Tema 1 - Buzurleac Ionut - NR 19 - 11533

2) Algoritmul lui Euclid extins aflati CMMDC al lui

~~11123 si 21103~~ 21103 si 11123

21103 = 11123 · 1 + 9980 · 1

~~9980~~ 11123 = 9980 · 1 + 1143

9980 = 1143 · 8 + 836

1143 = 836 · 1 + 307

836 = 307 · 2 + 222

307 = 222 · 1 + 85

222 = 85 · 2 + 52

~~85 = 58 · 1 + 34~~

~~54 = 34 + 20~~

~~34 = 20 + 14~~

~~20 = 14 · 1 + 6~~

~~14 = 6 · 2 + 2~~

~~6 = 3 · 2 + 0~~

85 = 52 + 33

52 = 33 + 19

33 = 19 + 14

19 = 14 · 1 + 5

14 = 5 · 2 + 4

5 = 4 · 1 + 1

=> cmmdc(11123, 21103) = 1

$X_{9980} = (1, -1)$

$X_{1143} =$ ~~$(2, -1) = (0, 1) - (1, -1)$~~ $= (-1, 2)$

~~14 = 5 · 2 + 4 · 1 + 1~~

~~19~~ 1143 = 11123 - 9980 = (0, 1) - (1, -1) = (-1, 2)

$X_{836} = X_{9980} - 8 \cdot X_{1143} = (1, -1) - 8(-1, 2) = (9, -17)$

$X_{307} = X_{1143} - X_{836} = (-1, 2) - (9, -17) = (-10, 19)$

$X_{222} = X_{836} - 2X_{307} = (9, -17) - (-20, 38) = (29, -55)$

$X_{85} = (-39, 74)$ și $X_{52} = (107, -203)$

$X_{33} = (-196, 277)$ $X_{19} = (253, -480)$

$X_{16} = (-399, 749)$

$X_5 = (692, -1373)$

$X_4 = (-1703, 3231)$

$X_1 = (2359, -4468)$

3) Calculați inversul lui 20 modulo 79

$(20, 79) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$ a.î. $1 = u \cdot 20 + v \cdot 79$

$\Rightarrow 1 \equiv u \cdot 20 \pmod{79} \Rightarrow \exists\ 20^{-1} \equiv u \pmod{79}$

Observăm că $40 \cdot 4 = 80 = 79 \cdot 1 + 1 \Rightarrow$

$20 \cdot 4 \equiv 1 \pmod{79} \Rightarrow 4 \equiv 20^{-1} \pmod{79}$