Matematik, KTH

Svar och lösningsförslag till ks4, 27 april 2015,
i SF1662 Diskret matematik

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 det i en grupptabell står 1 (identitetselementet) i rad i, kolumn j, står det också 1 i rad j, kolumn i. [Ja. $g_ig_j = 1 \Rightarrow g_j = g_i^{-1} \Rightarrow g_jg_i = 1$.]	×	
b)	Om antalet element i en grupp är ett primtal är gruppen säkert abelsk. [Ja. $\lvert G\rvert$ primtal ger G cyklisk och därmed abelsk.]	×	
c)	Om G är en grupp, $\lvert G\rvert = n\,(\in \mathbb{N})$ och $g \in G$ uppfyller $g^s = 1$ (G:s identitetselement), så är säkert $g^{\mathrm{sgd}(s,n)} = 1$. [Ja, $o(g) \mid s$, n, så $o(g) \mid \mathrm{sgd}(s,n)$ och därmed $g^{\mathrm{sgd}(s,n)} = 1$.]	×	
d)	Om $z \in \mathbb{Z}[i]$ och 61 är en delare till $\lvert z\rvert^2$ (dvs $61 \,\big|\, \lvert z\rvert^2$), måste $\frac{z}{6+5i} \in \mathbb{Z}[i]$. [Nej, det kan vara så att $\frac{z}{6-5i} \in \mathbb{Z}[i]$. Ex. $z = 6 - 5i$ har $\lvert z\rvert^2 = 61$.]		×
e)	Om polynomet $f(x) \in F[x]$ (F en kropp) är reducibelt så är säkert $f(a) = 0$ för något $a \in F$. [Nej, t.ex. $f(x) = (x^2 + x + 1)^2 \in \mathbb{Z}_2[x]$ reducibelt, $f(0) = f(1) = 1$.]		×
f)	Om en grupp G verkar på en mängd X gäller för alla $x \in X$ att $\lvert Gx\rvert \,\big|\, \lvert G\rvert$ (där Gx är banan för x). [Ja, $\lvert G\rvert = \lvert G_x\rvert \cdot \lvert Gx\rvert$.]	×	

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

Lösning:

$(G, *)$ är cyklisk omm det finns (minst) ett $g \in G$ sådant att $\langle g\rangle = G$.
(Här är $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$; $g^0 = 1$ och för $n \in \mathbb{Z}_+$ är $g^n = \underbrace{g * g * \cdots * g}_{n \text{ st}}$ och $g^{-n} = (g^{-1})^n$.)

---

b) (1p) Vi söker $x, y \in \mathbb{Z}_+$ med $x^2 + y^2 = 18\,241 (= 17 \cdot 29 \cdot 37)$.

Lösning:

$z = x + iy$ skall uppfylla $\lvert z\rvert^2 = 18241$, så dess (gaussiska) primfaktorer är en vardera av $(4 \pm i)$, $(5 \pm 2i)$ och $(6 \pm i)$ (de gaussiska primtal g som har $\lvert g\rvert^2 = 17$, 29 resp. 37). z är alltså (associerat med) en sådan produkt.
Man finner $(4 + i)(5 + 2i)(6 + i) = (18 + 13i)(6 + i) = 95 + 96i$, så en lösning är $x = 95$, $y = 96$. (Övriga lösningar fås genom att välja andra tecken i faktorerna, $(x, y) = (121, 60)$, $(135, 4)$, $(129, 40)$ (eller omkastat).)

Svar: Lösningar är $\{x, y\} = \{95, 96\}$, $\{121, 60\}$, $\{135, 4\}$, $\{129, 40\}$.

---

c) (1p) Vi skall beskriva fermattestet med bas b.

Lösning:

För att avgöra om $N \in \mathbb{Z}_+$ $(1 < b < N)$ är ett primtal: Är $b^{N-1} \equiv 1 \pmod N$?
Vid svar "nej": N är inte ett primtal, vid svar "ja": vet inte (säkert).

---

3) $(G, *)$, där $G = \{p, q, r, s, t, u\}$, är en grupp med 6 element och grupptabellen till höger. Vi skall (a, 1p) avgöra vilket element som är identitetselement, (b, 1p) finna en delgrupp H med precis två element och (c, 1p) finna alla H:s sidoklasser i G.

