LINKÖPINGS UNIVERSITET
Matematiska institutionen
Milagros Izquierdo

Tentamen i Diskret Matematik, TATA32 (916G24), ETE373 TEN3, 2025–01–14, kl 14–19.

Inga hjälpmedel. Ej räknedosa. Fullständiga motiveringar krävs.

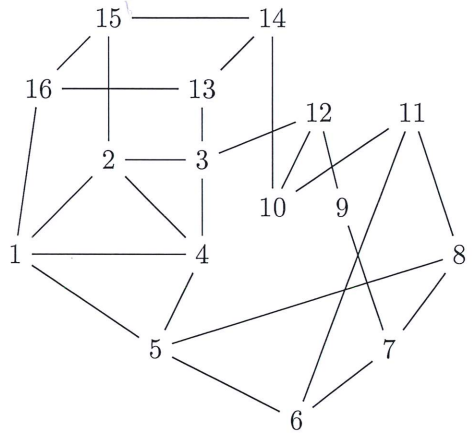
För betyg 3 behövs 15 poäng, för betyg 4, 20 poäng och 24 poäng för betyg 5, inklusive eventuella bonuspoäng.

---

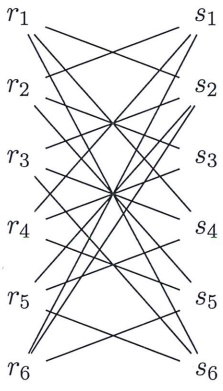
1. (a) Lös den diofantiska ekvuationen $40x^2 + 36y^2 = 1260$, där x, y är negativa heltal (2p)
   (b) Har ekvationen $x^2 - 2x + 3 \equiv 5 \bmod 13$ lösningar? Vilka? (1p)
   (c) Bestäm $1003^{7755} \bmod 180$. (3p)

2. (a) Visa att $(N, a) = (3599, 1183)$ är en bra avkrypteringsnyckel för ett RSA-kryptosystem (1p)
   (b) Ange den associerade krypteringsnyckeln k (2p)
   (c) Kryptera med denna nyckel k symbolen $x = 57$ (3p)

3. Studera om grafen G_1 nedan är Hamiltonsk, Eulersk, planär och bipartit. Ange kromatiska talet till grafen. Varje fråga ger 1p.



G_1



BG_2

4. (a) Ange en fullständig matchning i bipartita grafen BG_2 ovan. (2p)
   (b) Ange en optimal prefixkod för att överföra de 32 symbolerna i meddelandet HEJ VÄLKOMMEN TILL DISKRET MATEMATIK (3p)

5. En planär, sammanhängande graf G har 2 noder med gradtal 5 och resterande noder har gradtal 4. G har en region med gradtal 6, en med gradtal 4, tre regioner med gradtal 2 och resterande regioner är trianglar. Hur många noder, noder med gradtal 4, kanter, regioner och trianglar har G? (5p)

6. Formulera och bevisa Kinesiska restsatsen. (3p)

Svar TATA32/ETE373 Diskret Matematik (Dela) 14/1 2025

1a) Lös den diofantiska ekvationen $40x^2 + 36y^2 = 1260$
x, y negativa heltal

i) Gör ett variabelbyte $X = x^2$, $Y = y^2$ och lös

$40X + 36y = 1260$, $\text{sgd}(40, 36) = 4$, $4 \mid 1260$

Eftersom vi kan skriva $4 = (1)40 + (-1)36$ ger $X_0 = 1$, $Y_0 = -1$

$$\begin{cases} X = \frac{1260}{4} - 9n \geq 0 \\ Y = \frac{-1260}{4} + 10n \geq 0 \end{cases}$$ x, y kvadrater, så $\begin{cases} 315 \geq 9n, & 35 \geq n \\ 315 \leq 10n & 32 \leq n \end{cases}$

$n = 32$: $X_{32} = 27$, $Y_{32} = 5$ ej kvadrater

$n = 33$: $X_{33} = 18$, $Y_{33} = 15$ ej kvadrater

$n = 34$: $X_{34} = 9$, $Y_{34} = 25$ kvadrater

$n = 35$: $X_{35} = 0$, $Y_{35} = -35$ ej kvadrat

ii) Så $x = -3$ och $y = -5$

1b) Lös, om möjligt, $x^2 - 2x + 3 \equiv 5 \bmod 13$. Vi testar med alla x mellan 0 och 12 värde av pol. $p(x) = x^2 - 2x + 3 \bmod 13$

