Matematik, KTH

Svar och lösningsförslag till ks3, 9 oktober 2017, i SF1688 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 en ändlig grupp G verkar på en ändlig mängd X är antalet banor säkert en delare till $\lvert G\rvert$, gruppens ordning. [Nejdå. X (och därmed antalet banor) kan vara obegränsat stor.]		X
b)	Om $m < n \in \mathbb{Z}_+$ och $n = mq+r$ (med $q, r \in \mathbb{Z}$ och $0 \le r < m$), är m säkert inverterbart i $\mathbb{Z}_n$ omm r är det i $\mathbb{Z}_m$. [Ja, båda precis om $\mathrm{sgd}(m, n) = \mathrm{sgd}(r, m) = 1$.]	X	
c)	Om $a, m \in \mathbb{Z}_+$ och $\mathrm{sgd}(a, m) = 1$, är det säkert så att $a^m \equiv a \pmod{m}$. [Nej, men för primtal m. $3^4 \equiv 1 \not\equiv 3 \pmod{4}$.]		X
d)	En kommutativ ring R är en kropp omm det för alla $a, b \in R \setminus \{0\}$ finns precis ett $x \in R$ med $ax = b$. [Ja. $x = a^{-1}b$ om R är en kropp. $ax = 1$ med $x \in R$ ger a inverterbart.]	X	
e)	Karakteristiken för en ändlig kropp är alltid ett primtal. [Javisst, så är det.]	X	
f)	I varje kvotring $F[x]/(k(x))$ är 0 en produkt av två nollskilda element omm polynomet $k(x)$ är reducibelt. [Ja. Om $k(x)$ är reducibelt: $k(x) = f(x)g(x)$ (med $[f(x)], [g(x)] \neq 0$), $[f(x)][g(x)] = 0$. Om $k(x)$ är irreducibelt: $F[x]/(k(x))$ en kropp, så $[f(x)][g(x)] = 0$, $[f(x)] \neq 0$ ger $[g(x)] = 0$.]	X	

2a) (1p) $(G, *)$, $|G| = 52$, är en cyklisk grupp.
Vi söker antalet $g \in G$ med jämn ordning.

Lösning:
Alla element i G har en ordning som delar $|G|$ (för alla grupper G) och om $d \,\Big|\, |G|$ är antalet element av ordning d precis $\phi(d)$ (för cykliska grupper G).
Jämna delare till 52 är 2, 4, 26 och 52, så sökt är $\phi(2) + \phi(4) + \phi(26) + \phi(52) =$
$= 2(1-\frac{1}{2}) + 4(1-\frac{1}{2}) + 26(1-\frac{1}{2})(1-\frac{1}{13}) + 52(1-\frac{1}{2})(1-\frac{1}{13}) = 1+2+12+24 = 39.$

Svar: 39 av elementen i G har jämn ordning.

(Alternativt: om $G = \langle x \rangle$ är $o(x^i)$ jämn omm $4 \nmid i$, så för alla utom $\frac{52}{4} = 13$ element.)

---

b) (1p) $\sigma(n)$ ($n \in \mathbb{Z}_+$) är summan av n:s positiva delare. Vi söker $\sum_{d|n} \mu(d)\sigma(\frac{n}{d})$.

Lösning:
$\sigma(n) = \sum_{d|n} id(d)$, så enligt Möbius inversionsformel ($\sigma = 1 * id \Leftrightarrow id = \mu * \sigma$) är $\sum_{d|n} \mu(d)\sigma(\frac{n}{d}) = id(n) = n$.

Svar: Summan är n för alla $n \in \mathbb{Z}_+$.

---

c) (1p) Vi söker strukturen för $(F \setminus \{0\}, \cdot)$, då $(F, +, \cdot)$ är en ändlig kropp.

Lösning:

Svar: $(F \setminus \{0\}, \cdot)$ är en cyklisk grupp.

---

3) (3p) Vi söker antalet väsentligt olika färgningar av hörnen i en regelbunden femhörning, då det finns k färger att tillgå.

Lösning:

Vi använder Burnsides lemma (Thm. 21.4 i kursboken).
Gruppen G av symmetrirotationer för femhörningen har 10 element:

- id, identitetsavbildningen,
- 4 st vridningar vinklar $i \cdot \frac{2\pi}{5}$ ($i = 1, 2, 3, 4$) kring en axel genom femhörningens medelpunkt, vinkelrät mot dess plan (de har alla ordning 5 (primtal)) och
- 5 st vändningar kring axlar genom ett hörn och motstående sidas mittpunkt.

Vi behöver $|F(g)|(= |X_g|)$ för alla $g \in G$.

typ av g	antal sådana	cykler i dess permutation av hörnen	$\|F(g)\|$ $=k^{\text{antalet cykler}}$
id	1	$[1^5]$	k^5
vrid $i \cdot \frac{2\pi}{5}$	4	$[5]$	k
vänd	5	$[1\,2^2]$	k^3

Enligt lemmat är antalet banor för G:s verkan på färgningarna = antalet väsentligt olika färgningar $= \frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{10}(k^5 + 4\cdot k + 5\cdot k^3)$.

Svar: Hörnen kan färgas på $\frac{1}{10}(k^5 + 5k^3 + 4k)$ väsentligt olika sätt.

---

4) (3p) Vi skall finna det minsta $n \in \mathbb{Z}_+$ med $290^n = 348$ i $\mathbb{Z}_{396}$, eller förklara varför inget sådant n finns.

Lösning:

Enligt Kinesiska restsatsen är $(\mathbb{Z}_{396}, +, \cdot) \cong (\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_{11}, +, \cdot)$.
Om isomorfin kallas φ fås $\varphi(290) = (2, 2, 4)$, $\varphi(348) = (0, 6, 7)$, så de sökta n är precis de som uppfyller $2^n = 0$ i $\mathbb{Z}_4$, $2^n = 6$ i $\mathbb{Z}_9$ och $4^n = 7$ i $\mathbb{Z}_{11}$.
I $\mathbb{Z}_9$ är $2^1 = 2$, $2^2 = 4$, $2^3 = 1$, $2^4 = 2, \ldots$, så $2^n \neq 6$ i $\mathbb{Z}_9$ för alla $n \in \mathbb{Z}_+$ och det finns inget $n \in \mathbb{Z}_+$ som uppfyller att $290^n = 348$ i $\mathbb{Z}_{396}$.

Svar: Det finns inga sådana n.

---

5) (3p) Vi har $f(x) = x^5 + x^4 + x^3 + 2x^2 + 1$ och $g(x) = x^4 + 2x^3 + x^2 + x + 1$ i $\mathbb{Z}_3[x]$ och söker deras moniska största gemensamma delare $k(x)$.

Lösning:

Vi använder Euklides algoritm för att finna en största gemensam delare.
Polynomdivisioner ger $f(x) = g(x)\cdot(x + 2) + h(x)$ med $h(x) = 2x^3 + 2x^2 + 2$,
$g(x) = h(x)\cdot(2x + 2) + 0$
$h(x)$ är alltså en största gemensam delare till $f(x)$ och $g(x)$. Den moniska sgd:n $k(x)$ får vi genom att multiplicera med $2^{-1} = 2$. Den blir $k(x) = x^3 + x^2 + 1$.

Svar: $k(x) = x^3 + x^2 + 1$.
