UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2009-08-24

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 9:

$$8^{2009} + (2009)^8$$

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

a) Bestäm en största gemensam delare $d(x)$ i $\mathbf{Z}_3[x]$ till polynomen $f(x)$ och $g(x)$.

b) Bestäm polynom $a(x)$ och $b(x)$ sådana att i $\mathbf{Z}_3[x]$

$$d(x) = a(x) \cdot f(x) + b(x) \cdot g(x).$$

3. Konstruera en graf med minst 6 noder (hörn) som har en Eulercykel men ingen Hamiltoncykel.

4. a) Konstruera en cyklisk kodmängd C av längd 3 som innehåller 4 kodord.

b) Avgör om C är en grupp under addition av kodord modulo 2.

c) Hur stort fel kan säkert rättas med kodmängden C?

5. Skriv polynomet $f(x) = x^4 + 2x^3 + x + 5$ i $(\mathbf{Z}_7[x], +_7, \cdot_7)$ som en produkt av irreducibla polynom.

6. Låt M bestå av alla 2×2 – matriser på formen $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$
där a, b och c tillhör $\mathbf{Z}_3$ och $a \cdot c \neq 0$.

M blir då en grupp under matrismultiplikation där alla multiplikationer utföres modulo 3.

a) Visa att det finns en enhet i M samt att alla matriser i M har en invers.

b) Bestäm antalet element i M.

c) Låt H vara den delgrupp som genereras av matrisen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
Bestäm ordningen hos H.

7. a) Definiera vad som menas med en linjär kod.

b) Ange en metod för att konstruera linjära koder av godtycklig längd.

c) Ge ett villkor för din konstruktion som garanterar att kodmängden rättar minst ett fel.

8. a) Ange alla irreducibla polynom $f(x)$ av grad 2 i $(\mathbf{Z}_3[x], +_3, \cdot_3)$.

b) Hur många polynom finns i den kropp F som fås då man räknar i $(\mathbf{Z}_3[x], +_3, \cdot_3)$ modulo $f(x)$?