Matematik, KTH

Svar och lösningsförslag till ks4, 6 maj 2013,
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 och $g * h^{-1} = g^{-1} * h,\ g, h \in G$, måste $g = h$. [Nej. $g * h^{-1} = g^{-1} * h$ omm $g * g = h * h$, vilket gäller för t.ex. $g = 0$, $h = 1$ i $(\mathbb{Z}_2, +)$.]		×
b)	Om G och H är grupper är de direkta produkterna $G \times H$ och $H \times G$ säkert isomorfa. [En isomorfi ges av $\phi(g, h) = (h, g)$.]	×	
c)	Om p, q är två olika primtal, är $(\mathbb{Z}_{pq}, +, \cdot)$ en kropp. [Nej, det är en ring, men ingen kropp. p saknar invers i $\mathbb{Z}_{pq}$.]		×
d)	Om gruppen G verkar på mängden X är för varje $x \in X$ säkert $\{g \in G \mid gx = x\}$ en delgrupp till G. [Javisst. Det är stabilisatorn G_x för x.]	×	
e)	Om $a, b \in \mathbb{Z}$ är sådana att $a+bi$ är ett gaussiskt primtal, måste $a^2 + b^2$ vara ett (reellt) primtal. [Nej, t.ex. $3 = 3 + 0i$ är ett gaussiskt primtal, men $3^2 + 0^2 = 9 = 3 \cdot 3$.]		×
f)	Om n är ett udda heltal, $n \geq 3$ och $2^n \equiv 2 \pmod{n}$ är n säkert ett primtal. [Falskt för pseudoprimtal, bas 2, t.ex. 341.]		×

2a) (1p) $g \in G$, en grupp, uppfyller $g^{75} = 1$. Vi söker möjliga värden för $o(g)$.

Lösning:

Ordningen måste vara en delare till 75 och alla positiva delare till 75 (dvs 1, 3, 5, 15, 25, 75) är möjliga ordningar för g.

Svar: Alla möjliga värden för $o(g)$ är 1, 3, 5, 15, 25, 75.

---

b) (1p) Vi skall faktorisera $21 + 9i$ i gaussiska primtal.

Lösning:

$21 + 9i = 3(7 + 3i)$ och 3 är ett gaussiskt primtal (ty $\equiv_4 3$). $7^2 + 3^2 = 58 = 2 \cdot 29$. 2:an ger att $1+i$ är en primfaktor i $7+3i$, $\frac{7+3i}{1+i} = \frac{(7+3i)(1-i)}{2} = 5-2i$. $5^2+2^2 = 29$, ett reellt primtal, så $5 - 2i$ är ett gaussiskt primtal.

Svar: Den sökta faktoriseringen är $21 + 9i = 3(1 + i)(5 - 2i)$.

---

c) (1p) Vi skall avgöra om $f(x) = 2x^3 + 3x^2 + x + 3$ är irreducibelt i $\mathbb{Z}_5[x]$.

Lösning:

Eftersom $f(x)$ är av grad 3 är det reducibelt omm det har ett nollställe (faktorsatsen, eftersom en faktorisering utan enhet måste innehålla en förstagradsfaktor). Vi finner i $\mathbb{Z}_5$: $f(0) = 3$, $f(1) = 4$, $f(2) = 3$, $f(3) = 2$, $f(4) = 3$, så $f(x)$ saknar nollställen i $\mathbb{Z}_5$. **Svar: $f(x)$ är irreducibelt i $\mathbb{Z}_5[x]$.**

---

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

	e	a	b	c	d
e	_	a	_	_	_
a	_	c	_	_	e

Lösning:

Eftersom $ea = a$ är e (som namnet antyder) identitetselementet (multiplicera med a^{-1} från höger). Det ger första raden och första elementet i andra raden. Eftersom grupptabellen är en latinsk kvadrat, kan ab inte vara någon av e, a, b, c, så $ab = d$ och (åter latinsk kvadrat) $ac = b$, dvs

(Man kan också använda att gruppen är cyklisk (ty av primtalsordning) och att a är en generator (ty $\neq e$).)

	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$
$\boldsymbol{e}$	$\boldsymbol{e}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$
$\boldsymbol{a}$	$\boldsymbol{a}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{b}$	$\boldsymbol{e}$

---

4) (3p) Vi skall avgöra om $(\mathbb{Z}_{61} \setminus \{0\}, \cdot)$ genereras av elementet $8 (= 2^3)$.

Lösning:

Eftersom $|\mathbb{Z}_{61} \setminus \{0\}| = 60$, gäller $g^{60} = 1$ för alla $g \in \mathbb{Z}_{61} \setminus \{0\}$. Speciellt $2^{60} = 8^{20} = 1$, så ordningen för 8 i gruppen är ≤ 20, mindre än gruppens ordning, så den genereras inte av 8.

Svar: Nej, 8 genererar inte gruppen $(\mathbb{Z}_{61} \setminus \{0\}, \cdot)$.

---

5) (3p) Vi skall avgöra vilken av $75, 85, 95$ som är möjlig för n i ett RSA-system med $e = 15$. Vi skall också avgöra om man kan använda $d = 7$ för detta n.

Lösning:

Möjliga n-värden skall vara pq med p och q olika primtal, så att $\text{sgd}(e, m) = 1$, där $e = 15$ och $m = (p-1)(q-1)$. Man finner:
$n = 75 = 3 \cdot 5^2$ är inte en produkt av två olika primtal, så **75 är inte möjligt**.
$n = 85 = 5 \cdot 17$ ger $m = 4 \cdot 16 = 64$ och $\text{sgd}(e, m) = 1$, så **85 är möjligt**.
$n = 95 = 5 \cdot 19$ ger $m = 4 \cdot 18$ och $\text{sgd}(e, m) = 3 \neq 1$, så **95 är inte möjligt**.
Dekrypteringsparametern d till $n = 85$ skall uppfylla att $ed \equiv 1 \pmod{64}$, men $e \cdot 7 = 105 \equiv 41 \pmod{64}$, så d kan inte vara 7.

Svar: Enda möjliga $\boldsymbol{n}$ är 85. Motsvarande $\boldsymbol{d}$ är inte 7.