Some slides for 5th Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

20-09-2012

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

You are welcome to use Maple for computations.

To get some help type in Maple:

- >?mod
- >?isprime (or nextprime)
- >?ifactor
- >?igcdex

Do not forget that we use &^ to apply the repeated squaring algorithm in Maple. Type:

- >18^5705890543 mod 37;
- >18&^5705890543 mod 37;