UPPSALA UNIVERSITET PROV I MATEMATIK
Matematiska institutionen Diskret matematik
Ingrid Lindström IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2012-04-12

*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.** Bestäm de tre sista siffrorna i talet $(11)^{804}$ när talet anges i basen 10.

**2.** Låt $f(x) = x^5 + 2x^3 + x^2 + 2$ och låt $g(x) = x^4 + 6x^3 + 2x^2 + x$

**a)** Bestäm en största gemensam delare $d(x)$ i $\mathbf{Z}_{11}[x]$ till polynomen $f(x)$ och $g(x)$.

**b)** Bestäm alla största gemensamma delare till polynomen $f(x)$ och $g(x)$ i $\mathbf{Z}_{11}[x]$

**3. a)** Ange en linjär kodmängd med 4 kodord av längd 8 och som rättar minst två fel.

**b)** Ordet 11111111 ingår inte i kodmängden. Ange hur man kan rätta detta ord för att få ett kodord.

**4. a)** Konstruera ett träd G med 8 hörn (noder).

**b)** Komplementet till G har samma hörn som G men det finns en kant mellan två hörn i komplementet om och endast om det INTE finns en kant mellan hörnen i G. Hur många kanter finns det i komplementet?

**5.** I RSA-algoritmen låt de offentliga nycklarna vara $n = 143$ och $e = 7$. 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.

**6. a)** Bestäm ett irreducibelt polynom p(x) av grad 2 i $\mathbf{Z}_2[X]$ och låt $\mathbf{F}$ vara den kropp av polynom som fås genom att man vid multiplikation räknar modulo p(x) i $\mathbf{Z}_2[X]$.

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

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

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

**c)** Visa att $(\mathbf{Z}_2 \times \mathbf{Z}_2, \otimes, (0, 0))$ är isomorf med $(\mathbf{F}, +_2, 0)$.

**d)** Definiera en operation * på $\mathbf{Z}_2 \times \mathbf{Z}_2 - \{(0, 0)\}$ så att

$$(\mathbf{Z}_2 \times \mathbf{Z}_2 - \{(0, 0)\}, *, (1, 0)) \text{ blir isomorf med}$$

$$(\mathbf{F} - \{0\}, \text{multiplikation mod p(x)}, 1).$$

**7.** Visa att antalet irreducibla polynom av grad 2 i $\mathbf{Z}_p[X]$ med ledande koefficient 1 är $\frac{1}{2} \cdot p \cdot (p-1)$.

**8.** Bestäm alla irreducibla polynom av grad 2 i $\mathbf{Z}_3[X]$.