Matematik, KTH

Svar och lösningsförslag till ks4, 25 april 2016,
i SF1662 Diskret matematik

1) (För varje delfråga ger rätt svar $\frac{1}{2}$p, inget svar 0p, fel svar $-\frac{1}{2}$p)

		sant	falskt
a)	För alla grupper G och alla $x, y \in G$ med $x^2 = y^2$ är $x = y$. [Nej. Motex: i gruppen $(\{1, -1\}, \cdot)$, är $1^2 = (-1)^2$, $1 \neq -1$.]		X
b)	Om A, B är högersidoklasser till samma delgrupp H till gruppen G, finns det säkert en bijektion $f : A \to B$. [Jadå. Om $A = Hg_1$, $B = Hg_2$ ger $f(a) = ag_1^{-1}g_2$ en sådan bijektion.]	X	
c)	$(\mathbb{R}, +, \cdot)$, de reella talen med operationerna addition och multiplikation, utgör en ring. [Ja, en kropp, så en ring.]	X	
d)	Ett (icke-konstant) polynom med rationella koefficienter är säkert irreducibelt om det saknar reella nollställen. [Nej. T.ex. $(x^2 + 1)^2$ är reducibelt och saknar reella nollställen.]		X
e)	G (en ändlig grupp) verkar på X (en mängd). Om $x, y \in X$ har lika stora banor ($\lvert Gx\rvert = \lvert Gy\rvert$) är stabilisatorerna säkert lika stora ($\lvert G_x\rvert = \lvert G_y\rvert$). [Ja. $\lvert Gx\rvert \cdot \lvert G_x\rvert = \lvert Gy\rvert \cdot \lvert G_y\rvert$, alla i $\mathbb{Z}_+$.]	X	
f)	Om $N \in \mathbb{N}$, $N \geq 2$, och för alla $b = 1, 2, \ldots, N-1$ gäller att $b^{N-1} \equiv 1 \pmod{N}$ är N säkert ett primtal. [Ja, ty om $b \mid N$, $b > 1$, kan inte $N \mid (b^{N-1} - 1)$.]	X	

2a) (1p) $\phi : \mathbb{Z}_3 \to \mathbb{Z}_3$ ges av $\phi(0) = 0$, $\phi(1) = 2$, $\phi(2) = 1$. Vi ska avgöra om ϕ är en isomorfi av gruppen $(\mathbb{Z}_3, +)$ på sig själv (en automorfi).

Lösning:

i) ϕ är en bijektion (injektion och surjektion). *ii)* $\phi(x) = -x$ (alla $x \in \mathbb{Z}_3$), så $\phi(x + y) = -(x + y) = (-x) + (-y) = \phi(x) + \phi(y)$ (alla $x, y \in \mathbb{Z}_3$).
i),ii) ger (enligt definition) att ϕ är en automorfi.

Svar: Ja, ϕ är en automorfi för $(\mathbb{Z}_3, +)$.

2b) (1p) Vi ska faktorisera $7 - 11i$ i gaussiska primtal.

Lösning:

$|7 - 11i|^2 = 7^2 + (-11)^2 = 49 + 121 = 170 = 2 \cdot 5 \cdot 17$, så det ingår en faktor $1 + i$ ($2 = 1^2 + 1^2$), endera av $2 \pm i$ ($5 = 2^2 + 1^2$) och endera av $4 \pm i$ ($17 = 4^2 + 1^2$).
$\frac{7-11i}{1+i} = \frac{(7-11i)(1-i)}{1^2+1^2} = \frac{-4-18i}{2} = -2 - 9i$.
$\frac{-2-9i}{2+i} = \frac{(-2-9i)(2-i)}{2^2+1^2} = \frac{-13-16i}{5} \notin \mathbb{Z}[i]$, men $\frac{-2-9i}{2-i} = \frac{(-2-9i)(2+i)}{5} = \frac{5-20i}{5} = 1 - 4i$.
Det ger $7 - 11i = (1 + i)(2 - i)(1 - 4i) = (1 - i)(2 - i)(4 + i)$ (kan flytta $-1, \pm i$).

Svar: En sådan faktorisering är $(1 - i)(2 - i)(4 + i)$.

2c) (1p) Vi söker (minsta icke-negativa) resten då 1071^{795} divideras med 13.

