\ldots$$
$$=P_0(x)$$

Vermits de genererende functies gelijk zijn, zijn ook de gegenereerde rijen gelijk. □

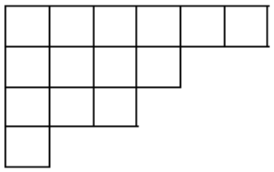
Een **Young tableau** is een grafische voorstelling van een partitie. Je schrijft vierkantjes op rijen om de verschillende termen van de partitie in dalende grootte op te geven:

$$14=4+3+3+2+1+1$$



Als je dit transponeert, krijg je:

$$14 = 6 + 4 + 3 + 1$$



Deze methode bewijst dat het aantal partities van n met m termen gelijk is aan het aantal partities van n waarbij de grootste term m is.

5.4 Beroemde genererende functies

We beëindigen dit hoofdstuk met een lijst van nuttige genererende functies.

Voor elke $n, m \in \mathbb{N}$ en elke $a \in \mathbb{R}$ geldt

- $(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = \sum_{i=0}^{n} \binom{n}{i}x^i$;
- $\frac{1-x^{n+1}}{1-x} = 1 + x + x^2 + \cdots + x^n = \sum_{i=0}^{n} x^i$;
- $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = \sum_{i=0}^{\infty} x^i$;
- $$\begin{aligned} \frac{1}{(1+x)^n} &= \binom{-n}{0} + \binom{-n}{1}x + \binom{-n}{2}x^2 + \cdots \\ &= \sum_{i=0}^{\infty} \binom{-n}{i}x^i \\ &= 1 + (-1)\binom{n+1-1}{1}x + (-1)^2\binom{n+2-1}{2}x^2 + \cdots \\ &= \sum_{i=0}^{\infty}(-1)^i\binom{n+i-1}{i}x^i \end{aligned}$$
- $$\begin{aligned} \frac{1}{(1-x)^n} &= \binom{-n}{0} + \binom{-n}{1}(-x) + \binom{-n}{2}(-x)^2 + \cdots \\ &= \sum_{i=0}^{\infty} \binom{-n}{i}(-x)^i \\ &= 1 + (-1)\binom{n+1-1}{1}(-x) + (-1)^2\binom{n+2-1}{2}(-x)^2 + \cdots \\ &= \sum_{i=0}^{\infty}\binom{n+i-1}{i}x^i \end{aligned}$$

Hoofdstuk 6: Recurrentievergelijkingen

In dit hoofdstuk gaan we verder met de studie van rijen. In het voorgaande hoofdstuk hebben we met rijen formele machtreeksen geassocieerd die zeer handig bleken bij het oplossen van telproblemen. Deze genererende functies werden voor het eerst ingevoerd door Abraham De Moivre in 1718 toen hij een exacte formule in functie van $n \in \mathbb{N}$ (zoals $a_n = 3n + 2$ of $b_n = (n\ +\ 1)(n\ +\ 2)(n\ +\ 3)$) wou voor de $n$de (of algemene) term van een rij die gegeven wordt door een zogenaamde **recurrentie relatie.**

Hierbij wordt rij gegeven door enkele begintermen en dan een **recursieve definitie** die a_n uitdrukt als functie van de voorgaande termen $a_0, a_1, a_2, \dots, a_{n-1}$

Voorbeeld.

$$a_0 = 1, a_1 = 1, a_n = a_{n-2} + a_{n-1} \text{ voor de rij } 1,1,2,3,5,8,13, \dots$$

We zullen nu onderzoeken wanneer zulke recursieve definitie kan `vertaald' worden in een formule voor de algemene term a_n die enkel afhangt van n.

6.1 Homogene eerste orde lineaire recurrentievergelijkingen

Deze zijn van de vorm

$$a_n = ra_{n-1}, \qquad (6.1)$$

Eerste orde betekent dat a_n enkel afhangt van a_{n-1} en niet van de voorgaande termen in de rij.
Lineair wil zeggen dat enkel de eerste macht van a_{n-1} voorkomt, niet a_{n-1}^5 of zo.
Homogeen betekent dat a_n naast a_{n-1} niet afhangt van iets anders. Dus niet $a_n = ra_{n-1} + \sin(n)$

Ook hangt r niet af van n. We zeggen dat het hier gaat om een recurrentievergelijking met **constante coëfficiënten.**

Die eerste orde homogene lineaire recurrentierelaties geven eigenlijk meetkundige rijen, die we reeds kennen vanuit het secundair onderwijs.