$p(0) = 3 \neq 5$; $p(1) = 2 \neq 5$, $p(2) = 3 \neq 5$, $p(3) = 6 \neq 5$

$p(4) = 11 \neq 5$; $p(5) = 18 \equiv 5$, $p(6) = 1 \neq 5$, $p(7) = 12 \neq 5$

$p(8) = 12 \neq 5$; $p(9) = 1 \neq 5$, $p(10) = 18 \equiv 5$, $p(11) = 11 \neq 5$, $p(12) = 6 \neq 5$

Lösningar $x \equiv 5$; $x \equiv 10$

1c) Vi använder KRS: $N = 180 = (2)^2(3)(5)$ och $n_1 = 4$, $n_2 = 9$, $n_3 = 5$

$$1003 \equiv \begin{cases} -1 \bmod 4 \\ 4 \bmod 9 \\ 3 \bmod 5 \end{cases} \quad \text{ty} \quad \begin{matrix} \varphi(4) = 2 \\ \varphi(9) = 6 \\ \varphi(5) = 4 \end{matrix}$$

$$\begin{cases} 1003^{7755} \equiv -1 \bmod 4 \\ 1003^{7755} \equiv 4^3 \equiv 1 \bmod 9 \\ 1003^{7755} \equiv 3^3 \equiv 2 \bmod 5 \end{cases}$$

Dessutom $N_1 = 45$ | $N_2 = 20$ | $N_3 = 36$

$45x_1 \equiv 1 \bmod 4$ | $20x_2 \equiv 1 \bmod 9$ | $36x_3 \equiv 1 \bmod 5$

$x_1 \equiv 1 \bmod 4$ | $x_2 \equiv 5 \bmod 9$ | $x_3 \equiv 1 \bmod 5$

Så $1003^{7755} \equiv (-1)(45)(1) + (1)(20)(5) + 2(36)(1) \equiv 127 \bmod 180$

2a) Visa att $(n,a) = (3599, 1183)$ är en bra avkrypteringsnyckel för ett RSA-system

Först $n = 3599 = 3600 - 1 = (59)(61)$, som är primtal

$\varphi(3599) = (58)(60) = (2)^3(3)(5)(29) = 3480$

$1183 = (7)(13)^2$

$\gcd(1183, 3480) = 1$, så $(3599, 1183)$ bra nyckel

2b) Vi löser $1183k \equiv 1 \bmod 3480$ genom att beräkna $1 = 4 \cdot 1183 + y\,3480$ med euklides algoritmen

$1 = (-353)\,1183 + (120)\,3480$ så

$k = -353 \equiv 3127 \pmod{3480}$

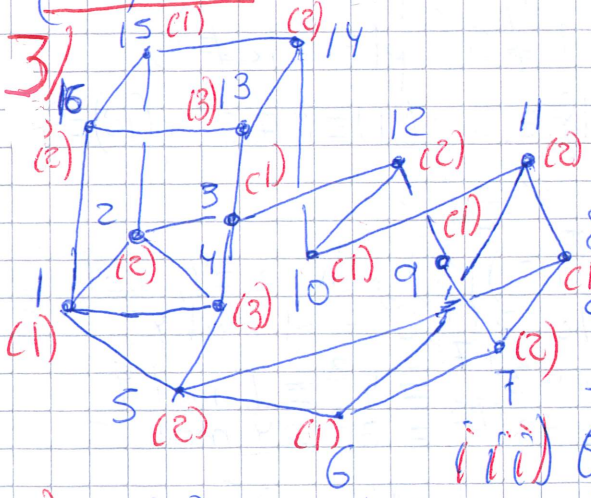
2c) $(57)^{3127} \bmod 3599$, igen med kRS

$57 \equiv \begin{cases} -2 \bmod 59 & \varphi(59) = 58 \\ -4 \bmod 61 & \varphi(61) = 60 \end{cases}$ $\quad 57^{3127} \equiv \begin{cases} (-2)^{53} \equiv 35 \bmod 59 \\ (-4)^7 \equiv 25 \bmod 61 \end{cases}$

$N_1 = 61$, $61x_1 \equiv 1 \bmod 59$, $2x_1 \equiv 1 \bmod 59$, $x_1 \equiv 30 \bmod 59$ | $N_2 = 59$, $59x_2 \equiv 1 \bmod 61$, $-2x_2 \equiv 1 \bmod 61$, $x_2 \equiv -31 \bmod 61$

$(57)^{3127} \equiv (35)(61)(30) + (25)(59)(-31) \equiv 16325 \equiv 1929 \bmod 3599$

3)

