Matematik, KTH

Svar och lösningsförslag till ks4, 14 april 2014,
i SF1662 Diskret matematik för CLGYM1, TSVDK2

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 $a, b, c \in G$, en grupp, och $ab = bc$ gäller säkert $a^{-1}bc = abc^{-1}$. [Ja. $a^{-1}bc = a^{-1}ab = b$, $abc^{-1} = bcc^{-1} = b$.]	X	
b)	Om H är en delgrupp till G och $g \in G$ finns säkert $g' \in G$ med $gH = Hg'$. [Nejdå. vänstersidoklasser behöver inte vara högersidoklasser.]		X
c)	Varje ring är också en kropp. [Nej, men varje kropp är en ring. Ringen $(\mathbb{Z}_4, +, \cdot)$ är inte en kropp ($2 \cdot 2 = 0$, så 2 är inte inverterbart).]		X
d)	Om $z \in \mathbb{Z}[i]$ och $\lvert z\rvert^2$ är ett (reellt) primtal, är z säkert ett gaussiskt primtal. [Ja. $z = z_1 z_2$ skulle ge $\lvert z\rvert^2 = \lvert z_1\rvert^2 \lvert z_2\rvert^2$ och $\lvert z_k\rvert = 1$ ger $z_k \in U(\mathbb{Z}[i])$.]	X	
e)	Antalet rotationssymmetrier för en kub är 18. [Nej, det är 24 (om x är ett hörn är $\lvert G\rvert = \lvert G_x\rvert \cdot \lvert Gx\rvert = 3 \cdot 8$).]		X
f)	Ett RSA-system med offentlig nyckel $(n, e) = (187, 7)$ kan ha dekrypteringsparameter $d = 13$. [Nej. $m = 10 \cdot 16 = 160$, $7 \cdot 13 = 91 \not\equiv_m 1$.]		X

2a) (1p) Vi skall ange definitionen av att en grupp $(G, *)$ är abelsk.

Lösning:

$(G, *)$ är abelsk omm $g * h = h * g$ för alla $g, h \in G$.

---

b) (1p) Vi skall faktorisera $7 + 9i$ i gaussiska primtal.

Lösning:

$|7 + 9i|^2 = 7^2 + 9^2 = 130 = 2 \cdot 5 \cdot 13$. 2:an ger att $1 + i$ ingår i faktoriseringen. $\frac{7+9i}{1+i} = \frac{(7+9i)(1-i)}{2} = 8 + i$. 5:an ger att en av $2 \pm i$ ingår $(2^2 + (\pm 1)^2 = 5)$. $\frac{8+i}{2+i} = \frac{(8+i)(2-i)}{5} = \frac{17}{5} - \frac{6}{5}i \notin \mathbb{Z}[i]$, så $2 + i$ ingår inte. $\frac{8+i}{2-i} = \frac{(8+i)(2+i)}{5} = 3 + 2i$, den återstående gaussiska primfaktorn $(3^2 + 2^2 = 13)$.

Svar: Den sökta faktoriseringen är $7 + 9i = (1 + i)(2 - i)(3 + 2i)$.

---

c) (1p) Vi söker alla $a \in \mathbb{Z}_3$ som gör $f(x) = x^3 + 2x + a \in \mathbb{Z}_3[x]$ irreducibelt.

Lösning:

$f(x)$ är irreducibelt omm det saknar nollställen i $\mathbb{Z}_3$ (eftersom $f(x)$ har grad 3 är det reducibelt omm det har en förstagradsfaktor, så enligt faktorsatsen omm det har ett nollställe i $\mathbb{Z}_3$). $f(0) = f(1) = f(2) = a$, så de sökta värdena är $a = 1, 2$.

Svar: De sökta värdena är $a = 1, 2$.

---

3) $G = \{a, b, c, d, f\}$ är en grupp med 5 element. Vi skall (a, 1p) bestämma $o(b)$, (b, 1p) avgöra vilket element som är 1 och (c, 1p) fylla i de sju namn som fattas i grupptabellens två första rader härintill.