Voorbeeld. Los de vergelijking $a_{n+1} = 3_{a_n}$ op met als **randvoorwaarde** $a_0 = 5$. W
e rekenen enkele elementen van de rij uit:

$$\begin{aligned} a_0 &= 5 \\ a_1 &= 3 \times 5 = 15 \\ a_2 &= 3 \times 15 = 3^2 \times 5 \\ a_3 &= 3 \times a_2 = 3^2 \times 5 \end{aligned}$$

We zien dat:

$$a_n = 3^n \times 5$$

Stelling 58.
Zij $r \in \mathbb{C}$ en $a_0 \in \mathbb{C}$. De oplossing van de recurrentievergelijking $a_{n+1} = r_{a_n}$ is steeds van de vorm:

$$a_n = r^n a_0$$

Voorbeeld.
Los de vergelijking $a_n = 7a_{n-1}$ op als je weet dat $a_2 = 98$. We weten dat $a_n = 7^n a_0$
zodat $a_2 = 7^2 a_0$. Hieruit volgt $a_0 = 2$ en dus $a_n = 7^n \times 2$.

Voorbeeld.
De vergelijking $a_{n+1}^2 = 5a_n^2$ lijkt op het eerste gezicht niet lineair te zijn. Maar als je de substitutie $b_n := a_n^2$ uitvoert, krijg je dat b_n voldoet aan $b_{n+1} = 5b_n$. Als we de beginvoorwaarde $a_0 = 2$ meegeven, vinden we dat $b_n = 5^n b_0$ met $b_0 = 4$. Dus geldt $b_n = 5^n \times 4$ zodat de uiteindelijke oplossing:

$$a_n = \left(\sqrt{5}\right)^n \times 2$$

Voorbeeld. We komen terug op het raadsel van vorig hoofdstuk: vul de rij $0, 2, 6, 12, 20, 30, 42, \ldots$ aan. Neem de verschillen:

$$\begin{aligned} a_1 - a_0 &= 2 \\ a_2 - a_1 &= 4 \\ a_3 - a_2 &= 6 \\ a_4 - a_3 &= 8 \end{aligned}$$

We zien dus dat $a_n - a_{n-1} = 2n$. Dit is een niet-homogene lineaire eerste orde recurrentievergelijking die we later zullen leren oplossen in het algemeen. Toch kunnen we hier reeds een oplossing bedenken:

$$\begin{aligned} &(a_n - a_{n-1}) + (a_{n-1} - a_{n-2}) + \cdots + (a_2 - a_1) + (a_1 - a_0) \\ &= 2n + n(n-1) + \cdots + 2 \times 2 + 2 \times 1 \end{aligned}$$

Zodat

$$a_n - a_0 = 2(1 + 2 + 3 + \cdots + n)$$

Waaruit we vinden dat:

$$a_n - 0 = 2 \times \frac{n(n+1)}{2}$$

Of

$$a_n = n^2 + n$$

Voorbeeld. Ook met niet-constante coëfficiënten kan gezond verstand tot een oplossing leiden.

$$a_n = n a_{n-1} \text{ met } a_0 = 1$$

geeft onmiddellijk $a_n = n!$

6.2 Homogene tweede orde lineaire recurrentievergelijkingen

Definitie 49. Zij $k \in \mathbb{N}_0$ en $0 \neq c_0, c_1, \ldots, c_k \neq 0$ reële getallen en $f: \mathbb{N} \to \mathbb{R}$ een functie.
Een lineaire recurrentievergelijking van orde k **met constante coëfficiënten** is een uitdrukking

$$c_0 a_n + c_1 a_n + \cdots + c_k a_{n-k} = f(n)$$

Om een eenduidige oplossing te hebben voor a_n, zijn **beginvoorwaarden** $a_0, a_1, .., a_{k-1}$ nodig.
Als $\forall n \in \mathbb{N}$ geldt dat $f(n) = 0$, heet de vergelijking **homogeen**.

