UPPSALA UNIVERSITET | PROV I MATEMATIK

Matematiska institutionen | Diskret matematik

Ingrid Lindström | IT, DVK, MaK, Lärarprogrammet, Fristående kurs

2011-04-29

Skrivtid: 8–13. *Inga hjälpmedel*. Alla svar ska MOTIVERAS.

Varje uppgift är värd 5 poäng. Minst 18 poäng krävs för betyget 3, 25 för betyget 4 och 32 för betyget 5.

Vänligen påbörja varje uppgift på en ny sida och skriv enbart på papperets ena sida.

LYCKA TILL!

1. Vi vill visa att $(3^{77} - 1)/2$ är ett udda sammansatt heltal. Detta görs i tre steg.

a) Bestäm den minsta icke-negativa resten då 3^{77} delas med 4.

b) Visa att $(3^{77} - 1)/2$ är ett udda heltal.

c) Visa att $(3^{77} - 1)$ är delbart med $(3^{11} - 1)$.

2. Låt $f(x) = x^5 + 2x^3 + x^2 + x + 1$ och låt $g(x) = x^4 + 3x^2 + 2$

a) Bestäm en största gemensam delare $d(x)$ i $\mathbf{Z}_7[x]$ till polynomen $f(x)$ och $g(x)$.

b) Bestäm alla största gemensamma delare till polynomen $f(x)$ och $g(x)$ i $\mathbf{Z}_7[x]$

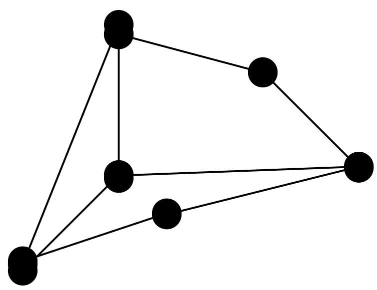
3. Låt H vara den 6x8-matris som har som kolonner binära representationer av talen 1, 3, 6, 8, 12, 20, 32, 48.

a) Hur många kodord innehåller den kodmängd som genereras av H? Ange dessa.

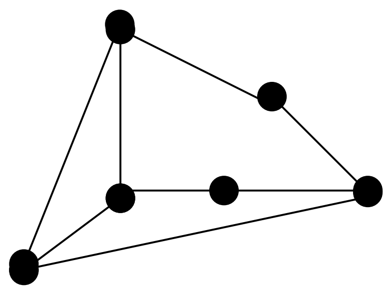
b) Hur stort fel kan säkert rättas med denna kodmängd?

c) Visa att 11111111 inte är ett kodord och ange en procedur för att rätta det utsända meddelandet 11111111 så att man får ett kodord i H.

4. Låt G vara grafen:



och H grafen:



Avgör om de båda graferna är isomorfa. Ange i så fall en isomorfi mellan dem. Bestäm vidare om det finns en Hamiltonväg i grafen G.

Var god vänd!

5. a) Den cartesiska produkten $(\mathbf{Z}_2 \times \mathbf{Z}_3, \otimes, (0, 0))$ består av alla ordnade par (a, b), där $a \in \mathbf{Z}_2$ och $b \in \mathbf{Z}_3$. Operationen $\otimes$ definieras genom

$$(a, b) \otimes (c, d) = (a +_2 c, b +_3 d).$$

Visa att $(\mathbf{Z}_2 \times \mathbf{Z}_3, \otimes, (0, 0))$ är en grupp.

b) Vi definierar en avbildning F från $(\mathbf{Z}_6, +_6, 0)$ till $(\mathbf{Z}_2 \times \mathbf{Z}_3, \otimes, (0, 0))$ genom

$$F(m) = (m \text{ modulo } 2, m \text{ modulo } 3).$$

Verifiera att F är en isomorfi.

6. a) Definiera vad som menas med en grupp, en ring respektive en kropp.

b) Ge ett exempel på en ring som inte är en kropp.

7. I RSA-algoritmen låt de offentliga nycklarna vara $n = 91$ och $e = 5$. Beräkna den hemliga nyckeln d sådan att $ed = 1$ modulo $\Phi(n)$. Abelard vill sända ett meddelande till Heloise som han kodat med talet 57. Beskriv hur Abelard medelst RSA-algoritmen krypterar sitt meddelande med användande av de offentliga nycklarna. Ange också hur Heloise dekrypterar meddelandet. Ange slutligen vilka matematiska resultat som RSA-algoritmen bygger på.

8. Konstruera en ändlig kropp med 8 element.