Introduction to Number Theory

Dhananjoy Dey

Indian Institute of Information Technology, Lucknow
ddey@iiitl.ac.in

July 19, 2021

Disclaimers

1

All the pictures used in this presentation are taken from freely available websites.

2

If there is a reference on a slide all of the information on that slide is attributable to that source whether quotation marks are used or not.

Outline

1. Divisibility and Modular Arithmetic

2. Integer Representations and Algorithms

3. Primes and Greatest Common Divisors

4. Solving Congruences

What is Number Theory?

NT

Number theory is concerned mainly with the study of the properties of the integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots,\},$$

particularly the positive integers $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

What is Number Theory?

NT

Number theory is concerned mainly with the study of the properties of the integers

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots, \},$$

particularly the positive integers $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$.

For example, in divisibility theory, all positive integers can be classified into three classes:

(i) Unit: 1
(ii) Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, . . .
(iii) Composite numbers: 4, 6, 8, 9, 10, 12, 14, 15, . . .

Famous Quotations Related to Number Theory

Quotation

The great mathematician **Carl Friedrich Gauss** called this subject *arithmetic* and he said:

“*Mathematics is the queen of sciences and arithmetic the queen of mathematics.*"

Famous Quotations Related to Number Theory

Prof G. H. Hardy

In the 1^{st} quotation Prof Hardy is speaking of the famous Indian Mathematician Ramanujan. This is the source of the often made statement that Ramanujan knew each integer personally.

(i) I remember once going to see him when he was lying ill at Putney. I had ridden in taxi cab number 1729 and remarked that number seemed to me rather dull one and that I hoped it was not an unfavorable omen. “No", he replied it is a very interesting number; it is the smallest number expressible as the sum of cubes of two integers in two different ways.

Famous Quotations Related to Number Theory

Prof G. H. Hardy

In the 1^{st} quotation Prof Hardy is speaking of the famous Indian Mathematician Ramanujan. This is the source of the often made statement that Ramanujan knew each integer personally.

(i) I remember once going to see him when he was lying ill at Putney. I had ridden in taxi cab number 1729 and remarked that number seemed to me rather dull one and that I hoped it was not an unfavorable omen. “No", he replied it is a very interesting number; it is the smallest number expressible as the sum of cubes of two integers in two different ways.

(ii) Pure mathematics is on the whole distinctly more useful than applied. For what is useful above all is technique and mathematical technique is taught mainly through pure mathematics[a].

[a] A Mathematician’s Apology by G. H. Hardy in November 1940

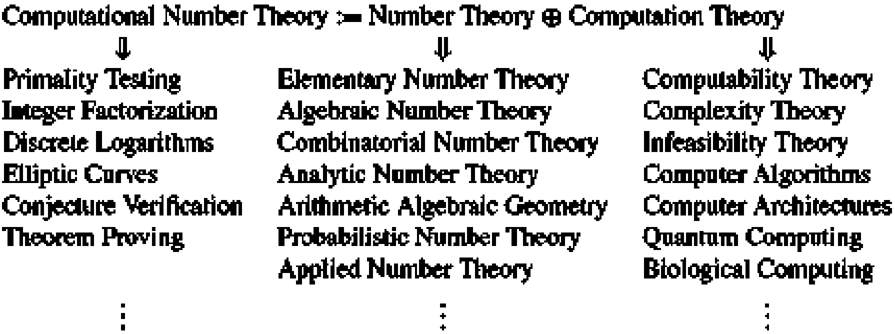
Motivation

NT

- Key ideas in number theory include divisibility and the primality of integers.
- Representations of integers, including binary and hexadecimal representations, are part of number theory.
- Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.
- Mathematicians have long considered number theory to be **pure mathematics**, but it has important applications to **computer science** and **cryptography**.

Computational Number Theory

Computational Number Theory



Computational Number Theory := Number Theory ⊕ Computation Theory

⇓	⇓	⇓
Primality Testing	Elementary Number Theory	Computability Theory
Integer Factorization	Algebraic Number Theory	Complexity Theory
Discrete Logarithms	Combinatorial Number Theory	Infeasibility Theory
Elliptic Curves	Analytic Number Theory	Computer Algorithms
Conjecture Verification	Arithmetic Algebraic Geometry	Computer Architectures
Theorem Proving	Probabilistic Number Theory	Quantum Computing
	Applied Number Theory	Biological Computing
⋮	⋮	⋮

The Floor & Ceiling of a Real Number

Definition

1. *The **floor** or the **greatest integer** function is defined as*

$$\lfloor x \rfloor \; = \; max\{n \in \mathbb{Z} \; : \; n \leq x\}$$

2. *The **ceiling** or the **least integer** function is defined as*

$$\lceil x \rceil \; = \; min\{n \in \mathbb{Z} \; : \; n \geq x\}$$

3. *The **nearest integer** function is defined as*

$$\lfloor x \rceil \; = \lfloor x + 1/2 \rfloor$$

Outline

1. Divisibility and Modular Arithmetic

2. Integer Representations and Algorithms

3. Primes and Greatest Common Divisors

4. Solving Congruences

Division

Definition

*If a & b are integers with $a \neq 0$, then a **divides** b if $\exists$ an integer c s/t $b = ac$.*

- When a divides b we say that a is a **factor** or **divisor** of b and that b is a **multiple** of a.
- The notation $a \mid b$ denotes that a divides b.
- If $a \mid b$, then $\frac{b}{a}$ is an integer.
- If a does not divide b, we write $a \nmid b$.

Properties of Divisibility

Theorem

Let $a, b, \ \& \ c$ *be integers, where* $a \neq 0$.

1. *If* $a \mid b$ *and* $a \mid c$*, then* $a \mid (b + c)$*;*
2. *If* $a \mid b$*, then* $a \mid bc$ *for all integers* c*;*
3. *If* $a \mid b$ *and* $b \mid c$*, then* $a \mid c$.

Corollary

If $a, b, \ \& \ c$ *are integers, where* $a \neq 0$*, s/t* $a \mid b$ *and* $a \mid c$*, then*

$$a \mid (mb + nc)$$

whenever $m \ \& \ n$ *are integers.*

Division Algorithm

- When an integer is divided by a positive integer, there is a **quotient** and a **remainder**. This is traditionally called the “Division Algorithm", but is really a theorem.

Theorem

If $a, d \in \mathbb{Z} \;\&\; d > 0$, *then* $\exists \,!\, q \;\&\; r \in \mathbb{Z}$ *s/t*

$$a = q.d + r, \; where\ 0 \leq r < d.$$

d *is called the* ***divisor***, a *is called the* ***dividend***, q *is called the* ***quotient*** *and* r *is called the* ***remainder***.

