Tema 1

Cătălin Răzeanu

1. Calc. CMMDC al lui 89017 și 21089 folosind algoritmul lui Euclid extins și det. coef. Bezout.

$(89017, 21089) = ?$ $\quad x_{89017} = (1, 0) \quad x_{21089} = (0, 1)$

$89017 = 21089 \cdot 4 + 4661 \Rightarrow x_{4661} = (1, -4)$

$21089 = 4661 \cdot 4 + 2445 \Rightarrow x_{2445} = (-4, 17)$

$4661 = 2445 \cdot 1 + 2216 \Rightarrow x_{2216} = (5, -21)$

$2445 = 2216 \cdot 1 + 229 \Rightarrow x_{229} = (-9, 38)$

$2216 = 229 \cdot 9 + 155 \Rightarrow x_{155} = (86, -363)$

$229 = 155 \cdot 1 + 74 \Rightarrow x_{74} = (-95, 401)$

$155 = 74 \cdot 2 + 7 \Rightarrow x_7 = (276, -1165)$

$74 = 7 \cdot 10 + 4 \Rightarrow x_4 = (-2855, 12051)$

$7 = 4 \cdot 1 + 3 \Rightarrow x_3 = (3131, -13216)$

$4 = 3 \cdot 1 + 1 \Rightarrow x_1 = (-5986, 25267)$

$3 = 1 \cdot 3 + 0$

$(89017, 21089) = 1$

$1 = -5986 \cdot 89017 + 25267 \cdot 21089$

2) f. Găsește inversul lui 9 în modulo 31

$(9, 31) = 1 \Rightarrow \exists\ 9^{-1} \bmod 31$

$31 = 9 \cdot 3 + 4 \Rightarrow x_4 = (1, -3)$

$9 = 4 \cdot 2 + 1 \Rightarrow x_1 = (-2, 7)$

$4 = 1 \cdot 4 + 0$

$x_{31} = (1, 0) \qquad x_9 = (0, 1)$

$1 = -2 \cdot 31 + 7 \cdot 9$

$1 \equiv 7 \cdot 9 \pmod{31}$

$\Rightarrow 9^{-1} = 7 \pmod{31}$