

BEWIJZEN

HOOFDSTUK 3: GEHELE GETALLEN

3.4 QUOTIËNT EN REST

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

R is zeker niet leeg, want als $a \geq 0$, dan is $a \in R$ want $a = b \cdot 0 + a$. Als $a < 0$ dan hebben we $a = ba + (1-b)a$ zodat $(1-b)a \in R$, want $(1-b)a \in \mathbb{N}$ omdat $1-b \leq 0$ en $a < 0$.

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 $q := y$ kunnen nemen.

Er blijft te tonen dat $0 \leq r < b$. Door de definitie van R is $0 \leq r$ in orde. Indien $r \geq b$, dan is $r - b \geq 0$ en uit $a = by + r \iff a = b(y+1) + (r-b)$ volgt dan $r-b \in R$ en dat is strijdig, want r was het kleinste element van R.

Stelling: r en q in de vorige stelling zijn uniek

Bewijs: Uit het ongerijmde. Onderstel dat

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

Veronderstel dat $q' < q$, zodat $q - q' \geq 1$. Dan krijgen we:

$$r' = a - bq' = (a - bq) + b(q - q') \geq r + b \geq b.$$

Strijdig. Bijgevolg is $q' < q$ niet waar. Analoog toon je dat $q' > q$ ook niet kan. Uiteindelijk moet dus $q' = q$ en dan ook $r = r'$.

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

cursus bekijken

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

Bewijs: $d \mid n \iff \exists k \in \mathbb{Z} : n = kd$ en $c \mid n/d \iff c \mid k \iff \exists l \in \mathbb{Z} : k = lc$. Bijgevolg is $n = lcd$ en dus volgt $c \mid n$ en aangezien $n/c = ld$ volgt ook $d \mid n/c$.

3.5 GROOTSTE GEMENE DELER

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

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

Eigenschap: Stel $a = bq + r$. Dan is $\text{ggd}(a, b) = \text{ggd}(b, r)$.

Bewijs: Stel $d \mid a$ en $d \mid b$. Dan zal ook $d \mid (a - bq)$ zodat $d \mid b$ en $d \mid r$. Omgekeerd: als $d \mid b$ en $d \mid r$ dan volgt $d \mid (bq + r)$ zodat $d \mid \text{ggd}(a, b)$.

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

Bewijs: Voor $b = 0$ is de stelling triviaal. Als $b \neq 0$, 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 $r_{k-3} = r_{k-5} - r_{k-4}q_{k-3}$ enz. Uiteindelijk vinden we

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

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

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

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

Gevolg: Zij a en b gehele getallen. Enkel veelvouden van $\text{ggd}(a, b)$ zijn te schrijven als $ma + nb$.

Bewijs. Schrijf $d = \text{ggd}(a, b) = ma + nb$, 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 $q = x - kd = (m' - km)a + (n' - kn)b$ een getal kleiner dan d dat te schrijven is als $ra + sb$, tegenspraak. $\square$

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

Gevolg: Als a en b relatief priem zijn, kan elk geheel getal geschreven worden als $ma + nb$.

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

Eigenschap: Een positief rationaal getal heeft een unieke schrijfwijze als a/b met a en b relatief priem en positief.

Bewijs:

Stel $\frac{a}{b} = \frac{a'}{b'}$ met $\text{ggd}(a, b) = 1 = \text{ggd}(a', b')$. Dan is $ab' = a'b$. Maar

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

Dus $b \mid b'$. Analoog bewijs je dat $b' \mid b$ zodat uiteindelijk $b = b'$ en bijgevolg $a = a'$. $\square$

3.6 PRIEMGETALLEN

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

Bewijs: Veronderstel even dat er minstens één 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 $m \in A$.

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

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

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

- $n = 1$ OK, triviaal
- $n = k \Rightarrow n = k + 1$
Onderstel dat $p \mid x_1 x_2 \cdots x_k x_{k+1}$ en stel $x := x_1 x_2 \cdots x_k$. Dan hebben we $p \mid x x_{k+1}$.
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 $\text{ggd}(p, x) = 1$ omdat p priem is en dus maar twee delers heeft en p niet de ggd kan zijn. De stelling van Bezout levert $m, n \in \mathbb{Z}$ zo dat $1 = mp + nx$. Dan geldt:

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

Vermits $p \mid mp x_{k+1}$ en $p \mid nx x_{k+1}$ (omdat $p \mid x x_{k+1}$), moet $p \mid x_{k+1}$.

Stelling: 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 twee verschillende ontbindingen:

$$p_1 p_2 \cdots p_k = n = p'_1 p'_2 \cdots p'_l$$

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

Uit $n = p_1 p_2 \cdots p_k$ leiden we af dat $p_1 \mid n$ en dus $p_1 \mid p'_1 p'_2 \cdots p'_l$. 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

$$p_1 p_2 \cdots p_k = p_1 p'_2 \cdots p'_l$$

zodat

$$p_2 \cdots p_k = p'_2 \cdots p'_l$$

hetgeen een tegenspraak is, want dan zou $p_2 \cdots p_k$ een getal kleiner dan n zijn met twee verschillende ontbindingen. $\square$

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 ontbinding van m en n : $m = 2^x h$ en $n = 2^y k$ met $x, y \in \mathbb{N}$ en h, k oneven (het zijn de producten van de priemfactoren $\neq 2$).

Dan is $m^2 = 2^{2x} h^2$ en $2n^2 = 2^{2y+1} k^2$. Deze twee getallen kunnen nooit gelijk zijn omdat we anders twee priemontbindingen zouden hebben voor m^2 , één met een even aantal factoren 2 één met een oneven aantal. $\square$

Stelling: Er zijn oneindig veel priemgetallen

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

$$m = p_1 p_2 \cdots p_n + 1.$$

Voor elk priemgetal p_i ($i \in [n]$) is $m - 1$ een veelvoud van p_i , dus $\forall i \in [n] : p_i \nmid m$. Maar m heeft een priemontbinding. Dus moeten er andere priemgetallen bestaan dan $p_1, p_2, \dots, p_n$. $\square$

Bewijs op pagina 53 bekijken

3.7 DE Φ -FUNCTIE VAN EULER (PHI)

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

Stelling:

Bewijs: Stel

$$S := \{(d, f) \mid d \mid n, f \in [d], \text{ggd}(d, f) = 1\}.$$

Dan geldt

$$\begin{aligned} |S| &= \sum_{d|n} |\{f \mid (d, f) \in S\}| \\ &= \sum_{d|n} \varphi(d). \end{aligned}$$

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

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

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

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

met $\text{ggd}(f, d) = \text{ggd}(f', d') = 1$. Uit Eigenschap 12 volgt dan $f' = f$ en $d' = d$.

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

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

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

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

$\square$

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

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Bewijs. We stellen weer voor $d \mid n$: $A_d := \{x \in [n] \mid d \mid x\} = \{kd \mid k \in [\frac{n}{d}]\}$ zodat $|A_d| = \frac{n}{d}$. Zoals in het voorbeeld hebben we nu

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

met

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

de som van de cardinaliteiten van alle doorsnedes van i van de k verzamelingen. Dit kunnen we nog schrijven als

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

Dus

$$\begin{aligned} \varphi(n) &= n - \left(n \left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_k} \right) \right. \\ &\quad \left. - n \left(\frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \cdots \right) \right. \\ &\quad \left. + \cdots \right. \\ &\quad \left. + (-1)^{k-1} n \left(\frac{1}{p_1 p_2 \cdots p_k} \right) \right) \\ &= n \left(1 - \frac{1}{p_1} \right) \left(1 - \frac{1}{p_2} \right) \cdots \left(1 - \frac{1}{p_k} \right). \end{aligned}$$

□

3.8 EQUIVALENTIERELATIES EN PARTITIES

Stelling: Een equivalentierelatie geeft steeds aanleiding tot een partitie.

Bewijs: Stel voor $x \in X$:

$$E_x := \{y \in X \mid y \mathcal{R} x\}.$$

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

- (P2) is voldaan omdat $\forall x \in X : E_x \subset X$, zodat $\mathcal{E} \subset X$ maar bovendien geeft de reflexiviteit van $\mathcal{R}$ dat $\forall x \in X : x \in E_x$, zodat $X \subset \mathcal{E}$.
- (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 $x \mathcal{R} z$ en $y \mathcal{R} z$ en bijgevolg $x \mathcal{R} y$ zodat $x \in E_y$. De transitiviteit toont aan dat $E_x \subset E_y$. Ook $y \in E_x$ zodat $E_y \subset E_x$.