- We define **div** and **mod** as $q = a\ div\ d$ and $r \equiv a \mod d$

Congruence Relation

Definition

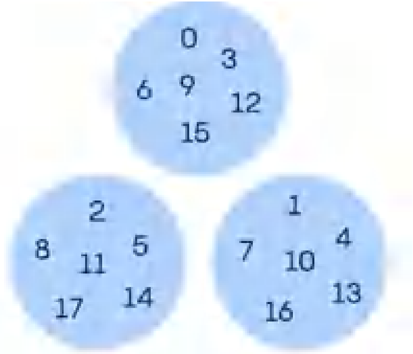
*If $a, b \in \mathbb{Z}$ and m is a positive integer, then a is **congruent to** b modulo m if $m \mid (a - b)$.*

- *The notation $a \equiv b \mod m$ says that a is congruent to b modulo m.*
- *We say that $a \equiv b \mod m$ is a **congruence** and that m is its **modulus**.*
- *Two integers are congruent $\mod m$ iff they have the same remainder when divided by m.*
- *If a is not congruent to b modulo m, we write*

$$a \not\equiv b \mod m$$

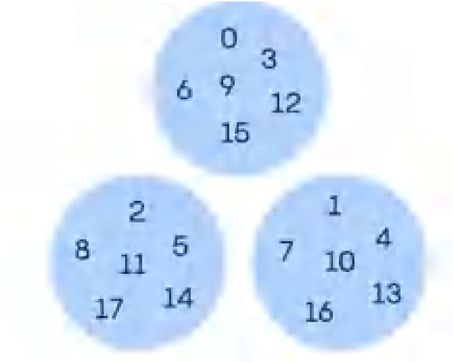
Congruence Relation

Example



Congruence Relation

Example

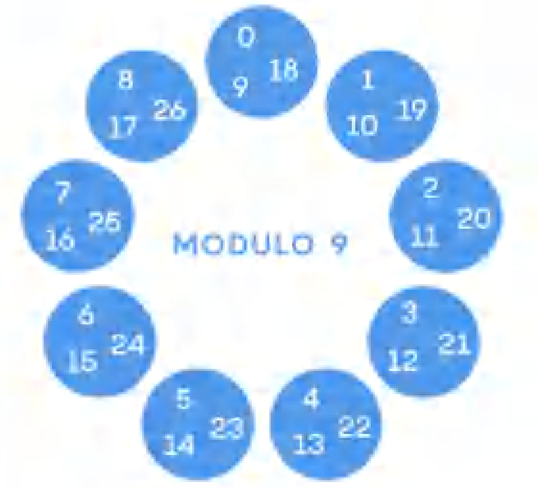


Exercise

Find the modulus.

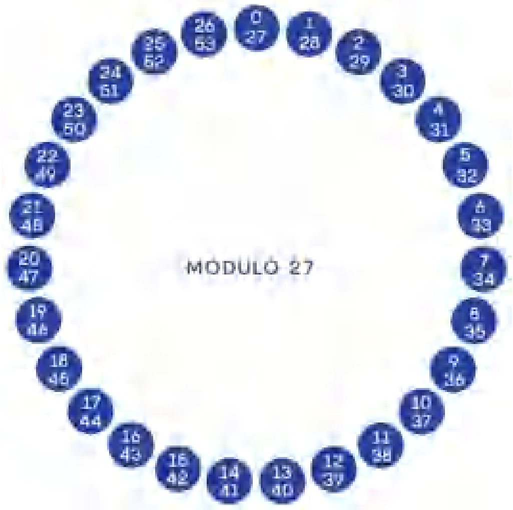
Congruence Relation

Example



Congruence Relation

Example



Congruence Relation

Theorem

Let m be a positive integer. The integers a & b are congruent modulo m iff there is an integer k s/t $a = b + km$.

Congruence Relation

Theorem

Let m be a positive integer. The integers a & b are congruent modulo m iff there is an integer k s/t $a = b + km$.

Proof.

- If $a \equiv b \mod m$, then (by the definition) we have $m \mid (a - b)$. Hence, there is an integer k s/t $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k s/t $a = b + km$, then $km = a - b$. Hence, $m \mid (a - b)$ and $a \equiv b \mod m$.

□

Congruence Relation

- The use of mod in $a \equiv b \mod m$ and $a \mod m = b$ are *different*.
  - $a \equiv b \mod m$ is a relation on the set of integers.
  - In $a \mod m = b$, the notation $\mod$ denotes a function.
- The relationship between these notations is made clear in the following theorem.

Theorem

Let a & b be integers, and let m be a positive integer. Then

$$a \equiv b \mod m$$

iff

$$a \mod m = b \mod m.$$

Congruences of Sums and Products

Theorem

Let m be a positive integer. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then

$$(a + c) \equiv (b + d) \mod m \text{ and } ac \equiv bd \mod m$$

Congruences of Sums and Products

Theorem

Let m be a positive integer. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then

$$(a+c) \equiv (b+d) \mod m \text{ and } ac \equiv bd \mod m$$

Proof.

- $\because a \equiv b \mod m$ and $c \equiv d \mod m$, there are integers $s \,\&\, t$ with $b = a + sm$ and $d = c + tm$.
- Therefore,
    - $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
    - $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.
- Hence, $(a + c) \equiv (b + d) \mod m$ and $ac \equiv bd \mod m$.

□

Algebraic Manipulation of Congruences

- Multiplying both sides of a valid congruence by an integer preserves validity.

  If $a \equiv b \mod m$ holds then $c.a \equiv c.b \mod m$, where c is any integer.

- Adding an integer to both sides of a valid congruence preserves validity.

  If $a \equiv b \mod m$ holds then $(c+a) \equiv (c+b) \mod m$, where c is any integer.

- Dividing a congruence by an integer does not always produce a valid congruence.
  E.g., $6 \equiv 15 \mod 9$; however, $\frac{6}{3} \not\equiv \frac{15}{3} \mod 9$

Computing the $\bmod m$ Function of Products and Sums

Corollary

Let m be a positive integer and let a & b be integers. Then

$$(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m$$

and

$$ab \mod m = ((a \mod m)(b \mod m)) \mod m.$$

- Let $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$
- The operation $+_m$ is defined as $a +_m b = (a+b) \mod m$.
- The operation $._m$ is defined as $a._m b = (a.b) \mod m$.
- $(\mathbb{Z}_m, +_m, \cdot_m)$ forms a commutative ring for any $m \in \mathbb{Z}$ and $m > 0$
- $(\mathbb{Z}_p, +_p, \cdot_p)$ forms a field for any prime p

Outline

1. Divisibility and Modular Arithmetic

2. Integer Representations and Algorithms

3. Primes and Greatest Common Divisors

4. Solving Congruences

Representations of a Number

- $(1234)_{10} =$

Representations of a Number

- $(1234)_{10} = 1.10^3 + 2.10^2 + 3.10^1 + 4.10^0$ to the base 10 – decimal
- $(1234)_{10} =$

Representations of a Number

- $(1234)_{10} = 1.10^3 + 2.10^2 + 3.10^1 + 4.10^0$ to the base 10 – decimal
- $(1234)_{10} = (10011010010)_2$

  $1.2^{10} + 0.2^9 + 0.2^8 + 1.2^7 + 1.2^6 + 0.2^5 + 1.2^4 + 0.2^3 + 0.2^2 + 1.2^1 + 0.2^0$ to the base 2 – binary

Representations of a Number

- $(1234)_{10} = 1.10^3 + 2.10^2 + 3.10^1 + 4.10^0$ to the base 10 – decimal
- $(1234)_{10} = (10011010010)_2$

  $1.2^{10} + 0.2^9 + 0.2^8 + 1.2^7 + 1.2^6 + 0.2^5 + 1.2^4 + 0.2^3 + 0.2^2 + 1.2^1 + 0.2^0$ to the base 2 – binary
- $(1234)_{10} = (2322)_8 = 2.8^3 + 3.8^2 + 2.8^1 + 2$ to the base 8 – octal

Representations of a Number

- $(1234)_{10} = 1.10^3 + 2.10^2 + 3.10^1 + 4.10^0$ to the base 10 – decimal
- $(1234)_{10} = (10011010010)_2$

  $1.2^{10} + 0.2^9 + 0.2^8 + 1.2^7 + 1.2^6 + 0.2^5 + 1.2^4 + 0.2^3 + 0.2^2 + 1.2^1 + 0.2^0$ to the base 2 – binary
- $(1234)_{10} = (2322)_8 = 2.8^3 + 3.8^2 + 2.8^1 + 2$ to the base 8 – octal
- $(1234)_{10} = (4D2)_{16} = 4.16^2 + D.16^1 + 2.16^0$ to the base 16 – hexadecimal

Base b Representations

- We can use positive integer b greater than 1 as a base to represent any number

Theorem

Let $b, n \in \mathbb{Z}$ and $b > 1,\ \&\ n > 0$. Then n can be expressed uniquely as:

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

where $k \in \mathbb{Z}, k > 0\ \&\ a_0, a_1, \ldots, a_k$ are nonnegative integers $< b$, and $a_k \neq 0$. The $a_j,\ \ j = 0, \ldots, k$ are called the base-b digits of the representation.

