

1a) (1p) Valensen $\delta(v)$ för ett hörn v i en graf är antalet grannar till hörnet (= antalet förekomster av v i elementen i E).

b) (1p) En hamiltoncykel i en graf $G = (V, E)$ är en cykel som passerar varje hörn precis en gång (= en permutation $v_1, v_2, \dots, v_n$ av V , där $\{v_i, v_{i+1}\}$ och $\{v_n, v_1\} \in E$ för $i = 0, \dots, n-1$).

c) (1p) Halls sats säger att en bipartit graf $G = (X \cup Y, E)$ (där $X \cap Y = \emptyset$) har en fullständig matchning (dvs en matchning där varje $x \in X$ är matchad) omm för varje $A \subseteq X$ gäller att $|J(A)| \geq |A|$, där $J(A) = \{y \in Y \mid \{x, y\} \in E \text{ för något } x \in A\}$.

2a) (1p) $p \in \mathbb{Z}$ är ett **primtal** omm $p \geq 2$ och dess enda delare är 1 och p (alternativt, omm det har precis två olika positiva delare).

b) (1p) $x \in \mathbb{Z}_m$ är inverterbart omm $\text{sgd}(x, m) = 1$.

c) (1p) $|A| = |B|$ omm det finns en bijektion $f: A \rightarrow B$.

3a) (1p) Binomialsatsen säger att $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$, där $n \in \mathbb{N}$ och $\binom{n}{k}$ är binomialtalet (formeln $\frac{n!}{k!(n-k)!}$ eller rekursionsformeln för $\binom{n}{k}$ krävs inte).

b) (1p) En binär relation $\mathcal{R}$ på en mängd X är reflexiv omm $x\mathcal{R}x$ för alla $x \in X$.

c) (1p) Principen om inklusion och exklusion för tre mängder A, B, C säger att $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$.

4a) (1p) $\pi \in S_n$ är en jämn permutation omm den kan skrivas som en produkt av ett jämnt antal transpositioner.

b) (1p) $\alpha, \beta \in S_n$ är konjugerade omm det finns $\sigma \in S_n$ med $\sigma\alpha\sigma^{-1} = \beta$.

c) (1p) Antalet permutationer i S_6 med cykelstruktur $[123]$ är $6 \cdot \binom{5}{2} \cdot 2 = 6 \cdot \frac{5 \cdot 4}{2 \cdot 1} \cdot 2 = 120$ (elementet i 1-cykeln kan väljas på 6 sätt, sedan kan elementen i 2-cykeln väljas på $\binom{5}{2}$ sätt och övriga 3 element kan bilda en 3-cykel på 2 sätt). Alternativt $\frac{6!}{1 \cdot 2 \cdot 3}$ (ordna alla 6, samma i -cykel kan skrivas på i sätt).

5) (3p) Vi söker antalet ytor en sammanhängande graf som ritas utan korsande kanter på ytan av en sfär delar in sfärens yta i, om antalet hörn är 5 mer än antalet ytor och antalet kanter är 5 mer än antalet hörn.

Lösning:

Med vanliga beteckningar gäller dels Eulers polyederformel $v - e + r = 2$ och dels att $v = r + 5$ och $e = v + 5$. De senare ger $e = r + 10$ så $(r + 5) - (r + 10) + r = 2$ och därmed $r = 7$.

Svar: Den delar in sfärens yta i 7 ytor.

6) (3p) Vi söker alla heltal x, y sådana att $186x + 69y = 3$.

Lösning:

Då ekvationen divideras med 3 fås den ekvivalenta $62x + 23y = 1$.

Euklides algoritm ger $62 = 2 \cdot 23 + 16$, $23 = 1 \cdot 16 + 7$, $16 = 2 \cdot 7 + 2$, $7 = 3 \cdot 2 + 1$ (så $\text{sgd}(62, 23) = 1$ och) $1 = 7 - 3 \cdot 2 = 7 - 3(16 - 2 \cdot 7) = -3 \cdot 16 + 7 \cdot 7 = -3 \cdot 16 + 7 \cdot (23 - 16) = 7 \cdot 23 - 10 \cdot 16 = 7 \cdot 23 - 10(62 - 2 \cdot 23) = -10 \cdot 62 + 27 \cdot 23$.

