MATEMATISKA INSTITUTIONEN
KTH
Examinator: Svante Linusson
telefon 790 9444

Svar på övningstentamen B i Diskret Matematik 5B1204, VT06
Varje rätt löst uppgift är värd 3 poäng. Max är 24 poäng. 10 poäng ger godkänt
Godkänt på lappskrivning 4 ger två bonuspoäng.
Hjälpmedel: Inga hjälpmedel tillåtna.
Motivera dina lösningar!!!

1. Formulera och bevisa Burnsides Lemma.

   Svar: Bokens bevis eller det bevis som jag gav på föreläsningen.

2. Låt $p(x) = x^5 + x^3 + 2x + 1 \in \mathbb{Z}_3[x]$. Faktorisera $p(x)$ i irreducibla faktorer.

   Svar: $\mathbb{Z}_3$ är en kropp så faktorsatsen säger att $p(\alpha) = 0$ omm $x - \alpha$ är en faktor till $p(x)$. Då $p(-1) = (-1)^5 + (-1)^3 + 2(-1) + 1 = -3 \equiv_3 0$ så är $-1 = 2 \in \mathbb{Z}_3$ ett nollställe och $x + 1$ är en delare till $p(x)$. Vi faktoriserar (i huvudet eller med s.k. lång division i trappa) och får $p(x) = (x+1)(x^4+2x^3+2x^2+x+1)$. Sätt $q(x) = x^4 + 2x^3 + 2x^2 + x + 1$. Då $q(0) = 1, q(1) = 1$ och $q(2) = 2$ i $\mathbb{Z}_3$ så finns inga fler linjära faktorer. Enda möjligheten att faktorisera längre är om $q(x)$ är produkten av två 2:a grads polynom. Vi ansätter $q(x) = (x^2+Ax+B)(x^2+Cx+D)$. Vi multiplicerar ut högerledet och identifierar koefficienter. Vi får då ekvationssystemet:
   $A + C = 2$
   $AC + B + D = 2$
   $AD + BC = 1$
   $BD = 1$
   Den sista ekvationen ger att $B = D \neq 0$, ty $1^{-1} = 1, 2^{-1} = 2$ i $\mathbb{Z}_3$. Den första ekvationen säger att $A = 2 - C$. Insatt i den tredje ekvationen får vi $1 = (2 - C)B + BC = 2B$ alltså är $B = D = 2$. Detta ger i andra ekvationen att $AC = 1$. Tillsammans med första ekvationen ger det en unik lösning $A = C = 1$. Då detta är en lösning till ekvationssystemet har vi att $p(x) = (x+1)(x^2+x+2)(x^2+x+2)$ är en faktorisering av $p(x)$ i irreducibla faktorer.

3. Amir och Berit skickar hemliga meddelanden med hjälp av RSA-krypto. Amir har bestämt sig för de offentliga kryptonycklarna $n_A = 91$, $e_A = 5$ och Berit har bestämt sig för $n_B = 77, e_B = 7$.

   (a) Hur skall Amir kryptera meddelandet 8 innan han skickar det till Berit?

   (b) Amir får svaret 11 från Berit. Vad skickade hon?

   Svar:

   (a) Amir skall kryptera med Berits offentliga nycklar, d.v.s $E_B(8) = 8^7 \pmod{77}$. Då $8^2 = 64 \equiv_{77} -13$ och $8^4 \equiv_{77} (-13)^2 = 169 \equiv_{77} 15$ så får vi $8^7 = 8^4 8^2 8 \equiv_{77} 15 \cdot (-13) \cdot 8 = -195 \cdot 8 \equiv_{77} 36 \cdot 8 \equiv_{77} 57$. Amir skall skicka 57 till Berit.

