

Number Theory

Chapter 4

Chapter Motivation

Number theory is the part of mathematics devoted to the study of the **integers** and their properties.

Key ideas in number theory concern

- divisibility and primality of integers
- representations of integers (e.g. binary and hexadecimal)

Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.

- Number theory is considered to be pure mathematics
- but it has important applications to computer science and cryptography

Divisibility and Modular Arithmetic

Section 4.1

Video 53: Division

- Division
- Properties of Division
- Division Algorithm

Division

Definition: If a and b are integers with $a \neq 0$, then a **divides** b if there exists an integer c such that $b = ac$. When a divides b we say that a is a **factor** or **divisor** of b and that b is a **multiple** of a .

Notations

- The notation $a \mid b$ denotes that a divides b .
- If a does not divide b , we write $a \nmid b$.
- If $a \mid b$, then $\frac{b}{a}$ is an integer.

Example: $3 \nmid 7$ and $3 \mid 12$

Properties of Divisibility

Theorem 1: Let a , b , and c be integers, where $a \neq 0$.

- i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
- ii. If $a \mid b$, then $a \mid bc$ for all integers c ;
- iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: Direct proof of (i)

Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence, $b + c = as + at = a(s + t)$.

Hence, $a \mid (b + c)$



Properties of Divisibility

Corollary: If a , b , and c be integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

Proof:

By part (ii) of Theorem 1 we see that $a \mid mb$ and $a \mid nc$ whenever m and n are integers.

By part (i) of Theorem 1 it follows that $a \mid mb + nc$.



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 it is in fact a theorem.

Division Algorithm (Theorem 2): If a is an integer and d a positive integer, then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$

Notation for Division

$$a = dq + r$$

d is called the **divisor**.

a is called the **dividend**.

q is called the **quotient**.

r is called the **remainder**.

We write

$$q = a \text{ div } d$$

$$r = a \text{ mod } d$$

div is a function:

mod is a function:

div: $\mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$

mod: $\mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$

Example

What are the quotient and remainder when 101 is divided by 11?

$$101 = 9 * 11 + 2$$

- the quotient is $101 \text{ div } 11 = 9$
- the remainder is $101 \text{ mod } 11 = 2$

What are the quotient and remainder when -11 is divided by 3?

$$-11 = -4 * 3 + 1$$

- the quotient is $-11 \text{ div } 3 = -4$
- the remainder is $-11 \text{ mod } 3 = 1$

Note: $0 \leq r < d$

Summary

- Division
- Divisibility under arithmetic operations
- Division Algorithm

Video 54: Congruence

- Congruences
- Properties of congruences

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then **a is congruent to b modulo m** if m divides $a - b$.

Notations

- The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m .
- We say that $a \equiv b \pmod{m}$ is a **congruence** and that m is its **modulus**.
- If a is not congruent to b modulo m , we write $a \not\equiv b \pmod{m}$

Example

Determine whether 17 is congruent to 5 modulo 6

$17 \equiv 5 \pmod{6}$ because 6 divides $17 - 5 = 12$.

Determine whether 24 and 14 are congruent modulo 6.

$24 \not\equiv 14 \pmod{6}$ since $24 - 14 = 10$ is not divisible by 6.

$(\bmod m)$ and $\bmod m$ Notations

The notations $a \equiv b \pmod{m}$ and $a \bmod m = b$ are different.

- $a \equiv b \pmod{m}$ is a *relation* on the set of integers.
- In $a \bmod m = b$, the notation **mod** denotes a *function*.


Theorem 3: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Corollary: Two integers are congruent **mod** m if and only if they have the same remainder when divided by m .

Theorem on Congruences

Theorem 4: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof:

- If $a \equiv b \pmod{m}$, then by definition of congruence $m \mid a - b$.
Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$.
Hence, $m \mid a - b$ and $a \equiv b \pmod{m}$. 

Congruences of Sums and Products

Theorem 5: Let m be a positive integer.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$,
then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Proof:

- Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers s and 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, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.



Example

Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$$

Algebraic Manipulation of Congruences

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

If $a \equiv b \pmod{m}$ then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer.

Proof: by Theorem 5 with $d = c$.