$\begin{cases} x_0 = -10 \\ y_0 = 27 \end{cases}$ är alltså en lösning till ekvationen. (x, y) uppfyller då ekvationen precis om $62(x - x_0) + 23(y - y_0) = 0$, dvs $62(x - x_0) = -23(y - y_0)$, så (entydig faktorisering och $\text{sgd}(62, 23) = 1$) $x - x_0 = 23k$, för något $k \in \mathbb{Z}$. Det ger $y - y_0 = -62k$. Man ser att $x = x_0 + 23k$, $y = y_0 - 62k$ också löser ekvationen för alla $k \in \mathbb{Z}$, så vi har funnit alla lösningar.

Svar: Alla lösningar ges av $\begin{cases} x = -10 + 23k, \\ y = 27 - 62k, \end{cases}$ för godtyckligt $k \in \mathbb{Z}$.

7) (3p) Vi söker antalet sätt att fördela 12 olika böcker och 6 identiska pennor bland 20 personer, då varje person kan få högst en bok.

Lösning:

Böckerna kan fördelas på $(20)_{12} = \frac{20!}{(20-12)!} = \frac{20!}{8!}$ sätt (antalet injektioner böcker $\rightarrow$ personer).

Pennorna kan fördelas på $\binom{20+6-1}{6} = \frac{25!}{6! \cdot 19!}$ sätt (6 pennor utses bland 25 pennväggar).

Multiplikationsprincipen ger svaret $\frac{20!}{8!} \cdot \frac{25!}{6! \cdot 19!} = \frac{20 \cdot 25!}{6! \cdot 8!}$.

Svar: Det sökta antalet sätt är $\frac{20 \cdot 25!}{6! \cdot 8!}$ ($= 10\,686\,184\,167\,859\,200\,000$).

8) $\pi \in S_8$ ges av $\pi(1)=3, \pi(2)=1, \pi(3)=8, \pi(4)=7, \pi(5)=4, \pi(6)=6, \pi(7)=5, \pi(8)=2$.

Vi skall (a, 1p) skriva π i cykelnotation, (b, 1p) avgöra om π är jämn eller udda och (c, 1p) finna $\tau \in S_8$ med $\pi\tau = \tau\sigma$, där $\sigma = (1\,6\,4)(2\,8\,3\,7)$.

Lösning:

a. $\pi(1) = 3, \pi(3) = 8, \pi(8) = 2, \pi(2) = 1, \pi(4) = 7, \dots$ ger att $\pi = (1\,3\,8\,2)(4\,7\,5)(6)$.

b. Eftersom π har ett udda antal (1) cykler av jämn längd är det en udda permutation.

c. $\pi\tau = \tau\sigma \Leftrightarrow \pi = \tau\sigma\tau^{-1}$ och $\tau\sigma\tau^{-1} = (\tau(1)\tau(6)\tau(4))(\tau(2)\tau(8)\tau(3)\tau(7))(\tau(5))$, så vi kan ta $\tau(1)=4, \tau(6)=7, \tau(4)=5, \tau(2)=1, \dots, \tau(5)=6$. Det ger $\tau = (1\,4\,5\,6\,7\,2)(3\,8)$.

Svar a: $\pi = (1\,3\,8\,2)(4\,7\,5)$, b: π är udda, c: t.ex. $\tau = (1\,4\,5\,6\,7\,2)(3\,8)$.

9) (4p) Vi söker $|V|$ och $|E|$ för en graf $G = (V, E)$ där varje komponent innehåller högst en cykel, precis 18 av komponenterna saknar cykel och medelvärdet av hörnens valenser är $\frac{78}{41}$.

Lösning:

Låt $v = |V|$, $e = |E|$. En komponent utan cykel är ett träd, så den innehåller ett hörn mer än kanter, medan en komponent med precis en cykel har en kant mer, dvs lika många hörn som kanter. Det ger att $v = e + 18$.

Medelvärdet av valenserna, $\frac{78}{41} = 2 - \frac{4}{41}$, är $\frac{1}{v} \sum_{x \in V} \delta(x) = \frac{1}{v} \cdot 2e = \frac{2(v-18)}{v} = 2 - \frac{36}{v}$, så $\frac{36}{v} = \frac{4}{41}$ och $v = \frac{36}{4} \cdot 41 = 369$ och $e = v - 18 = 351$.

Svar: Grafen har 369 hörn och 351 kanter.

10) Vi söker (a, 2p) alla möjliga cykelstrukturer för udda permutationer av ordning 12 i S_{10} och (b, 2p) det totala antalet udda permutationer av ordning 12 i S_{10} .

