Algorithms for Numbers and Public-Key Cryptography

Jean-Sébastien Coron

University of Luxembourg

February 26, 2018

Course Summary

- Algorithms for numbers
  - Describe basic algorithms for dealing with numbers
  - Implement them on a computer
- Public-key cryptography
  - Describe the basic public-key algorithms
  - Implement them on a computer

Course organization

- The course is based on lectures, homework and personal projects.
- Homework:
  - Implementation of the basic algorithms described in the lectures.
- Personal projects:
  - To be chosen among a list of possible topics. But you can also select your own topic.
  - You are encouraged to work in pairs.
  - Selection of project to be done before late March.

Course 1

- Basic number theory.
  - 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 $d = \mathrm{GCD}(a, b)$, then for all m such that $m|a$ and $m|b$, we have $m|d$.
- Example
  - $\mathrm{GCD}(9, 6) = 3$
  - $\mathrm{GCD}(7, 5) = 1$.

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

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 $\mathrm{PGCD}(a, n) = 1$.
  - 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 $\mathrm{PGCD}(a, n) = 1$.

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 $d = \mathrm{PGCD}(a, b)$.
  - Computes $s, t \in \mathbb{Z}$ such that $a \cdot s + b \cdot t = d$.
- Multiplicative inverse.
  - Let a, n with $n > 0$ and $\mathrm{PGCD}(a, n) = 1$.
  - 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 $\mathbb{Z}_7$:
    - $6 + 4 = 3$, $3 - 4 = 6$, $3 \cdot 6 = 4$.

Solving linear congruence

- Theorem: let two integers a, n with $n > 0$ such that $\mathrm{PGCD}(a, n) = 1$. 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 $\mathrm{PGCD}(a, n) = 1$, 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
  - Let two integers $n_1 > 1$ and $n_2 > 0$ with $\mathrm{PGCD}(n_1, n_2) = 1$.
  - 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 $\mathrm{PGCD}(n_1, n_2) = 1$, $n_1 \cdot n_2 | z''$.
  - $z \equiv z' \mod (n_1 \cdot n_2)$

Euler function

- Definition:
  - $\phi(n)$ for $n > 0$ is defined as the number of integers a comprised between 0 and $n-1$ such that $\gcd(a, n) = 1$.
  - $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$.
- Equivalently:
  - Let $\mathbb{Z}_n^*$ be the set of integers a comprised between 0 and $n-1$ such that $\gcd(a, n) = 1$.
  - Then $\phi(n) = |\mathbb{Z}_n^*|$.

Properties

- If $p \geq 2$ is prime, then

$$\phi(p) = p - 1$$

- More generally, for any $e \geq 1$,

$$\phi(p^e) = p^{e-1} \cdot (p - 1)$$

- For $n, m > 0$ such that $\gcd(n, m) = 1$, we have:

$$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$$

$\phi(p^e) = p^{e-1} \cdot (p-1)$

- If p is prime
  - Then for any integer $1 \leq a < p$, $\gcd(a, p) = 1$
  - Therefore $\phi(p) = p - 1$
- For $n = p^e$, the integers between 0 and n not co-prime with n are
  - $0, p, 2 \cdot p, \ldots, (p^{e-1} - 1) \cdot p$
  - There are p^{e-1} of them.
  - Therefore, $\phi(p^e) = p^e - p^{e-1} = p^{e-1} \cdot (p-1)$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$

- Consider the map:

$$\begin{array}{rcl} f : \mathbb{Z}_{nm}^* & \to & \mathbb{Z}_n^* \times \mathbb{Z}_m^* \\ a & \to & (a \mod n, a \mod m) \end{array}$$

  - From the Chinese remainder theorem, the map is a bijection.
  - Moreover, $\gcd(a, n \cdot m) = 1$ if and only if $\gcd(a, n) = 1$ and $\gcd(a, m) = 1$.
  - Therefore, $|\mathbb{Z}_{nm}^*| = |\mathbb{Z}_n^*| \cdot |\mathbb{Z}_m^*|$
  - This implies $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

Theorem

- If $n = p_1^{e_1} \dots p_r^{e_r}$ is the factorization of n into primes, then :

$$\phi(n) = \prod_{i=1}^{r} p_i^{e_i - 1} \cdot (p_i - 1) = n \prod_{i=1}^{r} (1 - 1/p_i)$$

  - Proof: immediate consequence of the two previous properties.

Multiplicative order

- The multiplicative order of an integer a modulo n is defined as the smallest integer $k > 0$ such that

$$a^k \equiv 1 \mod n$$

- Example

i	1	2	3	4
$1^i \mod 5$	1	1	1	1
$2^i \mod 5$	2	4	3	1
$3^i \mod 5$	3	4	2	1
$4^i \mod 5$	4	1	4	1

  - Modulo 5, 1 has order 1, 2 and 3 have order 4, and 4 has order 2.

Euler's theorem

- Theorem
  - For any integer $n > 1$ and any integer a such that $\gcd(a, n) = 1$, we have $a^{\phi(n)} \equiv 1 \mod n$.
- Proof
  - Consider the map $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$, such that $f(b) = a \cdot b$ for any $b \in \mathbb{Z}^*$.
  - f is a permutation, therefore :

$$\prod_{b \in \mathbb{Z}_n^*} b = \prod_{b \in \mathbb{Z}_n^*} (a \cdot b) = a^{\phi(n)} \cdot \left(\prod_{b \in \mathbb{Z}_n^*} b \right)$$

  - Therefore, we obtain $a^{\phi(n)} \equiv 1 \mod n$.

Fermat's little theorem

- Theorem
  - For any prime p and any integer $a \neq 0 \mod p$, we have $a^{p-1} \equiv 1 \mod p$. Moreover, for any integer a, we have $a^p \equiv a \mod p$.
- Proof
  - Follows from Euler's theorem and $\phi(p) = p - 1$.