Seminar 2 - Criptografie

Popescu Paul - Constantin
Facultatea de Matematică

Exercitiul 1.

$$\text{d) } (1547, 560) = 7$$

$$\begin{aligned}
1547 &= 2 \cdot 560 + 427 & x_{1547} &= (1,0), x_{560} = (0,1) \\
560 &= 1 \cdot 427 + 133 & x_{427} &= x_{1547} - 2 \cdot x_{560} = (1,0) - 2 \cdot (0,1) = (1,-2) \\
427 &= 3 \cdot 133 + 28 & x_{133} &= x_{560} - 1 \cdot x_{427} = (0,1) - (1,-2) = (-1,3) \\
133 &= 4 \cdot 28 + 21 & x_{28} &= x_{427} - 3 \cdot x_{133} = (1,-2) - 3 \cdot (-1,3) = (4,-11) \\
28 &= 1 \cdot 21 + 7 & x_{21} &= x_{133} - 4 \cdot x_{28} = (-1,3) - 4 \cdot (4,-11) = (-17,47) \\
21 &= 3 \cdot 7 + 0 & x_7 &= x_{28} - 1 \cdot x_{21} = (4,-11) - (-17,47) = (21,-58)
\end{aligned}$$

$$\Rightarrow 7 = 21 \cdot 1547 - 58 \cdot 560$$

Exercitiul 2.

$$\text{a) } \varphi(30) = 8 \quad \Rightarrow 1, 7, 11, 13, 17, 19, 23, 29$$

$$\text{c) } \varphi(800) = 800 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 800 \cdot \frac{1}{2} \cdot \frac{4}{5} = 320$$

Exercitiul 3.

$$\text{a) } 122x \equiv 1 (\text{mod} 343) \Rightarrow (122, 343) = ?$$

$$\begin{aligned}
343 &= 2 \cdot 122 + 99 \\
122 &= 1 \cdot 99 + 23 \\
99 &= 4 \cdot 23 + 7 \\
23 &= 3 \cdot 7 + 2 \\
7 &= 2 \cdot 3 + 1
\end{aligned}$$

$$x \equiv 122^{-1} (\text{mod} 343)$$

$$\begin{aligned}
99 = 343 - 2 \cdot 122 &\Rightarrow x_{99} = x_{343} - 2 \cdot x_{122} = (0,1) - 2(1,0) = (-2,0) \\
23 = 122 - 99 &\Rightarrow x_{23} = x_{122} - x_{99} = (1,0) - (-2,0) = (3,0) \\
7 = 99 - 4 \cdot 23 &\Rightarrow x_7 = x_{99} - 4 \cdot x_{23} = (-2,0) - 4(3,0) = (-14,0) \\
2 = 23 - 3 \cdot 7 &\Rightarrow x_2 = x_{23} - 3 \cdot x_7 = (3,0) - 3(-14,0) = (45,0) \\
3 = 2 - 1 \cdot 1 &\Rightarrow x_3 = x_2 - 1 \cdot x_1 = (45,0) - 1(-14,0) = (59,0) \\
1 = 7 - 2 \cdot 3 &\Rightarrow x_1 = x_7 - 2 \cdot x_3 = (-14,0) - 2(59,0) = (-132,0)
\end{aligned}$$

$$\Rightarrow x \equiv 211 \pmod{343}$$

Programe (C++):

cripto_tools.hpp:

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

int modulo(int a, int n) {
   if (a >= 0 && n > 0)
      return a % n;
   if (a < 0 && n > 0)
      return a % n + n;
   if (n == 0)
      return -1;
}

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;
}

int cmmdc(int a, int b) {
   if (a * b == 0) return a + b;    //if (a == 0) return b; if (b == 0) return a;

   int rest = 0;
   while (b) {
      rest = modulo(a, b);
      a = b;
      b = rest;
   }
   return a;
}

int invers(int a, int n) {
   int q, r, x0 = 1, x1 = 0, copy_n = n;
   a = modulo(a, n);
   while (n) {
      r = n;
      q = a / n;
      n = a % n;
      a = r;

      r = x1;
      x1 = x0 - q * x1;
      x0 = r;
   }
   if (a == 1)
      return modulo(x0, copy_n);
   return -1;
}
```

main.cpp:

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

int main()
{
   cout << a_la_b_mod_c(25, 28, 29) << endl;  //raspuns: 1

   cout << cmmdc(360, 294) << endl;  //raspuns: 6
   cout << cmmdc(1547, 560) << endl;  //raspuns: 7

   cout << invers(122, 343) << endl;  //raspuns: 211

   return 0;
}
```