Lösning:

a. Eftersom ordningen för en permutation är mcm till cykellängderna, måste en av dem vara en multipel av 4, men inte 8, så en 4-cykel måste ingå (≤ 10 ju). P.s.s. måste en cykellängd vara en multipel av 3, men inte 9. 6 går inte, eftersom [46]-permutationer är jämna, så (minst) en cykel måste ha längd 3. Det totala antalet cykler av jämn längd skall vara udda för udda permutation, så enda möjligheterna är $[3^2\,4]$ och $[1^3\,3\,4]$.

b. Antalet av typ $[3^2\,4]$ är $\frac{10!}{2 \cdot 3^2 \cdot 4} = \frac{10!}{72}$ (10! sätt placera in 1–10 i cyklerna, samma permutation om man kastar om 3-cyklerna, i sätt skriva samma i -cykel). P.s.s fås antalet av typ $[1^3\,3\,4]$ till $\frac{10!}{3! \cdot 3 \cdot 4} = \frac{10!}{72}$.

Det sökta antalet är summan av dem (additionsprincipen!), $\frac{10!}{36} = 10 \cdot 2 \cdot 7! = 20 \cdot 5040 = 100800$.

Svar a: Möjliga cykelstrukturer är $[3^2\,4]$ och $[1^3\,3\,4]$, b: Det finns 100 800 st.

11) Vi söker i $\mathbb{Z}_{1547}$ ($1547 = 7 \cdot 13 \cdot 17$) potenserna (a, 1p) 55^{1153} , (b, 1p) 12^{50} och (c, 2p) 26^{224} .

Lösning:

a. Eftersom $\phi(1547) = \phi(7 \cdot 13 \cdot 17) = 6 \cdot 12 \cdot 16 = 1152$ och $\text{sgd}(55, 1547) = 1$ ger Eulers sats att $55^{1152} = 1$ och därmed $55^{1153} = 55$ i $\mathbb{Z}_{1547}$.

b. $\text{sgd}(12, 7) = \text{sgd}(12, 13) = \text{sgd}(12, 17) = 1$, så enligt Fermats lilla sats (7, 13 och 17 är ju primtal) är $12^{48} = (12^6)^8 \equiv_7 1^8 = 1$, $12^{48} = (12^{12})^4 \equiv_{13} 1^4 = 1$, $12^{48} = (12^{16})^3 \equiv_{17} 1^3 = 1$, så $12^{48} - 1$ är delbart med 7, 13 och 17, så med 1547 och $12^{50} \equiv_{1547} 1 \cdot 12^2 = 144$.

c. Som i b) fås $26^{224} \equiv_7 5^{37 \cdot 6 + 2} = (5^6)^{37} \cdot 5^2 \equiv_7 1^{37} \cdot 25 \equiv_7 4$ (ty $7 \nmid 5$), $26^{224} \equiv_{13} 0^{224} = 0$ (ty $13 \mid 26$) och $26^{224} \equiv_{17} 26^{14 \cdot 16} = (26^{16})^{14} \equiv_{17} 1^{14} = 1$ (ty $17 \nmid 26$).

Med $x = 26^{224}$ har vi alltså $x \equiv_{13} 0$, $x \equiv_7 4$ och $x \equiv_{17} 1$. Kinesiska restsatsen!

Den första ger $x = 13s$ för något $s \in \mathbb{Z}$. Den andra ger då $13s \equiv_7 4$, så $0 \equiv_7 s + 4$, dvs $s = 7t + 3$ och $x = 13(7t + 3) = 91t + 39$ för något $t \in \mathbb{Z}$. Den tredje ekvationen ger $91t + 39 \equiv_{17} 6t + 5 \equiv_{17} 1$. Eftersom $\text{sgd}(3, 17) = 1$ kan vi multiplicera med 3 och får $18t + 15 \equiv_{17} t - 2 \equiv_{17} 3$, så $t = 17u + 5$ för något $u \in \mathbb{Z}$ och $x = 91(17u + 5) + 39 = 1547u + 455 + 39 \equiv_{1547} 494$.

Svar: Potenserna är a: 55, b: 144, c: 494 i $\mathbb{Z}_{1547}$.

