

**Svar och lösningsförslag till ks4, 24 april 2017,
i SF1662 Diskret matematik**

	sant	falskt
1) (För varje delfråga ger rätt svar $\frac{1}{2}p$, inget svar $0p$, fel svar $-\frac{1}{2}p$)		
a) Om $(G, *)$ är en grupp och $a * (b * c) = (a * b) * c$ för alla $a, b, c \in G$, är G säkert en cyklisk grupp. [Nej. Likheten gäller i alla grupper (associativitet) och det finns icke-cykliska grupper.]		×
b) Alla grupper av ordning 19 är isomorfa . [Ja, eftersom 19 är ett primtal är de alla cykliska, så isomorfa.]	×	
c) Varje ring är också en kropp. [Nej, $\mathbb{Z}$ är en ring, men ingen kropp. Varje kropp är en ring.]		×
d) Om S är en högersidoklass till en delgrupp H i en ändlig grupp G , finns säkert $n \in \mathbb{Z}_+$ med $ G = n S $. [Ja. $ S = H $ och $ H \mid G $ enligt Lagranges sats.]	×	
e) $f(x) = x^3 + x^2 + 2 \in \mathbb{Z}_3[x]$ är ett irreducibelt polynom. [Ja. Faktorisering utan konstant faktor ger en linjär faktor (grad = 3), så $f(x) = 0$, något $x \in \mathbb{Z}_3$, men $f(0) = 2$, $f(1) = 1$, $f(2) = 2$.]	×	
f) Ett carmichaeltal är ett primtal som för minst en bas inte klarar fermatetestet. [Nej. Carmichaeltal är inte primtal.]		×

2a) (1p) Vi söker antalet element i rotationssymmetrigruppen för ett triangulärt prisma (med två motstående liksidiga trianglar och tre kvadrater).

Lösning:

Kalla gruppen G . Om x är mittpunkten av en av trianglarna fås $|Gx| = 2$ (banan består av trianglarnas mittpunkter) och $|G_x| = 3$ (rotationer kring en axel genom x), så $|G| = |Gx| \cdot |G_x| = 2 \cdot 3 = 6$. **Svar: Gruppen har precis 6 element.**

2b) (1p) Vi ska faktorisera $17 - 7i$ i gaussiska primtal.

Lösning:

$|17 - 7i|^2 = 17^2 + (-7)^2 = 289 + 49 = 338 = 2 \cdot 13^2$, så det ingår en faktor $1 + i$ ($2 = 1^2 + 1^2$) och två faktorer $3 \pm 2i$ ($13 = 3^2 + 2^2$).
 $\frac{17-7i}{1+i} = \frac{(17-7i)(1-i)}{1^2+1^2} = \frac{10-24i}{2} = 5 - 12i$.
 $\frac{5-12i}{3+2i} = \frac{(5-12i)(3-2i)}{3^2+2^2} = \frac{-9-46i}{13} \notin \mathbb{Z}[i]$, men $\frac{5-12i}{3-2i} = \frac{(5-12i)(3+2i)}{3^2+2^2} = \frac{39-26i}{13} = 3 - 2i$.
 Det ger $17 - 7i = (1 + i)(3 - 2i)^2$ (där man som vanligt kan flytta $-1, \pm i$).

Svar: En sådan faktorisering är $(1 + i)(3 - 2i)^2$.

2c) (1p) Vi söker (minsta icke-negativa) resten då $24^{4^{2017}}$ divideras med 13.

Lösning:

Den sökta resten är det $x \in \mathbb{N}$, $x < 13$ som uppfyller $x \equiv_{13} 24^{4^{2017}} \equiv_{13} 11^{4^{2017}}$.
 13 är primtal och $13 \nmid 11$, så $11^{12} \equiv_{13} 1$ (Fermats lilla sats).
 $4^{2017} \equiv_{12} 4$ ($4 \cdot 4 = 16 \equiv_{12} 4$ etc.), så $11^{4^{2017}} = 11^{12k+4} = (11^{12})^k \cdot 11^4 \equiv_{13} 1^k \cdot (-2)^4 = 16 \equiv_{13} 3$ (för ett $k \in \mathbb{N}$).
Svar: Den sökta resten är 3.

