Matematik, KTH
B.Ek

Lösningar tentan (SF1630,) SF1631 DISKRET MATEMATIK, (F,) D, 28 januari 2012

Tryckfel kan förekomma.

1) G är en hamiltonsk graf och vi skall visa att om man tar bort $k > 0$ hörn från G, får man en graf med högst k komponenter.

Lösning:
Betrakta en viss hamiltoncykel i G. Då man tar bort $k(> 0)$ hörn, delas cykeln upp i högst k sammanhängande delar (om man tar bort k bitar av en cirkel, har man högst k bitar kvar). Hörnen i varje del av den uppdelade cykeln ligger i samma komponent av den beskurna grafen och varje komponent av denna innehåller minst ett hörn, så antalet komponenter är högst k. **Saken är klar.**

---

2) Vi söker alla $x \in \mathbb{Z}_{246}$ som uppfyller $117x = 36$.

Lösning:
Problemet motsvarar den diofantiska ekvationen $117x - 246k = 36$. Euklides algoritm ger $246 = 2 \cdot 117 + 12$, $117 = 9 \cdot 12 + 9$, $12 = 1 \cdot 9 + 3$, $9 = 3 \cdot 3$ så $\mathbf{sgd(117, 246) = 3}$ och $3 = 12 - 1 \cdot 9 = 12 - 1(117 - 9 \cdot 12) = -1 \cdot 117 + 10 \cdot 12 = -117 + 10(246 - 2 \cdot 117) = 10 \cdot 246 - 21 \cdot 117 = 10 \cdot 246 - 39 \cdot 246 + 82 \cdot 117 - 21 \cdot 117 = -29 \cdot 246 + 61 \cdot 117$ ($39 = \frac{117}{3}$, $82 = \frac{246}{3}$).
Multiplikation med 12 ger $-348 \cdot 246 + 117 \cdot 732 = 36$, så $\begin{cases} x_0 = 732 \\ k_0 = 348 \end{cases}$ är en lösning till den diofantiska ekvationen.
(x, k) uppfyller då ekvationen precis om $117(x - x_0) - 246(k - k_0) = 0$, dvs $39(x - x_0) = 82(k - k_0)$, så (entydig faktorisering) $x - x_0 = 82q$, godtyckligt $q \in \mathbb{Z}$. $0 \leq x < 246$ ger de tre värdena $x = 76, 158, 240$.

Svar: Alla lösningar i $\mathbb{Z}_{246}$ är $x = 76, 158, 240$.

---

3) Vi söker antalet sätt att fördela 30 (identiska) bullar och 15 (identiska) tårtbitar bland 20 (särskiljbara) barn, så att varje barn får minst en bulle och högst en tårtbit?

Lösning:
Bullarna kan fördelas på $\binom{19+10}{19} = \frac{29!}{19! \cdot 10!}$ sätt (först en bulle till varje barn, så väljs 19 väggar bland $19 + 10$ bullväggar).
Tårtbitarna kan fördelas på $\binom{20}{15} = \frac{20!}{15! \cdot 5!}$ sätt (välj vilka barn som får en).
Multiplikationsprincipen ger

Svar: De kan fördelas på $\frac{29! \cdot 20!}{19! \cdot 10! \cdot 15! \cdot 5!}$ (= 310545275040) sätt.

---

4) $f_{a,b} : \mathbb{Z}_3 \to \mathbb{Z}_3$ definieras av $f_{a,b}(x) = ax + b$. Vi skall visa att $\{f_{a,b}\ ;\ a, b \in \mathbb{Z}_3,\ a \neq 0\}$, med operationen sammansättning av funktioner, är en grupp och att den är isomorf med S_3, gruppen av permutationer av tre element.

Lösning:
De givna funktionerna verkar som permutationer av de tre elementen i $\mathbb{Z}_3$, enligt
$f_{1,0} : (0)$, $f_{1,1} : (0\ 1\ 2)$, $f_{1,2} : (0\ 2\ 1)$, $f_{2,0} : (1\ 2)$, $f_{2,1} : (0\ 1)$, $f_{2,2} : (0\ 2)$.
(T.ex. $f_{2,1}(0) = 2 \cdot 0 + 1 = 1$, $f_{2,1}(1) = 2 \cdot 1 + 1 = 0$, $f_{2,1}(2) = 2 \cdot 2 + 1 = 2$.)
Eftersom operationen i S_3 också är sammansättning av funktioner blir den givna mängden isomorf med S_3 och eftersom S_3 är en grupp, är den givna också det. **Saken är klar.**
(Gruppegenskaperna slutenhet, associativitet, identitet och invers kan också verifieras direkt.)