$*$	a	b	c	d	f
a	f	d	_	_	_
b	_	a	_	_	_

Lösning:

a. $o(b)$ är (enligt känd sats) en delare till $|G| = 5$. $b \neq 1$, ty $b * b \neq b$, så $o(b) = 5$.
b. Vi ser att $a = b^2$, $f = a^2 = b^4$, $d = a * b = b^3$ (och $b = b^1$), inget av dem 1 (eftersom $o(b) = 5$), så det återstående elementet $c = 1$.
c. Nu vet vi nog. $a * c = a * 1 = a$, $a * d = b^2 * b^3 = b^5 = 1 = c$,
$a * f = b^2 * b^4 = b^6 = b$,
$b * a = b * b^2 = b^3 = d$, $b * c = b * 1 = b$,
$b * d = b * b^3 = b^4 = f$, $b * f = b * b^4 = b^5 = 1 = c$.
Därmed är båda raderna klara.

$*$	a	b	c	d	f
a	f	d	a	c	b
b	d	a	b	f	c

Svar a: $o(b) = 5$, b: $c = 1$, c: Se ovan.

---

4) Vi söker de minsta icke-negativa resterna då 24^{100} divideras med (a, 2p) 17 och (b, 1p) 21.

Lösning:

a. Den sökta resten är det minsta icke-negativa heltal som är $\equiv_{17} 24^{100}$. Eftersom 17 är ett primtal och $17 \nmid 24$ ger Fermats lilla sats att $24^{16} \equiv_{17} 1$, så $24^{100} \equiv_{17} (24^{16})^6 \cdot 24^4 \equiv_{17} 1^6 \cdot 7^4 \equiv_{17} (-2)^2 = 4$ (ty $24 \equiv_{17} 7$ och $7^2 = 49 \equiv_{17} -2$).
b. Eftersom $21 = 3 \cdot 7$, där 3 och 7 är primtal, kan vi använda satsen som ligger till grund för RSA-kryptering. $n = 21 = 3 \cdot 7$ ger $m = 2 \cdot 6 = 12$, så $24^{k \cdot 12+1} \equiv_{21} 3^{k \cdot 12+1} \equiv_{21} 3$ för alla $k \in \mathbb{N}$. Det ger $24^{100} \equiv_{21} 3^{8 \cdot 12+1} \cdot 3^3 \equiv_{21} 3^4 = 81 \equiv_{21} 18$.

Svar a: Resten blir 4, b: Resten blir 18.

---

5) Vi skall (a, 1p) finna elementen i $G = U(\mathbb{Z}_{12})$, (b, 1p) stabilisatorn G_2 och banan $G2$ då G verkar på $X = \mathbb{Z}_{12}$ med multiplikation och (c, 1p) alla banor för G:s verkan på X.

Lösning:

a. $x \in G \Leftrightarrow \text{sgd}(x, 12) = 1$, så $G = \{1, 5, 7, 11\}$.
b. $1 \cdot 2 = 2$, $5 \cdot 2 = 10$, $7 \cdot 2 = 2$, $11 \cdot 2 = 10$, så man får stabilisatorn $G_2 = \{g \in G \mid g2 = 2\} = \{1, 7\}$ och banan $G2 = \{g2 \mid g \in G\} = \{2, 10\}$.
c. Banorna fås som i b: $G0 = \{0\}$, $G1 = G5 = G7 = G11 = \{1, 5, 7, 11\}$, $G2 = G10 = \{2, 10\}$, $G3 = G9 = \{3, 9\}$, $G4 = G8 = \{4, 8\}$, $G6 = \{6\}$.

Svar a: $G = \{1, 5, 7, 11\}$, b: $G_2 = \{1, 7\}$, $G2 = \{2, 10\}$
Banorna är $\{0\}$, $\{1, 5, 7, 11\}$, $\{2, 10\}$, $\{3, 9\}$, $\{4, 8\}$, $\{6\}$.