- The representation of n is called the base b expansion of n and is denoted by $(a_k a_{k-1} \ldots a_1 a_0)_b$.

Representation of a Number

- **Numbers in different bases**

Representation of a Number

- **Numbers in different bases**
  Any number n, $b^{k-1} \leq n < b^k$ is a k-digit number to the base b.

Representation of a Number

- **Numbers in different bases**
  Any number n, $b^{k-1} \leq n < b^k$ is a k-digit number to the base b.
- **Number of digits**

Representation of a Number

- **Numbers in different bases**
  Any number n, $b^{k-1} \leq n < b^k$ is a k-digit number to the base b.
- **Number of digits**

$$= [\log_b \; n] + 1.$$

Representation of a Number

- **Numbers in different bases**
  Any number n, $b^{k-1} \leq n < b^k$ is a k-digit number to the base b.
- **Number of digits**

$$= [\log_b \; n] + 1.$$

- **Number of bits**

Representation of a Number

- **Numbers in different bases**
  Any number n, $b^{k-1} \leq n < b^k$ is a k-digit number to the base b.
- **Number of digits**

$$= [\log_b \; n] + 1.$$

- **Number of bits**

$$= [\log_2 \; n] + 1 \approx [1.44 \times \; ln \; n] + 1.$$

Algorithm: Constructing Base b Expansions

```
Result: $(a_{k-1} \ldots a_1 a_0)_b$ is base $b$ expansion of $n$
procedure base $b$ expansion;
$q := n$;
$k := 0$;
while $q \neq 0$ do
    $a_k := q \mod b$;
    $q \leftarrow q \ div \ b$;
    $k \leftarrow k + 1$
end
return $(a_{k-1} \ldots a_1 a_0)$
```

Algorithm 1: Base Conversion

Bit Operation for Doing Arithmetic

Number of bit operations required to add 2 k-bit integers n & m

Bit Operation for Doing Arithmetic

Number of bit operations required to add 2 k-bit integers n & m

i. Look at the top and bottom bit and also at whether there's a carry above the top bit.

ii. If both bits are 0 and there is no carry, then put down 0.

iii. If either both bits are 0 and there is a carry; or one of the bits is 0, the other is 1 and there is no carry, then put down 1.

iv. If either one of the bits is 0, the other is 1, and there is a carry; or both bits are 1 and there is no carry then put down 0, put a carry in the next column.

v. If both bits are 1 and there is a carry, then put down 1, put a carry in the next column.

Bit Operation for Doing Arithmetic

Number of bit operations required to add 2 k-bit integers n & m

i. Look at the top and bottom bit and also at whether there's a carry above the top bit.
ii. If both bits are 0 and there is no carry, then put down 0.
iii. If either both bits are 0 and there is a carry; or one of the bits is 0, the other is 1 and there is no carry, then put down 1.
iv. If either one of the bits is 0, the other is 1, and there is a carry; or both bits are 1 and there is no carry then put down 0, put a carry in the next column.
v. If both bits are 1 and there is a carry, then put down 1, put a carry in the next column.

Time$(n + m) = k$-bit operations.

Algorithm: Addition of Integers

Number of bit operations required to add 2 k-bit integers n & m

Input: $n = n_k n_{k-1} \cdots n_2 n_1$ & $m = m_k m_{k-1} \cdots m_2 m_1$

Output: $n + m$ in binary.

Algorithm: $c \leftarrow 0$

```
for($i = 1$ $to$ $k$){
        if $sum(n_i, m_i, c) = 1$ $or$ $3$
             then $d_i \leftarrow 1$
             else $d_i \leftarrow 0$

        if $sum(n_i, m_i, c) \geq 2$
             then $c \leftarrow 1$
             else $c \leftarrow 0$}

if $c = 1$ then output $1d_k d_{k-1} \cdots d_2 d_1$

        else output $d_k d_{k-1} \cdots d_2 d_1$.
```

Bit Operation for Doing Arithmetic

- Number of bit operations required to multiply a k-bit integer n by an ℓ-bit integer m

Bit Operation for Doing Arithmetic

- Number of bit operations required to multiply a k-bit integer n by an ℓ-bit integer m

  i. at most ℓ rows can be obtained
  ii. each row consists of a copy of n shifted to the left a certain distance
  iii. suppose there are $\ell' \leq \ell$ rows.
  iv. multiplication task can be broken down into $\ell' - 1$ additions
  v. moving down from the 2^{nd} row to the ℓ'^{th} row, adding each new row to the partial sum of all of the earlier rows
  vi. each addition takes at most k-bit operations
  vii. total number of bit operations is at most $\ell \times k$.

Bit Operation for Doing Arithmetic

- Number of bit operations required to multiply a k-bit integer n by an ℓ-bit integer m

  i. at most ℓ rows can be obtained
  ii. each row consists of a copy of n shifted to the left a certain distance
  iii. suppose there are $\ell' \leq \ell$ rows.
  iv. multiplication task can be broken down into $\ell' - 1$ additions
  v. moving down from the 2^{nd} row to the ℓ'^{th} row, adding each new row to the partial sum of all of the earlier rows
  vi. each addition takes at most k-bit operations
  vii. total number of bit operations is at most $\ell \times k$.

Time$(n \times m) < k\ell$-bit operations.

Bit Operation for Doing Arithmetic

- Number of bit operations required to multiply two n-bit integers x & y

Bit Operation for Doing Arithmetic

- Number of bit operations required to multiply two n-bit integers x & y
- Let $n = 2t$. Then

$$x = 2^t x_1 + x_0 \ \& \ y = 2^t y_1 + y_0$$

Bit Operation for Doing Arithmetic

- Number of bit operations required to multiply two n-bit integers x & y
- Let $n = 2t$. Then

$$x = 2^t x_1 + x_0 \;\&\; y = 2^t y_1 + y_0$$

- $$x.y = u_2.2^{2t} + u_1.2^t + u_0$$

Bit Operation for Doing Arithmetic

- Number of bit operations required to multiply two n-bit integers x & y
- Let $n = 2t$. Then

$$x = 2^t x_1 + x_0 \;\&\; y = 2^t y_1 + y_0$$

- $$x.y = u_2.2^{2t} + u_1.2^t + u_0$$

  where $u_0 = x_0.y_0,\; u_2 = x_1.y_1 \;\&\; u_1 = (x_0 + x_1).(y_0 + y_1) - u_0 - u_2$.

Bit Operation for Modular Exponentiation

- Find $b^n \mod m$ efficiently, where $b, n, \& m$ are large integers.

Bit Operation for Modular Exponentiation

- Find $b^n \mod m$ efficiently, where $b, n, \ \& \ m$ are large integers.
- We use the binary expansion of $n = (a_{k-1}, \ldots, a_1, a_0)_2$, to compute b^n.

Bit Operation for Modular Exponentiation

- Find $b^n \mod m$ efficiently, where $b, n, \ \& \ m$ are large integers.
- We use the binary expansion of $n = (a_{k-1}, \ldots, a_1, a_0)_2$, to compute b^n.

$$b^n = (b)^{a_{k-1}2^{k-1}+\cdots+a_1 2+a_0} = (b)^{a_{k-1}.2^{k-1}} \ldots (b)^{a_1.2} . (b)^{a_0}$$

Bit Operation for Modular Exponentiation

- Find $b^n \mod m$ efficiently, where $b, n, \ \& \ m$ are large integers.
- We use the binary expansion of $n = (a_{k-1}, \ldots, a_1, a_0)_2$, to compute b^n.

$$b^n = (b)^{a_{k-1}2^{k-1}+\cdots+a_1 2+a_0} = (b)^{a_{k-1}.2^{k-1}} \ldots (b)^{a_1.2} . (b)^{a_0}$$

- Therefore, to compute b^n, we need only compute the values of

$$b, b^2, \left(b^2\right)^2 = b^4, \left(b^4\right)^2 = b^8, \ldots, (b)^{2^{k-1}}$$

and the multiply the terms b^{2^j} in this list, where $a_j = 1$.

