

# Theoretical Foundations

## Introduction to Computational Number Theory - Part 4

Jean-Sébastien Coron

Université du Luxembourg

October 10, 2009

- C programming
  - Functions
- Algorithmic number theory
  - Modular arithmetic.
  - Solving linear congruence equations.
  - Chinese remainder theorem.

- Syntax :

- `rtype fname(para1,para2,...)`  
  {  
    localvariables  
    functioncode  
  }

- Example :

- `double max(double a,double b)`  
  {  
    double m;  
    if(a>b) m=a; else m=b;  
    return m;  
  }

# Using the function

- ```
#include <stdio.h>
double max(double a,double b)
{
    double m;
    if(a>b) m=a; else m=b;
    return m;
}
int main()
{
    double x=3.5;
    double y=3.2;
    double z=max(x,y);
}
```

# void function

- A void function is a function that returns nothing.

```
#include <stdio.h>
void affiche(int a)
{
    printf("La valeur est:%d\n",a);
}
```

```
int main()
{
    int u=3;
    affiche(u);
}
```

# Printing an array

```
#include <stdio.h>
void affiche(int tab[],int n)
{
    int i;
    for(i=0;i<n;i++) printf("%d ",tab[i]);
    printf("\n");
}

int main()
{
    int t[5]={1,3,6,5,1}
    affiche(t,5);
}
```

- Let an integer  $n > 1$  called the modulus.
- Modular reduction
  - $r := a \bmod n$ , remainder of the division of  $a$  by  $n$ .
  - $0 \leq r < n$
  - Ex:  $11 \bmod 8 = 3$ ,  $15 \bmod 5 = 0$ .
- Congruence:
  - $a \equiv b \pmod n$  if  $n \mid (a - b)$ .
  - $a \equiv b \pmod n$  iif  $a$  and  $b$  have same remainder modulo  $n$ .
  - Ex:  $11 \equiv 19 \pmod 8$ .
  - If  $r := a \bmod n$ , then  $r \equiv a \pmod n$ .

- If  $a_0 \equiv b_0 \pmod{n}$  and  $a_1 \equiv b_1 \pmod{n}$ 
  - $a_0 + a_1 \equiv b_0 + b_1 \pmod{n}$
  - $a_0 - a_1 \equiv b_0 - b_1 \pmod{n}$
  - $a_0 \cdot a_1 \equiv b_0 \cdot b_1 \pmod{n}$
- Integers modulo  $n$ 
  - Integers modulo  $n$  are  $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$
  - Addition, subtraction or multiplication in  $\mathbb{Z}_n$  is done by first doing it in  $\mathbb{Z}$  and then reducing the result modulo  $n$ .
  - For example in  $\mathbb{Z}_7$ :
    - $6 + 4 = 3, 3 - 4 = 6, 3 \cdot 6 = 4.$



# Solving linear congruence

- Theorem: let two integers  $a, n$  with  $n > 0$  such that  $\text{PGCD}(a, n) = 1$ . Let  $b \in \mathbb{Z}$ . The equation  $a \cdot x \equiv b \pmod{n}$  has a unique solution  $x$  modulo  $n$ .
  - Let  $a^{-1}$  by the multiplicative inverse of  $a$  modulo  $n$ .

$$a \cdot a^{-1} \cdot x \equiv x \equiv a^{-1} \cdot b \pmod{n}$$

- Example :
  - Find  $x$  such that  $5 \cdot x \equiv 6 \pmod{7}$
  - 3 is the inverse of 5 modulo 7 because  $5 \cdot 3 \equiv 1 \pmod{7}$ .
  - $3 \cdot 5 \cdot x \equiv 15 \cdot x \equiv 1 \cdot x \equiv 3 \cdot 6 \equiv 4 \pmod{7}$
  - $x \equiv 4 \pmod{7}$

- Modular quotient  $b/a \pmod n$ .
  - Let  $a, b \in \mathbb{Z}$ , and  $n$  a modulus.
  - If  $\text{PGCD}(a, n) = 1$ , then one defines the *modular quotient*  $b/a \pmod n$  as  $b \cdot a^{-1} \pmod n$ .
  - With  $a^{-1}$  the multiplicative inverse of  $a$  modulo  $n$ .
- If  $c \equiv b/a \pmod n$ , then  $a \cdot c \equiv b \pmod n$ 
  - $c$  is solution of  $a \cdot x \equiv b \pmod n$
- Example :
  - $5/3 \equiv 4 \pmod 7$

- Chinese remainder theorem

- Let two integers  $n_1 > 1$  and  $n_2 > 0$  with  $\text{PGCD}(n_1, n_2) = 1$ .
- For all  $a_1, a_2 \in \mathbb{Z}$ , there exists an integer  $z$  such that

$$z \equiv a_1 \pmod{n_1}$$

$$z \equiv a_2 \pmod{n_2}$$

- $z$  is unique modulo  $n_1 \cdot n_2$ .

- Existence :

- Let  $m_1 = (n_2)^{-1} \pmod{n_1}$  and  $m_2 = (n_1)^{-1} \pmod{n_2}$

$$z := n_2 \cdot m_1 \cdot a_1 + n_1 \cdot m_2 \cdot a_2$$

- $z \equiv (n_2 \cdot m_1) \cdot a_1 \equiv a_1 \pmod{n_1}$
  - $z \equiv (n_1 \cdot m_2) \cdot a_2 \equiv a_2 \pmod{n_2}$
- Unicity modulo  $n_1 \cdot n_2$ 
    - Let  $z'' = z - z'$ . Then  $n_1 | z''$  and  $n_2 | z''$ .
    - Since  $\text{PGCD}(n_1, n_2) = 1$ ,  $n_1 \cdot n_2 | z''$ .
    - $z \equiv z' \pmod{n_1 \cdot n_2}$