Tema 1. Criptografie.

1. Calculați complexitatea algoritmului lui Euclid extins.

(2). Cmmdc

15. Determinați cmmdc al lui 55673 și 77687 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

(3). Inversul unui număr în $\mathbb{Z}_n$.

15. Determină inversul lui 16 în modulo 61.

---

3) $16^{-1} \bmod 61 \equiv 19 \bmod 61$

$(16, 61) = 1$

$61 = 16 \cdot 3 + 13$

$16 = 13 \cdot 1 + 3$

$13 = 3 \cdot 4 + 1 \Rightarrow 1 = 13 - 3 \cdot 4$

~~3 = 4 0 13~~ ~~3 = 1 3 + 0~~

~~4 =~~ ~~1 = 0 1 + 1~~

$1 = 13 - 3 \cdot 4 = 13 - (16 - 13) \cdot 4 = (61 - 3 \cdot 16) - (16 - (61 - 3 \cdot 16)) \cdot 4$

$= 61 - 3 \cdot 16 - 4 \cdot 16 + 4 \cdot 61 - 12 \cdot 16$

$= 5 \cdot 61 - 19 \cdot 16$

2)

$77687 = 55673 \cdot 1 + 22014$ $\quad X_{22014} = (1,0) - 1(0,1) = (1,-1)$

$55673 = 22014 \cdot 2 + 11645$ $\quad X_{11645} = (0,1) - 2 \cdot (1,-1) = (-2,3)$

$22014 = 11645 \cdot 1 + 10369$ $\quad X_{10369} = (1,-1) - 1 \cdot (-2,3) = (3,-4)$

$11645 = 10369 \cdot 1 + 1276$ $\quad X_{1276} = (-2,3) - 1(3,-4) = (-5,7)$

$10369 = 1276 \cdot 8 + 161$ $\quad X_{161} = (3,-4) - 8 \cdot (-5,7) = (43,-60)$

$1276 = 161 \cdot 7 + 149$ $\quad X_{149} = (-5,7) - 7 \cdot (43,-60) = (-306,427)$

$161 = 149 \cdot 1 + 12$ $\quad X_{12} = (43,-60) - 1(-306,427) = (349,-487)$

$149 = 12 \cdot 12 + 5$ $\quad x_5 = (-306, 427) - 12 \cdot (349, -487)$

$= (-4494, 6271)$

$12 = 5 \cdot 2 + 2$ $\quad x_2 = (349, -487) - 2 \cdot (-4494, 6271)$

$= (9337, -13029)$

$5 = 2 \cdot 2 + 1$ $\quad x_1 = (-4494, 6271) - 2 \cdot (9337, -13029)$

$2 = 2 \cdot 1 + 0$ $\quad x_0 = (-23168, 32329)$

$1 = -23168 \cdot 77687 + 32329 \cdot 55673$