KTH Matematik
B.Ek

Lösningar tentamen 5B1204 Diskret matematik för D2, 31 mars 2005

Teoridel

1a) Den homogena ekvationen har karakteristisk ekvation $x^2 - 2x - 3 = 0$, med lösningar $x = 3, -1$, så dess allmänna lösning är $a_n = A \cdot 3^n + B \cdot (-1)^n$, A, B godtyckliga. Läggs den till den givna partikulärlösningen till den inhomogena ekvationen fås (nytt A) **svaret: Den sökta allmänna lösningen är** $a_n = n \cdot 2^n + A \cdot 3^n + B \cdot (-1)^n$, A, B **godtyckliga**.
b) Se Biggs 15.2. **c)** Se Biggs 15.6,7.
2a) Se Biggs 17.2. **b)** Se Biggs 8.4.
3a) Se Biggs 5.2. **b)** Se Biggs 6.6.
c) Se Biggs 12.3. Olika kulor, olika lådor, så antalet ges av
multinomialtalet $\binom{n}{n_1,n_2,\ldots,n_k} = \frac{n!}{n_1!n_2!\cdots n_k!}$.
4a) $f(n) = \sum_{d|n} g(d)$, se Biggs 11.5 (omvändningen till thm 11.5.2).
b) Nej. Om $xy = z$ gäller för alla heltal $i, j, k \geq 0$ att $\theta^i(x)\theta^j(y) \equiv \theta^k(z) \pmod 9$, där $\theta(n) = n$:s siffersumma. Men $\theta(2372819) = 32$, $\theta^2(2372819) = \theta(32) = 5$, $\theta(6192458) = 35$, $\theta^2(6192458) = \theta(35) = 8$, $\theta(14694581999102) = 68$, $\theta^3(14694581999102) = \theta^2(68) = 5$ och $5 \cdot 8 \equiv 4 \not\equiv 5 \pmod 9$. Se Biggs 13.1. $(2372819 \cdot 6192458 = 14693581999102.)$
c) Eftersom 11, 13 och 15 är parvis relativt prima är alla lösningar till systemet av formen $a+k\cdot(11\cdot13\cdot15) = a+2145k$. Eftersom 2718 är en lösning kan vi ta $a = 573$, så **lösningarna är** $573 + 2145k$, k **heltal**. Se stencilen om kinesiska restsatsen.
5a) Se Biggs 20.8. **b)** Se Biggs 21.2,3. Om G är ändlig är $|Gx| \cdot |G_x| = |G|$.
c) Av de nämnda är $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ kroppar. Se Biggs 22.3.

