UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2009-12-16

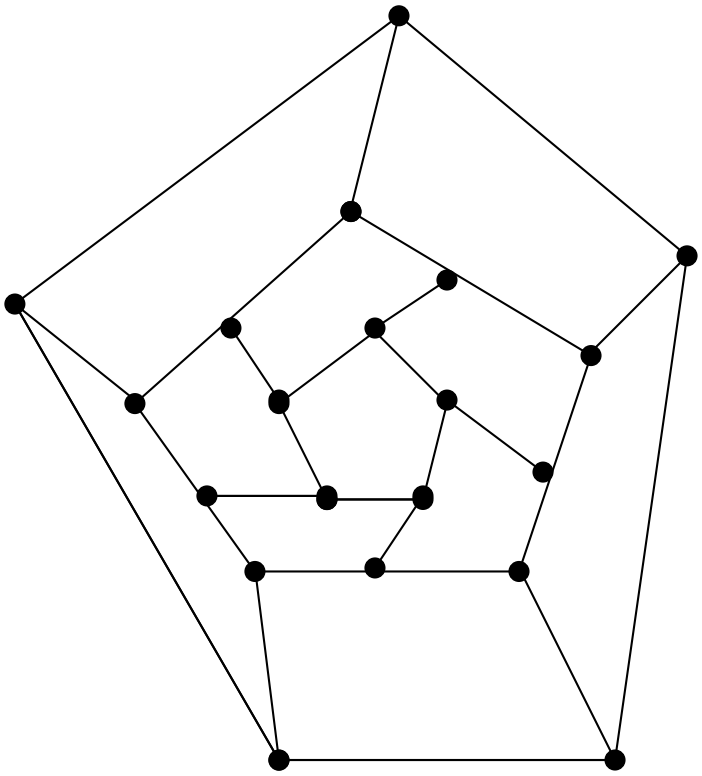
Skrivtid: 14-19. *Inga hjälpmedel*. Alla svar ska MOTIVERAS.
Varje uppgift är värd 5 poäng. Minst 18 poäng krävs för betyget 3, 25 för betyget 4 och 32 för betyget 5. Dessa poänggränser inkluderar eventuella bonuspoäng.
Vänligen påbörja varje uppgift på en ny sida och skriv enbart på papperets ena sida.

LYCKA TILL!

1. Skriv polynomet $f(x) = x^3 + x^2 + x + 1$ i $(\mathbf{Z}_5[x], +_5, \times_5)$ som en produkt av irreducibla polynom.

2. Bestäm de två sista siffrorna i talet 3^{485} när talet anges i basen 10. Formeln i uppgift 8 får användas.

3. Visa att det finns en Hamiltoncykel i följande graf med 20 hörn (noder)



4. a) Ange en matris H som genererar en linjär kodmängd av längd 7 som innehåller minst 9 kodord och som rättar minst ett fel. Avgör sedan om ordet 1111111 ingår i den genererade kodmängden.

b) Visa att det inte finns någon linjär kodmängd som innehåller åtta kodord av längd 6 och som rättar minst två fel.

Var god vänd!

UPPSALA UNIVERSITET
Matematiska institutionen
Ingrid Lindström

PROV I MATEMATIK
Diskret matematik
IT, DVK, MaK, Lärarprogrammet, Fristående kurs
2009-12-16

5. a) Låt U_8 bestå av alla positiva tal som är mindre än 8 och relativt prima med 8. Visa att U_8 utgör en grupp under multiplikation modulo 8.

b) Visa att följande båda grupper är isomorfa

$$(U_8, \times_8, 1) \quad \text{och} \quad (\mathbf{Z}_2 \times \mathbf{Z}_2, \otimes, (0, 0))$$

där den cartesiska produkten $\mathbf{Z}_2 \times \mathbf{Z}_2$ består av alla ordnade par (a, b) av element från $\mathbf{Z}_2$. Operationen $\otimes$ definieras genom

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

c) Låt $A = \{\Phi(a): a \in U_8\}$, där Φ är Eulers Φ-funktion. Enligt formeln i uppgift 8(a), så gäller ju att $\Phi(a \bullet b) = \Phi(a) \bullet \Phi(b)$ om a och b är olika element i U_8. Förklara varför man ändå inte kan definiera en isomorfi mellan gruppen $(U_8, \times_8, 1)$ och mängden A genom att låta $F: U_8 \to A$ vara definierad genom $F(a) = \Phi(a)$.
Rita sedan ett Hassediagram för A, där A är ordnad med hjälp av delbarhetsrelationen.

6. a) Finn alla irreducibla polynom av grad 3 med koefficienter från $\mathbf{Z}_2$.

b) Hur många polynom finns det i den kropp F som fås genom att man vid multiplikation räknar modulo p(x) i $\mathbf{Z}_2[X]$, där p(x) är ett av de polynom som erhållits i (a)?

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, där p(x) är ett av de polynom erhållits i (a).

7. I RSA-algoritmen låt de offentliga nycklarna vara $n = 77$ och $e = 19$. Beräkna den hemliga nyckeln d sådan att $ed = 1$ modulo $\Phi(n)$. Abelard vill sända ett meddelande till Heloise som han kodat med talet 50. Beskriv hur Abelard medelst RSA-algoritmen krypterar sitt meddelande med användande av de offentliga nycklarna. Ange också hur Heloise dekrypterar meddelandet. Ange slutligen vilka matematiska resultat som RSA-algoritmen bygger på.

8. a) Visa att för positiva heltal a, b: Om $SGD(a, b) = 1$, så $\Phi(a \bullet b) = \Phi(a) \bullet \Phi(b)$.
Om Du visar påståendet för specialfallet då a och b är primtal får du 2 poäng.

b) Ge ett motexempel till slutsatsen i (a) då a och b är positiva heltal som inte är relativt prima.