

Tenta B i 5B1204 Diskret Matematik, 23 augusti 2006

Varje rätt löst uppgift är värd 3 poäng. Max är 24 poäng och 10 räcker för godkänt. Möjlighet att komplettera får den som har 9 poäng.

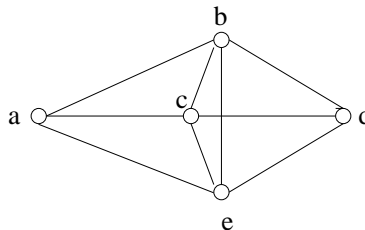
Godkänt på lappskrivning 4, VT06 ger två bonuspoäng.

Hjälpmedel: Inga hjälpmedel tillåtna.

Skrivtid: 14.00-19.00

Motivera dina lösningar!!!

1. Låt u, v vara godtyckliga element i en grupp G . Visa att det finns ett unikt element $x \in G$ så att $ux = v$.
2. Låt $p(x) = 3x^3 + 4x, q(x) = x^4 + 2x^3 + 4x^2 + x + 3 \in \mathbb{Z}_5[x]$. Vad är den monadiska största gemensamma delaren till $p(x)$ och $q(x)$ i $\mathbb{Z}_5[x]$?
3. Bush och Condoleezza skickar hemliga meddelanden till varandra med hjälp av RSA-krypto. Bush har bestämt sig för de offentliga nycklarna $n_B = 451 (= 41 \cdot 11)$ och $e_B = 89$. Condoleezza har bestämt sig för de offentliga nycklarna $n_C = 77$ och $e_C = 11$.
 - (a) Hur skall Bush kryptera meddelandet 9 innan han skickar det till Condoleezza.
 - (b) Bush får svaret 21 från Condoleezza. Vilket var det hemliga meddelandet från Condoleezza?
4. En lärare vill tilldela alla elever på kursen var sitt identitetsnummer i form av en binär sträng av längd n . Det finns 27 elever på kursen och läraren vill använda en linjär felrättande kod för att konstruera identitetsnumret. Han vill att det skall gå att korrigera ett fel i strängen. Vilket är det minsta möjliga värdet på n ?
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 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.)

6. Låt $G = \{u, v, x, y, z\}$ vara en mängd med 5 element. Avgör vilka av följande multiplikationstabeller som ger en korrekt gruppstabell (svar utan motivering ger som vanligt inga poäng).

(a)	·	u	v	x	y	z
	u	u	v	x	y	z
	v	v	x	y	z	u
	x	x	y	z	u	v
	y	y	z	u	v	x
	z	z	u	v	x	y

	u	v	x	y	z
u	x	z	u	v	y
v	y	x	v	z	u
x	u	v	x	y	z
y	z	u	y	x	v
z	v	y	z	u	x

	u	v	x	y	z
u	u	v	x	y	z
v	v	x	z	u	y
x	x	z	u	y	v
y	y	u	v	z	x
z	z	y	y	x	u

7. Är permutationsgruppen S_3 isomorf med $C_2 \times C_3$? (C_n betecknar här som i hela kursen den cykliska gruppen med n element.)
8. Visa att om ett element x i en grupp G har ordning st , där s och t är relativt prima, så kan x skrivas som en produkt av två andra element i G med ordning s respektive t .

Lycka Till!

Svante

Svar finns att hämta på kursens hemsida dagen efter skrivningen.