Lösning:

Den sökta resten är det $x \in \mathbb{N}$, $x < 13$ som uppfyller $x \equiv_{13} 1071^{795}$.
$1071 = 13 \cdot 82 + 5$ och $795 = 12 \cdot 66 + 3$, så $1071^{795} \equiv_{13} 5^{795} = (5^{12})^{66} \cdot 5^3$.
Enligt Fermats lilla sats är $5^{12} \equiv_{13} 1$ (ty 13 är primtal, $13 \nmid 5$ och $12 = 13 - 1$), så $1071^{795} \equiv_{13} 1^{66} \cdot 5^2 \cdot 5 \equiv_{13} 1 \cdot (-1) \cdot 5 = -5 \equiv_{13} 8$.

Svar: Den sökta resten är 8.

3) $(G, *)$, där $G = \{u, v, x, y, z\}$, är en grupp med 5 element och $u * u = x$, $u * x = y$, $u * y = z$. Vi söker (a, 1p) $o(u)$, u:s ordning, (b, 1p) G:s identitetselement och (c, 1p) hela G:s grupptabell.

Lösning:

a. $|G| = 5$, ett primtal, och $o(u) \neq 1$ ($u \neq 1$ (identitetselementet), ty $u^2 \neq u$). $o(u) \mid |G|$, så $o(u) = 5$.

b. $u*v \neq x, y, z$ (grupptabellen är en latinsk kvadrat) och $u*v \neq v$ ($u \neq 1$ enligt a.), så $u * v = u$ (latinsk kvadrat igen) och v är identitetselementet. (alt. $x = u^2$, $y = u^3$, $z = u^4$, alla $\neq 1$, så $v = 1$.)

c. $v = 1$, $u = u^1$, $x = u^2$, $y = u^3$, $z = u^4$ ger med $u^5 = 1$ tabellen härintill.

$*$	u	v	x	y	z
u	$\boldsymbol{x}$	u	$\boldsymbol{y}$	$\boldsymbol{z}$	v
v	u	v	x	y	z
x	y	x	z	v	u
y	z	y	v	u	x
z	v	z	u	x	y

Svar a: $o(u) = 5$, b: v är identitetselementet, c: Se ovan.

---

4) $G = U_{22}$, gruppen av inverterbara element i $(\mathbb{Z}_{22}, +, \cdot)$. Vi ska (a, 1p) finna $|G|$ och (b, 2p) avgöra om G är cyklisk och i så fall ange en generator för G.

Lösning:

a. $G = U_{22} = \{x \in \mathbb{Z}_{22} \mid \text{sgd}(x, 22) = 1\} = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$, så $|G| = 10$.

b. G är cyklisk omm något $g \in G$ har ordning $o(g) = |G| = 10$.
Eftersom $o(g) \mid 10$ är $o(g) = 10$ omm $o(g) \neq 1, 2, 5$. ($o(g) = 1$ omm $g = 1$.)
Vi prövar: $3^2 = 9$, $3^5 = 9{\cdot}9{\cdot}3 = (-7){\cdot}3 = 1$, $5^2 = 25 = 3$, $5^5 = 3{\cdot}3{\cdot}5 = 45 = 1$, men $7^2 = 5$, $7^5 = 5 \cdot 5 \cdot 7 = 3 \cdot 7 = 21 \neq 1$, så $o(7) = 10$.

Svar a: $|G| = 10$, b: G är cyklisk. 7 är en generator (liksom 13, 17, 19).

---

5) Vi har ett RSA-system med parametern $n = 299 = 13 \cdot 23$ och söker (a, 1p) det minsta möjliga värdet för krypteringsexponenten $e \geq 32$ och (b, 2p) en motsvarande dekrypteringsexponent d med $1 < d < n$.

Lösning:

a. $n = 13 \cdot 23$ ger $m = (13 - 1)(23 - 1) = 12 \cdot 22 = 2^3 \cdot 3 \cdot 11 = 264$. e skall uppfylla $\text{sgd}(e, m) = 1$, dvs $2, 3, 11 \nmid e$. Minsta möjliga värde ≥ 32 är $e = 35$.

b. d fungerar om $e \cdot d \equiv_m 1$, dvs $35d \equiv_{264} 1$. Vi använder Euklides algoritm:
$264 = 35 \cdot 7 + 19$, $35 = 19 \cdot 1 + 16$, $19 = 16 \cdot 1 + 3$, $16 = 3 \cdot 5 + 1$, så
$1 = 16 - 5(19 - 16) = -5 \cdot 19 + 6(35 - 19) = 6 \cdot 35 - 11(264 - 7 \cdot 35) =$
$= -11 \cdot 264 + 83 \cdot 35$. Det visar att $35 \cdot 83 \equiv_{264} 1$ och man kan ta $d = 83$.

Svar a: $e = 35$, b: $d = 83$ är ett möjligt val (215 är ett annat).