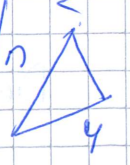


i) Bipartit är ej tillräckligt, ty t.ex. $d(6) = 3$ udda

ii) Hamiltonsk med en hamiltoncykel

$9 \to 12 \to 3 \to 13 \to 16 \to 1 \to 4 \to 2 \to 15 \to$
$\to 14 \to 10 \to 11 \to 6 \to 5 \to 8 \to 7 \to 9$

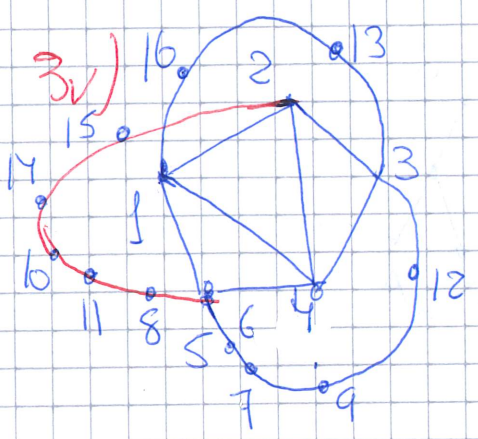
iii) Ej bipartit ty det finns trianglar



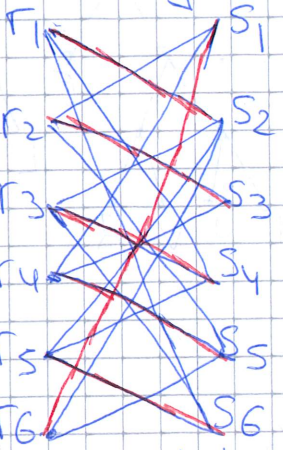
iv) $\chi(G) \geq 3$ (G ej bipartit), $\chi(G) = 3$ med en färgning som ovan (1), (2), (3) är lämplig

v) Ej planär; innehåller följande kantindelning av K_5

3 iv)



4a) En fullständig matchning i röd

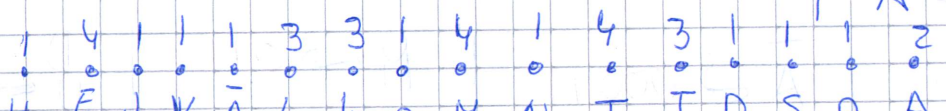


$r_1 \leftrightarrow s_2$
$r_2 \leftrightarrow s_3$
$r_3 \leftrightarrow s_4$
$r_4 \leftrightarrow s_5$
$r_5 \leftrightarrow s_6$
$r_6 \leftrightarrow s_1$

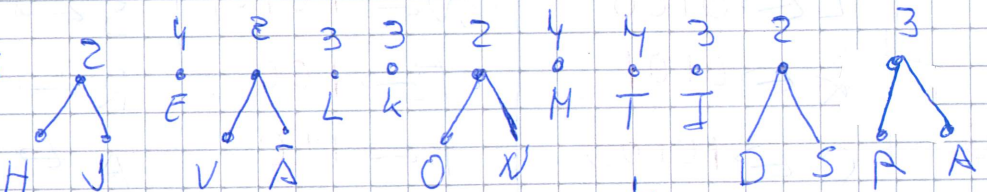
4b)

