

**Svar och lösningsförslag till ks4, 14 maj 2012,
i SF1662 Diskret matematik för CL1**

1) (För varje delfråga ger rätt svar $\frac{1}{2}$ p, inget svar 0p, fel svar $-\frac{1}{2}$ p.
Totalpoängen på uppgiften rundas av uppåt till närmaste icke-negativa heltal.)

	sant	falskt
a) Om $(G, *)$ är en grupp finns säkert för varje $g \in G$ (minst) ett $h \in G$ så att $h * h = g$. [Inte alls. I $(\mathbb{Z}_2, +)$ är t.ex. $0 + 0 = 1 + 1 \neq 1$.]		×
b) Alla grupper av ordning 23 är isomorfa . [Ja, eftersom 23 är ett primtal är de alla cykliska, så isomorfa.]	×	
c) Varje ring är också en kropp. [Nej, $\mathbb{Z}$ är en ring, men ingen kropp. Varje kropp är en ring.]		×
d) Om gruppen G verkar på mängden X (båda ändliga) är antalet banor $\frac{1}{ G } \sum_{x \in X} G_x $ (där $G_x = \{g \in G \mid gx = x\}$). [Ja. Början av härledningen av Burnside's lemma, $\frac{ G_x }{ G } = \frac{1}{ G_x }$.]	×	
e) $13^{242} \equiv 26 \pmod{143}$ [$143 = 11 \cdot 13$]. [Ja, $120 = 10 \cdot 12$, $241 \equiv_{120} 1$, så $13^{241} \equiv_{143} 13$ och $13 \cdot 13 = 169 \equiv_{143} 26$.]	×	
f) Ett carmichaeltal är ett primtal som för minst en bas inte klarar fermattestet. [Inte alls. Carmichaeltal är inte primtal.]		×

2a) (1p) Gruppen $(G, *)$ med $G = \{a, b, c, d, e, f, g\}$, $|G| = 7$ uppfyller $a * a = b$ och $b * b = c$. Vi söker $c * c$.

Lösning:

Eftersom $|G| = 7$, ett primtal, är G cyklisk och genereras av a (inte identitetsselementet, ty $a * a \neq a$). $b = a^2$, $c = b^2 = a^4$ ger $c * c = a^8 = a$ (ty $o(a) = |G| = 7$).

Svar: $c * c = a$.

b) (1p) H är en delgrupp till G . Vi söker stabilisatorn för H under G 's verkan $g(hH) = (gh)H$ på $X = \{gH \mid g \in G\}$, mängden av H 's vänstersidoklasser.

Lösning:

Stabilisatorn är $G_H = \{g \in G \mid gH = H\}$, så om $g \in G_H$ gäller $g \in H$ (ty $1 \in H$). Om $g \in H$ är $gH = H$ (ty H är en grupp), så $g \in G_H$.

Svar: Stabilisatorn är H .

c) (1p) Vi skall formulera **Fermats lilla sats**.

Lösning:

Om p är ett primtal och a ett heltal så att $p \nmid a$, gäller $a^{p-1} \equiv 1 \pmod{p}$.

Eller: Om p är ett primtal och $a \in \mathbb{Z}_p \setminus \{0\}$ är $a^{p-1} = 1$.

($a^p \equiv a \pmod{p}$ för alla $a \in \mathbb{Z}$ resp. $a^p = a$ för alla $a \in \mathbb{Z}_p$ godkänns också.)

3) G är $U(\mathbb{Z}_{24})$, de inverterbara elementen i $\mathbb{Z}_{24}$. Vi skall (a, 1p) finna alla element i G och (b, 2p) avgöra om gruppen $(G, \cdot)$ är **cyklisk**.

Lösning:

$$U(\mathbb{Z}_{24}) = \{r \in \mathbb{Z}_{24} \mid \text{sgd}(r, 24) = 1\} = \{1, 5, 7, 11, 13, 17, 19, 23\}.$$

Eftersom $5^2 = 25 \equiv_{24} 1$, $7^2 = 49 \equiv_{24} 1$, $11^2 = 121 \equiv_{24} 1$, $13^2 \equiv_{24} (-11)^2 \equiv_{24} 1$, $17^2 \equiv_{24} (-7)^2 \equiv_{24} 1$, $19^2 \equiv_{24} (-5)^2 \equiv_{24} 1$, $23^2 \equiv_{24} (-1)^2 = 1$, har alla element ordning 1 (identitets-elementet) eller 2 (alla andra element) och G är inte cyklisk. (Det räcker att visa att två olika element har ordning 2. I en cyklisk grupp $\langle g \rangle$ av ordning 8 har bara ett (g^4) det.)

Svar a: $G = \{1, 5, 7, 11, 13, 17, 19, 23\}$, b: G är inte cyklisk.

4) $\phi: \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ ges av $\phi(x) = -x$. Vi skall visa att ϕ är en **isomorfi** mellan $(\mathbb{Z}_m, +)$ och $(\mathbb{Z}_m, +)$ själv (dvs en automorfi).

Lösning:

ϕ är en isomorfi omm den är en bijektion som bevarar gruppstrukturen.

ϕ är en bijektion, ty $\phi(\phi(x)) = x$ för alla $x \in \mathbb{Z}_m$ (dvs $\phi^{-1}(= \phi)$ existerar).

Strukturen (dvs operationen $+$) bevaras, ty $\phi(x) + \phi(y) = -x + (-y) = -(x + y) = \phi(x + y)$.

Saken är klar.

5) Fred och George har varsitt (pytte-)RSA-system. Fred har $d = 33$ och George har $d = 35$.

Vi skall avgöra dels vem av dem som har $n = 119$ och vem som har $n = 145$ och dels vem som har $e = 11$ och vem som har $e = 17$.

Lösning:

$n = 119 = 7 \cdot 17$ ger $m = 6 \cdot 16 = 96 = 2^5 \cdot 3$, medan $n = 145 = 5 \cdot 29$ ger $m = 4 \cdot 28 = 112 = 2^4 \cdot 7$. Eftersom $\text{sgd}(m, d) = 1$ måste Fred ha $n = 145$ och George ha $n = 119$. Vidare skall $e \cdot d \equiv_m 1$. $11 \cdot 33 = 363 = 3 \cdot 96 + 75 = 3 \cdot 112 + 27$, så $e = 11$ hör inte ihop med $d = 33$. Således har Fred $e = 17$ och George $e = 11$.

(Kontroll: $11 \cdot 35 = 385 = 4 \cdot 96 + 1 (= 3 \cdot 112 + 49)$ och $17 \cdot 33 = 561 = 5 \cdot 112 + 1 (= 5 \cdot 96 + 81)$.)

Svar: Fred har $(n, e) = (145, 17)$ och George har $(n, e) = (119, 11)$.