Bit Operation for Modular Exponentiation

```
procedure modular exponentiation $b^n \mod m$;
$x := 1$;
$power := b \mod m$;
for $i := 0$ to $k - 1$ do
    if $a_i = 1$ then
        $x \leftarrow (x.power) \mod m$
    end
    $power \leftarrow (power.power) \mod m$
end
return $x\{x \ equals \ b^n \mod m\}$
```

Algorithm 2: Modular Exponentiation

Bit Operation for Modular Exponentiation

```
procedure modular exponentiation $b^n \mod m$;
$x := 1$;
$power := b \mod m$;
for $i := 0$ to $k - 1$ do
    if $a_i = 1$ then
        $x \leftarrow (x.power) \mod m$
    end
    $power \leftarrow (power.power) \mod m$
end
return $x\{x\ equals\ b^n \mod m\}$
```

Algorithm 3: Modular Exponentiation

Computational Complexity to compute $b^n \mod m = O((\log m)^2 \log n)$

Bit Operation for Modular Exponentiation

Exercise

Compute $3^{37} \mod 53$

Bit Operation for Modular Exponentiation

Exercise

Compute $3^{37} \mod 53$

Solution

- *Binary representation of* $37 = 32 + 4 + 1 = 100101$
- *First we repeatedly square* $3 \mod 53$ *until we have worked out* 3^{2^k} *for every* k *s/t* $2^k \leq 37$.
- *We get*
  $3^2 = 9, 3^4 = 9^2 = 81 \equiv 28, 3^8 \equiv 28^2 =$

Bit Operation for Modular Exponentiation

Exercise

Compute $3^{37} \mod 53$

Solution

- *Binary representation of* $37 = 32 + 4 + 1 = 100101$
- *First we repeatedly square* $3 \mod 53$ *until we have worked out* 3^{2^k} *for every* k *s/t* $2^k \leq 37$.
- *We get*
  $3^2 = 9, 3^4 = 9^2 = 81 \equiv 28, 3^8 \equiv 28^2 = 784 \equiv -11 (\because 15 \times 53 = 795),$
  $3^{16} \equiv 121 \equiv 15 \quad , 3^{32} \equiv 225 \equiv 13.$
- *Therefore,*
  $3^{37} \equiv 13 \times 28 \times 3 = 13 \times 84 \equiv 13 \times 31 = 403 \equiv 32.$

Outline

1. Divisibility and Modular Arithmetic
2. Integer Representations and Algorithms
3. Primes and Greatest Common Divisors
4. Solving Congruences

Primes

Definition

A positive integer $p > 1$ is called ***prime*** *if the only positive divisor of p are 1 and p.*

A positive integer $n > 1$ and is not prime is called ***composite****.*

Primes

Definition

*A positive integer $p > 1$ is called **prime** if the only positive divisor of p are 1 and p.*

*A positive integer $n > 1$ and is not prime is called **composite**.*

Theorem (The Fundamental Theorem of Arithmetic)

Every integer can be written as the product of primes (in order of nondecreasing size) in an essentially unique way.
Every nonzero integer n can be expressed as a product of the form

$$n = \pm p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

*where the p_i's are k distinct primes and the e_i's are integers with $e_i > 0$. This representation is **unique** up to the order in which the factors are written*[a].

[a] If we decide that 1 should be considered to be a prime, the uniqueness of this decomposition into primes would no longer hold!

The Fundamental Theorem of Arithmetic

Example

- $100 = 2.2.5.5 = 2^2.5^2$
- *641 = 641*
- $999 = 3.3.3.37 = 3^3.37$
- $1024 = 2.2.2.2.2.2.2.2.2.2 = 2^{10}$

The Sieve of Erastosthenes

- The Sieve of Erastosthenes can be used to find all primes not exceeding a specified positive integer n.

The Sieve of Erastosthenes

- The Sieve of Erastosthenes can be used to find all primes not exceeding a specified positive integer n.

  For example, begin with the list of integers between 1 and 100.

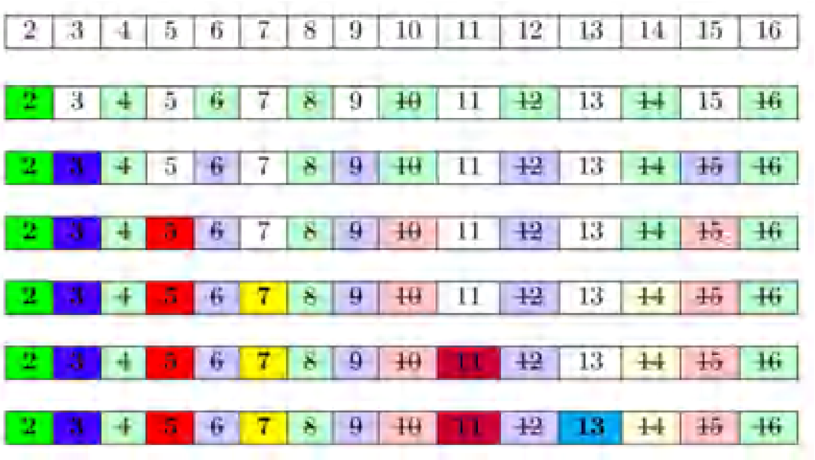
  (i) Delete all the integers, other than 2, divisible by 2.
  (ii) Delete all the integers, other than 3, divisible by 3.
  (iii) Next, delete all the integers, other than 5, divisible by 5.
  (iv) Next, delete all the integers, other than 7, divisible by 7.
  (v) Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,$$

$$71, 73, 79, 83, 89, 97\}$$

The Sieve of Erastosthenes

All prime numbers in the range [1 : 16]



2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~	15	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~
2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~

The Sieve of Erastosthenes

- If an integer n is a composite, then it has a prime divisor $\leq \sqrt{n}$.

The Sieve of Erastosthenes

- If an integer n is a composite, then it has a prime divisor $\leq \sqrt{n}$.
- To see this, note that if $n = ab$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
- Trial division, a very inefficient method of determining if a number n is prime, is to try every integer $k \leq \sqrt{n}$ and see if n is divisible by k.
- Computational complexity of this algo $= O(n \log \log n)$

Infinitude of Primes

Theorem (Euclid)

There are infinitely many primes.

Infinitude of Primes

Theorem (Euclid)

There are infinitely many primes.

Proof.

- Assume there are finitely many primes: $p_1, p_2, \ldots, p_n$
- Let $q = p_1 p_2 \ldots p_n + 1$
- Either q is prime or by the fundamental theorem of arithmetic it is a product of primes.
- But none of the primes p_j divides q since if $p_j \mid q$, then $p_j \mid (q - p_1 p_2 \ldots p_n)$, i.e., $p_j \mid 1$.
- Hence, there is a prime q not on the list $p_1, p_2, \ldots, p_n$.

This proof was given by Euclid The Elements. The proof is considered to be one of the most beautiful in all mathematics.

It is the first proof in The Book, inspired by the famous mathematician Paul Erdös' imagined collection of perfect proofs

maintained by God.

Mersene Primes

Definition

Prime numbers of the form $2^p - 1$, where p is prime, are called Mersene primes.

- $2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^5 - 1 = 31$, and $2^7 - 1 = 127$ are Mersene primes.

Mersene Primes

Definition

Prime numbers of the form $2^p - 1$, where p is prime, are called Mersene primes.