Wij concentreren ons op homogene van orde 2:

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} = 0, \qquad (6.2)$$

Geïnspireerd door het geval van orde 1 proberen we een oplossing te vinden van de vorm $a_n = cr^n$ voor constanten $c \neq 0$ en $r \neq 0$. We substitueren dit in (6.2) en bekomen

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} = 0, \qquad (6.3)$$

We delen dit alles door $cr^{n-2} \neq 0$ en krijgen

$$c_0 r^2 + c_1 r + c_2 = 0, \qquad (6.4)$$

Dit is een kwadratische vergelijking die we **de karakteristieke vergelijking** van de gegeven recurrentievergelijking noemen. De algemene methode voor het oplossen van kwadratische vergelijkingen leert ons dat er drie soorten oplossingen mogelijk zijn, naargelang de discriminant, $c_1^2 - 4c_0c_2$, positief, nul of negatief is. Er zijn dan respectievelijk twee reële oplossingen, één reële wortel met multipliciteit twee of twee complex toegevoegde oplossingen. We bekijken voorbeelden in elk van deze gevallen om de oplossingsmethode te schetsen

6.2.1 Twee reële wortels

Voorbeeld. Los volgende recurrentievergelijking op als je weet dat $a_0 = 1$ en $a_1 = 2$

$$a_n + a_{n-1} - 6a_{n-2} = 0$$

De karakteristieke vergelijking is:

$$r^2 + r - 6 = 0 \Leftrightarrow (r-2)(r+3) = 0$$

De wortels zijn dus 2 en -3. Bijgevolg zijn $a_n = 2^n$ en $a_n = (-3)^n$ oplossingen van de recurrentievergelijking, maar ook alle combinaties:

$$a_n = c_1 2^n + c_2 (-3)^n$$

van deze twee zijn oplossingen. De beginvoorwaarden laten ons toe de constanten c_1 en c_2 te expliciteren. We krijgen een stelsel

$$\begin{cases} 1 = a_0 = c_1 \times 1 + c_2 \times 1 \\ 2 = a_1 = c_1 \times 2 + c_2 \times (-3) \end{cases}$$

We lossen dit stelsel op:

$$\begin{cases} c_2 = 1 - c_1 \\ 2 = 2c_1 - 3c_2 \end{cases} \Leftrightarrow \begin{cases} c_2 = 1 - c_1 \\ 5c_1 = 5 \end{cases} \Leftrightarrow \begin{cases} c_2 = 0 \\ c_1 = 0 \end{cases}$$

Bijgevolg is een oplossing van de recurrentievergelijking, met beginvoorwaarden,

$$a_n = 2^n$$

Voorbeeld. We stellen nu een formule op voor de beroemde rij van Fibonacci: $0, 1, 1, 2, 3, 5, 8, \ldots$ die voldoet aan

$$F_{n+2} = F_{n+1} + F_n \text{ met } f_0 = 0 \text{ en } f_1 = 1.$$

De karakteristieke vergelijking is

$$r^2 - r - 1 = 0$$

De discriminant is 5 zodat we als oplossingen

$$r_+ = \frac{1+\sqrt{5}}{2}$$
$$r_- = \frac{1-\sqrt{5}}{2}$$

vinden. Een algemene oplossing is dus

$$a_n = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$$

De beginvoorwaarden geven

$$\begin{cases} 0 = F_0 = c_1 + c_2 \\ 1 = F_1 = c_1\left(\frac{1+\sqrt{5}}{2}\right) + c_2\left(\frac{1-\sqrt{5}}{2}\right) \end{cases} \Leftrightarrow \begin{cases} c_2 = -c_1 \\ 1 = c_1\sqrt{5} \end{cases} \Leftrightarrow \begin{cases} c_1 = \frac{1}{\sqrt{5}} \\ c_2 = -\frac{1}{\sqrt{5}} \end{cases}$$

Zodat

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

Opmerking. Dit is de zogenaamde “Formule van Binet”, dezelfde Binet als in de stelling van Cauchy-Binet (zie Appendix A).

