Théorie algorithmique des nombres

Cours no. 8

Jean-Sébastien Coron

Université du Luxembourg

November 8, 2009

Summary

- Algorithmic number theory.
  - Euler function.
  - Fermat little theorem.

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:

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

  - 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 $f : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$, 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 $\phi(p) = p - 1$.