Number Theory & Modular Arithmetic

Rocco DE NICOLA

IMT Lucca

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Outline

- Introduction
- Prime Numbers
- Modular Arithmetic
- Logarithms

Outline

- Introduction
- Prime Numbers
- Modular Arithmetic
- Logarithms

Why Number Theory

- Double Key Cryptography heavily relies on some properties of prime numbers that enable one to
  - Exchange secret keys on line without running the risk of it being intercepted by an adversary
  - Encrypt with one key and decrypt with the twin one
  - Limit the possibility of brute force attacks while guaranteeing efficient encryption and decryption

Requirements for asymmetric encryption

- Computationally inexpensive to create pairs of keys
- Computationally inexpensive to encrypt messages for a sender who knows the public key and to decrypt messages for a recipient who knows the private key (or viceversa)
- Computationally difficult for an opponent to discover the private key knowing the public key and to decipher a message without knowing the private key
- It must be possible to use one of the two related keys for encryption, and the other for decryption, interchangeably.

Requirements for asymmetric encryption

Public key schemes depend on appropriate so/called trap-door one-way functions

- one-way function
  - Y = f(X) Easy
  - X = f^{-1}(Y) hard - not feasible
- a trap-door one-way function
  - Y = f_k(X) is easy if k and X are known
  - X = f_k^{-1}(Y) is easy if k and y are known
  - X = f_k^{-1}(Y) is not feasible, if Y is known but k is not.

An easy problem can be solved in polynomial time relatively to the length of the input

An example of a one-way function

- Given the number 6895601 determine whether it is the product of two prime numbers, and what these numbers are.
- A natural solution would be to try dividing 6895601 by several prime numbers smaller than the number under consideration until you find the answer. Difficult!
- If one knows that 1931 is one of the numbers, the answer can be found by computing 6895601 ÷ 1931

Issues of asymmetric encryption

- Brute force attacks are theoretically possible.
- Very large keys are needed: a 64-bit private key scheme has a security more or less similar to that of a 512-bit RSA (the most used Public Key Cryptography).
- The problem is well known, but is made difficult enough to make it unworkable by resorting to very large numbers.
- Encryption and decryption are much slower than for single key schemes.

Number Theory

- Number theory is fundamental for facing the challenges of asymmetric encryption.
- The key ingredients for the development of a theory of double keys encryption are:
  - Prime numbers
  - Modular Arithmetic
  - Exponentiation and Logarithms

Outline

- Introduction
- Prime Numbers
- Modular Arithmetic
- Logarithms

Prime Numbers

- Natural numbers N: All positive integers starting from 1.
- Integers Z: All integers positive and negative, including 0
- a in Z is a divisor of b if b = k * a (for some k)
- *a* has always two trivial divisors 1 and a
- a >= 2 is prime if it has only trivial divisors

Two theorems

- Division Theorem: For each a in Z and n in N, there exist unique q and r such that $a = q * n + r$, where $0 <= r < n$
  - q is the quotient
  - r (= a mod n) is the remainder
- Decomposition Theorem: Each natural numbers either is a prime number or can be obtained as the product of powers of primes:
  - $91 = 7 * 13$
  - $3600 = 2^4 * 3^3 * 5^2$
  - $11011 = 7 * 11^2 * 13$

Numbers and prime numbers

- Theorem: If P is the set of prime numbers, any generic positive integer a can be written as the product of exponential prime numbers

$$a = \prod_{p \in P} p^{a_p} \qquad \text{where each } a_p \geq 0$$

- N.B.: For any specific number, for most prime numbers p in the formula, the corresponding exponent will be 0.

