

Tema 4

5/

22.  $\sqrt{16365}$

găsiți  
factoarele  
în m. prime  
a m. 16365

$$\begin{array}{r} 127 \\ \hline 16365 \\ -127 \\ \hline 365 \\ -365 \\ \hline 0 \end{array}$$

$$m = 127$$

$$F(0) = 127^2 - 16365 = -240$$

$$F(1) = 128^2 - 16365 = 15 = 3 \cdot 5$$

$$F(2) = 129^2 - 16365 = 272 = 2^4 \cdot 17$$

$$F(3) = 130^2 - 16365 = 531 = 3^2 \cdot 59$$

$$F(4) = 131^2 - 16365 = 732 \\ = 3^2 \cdot 2^3 \cdot 11$$

$$F(5) = 132^2 - 16365 = 1055 \\ = 5 \cdot 211$$

$$F(6) = 133^2 - 16365 = 1320$$

$$= 2^3 \cdot 3 \cdot 5 \cdot 11 \\ \cancel{= 2^3 \cdot 3 \cdot 11 \cdot 5}$$

$$\begin{array}{r} 272 \\ 136 \\ 68 \\ 34 \\ 12 \\ 1 \end{array} \left| \begin{array}{r} 2 \\ 2 \\ 2 \\ 2 \\ 17 \\ 1 \end{array} \right.$$

$$\begin{array}{r} 531 \\ 177 \\ 59 \\ 1 \end{array} \left| \begin{array}{r} 3 \\ 3 \\ 59 \\ 1 \end{array} \right.$$

$$\begin{array}{r} 1055 \\ 211 \\ 1 \end{array} \left| \begin{array}{r} 5 \\ 211 \\ 1 \end{array} \right.$$

$$F(1) \cdot F(4) \cdot F(6) = 3^4 \cdot 5^2 \cdot 2^6 \cdot 11^2 \\ = (3^2 \cdot 5 \cdot 2^3 \cdot 11)^2 \\ = 3960^2 \equiv 128^2 \cdot 131^2 = 2230144^2 \\ \equiv 98^2 \pmod{16365}$$

$$3960^2 - 98^2 \equiv 0 \pmod{16365} \quad 16365$$

$$(3960 - 98)(3960 + 98) \equiv 0 \pmod{16365}$$

$$3862 \cdot 4058 \equiv 0 \pmod{16365}$$

$$(3862, 16365) \cdot (4058, 16365) = 16365$$

## Implementati algoritmul de factorizare Fermat

```
#include <iostream>
```

```
#include <cmath>
```

```
long long int fermat (long long int m) {
```

```
    if (m == 0) {
```

```
        return -1;
```

```
}
```

```
    if (m - 1 <= 0) {
```

```
        return 2;
```

```
}
```

```
    long long int a = ceil(sqrt(m));
```

```
    long long b2 = a * a - m;
```

```
    long long b = sqrt(b2);
```

```
    while (b * b != b2) { a = a + 1;
```

```
        b2 = a * a - m
```

```
        b = sqrt(b2); }
```

```
    }
```

```
    return a - b;
```

```
}
```

```
int main
```

```
long long int m;
```

```
std::cout << "Introduceti m : ";
```

```
std::cin >> m;
```

```
std::cout << "Factorul de factorizare primul << m <<
```

```
" este : " << fermat(m) << std::endl;
```

2/tema 4 return 0; };

realiză o compariție între algoritmi de primălitate studiați la secundărie.

1. Algoritmul lui Fermat este în general eficient pentru numerele mici. În schimb, algoritmul Miller-Rabin este unul dintre cele mai eficiente algoritmi pentru teste de primălitate și este utilizat pe scară largă. Este considerat sigur și folosit în multe aplicări criptografice.

Algoritmul lui Lehman (metoda Fermat) este mai rapid decât testul lui Fermat obisnuit, dar nu este la fel de eficient și sigur pentru numerele mici precum Miller-Rabin sau Solovay-Strassen. Complexitatea lui fiind  $O(\log n)^4$  ceea ce îl face mai puțin eficient.

Algoritmul Solovay - Strassen este considerat sigur, eficient, similar cu Miller - Rabin, dar mai lent. Complexitate:  $O(k \cdot \log^3 n)$  unde k este nr. de iterații. În următorul algoritm studiat, QS, este un algoritm avansat, eficient pentru numerele mici, dar devine impreună cu numerele foarte mari. Este folosit mai mult pentru factorizare.

În general, pentru teste de primălitate rapide și sigure pentru numerele mici, algoritmii Miller-Rabin și Solovay-Strassen sunt preferați. Algoritmul QS este potrivit pentru factorizare și nu este utilizat în fel de teste de primălitate. Algoritmul lui Fermat și al lui Lehman sunt mai fermecători, dar sunt utilizati în detectarea compozitelor și a altor numere.

adâncă limitați de

2. Studiați algoritmul lui Pollard și aplicați-l pentru  $10905$ , un număr de factorizare năo.

$$m = 10905$$

$$g(x) = (x^2 + 1) \bmod 10905$$

$$i = 1, x_0 = 2$$

$$x_1 = g(x_0) = g(2) = 5 \rightarrow$$

$$T = x_0$$

$$H = x_0$$

$$T \leftarrow g(T) \Rightarrow T = g^{(7)} \\ = g(x_0) = g(2)$$

$$= 5$$

$$H \leftarrow g(g(H)) = g(g(x_0))$$

$$= g(g(2)) = g(5) \\ = 26$$

$$\gcd(1-2T, 10905) = \gcd(21, 10905)$$

$$\gcd(1T - H, m) = 1$$

$$i = 2, x_1 = 5$$

$$x_2 = g(x_1) = g(5) = 26$$

$$T = x_1$$

$$H = x_1$$

$$\begin{array}{r} 26 \\ 26 \\ \hline 156 \end{array}$$

$$\begin{array}{r} 52 \\ 676 \\ \hline 676 \end{array}$$

$$T \leftarrow g(T) \Rightarrow T = g(T) = g(x_1) = g(5) = 26$$

$$H \leftarrow g(g(H)) = g(g(5)) = g(26) =$$

$$26^2 + 1 = 677$$

$$\gcd(1-651, 10905) = \gcd(651, 10905) = 1$$

$$\begin{array}{r} 677 - \\ 651 \\ \hline 26 \end{array}$$

$$i = 3, x_2 = 26$$

$$x_3 = g(x_2) = g(26) = 677$$

$$T = x_2$$

$$H = x_2$$

$$T \leftarrow g(T) \Rightarrow T = g(T) = g(x_2) = 677$$

$$H \leftarrow g(g(H)) = g(g(677)) = 1355$$

$$\gcd(678, 10905) = 67$$

$$x_5 = 677$$

$$= g(x_5) = 1355$$

$$T = x_3$$

$$H = x_3$$

$$T \leftarrow g(T) \rightarrow T = g(T) = g(677) = 1355$$

$$H \leftarrow g(g(H)) = g(g(677)) = g(1355) = 2711$$

$$\gcd(1356, 10309) = 1$$

$$\gcd(1356, 10309)$$

i	x	g	
1	5	26	1
2	26	677	67
3	677	1355	1
4	1355	2711	