

Matematiska Institutionen
KTH

Lösningar till tentamensskrivning på kursen Algebra och kombinatorik för F3, 5B1302, 9 januari 2002.

1. Då $n = 77 = 11 \cdot 7$ så $m = (11 - 1)(7 - 1) = 60$. Vi behöver d sådant att $e \cdot d \equiv 1 \pmod{60}$. Med hjälp av Euklides algoritim får vi $d = 7$. Vi beräknar $D(9) = 9^7$ i ringen Z_{77} : $9^2 = 4$, $9^7 = 9(9^2)^3 = 9 \cdot (-13) = 37$.

Svar. 37.

2. a) Kolonnerna är olika vilket ger att minimavståndet är större än tre. Ordet $(0,0,1,1,1,0,0,0,0,0)$ och nollordet tillhör koden. Minimiavståndet är alltså tre.

b) Kodorden i uppgift a).

c) Matrisen har rang 4, ordlängden är 10, så antalet kodord är $2^{10-4} = 64$.

d) Matrisen multiplicerad med kolonnmatrisen $(1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1)^T$ blir kolonnen $(1 \ 1 \ 0 \ 1)^T$. Detta är matrisens femtekolonn, ordet på avstånd ett är alltså $(1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$.

3. a) Grafens kromatiska tal är större än ett eftersom minst en kant finns. Alltså gäller att $P(G, 1) = 0$, och $P(G, 1)$ är summan av alla polynomets koefficienter.

b) Till exempel en graf med noderna a, b, c och kant mellan noderna a och b och mellan b och c .

c) $P(G, 2) = -2$ Error.

4. Vi använder principen om inklusion-exklusion. Låt A_{ij} beteckna mängden av surjektioner f sådana att $f(i) = f(j)$. Låt $S(n, k)$ beteckna antalet partitioner av en mängd med n element i k stycken icke-tomma delmängder. Svaret ges då av formeln

$$4!S(6, 4) - (|A_{12}| + |A_{34}| + |A_{56}|) + (|A_{12} \cap A_{34}| + |A_{12} \cap A_{56}| + |A_{56} \cap A_{34}|) - (|A_{12} \cap A_{34} \cap A_{56}|)$$

När vi beräknar A_{ij} tänker vi oss i och j som samma element. Vi får

$$|A_{ij}| = 4!S(5, 4), \quad |A_{ij} \cap A_{kl}| = 4!S(4, 4), \quad \text{och} \quad |A_{12} \cap A_{34} \cap A_{56}| = 0.$$

Stirlingtalen $S(n, k)$ beräknas med hjälp av rekursionen

$$S(n, k) = S(n - 1, k - 1) + kS(n - 1, k).$$

Vi får då att antalet surjektioner med de givna kraven är

$$4!65 - (4!10 + 4!10 + 4!10) + (4!1 + 4!1 + 4!1) - 0 = 912.$$

Svar. Mindre än 1000.

5. Delgruppen kommer också att innehålla permutationen $(1\ 2)(2\ 3) = (1\ 2\ 3)$. Delgruppen innehåller således element av ordning två och tre. Talet sex delar alltså antalet element i delgruppen. Och antalet element i delgruppen delar antalet element i S_4 dvs talet 24. Enda möjligheterna är 6 och 12. Det finns bara en delgrupp till S_4 med 12 element, den delgrupp som består av jämna permutationer. Men $(1\ 2)$ är ingen jämn permutation. Permutationerna $(1\ 2)$ och $(2\ 3)$ kan båda betraktas som element i S_3 , som ju har sex element, och som kan betraktas som en delgrupp till S_4 . Enda möjliga delgrupp är en grupp med sex element, i princip S_3 .

Svar. $\{id, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

6. Vi betraktar klossens automorfigrupp G och beräknar antalet olika banor enligt formeln

$$\frac{1}{|G|} \sum_{g \in G} |F(g)|,$$

där $|F(g)|$ är antalet färgläggningar som fixeras av elementet g .

Vi betecknar klossens långsidor med siffrorna 1, 2, 3 och 4 och dess ändsidor med 5 och 6.

Låt φ beteckna permutationen $(1\ 2\ 3\ 4)$. Gruppen G består av åtta element, elementen $\varphi, \varphi^2, \varphi^3, id, \psi_1 = (5\ 6)(1\ 2), \psi_2 = (5\ 6)(3\ 4), \psi_3 = (5\ 6)(1\ 4)(2\ 3)$ och $\psi_4 = (5\ 6)(1\ 3)(2\ 4)$.

Simpel kombinatorik ger att $|F(\varphi)| = p^3$, eftersom långsidorna måste ha samma färg, om färgläggningen inte ändras efter automorfin φ , men kortsidorna kan färgas med vilken som helst av de p färgerna och oberoende av varandra. På samma sätt får man att

$$|F(\varphi^2)| = p^4, |F(\varphi^3)| = p^3, |F(id)| = p^6, |F(\psi_1)| = p^4, |F(\psi_2)| = p^4, |F(\psi_3)| = p^3, |F(\psi_4)| = p^3.$$

Antalet olika färgläggningar är lika med antalet banor så vi får

$$\textbf{Svar. } (4p^3 + 3p^4 + p^6)/8.$$

7. Eftersom talen r och s är relativt prima så finns det tal m och n sådana att

$$mr + ns = 1.$$

Då gäller att

$$a = a^{mr} \cdot a^{ns}.$$

Det räcker nu att visa att elementen $b = a^{mr}$ och $c = a^{ns}$ har ordning s och r .

Då $b^s = a^{mrs} = (a^{rs})^m = id^m = id$ så gäller att b 's ordning s' delar talet s . På samma sätt inses att c 's ordning r' delar talet r .

Men

$$a^{r's'} = (bc)^{r's'} = (b^{s'})^{r'} \cdot (c^{r'})^{s'} = id.$$

Då a 's ordning är rs , så måste rs dela $r's'$. Enda möjligheten, emedan både r' och s' är mindre än r respektive s , är att $r = r'$ och $s = s'$, dvs b och c har ordningarna r respektive s .

8. Ringen Z_{1716} är isomorf med den direkta produkten $Z_{13} \times Z_{132}$. Låt φ beteckna denna isomorfi och låt $\varphi(x) = (x_1, x_2)$.

Det gäller för en lösning x till ekvationen i fråga att

$$\varphi(x^{13} - x + 1) = (x_1^{13} - x_1 + 1, x_2^{13} - x_2 + 1) = (0, 0)$$

I ringen Z_{13} gäller, enligt en av Fermats satser, att $r^{13} = r$, för alla element r i ringen. Alltså finns ingen lösning alls till ekvationen $x_1^{13} - x_1 + 1 = 0$ i ringen Z_{13} . Det givna ekvationen saknar därmed lösning.

Svar. 0.