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

If $a \equiv b \pmod{m}$ then $c + a \equiv c + b \pmod{m}$, where c is any integer

Proof: by Theorem 5 with $d = c$.

Example

Since $14 \equiv 8 \pmod{6}$ also

$$28 \equiv 16 \pmod{6} \text{ and } 20 \equiv 14 \pmod{6}$$

Dividing both sides by 2 does not produce a valid congruence:

$$14/2 = 7 \text{ and } 8/2 = 4, \text{ but } 7 \not\equiv 4 \pmod{6}.$$

Dividing a congruence by an integer does not always produce a valid congruence!

Summary

- Definition of congruences
- **mod** m relation vs. **mod** function
- Congruences of arithmetic operations

Video 55: Modular Arithmetic

- Modular addition and multiplication
- Properties of modular arithmetic

$\text{mod } m$ Function of Products and Sums

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

$$(a + b) (\text{mod } m) = ((a \text{ mod } m) + (b \text{ mod } m)) \text{ mod } m$$

and

$$a \cdot b \text{ mod } m = ((a \text{ mod } m) \cdot (b \text{ mod } m)) \text{ mod } m.$$

Example: $280 \text{ mod } 6 = ((28 \text{ mod } 6) \cdot (10 \text{ mod } 6)) \text{ mod } 6 =$
 $= (4 \cdot 4) \text{ mod } 6 = 16 \text{ mod } 6 = 4$

Arithmetic Modulo m

Definitions: Let \mathbf{Z}_m be the set of nonnegative integers less than m :

$$\mathbf{Z}_m = \{0, 1, \dots, m - 1\}$$

The **addition modulo m** operation $+_m$ is defined as

$$a +_m b = (a + b) \bmod m.$$

The **multiplication modulo m** operation \cdot_m is defined as

$$a \cdot_m b = (a \cdot b) \bmod m.$$

Using these operations is said to be doing **arithmetic modulo m** .

Example

Computing $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Using the definitions:

$$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$$

$$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$$

Arithmetic Modulo m

The operations $+_m$ and \cdot_m satisfy many of the properties as ordinary addition and multiplication.

- **Closure:** If a and b belong to \mathbf{Z}_m , then $a +_m b$ and $a \cdot_m b$ belong to \mathbf{Z}_m .
- **Commutativity:** If a and b belong to \mathbf{Z}_m , then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- **Associativity:** If a , b , and c belong to \mathbf{Z}_m , then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
- **Distributivity:** If a , b , and c belong to \mathbf{Z}_m , then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Arithmetic Modulo m

The operations $+_m$ and \cdot_m satisfy many of the properties as ordinary addition and multiplication.

- **Identity elements:** The elements 0 and 1 are identity elements for addition and multiplication modulo m , respectively.
 - If a belongs to \mathbf{Z}_m , then $a +_m 0 = a$ and $a \cdot_m 1 = a$.
- **Additive inverses:** If $a \neq 0$ belongs to \mathbf{Z}_m , then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse:
 - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$

Commutative Ring

Multiplicative inverses have not been included since they do not always exist.

Example: There is no multiplicative inverse of 2 modulo 6.

In the terminology of abstract algebra:

\mathbf{Z}_m with $+_m$ is a **commutative group**

\mathbf{Z}_m with $+_m$ and \cdot_m is a **commutative ring**.

Summary

- Modular addition and multiplication
- Commutative Ring

Integer Representations and Algorithms

Section 4.2

Video 56: Integer Representation

- Base b representation of Integers

Representations of Integers

In general, we use *decimal*, or *base 10 notation* to represent integers.

Example: when we write 965, we mean $9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$.

We can represent numbers using any base b , where b is a positive integer greater than 1.

- The ancient Mayans used base 20 and the ancient Babylonians used base 60.
- The bases $b = 2$ (*binary*), $b = 8$ (*octal*), and $b = 16$ (*hexadecimal*) are important for computing and communications.

Base b Representations

Theorem 1: Let b be a positive integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form:

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

where k is a nonnegative integer, a_0, a_1, \dots, a_k are nonnegative integers less than b , and $a_k \neq 0$. The $a_j, j = 0, \dots, k$ are called the base- b digits of the representation.

