

Discrete Structure

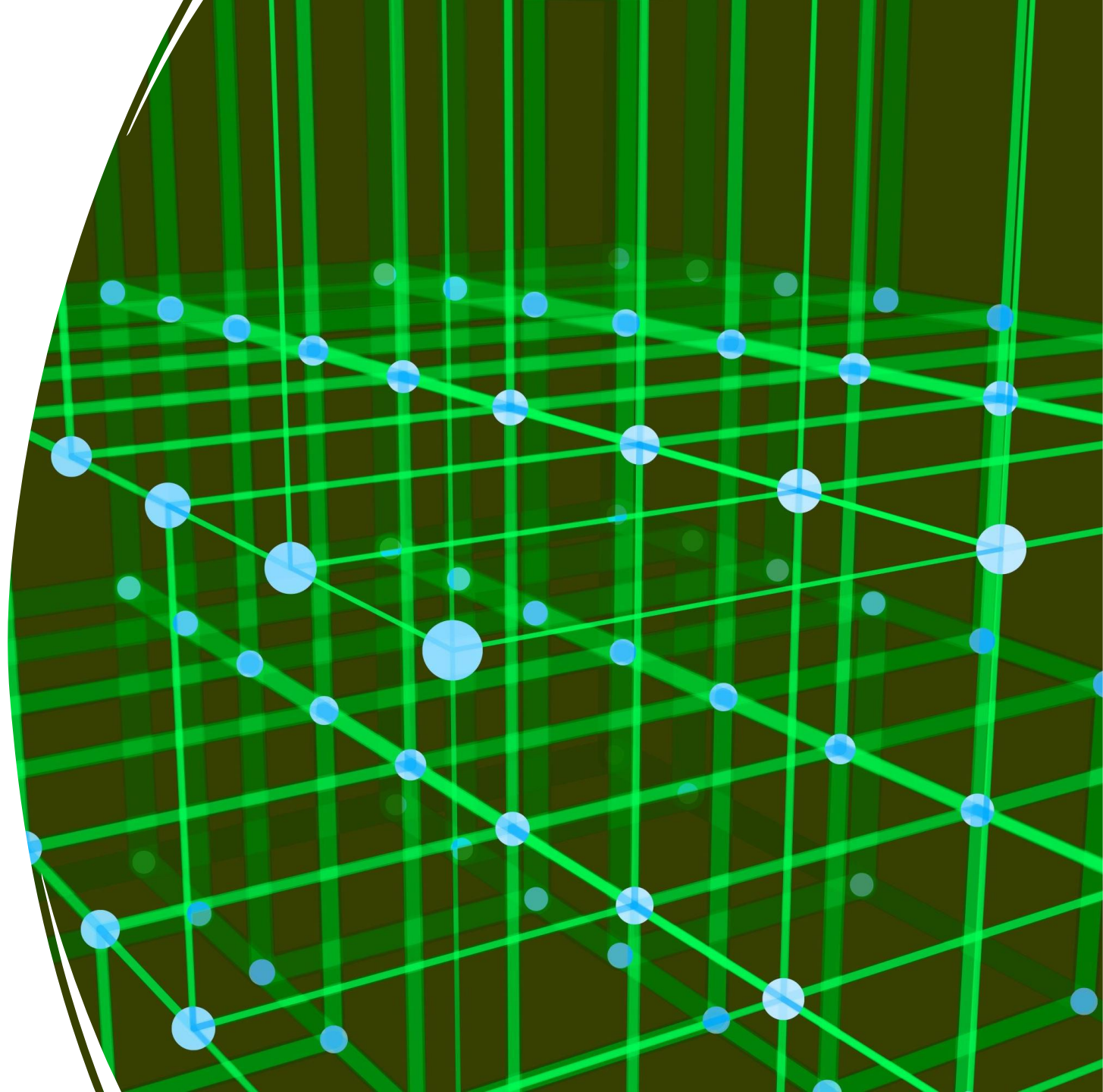
Chapter:2

Number Theory

Prepared by :

Kul Prasad Paudel

*Note: This slides is only for theory
containing definition and theorem. More
numerical will be practice in classes*



Divisibility and Modular Arithmetic

Division

When one integer is divided by a second nonzero integer, the quotient may or may not be


an integer. For example, $12/3 = 4$ is an integer, whereas $11/4 = 2.75$ is not

DEFINITION 1


If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. 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 . We write $a \nmid b$ when a does not divide b .

Remark: We can express $a \mid b$ using quantifiers as $\exists c(ac = b)$, where the universe of discourse is the set of integers.

EXAMPLE 1 Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution: We see that $3 \nmid 7$, because $7/3$ is not an integer. On the other hand, $3 \mid 12$ because $12/3 = 4$. 

EXAMPLE 2 Let n and d be positive integers. How many positive integers not exceeding n are divisible by d ?

