Matematik, KTH **SF1679 Diskret matematik**
B.Ek **hösten 2017**

Svar och anvisningar för hemuppgifter omgång 1, (till må 4 december)

1. $(0,3\text{p})$ $x, y \in \mathbb{Z}_+$, $\text{sgd}(x,y) = 1$ och $z \in \mathbb{Z}$, $|z| < xy$. Vi skall visa att det finns $u, v \in \mathbb{Z}$, $|u| < x$, $|v| < y$, med $\frac{z}{xy} = \frac{u}{x} + \frac{v}{y}$ och finna sådana u, v för $x = 711$, $y = 925$, $z = 76\,353$.

Lösning: Eftersom $\text{sgd}(x,y) = 1$ är $1 = ax + by$ för några $a, b \in \mathbb{Z}$ (hittas med Euklides algoritm). Låt $bz = xq + u$, där $q \in \mathbb{Z}$ och $\boldsymbol{|u| < x}$, $uz \geq 0$ (u minsta icke-negativa resten eller den $-x$) ger att $z = azx + (xq + u)y = uy + (az + qy)x$. Med $v = az + qy$ fås $|v|x = |vx| = |z - uy| \leq$ $\leq \max(|z|, |u|y) < xy$ (z, $uy \geq 0$ eller båda ≤ 0), så $\boldsymbol{|v| < y}$. $z = uy + vx$ ger $\boldsymbol{\frac{z}{xy} = \frac{u}{x} + \frac{v}{y}}$.
Då $x = 711$, $y = 925$, $z = 76\,353$ ger först Euklides algoritm:

$$\begin{aligned} 925 &= 711 \cdot 1 + 214 \\ 711 &= 214 \cdot 3 + 69 \\ 214 &= 69 \cdot 3 + 7 \\ 69 &= 7 \cdot 9 + 6 \\ 7 &= 6 \cdot 1 + 1 \end{aligned} \qquad \text{så (sgd}(711, 925) = 1 \text{ och)} \qquad \begin{aligned} 1 &= 7 - (69 - 9 \cdot 7) = \\ &= -69 + 10(214 - 3 \cdot 69) = \\ &= 10 \cdot 214 - 31(711 - 3 \cdot 214) = \\ &= -31 \cdot 711 + 103 \cdot (925 - 711) = \\ &= 103 \cdot 925 - 134 \cdot 711 \end{aligned}$$

och $76\,353 = -(134 \cdot 76\,353) \cdot 711 + (103 \cdot 76\,353) \cdot 925$, $bz = 103 \cdot 76\,353 = 7\,864\,359 =$ $= 711 \cdot 11\,060 + 699$, så $76\,353 = 699 \cdot 925 - (134 \cdot 76\,353 - 11\,060 \cdot 925) \cdot 711 = 699 \cdot 925 - 802 \cdot 711$ och alltså $\frac{76\,353}{711 \cdot 925} = \frac{699}{711} - \frac{802}{925}$. (Jfr partialbråksuppdelning av rationella funktioner.)
Svar: En lösning är $\boldsymbol{u = 699}$, $\boldsymbol{v = -802}$ ($\boldsymbol{u = -12}$, $\boldsymbol{v = 123}$ är en annan).

---

2. $(0,3\text{p})$ Vi söker alla $m, n \in \mathbb{N}$ som uppfyller $4953^m \cdot n \equiv 13\,383 \pmod{14\,553}$.