   (b) För att kunna dekryptera Berits meddelanden måste vi först bestämma Amirs dekrypteringsnyckel d_A. Då $n_A = 91 = 7 \cdot 13$ så är $m_A = 6 \cdot 12 = 72$ och dekrypteringsnyckeln skall uppfylla $5d_A \equiv_{72} 1$. Det löser vi med Euklides algoritm eller prövning och får $d_A = 29$. Att dekryptera 11 innebär nu att räkna ut $D_A(11) = 11^{29} \pmod{91}$. Först beräknar vi $11^2 = 121 \equiv_{91} 30$, $11^4 \equiv_{91} 30^2 = 900 \equiv_{91} -10$, $11^8 \equiv_{91} (-10)^2 = 100 \equiv_{91} 9$ och $11^{16} \equiv_{91} 9^2 = 81 \equiv_{91} -10$. Nu får vi att $11^{29} = 11^{16} 11^8 11^4 11^1 \equiv_{91} (-10) \cdot 9 \cdot (-10) \cdot 11 = 100 \cdot 99 \equiv_{91} 9 \cdot 8 = 72$. Berits meddelande till Amir var 72.

4. Låt C vara en linjär binär felrättande kod med kontrollmatris $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

(a) Hur många kodord finns det i C? (1 poäng)

(b) Hur många fel upptäcker C och hur många fel kan C rätta? (1 poäng)

(c) Visa att ordet $\mathbf{v} = 100101$ ligger på avstånd 2 eller mer från alla kodord i C. (1 poäng)

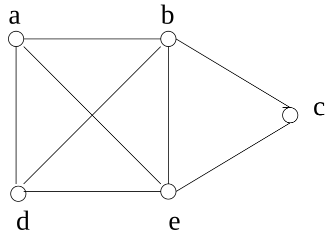
Svar:

(a) Antal kodord för en binär linjär kod ges av 2^k där k är kodens dimension. Då H har full rank så har vi $k = n - r = 6 - 3 = 3$, där n och r är antal kolumner och rader i H.

(b) Då alla kolumner är olika och nollskilda finns det en sats som säger att minimiavståndet mellan två kodord (δ) är minst 3. Notera att det finns kodord av vikt 3, t.ex. **101100**. I en linjär kod är minsta nollskilda vikten samma som minst nollskilda avständet så $\delta \leq 3$. Alltså så $\delta = 3$. Det innebär att C kan upptäcka 2 fel och rätta 1.

(c) Vi tänker kodordet $\mathbf{v}$ som en kolumnvektor och räknar ut $H\mathbf{v} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$. Detta skiljer sig från alla kolumner i H och följdaktligen räcker det inte med att justera $\mathbf{v}$ i en position för att få ett kodord. Alltså ligger $\mathbf{v}$ på avstånd minst 2 ifrån varje kodord.

5. Låt Γ vara följande graf.



På hur många sätt kan vi färga noderna i Γ med 3 färger om vi räknar två färgningar som lika ifall det finns en automorfi på grafen som överför den ena till den andra. D.v.s vi tar bort namnen på noderna så att vi inte kan skilja dem åt på så sätt. (Inga andra restriktioner på färgning av noderna finns, t.ex. kan två noder med gemensam kant ha samma färg.)

Svar: Vi använder Burnsides Lemma för att räkna ut antalet icke-isomorfa färgningar av Γ. Först måste vi bestämma automorfigruppen G för Γ. Den enda nod med valensen 2 är c så den måste avbildas på sig själv. Övriga noder skiljer sig åt genom att b, e är grannar till c vilket a, d inte är. Så b och e måste avbildas på b och e. Vi har begränsat möjligheterna till följande permutationer $\{id, (be), (ad), (ad)(be)\}$ och vi ser att alla dessa fyra är automorfier på Γ.

Vi gör nu en tabell över storleken på fixpunktsmängden för varje automorfi. För t.ex. $\pi = (be) = (a)(be)(c)(d)$ får vi att b och e måste ha samma färg för att färgningen skall vara en fixpunkt under verkan av π, men det är det enda villkoret. (Vi får välja en färg godtyckligt för varje cykel i π.) På samma sätt för övriga permutationer ger:

$\pi \in G$	$\lvert X_\pi \rvert$
id	3^5
(be)	3^4
(ad)	3^4
$(ad)(be)$	3^3

Enligt Burnsides Lemma får vi att antalet icke-isomorfa färgningar av Γ med tre färger är $\frac{1}{|G|}\sum_{\pi \in G} |X_\pi| = (243 + 81 + 81 + 27)/4 = 108$.

