TEMA 4

1. Studiați algoritmul de factorizare rho al lui Pollard și aplicați-l pentru 10909.

$x = 2$
$y = 2$
$f(x) = x^2 + 1$
$n = 10909$

$d = (|2-2|, 10909) = 1$

$x_1 = f(2) \pmod{10909} = 2^2 + 1 \pmod{10909} = 5$
$y_1 = f(f(2)) \pmod{10909} = f(5) \pmod{10909} = 26$

$d = (|5-26|, 10909) = 1$

$x_2 = f(5) \pmod{10909} = 26$
$y_2 = f(f(26)) \bmod 10909 = 152$

$d = (|26-152|, 10909) = 1$

$x_3 = f(26) \pmod{10909} = 667$
$y_3 = f(f(667)) \pmod{10909} = 9744$
$d = (|152-9744|, 10909) = 1$

$x_4 = f(667) \pmod{10909} = 152$
$y_4 = f(f(9744)) \pmod{10909} = 5725$
$d = (|152-5725|, 10909) = 1$
....

3. 1. Descompuneți numărul 11227 în factori săi primi.

$n = 11227$

$[\sqrt{11227}] = 105$

$t = [\sqrt{11227}] + 1 = 106$

$t^2 - n = 11236 - 11227 = 9 = 3^2 = s^2$

$t = 106, \ s = 3 \Rightarrow b = t + s = 109$

$a = t - s = 103$