Introduction to Public-Key Cryptography

Jean-Sébastien Coron

Université du Luxembourg

October 12, 2015

Course 4

- Basics of number theory for public-key cryptography
  - GCD
  - Euclid's algorithm
  - Euclid's extended algorithm
  - Modular arithmetic.

GCD

- Common divisor :
  - Let a, b be two integers. A common divisor of a and b is an integer m such that $m|a$ and $m|b$.
- GCD.
  - GCD of two integers a and b is the greatest common divisor of a and b.
  - If $d = \text{GCD}(a, b)$, then for all m such that $m|a$ and $m|b$, we have $m|d$.
- Example
  - $\text{GCD}(9, 6) = 3$
  - $\text{GCD}(7, 5) = 1$.

Euclid's algorithm

- Euclid's algorithm :
  - Input: a, b.
  - Let $r_0 = a$ and $r_1 = b$.
  - For $i \geq 0$, one defines the sequence (r_i) and (q_i) such that :

$$r_i = q_i \cdot r_{i+1} + r_{i+2}$$

    where q_i and r_{i+2} are the quotient and remainder of the division of r_i by r_{i+1}
  - The exists $k > 0$ such that $r_k = 0$.
  - Then $\mathrm{GCD}(a, b) = r_{k-1}$.

Proof

- Let $a > 0$ and $b \geq 0$.
  - If $b = 0$, then $\mathrm{GCD}(a, b) = \mathrm{GCD}(a, 0) = a$
  - Otherwise, let $a = b \cdot q + r$ with $0 \leq r < b$.
  - Then $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$.
  - (b, r) is less than (a, b).
- $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$
  - If $d|a$ and $d|b$, then $d|r$, and then $d|\mathrm{GCD}(b, r)$. Then $\mathrm{GCD}(a, b)|\mathrm{GCD}(b, r)$.
  - If $d'|b$ and $d'|r$, then $d'|a$, and then $d'|\mathrm{GCD}(a, b)$. Then $\mathrm{GCD}(b, r)|\mathrm{GCD}(a, b)$.
  - Then $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$.

Basic Properties of Integers

Theorem (Fundamental theorem of arithmetic)

Every non-zero integer n can be expressed as

$$n = \pm p_i^{e_1} \cdots p_r^{e_r}$$

where the p_i's are distinct primes and the e_i are positive integers. Moreover the decomposition is unique, up to reordering of the primes.

- Proof: existence is easy by recursion; unicity: see any standard textbook.

Basic Properties of Integers

Theorem (Division with remainder property)

For $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

Congruence

- Definition
  - Let $n > 0$, and $a, b \in \mathbb{Z}$.
  - a is *congruent* to b if $n|(a - b)$.
  - $a \equiv b \pmod{n}$.
  - n is called the *modulus*.
  - Should not be confused with the *mod* of Euclidean division.

Theorem

Let $n > 0$. For any integer a, there exists a unique integer b such that $a \equiv b \pmod{n}$ and $0 \leq b < n$, namely $b := a \bmod n$.

Examples and properties

- Examples :
  - $2 \equiv 8 \mod 3$ since $3|(8-2)$.
  - $12 \equiv 2 \mod 5$ since $5|(12-2)$.
- Properties :
  - $a \equiv b \mod n \Leftrightarrow \exists k \in \mathbb{Z}, a = b + k \cdot n$.
  - $a \equiv a \mod n$
  - $a \equiv b \mod n \Rightarrow b \equiv a \mod n$
  - $a \equiv b \mod n$ and $b \equiv c \mod n$ implies $a \equiv c \mod n$

Properties

- Addition and multiplication
  - If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then
  - $a + b \equiv a' + b' \mod n$ and $a \cdot b \equiv a' \cdot b' \mod n$.
- When computing modulo n, one can substitute to x a value x' congruent to x modulo n.
  - Computing a with $0 \leq a < 8$ such that $a \equiv 83 \cdot 72 \mod 7$.
  - First solution: $83 \cdot 72 = 5976$
    $a = 5976 \mod 7 = 5$.
  - Second solution: $83 \equiv 6 \mod 7$, $72 \equiv 2 \mod 7$,
    $83 \cdot 72 \equiv 6 \cdot 2 \equiv 12 \equiv 5 \mod 7$.

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 :
  - $2 \cdot 1 \equiv 2 \mod 6$
  - $2 \cdot 2 \equiv 4 \mod 6$
  - $2 \cdot 3 \equiv 0 \mod 6$
  - $2 \cdot 4 \equiv 2 \mod 6$
  - $2 \cdot 5 \equiv 4 \mod 6$

Euclid's extended algorithm

- Euclid's extended algorithm
  - Let $a, b \in \mathbb{Z}$ and $d = \text{PGCD}(a, b)$.
  - Computes $s, t \in \mathbb{Z}$ such that $a \cdot s + b \cdot t = d$.
- Multiplicative inverse.
  - Let a, n with $n > 0$ and $\text{PGCD}(a, n) = 1$.
  - With Euclid's extended algorithm, one computes s, t such that
    $$a \cdot s + n \cdot t = 1$$
  - Then $a \cdot s \equiv 1 \mod n$
  - s is one multiplicative inverse of a modulo n.

Euclid's extended algorithm

- Euclid's extended algorithm, for $a > 0$ and $b \geq 0$.
  - Two additional sequences u_i and v_i.
  - $r_0 = a$ and $r_1 = b$.
  - For $i \geq 0$, let $r_i = q_i \cdot r_{i+1} + r_{i+2}$
  - $u_0 := 1,\ v_0 := 0,\ u_1 := 0,\ v_1 := 1$ and for $i \geq 2$, one defines $u_i = u_{i-2} - q_{i-2} \cdot u_{i-1}$ and $v_i = v_{i-2} - q_{i-2} \cdot v_{i-1}$.
- There exists $k > 0$ such that $r_k = 0$.
  - Then $\mathrm{PGCD}(a, b) = r_{k-1} = u_{k-1} \cdot a + v_{k-1} \cdot b$.

Proof

- We always have $r_i = u_i \cdot a + v_i \cdot b$.
  - True for $r_0 = a = 1 \cdot a + 0 \cdot b$.
  - True for $r_1 = b = 0 \cdot a + 1 \cdot b$.
  - If $r_{i-2} = u_{i-2} \cdot a + v_{i-2} \cdot b$ and $r_{i-1} = u_{i-1} \cdot a + v_{i-1} \cdot b$, then :

$$\begin{aligned} u_i \cdot a + v_i \cdot b &= (u_{i-2} - q_{i-2} \cdot u_{i-1}) \cdot a + \\ &\quad (v_{i-2} - q_{i-2} \cdot v_{i-1}) \cdot b \\ &= r_{i-2} - q_{i-2} \cdot r_{i-1} \\ &= r_i \end{aligned}$$

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 $\mathbb{Z}_7$:
    - $6 + 4 = 3$, $3 - 4 = 6$, $3 \cdot 6 = 4$.