---

5) Vi skall visa att om p är ett primtal är $x^{p-1} - 1$ i $\mathbb{Z}_p[x]$ delbart med $x - a$ för alla $a \in \mathbb{Z}_p$, $a \neq 0$.

Lösning:
Enligt Fermats lilla sats är a ett nollställe till polynomet, så enligt faktorsatsen är $x^{p-1} - 1$ delbart med $x - a$ i $\mathbb{Z}_p[x]$.

---

6) Vi söker dels det minsta $e \geq 100$ så att $(1189, e)$ kan användas som krypteringsnyckel i ett RSA-system och dels ett d, så att $(1189, d)$ är en motsvarande dekrypteringsnyckel.

Lösning:
$n = 1189 = 29 \cdot 41$ ger $m = 28 \cdot 40 = 1120$. Villkoret på e är då $\text{sgd}(1120, e) = 1$, vilket inte är uppfyllt för $e = 100$, men väl för $\boldsymbol{e = 101}$ (primtal).
För att finna motsvarande d används Euklides algoritm: $1120 = 11 \cdot 101 + 9$; $101 = 11{\cdot}9{+}2$; $9 = 4{\cdot}2{+}1$ så $1 = 9{-}4{\cdot}2 = 9{-}4{\cdot}(101{-}11{\cdot}9) = -4{\cdot}101{+}45{\cdot}9 = -4{\cdot}101{+}45{\cdot}(1120{-}11{\cdot}101) = 45{\cdot}1120{-}499{\cdot}101 = 45{\cdot}1120{-}101{\cdot}1120{+}1120{\cdot}101{-}499{\cdot}101 = 621{\cdot}101{-}56{\cdot}1120$, så vi kan välja $\boldsymbol{d = 621}$.

Svar: $e = 101$, $d = 621$.

---

7) $\alpha \in S_9$: $\alpha(1)=3,\ \alpha(2)=7,\ \alpha(3)=1,\ \alpha(4)=9,\ \alpha(5)=8,\ \alpha(6)=5,\ \alpha(7)=4,\ \alpha(8)=6,\ \alpha(9)=2$. Vi söker a) α och α^{-1} på cykelform och b) ett $\sigma \in S_9$ så att $\sigma\alpha = \alpha^{-1}\sigma$.

Lösning:
$\alpha(1) = 3, \alpha(3) = 1$ ger en cykel $(1\,3)$, $\alpha(2) = 7, \alpha(7) = 4, \alpha(4) = 9, \alpha(9) = 2$ ger en cykel $(2\,7\,4\,9)$ och $\alpha(5){=}8, \alpha(8){=}6, \alpha(6){=}5$ ger en cykel $(5\,8\,6)$. Totalt $\alpha = (1\,3)(2\,7\,4\,9)(5\,8\,6)$ så $\alpha^{-1} = (3\,1)(9\,4\,7\,2)(6\,8\,5)$.
Att $\sigma\alpha = \alpha^{-1}\sigma$ är ekvivalent med $\sigma\alpha\sigma^{-1} = \alpha^{-1}$.
Men $\sigma\alpha\sigma^{-1} = (\sigma(1)\,\sigma(3))(\sigma(2)\,\sigma(7)\,\sigma(4)\,\sigma(9))(\sigma(5)\,\sigma(8)\,\sigma(6))$. Vi kan t.ex. välja $\sigma(1) = 3, \sigma(2) = 9, \sigma(3) = 1, \sigma(4) = 7, \sigma(5) = 6, \sigma(6) = 5, \sigma(7) = 4, \sigma(8) = 8, \sigma(9) = 2$, dvs i cykelform $\sigma = (1\,3)(2\,9)(4\,7)(5\,6)$.
Svar a: $\boldsymbol{\alpha = (1\,3)(2\,7\,4\,9)(5\,8\,6)}$, $\boldsymbol{\alpha^{-1} = (3\,1)(9\,4\,7\,2)(6\,8\,5)}$,
b: (t.ex.) $\boldsymbol{\sigma = (1\,3)(2\,9)(4\,7)(5\,6)}$.