□

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

(P1) $\forall A \neq B \in \mathcal{A}: A \cap B = \emptyset$

(P2) $\bigcup \mathcal{A} = V$

Stelling 22. Ook omgekeerd geeft elke partitie van een verzameling X aanleiding tot een equivalentierelatie.

Bewijs. Zij $\mathcal{A}$ een partitie van X . Definieer, voor $x, y \in X$:

$$x \mathcal{R} y \iff \exists A \in \mathcal{A} : x, y \in A.$$

Ga zelf als oefening na dat dit een equivalentierelatie is. $\square$

3.9 CONGRUENTIES

Eigenschap: $\equiv_m$ is een equivalentierelatie.

Bewijs: $\equiv_m$ is

- reflexief: $x \equiv_m x$ want $x - x = 0$ is een veelvoud van m ;
- symmetrisch: $x \equiv_m y \Rightarrow y - x = km \Rightarrow x - y = (-k)m \Rightarrow y \equiv_m x$;
- transitief: $x \equiv_m y$ en $y \equiv_m z \Rightarrow y - x = km$ en $z - y = lm \Rightarrow z - x = (z - y) + (y - x) = (k + l)m$.

$\square$

(definitie equivalentierelatie is belangrijk)

Stelling 23. $\equiv_m$ is 'compatibel' met '+' en '·' in $\mathbb{Z}$, i.e.: $\forall x_1, x_2, y_1, y_2 \in \mathbb{Z}$ met $x_1 \equiv_m x_2$ en $y_1 \equiv_m y_2$:

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

en

$$x_1 y_1 \equiv_m x_2 y_2.$$

Bewijs. Stel $x_2 - x_1 = km$ 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

$$\begin{aligned} x_2 y_2 - x_1 y_1 &= x_2 y_2 - x_1 y_2 + x_1 y_2 - x_1 y_1 \\ &= (x_2 - x_1) y_2 + (y_2 - y_1) x_1 \\ &= km y_2 + lm x_1 \\ &= (k y_2 + l x_1) m \end{aligned}$$

$\square$

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

$$x \equiv x_0 + x_1 + \dots + x_n \pmod{9}.$$

Bewijs.

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

Maar er geldt duidelijk dat $9 \mid 10^i - 1 = \underbrace{99 \dots 99}_{i \text{ keer}}$. Als we dan $\rho(x)$ schrijven voor $x_0 + x_1 + \dots + x_n$, dan hebben we aangetoond:

$$\forall x \in \mathbb{Z} : x \equiv \rho(x) \pmod{9}.$$

$\square$

3.10 MODULAIR REKENEN

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

Bewijs. De bewerkingen zijn inwendig: $E_k + E_l \in \mathbb{Z}_m$ en $E_k \times E_l \in \mathbb{Z}_m$. De commutativiteit komt neer op $E_k + E_l = E_l + E_k$ en $E_k \times E_l = E_l \times E_k$, wat klopt door de overeenkomstige eigenschappen van $+$ en $\times$ in $\mathbb{Z}$. Verder moeten we nog aantonen dat

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

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 $xy = xz = 1$. Dan $y = y \times 1 = y(xz) = (yx)z = 1 \times z = z$. $\square$

Stelling 25.

$$\forall x \in \mathbb{Z}_m : x \in \mathcal{U}_m \iff \text{ggd}(x, m) = 1.$$

Bewijs. $\boxed{\Rightarrow}$

$$\begin{aligned} x \in \mathcal{U}_m &\iff \exists y \in \mathbb{Z}_m : xy = 1 \\ &\iff \exists y \in \mathbb{Z}, \exists k \in \mathbb{Z} : xy - 1 = km \\ &\iff \exists y \in \mathbb{Z}, \exists k \in \mathbb{Z} : xy - km = 1 \end{aligned}$$

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

$$\boxed{\Leftarrow} \text{ ggd}(x, m) = 1 \Rightarrow \exists y, k \in \mathbb{Z} : xy + km = 1 \text{ of } xy - 1 = -km \text{ of nog } m \mid xy - 1 \text{ zodat } xy = 1 \text{ in } \mathbb{Z}_m.$$

$\square$

Gevolg 7. $|\mathcal{U}_m| = \varphi(m)$.

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 $x, y \in \mathcal{U}_m$, dan $xy \in \mathcal{U}_m$ en $(xy)^{-1} = y^{-1}x^{-1}$.

Bewijs. $xy \times y^{-1}x^{-1} = xx^{-1} = 1$ en inversen zijn uniek. $\square$

Stelling 26.

$$\forall y \in \mathcal{U}_m : y\mathcal{U}_m = \mathcal{U}_m.$$

Bewijs. Uit Lemma 3 volgt $y\mathcal{U}_m \subset \mathcal{U}_m$. Stel nu $x \in \mathcal{U}_m$. Dan is $x = y(y^{-1}x)$ en $y^{-1} \in \mathcal{U}_m$, want $y^{-1}y = 1$, zodat $y^{-1}x \in \mathcal{U}_m$. $\square$

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

Bewijs. Nummer de elementen van $\mathcal{U}_m$. Dus $\mathcal{U}_m = \{u_1, u_2, \dots, u_{\varphi(m)}\}$. Stel $u := u_1 u_2 \cdots u_{\varphi(m)}$. Dan is u een element van $\mathcal{U}_m$, want het is een product van elementen van $\mathcal{U}_m$.

Vermits $y\mathcal{U}_m = \mathcal{U}_m$ 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:

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

of nog

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

of

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

□

Stelling 28. Voor p priem hebben we

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

Bewijs. Als $p \nmid n$ is n inverteerbaar modulo p zodat $n^{\varphi(p)} \equiv_p 1$, of nog $n^{p-1} \equiv_p 1$, zodat $n^p \equiv_p n$.

Als $p \mid n$ is het duidelijk dat $n^p \equiv_p 0 \equiv_p n$. □

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

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

een oplossing die uniek is modulo $m = m_1 m_2 \cdots m_n$. 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.

Voor $k \in [n]$ stellen we eerst $M_k := m/m_k$. Dit is het product van alle moduli, behalve m_k . Vermits alle moduli relatief priem zijn, hebben we zeker $\text{ggd}(m_k, M_k) = 1$. Stelling 25 zorgt dan voor een getal y_k met

$$M_k y_k \equiv 1 \pmod{m_k}$$

Stel nu

$$x := a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \in \mathbb{Z}.$$

We tonen nu dat deze x een oplossing is van het stelsel. Merk eerst op dat $M_j \equiv 0 \pmod{m_i}$ van zodra $i \neq j$. Als we dus x reduceren modulo m_k , blijft er alleen maar

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$$

over.

Onderstel nu dat y een andere oplossing is van het stelsel. Dan geldt voor elke $k \in [n]$ dat $m_k \mid x - y$. Vermits alle m_k relatief priem zijn, volgt hieruit $m \mid x - y$. $\square$

HOOFDSTUK 4: GRAFFENTHEORIE

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

Eigenschap (handshake): In een eindige ongerichte graf G geldt steeds (som van alle graden) = 2 keer het aantal bogen)

Bewijs: Dubbeltelling: $\deg(v)$ is het aantal bogen die v bevatten en elke boog bevat 2 toppen.

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

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

Eigenschap: Voor een ongerichte graf G geldt dat: $d: V(\mathcal{G}) \times V(\mathcal{G}) \rightarrow \mathbb{N} \cup \{\infty\}: (u, v) \mapsto d(u, v)$

(lengte kortste wandeling is $d(u, v)$) Een metriek is.

Bewijs: Het is duidelijk dat $d(u, v) = 0 \Leftrightarrow u = v$ en dat $d(u, v) = d(v, u)$ voor elk paar toppen $u, v \in V(G)$. 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 u naar w die lengte $k + l$ heeft. De afstand $d(u, w)$ zal dus ten hoogste $k + l$ bedragen.