- $2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^5 - 1 = 31$, and $2^7 - 1 = 127$ are Mersene primes.
- $2^{11} - 1 = 2047$

Mersene Primes

Definition

Prime numbers of the form $2^p - 1$, where p is prime, are called Mersene primes.

- $2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^5 - 1 = 31$, and $2^7 - 1 = 127$ are Mersene primes.
- $2^{11} - 1 = 2047$ is not a Mersene prime since $2047 = 23 \times 89$.
- The largest known prime numbers are Mersene primes.
- The Great Internet Mersenne Prime Search (GIMPS) has discovered on 07 Dec 2018 the largest known prime number, $2^{82,589,933} - 1$, having 24,862,048 digits.

  A computer volunteered by Patrick Laroche from Ocala, Florida made the find on December 7, 2018. The new prime number, also known as $M_{82589933}$. It is more than one and a half million digits larger than the previous record prime number.

Distribution of Primes

- Mathematicians have been interested in the distribution of prime numbers among the positive integers. In the nineteenth century, the **prime number theorem** was proved which gives an asymptotic estimate for the number of primes not exceeding x.

Theorem (Prime Number Theorem)

The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound.

- The theorem tells us that the number of primes not exceeding x, can be approximated by $\frac{x}{\ln x}$.
- The odds that a randomly selected positive integer $< n$ is prime are approximately $\frac{\frac{n}{\ln n}}{n} = \frac{1}{\ln n}$.

Primes and Arithmetic Progressions

- Euclid proved that there are infinitely many primes.
- G. Lejuenne Dirchlet also showed that every arithmetic progression $ka + b$, $k = 1, 2, \ldots$, where $a \mathbin{\&} b$ have no common factor greater than 1 contains infinitely many primes in the 19th century
- Are there long arithmetic progressions made up entirely of primes?

Primes and Arithmetic Progressions

- Euclid proved that there are infinitely many primes.
- G. Lejuenne Dirchlet also showed that every arithmetic progression $ka + b$, $k = 1, 2, \ldots$, where a & b have no common factor greater than 1 contains infinitely many primes in the 19th century
- Are there long arithmetic progressions made up entirely of primes?
  - 5,11, 17, 23, 29 is an arithmetic progression of **5 primes**.
  - 199, 409, 619, 829, 1039,1249, 1459, 1669, 1879, 2089 is an arithmetic progression of **10 primes**.
- In the 1930s, Paul Erdös conjectured that for every positive integer $n > 1$, there is an arithmetic progression of length n made up entirely of primes. This was proven in 2006, by Ben Green and Terence Tau.

Primes Generation

- Number theory is noted as a subject for which it is easy to formulate conjectures, some of which are difficult to prove and others that remained open problems for many years.
- It would be useful to have a function $f(n)$ s/t $f(n)$ is prime $\forall n \in \mathbb{N}$.
- If we had such a function, we could generate large primes for use in cryptography and other applications.
- Consider the polynomial $f(n) = n^2 - n + 41$.

Primes Generation

- Number theory is noted as a subject for which it is easy to formulate conjectures, some of which are difficult to prove and others that remained open problems for many years.
- It would be useful to have a function $f(n)$ s/t $f(n)$ is prime $\forall n \in \mathbb{N}$.
- If we had such a function, we could generate large primes for use in cryptography and other applications.
- Consider the polynomial $f(n) = n^2 - n + 41$. This polynomial has the interesting property that $f(n)$ is prime for all positive integers $n \leq 40$.

Generating Primes

- The problem of generating large primes is of both theoretical and practical interest.
- Finding large primes, say with 300 hundred of digits, is important in cryptography.
- So far, no useful closed formula that always produces primes has been found.
- Fortunately, we can generate large integers which are almost certainly primes.

Generating Primes

- The problem of generating large primes is of both theoretical and practical interest.
- Finding large primes, say with 300 hundred of digits, is important in cryptography.
- So far, no useful closed formula that always produces primes has been found.
- Fortunately, we can generate large integers which are almost certainly primes.
- In 2002, AKS gave algorithm PRIMES is in P
- Miller-Rabin primality test proposed in 1980. It's a probabilistic algorithm. It is normally used to check primality of large number.

Conjectures about Primes

Conjecture (Goldbach's Conjecture)

- *In 1742, **Christian Goldbach** conjectured that every odd integer $n,\ n > 5$, is the sum of three primes.*
- ***Euler** replied that this conjecture is equivalent to the conjecture that every even integer $n,\ n > 2$, is the sum of two primes.*

Conjectures about Primes

Conjecture (Goldbach's Conjecture)

- *In 1742, **Christian Goldbach** conjectured that every odd integer $n,\ n > 5$, is the sum of three primes.*
- ***Euler** replied that this conjecture is equivalent to the conjecture that every even integer $n,\ n > 2$, is the sum of two primes.Now, this called **Goldbach's conjecture**.*

Conjectures about Primes

Conjecture (Goldbach's Conjecture)

- *In 1742, **Christian Goldbach** conjectured that every odd integer $n, \ n > 5$, is the sum of three primes.*
- ***Euler** replied that this conjecture is equivalent to the conjecture that every even integer $n, \ n > 2$, is the sum of two primes.Now, this called **Goldbach's conjecture**.*

As of early 2018, the conjecture has been checked for all positive even integers up to 4×10^{18}

Definition

Twin primes are pairs of primes that differ by 2

Conjectures about Primes

Conjecture (The Twin Prime Conjecture)

There are infinitely many twin primes.

Conjectures about Primes

Conjecture (The Twin Prime Conjecture)

There are infinitely many twin primes.

- The largest known twin primes found in Sep 2016, consists of the numbers

$$2,996,863,034,895 \times 2^{1,290,000} \pm 1,$$

having 3,88,342 decimal digits.

Conjectures about Primes

Conjecture (The Twin Prime Conjecture)

There are infinitely many twin primes.

- The largest known twin primes found in Sep 2016, consists of the numbers

$$2,996,863,034,895 \times 2^{1,290,000} \pm 1,$$

having 3,88,342 decimal digits.

- The latest known twin primes found in May 2021, consists of the numbers

$$17976255129 \times 2^{183241} \pm 1,$$

having 55,172 decimal digits.

Greatest Common Divisor

Definition

Given $a, b \in \mathbb{Z},\ b \neq 0$, *the* *greatest common divisor* a & b, *denoted* $\gcd(a, b)$, *is the positive common divisor of* a & b, *that is divisible by each of their common divisors. In other words, the largest integer* d *s/t* $d \mid a$ & $d \mid b$.

Definition

The integers a *and* b *are* *relatively prime* *if* $\gcd(a, b) = 1$.

Definition

The integers $a_1, a_2, \ldots, a_n$ *are* *pairwise relatively prime* *if* $\gcd(a_i, a_j) = 1$ *whenever* $1 \leq i < j \leq n$.

Finding the GCD Using Prime Factorizations

- Suppose that the prime factorizations of the positive integers a & b are

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n},$$

where each exponent is a nonnegative integer. Then

$$\gcd(a, b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \ldots p_n^{min(a_n,b_n)}$$

Finding the GCD Using Prime Factorizations

- Suppose that the prime factorizations of the positive integers a & b are

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n},$$

where each exponent is a nonnegative integer. Then

$$\gcd(a, b) = p_1^{min(a_1, b_1)} p_2^{min(a_2, b_2)} \dots p_n^{min(a_n, b_n)}$$

- Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Finding the Least Common Multiple (LCM)

Definition

The least common multiple of the positive integers a & b is the smallest positive integer that is divisible by both a & b. It is denoted by $lcm(a,b)$.