Numbers and prime numbers

- Corollarium: To perform a multiplication between two numbers it is sufficient to express both of them as product of primes and then add the corresponding exponents.
- Example
  - Since: $91 = 7 * 13$ and $11011 = 7 * 11^2 * 13$
  - We have: $91 * 11011 = 7^2 * 11^2 * 13^2$
  - Check! …

Minumum Common Multiple

- The Minimum Common Multiple of two integers a and b, MCM(a, b), is the smallest positive integer that is divisible for both a and b:
  - MCM(4,6) = 12 because
    - Multiple of 4: 4, 8, 12, 16, …
    - Multiple of 6: 6, 12, 18 , …

Greatest Common Divisor

- The Greatest Common Divisor of two integers a and b, GCD(a, b), is the largest positive integer that divides both a and b:
  - GCD(54,24) = 6 because
    - 54 * 1 = 27 * 2 = 18 * 3 = 9 * 6

      the divisors of 54 are: 1, 2, 3, 6, 9, 18, 27, 54
    - 24 * 1 = 12 * 2 = … 3 * 8 …

      the divisors of 24 are: 1, 2, 3, 4, 6, 8, 12, 24

Computing GCD

Euclid’s algorithm

- Given two natural numbers a and b,
  - if b is zero a is the MCD.
  - If b is different from 0, divide a by b and assign the remainder to r (a mod b). If r = 0 then b is the MCD, otherwise let a = b and b = r and repeat the division again.

Extended Euclid’s algorithm

- Keeping note of the quotients obtained during the algorithm, you can determine two integers p and q such that MCD(a, b) = ap + bq

Outline

- Introduction
- Prime Numbers
- Modular Arithmetic
- Logarithms

Modular Arithmetic

- It is a system of arithmetic for integers, where the numbers "wrap" when they reach a certain value - the module!
- It is based on a *congruence relation* over integers that is compatible with addition, subtraction and multiplication operations.
- Two numbers a and b are congruent relatively to n ($a \equiv b \pmod{n}$), if their difference a - b is an integer multiple of n.
- $a \equiv b \pmod{n}$ establishes that a and b have the same remainder if divided by n, i.e., $a = p * n + r$, $b = q * n + r$

Modular Arithmetic

- Example:
  - 38 ≡ 14 (mod 12) because
    - 38 − 14 = 24, which is a multiple of 12
    - Both 38 and 14 have the same remainder (2) if divided by 12.
- Properties:
  - Reflexivity: a ≡ a (mod n)
  - Symmetry: a ≡ b (mod n) if and only if b ≡ a (mod n)
  - Transitivity: If a ≡ b (mod n) and b ≡ c (mod n), then a ≡ c (mod n)

Congruence for Modular Arithmetic

Any two terms that are congruent modulo n can be used interchangeably in any arithmetic operation modulo n

- If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$ then:
  - $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
  - $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$
  - $a_1 * a_2 \equiv b_1 * b_2 \pmod{n}$
- If $a \equiv b \pmod{n}$, then:
  - $a^k \equiv b^k \pmod{n}$ for any non-negative integer k

Congruence for Modular Arithmetic

- A familiar use of modular arithmetic is in a 12-hour clock (the day is divided into two 12-hour periods); if the time is 7:00 now, then 8 hours later it will be 3:00.
- a (mod n) = d if and only if a = d + (k * n) for some k
- a is **congruent** to b (modulo n) if a (mod n) = b (mod n)
- $\mathbf{Z_n}$ is the set of equivalence classes induced by the congruence modulo n: $[0]_n$ $[1]_n$ …. $[n\text{-}1]_n$, with $[i]_n$ standing for the representative of the set of all the integers that are congruent to i modulo n.

Congruence for Modular Arithmetic

- $\mathbf{Z_n}$ is an *abelian group* over the sum:
  - $[a]_n + [b]_n = [a+b]_n$
  - $[0]_n$ is the identiy element
  - $[n-a]_n$ is the inverse of a.
- $\mathbf{Z_n}$ is finite and $|\mathbf{Z_n}| = n$
- $[i]_n = [i + k*n]_n$

Relatively prime numbers

- Two integers a and b are said to be relatively prime, mutually prime, or coprime if the only positive integer that divides both of them is 1.
- Any prime number that divides one out of two coprime numbers does not divide the other.
- The greatest common divisor (GCD) of two coprime numbers is 1.