- The representation of n given in Theorem 1 is called the *base b expansion of n* and is denoted by $(a_k a_{k-1} \dots a_1 a_0)_b$.
- We usually omit the subscript 10 for base 10 expansions.

Binary Expansions

Most computers represent integers and do arithmetic with binary (base 2) expansions of integers.

In these expansions, the only digits used are 0 and 1.

Example: Decimal expansion of the number with binary expansion $(1\ 0101\ 1111)_2$

$$\begin{aligned}(1\ 0101\ 1111)_2 &= \\ &1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = \\ &351\end{aligned}$$

Octal Expansions

The octal expansion (base 8) uses the digits {0, 1, 2, 3, 4, 5, 6, 7}.

Example: Decimal expansion of the number with octal expansion $(7016)_8$

$$(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$$

Hexadecimal Expansions

The hexadecimal expansion needs 16 digits.

The hexadecimal system uses the digits $\{0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F\}$.

The letters A through F represent the decimal numbers 10 through 15.

Decimal expansion of the number with hexadecimal expansion
 $(2AE0B)_{16}$?

$$(2AE0B)_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627$$

Base b Expansion Algorithm

```
procedure base_b_expansion( $n, b$ : positive integers with  $b > 1$ )  
   $q := n$   
   $k := 0$   
  while ( $q \neq 0$ )  
     $a_k := q \bmod b$   
     $q := q \operatorname{div} b$   
     $k := k + 1$   
  return( $a_{k-1}, \dots, a_1, a_0$ )  
   $\{(a_{k-1} \dots a_1 a_0)_b$  is base  $b$  expansion of  $n\}$ 
```

The digits in the base b expansion are the remainders of the division given by $q \bmod b$.

Example

Find the octal expansion of $(12345)_{10}$

Successively dividing by 8 gives:

$$12345 = 8 \cdot 1543 + 1$$

$$1543 = 8 \cdot 192 + 7$$

$$192 = 8 \cdot 24 + 0$$

$$24 = 8 \cdot 3 + 0$$

$$3 = 8 \cdot 0 + 3$$

The remainders are the digits from right to left yielding $(30071)_8$.

Comparison of Hexadecimal, Octal, and Binary Representations

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.																
Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Initial 0s are not shown

Each octal digit corresponds to a block of 3 binary digits.

Each hexadecimal digit corresponds to a block of 4 binary digits.

Conversion Between Binary, Octal, and Hexadecimal Expansions

Find the octal and hexadecimal expansions of $(11\ 1110\ 1011\ 1100)_2$.

- To convert to octal, we group the digits into blocks of three adding initial 0s as needed.

$(011\ 111\ 010\ 111\ 100)_2$,

The blocks from left to right correspond to the digits 3, 7, 2, 7, and 4. Hence, the expansion is $(37274)_8$.

- To convert to hexadecimal, we group the digits into blocks of four adding initial 0s as needed.

$(0011\ 1110\ 1011\ 1100)_2$,

The blocks from left to right correspond to the digits 3, E, B, and C. Hence, the expansion is $(3EBC)_{16}$.

Summary

- Binary, Octal, and Hexadecimal Expansions
- Computing an expansion
- Converting among expansions

Video 57: Arithmetic with Base 2 Expansions

- Addition
- Multiplication
- Modular Exponentiation

Binary Addition of Integers

```
procedure add(a, b: positive integers)
{the binary expansions of a and b are  $(a_{n-1}, a_{n-2}, \dots, a_0)_2$  and  $(b_{n-1}, b_{n-2}, \dots, b_0)_2$ , respectively}
c := 0
for j := 0 to n - 1
    d :=  $\lfloor (a_j + b_j + c)/2 \rfloor$ 
    sj :=  $a_j + b_j + c - 2d$ 
    c := d
sn := c
return(s0, s1, ..., sn)
{the binary expansion of the sum is  $(s_n, s_{n-1}, \dots, s_0)_2$ }
```

The number of additions of bits used by the algorithm to add two n -bit integers is $O(n)$.

Example

Adding $a = (1110)_2$ and $b = (1011)_2$.

