UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2011-12-19

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. Dessa poänggränser inkluderar eventuella bonuspoäng.
Vänligen påbörja varje uppgift på en ny sida och skriv enbart på papperets ena sida.

LYCKA TILL!

1. Bestäm den minsta icke-negativa resten då $(11)^{365}$ delas med 13.

2. Skriv polynomet $f(x) = x^4 + 2x^3 + 2x + 4$ i $(\mathbf{Z}_5[x], +_5, \times_5)$ som en produkt av irreducibla polynom.

3. a) Ange en matris H som genererar en linjär kodmängd med 4 kodord av längd 5 och som rättar minst ett fel.

b) Ordet 11111 ingår inte i kodmängden. Ange hur man kan rätta detta ord för att få ett kodord.

4. Visa att det inte kan finnas en linjär kodmängd med 4 kodord av längd 5 som rättar minst ett fel och som innehåller kodordet 11111.

5. a) Konstruera en graf G med 6 hörn (noder) och 8 kanter men som inte innehåller någon triangel.

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 trianglar finns det i komplementet?

6. Redogör för hur RSA-algoritmen fungerar. Ange också vilka matematiska resultat som tekniken bygger på. Beskriv speciellt hur Eulers sats används för att verifiera att algoritmen fungerar.

7. a) Låt p vara ett primtal. Den cartesiska produkten $(\mathbf{Z}_p \times \mathbf{Z}_p, \otimes, (0, 0))$ består av alla ordnade par (a, b), där $a \in \mathbf{Z}_p$ och $b \in \mathbf{Z}_p$. Operationen $\otimes$ definieras genom

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

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

b) Avgör om $(\mathbf{Z}_p \times \mathbf{Z}_p, \otimes, (0, 0))$ är isomorf med $(\mathbf{Z}_n, +_n, 0)$, där $n = p^2$.
Ange i så fall en isomorfi mellan grupperna.

8. Konstruera en ändlig kropp med exakt 25 element.