TEMA 1

7.1. Găsiți CMMMDC pentru 78513 și 10997 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout

$78513 = 10997 \cdot 7 + 1534$

$10997 = 1534 \cdot 5 + 1327$

$1534 = 1327 \cdot 1 + 607$

$1327 = 607 \cdot 2 + 113$

$607 = 113 \cdot 5 + 42$

$113 = 42 \cdot 2 + 29$

$42 = 29 \cdot 1 + 13$

$29 = 13 \cdot 2 + 3$

$13 = 3 \cdot 4 + 1$

$3 = 1 \cdot 3 + 0$

$(78513, 10997) = 1$

$X_{1534} = (1,0) - (0,7) = (1,-7)$

$X_{1327} = (0,1) + (-5,35) = (-5,36)$

$X_{607} = (1,-7) + (3,-36) = (6,-43)$

$X_{113} = (-5,36) + (-12,86) = (-17,122)$

$X_{42} = (6,-43) + (85,-610) = (91,-653)$

$X_{29} = (-17,122) + (-182,1306) = (-199,1428)$

$X_{13} = (91,-653) + (199,-1428) = (290,-2081)$

$X_3 = (-199,1428) + (-580,4162) = (779,5590)$

$X_1 = (290,-2081) + (3116,-22360) = (3406,-24441)$

$3406 \cdot 78513 - 24441 \cdot 10997 = 1$

7.2. Calculați inversul lui 8 din modulo 29

$8x \equiv 1 \pmod{29}$

$8x \equiv 1 + 29x$

$8^{-1} \equiv 8^{29-2} \pmod{29}$

$8^{-1} \equiv 8^{27} \pmod{29}$

$8^{27} \pmod{29}$

$8 \cdot (8^2)^{13} \pmod{29} \equiv 8 \cdot 25^{13} \pmod{29} \equiv$

$\equiv 8 \cdot (25^2)^6 \cdot 25 \pmod{29} \equiv 8 \cdot 18^6 \cdot 25 \pmod{29} \equiv$

$\equiv 8 \cdot 11^3 \cdot 25 \pmod{29} \equiv 8 \cdot 3 \cdot 11 \cdot 29 \pmod{29} \equiv 7 \pmod{29}$

inversul lui 8 modulo 29 este 7