Lösning: För $m = 0$ är alla lösningar i $\mathbb{N}$ tydligen $n = 13\,383 + 14\,553k$, $k \in \mathbb{N}$, annars:
Vi använder kinesiska restsatsen. $14\,553 = 3^3 \cdot 7^2 \cdot 11 = 27 \cdot 49 \cdot 11$, så

$$a \equiv_{14\,553} b \Leftrightarrow (a \equiv_{27} b,\ a \equiv_{49} b \text{ och } a \equiv_{11} b)$$

$4953^m \cdot n \equiv_{27} 13\,383 \Leftrightarrow 12^m \cdot n \equiv_{27} 18$, lösningar $m = 1:\ 4n \equiv_9 6 \Leftrightarrow n \equiv_9 -2 \cdot 6 \equiv_9 6$
$m = 2:\ 4^2 n \equiv_3 2 \Leftrightarrow n \equiv_3 2$
$m \geq 3:\ 0 \cdot n \equiv_3 2$, inga lösningar,
$4953^m \cdot n \equiv_{49} 13\,383 \Leftrightarrow 4^m \cdot n \equiv_{49} 6$, lösningar $m = 1:\ 4n \equiv_{49} 6 \Leftrightarrow n \equiv_{49} -12 \cdot 6 \equiv_{49} 26$
$m = 2:\ 4^2 n \equiv_{49} 6 \Leftrightarrow n \equiv_{49} -18 \equiv_{49} 31$,
$4953^m \cdot n \equiv_{11} 13\,383 \Leftrightarrow 3^m \cdot n \equiv_{11} 7$, lösningar $m = 1:\ 3n \equiv_{11} 7 \Leftrightarrow n \equiv_{11} 4 \cdot 7 \equiv_{11} 6$
$m = 2:\ 3^2 n \equiv_{11} 7 \Leftrightarrow n \equiv_{11} 5 \cdot 7 \equiv_{11} 2$.
Med $y_9 = 49 \cdot 11 b_1 \equiv_9 1$, så $b_1 \equiv_9 -1$ och vi kan ta $y_9 = -49 \cdot 11 = -539$,
$y_{49} = 9 \cdot 11 b_2 \equiv_{49} 1$, så $b_2 \equiv_{49} 1$ och vi kan ta $y_{49} = 9 \cdot 11 = 99$,
$y_{11} = 9 \cdot 49 b_3 \equiv_{11} 1$, så $b_3 \equiv_{11} 1$ och vi kan ta $y_{49} = 9 \cdot 49 = 441$.
Vi finner lösningarna $m = 1:\ n \equiv_{4851} -539 \cdot 6 + 99 \cdot 26 + 441 \cdot 6 = 1986$ ($4851 = 9 \cdot 49 \cdot 11$),
$m = 2:\ n \equiv_{1617} -539 \cdot 2 + 99 \cdot 31 + 441 \cdot 2 = 2873$ ($1617 = 3 \cdot 49 \cdot 11$).
(y_9 kan användas som "y_3", ty $y_9 \equiv_9 1 \Rightarrow y = 9 \equiv_3 1$.)

Svar: Alla lösningar ges av: $\boldsymbol{m = 0}$, $\boldsymbol{n = 13\,383 + 14\,553k}$, $\boldsymbol{k \in \mathbb{N}}$;
$\boldsymbol{m = 1}$, $\boldsymbol{n = 1986 + 4851k}$, $\boldsymbol{k \in \mathbb{N}}$; $\boldsymbol{m = 2}$, $\boldsymbol{n = 1256 + 1617k}$, $\boldsymbol{k \in \mathbb{N}}$.

---

3. $\mathcal{R}$, $\mathcal{S}$ är binära relationer på mängderna X respektive Y. Vi definierar $\mathcal{T}$ på $X \times Y$ enligt $(x_1, y_1)\mathcal{T}(x_2, y_2) \Leftrightarrow \begin{cases} 1.\ x_1\mathcal{R}x_2 \text{ eller} \\ 2.\ x_1 = x_2 \text{ och } y_1\mathcal{S}y_2 \end{cases}$ och den binära relationen $\mathcal{Q}$ på X^n ($n \in \mathbb{N}$ udda, ≥ 3) enligt majoritetsbeslut.
Vi skall avgöra vilka av **reflexivitet, symmetri, antisymmetri, transitivitet och välgrundning** som ärvs av (a, 0,3p) $\mathcal{T}$ från $\mathcal{R}$ och $\mathcal{S}$ respektive av (b, 0,3p) $\mathcal{Q}$ från $\mathcal{R}$.

