1) The Imitation Game

2) Utilizăm alg. lui Euclid cu împărțiri repetate

$$1010001101101 : 1000011111011 = 1 \text{ rest } 110111010$$
$$1000011111011$$
$$= 110111010$$

$$1000011111011 : 110111010 = 100 \text{ rest } 1100100111$$
$$110111010$$
$$= 11001001$$
$$0$$
$$1100100111$$
$$0$$
$$1100100111$$

$$110111010 : 1100100111 = 1 \text{ rest } 100111$$
$$1100100111$$
$$= 100111$$

$$1100100111 : 100111 = 1010 \text{ rest } 1101$$
$$100111$$
$$= 10110$$
$$0$$
$$101101$$
$$100111$$
$$= 1101$$
$$0$$
$$1101$$

$100111 : 1101 = ?$

$$\left.\begin{array}{l} 100111 - \\ \quad 1101 \\ \hline 11010 \end{array}\right. \Rightarrow 100111 \equiv 11010 \pmod{1101}$$

Dar $11010 = 10 \cdot 1101 \Rightarrow 11010 \equiv 0 \pmod{1101}$

$\Rightarrow 100111 \equiv 0 \pmod{1101} \Rightarrow \text{cmmdc}((1010001101101)_2, (1000011111011)_2) = (1101)_2$

Verificăm rez. în baza 10

$(1010001101101)_2 = 2^0 + 2^2 + 2^3 + 2^5 + 2^9 + 2^{11} = 1 + 4 + 16 + 32 + 512 + 2048 = 53 + 2560 = (2613)_{10}$

$(1000011111011)_2 = 2^0 + 2^1 + 2^3 + 2^4 + 2^5 + 2^6 + 2^{11} = 1 + 2 + 8 + 16 + 32 + 64 + 2048 = 123 + 2048 = (2171)_{10}$

$(1101)_2 = 2^0 + 2^2 + 2^3 = 1 + 4 + 8 = 13$

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

$2171 : 442 = 4 \text{ rest } 403$
1768
$= 403$

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

$403 : 39 = 10 \text{ rest } 13$
39
$= 13$
0
13

$39 : 13 = 3 \text{ rest } 0 \Rightarrow \text{cmmdc}((2163)_{10}, (2171)_{10}) = (13)_{10} = (1101)_2$

3) $0 \neq N$ are k biți $\Leftrightarrow (N)_2 = (\overline{a_{k-1} \dots a_0})_2 \Leftrightarrow (N)_{10} = \sum_{i=0}^{k-1} (a_i \cdot 2^i) \Leftrightarrow 2^{k-1} \leq N \leq 2^k$

Dacă știm $(N)_2$, at. conversia $(N)_2 \mapsto (N)_{10}$ este de complexitate $O(k)$, adică liniară, deoarece la fiecare pas al sumei are loc câte o înmulțire și o adunare

Dacă știm $(N)_{10}$, at. conversia $(N)_{10} \mapsto (N)_2$ este de complexitate $O(\log_2 N)$, dar cum $N \simeq 2^k$ at. $O(\log_2 N) = O(\log_2 2^k) = O(k)$ complexitate liniară

5.39)

a) $(101011)_2 = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^3 + 1 \cdot 2^5 = 1 + 2 + 8 + 32 = (43)_{10}$

b) $(3C)_{16} = 12 \cdot 16^0 + 3 \cdot 16^1 = 12 + 48 = (60)_{10}$

c) $(122)_6 = 2 \cdot 6^0 + 2 \cdot 6^1 + 1 \cdot 6^2 = 2 + 12 + 36 = (50)_{10} = (302)_4$

$50 : 4 = 12 \text{ rest } 2$
$12 : 4 = 3 \text{ rest } 0$
$3 : 4 = 0 \text{ rest } 3$

d) $(44)_7 + (11)_7 = 4 \text{ rest } 0$
44
$=$

6.59) $7^{58} \bmod 59$

$7^{58} = (7^2)^{29} = 49^{29} = 49 \cdot (49)^{28} = 49 \cdot (2401)^{14} \equiv 49 \cdot (41)^{14} = 49 \cdot (1681)^7 \equiv 49 \cdot (29)^7 = \underbrace{49 \cdot 29}_{=1421} \cdot (841)^3 \equiv 5 \cdot (15)^3 = \underbrace{5 \cdot 15}_{\neq 5} \cdot 225 \equiv \underbrace{16 \cdot 48}_{\neq 48} \equiv 1 \pmod{59}$