(want $d(u, v)$ is 0)

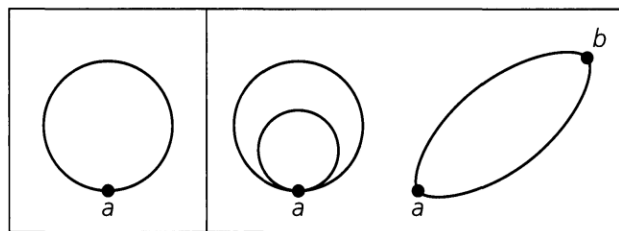
Stelling (Euler) 30: Zij G een ongerichte multigraf zonder geïsoleerde toppen. Dan geldt dat G een Eulergraf is als en slechts als G samenhangend is en alle toppen van G even graad hebben.

Bewijs. $\Rightarrow$ Omdat $\mathcal{G}$ een Eulercyclus heeft, bestaat er $\forall a, b \in V$ een pad van a naar b , namelijk dat deel van de cyclus dat start in a en aankomt in b . **Dus $\mathcal{G}$ is samenhangend.** ✓

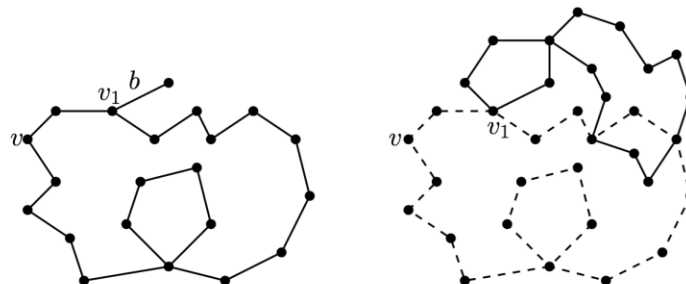
Kies een willekeurige top v in $\mathcal{G}$. Als we de Eulercyclus volgen, passeren we mogelijks verschillende keren in v . Elke doorgang in v gebruikt twee bogen: één om binnen te komen en één om terug buiten te gaan. Ook doorlopen we elke boog die v bevat juist één keer zodat $\deg(v)$ gelijk is aan tweemaal het aantal keer dat we in v komen, **wat een even getal is.** ✓

$\Leftarrow$ We moeten een Eulercyclus construeren.

Als het aantal bogen in $\mathcal{G}$ 1 of 2 is, dan ziet $\mathcal{G}$ er als volgt uit:



We gaan nu verder **per inductie** en onderstellen dat het resultaat waar is wanneer er minder dan n bogen zijn. Wanneer $\mathcal{G}$ n bogen heeft, neem dan v een willekeurige top. Kies een boog die v bevat. Die heeft een ander uiteinde u . Kies nu een boog die u bevat, maar niet de boog die je juist gebruikte om uit v te vertrekken. Blijf zo bogen toevoegen, zonder tweemaal dezelfde te gebruiken. Doordat de graad van elke top even is, kunnen we steeds verder (telkens we in een top binnenkomen, is er nog een ongebruikte boog om buiten te gaan). Doe dit tot we terug in v aankomen, dan hebben we een gesloten pad P gemaakt dat vertrekt en aankomt in v en geen enkele boog tweemaal gebruikt. Als alle bogen van $\mathcal{G}$ tot P behoren, hebben we een Eulercyclus.



Als er nog bogen zijn die niet tot P behoren, moet er, wegens de samenhang van $\mathcal{G}$, een boog b bestaan die niet tot P behoort, maar wel een top v_1 van P bevat. Laten we nu alle bogen van P weg uit de graf $\mathcal{G}$, dan houden we een graf $\mathcal{G}'$ over waarin alle toppen nog steeds even graad hebben (we lieten per top een even aantal bogen weg). Misschien is $\mathcal{G}'$ niet samenhangend, maar dan beschouwen we de samenhangscomponent die v_1 bevat. Deze bevat een Eulercyclus P_1 . Hetzelfde geldt voor alle resterende samenhangscomponenten. Zo krijgen we verschillende paden P_i in $\mathcal{G}$ die geen boog gemeenschappelijk hebben met P , maar wel allen een top v_i op P hebben. We kunnen alle paden combineren door in v te beginnen, het pad P te volgen tot in v_1 , dan het pad P_1 te nemen tot we weer in v_1 komen, waar we weer het pad P volgen tot in v_2 waar we P_2 volgen, enzovoort. Omdat $\mathcal{G}$ eindig is, stopt het proces en bekomen we een Eulercyclus voor $\mathcal{G}$. $\square$

Gevolg: Een samenhangende ongerichte multigraf G heeft een Eulerpad dat niet gesloten is als en slechts als G juist twee toppen heeft van oneven graad.

Bewijs:

$\Rightarrow$ Zij u en v de begin- en eindtop van het Eulerpad. De eerste boog van het pad geeft een bijdrage 1 tot de graad van u . Telkens het pad weer langs u gaat, neemt de graad met 2 toe. Dus zal de graad van u in het totaal oneven zijn. Analoog zal de graad van v oneven zijn omdat de laatste boog van het pad de graad met 1 laat toenemen. Alle overige toppen hebben duidelijk even graad.

$\Leftarrow$ Zij u en v de twee toppen met oneven graad. Voeg aan G de boog $\{u, v\}$ toe. Dan heeft elke top even graad en is vorige stelling van toepassing. We krijgen dus een gesloten Eulerpad. Als we hierin de boog $\{u, v\}$ weglaten, hebben we een Eulerpad in G .

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

Bewijs. Zij $\mathcal{H}$ een Hamiltoncyclus in $\mathcal{G}$. Noem de grafen die uit $\mathcal{G}$ en $\mathcal{H}$ respectievelijk ontstaan door weglaten van k toppen resp. $\mathcal{G}'$ en $\mathcal{H}'$. Voor $\mathcal{H}$ is de bewering zeker waar omdat $\mathcal{H}$ een cyclus is (en die valt uiteen in hoogstens k componenten). Maar $\mathcal{G}'$ bevat meer bogen dan $\mathcal{H}'$. Dus kan het aantal samenhangscomponenten van $\mathcal{G}'$ niet groter zijn dan dat van $\mathcal{H}'$. $\square$

Stelling: Zij G een multigraf waarbij het verwijderen van n toppen leidt tot $m > n$ samenhangscomponenten, dan is G geen Hamiltongraf.

Stelling (Dirac): Zij G een ongerichte simpele graf met $n > 3$ toppen. Als alle toppen van G minstens graad $n/2$ hebben, dan heeft G een Hamiltoncyclus.

Bewijs: Uit het ongerijmde.

Als de bewering uit de stelling onwaar is, moet er minstens één tegenvoorbeeld bestaan. Zij $\mathcal{G}'$ zo een tegenvoorbeeld met n toppen. Dus geldt voor elke $v \in V(\mathcal{G}')$ dat $\deg(v) \geq \frac{n}{2}$, maar er is geen Hamiltoncyclus. Voeg aan $\mathcal{G}'$ zoveel mogelijk bogen toe (door toppen te verbinden die niet adjacent zijn in $\mathcal{G}'$) zonder een Hamiltoncyclus te vormen. Noem deze graf $\mathcal{G}$. Vermits er geen Hamiltoncyclus is in $\mathcal{G}$, is $\mathcal{G}$ zeker niet de complete graf. Er moeten dus twee toppen v en w bestaan die niet verbonden zijn in $\mathcal{G}$. Vanwege de constructie van $\mathcal{G}$ zou het toevoegen van de boog $\{v, w\}$ een Hamiltoncyclus doen ontstaan. Dus bevat $\mathcal{G}$ een Hamiltonpad $v = v_1 \sim v_2 \sim \dots \sim v_n = w$.