Lösning:

- Om $\mathcal{R}$, $\mathcal{S}$ är reflexiva, är $\mathcal{T}$ och $\mathcal{Q}$ också det:
  $(x, y)\mathcal{T}(x, y)$ för alla $(x, y) \in X \times Y$, ty $x\mathcal{R}x$ för alla $x \in X$,
  $(u_1, \ldots, u_n)\mathcal{Q}(u_1, \ldots, u_n)$, för alla $(u_1, \ldots, u_n) \in X^n$, ty $\{i \in \mathbb{N}_n \mid u_i\mathcal{R}u_i\} = \mathbb{N}_n$,
- om $\mathcal{R}$, $\mathcal{S}$ är symmetriska, är $\mathcal{T}$ och $\mathcal{Q}$ också det:
  om $(x_1, y_1)\mathcal{T}(x_2, y_2)$: $x_1\mathcal{R}x_2 \Rightarrow x_2\mathcal{R}x_1 \Rightarrow (x_2, y_2)\mathcal{T}(x_1, y_1)$ eller
  $x_1 = x_2,\ y_1\mathcal{S}y_2 \Rightarrow x_2 = x_1,\ y_2\mathcal{S}y_1 \Rightarrow (x_2, y_2)\mathcal{T}(x_1, y_1)$,
  $(u_1, \ldots, u_n)\mathcal{Q}(v_1, \ldots, v_n) \Rightarrow |\{i \in \mathbb{N}_n \mid u_i\mathcal{R}v_i\}| > \frac{n}{2} \Rightarrow |\{i \in \mathbb{N}_n \mid v_i\mathcal{R}u_i\}| > \frac{n}{2} \Rightarrow$
  $\Rightarrow (v_1, \ldots, v_n)\mathcal{Q}(u_1, \ldots, u_n)$,
- även om $\mathcal{R}$, $\mathcal{S}$ är antisymmetriska, behöver varken $\mathcal{T}$ eller $\mathcal{Q}$ vara det:
  om X, Y är $\mathbb{N}$ och $\mathcal{R}$, $\mathcal{S}$ är $=$, är $(0, 0)\mathcal{T}(0, 1)$ och $(0, 1)\mathcal{T}(0, 0)$, men $(0, 0) \neq (0, 1)$
  och $(0, 0, 0)\mathcal{Q}(0, 0, 1)$ och $(0, 0, 1)\mathcal{Q}(0, 0, 0)$, men $(0, 0, 0) \neq (0, 0, 1)$,
- om $\mathcal{R}$, $\mathcal{S}$ är transitiva, är $\mathcal{T}$ också det, men inte säkert $\mathcal{Q}$:
  om $(x_1, y_1)\mathcal{T}(x_2, y_2)$ och $(x_2, y_2)\mathcal{T}(x_3, y_3)$, så $(x_1, y_1)\mathcal{T}(x_3, y_3)$, ty
  $(x_1\mathcal{R}x_2,\ x_2\mathcal{R}x_3) \Rightarrow x_1\mathcal{R}x_3 \Rightarrow (x_1, y_1)\mathcal{T}(x_3, y_3)$,
  $(x_1\mathcal{R}x_2,\ x_2 = x_3,\ y_2\mathcal{S}y_3) \Rightarrow x_1\mathcal{R}x_3 \Rightarrow (x_1, y_1)\mathcal{T}(x_3, y_3)$,
  $(x_1 = x_2,\ y_1\mathcal{S}y_2,\ x_2\mathcal{R}x_3) \Rightarrow x_1\mathcal{R}x_3 \Rightarrow (x_1, y_1)\mathcal{T}(x_3, y_3)$,
  $(x_1 = x_2,\ y_1\mathcal{S}y_2,\ x_2 = x_3,\ y_2\mathcal{S}y_3) \Rightarrow (x_1 = x_3,\ y_1\mathcal{S}y_3) \Rightarrow (x_1, y_1)\mathcal{T}(x_3, y_3)$,
  om X är $\mathbb{N}$ och $\mathcal{R}$ är $=$, är
  $(0, 0, 0)\mathcal{Q}(0, 0, 1)$ och $(0, 0, 1)\mathcal{Q}(0, 1, 1)$, men $(0, 0, 0)\not\mathcal{Q}(0, 1, 1)$,
- om $\mathcal{R}$, $\mathcal{S}$ är välgrundade, är $\mathcal{T}$ också det, men inte säkert $\mathcal{Q}$:
  om $\varnothing \neq A \subseteq X \times Y$, tag x_0 $\mathcal{R}$-minimalt i $A_X = \{x \in X \mid (x, y) \in A,\ \text{ngt } y \in Y\}$ $(\neq \varnothing)$
  och y_0 $\mathcal{S}$-minimalt i $A_0 = \{y \in Y \mid (x_0, y) \in A\}$ $(\neq \varnothing)$,
  då är (x_0, y_0) $\mathcal{T}$-minimalt i A, ty $(x, y)\mathcal{T}(x_0, y_0)$ med $(x, y) \in A$ kräver
  $x\mathcal{R}x_0$, $x \in A_X$ (omöjligt) eller $x = x_0$ (så $y \in A_0$) och $y\mathcal{S}y_0$ (omöjligt),
  om X är $\mathbb{N}$ och $\mathcal{R}$ är $<$, saknar $\{(0, 1, 2), (1, 2, 0), (2, 0, 1)\}$ $\mathcal{Q}$-minimalt element, ty
  $(0, 1, 2)\mathcal{Q}(1, 2, 0)$, $(1, 2, 0)\mathcal{Q}(2, 0, 1)$, $(2, 0, 1)\mathcal{Q}(0, 1, 2)$.

