UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2010-12-13

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!

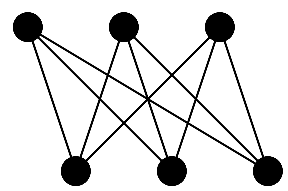
1. a) Bestäm den minsta icke-negativa resten då 3^{120} delas med 6.
b) Bestäm den minsta icke-negativa resten då 3^{120} delas med 7.

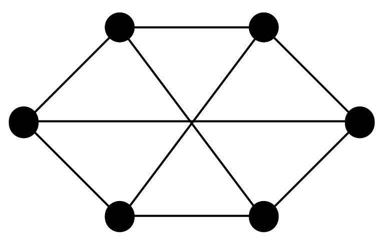
2. a) Visa att för varje positivt heltal n gäller att n^2 är kongruent modulo 5 med något av talen 0, 1 eller 4.
b) Visa att om 5 är en delare till $(a^2 + b^2 + c^2)$, så är 5 en delare till a eller b eller c, där a, b, c är positiva hela tal.

3. Skriv polynomet $f(x) = x^5 + 4x^4 + 3x^3 + x^2 + 6$ i $(\mathbf{Z}_7[x], +_7, \times_7)$ som en produkt av irreducibla polynom.

4. Bestäm den maximala dimensionen för en linjär kodmängd C, där C består av kodord av längd 8 och där C rättar minst två fel. Ange sedan en sådan kodmängd och verifiera att den är linjär.

5. Låt G vara grafen: och H grafen:





Avgör om de båda graferna är isomorfa. Ange i så fall en isomorfi mellan dem.

6. Bestäm ordningen hos de delgrupper till $\mathbf{Z}_{24}$ som genereras av elementen i gruppen med avseende på addition modulo 24. Ange sedan i ett Hassediagram hur delgrupperna är ordnade medelst inklusion.

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

8. Vi definierar följande två operationer på mängden $\mathbf{Z}$ av hela tal. För heltal x och y:
”Addition”: $x \oplus y = x + y - 1$

”Multiplikation”: $x \otimes y = x + y - x \cdot y$

Operationerna i högerledet är vanlig addition, subtraktion respektive multiplikation av hela tal. Bestäm enheter med avseende på operationerna $\oplus$ och $\otimes$ och visa att $\mathbf{Z}$ med dessa operationer och dessa enheter är en kommutativ ring. I uppgiften ingår att verifiera alla de lagar som gäller för en kommutativ ring.