Summary for Computational Number Theory at University of Minho

Alef Keuffer

June 13, 2022

Please contact me if you notice any mistaskes. This summary is not complete.

1 Topics worth learning

Theses topics had questions worth 3 points in past tests.

1. Use Fermat factorization
2. Use ρ-Pollard
3. Use $p-1$ Pollard
4. Solve congruence equation knowing facts related to primitive root and index.
5. Cipher a message using ElGamal + show that a number is a primitive root
6. Calculate $\varphi(n)$ + decipher RSA
7. Show there are not solutions for a congruence relation (quadratic residue)
8. Euler pseudoprime
9. Solovay-Strassen primality test
10. Miller-Rabin primality test
11. Suppose that if n is a product of two primes. Show that factoring n is equivalent to calculating $\varphi(n)$.
12. Calculate Jacobi Symbol

2 Encryption Systems

Let M denote the message, C the ciphertext.

2.1 ElGamal

$$\begin{array}{ll}
\text{PrivK} & \equiv 1 < \alpha < p-1 \\
\text{PubK} & \equiv \left(p \in \mathbb{P}, g : \langle g \rangle = \mathbb{Z}_p^*, b \stackrel{\text{def}}{=} g^\alpha\right) \\
C & \equiv \left(\gamma \stackrel{\text{def}}{=} g^k, \delta \stackrel{\text{def}}{=} Mb^k\right), \quad k \text{ random element in } \{2, \dots, p-2\} \\
M & \equiv \delta\gamma^{\alpha^{-1}} \pmod p
\end{array}$$

2.2 RSA

$$\begin{array}{ll}
\text{PrivK} & \equiv d \stackrel{\text{def}}{=} e^{-1} \pmod{\varphi(n) = (p-1)(q-1)} \\
\text{PubK} & \equiv \left(n \stackrel{\text{def}}{=} pq, e\right) \\
C & \equiv M^e \pmod n \\
M & \equiv C^d \pmod n
\end{array}$$

3 Prime factorization

3.1 Factoring given $\varphi(n)$

$\frac{-b+\sqrt{b^2-4n}}{2}$ where $b = n + 1 - \varphi(n)$ is a factor of n.

3.2 Fermat

Algorithm 1: Fermat factorization

Require: n odd $\in \mathbb{N}$
Ensure: $\left(a + \sqrt{a^2-n}\right)\left(a - \sqrt{a^2-n}\right) = n$
  $a \leftarrow \sqrt{\lceil n \rceil}$
  while $\sqrt{a^2-n} \notin \mathbb{Z}$ **do**
    $a \leftarrow a + 1$
  end while

3.3 ρ-Pollard

Algorithm 2: ρ-Pollard factorization

Require: b-smooth g, e.g. $g(x) = x^2 + 1$ **and** x_0, e.g., $x_0 \stackrel{\text{def}}{=} 2$
Ensure: $\gcd(|x-y|, n)$ is nontrivial factor of n
  $x \leftarrow x_0$
  $y \leftarrow x_0$
  while $\gcd(|x-y|, n) = 1$ **do**
    $x \leftarrow g(x)$
    $y \leftarrow g(g(y))$
  end while

3.4 Pollard $p-1$

The algorithm as presented by the professor

Algorithm 3: Pollard $p-1$ simplified

Require: n odd composite $\in \mathbb{N}$
Ensure: $\gcd(r-1, n)$ is a nontrivial factor of n
  $r_0 \leftarrow 2$
  $r \leftarrow r_0$
  while $\gcd(r-1, n) = 1$ **do**
    $r \leftarrow r * r_0 \pmod n$
  end while

4 Useful facts

4.1 Solving simple congruence equations knowing primitive roots

Let $z_i \in \mathbb{Z}$ and $I(a)$ be the the index with respect to a primitive root $g \in \mathbb{Z}_n^*$. To solve an equation of the type

$$z_1 x^{z_2} \equiv z_3 \pmod n$$

get

$$I\left(z_1 x^{z_2}\right) \equiv I(z_3) \iff z_2 I(x) \equiv I(z_3) - I(z_1) \pmod{\varphi(n)}$$

to the form

$$I(x) \equiv I(z_4) \pmod{\varphi(n)}$$

then conclude

$$x \equiv z_4 \pmod n$$

4.2 Euler's theorem

$$a \perp n \Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$$

4.3 Euler's totient function

4.3.1 Definition

$$\varphi(n) \stackrel{\text{def}}{=} n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

4.3.2 Useful facts

4.3.2.1 multiplicative $m \perp n \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

4.3.2.2 prime power argument $\varphi\left(p^k\right) = p^k - p^{k-1}$

4.4 Reduced residue system

$$\text{RRS}(n) = R \text{ s.t.} \begin{cases} \forall r \in R. \quad \gcd(r, n) = 1 \\ |R| = \varphi(n) \\ \forall r_1, r_2 \in R. \quad r_1 \not\equiv_n r_2 \end{cases}$$

4.5 Primitive root modulo n

4.5.1 Definition

$$g \text{ is primitive root modulo } n \text{ if and only if } \langle g \rangle = \mathbb{Z}_n^*$$

Alternatively, one can say g is a primitive root of n iff its order is $\varphi(n)$.