Svar a: $\mathcal{T}$ ärver reflexivitet, symmetri, transitivitet och välgrundning, men inte antisymmetri från $\mathcal{R}$ och $\mathcal{S}$,
b: $\mathcal{Q}$ ärver reflexivitet och symmetri, men inte övriga egenskaper från $\mathcal{R}$.

---

4. $(0, 3\text{p})$ Mängderna X, Y, Z har $|X| = k \leq |Y| = m \leq |Z| = n$. Vi söker antalet par (f, g), där $f\colon X \to Y$, $g\colon Y \to Z$, sådana att $gf\colon X \to Z$ är en injektion.

Lösning: f måste vara en injektion (om $f(x_1) = f(x_2)$ är $(gf)(x_1) = g(f(x_1)) = g(f(x_2)) = (gf)(x_2)$), så den kan väljas på $(m)_k = \frac{m!}{(m-k)!}$ sätt. g:s restriktion till $f[X] = \{f(x) \mid x \in X\}$ måste också vara en injektion ($g(f(x_1)) = g(f(x_2))$ skulle ge $(gf)(x_1) = (gf)(x_2)$). $|f[X]| = |X| = k$, så g på $f[X]$ kan väljas på $(n)_k = \frac{n!}{(n-k)!}$ sätt och g:s övriga värden sedan på n^{m-k} sätt.
Det totala antalet par (f, g) blir (multiplikationsprincipen) $\frac{m!}{(m-k)!} \cdot \frac{n!}{(n-k)!} \cdot n^{m-k}$.

Svar: Det sökta antalet är $\frac{m! \cdot n! \cdot n^{m-k}}{(m-k)! \cdot (n-k)!}$.