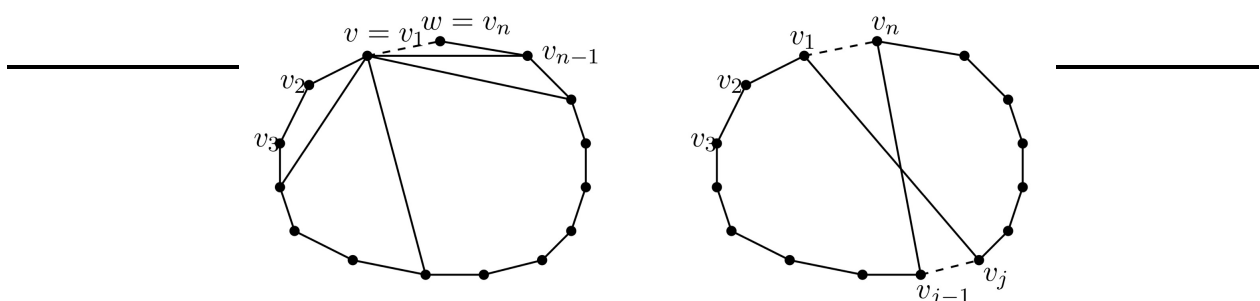
Bekijk de verzameling $\mathcal{G}_v$ van burens van v . Deze heeft minstens $\frac{n}{2}$ elementen. Dan bekijken we de verzameling van opvolgers van een buur van w op het Hamiltonpad. Dus

$$S' := \{v_{i+1} \mid v_i \in \mathcal{G}_w\}.$$

We hebben zeker $w \in S'$ en stellen daarom $S := S' \setminus \{w\}$. Er geldt dan $|S| \geq \frac{n}{2} - 1$. De verzamelingen $\mathcal{G}_v$ en S zijn deelverzamelingen van $\{v_2, v_3, \dots, v_{n-1}\}$ vermits v en w niet adjacent zijn.

De duiventil leert ons dat $|S \cap \mathcal{G}_v| \geq 1$. Dus bestaat er een top v_j met $v_j \sim v$ en $v_j \in S$, wat betekent dat $w = v_n \sim v_{j-1} \sim v_j$. Neem nu het pad $v = v_1 \sim v_j \sim v_{j+1} \sim \dots \sim v_n \sim v_{j-1} \sim v_{j-2} \sim \dots \sim v_1$. Dit is een Hamiltoncyclus, tegenspraak. $\square$

Foto in boek



Stelling: Een samenhangende gerichte (multi)graf G is een gerichte Eulergraf als en slechts als G sterk samenhangend en gebalanceerd is.

Bewijs:

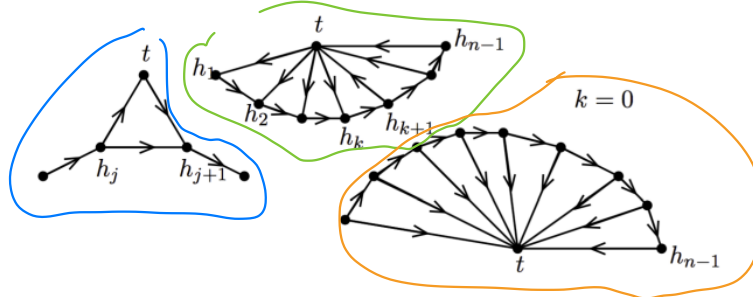
=> Als er een Eulercyclus bestaat in G is het duidelijk dat dat de graf gebalanceerd moet zijn omdat de cyclus in elke top evenveel moet binnenkomen als buitengaan. De Eulercyclus zorgt er ook voor dat er tussen elke twee toppen een gericht pad bestaat

<= Je kan gewoon het ongerichte bewijs van Stelling 30 aanpassen. Doe dit zelf!

Stelling: Elk toernooi heeft een gericht Hamiltonpad

Bewijs. Bij inductie op n , het aantal toppen in het toernooi $\mathcal{T}$.

Als $n = 1$ of $n = 2$ is de stelling duidelijk waar. Onderstel nu dat de stelling geldt voor alle toernooien met $n - 1$ toppen. Kies een willekeurige top t en stel $\mathcal{T}'$ gelijk aan de graf die ontstaat als je t en alle bogen waartoe t behoort verwijdert uit $\mathcal{T}$. Deze $\mathcal{T}'$ is een toernooi met $n - 1$ toppen en heeft dus een Hamiltonpad $h_1 \rightarrow h_2 \rightarrow \dots \rightarrow h_{n-1}$ wegens de inductiehypothese. Als er nu een $j \in [n - 2]$ bestaat met $h_j \rightarrow t \rightarrow h_{j+1}$, dan is $h_1 \rightarrow h_2 \rightarrow \dots \rightarrow h_j \rightarrow t \rightarrow h_{j+1} \rightarrow \dots \rightarrow h_{n-1}$ een Hamiltonpad in $\mathcal{T}$. Als er zo geen j bestaat, dan is er zeker een $k \in \{0, 1, \dots, n - 1\}$ met $\forall j \leq k: t \rightarrow h_j$ en $\forall j > k: t \leftarrow h_j$. Maar dan is $t \rightarrow h_1$ (indien $k \neq 0$) een boog die een Hamiltonpad $t \rightarrow h_1 \rightarrow h_2 \rightarrow \dots$ toelaat. In het geval $k = 0$ kunnen we t op het einde toevoegen: $h_1 \rightarrow h_2 \rightarrow \dots \rightarrow h_{n-1} \rightarrow t$.



□

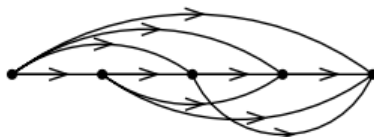
Def toernooi: Gerichte simpele graf door de bogen van een complete graf te oriënteren

Stelling: Een toernooi T heeft een gerichte Hamiltoncyclus als en slechts als T sterk samenhangend is. *

Bewijs:

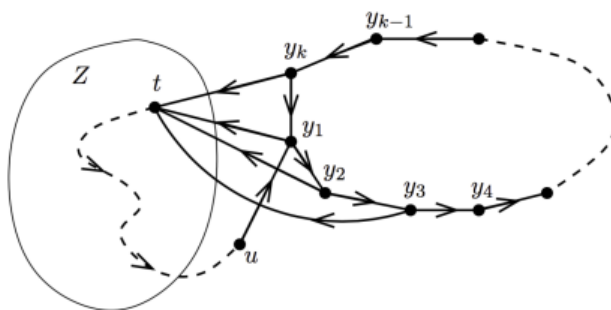
=> Als T een Hamiltoncyclus heeft, dan levert deze een gericht pad tussen elke twee toppen. (Volg de Cyclus)

⇐ Onderstel dat $\mathcal{T}$ sterk samenhangend is. We bewijzen eerst dat $\mathcal{T}$ een gerichte cyclus bevat.¹ Dit doen we uit het ongerijmde. Als $\mathcal{T}$ geen cyclus bevat dan geldt $\forall x, y, z \in \mathcal{T}: (x \rightarrow y \text{ en } y \rightarrow z) \Rightarrow x \rightarrow z$. Dan heet $\mathcal{T}$ een **transitief toernooi**. In zulk een toernooi kan je de punten van links naar rechts rangschikken zodat alle pijlen naar rechts wijzen. Zulk toernooi is duidelijk niet sterk samenhangend omdat er geen pad van rechts naar links gaat, tegenspraak. □



Dus hebben we een cyclus $C = y_1 \rightarrow y_2 \rightarrow \dots \rightarrow y_k \rightarrow y_1$. We veronderstellen dat hij maximale lengte heeft in $\mathcal{T}$ en toch geen Hamiltoncyclus is. Vermits $\mathcal{T}$ sterk samenhangend is, moet er een top t buiten C zijn die verbonden is met een top in C . Zonder de algemeenheid te schaden mogen we ervan uitgaan dat $y_1 \rightarrow t$ een pijl is. Als $t \rightarrow y_2$, zou $y_1 \rightarrow t \rightarrow y_2 \rightarrow y_3 \rightarrow \dots$ een **langere cyclus geven, tegenspraak**. Dus moet de boog tussen t en y_2 anders gericht zijn: $y_2 \rightarrow t$. Analoog moet $\forall i \in [k]: y_i \rightarrow t$.