- Suppose

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n},$$

where each exponent is a nonnegative integer. Then

$$lcm(a,b) = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \dots p_n^{max(a_n,b_n)}$$

Theorem

Let a & b be positive integers. Then

$$ab = \gcd(a,b) \times lcm(a,b)$$

Greatest Common Divisor

Theorem

- (i) $\gcd(a, b) = \gcd(b, a)$.
- (ii) $\gcd(a, a) = a$.
- (iii) $\gcd(a, b) = \gcd(a - b, b)$
- (iv) $\gcd(0, a) = a$.

Euclidean Algorithm

Euclidean algorithm for computing the $\gcd(a, b)$

Input: 2 non-negative integers a & b, with $a \geq b$.

Output: $\gcd(a, b)$

```
1 While $(b \neq 0)$ do
    1.1 Set $r \leftarrow a \ mod \ b$, $a \leftarrow b, \ b \leftarrow r$.
2 Return($a$)
```

Euclidean Algorithm

Euclidean algorithm for computing the $\gcd(a, b)$

Input: 2 non-negative integers a & b, with $a \geq b$.
Output: $\gcd(a, b)$

```
1 While $(b \neq 0)$ do
    1.1 Set $r \leftarrow a \bmod b$,
        $a \leftarrow b,\ b \leftarrow r$.
2 Return($a$)
```

$\gcd(4864, 3458)$

Euclidean Algorithm

Euclidean algorithm for computing the $\gcd(a, b)$

Input: 2 non-negative integers a & b, with $a \geq b$.

Output: $\gcd(a, b)$

```
1 While $(b \neq 0)$ do
    1.1 Set $r \leftarrow a \bmod b$,
        $a \leftarrow b,\ b \leftarrow r$.
2 Return$(a)$
```

$\gcd(4864, 3458)$

$$\begin{aligned} 4864 &= 1.3458 + 1406 \\ 3458 &= 2.1406 + 646 \\ 1406 &= 2.646 + 114 \\ 646 &= 5.114 + 76 \\ 114 &= 1.76 + 38 \\ 76 &= 2.38 + 0. \end{aligned}$$

Correctness of Euclidean Algorithm

Lemma

Let $a = bq + r$, *where* $a, b, q,\ \& \, r \in \mathbb{Z}$ *and* $r \geq 0$. *Then* $\gcd(a, b) = \gcd(b, r)$.

Correctness of Euclidean Algorithm

Lemma

Let $a = bq + r$*, where* $a, b, q, \ \& \, r \in \mathbb{Z}$ *and* $r \geq 0$*. Then* $\gcd(a, b) = \gcd(b, r)$*.*

Proof.

- Suppose that $d \mid a$ and $d \mid b$. Then d also divides $a - bq = r$. Hence, any common divisor of $a \ \& \ b$ must also be any common divisor of $b \ \& \ r$.
- Suppose that $d \mid b$ and $d \mid r$. Then $d \mid (bq + r) = a$. Hence, any common divisor of $a \ \& \ b$ must also be a common divisor of $b \ \& \ r$.
- Therefore, $\gcd(a, b) = \gcd(b, r)$.

□

GCDs as Linear Combinations

Bézout's Lemma

$\forall\ a, b \in \mathbb{Z},\ \ \exists\ s, t \in \mathbb{Z}$ s/t $gcd(a, b) = s.a + t.b$

Definition

If a & b are positive integers, then integers s & t s/t $\gcd(a, b) = sa + tb$ are called Bézout coefficients of a & b. The equation $\gcd(a, b) = sa + tb$ is called Bézout's identity.

- By Bézout's lemma, the $\gcd(a, b)$ can be expressed in the form $sa + tb$ where $s, t \in \mathbb{Z}$. This is a linear combination with integer coefficients of a & b.

Extended Euclidean Algorithm

Extended Euclidean algorithm

Input: 2 non-negative integers a & b, with $a \geq b$.
Output: $d = \gcd(a, b)$ & $x, y \in \mathbb{Z}$ s/t $ax + by = d$.

```
1 If $b = 0$ then set $d \leftarrow a,\ x \leftarrow 1,\ y \leftarrow 0$, and
  $return(d, x, y)$.
2 Set $x_2 \leftarrow 1,\ x_1 \leftarrow 0,\ y_2 \leftarrow 0,\ y_1 \leftarrow 1$.
3 While $(b > 0)$ do
    3.1 $q \leftarrow \lfloor a/b \rfloor,\ r \leftarrow a - qb$,
        $x \leftarrow x_2 - qx_1,\ y \leftarrow y_2 - qy_1$.
    3.2 $a \leftarrow b,\ b \leftarrow r,\ x_2 \leftarrow x_1$,
        $x_1 \leftarrow x,\ y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4 Set $d \leftarrow a,\ x \leftarrow x_2,\ y \leftarrow y_2$, and $return(d, x, y)$.
```

Extended Euclidean Algorithm

Extended Euclidean algorithm

Input: 2 non-negative integers a & b, with $a \geq b$.
Output: $d = \gcd(a, b)$ & $x, y \in \mathbb{Z}$ s/t $ax + by = d$.

```
1 If $b = 0$ then set $d \leftarrow a,\ x \leftarrow 1,\ y \leftarrow 0$, and
  $return(d, x, y)$.
2 Set $x_2 \leftarrow 1,\ x_1 \leftarrow 0,\ y_2 \leftarrow 0,\ y_1 \leftarrow 1$.
3 While $(b > 0)$ do
    3.1 $q \leftarrow \lfloor a/b \rfloor,\ r \leftarrow a - qb$,
        $x \leftarrow x_2 - qx_1,\ y \leftarrow y_2 - qy_1$.
    3.2 $a \leftarrow b,\ b \leftarrow r,\ x_2 \leftarrow x_1$,
        $x_1 \leftarrow x,\ y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4 Set $d \leftarrow a,\ x \leftarrow x_2,\ y \leftarrow y_2$, and $return(d, x, y)$.
```

$a = 4864,\ b = 3458$

Extended Euclidean Algorithm

Extended Euclidean algorithm

Input: 2 non-negative integers a & b, with $a \geq b$.
Output: $d = \gcd(a, b)$ & $x, y \in \mathbb{Z}$ s/t $ax + by = d$.

```
1  If $b = 0$ then set $d \leftarrow a,\ x \leftarrow 1,\ y \leftarrow 0$, and
   $return(d, x, y)$.
2  Set $x_2 \leftarrow 1,\ x_1 \leftarrow 0,\ y_2 \leftarrow 0,\ y_1 \leftarrow 1$.
3  While $(b > 0)$ do
     3.1  $q \leftarrow \lfloor a/b \rfloor,\ r \leftarrow a - qb$,
          $x \leftarrow x_2 - qx_1,\ y \leftarrow y_2 - qy_1$.
     3.2  $a \leftarrow b,\ b \leftarrow r,\ x_2 \leftarrow x_1$,
          $x_1 \leftarrow x,\ y_2 \leftarrow y_1$, and $y_1 \leftarrow y$.
4  Set $d \leftarrow a,\ x \leftarrow x_2,\ y \leftarrow y_2$, and $return(d, x, y)$.
```

$$a = 4864,\ \ b = 3458$$

q	r	x	y	a	b	x_2	x_1	y_2	y_1
—	—	—	—	4864	3458	1	0	0	1
1	1406	1	−1	3458	1406	0	1	1	−1
2	646	−2	3	1406	646	1	−2	−1	3
2	114	5	−7	646	114	−2	5	3	−7
5	76	−27	38	114	76	5	−27	−7	38
1	38	32	−45	76	38	−27	32	38	−45
2	0	−91	128	38	0	32	−91	−45	128

$$38 = 32.4864 - 45.3458$$

Consequences of Bézout's Theorem

Lemma

If $a, b, c \in \mathbb{N}$ s/t $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Lemma

If p is prime and $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some i.

Theorem

Let m be a positive integer and let $a, b, c \in \mathbb{Z}$. If $ac \equiv bc \mod m$ and $\gcd(c, m) = 1$, then $a \equiv b \mod m$.