Problemdel

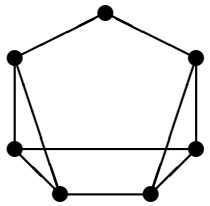
6a) Om H multipliceras med de mottagna orden (som kolonnvektorer) fås
$H\begin{bmatrix}1\\0\\0\\0\\0\\1\end{bmatrix} = \begin{bmatrix}1\\0\\1\\0\end{bmatrix}$, $H\begin{bmatrix}0\\1\\0\\0\\1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix}$, $H\begin{bmatrix}1\\1\\1\\1\\1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\1\\1\end{bmatrix}$, dvs H:s fjärde kolonn, nollkolonnen och H:s femte kolonn. Fel har alltså inträffat i fjärde, ingen och femte positionerna.
Svar: De sända orden var 100101, 010110 och 111100.
b) För att bestämma antalet kodord löser vi systemet $Hx = 0$ med Gausselimination:
$\begin{bmatrix}0&1&0&1&0&1\\1&0&1&0&0&1\\1&0&0&1&1&0\\0&1&1&0&1&0\end{bmatrix} \overset{\substack{r2\to r3,\\ r2\leftrightarrow r1}}{\sim} \begin{bmatrix}1&0&1&0&0&1\\0&1&0&1&0&1\\0&0&1&1&1&1\\0&1&1&0&1&0\end{bmatrix} \overset{r2\to r4}{\sim} \begin{bmatrix}1&0&1&0&0&1\\0&1&0&1&0&1\\0&0&1&1&1&1\\0&0&1&1&1&1\end{bmatrix} \overset{r3\to r1,r4}{\sim} \begin{bmatrix}1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&1&1&1\\0&0&0&0&0&0\end{bmatrix}$. Tre positioner (4, 5 och 6) kan tydligen väljas godtyckligt, varvid systemet bestämmer positionerna 1, 2 och 3 entydigt. Det finns alltså 2^3 kodord, så **svar: Koden innehåller 8 kodord**.
(Nämligen 000000, 011001, 101010, 110011, 111100, 100101, 010110, 001111.)
c) Vi söker antalet lösningar $0 \leq x \leq 1146$ till ekvationen $x^{271} \equiv x \pmod{1147}$, dvs antalet $x \in \mathbb{Z}_{1147}$ med $x^{271} = x$. Eftersom $1147 = 31 \cdot 37$ och 31 och 37 är relativt prima, är $\mathbb{Z}_{1147} \approx \mathbb{Z}_{31} \times \mathbb{Z}_{37}$ och det sökta antalet är antalet par $(y, z) \in \mathbb{Z}_{31} \times \mathbb{Z}_{37}$ där $y^{271} = y$ och $z^{271} = z$ (dvs $y(y^{270} - 1) = 0$ och $z(z^{270} - 1) = 0$).
Eftersom $\phi(31) = 30$ är $y^{270} = (y^{30})^9 = 1$ för alla $y \neq 0$ i $\mathbb{Z}_{31}$ och $y^{271} = y$ för **alla** $y \in \mathbb{Z}_{31}$. $\phi(37) = 36$ och $z^{270} = (z^{36})^7 z^{18} = z^{18}$, så lösningar till z-ekvationen är dels 0, dels alla lösningar till $z^{18} = 1$ i $\mathbb{Z}_{37}$. Eftersom $\mathbb{Z}_{37}$ är en ändlig kropp (37 är ju ett primtal) är $\mathbb{Z}_{37} \setminus \{0\}$ en cyklisk grupp med 36 element. Eftersom $18|36$ finns precis 18 olika lösningar till $z^{18} = 1$ (Biggs 20.9). Antalet $z \in \mathbb{Z}_{37}$ med $z(z^{270} - 1) = 0$ är alltså $1 + 18 = 19$.
Det sökta antalet par är då $31 \cdot 19 = 589$, **svar: 589 st** x **krypteras som sig själva.**

7a) Antalet sätt att fördela museidagarna = antalet injektioner (olika dagar för olika museer) från en 13-mängd (museerna) till en 34-mängd (lovdagarna) $= (34)_{13} = 34\cdot33\cdot\ldots\cdot22 = \frac{34!}{21!}$.
(Alternativt: Museidagarna kan väljas på $\binom{34}{13}$ sätt och för varje val kan museernas ordning väljas på 13! sätt, totalt alltså $\binom{34}{13}13! = \frac{34!}{21!13!}13! = \frac{34!}{21!}$ sätt.)
Svar: Antalet tillåtna fördelningar är $\frac{34!}{21!} (= 5778574175582208000)$**.**
b) Då det aldrig skall vara två museidagar i rad, kan man betrakta de $34 - 13 = 21$ museifria dagarna som "väggar" och placera museidagarna med högst en i vart och ett av de 22 "facken" mellan dem. Det kan göras på (injektion 13-mängd till 22-mängd) $(22)_{13} = \frac{22!}{9!}$ sätt. **Svar: Antalet tillåtna fördelningar är** $\frac{22!}{9!} (= 3097444686336000)$**.**