Stel nu even $Z := \{z \in V(\mathcal{T}) \setminus \{y_2\} \mid y_1 \rightarrow z\}$. Dan geldt, analoog aan voorgaande redenering, dat $\forall z \in Z: \forall i \in [k]: y_i \rightarrow z$. Maar vermits $\mathcal{T}$ sterk samenhangend is, moet er een pad van t naar y_1 bestaan. Dit pad moet minstens één top u buiten Z bevatten omdat je vanuit Z nooit (rechtstreeks) verbonden bent met y_1 . Maar een top buiten Z is, door de definitie van Z en van toernooi, onmiddellijk verbonden met y_1 zodat $t \rightarrow \dots \rightarrow u \rightarrow y_1 \rightarrow y_2 \rightarrow \dots \rightarrow y_k \rightarrow t$ een cyclus is die langer is (minstens twee toppen meer) dan C . Dit is een tegenspraak. □



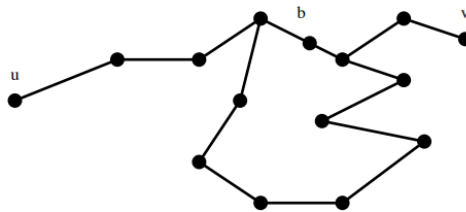
* $\forall v, w \in V(G)$ een gericht pad

4.6 BOMEN EN BOSSEN

Stelling: 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. $(1) \Rightarrow (2)$ Als G minimaal samenhangend is en toch een cyclus zou bevatten, dan kan je een boog b van deze cyclus weglaten zonder de samenhang te verliezen. Inderdaad: zij u en v toppen van G . Ofwel was u met v verbonden via een pad dat b niet bevat en dan blijven ze verbonden. Indien het pad wel de boog b bevatte, kunnen we een nieuw pad maken door de rest van de cyclus te volgen, wat tot een tegenspraak leidt.



$(2) \Rightarrow (1)$ Bij contrapositie: $\neg(1) \Rightarrow \neg(2)$.
Onderstel dat G niet minimaal samenhangend is. Dan is er een boog $b = \{u, v\}$ die we niet nodig hebben voor de samenhang. Dus is er in de graf G' die ontstaat uit G door het weglaten van de boog b , een pad van u naar v . Samen met b vormt dit pad een cyclus in G . $\square$

Gevolg: Een samenhangende ongerichte graf is een boom als en slechts als elke twee toppen verbonden zijn door juist één pad

Bewijs:

$\Rightarrow$ Als er voor elke twee toppen juist één verbinding is, is de graf in kwestie minimaal samenhangend.

Inderdaad: als je na het verwijderen van een boog $b = \{u, v\}$ nog een samenhangende graf zou hebben, zou er buiten de boog b nog een pad van u naar v zijn, tegenspraak.

$\Leftarrow$ Zij H een boom en veronderstel dat er twee paden zijn tussen twee toppen u en v . Neem dan de stukken van die paden die niet samenvallen. Dit zijn cycli, tegenspraak.

Lemma: Een boom op $n \geq 2$ toppen heeft minstens twee bladeren.

Bewijs: Neem een top t van de boom. Dan zijn er twee mogelijkheden:

- 1) t is geen blad Wandel dan vanuit t naar een buur, dan nog een buur, enz. zonder ooit een top tweemaal te bezoeken. Omdat de boom eindig is, stopt dit in een zekere top s . Dit moet een blad zijn, want als het proces gestopt zou zijn omdat s meerdere buren zou hebben die reeds eerder bezocht werden, betekent dit dat er meerdere paden van t naar s zijn, tegenspraak. Om het tweede blad te vinden gebruiken we dat t geen blad is en dus $\deg(t) > 1$ zodat we vanuit t nog een wandeling kunnen maken op zoek naar een ander blad.
- 2) t is een blad Neem dan de enige buur van t in plaats van t . Deze top heeft graad > 2 tenzij de boom bestaat uit twee toppen die één boog vormen. Maar in dit geval geldt het lemma duidelijk.

Stelling: Een boom met n toppen heeft $n - 1$ bogen

Bewijs: Per inductie op n . Voor $n = 1$ is de stelling duidelijk voldaan. Onderstel dat de stelling waar is voor n toppen en zij T een boom met $n + 1$ toppen. Het lemma verzekert ons het bestaan van een blad t . Uit T laten we t samen met de unieke boog op t weg. Dit levert een graf T_0 op die een boom is met n toppen en één verbinding minder dan T . Deze heeft wegens de inductiehypothese $n - 1$ bogen.

Eigenschap: Zij F een bos met n toppen en k samenhangscomponenten. Dan heeft F juist $n - k$ bogen.

Bewijs. We hebben k bomen met respectievelijk $n_1, n_2, \dots, n_k$ toppen. Die hebben dus elk $n_i - 1$ bogen zodat het totaal aantal bogen $n_1 - 1 + n_2 - 1 + \dots + n_k - 1 = (\sum_{i=1}^k n_i) - k = n - k$. $\square$

Stelling (cayley): Voor elke $n \in \mathbb{N} \setminus \{0, 1\}$ is het aantal genummerde bomen met n toppen gelijk aan n^{n-2} . (het aantal bomen in een complete graf is n^{n-2})

Bewijs. Gegeven een boom met n toppen, dan kan je daarin twee (niet noodzakelijk verschillende) toppen als wortel kiezen (we noemen de boom **dubbel geworteld**). Er zijn dus n^2 manieren om de gegeven boom dubbel te wortelen. Als we t_n gelijk stellen aan het aantal genummerde bomen met n toppen, hebben we $n^2 t_n$ dubbel gewortelde genummerde bomen op n toppen.

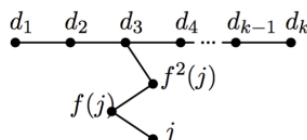
We tonen nu dat het aantal dubbel gewortelde bomen n^n bedraagt. Dit doen we door een bijectie te maken tussen die dubbel gewortelde bomen en de verzameling functies van $[n]$ naar $[n]$.

Zij $f: [n] \rightarrow [n]$ een afbeelding en stel

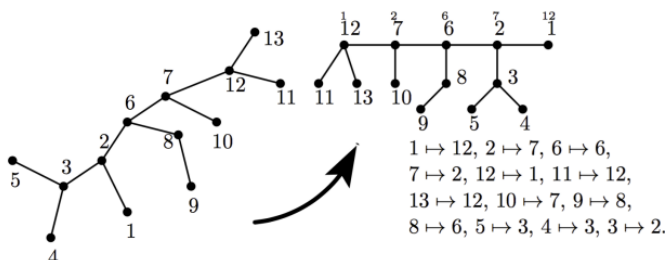
$$C := \{x \in [n] \mid \exists i \in \mathbb{N}_0: f^i(x) = x\},$$

welke we de *cyclische punten* van f noemen. We ordenen $C = \{c_1, c_2, \dots, c_k\}$ zó dat $c_1 < c_2 < \dots < c_k$. Stel nu voor elke $j \in [k]$: $d_j := f(c_j)$. Schrijf nu de getallen d_i naast de toppen van een pad P_k van lengte k . We nemen d_1

als eerste wortel en d_k als tweede. Voor $j \notin C$ maken we bogen $j \sim f(j)$. Dit geeft een dubbel gewortelde genummerde boom. Inderdaad: als we f verschillende keren laten inwerken op $j \notin C$, komen we uiteindelijk in een cyclisch punt terecht. Het pad $d_1 \sim d_2 \sim \dots \sim d_k$ verzekert de samenhang zonder dat er cyclussen komen omdat deze van cyclische punten zouden komen en we hebben er juist voor gezorgd dat die in de graf geen cyclus vormen.



Omgekeerd: een dubbel gewortelde genummerde boom tekenen we zó dat het pad tussen de twee wortels mooi recht ligt (dit zal overeenkomen met het pad P_k van hierboven). Voor j niet op dat rechte pad, stel je dan $f(j)$ gelijk aan de eerste buur van j op het unieke pad van j naar een top van het rechte pad. Op het rechte pad definiëren we het beeld van de i -de (te beginnen met de kleinste) top als die die op de i -de plaats staat op het rechte pad (te beginnen met de “linkse” wortel die nummer 1 krijgt).



$\square$

Gevolg: Het aantal gewortelde genummerde bomen op n toppen is n^{n-1} .

Gevolg: 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 burens van deze top maak je wortel van de samenhangscomponenten die overblijven. Dus is het aantal gewortelde genummerde bossen juist $(n+1)^{(n+1)-2} = (n+1)^{n-1}$). $\square$

Gierigheidsalgoritme van 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.

