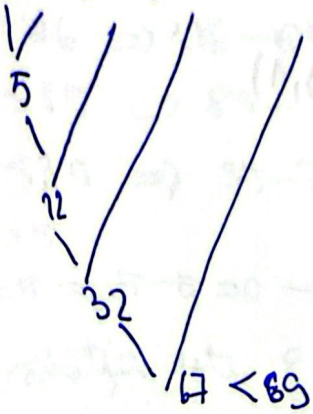
Temă

8. Pentru fiecare din șirurile următoare, decideți dacă este supracrescător și determinați toate soluțiile problemei rucsacului cu volumul corespunzător.

a) (2, 3, 7, 20, 35, 69) , V = 45



69 > 45

35 < 45 ⇒ 45 − 35 = 10

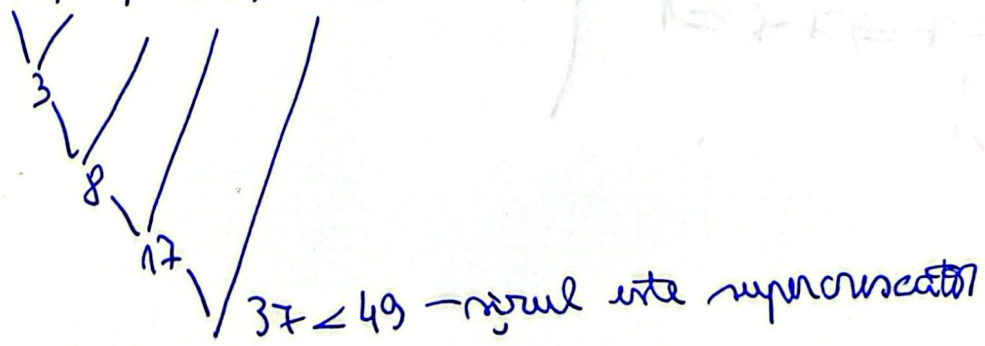
20 > 10

7 < 10 ⇒ 10 − 7 = 3

3 = 3 ⇒ 3 − 3 ⇒ rucsacul este umplut complet

Deci, soluția este: $\mathcal{E} = (0, 1, 1, 0, 1, 0)$

b) (1, 2, 5, 9, 20, 49) , V = 73



49 < 73 ⇒ 73 − 49 = 24

20 < 24 ⇒ 24 − 20 = 4

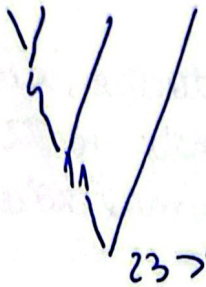
9 > 4 ⇒ 5 > 4

2 < 4 ⇒ 4 − 2 = 2

1 < 2 ⇒ 2 − 1 = 1

⇒ nu există soluții

c) $(1, 3, 7, 12, 22, 45)$, $V = 67$



$23 > 22 \Rightarrow$ șirul nu este supercrescător

$45 < 67 \Rightarrow 67 - 45 = 22$

$22 = 22 \Rightarrow 22 - 22 = 0$

Deci o soluție este: $\varepsilon_0 = (0, 0, 0, 0, 1, 1)$

O altă soluție este:

$$\varepsilon_1 = (0, 1, 1, 1, 0, 1)$$

d) $(2, 3, 6, 11, 21, 40)$, $V = 39$

$11 = 11 \Rightarrow$ șirul nu este supercrescător

$40 > 39$

$21 < 39 \Rightarrow 39 - 21 = 18$

$21 > 18$

$11 < 18 \Rightarrow 18 - 11 = 7$

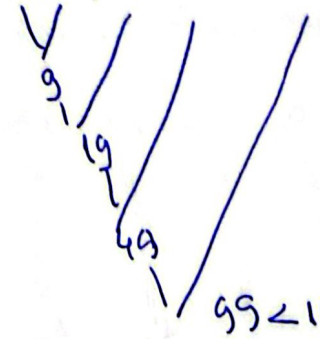
$6 < 7 \Rightarrow 7 - 6 = 1$

$3 > 1$

$2 > 1$

$\Rightarrow$ nu există soluție

e) (4, 5, 10, 30, 50, 101) , V = 186



99 < 101 ⇒ șirul este supercrescător

101 < 186 ⇒ 186 − 101 = 85
50 < 85 ⇒ 85 − 50 = 35
30 < 35 ⇒ 35 − 30 = 5
10 > 5
5 = 5 ⇒ 5 − 5 = 0 → rucsacul este umplut complet