7c) Den givna permutationen α är i cykelnotation (174)(2593)(68), så α^{-1} är (147)(2395)(68). $\alpha\beta = \beta\alpha^{-1}$ betyder att $\alpha = \beta\alpha^{-1}\beta^{-1}$, dvs (174)(2593)(68) skall vara samma permutation som $\big(\beta(1)\beta(4)\beta(7)\big)\big(\beta(2)\beta(3)\beta(9)\beta(5)\big)\big(\beta(6)\beta(8)\big)$. β måste tydligen ta 3-cykeln till 3-cykeln etc. $\beta(1)$ kan vara 1, 7 eller 4. Då det valts är värdena för $\beta(4)$ och $\beta(7)$ bestämda. P.s.s. kan värdena för (t.ex.) $\beta(2)$ och $\beta(6)$ väljas bland 2, 5, 9, 3 respektive 6, 8. Då blir övriga bestämda och totala antalet möjligheter är $3 \cdot 4 \cdot 2 = 24$. **Svar: 24 stycken.**

8a) Eftersom $31 \equiv_{13} 5$ är $31^2 \equiv_{13} 25 \equiv_{13} -1$ och $31^4 \equiv_{13} (-1)^2 = 1$. Vidare är $3^2 \equiv_4 1$, så $3^{2005} = (3^2)^{1002}3 \equiv_4 3$, dvs $3^{2005} = 4k+3$ för något $k \in \mathbb{N}$. Således är $31^{3^{2005}} = (31^4)^k 31^3 \equiv_{13} 31^3 \equiv_{13} 5^3 \equiv_{13} -5 \equiv_{13} 8$. **Svar: Resten blir 8.**
b) Eftersom 19 är ett primtal gäller $n^{19} \equiv_{19} n$, dvs $n^{19} = 19k+n$ för något $k \in \mathbb{Z}$. P.s.s. är $n^{13} = 13\ell + n$ för något $\ell \in \mathbb{Z}$. Insatt får vi $13n^{19} + 19n^{13} + 215n = 13(19k+n) + 19(13\ell + n) + 215n = 13 \cdot 19(k+\ell) + (13+19+215)n = 247(k+\ell+n)$. **Saken är klar.**
c) Fall 1: $n = p^r$, en potens av ett primtal p, $r \geq 0$. Alla delare till n är då $1, p, p^2, \ldots, p^r$, så $\prod_{d|n} d = 1 \cdot p \cdot p^2 \cdot \cdots \cdot p^r = p^{0+1+2+\cdots+r} = p^{\frac{r(r+1)}{2}}$. Således $\prod_{d|n} d = n^2 = p^{2r}$ omm $\frac{r(r+1)}{2} = 2r$ dvs omm $r = 0$ eller $r = 3$, dvs $n = 1$ eller $n = p^3$.
Fall 2: n är delbart med två olika primtal p, q. Då är $n = pqm$, något $m \in \mathbb{N}$, och n har (de olika) delarna pm, qm, pqm, så $\prod_{d|n} d \geq pm \cdot qm \cdot pqm = p^2q^2m^3 = n^2 \cdot m$. Om $\prod_{d|n} d = n^2$ måste alltså $m = 1$ och $n = pq$. Å andra sidan, om $n = pq$, p, q olika primtal, är alla n:s delare $1, p, q, pq$ och $\prod_{d|n} d = 1 \cdot p \cdot q \cdot pq = p^2q^2 = n^2$. **Saken är klar.**

9a) i) 0,2,3,3,4,4,5 : **omöjligt**, ty summan av valenserna skall vara 2 gånger antalet kanter, ett jämnt tal.
ii) 2,3,3,3,3,3,3 : **möjligt**, se figuren till höger.
iii) 2,2,3,5,5,5,6 : **omöjligt**, ty de tre första hörnen kan ha högst 7 kanter till de sista fyra, men dessa måste ha minst 9 kanter till de första tre (minst 2,2,2,3 "utåt").



