

Svarsförslag för lappskrivning 2A, fredag 4 oktober 2013
i SF1630(/5B1203) Diskret matematik, för D (m.fl.)

(Tryckfel kan förekomma.)

a-versionen (b-versionen på andra sidan):

a1a. (1p) Vi skall ange när en funktion $f : X \rightarrow Y$ är en **injektion**.

Lösning: f är en injektion omm det för varje $y \in Y$ finns högst ett $x \in X$ med $y = f(x)$.

(Flera alternativ möjliga, t.ex. ” f är en injektion omm för alla $x_1, x_2 \in X$ gäller $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ ”.)

a1b. (1p) Sökt är ett nödvändigt och tillräckligt villkor på heltalen a, b och c för att det skall finnas $x, y \in \mathbb{Z}$ sådana att $ax + by = c$.

Lösning: Det sökta villkoret är att $\text{sgd}(a, b) \mid c$, dvs den största gemensamma delaren till koefficienterna är en delare till högerledet.

a1c. (1p) Vi skall formulera **kinesiska restsatsen**.

Lösning: Om de positiva heltalen $m_1, m_2, \dots, m_k$ är parvis relativt prima (dvs

$\text{sgd}(m_i, m_j) = 1$ om $i \neq j$) har systemet av kongruenser
$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$
 en lösning x som är entydig $\pmod{m}$, där $m = m_1 m_2 \dots m_k$.

a1d. (1p) Vi skall formulera **postfacksprincipen**.

Lösning: ”Om $m < n$ finns ingen injektion från $\mathbb{N}_n$ till $\mathbb{N}_m$ ”,
”Om n brev läggs i m postfack och $m < n$ måste minst ett fack få minst två brev” eller liknande.

a2. (4p) Vi söker 80^{-1} i $\mathbb{Z}_{407}$.

Lösning: Vi använder Euklides algoritm och finner

$$\begin{cases} 407 = 5 \cdot 80 + 7, \\ 80 = 11 \cdot 7 + 3, \text{ och därur att} \\ 7 = 2 \cdot 3 + 1, \end{cases} \quad \begin{cases} 1 = 7 - 2 \cdot 3 = 7 - 2(80 - 11 \cdot 7) = \\ = -2 \cdot 80 + 23 \cdot 7 = \\ = -2 \cdot 80 + 23(407 - 5 \cdot 80) = \\ = 23 \cdot 407 - 117 \cdot 80, \end{cases}$$

så $80^{-1} = -117 = 290$ i $\mathbb{Z}_{407}$.

Svar: $80^{-1} = 290$ i $\mathbb{Z}_{407}$.

b-versionen:

b1a. (1p) Vi skall ange när en funktion $f : X \rightarrow Y$ är en **surjektion**.

Lösning: f är en surjektion omm det för varje $y \in Y$ finns minst ett $x \in X$ med $y = f(x)$.

b1b. Vi skall dels ($\frac{1}{2}$ p) ange vad det betyder att x är **inverterbart** i $\mathbb{Z}_m$ och dels ($\frac{1}{2}$ p) ange ett nödvändigt och tillräckligt villkor på m och x för att x skall vara inverterbart i $\mathbb{Z}_m$.

Lösning: $x \in \mathbb{Z}_m$ är inverterbart omm det finns ett $y \in \mathbb{Z}_m$ sådant att $xy = 1$ i $\mathbb{Z}_m$. x är inverterbart i $\mathbb{Z}_m$ omm $\text{sgd}(x, m) = 1$.

b1c. (1p) Vi skall formulera Fermats lilla sats.

Lösning: Om p är ett primtal och $p \nmid x$ (dvs x inte är en multipel av p) gäller $x^{p-1} \equiv 1 \pmod{p}$. (Formulering i $\mathbb{Z}_p$ går också bra.)

b1d. (1p) Vi skall ange vad det betyder att en oändlig mängd är **uppräknelig**.

Lösning: Den oändliga mängden X är uppräknelig omm det finns en bijektion $f : \mathbb{N} \rightarrow X$ från de naturliga talen till X (dvs om det finns en oändlig följd som innehåller varje element i X precis en gång).

b2. (4p) Vi söker heltal x och y sådana att $320x + 102y = 6$.

Lösning: Vi använder Euklides algoritm och finner

$$\begin{cases} 320 = 3 \cdot 102 + 14, \\ 102 = 7 \cdot 14 + 4, \\ 14 = 3 \cdot 4 + 2, \end{cases} \quad \text{och därur att} \quad \begin{cases} 2 = 14 - 3 \cdot 4 = 14 - 3(102 - 7 \cdot 14) = \\ = -3 \cdot 102 + 22 \cdot 14 = \\ = -3 \cdot 102 + 22(320 - 3 \cdot 102) = \\ = 22 \cdot 320 - 69 \cdot 102, \end{cases}$$

Multiplikation med 3 ger att $x = 22 \cdot 3 = 66$, $y = -69 \cdot 3 = -207$ löser ekvationen. (En annan lösning är $x = 15$, $y = -47$.)

Svar: En lösning är $x = 66$, $y = -207$.