3) G är $U(\mathbb{Z}_{24})$, de inverterbara elementen i $\mathbb{Z}_{24}$. Vi skall (a, 1p) finna alla element i G och (b, 2p) avgöra om gruppen $(G, \cdot)$ är cyklisk.

Lösning:

a. $U(\mathbb{Z}_{24}) = \{r \in \mathbb{Z}_{24} \mid \text{sgd}(r, 24) = 1\} = \{1, 5, 7, 11, 13, 17, 19, 23\}$.
b. $5^2 = 25 \equiv_{24} 1$, $7^2 = 49 \equiv_{24} 1$, $11^2 = 121 \equiv_{24} 1$, $13^2 \equiv_{24} (-11)^2 \equiv_{24} 1$,
 $17^2 \equiv_{24} (-7)^2 \equiv_{24} 1$, $19^2 \equiv_{24} (-5)^2 \equiv_{24} 1$, $23^2 \equiv_{24} (-1)^2 = 1$, så alla element har ordning 1 (identitetselementet) eller 2 (alla andra element) och G är inte cyklisk.
(Det räcker att visa att två olika element har ordning 2. I en cyklisk grupp $\langle g \rangle$ av ordning 8 har bara ett (g^4) det.)

Svar a: $G = \{1, 5, 7, 11, 13, 17, 19, 23\}$, b: G är inte cyklisk.

4) (3p) Två rader från grupptabellen för gruppen $(G, *)$ syns till höger.
Vi ska fylla i de tomma positionerna (de med $-$).

$*$	a	b	c	d	f	g
a	b	$-$	$-$	c	$-$	$-$
b	$-$	b	$-$	$-$	$-$	$-$

Lösning:

Eftersom $b * b = b = b * 1$ är $b = 1$, identitetselementet. Detta ger andra raden och att $a * b = a$.
 $a * c = a * (a * d) = (a * a) * d = b * d = d$. Alla element förekommer exakt en gång i varje rad och i varje kolumn i grupptabellen, så $a * f = g$ och $a * g = f$. Det ger raderna i tabellen:

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

5) (3p) Donald och Vladimir har varsitt RSA-system. Donald har $d = 33$ och Vladimir har $d = 35$. Vi skall avgöra dels vem av dem som har $n = 119$ och vem som har $n = 145$ och dels vem som har $e = 11$ och vem som har $e = 17$.

Lösning:

$n = 119 = 7 \cdot 17$ ger $m = 6 \cdot 16 = 2^5 \cdot 3 = 96$, medan $n = 145 = 5 \cdot 29$ ger $m = 4 \cdot 28 = 2^4 \cdot 7 = 112$. Eftersom $\text{sgd}(m, d) = 1$ måste Donald ha $n = 145$ ($3 \mid 96, 33$) och Vladimir då $n = 119$ (dessutom $7 \mid 112, 35$, så han kan inte ha $n = 145$).
Vidare skall $e \cdot d \equiv_m 1$. $11 \cdot 33 = 363 = 3 \cdot 96 + 75 = 3 \cdot 112 + 27$, så $e = 11$ hör inte ihop med $d = 33$. Således har Donald $e = 17$ och Vladimir $e = 11$.
(Kontroll: $11 \cdot 35 = 385 = 4 \cdot 96 + 1 (= 3 \cdot 112 + 49)$ och $17 \cdot 33 = 561 = 5 \cdot 112 + 1 (= 5 \cdot 96 + 81)$.)

Svar: Donald har $(n, e) = (145, 17)$. Vladimir har $(n, e) = (119, 11)$.