Matematik, KTH **SF1662, Diskret matematik för CL1, vt 2012**

Svar och lösningsförslag till övningsks 4.

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 grupperna G_1 och G_2 är isomorfa så är de lika stora. [Ja, isomorfin är en bijektion mellan dem.]	×	
b)	Sidoklasser till en och samma delgrupp H till en grupp G är lika stora. [Ja, de är båda lika stora som H.]	×	
c)	Om elementet g i en grupp G med gruppoperationen $\circ$ har ordning 20 så har elementet $g \circ g$ ordning 10. [Ja, $(g \circ g)^k = e$ för $k = 10$, men inte för mindre $k > 0$.]	×	
d)	Om en ändlig grupp G verkar på mängden X och $x \in X$ är antalet element i banan Gx en delare till $\lvert G\rvert$. [Ja, $\lvert G\rvert = \lvert G_x\rvert \cdot \lvert Gx\rvert$.]	×	
e)	Ett RSA-krypto kan ha parametrarna $n = 46$ och $e = 2$. [Nej, $n = 46 = 2 \cdot 23$ ger $m = 1 \cdot 22 = 22$ och $\text{sgd}(22, 2) \neq 1$.]		×
f)	Ett RSA-krypto kan ha $d = 5$ och $e = 5$. [Ja, $n = 35 = 5 \cdot 7$ ger $m = 4 \cdot 6 = 24$ och $5 \cdot 5 \equiv 1 \pmod{24}$.]	×	

2a) (1p) Låt gruppen G ha vidstående grupptabell. Bestäm ett element x i G sådant att $bxc = f$.

$\circ$	a	b	c	d	f
a	a	b	c	d	f
b	b	c	d	f	a
c	c	d	f	a	b
d	d	f	a	b	c
f	f	a	b	c	d

Lösning:
Eftersom $bd = f$, gäller $bxc = f$ omm $xc = d$ (multiplicera med b^{-1} från vänster). Men $bc = d$, så $xc = d$ omm $x = b$, p.s.s.
Svar: $x = b$.

---

b) (1p) Du vill ha ett RSA-krypto med parametern $n = 65$. Ange ett möjligt värde på parametern e.

Lösning:
$n = 65 = 5 \cdot 13$ ger $m = 4 \cdot 12$. Kravet på e är $\text{sgd}(m, e) = 1$, så t.ex. $e = 5$ går bra. **Svar: T.ex. $e = 5$ fungerar.**

---

c) (1p) Formulera "Burnsides lemma", en formel för antalet banor då en ändlig grupp G verkar på en mängd X. Förklara kortfattat ingående beteckningar.

Lösning:
Antalet banor är $\frac{1}{|G|} \sum_{g \in G} |X_g|$ där $X_g = \{x \in X \mid gx = x\}$ är mängden av de element i X som g lämnar invarianta.

---

3) (3p) Betrakta gruppen $(\mathbb{Z}_{13} \setminus \{0\}, \cdot)$. Avgör om denna grupp genereras av elementet 2.

Lösning:
Frågan är om varje element i $Z_{13} \setminus \{0\}$ kan skrivas som 2^n, något n.
Man finner

n	1	2	3	4	5	6	7	8	9	10	11	12
2^n	2	4	8	3	6	12	11	9	5	10	7	1

och eftersom alla element i gruppen finns med på andra raden,
svar: Ja, $Z_{13} \setminus \{0\}$ genereras av elementet 2.
Alternativt: 2 genererar gruppen omm $o(2) = 12$, gruppens ordning, och eftersom $o(2) \mid 12$, räcker det att verifiera att $(2^1,\ 2^2,\ 2^3,)\ 2^4,\ 2^6 \neq 1$.

---

4) (3p) Ett RSA-krypto har de offentliga nycklarna $n = 39$ och $e = 11$. Bestäm parametern d och ange hur meddelande 2 kan dekrypteras, dvs ange hur $D(2)$ beräknas.
(Du behöver alltså inte beräkna $D(2)$ för att få full poäng på denna uppgift men du skall berätta hur man går till väga.)

Lösning:
$n = 39 = 3 \cdot 13$ ger $m = 2 \cdot 12 = 24$. d bestäms av att $e \cdot d \equiv 1 \pmod{m}$.
Man finner d (genom inspektion eller) med Euklides algoritm:

$$24 = 2 \cdot 11 + 2 \qquad 1 = 11 - 5 \cdot 2 = 11 - 5(24 - 2 \cdot 11) =$$
$$11 = 5 \cdot 2 + 1 \qquad = -5 \cdot 24 + 11 \cdot 11,$$

så $d = 11$ och $D(2) = 2^{11}$ i $\mathbb{Z}_{39}$ (dvs $0 \leq D(2) < 39$ och $D(2) \equiv 2^{11} \pmod{39}$).
Svar: $d = 11$ och $D(2) = 2^{11}$ i $\mathbb{Z}_{39}$ (så $D(2) = 20$).

---

5) (3p) Bestäm en delgrupp med tre element till den grupp G som har vidstående grupptabell:

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

Lösning:
Man kan betrakta tabellen tills man hittar en 3-delmängd till G som är sluten under $\circ$.
Mer systematiskt kan man notera att a har ordning 6 och således $aa = b$ ordning 3. b genererar alltså en delgrupp med tre element. $b^2 = d$, så
svar: $\{e, b, d\}$ är en delgrupp av ordning tre till G.