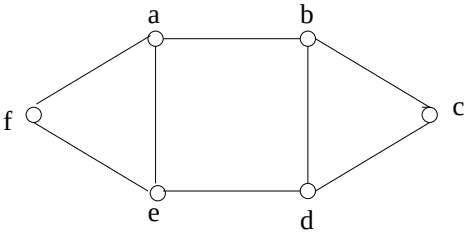
MATEMATISKA INSTITUTIONEN
KTH
Examinator: Svante Linusson
telefon 790 9444

Tenta B i 5B1204 Diskret Matematik för D, 16 maj 2006

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. Möjlighet att kompletera får den som har 9 poäng.
Godkänt på lappskrivning 4 ger två bonuspoäng.
Skrivtid: 8.00-13.00.
Hjälpmedel: Inga hjälpmedel tillåtna.
Motivera dina lösningar!!!

1. Formulera och bevisa Faktorsatsen för polynomringen över en kropp.
2. Låt $p(x) = x^4+3x^2+3x+2$, $q(x) = 4x^3+2x^2+4x+1 \in \mathbb{Z}_5[x]$. Bestäm monadiska största gemensamma delaren till $p(x)$ och $q(x)$ i $\mathbb{Z}_5[x]$.
3. Du deltar i ett RSA-krypto system och skall skicka ett meddelande till Alice. Hon har bestämt sig för de offentliga nycklarna $n_A = 143$ och $e_A = 11$.
   (a) Kryptera 24 så att du kan skicka det till Alice.
   (b) Du tjuvlyssnar och hör att Bengt skickat 17 till Alice. Dekryptera meddelandet.
4. Låt C vara en linjär binär felrättande kod som rättar ett fel och har kontrollmatris $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$.
   Tre kodord från C sänds till dig och du tar emot de tre orden $\{100100, 100011, 110111\}$. Om vi antar att högst ett fel har uppstått under sändningen av varje ord, vilka ord sändes?
5. Låt Γ vara följande graf.



   På hur många sätt kan vi färga noderna i Γ med 2 färger om vi räknar två färgningar som lika ifall det finns 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. Låt $G = \{e, a, b, c, d\}$ vara en grupp med 5 element där $eb = b, aa = d$ och $ad = c$. Bestäm fullständiga grupptabellen för G.
7. Både x^2+1 och x^2+x+2 är irreducibla polynom i $\mathbb{Z}_3[x]$. Vi har i kursen lärt oss att både $\mathbb{Z}_3[x]/(x^2+1)$ och $\mathbb{Z}_3[x]/(x^2+x+2)$ är ändliga kroppar med 9 element. Enligt teorin för ändliga kroppar är de isomorfa. Ange en isomorfi av de multiplikativa grupperna i respektive kropp.
8. Hur många irreducibla polynom av grad 3 finns det i $\mathbb{Z}_5[x]$?

Lycka Till!

Svante

Svar finns att hämta på kursens hemsida efter skrivningstidens slut.