Some slides for 4th Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

18-09-2012

Euler's theorem

For RSA:

- $N = p \cdot q$, p and q primes.
- e a number for encription, d a number for decription.
- Public: N, e. Private: d.
- Message: $X, 0 \leq X < N$.
- Encription: $f(X) = [X^e]_N$
  Decription: $g(X) = [X^d]_N$.
  $g(f(X)) = X$.

Question: How do we choose e and d?
Answer: Using Euler's φ function

Euler's theorem

$$(\mathbb{Z}/N)^* = \{X \in \mathbb{Z}/N : \gcd(X, N) = 1\},$$

for $N \in \mathbb{N}$

Euler's φ-function:

$$\varphi(N) = \mid (\mathbb{Z}/N)^* \mid$$

Proposition 1.7.1

Let $m, n \in \mathbb{N}$, relative prime. Then

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Proof:

- Let $N = mn$, consider remainder map
$$r : \mathbb{Z}/N \to \mathbb{Z}/m \times \mathbb{Z}/n$$
- Claim:
$$r((\mathbb{Z}/N)^*) = (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$$

Hence, the result holds because r is bijective.

The claim: $r((\mathbb{Z}/N)^*) = (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$

$$\gcd(X, N) = 1 \Leftrightarrow \gcd([X]_m, m) = 1, \gcd([X]_n, n) = 1$$

- By Proposition 1.5.1(ii),

$$\begin{cases} \gcd(X, m) = \gcd([X]_m, m) \\ \gcd(X, n) = \gcd([X]_n, n) \end{cases}$$

- But, by Corollary 1.5.11,

$$\left.\begin{array}{r} \gcd(X, m) = 1 \\ \gcd(X, n) = 1 \end{array}\right\} \Leftrightarrow \gcd(X, nm) = 1$$

Theorem 1.7.2 (Euler)

Let $n \in \mathbb{N}$, $a \in \mathbb{Z}$ relative prime. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof:

- List the numbers (lower than n) relative prime to n:

$$0 < a_1 < \cdots < a_{\varphi(n)} < n$$

Claim: $\{[aa_1]_n, \ldots, [aa_{\varphi(n)}]_n\} = \{a_1, \ldots, a_{\varphi(n)}\}$

- $[aa_i]_n = [aa_j]_n \Rightarrow n \mid a(a_i - a_j) \Rightarrow n \mid (a_i - a_j) \Rightarrow i = j$.
- $\gcd(n, aa_i) = 1 \Rightarrow \gcd(n, [aa_i]_n) = 1$

- Hence $[aa_1]_n \cdots [aa_{\varphi(n)}]_n = a_1 \cdots a_{\varphi(n)}$
- Then $aa_1 \cdots aa_{\varphi(n)} \equiv a_1 \cdots a_{\varphi(n)} \pmod{n}$, but $aa_1 \cdots aa_{\varphi(n)} = a^{\varphi(n)} a_1 \cdots a_{\varphi(n)}$.
- That is, $n \mid a_1 \cdots a_{\varphi(n)}(a^{\varphi(n)} - 1)$.
- By corollary 1.5.10, $n \mid (a^{\varphi(n)} - 1)$.
- That is, $a^{\varphi(n)} \equiv 1 \pmod{n}$

Prime numbers

A prime number is a natural number $p > 1$ such that

$$\mathrm{div}(p) = \{1, p\}$$

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

Lemma 1.8.1

Every non-zero natural number $n \in \mathbb{N} \setminus \{0\}$ is a product of prime numbers.

Proof by induction:

1. 1 is the empty product of prime numbers by definition.
2. Assume that for $m < n$, m is product of primes. Is n prime?
    - Yes. Then $n = n$ is product of primes.
    - No. Then $n = n_1 n_2$. With $n_1, n_2 < n$. Apply induction hypothesis.

Theorem 1.8.2 (Euclid)

There are infinitely many prime numbers

Proof:

- Assume that $p_1, \ldots, p_n$ are all the prime numbers.
- Set $N = p_1 \cdots p_n + 1$
- By previous lemma, there exists p such that $p \mid N$.
- However, $p_i \nmid N$ for all i. Therefore, we have a new prime.

Lemma 1.8.3

Let p be a prime number and suppose that $p \mid ab$, where, $a, b \in \mathbb{Z}$. Then, $p \mid a$ or $p \mid b$.

Proof:

- If $p \mid a$ we finish.
- If $p \nmid a$, then $\gcd(a, p) = 1$

Hence by corollary 1.5.10 $p \mid b$.

Theorem 1.8.5

Every natural number can be factored uniquely into a product of prime numbers (up to changing the order)

Proof:

- For $n = 1$ is trivial ($1 =$ empty product of prime numbers).
- For $n > 1$, $n = p_1 \cdots p_r = q_1 \cdots q_s$.
- If there exists i such that $p_i \in \{q_1, \ldots, q_s\}$, divide both sides by p_i. So we assume $p_i \neq q_j$ for all i, j.
- Since $p_1 \mid q_1 \cdots q_s$, we have $p_1 \mid q_1$, or $p_1 \mid q_2$, ..., or $p_1 \mid q_s$.
- If $p_i \mid q_j \Rightarrow p_i = q_j$, contradiction.

With factorization into a product of prime numbers:

- Divisors
- Greatest common divisor
- Least common multiple

Can this be used to compute $\varphi(n)$?

Computing $\varphi(n)$

knowing the prime factorization of a number:

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_s^{r_s}),$$

where $n = p_1^{r_1} \cdots p_s^{r_s}$, $p_i \neq p_j$ for all $i \neq j$.

How do we compute $\varphi(p^m)$?

Computing $\varphi(n)$

knowing the prime factorization of a number:

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_s^{r_s}),$$

where $n = p_1^{r_1} \cdots p_s^{r_s}$, $p_i \neq p_j$ for all $i \neq j$.

How do we compute $\varphi(p^m)$?

- $\gcd(x, p) = 1 \Leftrightarrow p \nmid x$
- $x \leq p^m$ is NOT relative prime to $p^m \Leftrightarrow p \mid x$

Hence, $\varphi(p^m) = p^m - p^{m-1}$.

$$\varphi(n) = (p_1^{r_1} - p_1^{r_1-1}) \cdots (p_s^{r_s} - p_s^{r_s-1}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)$$