Lemma: 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: onderstel dat er zo geen boog is. Dus om het even welke boog van F' je toevoegt aan F , je verkrijgt telkens weer een cyclus. Dus alle bogen van F' verbinden toppen van eenzelfde samenhangscomponent van F . Dan moet F' minstens evenveel componenten hebben als F . Als het aantal samenhangscomponenten van F gelijk is aan k , weten we dat F juist $n - k$ bogen heeft. Maar gegeven was dat F' meer bogen heeft dan F , tegenspraak. $\square$

Stelling: Het gierigheidsalgoritme vindt steeds een opspannende boom met minimaal gewicht.

Bewijs. Noem het resultaat van het gierigheidsalgoritme $\mathcal{T}$ en onderstel dat de graf $\mathcal{G}$ een lichtere opspannende boom $\mathcal{H}$ heeft. Orden de bogen van $\mathcal{H}$ zó dat $w(h_1) \leq w(h_2) \leq \dots \leq w(h_{n-1})$. We doen hetzelfde voor $\mathcal{T}$ zodat $w(t_1) \leq w(t_2) \leq \dots \leq w(t_{n-1})$. Vermits het gierigheidsalgoritme begint met de allerlichtste boog, moet gelden

$$w(t_1) \leq w(h_1)$$

Zij i de eerste index waar $\mathcal{H}$ lichter wordt dan $\mathcal{T}$. Dus i is het kleinste getal zodat

$$\sum_{j=1}^i w(h_j) < \sum_{j=1}^i w(t_j)$$

Door onze veronderstelling bestaat zulke $i > 1$. Vermits i de eerste index is waar $\mathcal{H}$ lichter wordt, geldt zeker $w(h_i) < w(t_i)$ en ook

$$\sum_{j=1}^{i-1} w(h_j) \geq \sum_{j=1}^{i-1} w(t_j)$$

Stel $\mathcal{T}_{i-1}$ gelijk aan het bos dat geleverd wordt door het gierigheidsalgoritme na $i - 1$ stappen. Stel ook $\mathcal{H}_i$ gelijk aan het bos dat bestaat uit de bogen $h_1, h_2, \dots, h_i$. Volgens voorgaand lemma kunnen we een boog van $\mathcal{H}_i$ toevoegen aan $\mathcal{T}_{i-1}$ zodanig dat het nog een bos blijft. Deze boog is een zekere h_j met $j \leq i$. Maar nu geldt

$$w(h_j) \leq w(h_i) < w(t_i)$$

Dit toont dat het gierigheidsalgoritme nooit t_i zou kiezen in de i -de stap, maar eerder h_j die lichter is, tegenspraak. $\square$

Stelling 40 (Kirchhoff). *Zij $\mathcal{G}$ een gerichte multigraf zonder lussen en zij B de incidentiematrix van $\mathcal{G}$. Stel B_0 gelijk aan de matrix die ontstaat na verwijdering van om het even welke rij van B . Het aantal opspannende bomen in $\mathcal{G}$ is dan gelijk aan $\det B_0 B_0^\top$.*

Bewijs. Door henummering van de n toppen kan je er steeds voor zorgen dat de weggelaten rij de laatste is. Als $m < n-1$ kan $\mathcal{G}$ zeker niet samenhangend zijn en zijn er dus geen opspannende bomen. Neem C een willekeurige $(n-1 \times n-1)$ -deelmatrix van B_0 . We bewijzen nu dat $|\det C| = 1$ als en slechts als de deelgraf $\mathcal{G}_C$ bepaald door de kolommen van C (dit zijn juist $n-1$ pijlen van $\mathcal{G}$) een opspannende boom is. Anders is $\det C = 0$. We doen dit per inductie op n .

De basisstap van de inductie is voor $n = 2$. Voor zulke kleine grafen is de stelling duidelijk waar.

Onderstel in een eerste geval dat er in $\mathcal{G}_C$ een top v_i is van graad (= in- + uitgraad) 1. Dit betekent dat de i -de rij van C juist één niet-nul element bevat (en dat element is ± 1). We kunnen $\det C$ ontwikkelen volgens de i -de rij. Nu kunnen we de inductiehypothese gebruiken, want de cofactor die we moeten uitrekenen is de determinant van de matrix die overeenkomt met de graf $\mathcal{G}_C$ waar we v_i uit hebben weggelaten. We noteren deze graf $\mathcal{G}_C - v_i$. Dit is duidelijk een opspannende boom van $\mathcal{G} - v_i$ als en slechts als $\mathcal{G}_C$ een opspannende boom was van $\mathcal{G}$.

Als er nu geen top is van graad 1 in $\mathcal{G}_C$ (behalve misschien v_n , de top die we weglieten in B_0), dan kan $\mathcal{G}_C$ geen boom zijn en nog minder een opspannende boom. Maar $\mathcal{G}_C$ heeft wel $n-1$ pijlen en $n-1$ toppen. Dus moet $\mathcal{G}_C$ een top van graad nul 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 is, bevat elke kolom van C een $+1$ en een -1 . Bijgevolg is de som van alle rijen van C de nulrij zodat de rijen van C lineair afhankelijk zijn en $\det C = 0$.

Nu gebruiken we de formule van Cauchy-Binet (zie Appendix A) die zegt dat

$$\det B_0 B_0^\top = \sum_{C \text{ een } (n-1 \times n-1)\text{-deelmatrix van } B_0} (\det C)^2.$$

Maar we weten dat $(\det C)^2 = 1$ of 0 , naargelang de kolommen van C een opspannende boom bepalen of niet. $\square$

Stelling 41. *Het aantal opspannende bomen in een ongerichte simpele graf is gelijk aan elke cofactor van $L_{\mathcal{G}}$.*

Bewijs. We maken van $\mathcal{G}$ een gerichte graf $\mathcal{H}$ door elke boog $u \sim v$ te vervangen door twee pijlen $u \rightarrow v$ en $u \leftarrow v$.

Zij B_0 de incidentiematrix van $\mathcal{H}$, met de laatste rij weggelaten. We bewijzen dat $B_0 B_0^\top = 2L_{0\mathcal{G}}$, waarbij deze laatste matrix ontstaat uit $L_{\mathcal{G}}$ door de laatste rij en laatste kolom weg te laten. Op plaats (i, j) van $B_0 B_0^\top$ staat het scalair product van de i -de en de j -de rij van B_0 i.e. $\sum_{k=1}^m b_{ik} b_{jk}$. 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 $2 \deg(v_i)$ op plaats (i, i) . Voor $i \neq j$ zal elke pijl $v_i \rightarrow v_j$ 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 $\det B_0 B_0^\top = \det 2L_{0\mathcal{G}} = 2^{n-1} \det L_{0\mathcal{G}}$. Maar elke opspannende boom van $\mathcal{G}$ geeft aanleiding tot 2^{n-1} opspannende bomen in $\mathcal{H}$ omdat er 2^{n-1} manieren zijn om de bogen te oriënteren. $\square$

Stelling 42. *Zij $k > 0$. Het element op plaats (i, j) in de k -de macht $A_{\mathcal{G}}^k$ geeft het aantal (gerichte) wandelingen van lengte k van top i naar top j .*

Bewijs. Per inductie op k . Voor $k = 1$ tellen we wandelingen van lengte 1, dus pijlen. De definitie van $A_{\mathcal{G}}$ doet de rest.

Onderstel dat de stelling waar is voor de k -de macht. Zij l een top van $\mathcal{G}$. 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

$$\sum_{l \in V(\mathcal{G})} b_{il} a_{lj} =: c_{ij}$$

De inductiehypothese levert dat b_{il} het element is op plaats (i, l) in $A_{\mathcal{G}}^k$ zodat c_{ij} juist het element is op plaats (i, j) van het matrixproduct $A_{\mathcal{G}}^k A_{\mathcal{G}} = A_{\mathcal{G}}^{k+1}$. $\square$

Stelling 43. *Zij $\mathcal{G}$ een ongerichte multigraf op n toppen met adjacentiematrix $A_{\mathcal{G}}$. Dan is $\mathcal{G}$ samenhangend **als en slechts als** $(I_n + A_{\mathcal{G}})^{n-1}$ enkel strikt positieve elementen heeft.*

Bewijs. Merk op dat een pad tussen twee toppen van $\mathcal{G}$ ten hoogste $n - 1$ bogen heeft. Dus is $\mathcal{G}$ samenhangend als en slechts als er $\forall i, j \in V(\mathcal{G})$ een $k \leq n - 1$ is met een pad van lengte k van de i -de naar de j -de top. Dus $\forall i, j \in V(\mathcal{G}): \exists k < n: (A_{\mathcal{G}}^k)_{ij} > 0$. Vermits $(I_n + A_{\mathcal{G}})^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} A_{\mathcal{G}}^k$, is de stelling bewezen. $\square$

4.7 BIPARTIETE GRAFFEN

Stelling: Een ongerichte multigraf G is bipartiet als en slechts als G geen cyclus bevat van oneven lengte.

