Gherasim Ana-Teodora

Temă seminar 1

1) Alte exemple de literatură unde este descrisă criptarea/decriptarea sunt: „Cryptonomicon" de Neal Stephenson, „Digital Fortress" de Dan Brown și „Enigma" de Robert Harris.

2) $\overset{a=}{1010.0011.0101}$ și $\overset{b=}{1000.0111.1011}$

$(2613_{(10)})$ $(2171_{(10)})$

$a > b \Rightarrow a = a - b$

$$
\begin{array}{rl}
a = & 1010.0011.0101 - \\
 & 1000.0111.1011 \\
\hline
 & 0001.1011.1010 \quad (442_{(10)})
\end{array}
$$

$a = 1.1011.1010$ $b = 1000.0111.1011$

$$
b > a \Rightarrow b = b - a \Rightarrow
\begin{array}{r}
1000.0111.1011 - \\
0001.1011.1010 \\
\hline
110.1100.0001 \quad (1729_{(10)})
\end{array}
$$

$$
b > a \Rightarrow
\begin{array}{rl}
0110.1100.0001 - & \\
0001.1011.1010 & \\
\hline
0101\ 0000.0111 - & (1287_{(10)}) \\
0001.1011.1010 & \\
\hline
11.0100.1101 - & (845_{(10)}) \\
01.1011.1010 & \\
\hline
01.1001.0011 & (403_{(10)})
\end{array}
$$

$$
a > b \Rightarrow a = a - b \Rightarrow
\begin{array}{rl}
1.1011.1010 - & \\
1.1001.0011 & \\
\hline
0.0010.0111 & (39_{(10)})
\end{array}
$$

$$
b > a \Rightarrow b = b - a \Rightarrow
\begin{array}{rl}
1.1001.0011 - & \\
10.0111 & \\
1.0110.1100 & 4) \\
10.0111 & \\
1.0100.0101 & 325) \\
10.0111 & \\
\hline
1.0001.1110 & (286)
\end{array}
$$

$$\begin{array}{r} 1.0001.1110- \\ 10.0111 \\ \hline 0.1111.0111 \end{array} (247) \longrightarrow \begin{array}{r} 0.1111.0111- \\ 10.0111 \\ \hline 1101.0000 \end{array} \longrightarrow \begin{array}{r} 1101.0000- \\ 10.0111 \\ \hline 10101001 \end{array} \quad \ldots \quad b = \underset{(52)}{110100}$$

$$\begin{array}{r} 11.0100- \\ 10.0111 \\ \hline 001101 \end{array} \quad (13)$$

$a = 10.0111$ și $b = 1101$

$$a > b \Rightarrow \begin{array}{r} 10.0111- \\ 1101 \\ \hline 1.1010- \\ 1101 \\ \hline 0.1101 \end{array} \begin{array}{l} \\ \\ \\ (26) \\ \\ (13 \end{array}$$

$a = b = 13 \Rightarrow$ cmmdc $(a,b) = 13$

3) • Transformarea unui nr. din baza 2 în 10: $n_{10} = \sum_{i=0}^{k-1} r_i 2^i$

$\swarrow$ nr%10 $\in \{0,1\}$

→ procesul are k înmulțiri ⇒ complexitatea este $O(k)$
(la fel și pt o bază b)

• Transformarea unui nr din baza 10 în 2 se face prin împărțirea succesivă la 2

Fie N nr. în baza 10 de k cifre ⇒ în baza 2 are $\approx \log_2 N$ cifre
→ împărțiri la 2 ⇒ $O(\log_2 N) \approx O(\log_2 10^k) \approx O(k \log_2 10)$

(în baza b: $O(k \log_2 b)$)

5) 15. a) $\overset{5}{1}\overset{4}{1}\overset{3}{0}\overset{2}{1}\overset{1}{1}\overset{0}{0}_{(2)} = 2 + 2^2 + 2^4 + 2^5 = 2 + 4 + 16 + 32 = 54_{(10)}$

b) $3B_{(16)} = 11 \cdot 16^0 + 3 \cdot 16 = 11 + 48 = 59_{(10)}$

c) $111_{(7)} = 1 \cdot 7^0 + 1 \cdot 7^1 + 1 \cdot 7^2 = 1 + 7 + 49 = 57_{(10)}$

$$\begin{array}{lll}
57:4=14 & :4=3 & :4=0 \quad \Rightarrow 111_{(7)} = 321_{(4)} \\
\underline{4} & \underline{12} & \underline{0} \\
17 & =2 & 3 \\
\underline{16} & & \\
=1 & &
\end{array}$$

d) $$\begin{array}{l}
140_{(6)} : 14_{(6)} = 10_{(6)} \\
\underline{14} \\
==0 \\
\underline{0} \\
=
\end{array}$$

verificare: $$\left.\begin{array}{l}
140_{(6)} = 4\cdot 6 + 1\cdot 6^2 = 24+36 = 60 \\
14_{(6)} = 4\cdot 1 + 1\cdot 6 = 10
\end{array}\right\} \Rightarrow 60:10 = 6 = 10_{(6)}$$

6) 15. $15^{30} \bmod 31 = (15^2)^{15} = (225)^{15} = 29^{15} = (-2)^{15} = -2\cdot(-2)^{14} =$

$= -2\cdot (4)^7 = -2\cdot 4\cdot 4^6 = -8\cdot(16)^3 = -8\,(-15)^3 = -8\cdot(-15)\cdot 15^2 =$

$= 120\cdot 225 = 27\cdot 29 = -2\cdot(-4) = 8$