CIS 5371
Cryptography

Introduction to Number Theory

Preview

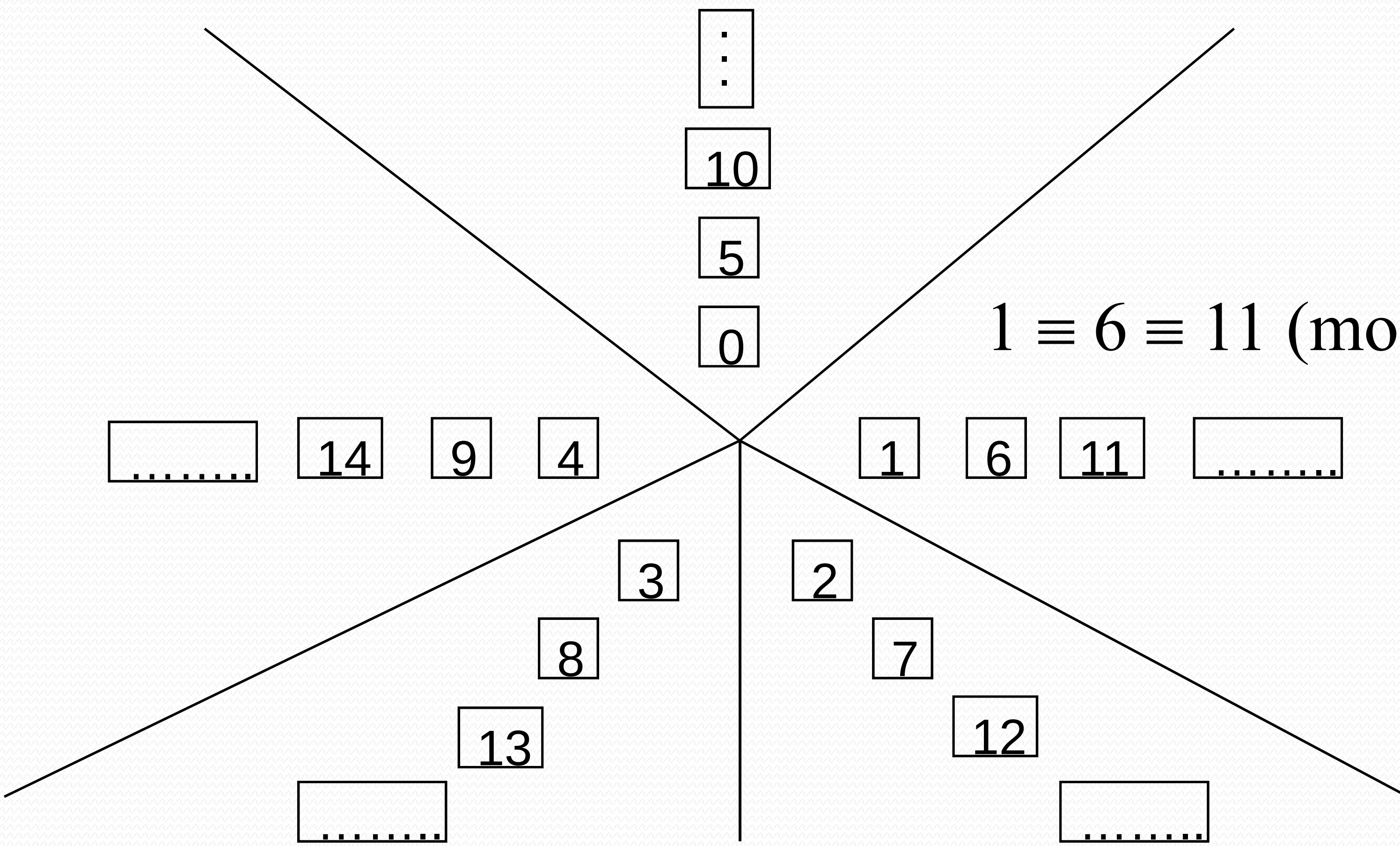
- Number Theory Essentials
- Congruence classes, Modular arithmetic
- Prime numbers challenges
- Fermat's Little theorem
- The Totient function
- Euler's Theorem
- Quadratic residuocity
- Foundation of RSA