Deci soluția este: ε = (0, 1, 0, 1, 1, 1)

f) (3, 5, 8, 15, 28, 60) , V = 43

8 = 8 ⇒ șirul nu este supercrescător

60 > 43
28 < 43 ⇒ 43 − 28 = 15
15 = 15 ⇒ 15 − 15 = 0

⇒ Deci soluția este ε = (0, 0, 0, 1, 1, 0)

9 $K \in \mathbb{N}$

$a_0, a_1, \dots, a_{K-1}$ minimal

a_0	a_1	a_2	a_3	a_4
1	2	4	8	16
2^0	2^1	2^2	2^3	...

$a_i = 2^i, \ \forall i = \overline{0, K-1}$

$V = 473$

$a_0, a_1, \dots, a_{K-1} = 2^{K-1}$

$2^8 = 256$

$2^9 = 512 \Rightarrow a_i \geq 512, \ \forall i \geq 9$

$2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, \dots, 2^{K-1}$

Fie $\underline{K \geq 9}$

$2^8 = 256 < 473 \Rightarrow V_0 = 473 - 256 = 217$

$2^7 = 128 < 217 \Rightarrow V_1 = 217 - 128 = 89$

$2^6 = 64 < 89 \Rightarrow V_2 = 89 - 64 = 25$

$2^5 = 32 > 25$

$2^4 = 16 < 25 \Rightarrow V_3 = 9$

$2^3 = 8 < 9 \Rightarrow V_4 = 1$

2^2

2^1

$2^0 = 1 \leq 1 \Rightarrow V_5 = 0$

$\varepsilon = (1, 0, 0, 1, 1, 0, 1, 1, 1, \underbrace{0, \dots, 0})$

$\underbrace{2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7} = \frac{2^8 - 1}{2 - 1} = 255 < 473$