Z^*_n : the multiplicative group for Z_n

- The set $\mathbf{Z}^*_n$ is the set of elements coprime w.r.t. n
  - Es $\mathbf{Z}^*_{15} = \{1,2,4,7,8,11,13,14\}$
  - Product: $[a]_n * [b]_n = [a * b]_n$
- $\mathbf{Z}^*_n$ is an abelian group:
  - The group is closed
  - GCD(a * b, n) = 1 since GCD(a, n) = 1 and GCD(b,n) = 1
  - The identity element is $[1]_n$,
  - Multipication is associative and commutative.
  - The cardinality of $\mathbf{Z}^*_n$ is $\phi(n)$ (Euler's totient)
  - There exists an inverse (b) of any element (a):
    1. GCD(a, n) = a * b + n * c due to extended Euclid algorithm
    2. Since GCD(a, n) = 1 by hypotesis we have a * b + n * c = 1.
    3. Since n X c ≡ 0 (mod n) it follows a X b ≡ 1 (mod n)

Euler's Theorem – Totient Function ϕ

- Given an integer n, the totient function of a number n – $\phi(n)$ – corresponds to the number of integers smaller than n that are coprime to n.
  - $\phi(15)$ = #{1,2,4,78,11,13,14} = 8
  - $\phi(17)$ = 16 because all integers from 1 to 16 are prime relatively to 17.
- $\phi(n)$ can be computed on the basis of the decomposition theorem
- $\phi(p)$ = p-1 if p is prime
  - $\phi(17)$ = 16 because all integers from 1 to 16 are prime relatively to 17.
- $\phi(n)$ = (p-1)*(q-1) if n is the product of two primes (n=p*q)
  - $\phi(15)$ = #{1,2,4,7,8,11,13,14} = 8 (4*2 because 15 = 5*3)

Fermat's little theorem

- Fermat's little theorem: Given an integer a and a prime p with a not divisible by p, we have: $a^{p-1} = 1 \pmod{p}$
- An Example: $7^{18} \equiv 1 \pmod{19}$

$$
\begin{aligned}
a &= 7, p = 19 \\
7^2 &= 49 \equiv 11 \pmod{19} \\
7^4 &\equiv 121 \equiv 7 \pmod{19} \\
7^8 &\equiv 49 \equiv 11 \pmod{19} \\
7^{16} &\equiv 121 \equiv 7 \pmod{19} \\
a^{p-1} &= 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}
\end{aligned}
$$

Picture from: *W. Stalling: Cryptography and Network Security, International Edition, Pearson*

A variant of Fermat’s little theorem

A variant of Fermats’s little theorem

Given an integer a and a prime p:

- $a^p = a \pmod p$

$$p = 5, a = 3 \qquad a^p = 3^5 = 243 \equiv 3(\bmod 5) = a(\bmod p)$$
$$p = 5, a = 10 \qquad a^p = 10^5 = 100000 \equiv 10(\bmod 5) \equiv 0(\bmod 5) = a(\bmod p)$$

N.B.: In this case there is no requirement that a be not divisible by p

Picture from: *W. Stalling: Cryptography and Network Security, International Edition, Pearson*

Euler's Theorem revisited

- Euler's Theorem:
  - Given two integers a and n that are coprime:
    $a^{\phi(n)} = 1 \pmod{n}$

- An obvious variant of Euler's Theorem:
  - Given two integers a and n that are coprime:
    $a^{\phi(n)+1} = a \pmod{n}$

Examples for Euler's theorem

- Given two integers a and n that are coprime :
  - $a^{\phi(n)} = 1 \pmod{n}$

Two examples

- Given a = 3 and n = 10
  - $\phi(10) = \#\{1,3,7,9\} = 4$
  - $a^{\phi(10)} = 3^4 = 81 = 1 \pmod{10}$
- Given a = 2 and n = 11,
  - $\phi(11) = 10$
  - $a^{\phi(10)} = 2^{10} = 1024 = 1 \pmod{11}$

Outline

- Introduction
- Prime Numbers
- Modular Arithmetic
- Logarithms

Why logarithms

- All the systems at the basis of public key cryptography relay on properties of the multiplicative group modulo p, denoted by $\mathbb{Z}^*_p$, for a prime p.
- Their security ultimately depends on the intractability of solving the *Discrete Logarithm Problem:* if you are given $g \in \mathbb{Z}^*_p$ and g^n mod p then you have to find n.
- For Diffie-Hellman key exchange an eavesdropper only sees p, g, g^a and g^b. Given these values, to find the exchanged key, he/she has to find g^{a*b} mod p.