Number Theory Essentials

- Prime Numbers
  - A number $a \in I$ is a prime iff
    $it's\ only\ factors\ are\ itself\ and\ 1$
    $Equivalently,\ \forall\ x \in I,\ \gcd(x,a) = 1$
  - $a, b \in I$ are relatively prime iff :
    - $\gcd(a,b) = 1$
- Fundamental theorem of arithmetic:

Every integer has a unique factorization that is a product of prime powers.

Congruence Classes: the integers modulo 5



$1 \equiv 6 \equiv 11 \pmod 5$

Modular arithmetic

- Form: $a \equiv b \bmod n$
- The modulo relation partitions the integers into congruence classes
- The congruence class of an integer 'a' is the set of all integers congruent to 'a' modulo 'n'.
- $a \equiv b \bmod n$ asserts that 'a' and 'b' are members of the same congruence class *modulo* 'n'

The integers modulo *n*

- $\forall\, a,b,n \in I,\ a \equiv b \bmod n$ iff $n \mid (a\text{-}b)$ *
  - $28 \equiv 6 \bmod 11$: $(28\text{-}6)/11 = 2 \in I$
  - $219 \equiv 49 \bmod 17$: $(219\text{-}49)/17 = 10 \in I$
  - *Symmetry*:
    If $a \equiv b \bmod n$ then $b \equiv a \bmod n$
  - *Transitivity*:
    If $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$

Modular arithmetic: notation

Form: $a \equiv b \bmod n$ (congruence *relation*)

$a = b \bmod n$ (modulus *operator*)

$\equiv$ indicates that the integers a and b fall into the same congruence class modulo n

$=$ means that integer a is the reminder of the division of integer b by integer n.

Example: $14 \equiv 2 \bmod 3$ and $2 = 14 \bmod 3$

Modular arithmetic & cryptography

- Modular computations can be utilized to scramble data.
- Cryptographic systems utilize modular (or elliptic curve (EC)) arithmetic.
- Several cryptographic systems use prime modulus arithmetic.

Prime Number Challenges

1. Finding large prime numbers.
2. Recognizing large numbers as prime.

How Do We Find Large Prime Numbers?

- Look them up ?
- Compute them ?
- Do they REALLY have to be prime?

Finding large primes

- The probability of a randomly chosen number being prime is: 1/ln *n*
- For a 100 digit number, the chance is about 1/230
- Guess and check, should take 230 tries on the average
- How do we check? Answer: *Primality testing*.

Fermat's Little Theorem

- For every prime number p and $a \in$ I with $0 < a < p$ we have: $a^p \equiv a \bmod p$
- Equivalently, if p is prime number and $a \in$ I with $0 < a < p$ then: $a^{p-1} \equiv 1 \bmod p$

Fermat's Little Theorem $a^{p-1} = 1 \bmod p$: examples

Let $p = 5$, pick values for a:

- $a = 2$: $2^4 = 16 \bmod 5 = 1$
- $a = 3$: $3^4 = 81 \bmod 5 = 1$
- $a = 4$: $4^4 = 256 \bmod 5 = 1$

Fermat's Little Theorem $a^{p-1} = 1 \bmod p$: examples

- Let p = 11, pick values a :
  - a=3: 3^{10} = 59049 mod 11 = 1
  - a=5: 5^{10} = 9765625 mod 11 = 1
  - a=7: 7^{10} = 282475249 mod 11 = 1
  - a=8: 8^{10} = 1073741824 mod 11 = 1

Fermat's Little Theorem $a^{p-1} = 1 \bmod p$: examples

- For $a = 2$, p cannot be 2, 4, 6, 8, etc.
- For $a = 5$, p cannot be 5 , 10, 15, etc.
- Choosing p smaller than a produces unpredictable results.
- In general, if $a^{p-1} = 1 \bmod p$, for some random $1 < a < p$, then p is a prime with high probability.