$\nexists$ sol pt $K < 9$

10 A_{26}

$W = \{34, 51, 58, 11, 39\}$

$b = 18$, $m = 61$

$t = WHY$

$W = 22 = 10110 \Rightarrow c_1 = 0.34 + 1.51 + 1.58 + 0.11 + 1.39$

$c_1 = 148$

$H = 7 = 00111 \Rightarrow c_2 = 1.34 + 1.51 + 1.58 + 0.11 + 0.39$

$c_2 = 143$

$Y = 24 = 11000 \Rightarrow c_3 = 0.34 + 0.51 + 0.58 + 1.11 + 1.39$

$c_3 = 50$

$c = (148, 143, 50)$

$b \cdot w_0 = 18 \cdot 34 \pmod{61} = 2$

$b \cdot w_1 = 18 \cdot 51 \pmod{61} = 3$

$b \cdot w_2 = 18 \cdot 58 \pmod{61} = 7$

$b \cdot w_3 = 18 \cdot 11 \pmod{61} = 15$

$b \cdot w_4 = 18 \cdot 39 \pmod{61} = 31$

$v = \{2, 3, 7, 15, 31\}$

$v_1 = b \cdot 148 \pmod{m} = 18 \cdot 148 \pmod{61} = 41$

$\varepsilon = (1, 0, 1, 1, 0) \Rightarrow 22 \rightarrow W$

$31 < 41 \Rightarrow 41 - 31 = 10$

$15 > 10$

$7 < 10 \Rightarrow 10 - 7 = 3$

$3 = 3 \Rightarrow 3 - 3 = 0$

$v_2 = 18 \cdot 143 \pmod{61} = 18 \cdot 143 \pmod{61} = 12$

$\varepsilon = (0,0,1,1,1) \rightarrow 7 = H$

$31 > 12$

$15 > 12$

$7 < 12 \Rightarrow 12 - 7 = 5$

$3 < 5 \Rightarrow 5 - 3 = 2$

$2 = 2 \Rightarrow 2 - 2 = 0$

$v_3 = 18 \cdot 85 \pmod{61} = 18 \cdot 85 \pmod{61} = 5$

$\varepsilon = (1,1,0,0,0) \rightarrow 24 \rightarrow Y$

mesaj decriptat = WHY

12

a) $m = p \cdot q = 43 \cdot 47 = 2021$

b) $m = 109$

$109 : 2 = 54$ (Rest 1) $\quad 54 : 2 = 27$ (Rest 0) $\quad 27 : 2 = 13$ (Rest 1) $\quad 13 : 2 = 6$ (Rest 1) $\quad 6 : 2 = 3$ (Rest 0)

$3 : 2 = 1$ (Rest 1) $\quad 1 : 2 = 0$ (Rest 1)

$= 1101101 \Rightarrow m = 1101101_{(2)} = 1757_{(10)}$

$c = m^2 \pmod m = 1757^2 \pmod{2021} = 982$

2) $n = 253$

a) $(p, q) = ?$

$\sqrt{2 \cdot 53}$ | 15

1 | $25 \cdot 5 = 125$

153

125

$16^2 - 253 = 256 - 253 = 3$

$17^2 - 253 = 289 - 253 = 36 \Rightarrow 253 = 17^2 - 6^2$

$253 = 11 \cdot 23$

$(p, q) = (23, 11)$ ✓

e) $c = 170$

$up + vq = 1$

$x_{23} = (1, 0) \quad x_{11} = (0, 1)$

$23 = 11 \cdot 2 + 1 \Rightarrow x_1 = (1, 0) - 2(0, 1) = (1, -2)$

$23 \cdot (1) + 11 \cdot (-2) = 1$

$u = 1 \quad v = -2$

$r = \alpha^{\frac{p+1}{4}} \pmod p = 170^{6} \pmod{23} = 3$

$s = \alpha^{\frac{q+1}{4}} \pmod q = 170^{3} \pmod{11} = 4$

$x = Mps + Vqr \pmod n = 1 \cdot 23 \cdot 4 + (-2) \cdot 11 \cdot 3 =$
$= 92 - 66 = 26$

$y = Mps - Vqr \pmod n = 92 + 66 = 158$

Sol: $26, -26, 158, -158$
$-26 \equiv 227$
$-158 \equiv 95$

$95 = 1011\underline{1111}$

$158 = 1001\underline{1110}_{(2)}$

18. Alice utilizează un criptosistem Markle - Hellman pe un alfabet cu 26 de caractere (litere A-Z), unitățile de mesaj având un caracter. Cheia publică a lui Alice este șirul $\{8, 24, 3, 14, 57\}$, iar cheia secretă este $(b=23, m=61)$. Bob dorește să-i trimită lui Alice mesajul HELLO. Criptați mesajul.

Alfabet 26 de caractere

$w = \{8, 24, 3, 14, 57\}$

$b = 23$, $m = 61$ ~ cheia secretă

t = HELLO

H = 7 = 00111

$c_1 = 1 \cdot 8 + 1 \cdot 24 + 1 \cdot 3 + 0 \cdot 14 + 0 \cdot 57 = 35$

E = 4 = 00100

$c_2 = 0 \cdot 8 + 0 \cdot 24 + 1 \cdot 3 + 0 \cdot 14 \cdot 0 \cdot 57 = 3$

L = 11 = 01011

$c_3 = 1 \cdot 8 + 1 \cdot 24 + 0 \cdot 3 + 1 \cdot 14 + 0 \cdot 57 = 46$

O = 14 = 01110

$c_4 = 0 \cdot 8 + 1 \cdot 24 + 1 \cdot 3 + 1 \cdot 14 + 0 \cdot 57 = 41$

Criptarea este: (35, 3, 46, 46, 41)