Some slides for 4th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

17-09-2010

From last lecture

Lemma 1.8.1

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

Theorem 1.8.2 (Euclid)

There are infinitely many prime numbers

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 $p \mid b$.

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 $p_i \neq p_j$ 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, $\varphi(p^m) = p^m - p^{m-1}$.

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

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: $g(X) = [X^d]_N$.
  $g(f(X)) = X$.

How do we choose e and d?

We know:
$g(f(X)) = [[X^e]^d] = [X^{ed}] = X$ if and only if $X \equiv X^{ed} \pmod N$
$\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$

Let X be any integer and k a natural number. Then

$$X^{k(p-1)(q-1)+1} \equiv X (\mathrm{mod}\ N)$$

Proof:

- It is enough to prove that $X^{k(p-1)(q-1)+1} \equiv X (\mathrm{mod}\ p)$.
- If $p \mid x$. Thus, $[X]_p = 0 = [X^{k(p-1)(q-1)+1}]_p$, we have $X^{k(p-1)(q-1)+1} \equiv X (\mathrm{mod}\ N)$.
- If $p \nmid x$. Thus, $\gcd(p, x) = 1$, by Euler Theorem $X^{\varphi(p)} = X^{p-1} \equiv 1 (\mathrm{mod}\ p)$ and

$$X^{k(p-1)(q-1)} \equiv (X^{p-1})^{k(q-1)} \equiv 1 (\mathrm{mod}\ p)$$

- Multiply the previous congruence with X

Encryption and decryption exponents

Finding astronomical prime numbers

Fermat's little theorem

Let p be a prime number and a an integer with $gcd(a, p) = 1$. Then
$$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

Definition 1.9.3

Let N be a composite natural number and a an integer. Then N is called a pseudoprime relative to the base a if
$$a^{N-1} \equiv 1 (\mathrm{mod}\ N)$$

- $gcd(a, N) \neq 1 \Rightarrow$ N cannot be a pseudoprime relative to a (EX 1.41).
- Carmichael numbers (or pseudoprimes).

Lemma 1.9.4

Let p be a prime number and $x \in \mathbb{Z}$. If $x^2 \equiv 1 \pmod{p}$ then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$

Proof:

- $p \mid (x^2 - 1) = (x+1)(x-1)$.
- Then $p \mid (x+1)$ or $p \mid (x-1)$

An odd composite N is called a strong pseudoprime relative to the base a if either

$$a^q \equiv 1 \pmod N$$

or there exists $i = 0, \ldots, k-1$ such that

$$a^{2^i q} \equiv -1 \pmod N,$$

where $N - 1 = 2^k q$ and $2 \nmid q$.

Proposition 1.9.6

Let p be an odd prime number and suppose that

$$p - 1 = 2^k q,$$

where $2 \nmid q$. If $a \in \mathbb{Z}$ and $gcd(a, p) = 1$ then either

$$a^q \equiv 1 (\mathrm{mod}\ p)$$

or there exists $i = 0, \ldots, k-1$ such that

$$a^{2^i q} \equiv (\mathrm{mod}\ p).$$

Proof:

- Let $a_i = a^{2^i q}, i = 0, \ldots k$.
- By Fermat's th: $a_k \equiv 1 (\mathrm{mod}\ p)$ and $a_{i+1} = a_i^2$, for $i = 0, \ldots, k-1$.
- Therefore, $a_0 \equiv 1 (\mathrm{mod}\ p) \Leftrightarrow a_k \equiv 1 (\mathrm{mod}\ p)$ for every i.

- Let $a_i = a^{2^i q}, i = 0, \dots k$.
- By Fermat's th: $a_k \equiv 1 \pmod{p}$ and $a_{i+1} = a_i^2$, for $i = 0, \dots, k-1$.
- Therefore, $a_0 \equiv 1 \pmod{p} \Leftrightarrow a_i \equiv 1 \pmod{p}$ for every i.
- If $a_0 \not\equiv 1 \pmod{p}$, then $\exists a_i, i \geq 0$, such that $a_i \not\equiv 1 \pmod{p}$.
- Let j be the largest index with this property.
- Since $j < k$ and $a_j^2 \equiv a_{j+1} \equiv 1 \pmod{p}$, we get $a_j \equiv -1 \pmod{p}$ (by previous lemma).

Theorem 1.9.7 (Rabin)

Suppose that $N > 4$ is an odd composite integer and let B be the number of bases a ($1 < a < N$) such that N is a strong pseudoprime relative to a. Then

$$B < \varphi(N)/4 \leq (N-1)/4$$