UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2012-08-30

Skrivtid: 14-19. *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 det minsta positiva heltal som är kongruent med uttrycket modulo 12:

$$8^{2012} + (2012)^8$$

2. Låt H vara den 6x8-matris som har som kolonner binära representationer av 8 *olika* Fibonaccital.

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 11111000 inte är ett kodord.

3. Skriv polynomet $f(x) = x^5 + x^3 + 2x^2 + 2$ i $(\mathbf{Z}_7[x], +_7, \times_7)$ som en produkt av irreducibla polynom.

4. a) Konstruera en graf G som har som hörn alla ”ord” av längd 3 som kan bildas av 0:or och 1:or. Det finns en kant mellan två hörn i G om och endast om distansen mellan orden är 1. Hur många hörn och kanter finns det i grafen?

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?

c) Avgör om det finns någon Hamiltoncykel i grafen G. Ange en sådan i så fall.

5. 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.

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

b) Ge ett exempel vardera på en grupp, en ring respektive en kropp.

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

7. Visa att antalet irreducibla polynom av grad 3 i $\mathbf{Z}_p[X]$ med ledande koefficient 1 är $1/3 \cdot p \cdot (p-1) \cdot (p+1)$.

8. Bestäm alla irreducibla polynom av grad 3 i $\mathbf{Z}_3[X]$.