$*$	p	q	r	s	t	u
p	t	r	u	p	s	q
q	u	s	t	q	r	p
r	q	p	s	r	u	t
s	p	q	r	s	t	u
t	s	u	q	t	p	r
u	r	t	p	u	q	s

Lösning:

a. $p * s = p$, så s måste vara identitetselementet (och $s * x = x * s = x$ för alla $x \in G$).
b. H kan vara $\{s, x\}$, där $x * x = s$, $x \neq s$ (identitetselementet). Vi tar $H = \{s, q\}$.
c. Man finner $s * H = q * H = \{s, q\} (= H)$, $H * s = H * q = \{s, q\} (= H)$,
$p * H = r * H = \{p, r\}$, $H * p = H * u = \{p, u\}$,
$t * H = u * H = \{t, u\}$. $H * r = H * t = \{r, t\}$.

Svar a: s är identitetselement, b: T.ex. $H = \{s, q\}$,
c: Vä: $\{s, q\}$, $\{p, r\}$, $\{t, u\}$, hö: $\{s, q\}$, $\{p, u\}$, $\{r, t\}$.

---

4) Vi söker (a, 1p) ett udda n bland $81, \ldots, 99$ så att $(n, 21)$ kan vara parametrar i ett RSA-system, (b, 1p) ett motsvarande d och (c, 1p) 10^{8823} i $\mathbb{Z}_{473}$.

Lösning:

a. n skall vara en produkt av två olika primtal, $n = p \cdot q$, sådana att $\text{sgd}(e, m) = 1$, där $m = (p-1)(q-1)$. Det enda bland de givna som uppfyller detta med $e = 21 (= 3 \cdot 7)$ är $n = 85 = 5 \cdot 17$ (så $m = (5-1)(17-1) = 64 = 2^6$).
b. d bestäms av att $d \cdot e \equiv_m 1$. Eftersom $m = 64 = 3 \cdot 21 + 1$, så $1 = 1 \cdot 64 - 3 \cdot 21 = (1-21)64 + (64-3)21 = -20 \cdot 64 + 61 \cdot 21$, kan man ta $d = 61$.
c. Enligt satsen som ligger till grund för RSA gäller (eftersom $473 = 11 \cdot 43$) för alla $x \in \mathbb{Z}$ och $k \in \mathbb{N}$ att $x^{k(11-1)(43-1)+1} = x^{420k+1} \equiv_{473} x$, så $10^{8823} = 10^{420 \cdot 21 + 3} = 10^{420 \cdot 21 + 1} \cdot 10^2 \equiv_{473} 10^3 = 1000 \equiv_{473} 54$.

Svar a: Enda möjliga n är 85, b: Man kan ta $d = 61$,
c: $10^{8823} = 54$ i $\mathbb{Z}_{473}$.

---

5) $G = U(\mathbb{Z}_{34})$, de inverterbara (under $\cdot$) elementen i $(\mathbb{Z}_{34}, +, \cdot)$. Vi skall finna (a, 1p) G:s ordning, (b, 1p) ordningen $o(3)$ för $3 \in G$ och (c, 1p) $o(13)$.

Lösning:

a. $G = \{x \in G \mid \text{sgd}(x, 34) = 1\}$, så $(34 = 2 \cdot 17)$ G innehåller alla udda heltal ≥ 1 och ≤ 33 som inte är (delbara med) 17. De är totalt 16 st.
b. $3 \in G$, så $o(3) \,\big|\, |G| = 16$ (följer av Lagranges sats). Tänkbara värden är alltså 1, 2, 4, 8, 16. Vi finner $3^1 = 3$, $3^2 = 9$, $3^4 = 9^2 = 81 = 13$, $3^8 = 13^2 = 169 = 170 - 1 = -1 = 33$, så $o(3) \neq 1, 2, 4, 8$. Alltså $o(3) = 16$ (så G är cyklisk).
c. Eftersom $13 = 3^4$ och $o(3) = 16$ är $o(13) = 4$ ($13^1 \neq 1$, $13^2 = 3^8 \neq 1$, $13^4 = 3^{16} = 1$.)

Svar a: G:s ordning $|G| = 16$, b: $o(3) = 16$, c: $o(13) = 4$.