First $a_0 + b_0 = 0 + 1$

So $d = 0$, $s_0 = a_0 + b_0 - 2d = 1$ and $c = 0$

Next $a_1 + b_1 + c = 1 + 1 + 0 = 2$

So $d = 1$, $s_1 = 0$ and $c = 1$

Next $a_2 + b_2 + c = 1 + 0 + 1 = 2$

So $d = 1$, $s_2 = 0$ and $c = 1$

Finally $a_3 + b_3 + c = 1 + 1 + 1 = 3$

So $d = 1$, $s_3 = 1$ and $c = 1$

Then $s_4 = c = 1$ and the result is $(1\ 1001)_2$

Binary Multiplication

Two observations

$$a \cdot b = a \cdot (b_k 2^k + b_{k-1} 2^{k-1} + \dots + b_1 2 + b_0) = ab_k 2^k + ab_{k-1} 2^{k-1} + \dots + ab_1 2^1 + ab_0 2^0$$

Multiplying a binary number by 2^j corresponds to add j zeros at the end

Example: Multiply $a = (110)_2$ and $b = (101)_2$

$$ab_0 2^0 = (110)_2 \cdot 1 \cdot 2^0 = (110)_2 \cdot 2^0 = (110)_2$$

$$ab_1 2^1 = (110)_2 \cdot 0 \cdot 2^1 = (000)_2 \cdot 2^1 = (0000)_2$$

$$ab_2 2^2 = (110)_2 \cdot 1 \cdot 2^2 = (110)_2 \cdot 2^2 = (11000)_2$$

$$\text{finally compute the sum } (110)_2 + (0000)_2 + (11000)_2 = (11110)_2$$

Binary Multiplication of Integers

```
procedure multiply(a, b: positive integers)
{the binary expansions of a and b are  $(a_{n-1}, a_{n-2}, \dots, a_0)_2$  and  $(b_{n-1}, b_{n-2}, \dots, b_0)_2$ , respectively}
for j := 0 to n - 1
    if  $b_j = 1$  then  $c_j = a$  with j zeros appended
    else  $c_j := 0$ 
{ $c_0, c_1, \dots, c_{n-1}$  are the partial products}
p := 0
for j := 0 to n - 1
    p := p +  $c_j$ 
return p
```

The number of additions of bits used by the algorithm to multiply two n -bit integers is $O(n^2)$.

Binary Modular Exponentiation

In cryptography, it is important to be able to find $b^n \bmod m$ efficiently, where b , n , and m are large integers.

- Use the binary expansion of n , $n = (a_{k-1}, \dots, a_1, a_0)_2$, to compute b^n .

Note that:

$$b^n = b^{a_{k-1} \cdot 2^{k-1} + \dots + a_1 \cdot 2 + a_0} = b^{a_{k-1} \cdot 2^{k-1}} \dots b^{a_1 \cdot 2} \cdot b^{a_0}.$$

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

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

- and then multiply the terms b^{2^j} in this list, for all $a_j = 1$.

Example

Example: Compute 3^{11} using this method.

Note that $11 = (1011)_2$ so that $3^{11} = 3^8 3^2 3^1 =$

$$((3^2)^2)^2 3^2 3^1 = (9^2)^2 \cdot 9 \cdot 3 = (81)^2 \cdot 9 \cdot 3 = 6561 \cdot 9 \cdot 3 = 117,147.$$

Binary Modular Exponentiation Algorithm

The algorithm successively finds

$$b \bmod m, b^2 \bmod m, b^4 \bmod m, \dots, b^{2^{k-1}} \bmod m,$$

and multiplies together the terms b^{2^j} where $a_j = 1$.

```
procedure modular_exponentiation(b: integer,  $n = (a_{k-1}a_{k-2}\dots a_1a_0)_2$ , m: positive integers)
  x := 1
  power := b mod m
  for i := 0 to k - 1
    if  $a_i = 1$  then x := (x · power) mod m
    power := (power · power) mod m
  return x
```

$O((\log m)^2 \log n)$ bit operations are used to find $b^n \bmod m$.

Summary

- Binary Addition and Multiplication
 - Complexity $O(n)$ and $O(n^2)$
- Binary Modular Exponentiation

Primes and Greatest Common Divisors

Section 4.3

Video 58: Primes

- Primes
- Basic Theorems on Primes

Primes

Definition: A positive integer p greater than 1 is called **prime** if the only positive factors of p are 1 and p . A positive integer that is greater than 1 and is not prime is called **composite**.