4.5.2 Useful facts

4.5.2.1 Fact $\langle g \rangle = \mathbb{Z}_p^* \Rightarrow g^{\frac{p-1}{2}} \equiv -1 \pmod p$

4.5.2.2 Condition for existence of primitive root $\mathbb{Z}_n^*$ is cyclic iff n is equal to $2, 4, p^k, 2p^k$ where p^k is the power of and odd prime number. When (and only when) this group $\mathbb{Z}_n^*$ is cyclic, a generator of this cyclic group is called a primitive root modulo n.

When $\mathbb{Z}_n^*$ is non-cyclic, such primitive root elements mod n do not exist.

4.5.2.3 Number of primitive roots The number of primitive roots modulo n, if there are any, is equal to

$$\varphi(\varphi(n))$$

4.5.3 Showing g is primitive root of n

$$\forall i \in \{1, \dots, k\}. \quad g^{\frac{\varphi(n)}{p_i}} \not\equiv 1 \bmod n \Rightarrow \langle g \rangle = Z_n^*$$

Where $p_1, \dots, p_k$ are the different prime factors of $\varphi(n)$.

4.6 Jacobi symbol

4.6.1 Definition The Jacobi symbol $\left(\frac{a}{n}\right)$ is defined as the product of the Legendre symbol corresponding to the prime factors of n:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

4.6.2 Legendre symbol Definition of the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod p \\ 1 & \text{if } a \not\equiv 0 \pmod p \text{ and for some integer } x : a \equiv x^2 \pmod p \\ -1 & \text{if } a \not\equiv 0 \pmod p \text{ and there is no such } x \end{cases}$$

4.6.3 Useful properties

4.6.3.1 Modular equivalence

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \Longleftarrow a \equiv b \pmod n$$

4.6.3.2 Coprimality

$$\left(\frac{a}{n}\right) = 0 \Longleftarrow \gcd(a, n) \neq 1$$

4.6.3.3 Multiplicative Completely multiplicative function (if fixing one of the arguments):

$$\left(\frac{ab}{mn}\right) = \left(\frac{a}{mn}\right)\left(\frac{b}{mn}\right) = \left(\frac{ab}{m}\right)\left(\frac{ab}{n}\right)$$

4.6.3.4 Quadratic reciprocity Law of quadratic reciprocity: if p and q are odd positive coprime integers, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

4.6.3.5 Euler's criteria $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

4.6.3.6 Extra

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$
$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$
$$\left(\frac{1}{n}\right) = \left(\frac{n}{1}\right) = 1$$

5 Primality testing

5.1 Pseudoprimes

5.1.1 Weak pseudoprime A composite number n such that $b^n \equiv b \pmod n$ is a weak pseudoprime to base b.

5.1.2 Strong pseudoprime A composite number n such that it passes the Miller-Rabin test for base b.

5.1.3 Euler pseudoprime An odd composite integer n is called an Euler pseudoprime to base b, if

$$\gcd(b, n) = 1 \wedge b^{\frac{n-1}{2}} \equiv \pm 1 \pmod n$$

5.1.4 Fermat pseudoprime A composite integer n is called a Fermat pseudoprime to base $b > 1$ if

$$b^{n-1} \equiv 1 \pmod n$$

5.1.5 Carmichael number n is a Carmichael number if it's a Fermat pseudoprime for all values b coprime to n.

5.2 Solovay-Strassen

$\left(\frac{b}{n}\right) = 0 \vee \left(\frac{b}{n}\right) \not\equiv b^{\frac{n-1}{2}} \bmod n \Rightarrow n$ is not prime

5.3 Miller-Rabin

Let $n - 1 = 2^e d$ with n, d odd.

Let $\gcd(1 < b < n, n) = 1$.

If $b^d \equiv 1 \bmod n$ or $b^{2^{0 \leq j < e} d} \equiv -1 \bmod n$, then n passes the test for base b.

If n is composite, the probability that n passes the test for k bases is $< \frac{1}{4k}$.