(Diskret matte D, ht17: F21, den sista, fr 13 okt 2017)

Några problem (de flesta gamla tentauppgifter) som repetition:

1. Hur många ytor kan en reguljär, eulersk, enkel, plan graf med v hörn dela in planet i?

Om grafen är k-reguljär kan k vara 0, 2 eller 4 (jämnt, ty eulersk graf, inte ≥ 6, ty varje planär graf har minst ett hörn med valens ≤ 5).
$k = 0$: isolerade hörn, så $r = 1$,
$k = 2$: C_v, ty bara en komponent i en eulersk graf utan isolerade hörn, så $r = 2$,
$k = 4$: $e = 2v$ (eftersom $\sum_{x \in V} \delta(x) = 2|E|$), så Eulers formel (plan, sammanhängande graf) ger $v - 2v + r = 2$, så $r = 2 + v$.

Svar: Möjliga antal ytor är 1, 2 och $2 + v$.

2. De 52 korten i en kortlek delas upp i 13 högar med 4 kort i varje. Visa att man kan dra ett kort slumpmässigt ur den första högen och komplettera med ett kort var ur de övriga högarna, så att man får kort med 13 olika valörer.

Låt $G = (X \cup Y, E)$ med $X = \{$de 12 återstående högarna$\}$, $Y = \{$de 12 återstående valörerna$\}$ och kanter från varje hög till dess ingående valörer i Y.
k st av högarna i X innehåller minst k av valörerna i Y ($4k$ kort, varav högst 3 av den redan dragna valören). Halls sats ger påståendet. **Saken är klar.**

3. Minns att **fibonaccitalen** $\{F_n\}_{n \in \mathbb{N}}$ definieras rekursivt av $F_0 = 0$, $F_1 = 1$ och $F_{n+2} = F_{n+1} + F_n$ för $n \in \mathbb{N}$.
Visa att $\text{sgd}(F_m, F_n) = F_{\text{sgd}(m,n)}$ för alla $m, n \in \mathbb{N}$.

Induktion över $m \geq n$. Om $m = n$ eller $n = 0$ är påståendet uppenbart.
Låt $m > n > 0$. $\left(\begin{smallmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{smallmatrix}\right) \overset{*}{=} \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)^m = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{m-n} \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)^n$ ($*$ visas med induktion),
så $F_m = F_{m-n}F_{n+1} + F_{m-n-1}F_n$. Det ger $\text{sgd}(F_m, F_n) = \text{sgd}(F_{m-n}, F_n)$
(ty $\text{sgd}(F_{n+1}, F_n) = 1$, visas med induktion).
Induktionsantagandet (underförstått) ger $\text{sgd}(F_{m-n}, F_n) = F_{\text{sgd}(m-n,n)} = F_{\text{sgd}(m,n)}$.

4. 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.)

5. 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 $\text{sgd}(|H|, |K|) = 1$.

6. 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 $a + a = 0$ för ett godtyckligt $a \in R$. **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.)

7. 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 $p \mid q-1 (> 0)$ så $q - 1 \geq p$ dvs $q > p$. **Saken är klar.**

8. Hur många väsentligt olika färgningar med högst k färger av **kanterna** i en ikosaeder finns det?

Burnsides lemma (Thm 21.4 i Biggs). För varje (typ av) symmetrirotation g:

typ av g	g:s permutation av ikosaederns kanter	antal sådana g	$\lvert F(g)\rvert = k^{\text{antalet cykler}}$
id	$[1^{30}]$	1	k^{30}
rot $hh \pm \frac{2\pi}{5}$	$[5^6]$	12	k^6
rot $hh \pm \frac{4\pi}{5}$	$[5^6]$	12	k^6
rot $kk\,\pi$	$[1^2\,2^{14}]$	15	k^{16}
rot $ss \pm \frac{2\pi}{3}$	$[3^{10}]$	20	k^{10}

("rot $xx\,v$": rotation vinkeln v kring en axel genom ikosaederns och sidors(s), kanters(k) eller hörns(h) medelpunkter.)
$|F(g)|$: antalet g-invarianta (dvs samma färg på alla kanter i samma cykel) färgningar.
Lemmat ger antalet färgningar: $\frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{60}(k^{30} + 15k^{16} + 20k^{10} + 24k^6)$.

Svar: Det sökta antalet är $\frac{1}{60}(k^{30} + 15k^{16} + 20k^{10} + 24k^6)$.
($k = 2$ ger antalet olika färgningar med två färger: 17 912 448.)

9a. 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 $g(x)$, är alla irreducibla faktorer till $f(x)$ (betraktat som ett element i $F[x]$) av första graden. Finn ett sådant $g(x)$ och en generator för F:s multiplikativa grupp $(F \setminus \{0\}, \cdot)$.
(Gjordes inte på föreläsningen.)

$f(x) = x^4 + 2x^2 + x + 2$ 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 $\beta \in F \setminus \{0\}$ är en generator omm $\beta^4 \neq 1$. $\alpha^4 = (\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 + 2\alpha + 1 = 2 \neq 1$, 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 $f(x) = (x+2)^2(x+2\alpha)(x+\alpha+2)$ i $F[x]$.)

10. Finn en kontrollmatris H för en linjär binär kod $\mathcal{C}$ som rättar ett fel, med $|\mathcal{C}| = 16$ och 1011010, 1100010 $\in \mathcal{C}$.
(Gjordes inte på föreläsningen.)

$\mathcal{C}$ 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 $\mathbf{0} = \left[\begin{smallmatrix}0\\0\\0\end{smallmatrix}\right]$.
1100010 $\in \mathcal{C}$ ger att summan av kolonnerna 1, 2 och 6 är $\mathbf{0}$.
Så (summan av 3 och 4)=(summan av 1 och 6)=kolonn 2 (alla olika) och 5 och 7 får vara de två lediga nollskilda kolonnerna (för att koden skall rätta ett fel), t.ex.

Svar: Man kan ta $H = \left[\begin{smallmatrix}1&0&0&0&1&1&1\\0&1&0&1&0&1&1\\0&0&1&1&1&0&1\end{smallmatrix}\right]$.

11. 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. [$1189 = 29 \cdot 41$]

(Gjordes inte på föreläsningen.)

$n = 1189 = 29 \cdot 41$ 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). Ett motsvarande d uppfyller $e \cdot d \equiv_{1120} 1$ och fås med Euklides algoritm:
$1120 = 101 \cdot 11 + 9$; $101 = 9 \cdot 11 + 2$; $9 = 2 \cdot 4 + 1$, så $1 = 9 - 4 \cdot (101 - 11 \cdot 9) =$
$= -4 \cdot 101 + 45 \cdot (1120 - 11 \cdot 101) = 45 \cdot 1120 - 499 \cdot 101 = (45 - 101) \cdot 1120 +$
$+(1120 - 499) \cdot 101 = 621 \cdot 101 - 56 \cdot 1120$. Vi kan välja $d = 621$.

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: $d = 61 + 280n$, $n \in \mathbb{N}$.)