Example:

The integer 7 is prime because its only positive factors are 1 and 7

The integer 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: If n is an integer greater than 1, then n can be written as the product of primes.

Examples:

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$$

$$641 = 641$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$$

$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$$

Proof of Fundamental Theorem of Arithmetic

Proof: (strong induction) Let $P(n)$ be the proposition that n can be written as a product of primes.

- BASIS STEP: $P(2)$ is true since 2 itself is prime.
- INDUCTIVE STEP: The inductive hypothesis is $P(j)$ is true for all integers j with $2 \leq j \leq k$. To show that $P(k + 1)$ must be true under this assumption, two cases need to be considered:
 - If $k + 1$ is prime, then $P(k + 1)$ is true.
 - Otherwise, $k + 1$ is composite and can be written as the product of two positive integers a and b with $2 \leq a \leq b < k + 1$. By the inductive hypothesis a and b can be written as the product of primes and therefore $k + 1$ can also be written as the product of those primes.

Hence, it has been shown that every integer greater than 1 can be written as the product of primes. 

Trial Division

Theorem: If n is a composite integer, then n has a prime divisor less than or equal to \sqrt{n} .

Proof:

If n is composite it can be written as $n = ab$.

Either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$: if this is not the case, i.e. $a > \sqrt{n}$ and $b > \sqrt{n}$, $ab > n$, which is a contradiction.

W.l.o.g. assume $a \leq \sqrt{n}$.

Then either a is prime, or a has a prime factor that is smaller than \sqrt{n} .

In either case the theorem follows.





Eratosthenes
(276-194 B.C.)

The Sieve of Eratosthenes

The *Sieve of Eratosthenes* can be used to find all primes not exceeding a specified positive integer.

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

- Delete all the integers, other than 2, divisible by 2.
- Delete all the integers, other than 3, divisible by 3.
- Next, delete all the integers, other than 5, divisible by 5.
- Next, delete all the integers, other than 7, divisible by 7.
- 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 Eratosthenes

TABLE 1 The Sieve of Eratosthenes.

<i>Integers divisible by 2 other than 2 receive an underline.</i>										<i>Integers divisible by 3 other than 3 receive an underline.</i>									
1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	9	<u>10</u>	1	2	3	<u>4</u>	5	<u>6</u>	7	8	<u>9</u>	<u>10</u>
11	<u>12</u>	13	<u>14</u>	15	<u>16</u>	17	<u>18</u>	19	<u>20</u>	11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
21	<u>22</u>	23	<u>24</u>	25	<u>26</u>	27	<u>28</u>	29	<u>30</u>	21	<u>22</u>	23	<u>24</u>	25	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>
31	<u>32</u>	33	<u>34</u>	35	<u>36</u>	37	<u>38</u>	39	<u>40</u>	31	<u>32</u>	<u>33</u>	<u>34</u>	35	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>
41	<u>42</u>	43	<u>44</u>	45	<u>46</u>	47	<u>48</u>	49	<u>50</u>	41	<u>42</u>	43	<u>44</u>	45	<u>46</u>	47	<u>48</u>	49	<u>50</u>
51	<u>52</u>	53	<u>54</u>	55	<u>56</u>	57	<u>58</u>	59	<u>60</u>	51	<u>52</u>	53	<u>54</u>	55	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>
61	<u>62</u>	63	<u>64</u>	65	<u>66</u>	67	<u>68</u>	69	<u>70</u>	61	<u>62</u>	<u>63</u>	<u>64</u>	65	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>
71	<u>72</u>	73	<u>74</u>	75	<u>76</u>	77	<u>78</u>	79	<u>80</u>	71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u>78</u>	79	<u>80</u>
81	<u>82</u>	83	<u>84</u>	85	<u>86</u>	87	<u>88</u>	89	<u>90</u>	81	<u>82</u>	83	<u>84</u>	85	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>
91	<u>92</u>	93	<u>94</u>	95	<u>96</u>	97	<u>98</u>	99	<u>100</u>	91	<u>92</u>	<u>93</u>	<u>94</u>	95	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>
<i>Integers divisible by 5 other than 5 receive an underline.</i>										<i>Integers divisible by 7 other than 7 receive an underline; integers in color are prime.</i>									
1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	<u>9</u>	<u>10</u>	1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	<u>9</u>	<u>10</u>
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>	11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
21	<u>22</u>	23	<u>24</u>	<u>25</u>	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>	21	<u>22</u>	23	<u>24</u>	25	<u>26</u>	<u>27</u>	<u>28</u>	29	<u>30</u>
31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>	31	<u>32</u>	<u>33</u>	<u>34</u>	<u>35</u>	<u>36</u>	37	<u>38</u>	<u>39</u>	<u>40</u>
41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</u>	41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</u>
51	<u>52</u>	53	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>	51	<u>52</u>	53	<u>54</u>	55	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>
61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>	61	<u>62</u>	<u>63</u>	<u>64</u>	<u>65</u>	<u>66</u>	67	<u>68</u>	<u>69</u>	<u>70</u>
71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u>78</u>	79	<u>80</u>	71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	<u>77</u>	<u>78</u>	79	<u>80</u>
81	<u>82</u>	83	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>	81	<u>82</u>	83	<u>84</u>	85	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>
91	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>	91	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>



