Teme seminarul 4 - Criptografie

2) Studiați algoritmul de factorizare rho al lui Poland și aplicați-l pentru 10909.

Algoritmul rho al lui Pollard este un algoritm probabilistic pentru factorizarea numerelor întregi.

Aplicarea algoritmului pentru 10909:

1. Alegem funcția $f(x) = (x^2+1) \bmod 10909$ și punctul de pornire $x=2$
2. Inițializăm $x=2$; $y=2$, $d=1$
3. Iterăm până când $d \neq 1$ și $d \neq 10909$

Pas 1: $x = f(x) = (2^2+1) \bmod 10909 = 5$

$y = f(f(y)) = f(f(2)) = f(5) = (5^2+1) \bmod 10909 = 26$

$d = (|5-26|, 10909) = (21, 10909) = 1$

Pas 2 $x = f(x) = (5^2+1) \bmod 10909 = 26$

$y = f(f(y)) = f(f(26)) = f(677)$

$f(677) = (677^2+1) \bmod 10909 = 4581$

$d = (|26-4581|, 10909) = (4555, 10909) = 10909$

Algoritmul a eșuat.

Reluăm cu alte valori

Pas 3: Alegem $f(x) = (x^2+2) \bmod 10909$

$x = 3$, $y = 3$, $d = 1$

Pas 4: $x = f(x) = (3^2+2) \bmod 10909 = 11$

$y = f(f(y)) = f(f(3)) = f(11) = (11^2+2) \bmod 10909 = 123$

$d = (|11-123|, 10909) = (112, 10909) = 1$

Pas 5.

$x = f(x) = (11^2+2) \bmod 10909 = 123$

$y = f(f(y)) = f(f(123)) = f(4222) = (4222^2+2) \bmod 10909 =$

$f(123) = (123^2+2) \bmod 10909 = 15131 \bmod 10909 = 4222$

$17825284 \bmod 10909 = 10887$

$d = (|123 - 10887|, 10909) = (10764, 10909) = 1$

Pas 6:

$x = f(x) = (123^2+2) \bmod 10909 = 15131 \bmod 10909 = 4222$

$y = f(f(y)) = f(f(10887)) = f(486) = (486^2+2) \bmod 10909$

$f(10887) = (10887^2+2) \bmod 10909 = 486$

$= 236198 \bmod 10909 = 7109$

$d = (|4222 - 7109|, 10909) = (2887, 10909) = 1$

Algoritmul copiază din nou. Alegem alte valori

$f(x) = (x^2+3) \bmod 10909$

$x = 4$

Pas 7

$x = f(x) = (19 \bmod 10909 = 19$

$y = f(f(y)) = f(f(4)) = f(19) = 19^2+3 \bmod 10909 = 364$

$d = (|19 - 364|, 10909) = (345, 10909) = 1$

Pas 8

$x = f(x) = 19^2+3 \bmod 10909 = 364$

$y = f(f(y)) = f(f(364)) = f(1591) = 1591^2+3 \bmod 10909 = 396$

$f(364) = 364^2+3 \bmod 10909 = 1591$

$d = (|364 - 396|, 10909) = (32, 10909) = 1$

$f(x) = (x^2+1) \bmod 10909$ și $x_0 = 2$

1. $x = (2^2+1) \bmod 10909 = 5$
   $y = f(f(2)) = f(5) = (5^2+1) \bmod 10909 = 26$
   $d = (|x-y|, 10909) = (21, 10909) = 1$ (nu este divizor)
   5 - 26

2. $x = f(x) = 5^2+1 \bmod 10909 = 26$
   $y = f(f(5)) = f(26) = (26^2+1) \bmod 10909 = 677$
   $d = (|x-y|, 10909) = (|26-677|, 10909) = (651, 10909) = 1$
   (nu este divizor

3. $x = f(x) = f(26) = 677$
   $y = f(f(y)) = f(677) = (677^2+1) \bmod 10909 = 152$
   $d = (|677-152|, 10909) = (525, 10909) = 1$ (nu este divizor

4. $x = f(x) = f(677) = 152$
   $y = f(f(y)) = f(152) = (152^2+1) \bmod 10909 = 1287$
   $d = (|152-1287|, 10909) = (1135, 10909) = 1$

5. $x = f(x) = f(152) = 1287$
   $y = f(f(y)) = f(1287) = (1287^2+1) \bmod 10909 = 9111$
   $d = (|1287-9111|, 10909) = (7824, 10909) = 1$

6. $x = f(x) = f(1287) = 9111$
   $y = f(9111) = (9111^2+1) \bmod 10909 = 3741$
   $d = (|9111-3741|, 10909) = (5370, 10909) = 1$

7. $x = f(x) = f(9111) = 3741$
   $y = f(3741) = (3741^2+1) \bmod 10909 = 9744$
   $d = (|3741-9744|, 10909) = (6003, 10909)$

...

5) 23. Descompuneți numărul 16 547 în factori săi primi

$[\sqrt{n}] = 128$

$\sqrt{1,65,47}$ | 128

1

$=65$

44

2147

1984

$=163$

$22 \times 2 = 44$

$248 \times 8 = 1984$

a) $t = [\sqrt{n}] + 1 = 129$

$t^2 = 129^2 = 16641$

$t^2 - n = 16641 - 16547 = 94 \neq s^2$

b) $[\sqrt{n+1}] = 129 + 1 = 130$

$t^2 = 130^2 = 16900$

$t^2 - n = 16900 - 16547 = 353$

c) $[\sqrt{n+1}] = 130 + 1 = 131$

$t^2 = 131^2 = 17161$

$t^2 - n = 17161 - 16547 = 614 \neq s^2$

d) $[\sqrt{n+1}] = 131 + 1 = 132$

$t^2 = 13^2 = 17424$

$t^2 - n = 17424 - 16547 = 877 \neq s^2$

e) $t = 132 + 1 = 133$

$t^2 = 133^2 = 17689$

$t^2 - n = 17689 - 16547 = 1142 \neq s^2$

...

Numărul 16547 este prim