symbol	valens
H	1
E	4
J	1
V	1
Ä	1
L	3
K	3
O	1
M	4
N	1
T	4
I	3
D	1
S	1
R	1
A	2

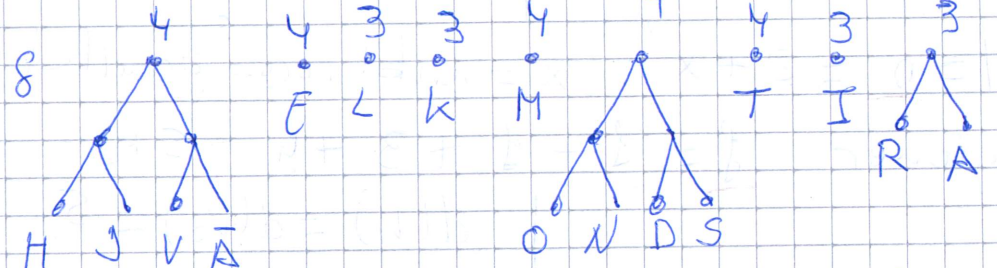
Steg 1



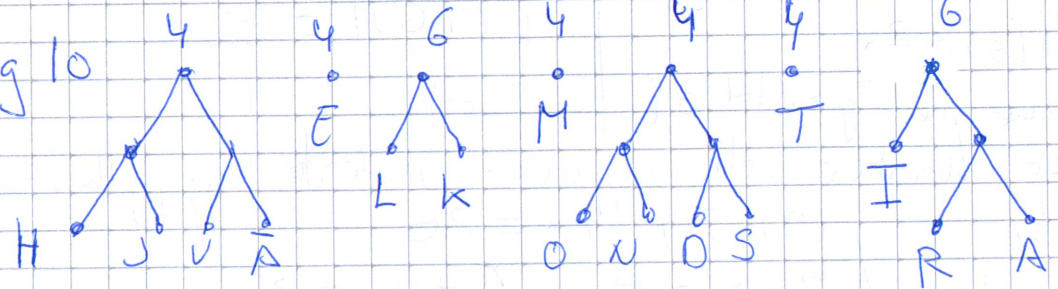
Steg 6



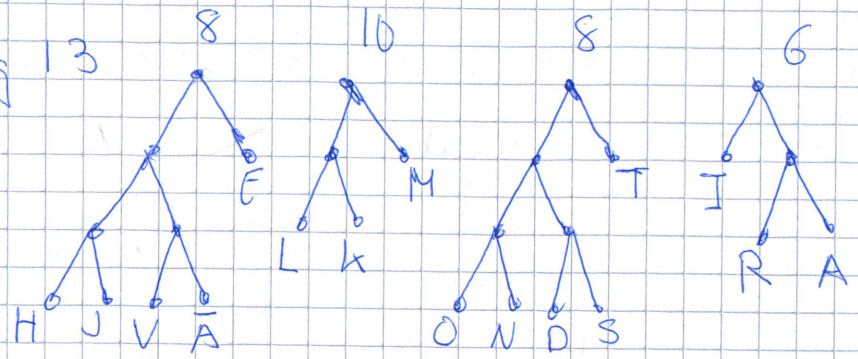
Steg 8



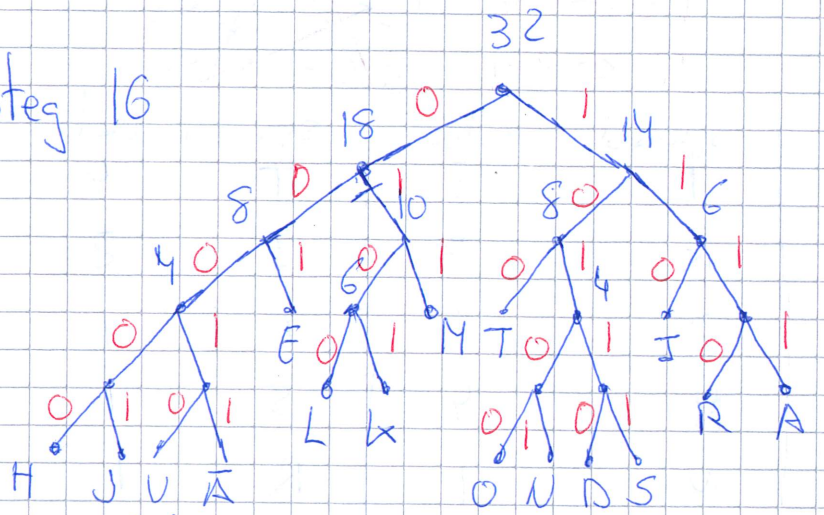
Steg 10



- Steg 13



- Steg 16



Koden blir

H ↔ 00000	Å ↔ 00011	M ↔ 011	D ↔ 10110
J ↔ 00001	L ↔ 0100	N ↔ 10101	S ↔ 10111
E ↔ 001	K ↔ 0101	T ↔ 100	R ↔ 1110
V ↔ 00010	O ↔ 10100	I ↔ 110	Å ↔ 1111

5) $|V(G)| = n = 2 + x$; x = antal noder gradtal 4

f = antal regioner $\quad f = 1 + 1 + 3 + y = 5 + y$

$d(F_1) = 6$
$d(F_2) = 4$
$d(F_3) = d(F_4) = d(F_5) = 2$

$d(V_1) = d(V_2) = 5$

$|E(G)| = e$

y = antal regioner med gradtal 3 (triangular)

Antal noder, kanter och regioner måste uppfylla

HSL noder: $(2)(5) + 4x = 2e$

Eulersformeln: $2 + x - e + 5 + y = 2$

HSL regioner: $(1)(6) + (1)(4) + (3)(2) + (y)(3) = 2e$

Vi får $x = 6$, $|V(G)| = 8$; $y = x = 6$, $f = 11$, $e = 17$