

Svarsförslag för lappskrivning 2A, onsdag 28 september 2016
i SF1630 Diskret matematik, för D (m.fl.)

(Tryckfel kan förekomma.)

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

a1a. (1p) Sökt är definitionen av att en oändlig mängd X är **uppräknelig**.

Lösning: X är uppräknelig om det finns en bijektion $f : \mathbb{N} \rightarrow X$ (där $\mathbb{N}$ är mängden av de naturliga talen).

a1b. (1p) Vi söker den minsta icke-negativa resten då 76^{200} divideras med 67.

Lösning: Det gäller att finna $x \in \{0, 1, \dots, 66\}$ med $x \equiv_{67} 76^{200}$.
Eftersom 67 är primtal och $67 \nmid 76$ ger Fermats lilla sats att $76^{66} \equiv_{67} 1$, så
 $76^{200} = (76^{66})^3 \cdot 76^2 \equiv_{67} 1^3 \cdot 9^2 = 81 \equiv_{67} 14$ och alltså $x = 14$.

Svar: Den sökta resten är 14.

a1c. (1p) Vi söker alla $x \in \mathbb{Z}$ som uppfyller $x \equiv_{13} 3$, $x \equiv_{14} 3$ och $x \equiv_{15} 3$.

Lösning: En möjlighet är $x = 3$ och eftersom 13, 14 och 15 är parvis relativt prima ger kinesiska restsatsen att alla lösningar är $x = 3 + n \cdot 13 \cdot 14 \cdot 15 = 3 + n \cdot 2730$ för $n \in \mathbb{Z}$.

Svar: Alla sådana x ges av $3 + n \cdot 2730$, för godtyckligt $n \in \mathbb{Z}$.

a1d. (1p) Sökt är definitionen av att en funktion $f : X \rightarrow Y$ är en surjektion.

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

a2. (4p) Vi skall avgöra om 183^{-1} existerar i $\mathbb{Z}_{391}$, och i så fall finna den.

Lösning: Euklides algoritm: $391 = 183 \cdot 2 + 25$, $183 = 25 \cdot 7 + 8$, $25 = 8 \cdot 3 + 1$.
Således är $\text{sgd}(183, 391) = 1$ och $183 \in \mathbb{Z}_{391}$ är inverterbart.
Vi finner $1 = 25 - 3(183 - 7 \cdot 25) = -3 \cdot 183 + 22(391 - 2 \cdot 183) = 22 \cdot 391 - 47 \cdot 183$.
Det ger att $183^{-1} = -47 = 344$ i $\mathbb{Z}_{391}$.

Svar: $183 \in \mathbb{Z}_{391}$ är inverterbart och $183^{-1} = 344$.

b-versionen:

b1a. (1p) Sökt är definitionen av att en oändlig mängd X är **uppräknelig**.

Lösning: X är uppräknelig omm det finns en bijektion $f : \mathbb{N} \rightarrow X$ (där $\mathbb{N}$ är mängden av de naturliga talen).

b1b. (1p) Vi söker alla $x \in \mathbb{Z}$ som uppfyller $x \equiv_{13} 7$, $x \equiv_{15} 7$ och $x \equiv_{17} 7$.

Lösning: En möjlighet är $x = 7$ och eftersom 13, 15 och 17 är parvis relativt prima ger kinesiska restsatsen att alla lösningar är $x = 7 + n \cdot 13 \cdot 15 \cdot 17 = 7 + n \cdot 3315$ för $n \in \mathbb{Z}$.

Svar: Alla sådana x ges av $7 + n \cdot 3315$, för godtyckligt $n \in \mathbb{Z}$.

b1c. (1p) Vi söker den minsta icke-negativa resten då 61^{158} divideras med 53.

Lösning: Det gäller att finna $x \in \{0, 1, \dots, 52\}$ med $x \equiv_{53} 61^{158}$. Eftersom 53 är primtal och $53 \nmid 61$ ger Fermats lilla sats att $61^{52} \equiv_{53} 1$, så $61^{158} = (61^{52})^3 \cdot 61^2 \equiv_{53} 1^3 \cdot 8^2 = 64 \equiv_{53} 11$ och alltså $x = 11$.

Svar: Den sökta resten är 11.

b1d. (1p) Sökt är definitionen av att en funktion $f : X \rightarrow Y$ är en injektion.

Lösning: f är en injektion omm det för varje $y \in Y$ finns högst ett $x \in X$ sådant att $y = f(x)$. (Alt. omm $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ för alla $x_1, x_2 \in X$.)

b2. (4p) Vi skall avgöra om 137^{-1} existerar i $\mathbb{Z}_{436}$, och i så fall finna den.

Lösning: Euklides algoritm: $436 = 137 \cdot 3 + 25$, $137 = 25 \cdot 5 + 12$, $25 = 12 \cdot 2 + 1$. Således är $\text{sgd}(137, 436) = 1$ och $137 \in \mathbb{Z}_{436}$ är inverterbart. Vi finner $1 = 25 - 2(137 - 5 \cdot 25) = -2 \cdot 137 + 11(436 - 3 \cdot 137) = 11 \cdot 436 - 35 \cdot 137$. Det ger att $137^{-1} = -35 = 401$ i $\mathbb{Z}_{436}$.

Svar: $137 \in \mathbb{Z}_{436}$ är inverterbart och $137^{-1} = 401$.
