MATEMATISKA INSTITUTIONEN
KTH
Examinator: Svante Linusson
telefon 790 9444

Övningstentamen B i Diskret Matematik 5B1204, VT06

Varje rätt löst uppgift är värd 3 poäng. Max är 24 poäng. 10 poäng ger betyg 3, 14 poäng ger betyg 4 och 18 poäng ger betyg 5.
Godkänt på lappskrivning 4 ger två bonuspoäng.
Hjälpmedel: Inga hjälpmedel tillåtna.
Motivera dina lösningar!!!

1. Formulera och bevisa Burnsides Lemma.

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

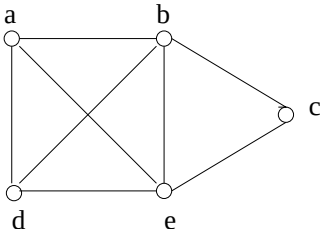
4. Låt C vara en linjär binär felrättande kod med kontrollmatris $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

   (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)

5. Låt G vara följande graf.



   På hur många sätt kan vi färga noderna i G med 3 färger om vi räknar två färgningar som lika ifall det finns någon 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.)

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

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

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 $H_i \neq G$, $i = 1, 2$.

Lycka Till!

Svante