Bewijs. $\Rightarrow$ We hebben dit reeds opgemerkt. Onderstel dat er een cyclus $v_1 \sim v_2 \sim \dots \sim v_{2m+1}$ is en v_1 rood werd gekleurd. Dan moet v_2 blauw, v_3 rood, $\dots$, v_{2m+1} rood. Maar dan mag v_1 niet adjacent zijn met v_{2m+1} , tegenspraak.

$\Leftarrow$ Gegeven is een graf G zonder oneven cyclus. We kleuren G met 2 kleuren. Kies een top v en kleur hem rood. Kleur al zijn burens blauw. In het algemeen krijgt een top t de rode kleur als zijn afstand tot v even is en anders de blauwe kleur. We herhalen dit desnoods in elke samenhangscomponent.

We tonen aan dat deze kleuring de graf bipartiet maakt. Veronderstel dat twee adjacenten toppen x en y rood zijn. Dan is er een pad van even lengte van x tot v en een pad van even lengte van y tot v . Dit levert minstens een cyclus van oneven lengte, tegenspraak. Analoog als twee blauwe toppen adjacent zijn. $\square$

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.

Bewijs:

Kies G zo dat geen andere bipartiete graf met n toppen meer bogen heeft. Stel r gelijk aan het aantal rode toppen en b het aantal blauwe. Doordat G maximaal is, is het duidelijk dat elke rode top verbonden is met elke blauwe. Dus heeft G juist rb bogen. Dit is gelijk aan $r(n-r)$. Zoek nu zelf $r \in [n]$ zodat de functie $f(r) = r(n-r)$ een maximum bereikt.

➔ Meer bogen wilt zeggen dat de graf niet bipartiet is

Stelling 46. Zij H een ongerichte simpele graf met $2m$ toppen ($m \geq 2$) en minstens $m^2 + 1$ bogen. Dan bevat H een driehoeksgraf.

Bewijs. Per inductie op m .

Voor $m = 2$ krijgen we dat H een deelgraf is van K_4 met minstens 5 bogen. Vorige stelling zegt dat H niet bipartiet is en dus een cyclus heeft van oneven lengte. Dit moet een driehoek zijn omdat H maar vier toppen heeft.

Als de stelling waar is voor alle grafen met minder dan $2m$ toppen, nemen we in H twee adjacenten toppen u en v . Als $\deg(u) + \deg(v) > 2m$ hebben deze toppen een gemeenschappelijke buur die een driehoek geeft. Als $\deg(u) + \deg(v) \leq 2m$, zal het verwijderen van u en v , samen met alle bogen waartoe ze behoren, het aantal bogen doen afnemen 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 bevat wegens de inductiehypothese een driehoek. $\square$

Stelling 47 (Turán). *Zij $\mathcal{G}$ 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 $\mathcal{G}$ ten hoogste $(r-2)n^2/(2r-2)$.*

Bewijs. Per inductie op r .

Voor $r = 2$ is $\mathcal{G}$ een graf zonder bogen. De bovengrens $(r-2)n^2/(2r-2)$ is in dit geval ook gelijk aan nul.

Voor de inductiestap gaan we van r naar $r+1$. We nemen dus een graf $\mathcal{G}$ die geen deelgraf K_{r+1} bevat en n toppen heeft. Stel $\mathcal{H}$ gelijk aan de grootste deelgraf van $\mathcal{G}$ die geen deelgraf K_r heeft. Noteer x voor het aantal toppen in $\mathcal{H}$.

Beschouw een top v van $\mathcal{G}$. Vermits $\mathcal{G}$ geen K_{r+1} omvat, kan er in de buurt $\mathcal{G}_v$ zeker geen K_r voorkomen (samen met v zouden we anders een K_{r+1} hebben). Vermits de grootste deelgraf van $\mathcal{G}$ die geen K_r omvat x toppen heeft, weten we dat $\mathcal{G}_v$ niet meer toppen kan hebben dan x . Met andere woorden geldt voor elke top $\deg v \leq x$. We beschouwen nu de bogen die niet volledig in $\mathcal{H}$ liggen. Dit zijn dus bogen met minstens één top buiten $\mathcal{H}$. We zullen dit aantal bogen afschatten. Er zijn $n-x$ toppen buiten $\mathcal{H}$ en elk van die toppen heeft graad ten hoogste x . Dus kunnen er niet meer bogen zijn dan $(n-x)x$ buiten $\mathcal{H}$.

De inductiehypothese, toegepast op $\mathcal{H}$, geeft dat het aantal bogen binnen $\mathcal{H}$ niet meer is dan $(r-2)x^2/(2r-2)$. In totaal is het aantal bogen in $\mathcal{G}$ dus ten hoogste $((r-2)x^2/(2r-2)) + x(n-x)$.

Vermits

$$\frac{r-2}{2r-2}x^2 + x(n-x) = \frac{r-1}{2r}n^2 - \frac{r}{2r-2} \left(x - \frac{(r-1)n}{r} \right)^2 \leq \frac{r-1}{2r}n^2$$

is de stelling bewezen. $\square$

4.8 KOPPELINGEN

Stelling 48 (Petersen, 1891). *Gegeven een ongerichte graf $\mathcal{G}$. Een koppeling K in $\mathcal{G}$ is een maximumkoppeling **als en slechts als** er in $\mathcal{G}$ geen vergrotend K -wisselpad bestaat.*

Bewijs. $\Rightarrow$ Als K een maximumkoppeling is, kan er natuurlijk geen vergrotend K -wisselpad bestaan omdat de koppeling anders kan vergroot worden via de hierboven beschreven methode.

$\Leftarrow$ Veronderstel dat K een koppeling is die geen maximumkoppeling is. We moeten tonen dat er een vergrotend K -wisselpad bestaat. Omdat K geen maximumkoppeling is, moet er in $\mathcal{G}$ een koppeling K' bestaan die meer bogen heeft dan K . Stel nu $E' := K \setminus K' \cup K' \setminus K$, dit zijn de bogen die in K of K' zitten, maar niet in $K \cap K'$. Noteer $\mathcal{H}$ de deelgraf van $\mathcal{G}$ met als bogenverzameling E' en als toppenverzameling de uiteinden van de bogen in E' . Omdat K en K' koppelingen zijn, moet elke samenhangscomponent van $\mathcal{H}$ een cyclus of pad zijn waarvan de bogen afwisselend in K en in K' zitten. Componenten met maar één boog kunnen ook voorkomen. Aangezien K' groter is dan K , moet er tenminste één component van $\mathcal{H}$ zijn die meer bogen van K' bevat dan van K . Deze component is dan een pad waarvan de eerste en laatste top K -onverzadigd zijn. Het is dus een vergrotend K -wisselpad. $\square$

Stelling 49 (P. Hall, 1935). *Zij $\mathcal{G} = (V_1 \cup V_2, E)$ een bipartiete ongerichte graf. Een toewijzing van V_1 in V_2 bestaat **als en slechts als** 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 burens 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 $\forall W \subset V_1: |H(W)| \geq |W|$). We bewijzen per inductie op $|V_1|$ dat er een toewijzing van V_1 in V_2 bestaat. Als $|V_1| = 1$, dan is V_1 een singleton $\{u\}$. De voorwaarde van Hall geeft $|H(\{u\})| \geq 1$. De top u heeft dus ten minste één 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 .

