(Diskret matte D, ht16: F30, den sista, on 14 dec 2016)

Några problem (de flesta gamla tentauppgifter) som repetition:

1. Definiera den binära operationen $\circ$ på $\mathbb{Z}$ enligt $m \circ n = m + n + 3$ för $m, n \in \mathbb{Z}$. Visa att $(\mathbb{Z}, \circ)$ är en grupp och att den är isomorf med $(\mathbb{Z}, +)$.

Definitionen av $\circ$ ger att $(m+3)+(n+3) = m \circ n + 3$. Definiera $\alpha : \mathbb{Z} \to \mathbb{Z}$ enligt $\alpha(n) = n + 3$. α är en bijektion (ty den har en invers, given av $\alpha^{-1}(n) = n - 3$) och enligt ovan gäller $\alpha(m \circ n) = \alpha(m) + \alpha(n)$. Det betyder att $(\mathbb{Z}, \circ)$ har samma struktur som $(\mathbb{Z}, +)$ (speciellt är den en grupp, med identitet (nolla) $\alpha^{-1}(0) = -3$ och inversen till n given av $\alpha^{-1}(-\alpha(n)) = \alpha^{-1}(-n+3) = -(n+3) - 3 = -n - 6$ och α är en isomorfi mellan grupperna.

Saken är klar, en isomorfi $(\mathbb{Z}, \circ) \to (\mathbb{Z}, +)$ ges av $\alpha(n) = n + 3$.
(Man kan förstås också verifiera gruppaxiomen för $(\mathbb{Z}, \circ)$ direkt.)

2. Låt H, K vara delgrupper till en ändlig grupp G. Om $|H|$ och $|K|$ är relativt prima och a, $b \in G$, vilka värden är möjliga för $|aH \cap bK|$?

$aH \cap bK$ kan vara tom (t.ex. om $H = \{1\}$ och $a \notin bK$).
Om $c \in aH \cap bK$ är $aH = cH$ och $bK = cK$, ty (vänster)sidoklasser är identiska eller disjunkta. Men $cH \cap cK = c(H \cap K)$ (ty $g \mapsto cg$ är injektiv i en grupp). Om $g \in H \cap K$ gäller $g \in H$, K, så $o(g) \mid |H|$, $|K|$ och alltså $o(g) \mid \text{sgd}(|H|, |K|) = 1$, så $o(g) = 1$, dvs $g = 1$ och $|H \cap K| = 1$. Det ger $aH \cap bK = \{c \cdot 1\} = \{c\}$, så $|aH \cap bK| = 1$ i det fallet.

Svar: $|aH \cap bK|$ kan vara 0 eller 1 om $\text{sgd}(|H|, |K|) = 1$.

3. Visa att i en ring $(R, +, \cdot)$ där $x \cdot x = x$ för alla $x \in R$, är $x + x = 0$ för alla $x \in R$.

För ett godtyckligt $a \in R$ gäller $a \cdot a = a$ och $(a+a) \cdot (a+a) = a + a$. Med axiom för en ring (distributivitet) fås $(a+a) \cdot (a+a) = (a+a) \cdot a + (a+a) \cdot a = (a \cdot a + a \cdot a) + (a \cdot a + a \cdot a) = (a+a) + (a+a) = a + a$. Eftersom $(R, +)$ är en grupp ger detta att $a + a = 0$, så (a var godtyckligt) **saken är klar**.
(Dessutom följer det att R är kommutativ, ty för alla $a, b \in R$: $a + b = (a+b) \cdot (a+b) =$
$= \ldots = a + a \cdot b + b \cdot a + b \Rightarrow a \cdot b + b \cdot a = 0 = a \cdot b + a \cdot b$ (enligt ovan) etc.)

