UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2011-08-15

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.

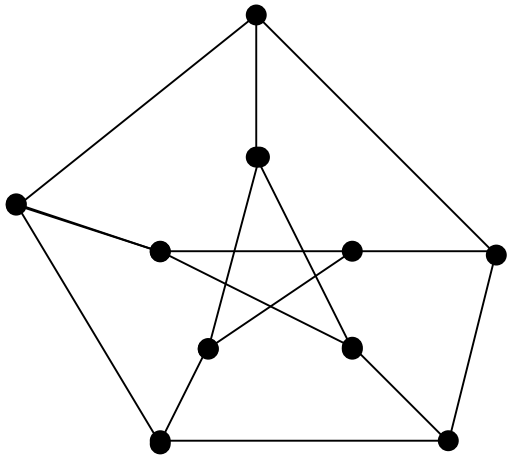
LYCKA TILL!

1. Bestäm de tre sista siffrorna i talet 3^{808} när talet anges i basen 10.

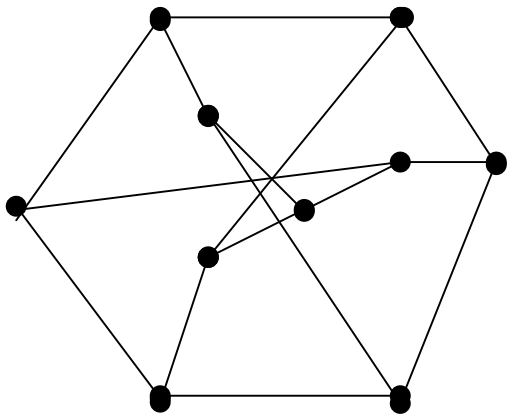
2. Skriv polynomet $f(x) = x^4 + 6x^2 + 2$ i $(\mathbf{Z}_7[x], +_7, \times_7)$ som en produkt av irreducibla polynom.

3. a) Ange en matris H som genererar de fyra kodorden: 0000, 1100, 0011, 1111.
b) Motivera varför kodmängden är linjär.
c) Hur stort fel kan säkert rättas med denna kodmängd?

4. a) Visa att det finns en Hamiltonväg i följande graf G med 10 hörn (noder)



b) Avgör om G är isomorf med följande graf H med 10 hörn (noder). Ange i så fall en isomorfi mellan dem.



Var god vänd

UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2011-08-15

5. I RSA-algoritmen låt p och q vara primtal, så att $p > q$ och låt $n = p \bullet q$. Låt vidare $r = \Phi(n)$, där Φ är Eulers Φ-funktion. Visa att om n och r är kända, så kan vi bestämma p och q som uttryck i n och r.

6. a) Låt p och q vara olika primtal. Den cartesiska produkten $(\mathbf{Z}_p \times \mathbf{Z}_q, \otimes, (0, 0))$ består av alla ordnade par (a, b), där $a \in \mathbf{Z}_p$ och $b \in \mathbf{Z}_q$. Operationen $\otimes$ definieras genom

$$(a, b) \otimes (c, d) = (a +_p c, b +_q d).$$

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

b) Om p och q är olika primtal definierar vi en avbildning F från $(\mathbf{Z}_{p \cdot q}, +_{p \cdot q}, 0)$ till $(\mathbf{Z}_p \times \mathbf{Z}_q, \otimes, (0, 0))$ genom

$$F(m) = (m \text{ modulo } p, m \text{ modulo } q).$$

Verifiera att F är en isomorfi.

7. 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 $\Phi(1024)$.

8. Konstruera en ändlig kropp med 9 element.