UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2010-04-08

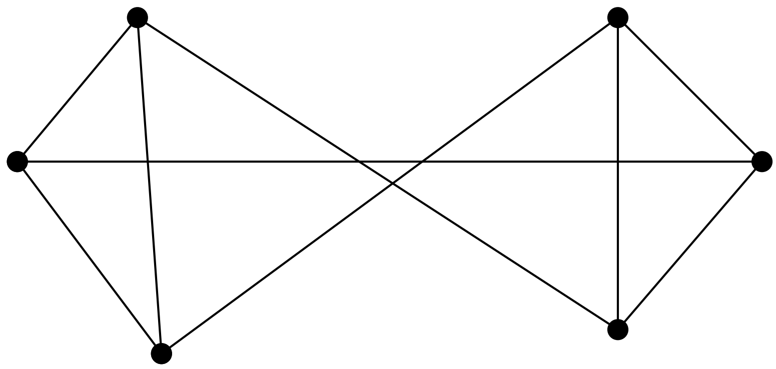
Skrivtid: 8-13. *Inga hjälpmedel*. Alla svar ska MOTIVERAS.
Varje uppgift är värd 5 poäng. Minst 18 poäng krävs för betyget 3, 25 för betyget 4 och 32 för betyget 5.
Vänligen påbörja varje uppgift på en ny sida och skriv enbart på papperets ena sida.

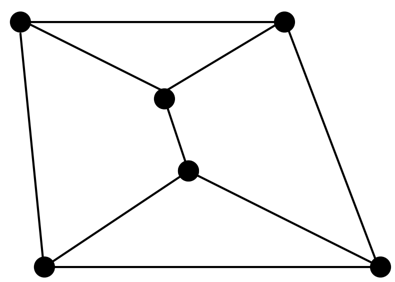
LYCKA TILL!

1. Bestäm de tre sista siffrorna i talet 3^{405} när talet anges i basen 10.

2. Skriv polynomet $f(x) = x^4 + 6$ i $(\mathbf{Z}_7[x], +_7, \times_7)$ som en produkt av irreducibla polynom.

3. Avgör om följande båda grafer G och H är isomorfa. Ange i så fall en isomorfi mellan dem.





4. Visa att det inte finns någon kodmängd som innehåller åtta kodord av längd 8 och som rättar minst två fel.

5. a) Den cartesiska produkten $(\mathbf{Z}_2 \times \mathbf{Z}_3, \otimes, (0, 0))$ består av alla ordnade par (a, b), där $a \in \mathbf{Z}_2$ och $b \in \mathbf{Z}_3$. Operationen $\otimes$ definieras genom

$$(a, b) \otimes (c, d) = (a +_2 c, b +_3 d).$$

Visa att $(\mathbf{Z}_2 \times \mathbf{Z}_3, \otimes, (0, 0))$ är en grupp.

b) Avgör om $(\mathbf{Z}_2 \times \mathbf{Z}_3, \otimes, (0, 0))$ är isomorf med $(\mathbf{Z}_6, +_6, 0)$.

6. a) Ange ett irreducibelt polynom av grad 3 med koefficienter från $\mathbf{Z}_5$.

b) Hur många polynom finns det i den kropp F som fås genom att man vid multiplikation räknar modulo p(x) i $\mathbf{Z}_5[X]$, där p(x) är det polynom som angavs i (a)?

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) Visa att om m är ett positivt heltal och p ett primtal, så gäller att

$$\Phi(p^m) = p^m - p^{m-1}$$

där Φ är Eulers Φ-funktion.

b) Använd formeln i (a) för att bestämma $\Phi(256)$.