Matematiska Institutionen
KTH

Diskret Matematik för F3 och F1spec (5B1203)
Lösningar till tentamensskrivning, onsdag den 18 augusti 2004.

1. $n = 91 = 7 \cdot 13 \Rightarrow \varphi(n) = 6 \cdot 12 = 72,\ e = 5.$

(a) $3^5 \equiv 61 \pmod{91} \Rightarrow E(3) = 61.$

$6^5 \equiv 41 \pmod{91} \Rightarrow E(6) = 41.$

(b) Minsta positiva lösning till $5d \equiv 1 \pmod{72}$ är $d = 29$:

$3^{29} \equiv 61 \pmod{91} \Rightarrow D(3) = 61.$

$D(41) = 6$, eftersom $E(6) = D^{-1}(6) = 41$ (enl. del a)

2. Tag bort en kant ur cykeln. Detta ger en ny graf G' med 87 noder, 79 kanter, ingen cykel, och lika många sammanhängande komponenter som G. Varje sammanhängande komponent i G' är ett träd (då cykler saknas), och har därför # noder - # kanter $= 1$. Eftersom $87 - 79 = 8$ måste G' (och därför även G) ha 8 komponenter.

3. (a) Det är alla tal som börjar med 355242, 3554, 4, eller 5.

Antal som börjar med 355242: 1
Antal som börjar med 3554: 3
Antal som börjar med 4: $\binom{6}{2,2,1,1} = 6!/4 = 180$
Antal som börjar med 5: $\binom{6}{2,1,1,1,1} = 6!/2 = 360$
Totalt: $1 + 3 + 180 + 360 = 544$.

(b) Problemet kan beskrivas så att vi har en linjär konfiguration

$$L\ 0\ L\ 0\ L\ 0\ L\ 0\ L\ 0\ L$$

av 5 nollor och 6 lådor L. Vi lägger först en etta i var och en av de fyra mellersta lådorna. Ytterligare 6 ettor skall sedan fritt fördelas till de 6 lådorna. Detta kan göras på $\binom{6+6-1}{6} = 462$ olika sätt.

Svar: 462.

4. (a) Enligt faktorsatsen gäller (då $\mathbb{Z}_3$ är en kropp): $x - b$ delar $p(x) \Leftrightarrow p(b) = 0$. Därför: Inga förstagradsfaktorer $\Leftrightarrow$ inga rötter i $\mathbb{Z}_3$

$$\Leftrightarrow \begin{cases} a_0 \neq 0 & \text{(dvs. 0 är ej rot)} \\ \sum_{i=0}^{n} a_i \neq 0 & \text{(dvs. 1 är ej rot)} \\ \sum_{i=0}^{n} (-1)^i a_i \neq 0 & \text{(dvs. } -1 \text{ är ej rot)} \end{cases}$$

(b) Med hjälp av (a) bestäms direkt alla moniska irreducibla 2-gradspolynom i $\mathbb{Z}_3[x]$: $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2$. De icke-moniska erhålls sedan genom multiplikation med 2, totalt alltså 6 polynom.

5. Vi observerar att

$$c_{10} = \sum_{i=1}^{9} ic_i \pmod{11} \quad \Leftrightarrow \quad \sum_{i=1}^{10} ic_i = 0 \pmod{11}$$

(a) Om c_j och c_k byter plats, $c_j \neq c_k$, så blir checksumman

$$\sum_{i=1, i\neq j,k}^{10} ic_i + jc_k + kc_j \equiv -jc_j - kc_k + jc_k + kc_j = (j-k)(c_k - c_j) \neq 0 \pmod{11}.$$

Här följer den sista olikheten av att $(j-k) \neq 0 \pmod{11}$ och $(c_k - c_j) \neq 0 \pmod{11}$, och av att $\mathbb{Z}_{11}$ är en kropp eftersom 11 är ett primtal.

(b) Om c_j ändras till c'_j så blir checksumman

$$\sum_{i=1, i\neq j}^{10} ic_i + jc'_j \equiv jc'_j - jc_j = j(c'_j - c_j) \neq 0 \pmod{11}.$$

Här följer den sista olikheten av att $j \neq 0 \pmod{11}$ och $(c'_j - c_j) \neq 0 \pmod{11}$, eftersom $\mathbb{Z}_{11}$ är en kropp.

6. Symmetrigruppen har 4 element: vridning $0, 90, 180, 270$ grader runt symmetriaxeln genom pyramidens spets. Gruppen verkar på mängden av färgningar av pyramiden, och enligt formeln för antalet banor (Biggs sid. 288) får vi svaren

(a) Antalet distinkta färgläggningar $= \frac{1}{4}(m^5 + m^2 + m^3 + m^2) = \frac{m^2}{4}(m^3 + m + 2)$.