12) Med $A = \{a_1, a_2, \dots, a_r\}$ och $B = \{b_1, b_2, \dots, b_s\}$ disjunkta med $|A| = r \geq 1$, $|B| = s \geq 1$, skall vi (a, 3p) visa att q_n , antalet ord i $A \cup B$ av längd n och ett udda antal förekomster av element från A , uppfyller $q_n = (s-r)q_{n-1} + r(r+s)^{n-1}$ för $n = 1, 2, \dots$ och $q_0 = 0$ och (b, 2p) bestämma q_n för $n = 0, 1, 2, \dots$

Lösning:

a. $q_n =$ antalet ord av längd n i alfabetet $A \cup B$ med ett udda antal från $A =$
= (antalet som slutar på element i B) + (antalet som slutar på element i A) =
= $s \cdot$ (antalet av längd $n-1$ med ett udda antal ur A) +

+ $r \cdot$ (antalet av längd $n-1$ med ett jämnt antal ur A) =
= $sq_{n-1} + r((r+s)^{n-1} - q_{n-1}) = (s-r)q_{n-1} + r(r+s)^{n-1}$ för $n = 1, 2, \dots$

$q_0 = 0$, eftersom det enda ordet av längd 0 inte innehåller ett udda antal från A .

(Att $A \cap B = \emptyset$ användes vid det andra '=' ovan (additionsprincipen).) **a-saken är klar.**

b. Den homogena rekursionsekvationen $q_n = (s-r)q_{n-1}$ har karakteristisk ekvation $x = s-r$, så dess allmänna lösning är $q_n = C(s-r)^n$.

En partikulärlösning till den inhomogena ekvationen fås med ansatsen $q_n = a(r+s)^n$:

$a(r+s)^n = (s-r)a(r+s)^{n-1} + r(r+s)^{n-1}$, vilket ger $a(r+s) = a(s-r) + r$, så $a = \frac{1}{2}$.

Den allmänna lösningen är alltså $q_n = \frac{1}{2}(r+s)^n + C(s-r)^n$.

$q_0 = 0$ ger $C = -\frac{1}{2}$, så den sökta lösningen är $q_n = \frac{1}{2}((r+s)^n - (s-r)^n)$.

Svar a: Visat ovan, b: $q_n = \frac{1}{2}((r+s)^n - (s-r)^n)$ för $n = 0, 1, 2, \dots$

13) (5p) Vi skall visa att om p är ett primtal och $2p+1$ inte är ett primtal finns inget $x \in \mathbb{Z}$ med $\phi(x) = 2p$.

Lösning:

Vi antar att $x \in \mathbb{Z}$ och $\phi(x) = 2p$ och skall härleda en motsägelse.

Låt $x = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, där p_i :na är olika primtal och alla $e_i \in \mathbb{Z}_+$. Enligt en känd sats är då $\phi(x) = p_1^{e_1-1}(p_1-1) \dots$

$p \geq 5$ (ty $2 \cdot 2 + 1$ och $2 \cdot 3 + 1$ är primtal) och därmed udda, så högst ett p_i är udda (annars ingår en faktor 2^2 i $\phi(x)$).

Fall 1: $p_1 = 2$. Då är $x = 2^{e_1}$ eller $2^{e_1} \cdot p_2^{e_2}$, där $e_1 = 1$ eller 2 (annars en faktor 2^2 i $\phi(x)$).

$x = 2^{e_1}$ ger $\phi(x) = 2^{e_1-1}$, dvs $\phi(x) = 1$ eller 2, båda $\neq 2p$. Omöjligt.

$x = 2^{e_1} \cdot p_2^{e_2}$ ger $\phi(x) = 2^{e_1-1} \cdot p_2^{e_2-1}(p_2-1)$, dvs $\phi(x) = p_2^{e_2-1}(p_2-1)$ eller $2p_2^{e_2-1}(p_2-1)$.

I det första fallet är $p = p_2^{e_2-1} \frac{(p_2-1)}{2}$ och $p_2 - 1 = 2$ eller $2p$, båda omöjliga ($p_2 \neq 3$, ty $p \neq 3^{e_2-1}$, $p_2 \neq 2p+1$, ty p_2 primtal). I det andra fallet är $p = p_2^{e_2-1}(p_2-1)$ och $p_2 - 1 = 1$ eller p , båda omöjliga ($p_2 \neq 2$, ty $p \neq 2^{e_2-1}$, $p_2 \neq p+1$, ty $p+1$ är inte ett primtal (p är ju ett udda primtal)).

Fall 2: $p_1 > 2$. Då är $x = p_1^{e_1}$ (högst ett udda p_i) och $\phi(x) = p_1^{e_1-1}(p_1-1)$, vilket är omöjligt på samma sätt som i "det första fallet" ovan.

Fler fall finns inte, så **saken är klar.**