Opmerking. Het is verbazend dat Formule (6.5) voor elke waarde van n een geheel getal geeft.
Dat ligt aan de zeer speciale eigenschappen van het getal $(1+\sqrt{5}) = 2$. Dit getal komt nog voor op andere plaatsen in de Wiskunde en in de natuur. Het is de zogenaamde Gulden snede' (Engels: “Golden ratio”).

Voorbeeld.
Voor $N \in \mathbb{N}$ stellen we a_n gelijk aan het aantal deelverzamelingen van $[n]$ die geen opeenvolgende getallen bevatten. De toegelaten deelverzamelingen van $[3]$ zijn bijvoorbeeld $\emptyset, \{1\}, \{2\}, \{3\}\ en\ \{1,3\}$. Je kan zelf nagaan dat $a_0 = 1, a_1 = 2, a_2 = 3, a_3 = 5$ en $a_4 = 8$. We bepalen een recurrentievergelijking voor de rij $(a_n)_n$.

Een toegelaten deelverzameling A van $[n]$ valt in één van volgende gevallen:

1. $n \in A$: dan moet $n-1 \notin A$ en is $A\backslash\{n\}$ en toegelaten deelverzameling voor $[n-2]$. Het aantal deelverzamelingen A in deze situatie is dus a_{n-2}
2. $n \notin A$: dan is A een toegelaten deelverzameling van $[n-1]$. Zo zijn er juist a_{n-1}.

We krijgen dus de recurrentievergelijking

$$a_n = a_{n-1} + a_{n-2}, \qquad met\ a_0 = 1\ en\ a_2 = 2$$

Dit lijkt op de Fibonacci-rij F_n uit vorig voorbeeld. We hebben $\forall n \in \mathbb{N}: a_n = F_{n+2}$ zodat:

$$a_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+2}\right]$$

We tonen even dat de methode met de karakteristieke vergelijking ook werkt voor recurrentievergelijkingen van hogere orde.

Voorbeeld. Los op :

$$2a_{n+3} = a_{n+2} + 2a_{n+1} - a_n, \qquad met\ a_0 = 0, a_1 = 1\ en\ a_2 = 2$$

De karakteristieke vergelijking is

$$2r^3 - r^2 - 2r + 1 = 0$$

Gelukkig kunnen we deze veelterm op zicht ontbinden tot $(2r-1)(r-1)(r+1)$. De wortels zijn nu duidelijk $\frac{1}{2}, 1\ en\ -1$. Bijgevolg is de oplossing van de vorm

$$a_n = c_1(1)^n + c_2(-1)^n + c_3\left(\frac{1}{2}\right)^n$$

Met de beginvoorwaarden vinden we:

$$a_n = \frac{5}{2} + \frac{1}{6}(-1)^n - \frac{8}{3}\left(\frac{1}{2}\right)^n$$

6.2.2 Twee complex toegevoegde wortels

Voor een opfrissing over complexe getallen verwijzen we naar Appendix B. Aan de hand van de goniometrische vorm van een complex getal kunnen we gemakkelijk machten berekenen, want de stelling van De Moivre zegt

$$\Big(r\big(\cos(\theta) + i \times sin(\theta)\big)\Big)^n = r^n(\cos(n\theta) + i \times \sin(n\theta))$$

Voorbeeld. Bepaal $\left(1+\sqrt{3}i\right)^{10}$.

We bepalen eerst de goniometrische vorm van $1+\sqrt{3}i$. Dat is $2\left(\cos\left(\frac{\pi}{3}\right) + i\sin(3)\right)$.

Hieruit volgt

$$\begin{aligned}
&\left(1+\sqrt{3}i\right)^{10} = 2^{10}\left(\cos\left(\frac{10}{3}\pi\right) + i\sin\left(\frac{10}{3}\pi\right)\right)\\
&= 2^{10}\left(\cos\left(\frac{4}{3}\pi\right) + i\sin\left(\frac{4}{3}\pi\right)\right)\\
&= 2^{10}\left(-\frac{1}{2} + \left(-\frac{\sqrt{3}}{2}\right)i\right)\\
&= -2^9\left(1+\sqrt{3}i\right)
\end{aligned}$$

Voorbeeld. Los op:

$$a_n = 2(a_{n-1} - a_{n-2})\ met\ a_0 = 1\ en\ a_1 = 2$$

De karakteristieke vergelijking is