Criptografie - Tema 3

Popescu Paul - Constantin
Facultatea de Matematică

1. Demonstrați că dacă $n = \prod_{i=i}^{k} p_i^{\alpha_i}$ şi $a^{p_i} \equiv a \pmod{p_i}, \forall p_i$, atunci $a^n \equiv a \pmod{n}$

2. Folosind exercițiul anterior, arătați că numerele 1729, 10585 și 75361 sunt numere Carmichael.

3. Arătați că dacă $2^n - 1$ este prim, atunci n este prim.

Vom demonstra că dacă $2^n - 1$ este un număr prim, atunci n trebuie să fie prim, folosind raționamentul prin contradicție.

Pasul 1: Presupunerea contrară
Presupunem că $2^n - 1$ este un număr prim și că n nu este prim, adică n este compus. Atunci, putem scrie n ca produsul a doi întregi pozitivi mai mici decât n:

$$n = ab, \quad \text{unde } a, b > 1.$$

Pasul 2: Factorizarea lui $2^n - 1$ Dacă $n = ab$, atunci putem rescrie:

$$2^n - 1 = 2^{ab} - 1.$$

Există un rezultat cunoscut în teoria numerelor, conform căruia pentru orice numere naturale x și y:

$$x^y - 1 = (x^{y_1} - 1)(x^{y_2} + x^{y_3} + \cdots + x^{y_k} + 1).$$

Aplicând această identitate pentru $x = 2^a$ și $y = b$, obținem:

$$2^{ab} - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right).$$

Astfel, $2^n - 1$ se poate scrie ca produsul a două numere mai mari decât 1: - $2^a - 1$, care este un număr mai mare decât 1 pentru $a > 1$, - Un al doilea factor care este, de asemenea, mai mare decât 1.

Pasul 3: Contradicția
Deoarece am presupus că $2^n - 1$ este prim, el nu poate fi scris ca produsul a două numere întregi pozitive mai mari decât 1. Dar am arătat că, dacă n este compus, atunci $2^n - 1$ este compus, ceea ce este o contradicție.

Concluzia
Prin urmare, n nu poate fi compus și trebuie să fie prim. Așadar, dacă $2^n - 1$ este un număr prim, atunci n este prim. $\square$

4. Demonstrați legea reciprocității pătratice.

Fie p și q două numere prime impare distincte. Atunci are loc relația:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}, \tag{1}$$

unde $\left(\frac{a}{p}\right)$ este simbolul lui Legendre definit ca:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{dacă } a \text{ este un pătrat perfect modulo } p, \\ -1, & \text{dacă } a \text{ nu este un pătrat perfect modulo } p, \\ 0, & \text{dacă } p \text{ divide } a. \end{cases} \tag{2}$$

Demonstrația Legii Reciprocității Pătratice
Vom prezenta o demonstrație bazată pe sumele Gaussiene.

Definiția Sumei Gaussiene
Se definește suma Gauss pentru un număr prim p:

$$G_p = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) e^{2\pi ik/p}. \tag{3}$$

Se poate demonstra că:

$$G_p^2 = \left(\frac{-1}{p}\right) p. \tag{4}$$

Proprietatea Fundamentală a Sumei Gaussiene
Se arată că pentru două numere prime impare p și q:

$$G_p G_q = \left(\frac{q}{p}\right) G_p G_q. \tag{5}$$

Comparând rezultatele pentru G_p^2 și G_q^2, obținem exact forma legii reciprocității pătratice.

$\square$

5. Implementați o funcție care să calculeze simbolul lui Jacobi.

simbolJacobi.hpp:

```cpp
#include <iostream>
using namespace std;

int simbolJacobi(int a, int n) {
   if (n <= 0 || n % 2 == 0)
   throw invalid_argument("n trebuie sa fie un numar impar pozitiv");

   a = a % n;
   int result = 1;

   while (a) {
      while (a % 2 == 0) {
         a /= 2;
         if (n % 8 == 3 || n % 8 == 5)
         result = -result;
      }

      a = a ^ n;
      n = a ^ n;
      a = a ^ n;

      if (a % 4 == 3 && n % 4 == 3)
      result = -result;

      a %= n;
   }

   return (n == 1) ? result : 0;
}
```

main.cpp

```cpp
#include "simbolJacobi.hpp";

int main()
{
   cout << simbolJacobi(93, 107) << endl;

   return 0;
}
```