4. Låt p och q vara primtal sådana att $q \mid 2^p - 1$. Visa att $q > p$.

$q \mid 2^p - 1$ betyder att $2^p = 1$ i $\mathbb{Z}_q$, dvs $o(2) = p$ i $\mathbb{Z}_q$ (p är ju ett primtal och $o(2) \neq 1$). Men $(\mathbb{Z}_q \setminus \{0\}, \cdot)$ är en grupp av ordning $q - 1$, så $p \mid q - 1 (> 0)$ och **påståendet följer**.

5a. Faktorisera $f(x) = x^4 + 2x^2 + x + 2 \in \mathbb{Z}_3[x]$ i irreducibla faktorer.
b. I kroppen $F = \{b_1\alpha + b_0 \mid b_0, b_1 \in \mathbb{Z}_3\}$, med $g(\alpha) = 0$ för ett lämpligt andragradspolynom, är alla irreducibla faktorer till $f(x)$ av första graden. Finn ett sådant $g(x)$ och en generator för F:s multiplikativa grupp $(F \setminus \{0\}, \cdot)$.

$f(x) = x^4 + 2x^2 + x + 2$ har enligt faktorsatsen en förstagradsfaktor precis om det har ett nollställe. $f(0) = 2$, men $f(1) = 0$, så $f(x)$ är delbart med $x - 1 = x + 2$. Division ger att $f(x) = (x+2)\varphi(x)$ med $\varphi(x) = x^3 + x^2 + 1$. Vi söker på samma sätt nollställen till $\varphi(x)$. ($\varphi(0) \neq 0$ eftersom $f(0) \neq 0$ och) $\varphi(1) = 0$, så $\varphi(x) = (x+2)\psi(x)$, där division ger $\psi(x) = x^2 + 2x + 2$. $\psi(1) = 2, \psi(2) = 1$, så $\psi(x)$ saknar förstagradsfaktor och är alltså (eftersom det är av grad ≤ 3) irreducibelt (liksom $x + 2$).
För att $\psi(x)$ skall kunna faktoriseras måste det ha ett nollställe, så vi väljer $g(x) = x^2 + 2x + 2$. Då är i F $\alpha^2 + 2\alpha + 2 = 0$, så $\alpha^2 = \alpha + 1$. Gruppen $(F \setminus \{0\}, \cdot)$ har ordning 8, så dess element har ordning 1, 2, 4 eller 8. Generatorer är precis de som har ordning 8, så $g \in F \setminus \{0\}$ är en generator omm $g^4 \neq 1$. $\alpha^4 = (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 + 2\alpha + 1 = 2 \neq 1$, så α är en generator.

Svar a: $f(x) = (x+2)^2(x^2 + 2x + 2)$,
b: Med $g(x) = x^2 + 2x + 2$ är α en generator.

(Division av $g(x)$ med $x - \alpha = x + 2\alpha$ ger faktoriseringen av $f(x)$ i $F[x]$:
$f(x) = (x+2)^2(x + 2\alpha)(x + \alpha + 2)$.)

6. I vart och ett av de sex hörnen på en kloss i form av ett triangulärt prisma sitter en färgad kula. Hur många väsentligt olika (dvs så att de inte blir lika hur man än vrider klossen i rummet) sätt att fördela kulornas färger finns det, om man har kulor av k st färger att tillgå?
Klossens sidoytor är två motstående liksidiga trianglar och tre kvadrater.

Vi använder Burnsides lemma (Thm 21.4 i Biggs).
Prismats grupp av symmetrirotationer har 6 element ($|G_x| = 1, |Gx| = 6$ för alla hörn x): Identitetselementet (bevarar alla konfigurationer, $|F(id)| = k^6$), två rotationer $\pm\frac{2\pi}{3}$ kring axeln genom de triangulära ytornas mittpunkter (bevarar konfigurationer med samma färg på kulorna vid varje triangel, $|F(g)| = k^2$) och tre rotationer π kring axlar genom mittpunkten av en kvadrat och motstående kant (bevarar konfigurationer med motstående hörn i kvadraten och kantens hörn parvis likfärgade, $|F(g)| = k^3$).
Lemmat ger antalet väsentligt olika färgningar, $\frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{6}(k^6 + 2k^2 + 3k^3)$.