---

8) Vi söker alla monadiska irreducibla polynom i $\mathbb{Z}_5[x]$ som är delare till både $p(x) = x^6 + 4x^5 + x^4 + x^3 + x^2 + 2x + 1$ och $q(x) = x^5 + 2x^4 + 3x^3 + x^2 + 4x + 3$.

Lösning:
De sökta polynomen är precis de (monadiska) irreducibla faktorerna i $\text{sgd}(p(x), q(x))$.
Division i $\mathbb{Z}_5[x]$ ger: $p(x) = (x+2) \cdot q(x) + r_1(x)$, $r_1(x) = 4x^4 + 4x^3 + x$,
$q(x) = (4x+4) \cdot r_1(x) + r_2(x)$, $r_2(x) = 2x^3 + 2x^2 + 3$,
$r_1(x) = 2x \cdot r_2(x) + 0$.
Så (monadiska) $\text{sgd}(p(x), q(x)) = 3 \cdot r_2(x) = x^3 + x^2 + 4 = d(x)$.
Vi söker irreducibla faktorer i $d(x)$. $d(0) = 4$, $d(1) = 1$, $d(2) = 1$, $d(3) = 0$, så en (irreducibel) faktor är $x - 3 = x + 2$. Division ger $d(x) = (x+2)(x^2+4x+2) = (x+2) \cdot e(x)$. $e(3) = 3$, $e(4) = 4$, så $e(x)$ saknar nollställen och är alltså irreducibelt (andragradspolynom utan nollställen är irreducibla).

Svar: De sökta faktorerna är $\boldsymbol{x + 2}$ och $\boldsymbol{x^2 + 4x + 2}$.

---

9) Kanterna i K_{17} har färgats med tre färger. Vi ska visa att det finns en enfärgad triangel.

Lösning:
Som i exemplet i Biggs 10.1, men "ett steg till".
Välj ett hörn, v_0 säg. Bland dess 16 kanter måste minst 6 ha samma färg, f_0 säg ("generaliserade postfacksprincipen", Biggs 10.1). Låt V' vara mängden av v_0:s "f_0-grannar". Om någon kant inom V' har färg f_0 ger den med två kanter till v_0 en enfärgad triangel. Annars, tag ett hörn v_1 i V', det har minst 5 grannar i V' och alla kanter till dessa har en av två färger. Det finns alltså minst tre kanter (inom V') från v_1 med samma färg, f_1 säg. Låt V'' vara mängden av v_1:s "f_1-grannar" i V'. Om någon kant inom V'' har färg f_1 ger den med två kanter till v_1 en enfärgad triangel, annars har alla kanter inom V'' samma färg, men $|V''| \geq 3$, så i alla fallen finns en enfärgad triangel. **Saken är klar.**

---

10) p är ett primtal. Vi skall visa a) att om $p \equiv 3 \pmod 4$ gäller för alla heltal m att $p \nmid m^2 + 1$ och b) att om $p \equiv 1 \pmod 4$ finns ett heltal n, så att $p \mid n^2 + 1$.

Lösning:

a) $p \nmid m^2 + 1$ innebär precis att $m^2 + 1 \neq 0$ i $\mathbb{Z}_p$. Det gäller alltså att visa att det inte finns m med $m^2 = -1$ i $\mathbb{Z}_p$ om p är ett primtal av form $4k + 3$.

I gruppen $(\mathbb{Z}_p \setminus \{0\}, \times)$ skulle ett sådant m ha ordning 4 (ty $m^4 = 1$, men $m^2 \neq 1$), men $4 \nmid p - 1 = 4k + 2$, gruppens ordning. Ett sådant m finns alltså inte.

b) Nu är p ett primtal av form $4k + 1$ och det gäller att visa att det finns ett n så att $n^2 = -1$ i $\mathbb{Z}_p$.

Eftersom $\mathbb{Z}_p$ är en ändlig kropp är $(\mathbb{Z}_p \setminus \{0\}, \times)$ en cyklisk grupp av ordning $p - 1 = 4k$. Låt g vara en generator för denna grupp och betrakta $n = g^k$. $n^4 = g^{4k} = 1$, men $n^2 = g^{2k} \neq 1$, eftersom g har ordning $4k$. Då är $n^2 = -1$, ty i en kropp har ekvationen $y^2 = 1$ bara lösningarna $y = 1$ och $y = -1$ (ty $y^2 - 1 = (y - 1)(y + 1)$ och i en kropp kan en produkt bara vara 0 om en faktor är det) och $y = n^2 \neq 1$ är en lösning.

Sakerna är klara.