

TEMA 1

1. Alte exemple din literatura unde este descrisă criptarea/decriptarea: "The Da Vinci Code" de Dan Brown, "The Secret Adversary" de Agatha Christie, "Enigma" de Robert Harris, "The Gold Bug" de Edgar Allan Poe.

2. ~~1010001110101~~
~~12 11 10 9 8 7 6 5 4 3 2 1 0~~

1010001110101₍₂₎
11 10 9 8 7 6 5 4 3 2 1 0

$$= 1 \cdot 2^{11} + 0 \cdot 2^{10} + 1 \cdot 2^9 + 0 \cdot 2^8 + 0 \cdot 2^7 + 0 \cdot 2^6 + \\ + 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

$$= 2^{11} + 2^9 + 2^5 + 2^4 + 2^2 + 1$$

$$= 2048 + 512 + 32 + 16 + 4 + 1$$

$$= 2560 + 33 + 20$$

$$= 2560 + 53$$

$$= 2613_{(10)}$$

100001111011₍₂₎
11 10 9 8 7 6 5 4 3 2 1 0

$$= 1 \cdot 2^{11} + 0 \cdot 2^{10} + 0 \cdot 2^9 + 0 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + \\ + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

$$= 2^{11} + 2^6 + 2^5 + 2^4 + 2^3 + 2 + 1$$

$$= 2048 + 64 + 32 + 16 + 8 + 3$$

$$= 2080 + 80 + 11$$

$$= 2171_{(10)}$$

$$\text{cmmdc}(2613, 2171) = ?$$

$$2613 : 2171 = 1 \text{ rest } 442$$

$$2171 : 442 = 4 \text{ rest } 403$$

$$442 : 403 = 1 \text{ rest } 39$$

$$403 : 39 = 10 \text{ rest } 13$$

$$39 : 13 = 3 \text{ rest } \underline{\underline{0}}$$

$$\begin{array}{r} 2613 : 2171 = 1 \\ 2171 \\ \hline 442 \end{array}$$

$$\begin{array}{r} 2171 : 442 = 4 \\ 1768 \\ \hline 403 \end{array}$$

$$\begin{array}{r} 442 : 403 = 1 \\ 403 \\ \hline 39 \end{array}$$

$$\Rightarrow \text{cmmdc}(2613, 2171) = 13$$

$$13 = 2 \cdot 6 + \underline{1}$$

$$6 = 2 \cdot 3 + \underline{0}$$

$$3 = 2 \cdot 1 + \underline{1}$$

$$1 = 2 \cdot 0 + \underline{1}$$

$$\underline{13_{(10)} = 1101_{(2)}}$$

3. Conversia unei număr din baza 10 într-o bază b

Fie N numărul în baza 10.

Pentru a-l scrie în baza b , împărțim N la b până obținem restul 0, reținând celelalte resturi.
 N în baza b este format din resturi, de la ultimul la primul.

N în baza 10 are val. max $10^h - 1$. Nr. de diviziuni necesare:

$$\log_b(10^h) = h \log_b 10$$

Fiecare diviziune este $O(1) \Rightarrow$ conversia are complexitatea $O(h)$

Conversia unui număr dat în baza b în baza 10

$$N = d_m \cdot b^m + d_{m-1} \cdot b^{m-1} + \dots + d_1 \cdot b^1 + d_0 \cdot b^0$$

$$m \approx n / \log_{10} b$$

$$N = d_0 + b(d_1 + b(d_2 + \dots + b(d_m) \dots)) \quad (\text{met. Horner})$$

Implică m operații de înmulțire și adunare \Rightarrow complexitate $O(n)$

5.

$$\begin{aligned} 21. \quad a) \quad 1010110_{(2)} &= 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 \\ &= 2^6 + 2^4 + 2^2 + 2 \\ &= 64 + 16 + 4 + 2 \\ &= 66 + 20 \\ &= 86_{(10)} \end{aligned}$$

$$\begin{aligned} b) \quad 21D_{(16)} &= \begin{matrix} 21 & (13) \\ 21 & 0 \end{matrix}_{(16)} = 2 \cdot 16^2 + 1 \cdot 16^1 + 13 \cdot 16^0 = \\ &= 2 \cdot 256 + 16 + 13 = 512 + 29 \\ &= 541_{(10)} \end{aligned}$$

$$c) \quad 101_{(6)} = 1 \cdot 6^2 + 0 \cdot 6^1 + 1 \cdot 6^0 = 36 + 1 = 37_{(10)}$$

$$37 = 3 \cdot 12 + 1$$

$$12 = 3 \cdot 4 + 0$$

$$4 = 3 \cdot 1 + 1$$

$$1 = 3 \cdot 0 + 1$$

$$37_{(10)} = 1101_{(3)}$$

$$d) 46_{(8)} \cdot 12_{(8)} =$$

$$= 574_{(8)}$$

$$\begin{array}{r} 46 \\ 12 \\ \hline 92 \\ 46 \\ \hline 452 \end{array}$$

$$\begin{array}{r} 46 \\ 12 \\ \hline 114 \\ 46 \\ \hline 574_{(8)} \end{array}$$

6. 21.

$$10^{23} \pmod{23} = 10 \cdot (10^2)^{11} = 10 \cdot 100^{11} = 10 \cdot 100 \cdot (100^2)^5 =$$

$$= 10 \cdot 8^{11} = 10 \cdot 8 \cdot (8^2)^5 = 80 \cdot 64^5 =$$

$$= 11 \cdot 18^5 = 11 \cdot 18 \cdot (18^2)^2 =$$

$$= 198 \cdot 324^2 = 14 \cdot 2^2 = 14 \cdot 4 = 56 = 10$$

$$\begin{array}{r} 100 : 23 = 4 \\ 92 \\ \hline 8 \end{array}$$

$$\begin{array}{r} 80 : 23 = 3 \\ 69 \\ \hline 11 \\ 64 : 23 = 2 \\ 46 \\ \hline 18 \\ 18 \cdot 11 \\ \hline 18 \\ 18 \\ \hline 198 \end{array} \quad \begin{array}{r} 18 \cdot 18 \\ \hline 144 \\ 18 \\ \hline 324 \end{array}$$

$$\begin{array}{r} 198 : 23 = 8 \\ 184 \\ \hline 14 \\ 324 : 23 = 14 \\ 23 \\ \hline 94 \\ 92 \\ \hline 2 \end{array}$$

$$\begin{array}{r} 56 : 23 = 2 \\ 46 \\ \hline 10 \end{array}$$