b) Kalla grafen $G = (V, E)$. Låt $v_1, v_2, \ldots, v_k$ vara en stig av maximal längd i G (en sådan finns eftersom det finns stigar (t.ex. u, v om $\{u, v\} \in E$) och deras längd inte kan överskrida $|V|$). Eftersom v_k har valens minst 2 finns en kant från v_k till ett hörn $u \neq v_{k-1}$. u måste vara v_i för något $i = 1, 2, \ldots, k-2$, annars skulle stigen kunna utvidgas. Då är $v_i, v_{i+1}, \ldots, v_k$ en cykel i G, **saken är klar.**
(Alternativt, låt G sakna cykler. Då är varje komponent (V', E') ett träd med $|E'| = |V'|-1$. Men $2|E'| = \sum_{v \in V'} \delta(v) \geq 2|V'|$, motsägelse.)
c) Låt antalet kanter vara e, antalet hörn med valens 5 x och antalet ytor med 4 kanter y. Då gäller $2e = \sum \delta(v_i) = 3 \cdot 13 + 5x = 39 + 5x$ och motsvarande för ytorna, $2e = 6 + 4y$. Eulers polyederformel (grafen är ju plan och sammanhängande) ger $v - e + r = 13 + x - e + y + 1 = 2$.
Så $\begin{cases} 5x - 2e &= -39 \\ 4y - 2e &= -6 \\ x + y - e &= -12 \end{cases}$. Lösning av ekvationssystemet ger $x = 3$, $y = 12$ (och $e = 27$).
Svar: 3 hörn har valens 5 och 12 ytor har 4 kanter.

10a) Vi använder Euklides algoritm. Polynomdivision (i $\mathbb{Z}_5[x]$) ger
$p(x) = x^5+4x^3+2x^2+3x+3 = (x+1)(x^4+4x^3+4x^2+x+2)+x^3+2x^2+1 = (x+1)q(x)+s(x)$,
$q(x) = x^4 + 4x^3 + 4x^2 + x + 2 = (x+2)(x^3 + 2x^2 + 1) = (x+2)s(x)$, så $r(x) = s(x)$.
Svar: Största gemensamma delaren $r(x) = x^3 + 2x^2 + 1$**.**
b) $g(x) = x^2 + 1$ är irreducibelt, ty om det vore reducibelt skulle det ha en linjär faktor och därmed ett nollställe i $\mathbb{Z}_3$, men $g(0) = 1, g(1) = g(2) = 2$.
Låt $F = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$ vara motsvarande kropp. I F gäller $x^2 = x^2 + 1 + 2 = 2, x^3 = x^2x = 2x, x^4 = x^3x = 2x^2 = 2 \cdot 2 = 1$, så x är inte ett primitivt element i F. Eftersom $F \setminus \{0\}$ har $8 = 2^3$ element, har vart och ett av dess element multiplikativ ordning 1,2,4 eller 8. Elementen $f = x, 2, 2x, 1$ uppfyller $f^4 = 1$, vilken har exakt 4 lösningar. Övriga nollskilda element i F har alltså ordning 8 och är därmed primitiva element, t.ex. **svar:** $x + 1$ **är ett primitivt element.**
c) 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, $|F(id)| = k^5$), två rotationer $\pm\frac{2\pi}{3}$ kring axeln genom de triangulära ytornas mittpunkter (bevarar konfigurationer med samma färg på alla kvadraterna, $|F(g)| = k^3$) och tre rotationer π kring axlar genom mittpunkten av en kvadrat och motstående kant (bevarar konfigurationer med trianglarna likfärgade, liksom de två andra kvadraterna, $|F(g)| = k^3$).
Lemmat ger antalet väsentligt olika färgningar, $\frac{1}{|G|}\sum_{g \in G} |F(g)|$, dvs **svar:** $\frac{1}{6}(k^5 + 5k^3)$**.**