Outline

1. Divisibility and Modular Arithmetic
2. Integer Representations and Algorithms
3. Primes and Greatest Common Divisors
4. Solving Congruences

Linear Congruences

Definition

A congruence of the form

$$ax \equiv b \mod m,$$

where $m \in \mathbb{N}, a \,\&\, b \in \mathbb{Z}$, and x is a variable, is called a linear congruence.

- The solutions to a linear congruence $ax \equiv b \mod m$ are all integers x that satisfy the congruence.

Definition

An integer $\bar{a}$ is said to be an (the) inverse of a modulo m if

$$\bar{a}.a \equiv 1 \mod m.$$

Solution of Linear Congruences

- One method of solving linear congruences is by finding the inverse $\bar{a}$, if it exists.
- Although we can not divide both sides of the congruence by a, we can multiply by $\bar{a}$ to solve for x.

Theorem

If a & m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.

Solution of Linear Congruences

Theorem

Let $a, m \in \mathbb{Z}$ *with* $m > 0$*, and let* $d := \gcd(a, m)$*.*

1. *For every* $b \in \mathbb{Z}$*, the congruence* $ax \equiv b \mod m$ *has a solution iff* $d \mid b$*.*
2. *For every* $x \in \mathbb{Z}$*, we have* $ax \equiv 0 \mod m$ *iff* $x \equiv 0 \mod \frac{m}{d}$*.*
3. *For all* $x, x' \in \mathbb{Z}$*, we have* $ax \equiv ax' \mod m$ *iff* $x \equiv x' \mod \frac{m}{d}$

Solution of Linear Congruences

Theorem

Let $a, m \in \mathbb{Z}$ *with* $m > 0$*, and let* $d := \gcd(a, m)$*.*

1. *For every* $b \in \mathbb{Z}$*, the congruence* $ax \equiv b \mod m$ *has a solution iff* $d \mid b$*.*
2. *For every* $x \in \mathbb{Z}$*, we have* $ax \equiv 0 \mod m$ *iff* $x \equiv 0 \mod \frac{m}{d}$*.*
3. *For all* $x, x' \in \mathbb{Z}$*, we have* $ax \equiv ax' \mod m$ *iff* $x \equiv x' \mod \frac{m}{d}$

Proof.

Let $b \in \mathbb{Z}$ be given. Then we have

$ax \equiv b \mod m$ for some $x \in \mathbb{Z}$

$\Leftrightarrow ax = b + my$ for some $y \in \mathbb{Z}$

$\Leftrightarrow ax - my = b$

$\Leftrightarrow d \mid b$ □

Solution of Linear Congruences

Example

In the following table is an illustration for $m = 15$ *and* $a = 1, 2, 3, 4, 5$.

$1.x$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$2.x$	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
$3.x$	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
$4.x$	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
$5.x$	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10

Chinese Remainder Theorem

- In the first century, the Chinese mathematician Sun-Tsu asked: *There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?*

Chinese Remainder Theorem

- In the first century, the Chinese mathematician Sun-Tsu asked: *There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?*
- This puzzle can be translated into the solution of the system of congruences:
  $x \equiv 2 \mod 3$,
  $x \equiv 3 \mod 5$,
  $x \equiv 2 \mod 7$?
- Now, we'll see how the Chinese Remainder Theorem can be used to solve Sun-Tsu's problem.

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

If the integers $n_1, n_2, \cdots, n_k$ *are pairwise relatively prime, then the system of simultaneous congruences*

$$x \;\equiv\; a_i \; mod \; n_i,$$

for $1 \leq i \leq k$ *has a* $!$ *solution modulo* $n = n_1 n_2 \cdots n_k$ *which is given by*

$$x = \sum_{i=1}^{k} a_i N_i M_i \; mod \; n,$$

where $N_i = n/n_i \;\&\; M_i = N_i^{-1} \; mod \; n_i$.

Chinese Remainder Theorem

Example

Consider the 3 congruences from Sun-Tsu's problem:
$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 2 \mod 7.$

- $n = 3.5.7 = 105, \; N_1 = n/3 = 35, \; N_2 = 21, \; \& \; N_3 = 15$

Chinese Remainder Theorem

Example

Consider the 3 congruences from Sun-Tsu's problem:
$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 2 \mod 7.$

- $n = 3.5.7 = 105, \; N_1 = n/3 = 35, \; N_2 = 21, \; \& \; N_3 = 15$
- *We see that*
  - $35^{-1} \mod 3 \equiv 2 \mod 3$
  - $21^{-1} \mod 5 \equiv 1 \mod 5$
  - $15^{-1} \mod 7 \equiv 1 \mod 7$
- *Now we have*

$$x = a_1 N_1 M_1 + a_2 N_2 M_2 + a_3 N_3 M_3 \mod n$$

Chinese Remainder Theorem

Example

Consider the 3 congruences from Sun-Tsu's problem:
$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 2 \mod 7.$

- $n = 3.5.7 = 105, \; N_1 = n/3 = 35, \; N_2 = 21, \; \& \; N_3 = 15$
- *We see that*
  - $35^{-1} \mod 3 \equiv 2 \mod 3$
  - $21^{-1} \mod 5 \equiv 1 \mod 5$
  - $15^{-1} \mod 7 \equiv 1 \mod 7$
- *Now we have*

$$x = a_1N_1M_1 + a_2N_2M_2 + a_3N_3M_3 \mod n$$

$$x = 2.35.2 + 3.21.1 + 2.15.1 = 233 \equiv 23 \mod 105$$

Fermat's Little Theorem

Theorem

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$ Furthermore, for every integer a we have $a^p \equiv a \mod p$.

Fermat's Little Theorem

Theorem

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$ Furthermore, for every integer a we have $a^p \equiv a \mod p$.

Proof.

- Claim: $\because p \nmid a$, the integers $0.a, 1.a, \ldots, (p-1)a$ are distinct residues of $\mod p$
- Thus, $1.a, \ldots, (p-1)a$ are simply a arrangement of $1, 2, \ldots (p-1)$ under $\mod p$
- We have $a^{p-1}(p-1)! \equiv (p-1)! \mod p$
- So, $p \mid \Big((p-1)!(a^{p-1}-1)\Big) \Rightarrow p \mid (a^{p-1}-1)$

□

Fermat's Little Theorem

Exercise

Find $7^{222} \mod 11$.

Corollary

If $p \nmid a$ *and* $n \equiv m \mod (p-1)$, *then* $a^n \equiv a^m \mod p$

Exercise

Find the last base-7 digit in $2^{1000000}$

Euler phi Function

Definition

For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1,\ n]$ which are relatively prime to n. The function ϕ is called the ***Euler phi function***.

Properties of Euler phi function

i. If p is a prime, then $\phi(p) =$

Euler phi Function

Definition

For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1, \ n]$ which are relatively prime to n. The function ϕ is called the ***Euler phi function****.*

Properties of Euler phi function

i. If p is a prime, then $\phi(p) = p - 1$.

ii. The Euler phi function is **multiplicative**. That is, if $gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

iii. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, is the prime factorization of n, then

$$\phi(n) =$$

Euler phi Function

Definition

For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1,\ n]$ which are relatively prime to n. The function ϕ is called the ***Euler phi function***.

Properties of Euler phi function

i. If p is a prime, then $\phi(p) = p - 1$.

ii. The Euler phi function is **multiplicative**. That is, if $gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

iii. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, is the prime factorization of n, then

$$\phi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\ldots\left(p_k^{k_1} - p_k^{k_1-1}\right) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right).$$

Euler's Generalization

Theorem

If $\gcd(a, m) = 1$, *then* $a^{\phi(m)} \equiv 1 \mod m$.

Euler's Generalization

Theorem

If $\gcd(a, m) = 1$*, then* $a^{\phi(m)} \equiv 1 \mod m$*.*

Proof.

