UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2008-12-12

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. 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 sista siffran i talet 3^{103} när talet anges i basen 10.

2. a) Bestäm alla rötter till ekvationen $x^2 + x + 1 = 0$ i $(\mathbf{Z}_7, +_7, \times_7)$.

b) Bestäm alla rötter till ekvationen $x^2 + x + 1 = 0$ i $(\mathbf{Z}_8, +_8, \times_8)$.

3. Trädet T_n har n noder (hörn), där n är ett positivt heltal.

a) Hur många kanter har T_n ?

b) Bestäm det största n så att för varje m sådant att $2 \le m \le n$ gäller att det finns en Eulerväg i trädet T_m.

c) Om närliggande noder (de som är förbundna med en kant) ska ha olika färg, ange det minsta antalet färger som behövs för att måla ett godtyckligt träd.

4. Låt H vara den 3x5-matris som har som kolonner binära representationer av talen 1, 2, 3, 4, 5.

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 11110 inte är ett kodord och ange en procedur för att rätta det utsända meddelandet 11110 så att man får ett kodord i H.

5. a) Visa att följande grupper är isomorfa.

$$(\mathbf{Z}_6, +_6, 0) \quad \text{och} \quad (\mathbf{Z}_7 - \{0\}, \times_7, 1)$$

b) Ange ett villkor på det positiva heltalet m+1 som medför att $(\mathbf{Z}_m, +_m, 0)$ och $(\mathbf{Z}_{m+1} - \{0\}, \times_{m+1}, 1)$ blir isomorfa grupper.

6. a) Visa att polynomet $p(x) = x^3 + x + 1$ är irreducibelt i $\mathbf{Z}_2[X]$.

b) Hur många polynom finns det i den kropp F som fås genom att man vid multiplikation räknar modulo p(x) över $\mathbf{Z}_2[X]$?

c) Visa att polynomet x genererar alla polynom i den multiplikativa gruppen $(F^*, \times_{mod}, 1)$, där $F^* = F - \{0\}$. Vid multiplikation räknas modulo p(x) och vid addition modulo 2.

7. Redogör för hur RSA-algoritmen fungerar. Ange också vilka matematiska resultat som tekniken bygger på.

8. Låt U bestå av alla delmängder till mängden $\mathbf{Z}_n$. Den symmetriska differensen $A \oplus B$ mellan två mängder i U definieras genom

$$A \oplus B = (A \cup B) - (A \cap B)$$

Visa att U blir en ring under operationerna $\oplus$ och $\cap$.