# Mathematics and Cryptography

## Course 2

Jean-Sébastien Coron

University of Luxembourg

# Summary

- Introduction to algorithmic number theory
  - Modular arithmetic.
  - Solving linear congruence equations.
  - Chinese remainder theorem.

# Modular arithmetic

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

# Modular arithmetic

- If $a_0 \equiv b_0 \mod n$ and $a_1 \equiv b_1 \mod n$
  - $a_0 + a_1 \equiv b_0 + b_1 \mod n$
  - $a_0 - a_1 \equiv b_0 - b_1 \mod n$
  - $a_0 \cdot a_1 \equiv b_0 \cdot b_1 \mod n$
- Integers modulo $n$
  - Integers modulo $n$ are $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
  - 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 $\mathbb{Z}_7$:
    - $6 + 4 = 3$, $3 - 4 = 6$, $3 \cdot 6 = 4$.

# Multiplicative inverse

- Multiplicative inverse :
  - Let $n > 0$ and $a \in \mathbb{Z}$. An integer $a'$ is a *multiplicative inverse* of $a$ modulo $n$ if $a \cdot a' \equiv 1 \mod n$.
- Theorem :
  - Let $n, a \in \mathbb{Z}$ with $n > 0$. Then $a$ has a multiplicatif inverse modulo $n$ iff $\text{PGCD}(a, n) = 1$.
  - Proof ($\Rightarrow$)
    - If $a'$ is a multiplicative inverse of $a$ modulo $n$, then $a \cdot a' \equiv 1 \mod n$.
    - Let $k \in \mathbb{Z}$ such that $a \cdot a' = 1 + k \cdot n$.
    - If $d|a$ and $d|n$, then $d|1$. Therefore $\text{PGCD}(a, n) = 1$.

# Example

- A multiplicative inverse of 5 modulo 7 is 3 because

$$3 \cdot 5 \equiv 15 \equiv 1 \mod 7$$

- 2 has no multiplicative inverse modulo 6 :
  - $2 \cdot 1 \equiv 2 \mod 6$
  - $2 \cdot 2 \equiv 4 \mod 6$
  - $2 \cdot 3 \equiv 0 \mod 6$
  - $2 \cdot 4 \equiv 2 \mod 6$
  - $2 \cdot 5 \equiv 4 \mod 6$

# 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 $a \cdot x \equiv b \mod n$ has a unique solution $x$ modulo $n$.
  - Let $a^{-1}$ by the multiplicative inverse of $a$ modulo $n$.

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

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

# Modular division

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

# Chinese remainder theorem

- 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

$$\begin{aligned} z &\equiv a_1 \mod n_1 \\ z &\equiv a_2 \mod n_2 \end{aligned}$$

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

# Proof

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

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

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