Euclid

(325 B.C.E. – 265 B.C.E.)

Infinitude of Primes

Theorem: There are infinitely many primes (Euclid).

Proof: Assume finitely many primes: p_1, p_2, \dots, p_n

- Let $q = p_1 p_2 \cdots p_n + 1$
- Either q is prime or by the fundamental theorem of arithmetic it is a product of primes.
 - None of the primes p_j divides q since
if $p_j \mid q$, then p_j divides $q - p_1 p_2 \cdots p_n = 1$.
 - Hence, there is a prime not on the list p_1, p_2, \dots, p_n .
 - It is either q , or if q is composite, it is a prime factor of q .
 - This contradicts the assumption that p_1, p_2, \dots, p_n are all the primes.
- Consequently, there are infinitely many primes. ◀

Summary

- Primes
- Basic Theorems on Primes
 - Fundamental Theorem of Arithmetic
 - Trial Division
- Sieve of Erastosthenes
- Euclid's Theorem

Video 59: GCD and LCM

- Greatest common divisor
- Least common Multiple

Greatest Common Divisor

Definition: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the **greatest common divisor** of a and b .

The greatest common divisor of a and b is denoted by **$\gcd(a, b)$** .

Example:

$$\gcd(24, 36) = 12$$

$$\gcd(17, 22) = 1$$

$$\gcd(17, 0) = 17$$

Relatively Prime

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

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

Examples

17 and 22 are relatively prime

The integers 10, 17 and 21 are pairwise relatively prime.

$$\gcd(10, 17) = 1$$

$$\gcd(10, 21) = 1$$

$$\gcd(17, 21) = 1$$

The integers 10, 19, and 24 are not pairwise relatively prime.

$$\gcd(10, 24) = 2$$

Finding the Greatest Common Divisor

Suppose the prime factorizations of a and b are:

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

where each exponent is a nonnegative integer. Then:

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

- 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.

Example

$$120 = 2^3 \cdot 3 \cdot 5 = 2^3 \cdot 3^1 \cdot 5^1$$

$$500 = 2^2 \cdot 5^3 = 2^2 \cdot 3^0 \cdot 5^3$$

Then

$$\gcd(120, 500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

Least Common Multiple

Definition: The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b . It is denoted by **$\text{lcm}(a, b)$** .

The least common multiple can also be computed from the prime factorizations.

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

Example: $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$

Theorem: Let a and b be positive integers. Then $ab = \text{gcd}(a, b) \cdot \text{lcm}(a, b)$

Euclidean Algorithm

The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers.

It is based on the idea that $\gcd(a, b)$ is equal to $\gcd(r, b)$ when $a > b$ and r is the remainder when a is divided by b .