(b) Antalet distinkta färgläggningar i vilka basens färg inte förekommer på någon triangulär sida $= m \cdot \frac{1}{4}((m-1)^4 + (m-1) + (m-1)^2 + (m-1))$
$= \frac{m(m-1)}{4}((m-1)^3 + m + 1)$.

7. (a) Vi har att

$$ax + b = ay + b \quad \Rightarrow \quad a(x-y) = 0 \quad \Rightarrow \quad x = y,$$

där den sista implikationen beror på att $a \neq 0$ och $\mathbb{F}_q$ är en kropp. Avbildningen $f_{a,b}$ är således injektiv, och eftersom $\mathbb{F}_q$ är ändlig så måste $f_{a,b}$ vara bijektiv, eller med andra ord, $f_{a,b}$ är en permutation.

(b) *Binär operation:* Om $f_{a,b} \in G$ och $f_{c,d} \in G$ så gäller att även $f_{a,b} \circ f_{c,d} \in G$, eftersom $f_{a,b} \circ f_{c,d}(x) = f_{a,b}(f_{c,d}(x)) = a(cx+d) + b = f_{ac,ad+b}(x)$.
Associativitet: Sammansättning av avbildningar är alltid associativ. Kolla!
Enhetselement: $f_{1,0}(x) = x$ är identitetsavbildningen.
Inverser: $f_{a,b} \circ f_{c,d}(x) = a(cx+d) + b = x$, för alla $x \in \mathbb{F}_q$, har lösningen $c = a^{-1}$, $d = -b \cdot a^{-1}$. Således: $(f_{a,b})^{-1} = f_{a^{-1}, -ba^{-1}}$.

(c) Elementet a kan väljas på $q-1$ olika sätt och b på q olika sätt. Om vi visar att dessa val ger upphov till distinkta avbildningar $f_{a,b}$, så följer att gruppen G har $q(q-1)$ element.
Antag att $f_{a,b} = f_{c,d}$, dvs $ax + b = cx + d$ för alla $x \in \mathbb{F}_q$. Då följer

$$(a-c)x = d - b, \quad \forall x \in \mathbb{F}_q.$$

Om $a \neq c$ så skulle denna ekvation ha endast en lösning $x = (a-c)^{-1}(d-b)$, vilket ger en motsägelse. Alltså: $a = c$, och då följer även $b = d$.

(d) $G_c = \{f_{a,b} \in G : f_{a,b}(c) = c\}$ och $ac + b = c \quad \Rightarrow \quad (a-1)c = -b$.
Om $c = 0$: Då $b = 0$, och a kan väljas på $q-1$ olika sätt.
Om $c \neq 0$: För varje val av a (det finns $q-1$ sådana val) finns det exakt ett passande b.
`Alternativt:` Gruppen G verkar transitivt (dvs med bara en bana) på mängden $\mathbb{F}_q$ (detta följer av (f)). Således, (se Biggs sid. 286)

$$|G_c| = \frac{|G|}{|\mathbb{F}_q|} = \frac{q(q-1)}{q} = q - 1.$$

(e) $G_0 = \{f_{a,0} : a \in \mathbb{F}_q^*\}$ (se del (d)). Låt g vara ett primitivt element i $\mathbb{F}_q^*$. Således, $\mathbb{F}_q^* = \{g^k : k = 1, \ldots, q-1\}$. Eftersom $f_{a_1,0} \circ f_{a_2,0} = f_{a_1 a_2,0}$ kan vi dra slutsatsen att G_0 genereras av $f_{g,0}$.

(f) Uppgiften innebär att vi skall lösa systemet $\begin{cases} ax_1 + b &= x_2 \\ ay_1 + b &= y_2 \end{cases}$

Vi har: $\quad a(x_1 - y_1) = x_2 - y_2 \quad \Rightarrow \quad a = \dfrac{x_2 - y_2}{x_1 - y_1} \neq 0$ och $b = x_2 - ax_1$.

Således finns det alltid exakt en lösning.

8. (a) Låt p vara det minsta primtal som delar n. Då gäller:

$$\varphi(n) \leq n(1 - \frac{1}{p}) \leq n - \frac{n}{\sqrt{n}} = n - \sqrt{n}.$$

(b) Utgående från primtalsfaktoriseringen $n = p_1^{e_1} \cdots p_k^{e_k}$, där $p_i \geq 3$ och $e_i \geq 1$:

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1) \geq \prod_{i=1}^{k} p_i^{e_i - 1/2} \geq \prod_{i=1}^{k} p_i^{e_i/2} = \sqrt{n}.$$

Vi har här använt de elementära olikheterna $x - 1 \geq \sqrt{x}$ för $x \geq 3$, och $x - 1/2 \geq x/2$ för $x \geq 1$.