We nemen nu aan dat de stelling waar is voor alle bipartiete grafen met $|V_1| \leq k$. We onderscheiden twee gevallen voor een bipartiete graf $\mathcal{G} = (V_1 \cup V_2, E)$ met $|V_1| = k + 1$. Het eerste geval is dat elke echte deelverzameling van V_1 meer burens 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 . Voor een willekeurige top $u \in V_1$ hebben we dus minstens twee burens in V_2 . Noem één van die burens v . We wijzen v alvast toe aan u en bekijken de bipartiete graf $\mathcal{G}'$ die ontstaat wanneer we $u \sim v$ uit $\mathcal{G}$ weglaten. Deze graf heeft k toppen in V_1 en elke deelverzameling W van V_1 heeft tenminste $|W| + 1$ burens in V_2 en bijgevolg tenminste $|W|$ burens in $V_2 \setminus \{v\}$. Voor de graf $\mathcal{G}'$ geldt dus de voorwaarde van

Hall zodat we uit de inductiehypothese een toewijzing krijgen van $V_1 \setminus \{u\}$ in $V_2 \setminus \{v\}$. Samen met de boog $u \sim v$ vormt deze een toewijzing van V_1 in V_2 .

Kritisch geval Nu is er minstens één 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.

Voor de deelgraf geïnduceerd op $V_1 \setminus W' \cup V_2 \setminus H(W')$ kunnen we de voorwaarde van Hall ook aantonen. Zij W een deelverzameling van $V_1 \setminus W'$. Dan heeft $W' \cup W$ ten minste $|W' \cup W|$ burens in V_2 (door de voorwaarde van Hall). Maar vermits precies $|W'|$ van die burens in $H(W')$ liggen, moeten minstens $|W|$ van hen in $V_2 \setminus H(W')$ liggen. Omdat $|V_1 \setminus W'| \leq k$ is ook hier de inductiehypothese van toepassing zodat we een toewijzing van $V_1 \setminus W'$ in $V_2 \setminus H(W')$ krijgen die samen met de toewijzing van W' in $H(W')$ uiteindelijk een toewijzing van V_1 in V_2 oplevert. $\square$

Stelling 50 (König). *Zij $\mathcal{G} = (V_1 \cup V_2, E)$ 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.

Stelling 51 (König–Egerváry, 1931). Voor een bipartiete ongerichte graf $\mathcal{G} = (V_1 \cup V_2, E)$ geldt

$$\max |K| = \min |U|$$

waarbij K de verzameling van alle koppelingen van $\mathcal{G}$ doorloopt en U de verzameling van alle overdekkingen van $\mathcal{G}$.

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

$$|K_{\max}| = |V_1| - (|W^*| - |H(W^*)|) = |(V_1 \setminus W^*) \cup H(W^*)|.$$

De verzameling

$$U := (V_1 \setminus W^*) \cup H(W^*)$$

heeft het gewenste aantal elementen en is een overdekking. Inderdaad: de verzameling $V_1 \setminus W^*$ overdekt alle bogen met een uiteinde in $V_1 \setminus W^*$ en $H(W^*)$ overdekt alle bogen met een uiteinde in W^* . $\square$

4.10 PLANAIRE GRAFFEN

[HTTPS://NL.WIKIPEDIA.ORG/WIKI/GRAFENTHEORIE#DE_PLANAIRE_GRAAF](https://nl.wikipedia.org/wiki/Grafentheorie#DE_PLANAIRE_GRAAF)

Stelling 52 (weeral van Euler): Voor een samenhangende planaire ongerichte multigraf G geldt steeds

$$v - e + f = 2.$$

↳ *Toppen*

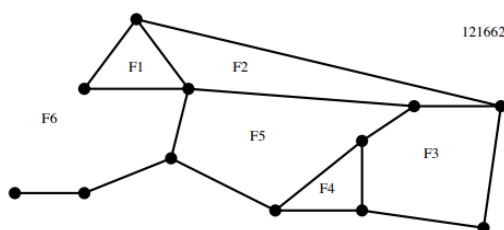
Bewijs: We geven een bewijs per inductie op e , het aantal bogen in G .

Als $e = 1$, dan is de graf ofwel isomorf met het pad P_2 ofwel een lus. In het eerste geval hebben we $v = 2$ en $f = 1$ en in het tweede geldt $v = 1$ en $f = 2$. In beide gevallen is de formule van Euler voldaan.

Onderstel dat de stelling geldt voor alle planaire grafen met $e - 1$ bogen. Er zijn twee gevallen.

[1] We kunnen uit G een boog b weglaten zodat $G' := G - b$ nog steeds samenhangend is. Dan maakt b deel uit van een cyclus in G . Daarom behoort b tot de rand van twee gebieden. De graf G' heeft dan $e - 1$ bogen, $f - 1$ gebieden en v toppen. De inductiehypothese geeft $v - (e - 1) + (f - 1) = 2$.

[2] Er is geen boog die we kunnen weglaten zonder de samenhang te verliezen. Dan is G een boom. Bijgevolg geldt $f = 1$ en $v = e + 1$. $\square$



Stelling 53. *Zij $\mathcal{G}$ een samenhangende planaire ongerichte simpele graf met minstens twee bogen. Dan geldt $3f \leq 2e$ en $e \leq 3v - 6$.*

Bewijs. De stelling is duidelijk waar wanneer er maar één 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 6

Bewijs. We weten $e \leq 3v - 6$. Dus moet

$$\sum_{x \in V(\mathcal{G})} \deg(x) = 2e \leq 6v - 12.$$

Mocht elke top x graad ≥ 6 hebben, zou $\sum_{x \in V(\mathcal{G})} \deg(x) \geq 6v$, tegenspraak. □

Stelling 54 (Kuratowski, 1930). *Een multigraf is planair **als en slechts als** hij geen deelgraf bevat die boogequivalent is met $K_{3,3}$ of met K_5 .*

Stelling 55. *Elke samenhangende planaire ongerichte simpele graf $\mathcal{G}$ kan met 6 kleuren gekleurd worden.*

Bewijs. We doen dit bij inductie op v , het aantal toppen van de planaire graf $\mathcal{G}$.

Voor $v = 1$ is het duidelijk in orde.

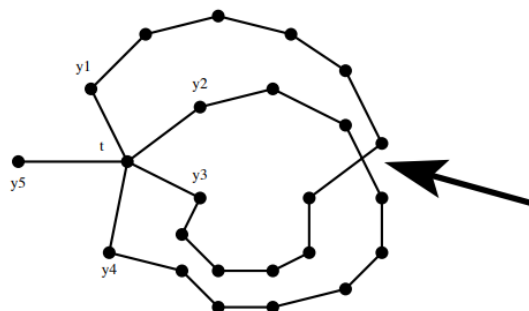
Onderstel nu dat de stelling geldt voor alle planaire grafen met $v - 1$ toppen. Uit Gevolg 14 weten we dat $\mathcal{G}$ een top t heeft met $\deg(t) \leq 5$. Als we t weglaten, krijgen we een graf $\mathcal{G}'$ met $v - 1$ toppen. Deze kan dus gekleurd worden met 6 kleuren. Vermits t hoogstens 5 buren heeft (die in $\mathcal{G}'$ 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 $\mathcal{G}$ 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 vijf kleuren als t echt 5 buren heeft, elk van een andere kleur in de kleuring van $\mathcal{G}'$. 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 $\mathcal{G}'$ de graf die uit $\mathcal{G}$ ontstaat als je t weglaat, alsook de 5 bogen op t . Als $\mathcal{G}'$ 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 $\mathcal{G}'$ 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. $\square$

HOOFDSTUK 5 GENERERENDE FUNCTIE

Stelling 57. Voor elk niet-nul natuurlijk getal n geldt $p_{\neq}(n) = p_o(n)$.

Bewijs. De genererende functie voor $p_o(n)$ is

$$\begin{aligned} P_o(x) &= (1 + x + x^2 + \dots)(1 + x^3 + x^6 + \dots) \dots \\ &= \frac{1}{1-x} \cdot \frac{1}{1-x^3} \cdot \dots \end{aligned}$$

Merk op dat

$$1 + x = \frac{1-x^2}{1-x}, 1 + x^2 = \frac{1-x^4}{1-x^2}, \dots$$

zodat

$$\begin{aligned} P_{\neq}(x) &= (1+x)(1+x^2)(1+x^3) \dots \\ &= \frac{1-x^2}{1-x} \cdot \frac{1-x^4}{1-x^2} \cdot \frac{1-x^6}{1-x^3} \cdot \frac{1-x^8}{1-x^4} \cdot \dots \\ &= P_o(x) \end{aligned}$$

Vermits de genererende functies gelijk zijn, zijn ook de gegenereerde rijen gelijk. $\square$