Cyclic Group

- A group can be cyclic, i.e., can be generated by the iterated composition of the operator on an element, said “generator”
- Z^X_q, for a prime q, is a cyclic group (Gauss), thus there exists a such that a mod q, a^2 mod q, … , a^{q-1} mod q, generate (in any order) all the elements of Z^X_q (1, 2, 3, … , q-1)

Primitive Roots

- A number g is a primitive root modulo n if every number a coprime to n is congruent to a power of g modulo n.
- g is a primitive root modulo n if for every integer a coprime to n, there exists an integer k such that

$$g^k \equiv a \pmod{n}.$$

- Such a value k is called the index or discrete logarithm of a to the base g modulo n.

Discrete Logarithms

- The logarithm $\log_b a$ is a number x such that $b^x = a$
- The discrete logarithm $\log_b a$ is an integer k such that $b^k = a$
- Given 1 <= b <= q-1, there is a unique i such that $a^i \bmod q = b$.
- i is the *discrete logarithm of b* with base a and modulo q:
  - $i = dlog_{a,q}(b)$
- Important algorithms in public-key cryptography base their security on the assumption that the discrete logarithm problem when modular arithmetic is used has no efficient solution.

Computing Primitive Roots

- The k^{th} power of a number modulo p may be computed by computing its k^{th} power as an integer and then finding the remainder after division by *p*.
- To compute 3^4 (mod 17) compute $3^4 = 81$, and then divide 81 by 17, obtaining a remainder of 13, i.e., $3^4 = 13$ (mod 17).
- It is more efficient to reduce modulo p multiple times during the computation.
  - To compute 3^7 (mod 17) compute $3^3 * 3^4$ (mod 17) = 3^3 (mod 17) * 3^4 (mod 17) = 3^3 (mod 17) * 3 (mod 17) 3^3 (mod 17) = 10 * 3 * 10 = 300 = 11 (mod 17)

Primitive Roots: an example

The number 3 is a primitive root modulo 7 because the relative prime of 7 are 1, 2, 3, 4, 5, 6 and they can be obtained as follows:

$$
\begin{aligned}
3^1 &= 3 = 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod{7} \\
3^2 &= 9 = 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod{7} \\
3^3 &= 27 = 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod{7} \\
3^4 &= 81 = 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod{7} \\
3^5 &= 243 = 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod{7} \\
3^6 &= 729 = 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod{7} \\
3^7 &= 2187 = 3^6 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod{7}
\end{aligned}
$$

The discrete logarithm problem

- The discrete logarithm is just the inverse operation of computing primitive roots.
- Given a secret number *b* that satisfies

$$b^e \equiv c \pmod{n}$$

  The problem is to find *b* given only the integers *c, e* and *n*.
- Without the modulus function one could rely on the correspondence

$$\log_b(c) = e$$

  but the modular arithmetic prevents you using logarithms calculation effectively.

The discrete logarithm problem

- Consider the equation $3^k \equiv 13 \pmod{17}$ for k.
- As seen above, one solution is $k = 4$, but it is not the only solution.
- Since $3^{16} \equiv 1 \pmod{17}$ – Fermat's little theorem – it also follows that for any integer *n, we have* $3^{4+16n} \equiv 3^4 \times (3^{16})^n \equiv 13 * 1^n \equiv 13 \pmod{17}$.
- Hence the equation has infinitely many solutions of the form $4 + 16n$.

Chinese remainder theorem

- **Chinese remainder theorem:** if the remainders of the division of an integer *n* by several integers is known, then it is possible to uniquely determine the remainder of the division of *n* by the product of these integers, under the condition that the divisors are pairwise coprime.
- The theorem is widely used for computing with large integers, as it allows replacing a computation by several similar computations on small integers.

Grazie

Number Theory & Modular Arithmetic

Rocco DE NICOLA

IMT Lucca

https://cybersecnatlab.it