6. Implementați algoritmul Solovay–Strassen.

`SolovayStrassen.hpp`:

```cpp
#include <iostream>
using namespace std;

int a_la_b_mod_c(int a, int b, int c) {

   a = a % c;
   int p = 1;
   while (b) {
      if (b % 2) {
         p = (p * a) % c;
      }
      a = (a * a) % c;
      b /= 2;
   }
   return p;
}

bool SolovayStrassen(long long n, int k) {
   if (n < 2) return false;
   if (n == 2 || n == 3) return true;
   if (n % 2 == 0) return false;

   srand(time(0));

   for (int i = 0; i < k; i++) {
      long long a = 2 + rand() % (n - 3);
      int jacobi = simbolJacobi(a, n);
      if (jacobi == 0) return false;

      long long rezultatTest = a_la_b_mod_c(a, (n - 1) / 2, n);

      if ((rezultatTest - jacobi) % n != 0)
      return false;
   }

   return true;
}
```

`main.cpp`

```cpp
#include "SolovayStrassen.hpp";

int main()
{
   int numar_teste = 3;
   cout << SolovayStrassen(929, numar_teste) << endl;

   return 0;
}
```

7. Algoritmul AKS (pdf separat)

8. Descrieți simbolul lui Kronecker.

In teoria numerelor, simbolul lui Kronecker, notat $\left(\frac{a}{n}\right)$ este o generalizare al simbolului lui Jacobi pentru toate numelele intregi n. A fost introdus in 1885, de catre Leopold Kronecker. Fie $n \in \mathbb{Z}, n \neq 0$. Prin factorizarea acestuia in numere prime obtinem:

$$n = u \cdot p_1^{e_1} + \cdots + p_k^{e_k}$$

unde $u = \pm 1$, iar numerele p_i sunt prime. Fie $a \in \mathbb{Z}$. Simbolul Kronecker $\left(\frac{a}{n}\right)$ este definit ca:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{u}\right) \prod_{k}^{i=1} \left(\frac{a}{p_i}\right)^{e_i}$$

Pentru p_i impare, numarul $\left(\dfrac{a}{n}\right)$ este doar simbolul lui Legendre.
Pentru cazul in care $p_i = 2$, definim $\left(\dfrac{a}{n}\right)$ ca:

$$\left(\frac{a}{2}\right) := \begin{cases} 0 & \text{daca } a \text{ este par} \\ 1 & \text{daca } a \equiv \pm 1 \pmod{8} \\ -1 & \text{daca } a \equiv \pm 3 \pmod{8} \end{cases}$$

Atunci cand $u = 1$, $\left(\dfrac{a}{n}\right) = 1$. Cand $u = -1$, acesta este definit:

$$\left(\frac{a}{-1}\right) := \begin{cases} 1 & \text{daca } a < 0 \\ -1 & \text{daca } a \geq 0 \end{cases}$$

In final, pentru $u = 0$ definim:

$$\left(\frac{a}{0}\right) := \begin{cases} 1 & \text{daca } a \pm 1 \\ 0 & \text{altfel} \end{cases}$$

9. Folosiți algoritmul Miller-Rabin pentru a determina primalitatea numărului 929 (cel mult 3 martori).

$$929 - 1 = 928 = 2^5 \cdot 29$$

$b = 2$
$\Rightarrow 2^{29} \pmod{929} = 883$
$\Rightarrow (2^{29})^2 \pmod{929} = 258$
$\Rightarrow (2^{29})^4 \pmod{929} = 605$
$\Rightarrow (2^{29})^8 \pmod{929} = -1$

$b = 3$
$\Rightarrow 3^{29} \pmod{929} = 701$
$\Rightarrow (3^{29})^2 \pmod{929} = 889$
$\Rightarrow (3^{29})^4 \pmod{929} = 671$
$\Rightarrow (3^{29})^8 \pmod{929} = 605$
$\Rightarrow (3^{29})^{16} \pmod{929} = -1$

$b = 5$
$\Rightarrow 5^{29} \pmod{929} = 911$
$\Rightarrow (5^{29})^2 \pmod{929} = 324$
$\Rightarrow (5^{29})^4 \pmod{929} = -1$

$\Rightarrow$ numărul 929 este prim.

10. Folosind QS sau Fermat, factorizați numarul 6767.

$$\sqrt{6767} \approx 82.26 \Rightarrow \lfloor\sqrt{6767}\rfloor = 82$$
$$t = \lfloor\sqrt{6767}\rfloor + 1 = 83$$
$$t^2 - n = 83^2 - 6767 = 122 \neq s^2$$

$$t = 84$$
$$t^2 - n = 84^2 - 6767 = 289 = 17^2 = s^2$$

$$t = 84, s = 17 \Rightarrow b = 101, a = 67 \Rightarrow 101 \cdot 67 = 6767$$