Some slides for lecture 9, Algebra 1, EVU

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

5-5-2011

$\mathbb{Z}/N$ and $(\mathbb{Z}/N)^*$

Euler's φ function

Proposition

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

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

Proof:

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

Hence, the result holds because r is bijective.

Theorem 1.7.2 (Euler)

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

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

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 $\varphi(p^m)$?

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

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

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

Public-key crytography (from Wikipedia)

- The key used to encrypt a message is not the same as the key used to decrypt it.
- Each user has a pair of cryptographic keys-a public key and a private key. The private key is kept secret, while the public key may be widely distributed.
- Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key.
- The keys are related mathematically, but the private key cannot feasibly (ie, in actual or projected practice) be derived from the public key.
- The discovery of algorithms that could produce public/private key pairs revolutionized the practice of cryptography beginning in the middle 1970s.

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

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

Proof:

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

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

- Multiply the previous congruence with X

Encryption and decryption exponents

- Choose e relative prime to $\varphi(N) = (p-1)(q-1)$.
- Then there exists λ and μ such that

$$\lambda(p-1)(q-1) + \mu e = 1$$

  with $0 < \mu < (p-1)(q-1)$.
- Let $k = -\lambda$ and $d = \mu$.

Then $de = 1 + k(p-1)(q-1)$ and $[X^{ed}] = [X]$.

- One has that $d = e^{-1}$ in $(\mathbb{Z}/\varphi(N)\mathbb{Z})^*$.

ElGamal

Based on discrete logarithm problem:

Given a prime p and $y, g \in \mathbb{N}$, find x such that

$$y \equiv g^x \pmod{p}$$

1. Alice and Bob choose p, a big prime, and $g \in \mathbb{N}$ s.t. $0 < g < p$ and g has order $p - 1$ in $(\mathbb{Z}/p\mathbb{Z})^*$ (a generator of $(\mathbb{Z}/p\mathbb{Z})^*$)
2. Alice chooses a, with $0 < a < p$ and computes $[g^a]_p$.
   Secret Key=a
   Public Key=$[g^a]_p$
3. Bob chooses b with $0 < b < p$ and computes $[g^b]_p$.
   Secret Key=b
   Public Key=$[g^b]_p$

4. Alice wants to send a message m, $0 < m < p$ to Bob. She sends:
$$\left([g^a]_p, [m(g^b)^a]_p\right)$$
5. Bob gets $([x_1]_p, [x_2]_p)$ and computes
$$[x_2]_p([x_1^b]_p)^{-1} = [mg^{ab}]_p([g^{ab}]_p)^{-1} = [m]_p$$
and since $m < p$ he can recover m.

To encrypt the message one uses the public key of the receiver and the secret key of the sender.

6. Eve?: she had to compute b from $[g^b]_p$

- ElGamal can be defined using a cyclic group G, for instance using an elliptic curve.
- In the previous slides, it has been described using $G = (\mathbb{Z}/p\mathbb{Z})^*$. Exercise: prove that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

Maple:

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.