If $a^{p-1} = 1 \bmod p$ for $1 < a < p$ then p is a prime with high probability

A primality test

1. Select p, a large number
2. Select a random number a: $1 < a < p$
3. Compute $x = a^{p-1} \bmod p$
   a. If $x \neq 1$, then p is not prime
   b. If $x = 1$, then p is a prime with high probability

If $a^{p-1} = 1 \bmod p$ for $1 < a < p$ then p is prime with high probability

If $a^{p-1} = 1 \bmod p$, then the probability that p is not a prime is $1/10^{13}$

Exponentiations

$381^{1502} \bmod 751$

$= 381^2 \times 381^{750} \times 381^{750} \bmod 751$

$= 381^2 \bmod 751 \times 1 \bmod 751$

$= 145161 \bmod 751$

$= 218$

Exponentiations

$$a^{p\text{-}1} \equiv 1 \bmod p$$

- $7^{13} \bmod 11 \equiv x$
- $7^{10} \bmod 11 * 7^{3} \bmod 11 \equiv x$
- $1 \bmod 11 * 7^{3} \bmod 11 \equiv x$
- $7^{3} \bmod 11 \equiv x$
- $346 \bmod 11 \equiv 5$

The totient function $\phi(n)$

- $\phi(n)$ is the number of positive integers less than n that are relatively prime to n
- The function $\phi(n)$ returns the cardinality of Z_n^*
- Z_n^* forms a group of *order* (cardinality) $\phi(n)$ with respect to multiplication
- Euler's theorem: $\forall\, x \in Z_n^*$ we have $x^{\phi(n)} = x$
- $\forall\, p \in$ Primes, $\phi(p) = p - 1$

Deriving $\phi(n)$

- Primes: $\phi(p) = p\text{-}1$
- Product of 2 primes: $\phi(pq) = (p\text{-}1)(q\text{-}1)$
- General case (i.e. for all integers x) = ?

Deriving $\phi(n)$

Product of 2 relatively prime numbers

- if gcd $(m,n) = 1$, then: $\phi(mn) = \phi(m) * \phi(n)$
- $15 = 3*5$ and
- Example: $\phi(15)=2*4=8$

Deriving $\phi(n)$

- Product of n relatively prime numbers
  - if gcd $(a_1, a_2, \ldots, a_n) = 1$, then

    $\phi(a_1 a_2 \cdots a_n) = \phi(a_1) * \phi(a_2) * \cdots * \phi(a_n)$

Example: 30 = 2*3*5 and so $\phi(30)=1*2*4 = 8$.

Quadratic Residuosity

- An integer a is a quadratic residue with respect to n if:
  - a is relatively prime to n and
  - there exists an integer b such that: $a = b^2 \bmod n$
- Quadratic Residues for $n = 7$: QR(7)={1, 2, 4}
  - $a = 1$: $b = 1$ ($1^2 = 1 \bmod 7$), 6, 8, 13, 15, 16, 20, 22, …
  - $a = 2$: $b = 3$ ($3^2 = 2 \bmod 7$), 4, 10, 11, 17, 18, 24, 25, …
  - $a = 4$: $b = 5$, 9, 12, 19, 23, 26, …
- Notice that 2, 3, 5, and 6 are not QR mod 7.
- QR(n) forms a group with respect to multiplication.

The Foundation of RSA

- $x^y \bmod n = x^{(y \bmod \phi(n))} \bmod n$
- The proof of this follows from Euler's Theorem
- If $y \bmod \phi(n) = 1$,

  then for any x : $x^y \bmod n = x \bmod n$
- If we can choose e and d such that

  $ed = y \bmod \phi(n)$

then we can encrypt by raising x to the e^{th} power and decrypt by raising to the d^{th} power.