---

5. $\pi, \sigma \in S_{11}$ ges av

i	1	2	3	4	5	6	7	8	9	10	11
$\pi(i)$	9	11	2	3	10	1	4	5	6	8	7
$\sigma(i)$	11	10	1	3	9	5	4	2	6	8	7

. Vi söker (a, $0{,}2$p) antalet $\tau \in S_{11}$ med $\tau\pi = \sigma\tau$ och ett sådant τ och (b, $0{,}3$p) alla $\tau \in S_{11}$ med $\tau\pi = \sigma\tau^{-1}$.

Lösning: På cykelform: $\pi = (1\ 9\ 6)(2\ 11\ 7\ 4\ 3)(5\ 10\ 8)$, $\sigma = (1\ 11\ 7\ 4\ 3)(2\ 10\ 8)(5\ 9\ 6)$.
a. $\tau\pi = \sigma\tau \Leftrightarrow \sigma = \tau\pi\tau^{-1} = \big(\tau(1)\ \tau(9)\ \tau(6)\big)\big(\tau(2)\ \tau(11)\ \tau(7)\ \tau(4)\ \tau(3)\big)\big(\tau(5)\ \tau(10)\ \tau(8)\big)$.
$\tau(1)$ kan väljas på **6 sätt** (de i σ:s 3-cykler), valet bestämmer $\tau(9)$, $\tau(6)$,
$\tau(2)$ kan väljas på **5 sätt** (de i σ:s 5-cykel), valet bestämmer $\tau(11)$, $\tau(7)$, $\tau(4)$, $\tau(3)$,
$\tau(5)$ kan väljas på **3 sätt** (de i σ:s andra 3-cykel), valet bestämmer $\tau(10)$, $\tau(8)$.
Totalt finns det alltså $6 \cdot 5 \cdot 3 = 90$ olika möjliga τ (multiplikationsprincipen). De ”första” valen ger exemplet $\tau = (1\ 2)(3)(4)(5)(6\ 8)(7)(9\ 10)(11) = (1\ 2)(6\ 8)(9\ 10)$ ($\tau = \tau^{-1}$, så en lösning i b).
b. $\tau\pi = \sigma\tau^{-1} \Leftrightarrow \tau\pi\tau = \sigma \Leftrightarrow (\tau\pi)^2 = \sigma\pi = (1\ 6\ 11\ 4)(2\ 7\ 3\ 10)(5\ 8\ 9)$.
En k-cykel kvadrerad är en k-cykel (om k är udda) eller två $\frac{k}{2}$-cykler (k jämnt). $\tau\pi$ måste bestå av en 8-cykel (4 möjliga, 4-cyklerna ”tråcklas ihop”) och en 3-cykel (entydigt bestämd), $\tau\pi = (1\ 2\ 6\ 7\ 11\ 3\ 4\ 10)(5\ 9\ 8)$, $(1\ 10\ 6\ 2\ 11\ 7\ 4\ 3)(5\ 9\ 8)$, $(1\ 3\ 6\ 10\ 11\ 2\ 4\ 7)(5\ 9\ 8)$, $(1\ 7\ 6\ 3\ 11\ 10\ 4\ 2)(5\ 9\ 8)$, vilka ger $\tau = (\tau\pi)\pi^{-1} = (1\ 7\ 3\ 10\ 9\ 2\ 4\ 11\ 6\ 8)(5)$, $(1\ 2)(3)(4)(5)(6\ 8)(7)(9\ 10)(11)$, $(1\ 10\ 9\ 3\ 7\ 2\ 6\ 8\ 11\ 4)(5)$, $(1\ 3\ 2\ 11)(4\ 6\ 8)(5)(7\ 10\ 9)$.

Svar a: Det finns 90 sådana τ, däribland (1 2)(6 8)(9 10),
b: Det finns 4 sådana τ, nämligen (1 7 3 10 9 2 4 11 6 8), (1 2)(6 8)(9 10), (1 10 9 3 7 2 6 8 11 4) och (1 3 2 11)(4 6 8)(7 10 9).