Example:

Find $\gcd(91, 287)$:

$$287 = 91 \cdot 3 + 14, \text{ therefore } \gcd(287, 91) = \gcd(14, 91) = \gcd(91, 14)$$


$$91 = 14 \cdot 6 + 7, \text{ therefore } \gcd(91, 14) = \gcd(7, 14) = \gcd(14, 7)$$

$$14 = 7 \cdot 2 + 0, \text{ therefore } \gcd(14, 7) = 7$$

Correctness of Euclidean Algorithm

Lemma 1: Let $a = bq + r$, where a , b , q , and r are integers.
Then $\gcd(a, b) = \gcd(b, r)$.

Proof:

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

Euclidean Algorithm

```
procedure gcd(a, b: positive integers,  $a > b$ )  
x := a  
y := b  
while  $y \neq 0$   
    r := x mod y  
    x := y  
    y := r  
return x
```

```
procedure gcd(a, b: positive integers,  $a > b$ )  
if  $b = 0$  then return a  
    else return gcd(b, a mod b)
```

Correctness of Euclidean Algorithm

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$.

Successive applications of the division algorithm yields:

$$\begin{aligned} r_0 &= r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\ &\vdots \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n. \end{aligned}$$

Eventually, a remainder of zero occurs in the sequence of terms: $a = r_0 > r_1 > r_2 > \cdots \geq 0$. The sequence can't contain more than a terms.

By Lemma 1 $\gcd(a, b) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$.

Hence the greatest common divisor is the last nonzero remainder in the sequence of divisions.

Complexity of Euclidean Algorithm

Theorem (Lamé's theorem): Let a and b be positive integers with $a \geq b$. Then the number of divisions used by the Euclidean algorithm to find $\gcd(a, b)$ is less than or equal to five times the number of decimal digits in b .

Therefore the Euclidean algorithm has complexity $O(\log b)$.

Summary

- Greatest common divisor
- Least common Multiple
- Euclidean Algorithm

Video 60: More Facts about Primes

- Important facts about Primes
- Finding large Primes
- Open problems on Primes

Uniqueness of Prime Factorization

Theorem: If p is a positive integer then its factorization into primes of non-decreasing order is unique.

Distribution of Primes

Definition: $\pi(x)$ denotes the number of primes not exceeding x .

Prime Number Theorem: The ratio $\frac{\pi(x)}{\frac{x}{\ln(x)}}$ approaches 1 as x grows without bound.

- The odds that a randomly selected positive integer less than n is prime are approximately $\frac{1}{\ln(n)}$.

Primes and Arithmetic Progressions

Are there long arithmetic progressions made up entirely of primes?

- 5, 11, 17, 23, 29 is an arithmetic progression of five primes.
- 199, 409, 619, 829, 1039, 1249, 1459, 1669, 1879, 2089 is an arithmetic progression of ten primes.
- In the 1930s, Paul Erdős conjectured that for every positive integer n greater than 1, there is an arithmetic progression of length n made up entirely of primes.
- This was proven in 2006, by Ben Green and Terence Tao.

Mersene Primes

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

Examples

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

$2^{11} - 1 = 2047$ is not a Mersene prime since $2047 = 23 \cdot 89$.

There is an efficient test for determining if $2^p - 1$ is prime.

- The largest known prime numbers are Mersene primes.
- As of mid 2018, the largest is $2^{82,589,933} - 1$, which has nearly 25 million decimal digits.
- The *Great Internet Mersene Prime Search* (GIMPS) is a distributed computing project to search for new Mersene Primes. <http://www.mersenne.org/>

Conjectures

Goldbach's Conjecture: Every even integer n , $n > 2$, is the sum of two primes.

- It has been verified by computer for all positive even integers up to $1.6 \cdot 10^{18}$.
- The conjecture is believed to be true by most mathematicians.

The Twin Prime Conjecture: There are infinitely many pairs of twin primes. Twin primes are pairs of primes that differ by 2.

- Examples are 3 and 5, 5 and 7, 11 and 13, etc.
- The current world's record for twin primes (as of 2018) consists of numbers $2996863034895 \cdot 2^{1290000} \pm 1$, which have 388,342 decimal digits.

Summary

- Uniqueness of Prime Factorization
- Distribution of Primes
- Primes and Arithmetic Progressions
- Mersene Primes
- Goldbach's Conjecture
- The Twin Prime Conjecture