Svar: Det sökta antalet fördelningar är $\frac{1}{6}(k^6 + 3k^3 + 2k^2)$.
(16 för $k = 2$, 138 för $k = 3$, 720 för $k = 4$, ...)

7. Finn en kontrollmatris H för en linjär binär kod $\mathcal{C}$ som rättar ett fel, med $|\mathcal{C}| = 16, \quad 1011010 \in \mathcal{C},\ 0011000 \notin \mathcal{C}$.

$\mathcal{C}$ har tydligen längd 7 och dimension 4 ($16 = 2^4$), så H:s rang skall vara 3. Vi tar alltså H som en 3×7-matris ($\mathcal{C}$ blir en Hammingkod).
$1011010 \in \mathcal{C}$ ger att summan av kolonnerna 1, 3, 4 och 6 är $\mathbf{0} = \left[\begin{smallmatrix}0\\0\\0\end{smallmatrix}\right]$.
$0011000 \notin \mathcal{C}$ ger att summan av kolonnerna 3 och 4 inte är $\mathbf{0}$.
Så man kan ta (summan av 1 och 6)=(summan av 3 och 4)$\neq \mathbf{0}$ och fylla ut med alla kolonner olika och $\neq \mathbf{0}$ (för att koden skall rätta ett fel), t.ex.
Svar: Man kan ta $\boldsymbol{H} = \left[\begin{smallmatrix}1&0&0&0&1&1&1\\0&1&0&1&0&1&1\\0&0&1&1&1&0&1\end{smallmatrix}\right]$.

8. Finn det minsta talet $e \geq 100$ sådant att $(1189, e)$ kan användas som krypteringsnyckel i ett RSA-system. Finn också ett tal d, så att $(1189, d)$ är en motsvarande dekrypteringsnyckel. [$1189 = 29 \cdot 41$]

$n = 1189 = 29 \cdot 41$ ger $m = 28 \cdot 40 = 2^5 \cdot 5 \cdot 7 = 1120$. Villkoret på e är då $\text{sgd}(1120, e) = 1$, vilket inte är uppfyllt för $e = 100$, men väl för $\boldsymbol{e = 101}$ (primtal).
För att finna motsvarande d används Euklides algoritm: $1120 = 101 \cdot 11 + 9$; $\quad 101 = 9 \cdot 11 + 2$; $\quad 9 = 2 \cdot 4 + 1$ så $1 = 9 - 4 \cdot 2 = 9 - 4 \cdot (101 - 11 \cdot 9) = -4 \cdot 101 + 45 \cdot 9 = -4 \cdot 101 + 45 \cdot (1120 - 11 \cdot 101) = 45 \cdot 1120 - 499 \cdot 101 = 45 \cdot 1120 - 101 \cdot 1120 + 1120 \cdot 101 - 499 \cdot 101 = 621 \cdot 101 - 56 \cdot 1120$, så vi kan välja $\boldsymbol{d = 621}$.

Svar: $\boldsymbol{e = 101}$, $\boldsymbol{d = 621}$.
(För att finna **alla** användbara d: $x^{e\cdot d} \equiv_{p\cdot q} x$ alla $x \Leftrightarrow (p-1), (q-1) \mid (e \cdot d - 1)$ (kinesiska restsatsen, grupperna $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ är cykliska för p primtal) $\Leftrightarrow \text{mgm}(p-1, q-1) \mid (e \cdot d - 1)$, så $d = e^{-1}$ i $\mathbb{Z}_{\text{mgm}(p-1,q-1)}$. I vårt fall: $d = 101^{-1} = 61$ i $\mathbb{Z}_{280}$, så alla möjliga värden: $d = 61 + 280n$, $n \in \mathbb{N}$.)