- We first prove the theorem for $m = p^{\alpha}$.
- Use mathematical induction on α. The case $\alpha = 1$ is precisely Fermat's Little Theorem.
- Suppose that $\alpha \geq 2$, this holds for the $m = p^{\alpha-1}$. Thus, we have

$$a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + p^{\alpha-1}.k$$

for some integer k.

□

Euler's Generalization

Proof.

- Now, raising both sides of the equation $a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + p^{\alpha-1}.k$ to the p-th power, we have

  $$a^{p^{\alpha}-p^{\alpha-1}} = \left(1 + p^{\alpha-1}.k\right)^p$$

  $$\Rightarrow a^{\phi(p^{\alpha})} \equiv 1 \mod p^{\alpha},$$

Euler's Generalization

Proof.

- Now, raising both sides of the equation $a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + p^{\alpha-1}.k$ to the p-th power, we have

  $$a^{p^{\alpha}-p^{\alpha-1}} = \left(1 + p^{\alpha-1}.k\right)^p$$

  $$\Rightarrow a^{\phi(p^{\alpha})} \equiv 1 \mod p^{\alpha},$$

  using the fact that the binomial coefficients in $(1+x)^p$ are each divisible by p (except in the 1 and x^p at the ends)
- This proves the proposition for prime powers.
- Finally, by the multiplicativity of ϕ, it is clear that $a^{\phi(m)} \equiv 1 \mod m$

□

Euler's Generalization

Proof.

- Now, raising both sides of the equation $a^{p^{\alpha-1}-p^{\alpha-2}} = 1 + p^{\alpha-1}.k$ to the p-th power, we have

  $$a^{p^{\alpha}-p^{\alpha-1}} = \left(1 + p^{\alpha-1}.k\right)^{p}$$

  $$\Rightarrow a^{\phi(p^{\alpha})} \equiv 1 \mod p^{\alpha},$$

  using the fact that the binomial coefficients in $(1 + x)^p$ are each divisible by p (except in the 1 and x^p at the ends)
- This proves the proposition for prime powers.
- Finally, by the multiplicativity of ϕ, it is clear that $a^{\phi(m)} \equiv 1 \mod m$

□

Exercise

Compute $2^{1000000} \mod 77$.

Pseudo-primes

Definition

Let b be a positive integer. If n is a composite integer, and $b^{n-1} \equiv 1 \mod n$, then n is called a pseudo-prime to the base b.

Pseudo-primes

Definition

Let b be a positive integer. If n is a composite integer, and $b^{n-1} \equiv 1 \mod n$, then n is called a pseudo-prime to the base b.

Example

The integer 341 is a pseudo-prime to the base 2.

$$341 = 11 \times 31$$

$$2^{340} \equiv 1 \mod 341$$

Pseudo-primes

- Given a positive integer n, s/t $2^{n-1} \equiv 1 \mod n$:

Pseudo-primes

- Given a positive integer n, s/t $2^{n-1} \equiv 1 \mod n$:
  - If n does not satisfy the congruence, it is **composite**.
  - If n does satisfy the congruence, it is either *prime* or a *pseudo-prime* to the base 2.
- Doing similar tests with additional bases b, provides more evidence as to whether n is prime.
- Among the positive integers not exceeding a positive real number x, compared to primes, there are relatively few pseudo-primes to the base b.
  - E.g., among the positive integers $< 10^{10}$ there are 455,052,512 primes, but only 14,884 pseudo-primes to the base 2.

Carmichael Numbers

Definition

A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \mod n \ \forall\ b, b \in \mathbb{N}$ with $\gcd(b, n) = 1$ is called a Carmichael number.

Carmichael Numbers

Definition

A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \mod n \ \forall\ b, b \in \mathbb{N}$ with $\gcd(b,n) = 1$ is called a Carmichael number.

Example

The integer 561 is a Carmichael number. To see this:

- $561 = 3 \times 11 \times 17.$
- *If* $\gcd(b,561) = 1$, *then* $\gcd(b,3) = 1$, $\gcd(b,11) = 1$ *and* $\gcd(b,17) = 1$.
- *If* $\gcd(b,561) = 1$, *we have*

$$b^{560} = \left(b^2\right)^{280} \equiv 1 \mod 3,$$

$$b^{560} = \left(b^{10}\right)^{56} \equiv 1 \mod 11,$$

$$b^{560} = \left(b^{16}\right)^{35} \equiv 1 \mod 17.$$

Carmichael Numbers

Definition

A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \mod n \; \forall\, b, b \in \mathbb{N}$ with $\gcd(b, n) = 1$ is called a Carmichael number.

Example

The integer 561 is a Carmichael number. To see this:

- $561 = 3 \times 11 \times 17.$
- *If* $\gcd(b, 561) = 1$, *then* $\gcd(b, 3) = 1$, $\gcd(b, 11) = 1$ *and* $\gcd(b, 17) = 1$.
- *If* $\gcd(b, 561) = 1$, *we have*

$$b^{560} = \left(b^2\right)^{280} \equiv 1 \mod 3,$$

$$b^{560} = \left(b^{10}\right)^{56} \equiv 1 \mod 11,$$

$$b^{560} = \left(b^{16}\right)^{35} \equiv 1 \mod 17.$$

There are infinitely many Carmichael numbers

Primitive Roots

Definition

A primitive root *modulo a prime* p *is an integer* g *in* $\mathbb{Z}_p^*$ *s/t every nonzero element of* $\mathbb{Z}_p$ *is a power of* g*.*

Example

(i) *2 is a primitive root of 11.*

(ii) *3 is not a primitive root of 11.*

Powers of $3 \mod 11$*:*
$3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 5,\ 3^4 \equiv 4,\ 3^5 \equiv 1$

Important Fact: There is a primitive root modulo p for every prime number p.

Discrete Logarithms

Definition

Suppose that p is prime, g is a primitive root modulo p, and a is an integer s/t $1 \leq a \leq p-1$. If $g^x \equiv a \mod p$ for $1 \leq x \leq p-1$, we say that x is the discrete logarithm of $a \mod p$ to the base g and we write $x = \log_g a$.

Example

(i) $2^8 \equiv 3 \mod 11 \Rightarrow \log_2 3 = 8$, *the discrete logarithm of 3 modulo 11 to the base 2 is 8.*

(ii) $2^4 \equiv 5 \mod 11 \Rightarrow \log_2 5 = 4$, *the discrete logarithm of 5 modulo 11 to the base 2 is 4.*

Discrete Logarithms

Definition

Suppose that p is prime, g is a primitive root modulo p, and a is an integer s/t $1 \leq a \leq p-1$. If $g^x \equiv a \mod p$ for $1 \leq x \leq p-1$, we say that x is the discrete logarithm of $a \mod p$ to the base g and we write $x = \log_g a$.

Example

(i) $2^8 \equiv 3 \mod 11 \Rightarrow \log_2 3 = 8$, *the discrete logarithm of 3 modulo 11 to the base 2 is 8.*

(ii) $2^4 \equiv 5 \mod 11 \Rightarrow \log_2 5 = 4$, *the discrete logarithm of 5 modulo 11 to the base 2 is 4.*

There is no known polynomial time algorithm for computing the discrete logarithm of $a \mod p$ to the base g when p, g, a are given. The problem plays a role in cryptography.

References

- Tom M. Apostol,
  Introduction to Analytical Number Theory, Springer, 1976.
- Owen D. Byer, Deirdre L. Smeltzer, and Kenneth L. Wantz,
  Journey into Discrete Mathematics, MAA Press, 2018.
- Gerard O'Regan,
  Guide to Discrete Mathematics: An Accessible Introduction to the History, Theory, Logic and Applications, Springer, 2016.
- Kenneth H. Rosen,
  Discrete Mathematics and Its Applications, McGraw-Hill, 2019.

The End

Thanks a lot for your attention!