

**Svar och lösningsförslag till fiktiva ks2, oktober 2017,
i SF1688 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)	Om en grupp G , $ G = 37$, verkar på en mängd X , $ X = 80$, finns säkert $x \in X$ med $gx = x$ för alla $g \in G$. [Ja. 37 är ett primtal, så $ Gx = 1$ eller 37 för varje $x \in X$ och $37 \nmid 80$.]	×	
b)	$45 \in \mathbb{Z}_{7261}$ är inverterbart. [Ja. $45 = 3^2 \cdot 5$ och $3, 5 \nmid 7261$, så $\text{sgd}(45, 7261) = 1$.]	×	
c)	$15^{387} \equiv 60 \pmod{221}$. [Ja. $\phi(221) = \phi(13 \cdot 17) = 12 \cdot 16 = 192$ och $\text{sgd}(15, 221) = 1$, så (Euler) $15^{192} \equiv_{221} 1$ och $15^2 = 225 \equiv_{221} 4$ etc.]	×	
d)	Om $(F, +, \cdot)$, $ F = 32$, är en kropp, finns säkert $f_i \in F$ ($i = 1, 2, 3, 4$) så att varje $f \in F$ är en summa av f_i :n. [Nej. $32 = 2^5$, $(F, +) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Det behövs 5 st f_i :n.]		×
e)	Om $(F, +, \cdot)$ är en ändlig kropp med karakteristisk p , är $f = 1$ den enda lösningen till ekvationen $f^p = 1$ i F . [Ja. $0^p = 0$ och $f \in F \setminus \{0\} \Rightarrow o(f) \mid (p^r - 1)$. Bara 1 har ordning 1.]	×	
f)	$f^2 + 1 = 0$ för något $f \in F = \mathbb{Z}_7[x]/(x^3 + 2x + 1)$. [Nej. $x^3 + 2x + 1 \in \mathbb{Z}_7[x]$ irreducibelt, så F en kropp, $ F \setminus \{0\} = 7^3 - 1 = 342$. $f^2 = -1$ ger $f^4 = 1$ och $f, f^2 \neq 1$, så $o(f) = 4$, men $4 \nmid 342$.]		×

2a) (1p) Vi skall ge ett uttryck för antalet banor då gruppen G verkar på mängden X (G, X ändliga).

Lösning:

Antalet banor är ("Burnsides lemma") $\frac{1}{|G|} \sum_{g \in G} |F(g)|$,
där $F(g) = \{x \in X \mid gx = x\} (= X_g)$.

b) (1p) Vi söker antalet $f \in F$, en kropp med $|F| = 7^3 = 343$, med multiplikativ ordning 57.

Lösning:

$(F \setminus \{0\}, \cdot)$ är en cyklisk grupp av ordning $7^3 - 1 = 342 = 6 \cdot 57$, så $57 \mid |F \setminus \{0\}|$.
Det betyder (känd sats) att det finns precis
 $\phi(57) = \phi(3 \cdot 19) = 2 \cdot 18 = 36$ element av ordning 57 i F .

Svar: Det sökta antalet är 36.

c) (1p) Vi skall ge definitionen av **karakteristiken** för en ändlig kropp.

Lösning:

Det minsta $m \in \mathbb{Z}_+$ som gör $\underbrace{1 + 1 + \dots + 1}_{m \text{ st}} = 0$ i kroppen F kallas karakteristiken för F .

3) (3p) Vi söker alla $x \in \mathbb{Z}$ som uppfyller $x^2 \equiv 341 \pmod{572}$.

Lösning:

$572 = 4 \cdot 11 \cdot 13$, så $\equiv_{572}$ gäller omm $\equiv_4, \equiv_{11}$ och $\equiv_{13}$ (Kinesiska restsatsen).

Prövning ger att $x^2 \equiv_4 341 \equiv_4 1$ omm $x \equiv_4 \pm 1$,

$x^2 \equiv_{11} 341 \equiv_{11} 0$ omm $x \equiv_{11} 0$ och

$x^2 \equiv_{13} 341 \equiv_{13} 3$ omm $x \equiv_{13} \pm 4$.

För att finna motsvarande $x \in \mathbb{Z}$ bestämmer vi $y_1 \equiv_4 1, \equiv_{11} 0, \equiv_{13} 0$ och

$y_3 \equiv_4 0, \equiv_{11} 0, \equiv_{13} 1$:

$y_1 = 11 \cdot 13 \cdot b_1 \equiv_4 1 \Leftrightarrow 3b_1 \equiv_4 1$. Vi kan ta $b_1 = -1$, så $y_1 = -143$,

$y_3 = 4 \cdot 11 \cdot b_3 \equiv_{13} 1 \Leftrightarrow 5b_3 \equiv_{13} 1$. Vi tar $b_3 = 8$, så $y_3 = 352$.

Vi får alla lösningar mod 572: $x = (\pm 1) \cdot (-142) + (\pm 4) \cdot 352 \equiv_{572} \pm 121, \pm 165$.

Svar: Alla sådana x ges av $\pm 121, \pm 165 + 572n, n \in \mathbb{Z}$ godtyckligt.

(Samma mängd x kan uttryckas med $x = 121, 165, 407, 451 + 572n, n \in \mathbb{Z}$ godtyckligt.)

4) (3p) Vi har $f(n) = \sum_{d|n} \mu(d) \operatorname{sgd}(\frac{n}{d}, m)$, för ett givet $m \in \mathbb{Z}_+$, och söker $g(n) = \sum_{d|n} f(d)$. (Summer över n :s positiva delare.)

Lösning:

Enligt Möbius inversionsformel är $g(n) = \operatorname{sgd}(n, m)$. ($h = 1 * f \Leftrightarrow f = \mu * h$.)

Svar: $g(n) = \operatorname{sgd}(n, m)$ för alla $n \in \mathbb{Z}_+$.

5) $R = \mathbb{Z}_5[x]/(k(x))$ med $k(x) = x^4 + 2x^3 + 4x^2 + 4 \in \mathbb{Z}_5[x]$ och vi (a, 1p) söker $|R|$ och (b, 2p) ska avgöra om $\alpha^2 + 2\alpha + 3 \in R$ är inverterbart och i så fall bestämma dess invers. $\alpha \in R$ motsvarar polynomet x (dvs är $[x]$).

Lösning:

a. Elementen i R representeras bijektivt av polynom i $\mathbb{Z}_5[x]$ med grad $< \deg k(x) = 4$, så $|R| = 5^4 = 625$ (4 koefficienter i $\mathbb{Z}_5$ bestämmer polynom av grad högst 3).

b. Vi låter $f(x) = x^2 + 2x + 3$ och söker (Euklides algoritm) $\operatorname{sgd}(f(x), k(x))$ i $\mathbb{Z}_5[x]$.

Polynomdivision ger $k(x) = f(x)(x^2 + 1) + g(x)$, $g(x) = 3x + 1$ och

$f(x) = g(x)2x + 3$, så 3 är en sgd och

$3 = f(x) - 2x(k(x) - (x^2 + 1)f(x)) = (2x^3 + 2x + 1)f(x) + 3xk(x)$.

2· i båda leden ger $f(x)(4x^3 + 4x + 2) + xk(x) = 1$, så $f(x)(4x^3 + 4x + 2) \equiv_{k(x)} 1$,

dvs $f(x)^{-1} = 4x^3 + 4x + 2$ i R .

Svar a: $|R| = 625$, **b:** Inverterbart, $(\alpha^2 + 2\alpha + 3)^{-1} = 4\alpha^3 + 4\alpha + 2$.