6. Betrakta $p(x) = x^2 - x - 3 \in \mathbb{Z}_5[x]$. Är $p(x)$ ett primitivt irreducibelt polynom?

Svar: I $\mathbb{Z}_5$ har vi att $p(0) = 2, p(1) = 2, p(2) = 4, p(3) = 3$ och $p(4) = 4$ så enligt faktorsatsen saknas linjära faktorer. Alltså är $p(x)$ irreducibelt och $\mathbb{Z}_5[x]/(p(x))$ är en kropp med 25 element. Enligt definitionen är $p(x)$ primitivt om x genererar hela den mulitplikativa gruppen som har ordning 24.

Varje element har ordning som är delare till 24 så även x. Vi räknar i $\mathbb{Z}_5[x]/(p(x))$ ut potenser av x som är delare till 24. $x^2 = x+3$, $x^3 = x^2+3x = 4x+3$, $x^4 = 4x^2+3x = 4(x+3)+3x = 2x+2$, $x^6 = (x^3)^2 = (4x+3)^2 = x^2+4x+4 = 2$, $x^8 = x^6x^2 = 2(x+3) = 2x+1$ och $x^{12} = (x^6)^2 = 2^2 = 4$. Vi ser att x inte har ordning 1,2,3,4,6,8 eller 12. Alltså har x ordning 24 och genererar följdaktligen hela den multiplikativa gruppen i kroppen. Alltså är $p(x)$ ett primitivt polynom.

7. Bevisa att gruppen $C_3 \times C_6$ inte är isomorf med gruppen C_{18}.

   Svar: Ett godtyckligt element i $C_3 \times C_6$ är på formen (x^i, y^j), där $0 \leq i \leq 2, 0 \leq j \leq 5$ och $x^3 = y^6 = 1$. Då har vi att $(x^i, y^j)^6 = (x^{6i}, y^{6j}) = (1^{2i}, 1^j) = (1,1)$ som är identiteten. Alltså har varje element i gruppen $C_3 \times C_6$ ordning 1,2,3 eller 6 (en delare till 6).

   Men varje element i C_{18} är på formen z^i, $0 \leq i \leq 17$ för någon generator z. Speciellt har z ordning 18. Grupperna kan alltså inte vara isomorfa.

8. Låt G vara en grupp med minst 2 element. Visa att G inte kan skrivas som unionen av två äkta delgrupper. D.v.s. vi kan inte skriva $G = H_1 \cup H_2$ där H_1, H_2 är delgrupper till G och $H_i \neq G$, $i = 1, 2$.

   Svar: Vi antar motsatsen att $G = H_1 \cup H_2$ för två äkta delgrupper H_1, H_2 till G. Enligt detta antagande finns element $x_1 \in H_1 \setminus H_2$ och $x_2 \in H_2 \setminus H_1$. Då H_1, H_2 är delgrupper har vi $x_1^{-1} \in H_1$ och $x_2^{-1} \in H_2$. Betrakta nu sammansättningen $y = x_1x_2$. Slutenhetsaxiomet för G ger att $y \in G$. Om $y \in H_2$ skulle slutenhetsaxiomet för H_2 ge att $yx_2^{-1} \in H_2$, men $yx_2^{-1} = x_1x_2x_2^{-1} = x_1$, en motsägelse så $y \notin H_2$. Om $y \in H_1$ skulle slutenhetsaxiomet för H_1 ge att $x_1^{-1}y \in H_1$, men $x_1^{-1}y = x_1^{-1}x_1x_2 = x_2$, en motsägelse så $y \notin H_1$. Alltså är $G \neq H_1 \cup H_2$.