Solution: The positive integers divisible by d are all the integers of the form dk , where k is a positive integer. Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < dk \leq n$, or with $0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d . 



Theorem 1

Let a , b , and c be integers, where $a \neq 0$ Then

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 $a \mid c$

The Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder, as the division algorithm shows.

THEOREM 2 **THE DIVISION ALGORITHM** Let a be an integer and d a positive integer. Then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$.

DEFINITION 2 In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*. This notation is used to express the quotient and remainder:

$$q = a \operatorname{div} d, \quad r = a \operatorname{mod} d.$$

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

Solution: We have

$$101 = 11 \times 9 + 2$$

Hence, the quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is

$$2 = 101 \text{ mod } 11$$

Practice

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

Find the quotient and remainder when 133 is divisible by 4

Exercise

What are the quotient and remainder when

- a) 19 is divided by 7?
- b) -111 is divided by 11?
- c) 789 is divided by 23?
- d) 1001 is divided by 13?
- e) 0 is divided by 19?
- f) 3 is divided by 5?
- g) -1 is divided by 3?
- h) 4 is divided by 1?

What time does a 24-hour clock read

- a) 100 hours after it reads 2:00?
- b) 45 hours before it reads 12:00?
- c) 168 hours after it reads 19:00?

What time does a 12-hour clock read

- a) 80 hours after it reads 11:00?
- b) 40 hours before it reads 12:00?
- c) 100 hours after it reads 6:00?

1X Show that if a , b , c , and d are integers, where $a \neq 0$, such that $a \mid c$ and $b \mid d$, then $ab \mid cd$.

2X Show that if a , b , and c are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$.

Modular Arithmetic

In some situations, we care only about the remainder of an integer when it is divided by some specified positive integer. For instance, when we ask what time it will be (on a 24-hour clock) 50 hours from now, we care only about the remainder when 50 plus the current hour is divided by 24. Because we are often interested only in remainders, we have special notations for them.

Definition 3:

If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate 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** (plural **moduli**). If a and b are not congruent modulo m , we write $a \not\equiv b \pmod{m}$.

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 $a \bmod m = b \bmod m$.

Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod{6}$

However, because

$24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$

Evaluate these quantities

- a) $-17 \bmod 2$
- b) $144 \bmod 7$
- c) $101 \bmod 13$
- d) $199 \bmod 19$
- e) $13 \bmod 3$
- f) $-97 \bmod 11$
- g) $155 \bmod 19$
- h) $-221 \bmod 23$

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 $a \equiv b \pmod{m}$, by the definition of congruence (Definition 3), we know that

$$m \mid (a - b)$$

This means that there is an integer k such that $a - b = km$, so that $a = b + km$

Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, m divides $a - b$, so that $a \equiv b \pmod{m}$

THEOREM 5

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

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

Evaluate the following as congruent or not.

$$7 \equiv 2 \pmod{5} \text{ and } 11 \equiv 1 \pmod{5}$$

Find counterexamples to each of these statements about congruences.

a) If $ac \equiv bc \pmod{m}$, where a, b, c , and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$

b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d , and m are integers with c and d positive and $m \geq 2$, then $ac \equiv bd \pmod{m}$

Arithmetic Modulo m

We can define arithmetic operations on \mathbb{Z}_m , the set of nonnegative integers less than m , that is, the set $\{0, 1, \dots, m-1\}$. In particular, we define addition of these integers, denoted by $+_m$ by

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

where the addition on the right-hand side of this equation is the ordinary addition of integers, and we define multiplication of these integers, denoted by \cdot_m by

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

where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers. The operations $+_m$ and \cdot_m are called addition and multiplication modulo m and when we use these operations, we are said to be doing **arithmetic modulo m** .

Arithmetic Modulo m

Exercise

- i. Use the definition of addition and multiplication in Z_m to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.*
- ii. Write out the addition and multiplication tables for Z_5 (by addition and multiplication we mean $+_5$ and \cdot_5).*
- iii. Write out the addition and multiplication tables for Z_6 (by addition and multiplication we mean $+_6$ and \cdot_6).*

The operations $+_m$ and \cdot_m satisfy many of the same properties of ordinary addition and multiplication of integers. In particular, they satisfy these properties:

Closure If a and b belong to \mathbf{Z}_m , then $a +_m b$ and $a \cdot_m b$ belong to \mathbf{Z}_m .

Associativity If a , b , and c belong to \mathbf{Z}_m , then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

Commutativity If a and b belong to \mathbf{Z}_m , then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

Identity elements The elements 0 and 1 are identity elements for addition and multiplication modulo m , respectively. That is, if a belongs to \mathbf{Z}_m , then $a +_m 0 = 0 +_m a = a$ and $a \cdot_m 1 = 1 \cdot_m a = a$.

Additive inverses If $a \neq 0$ belongs to \mathbf{Z}_m , then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.

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 $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

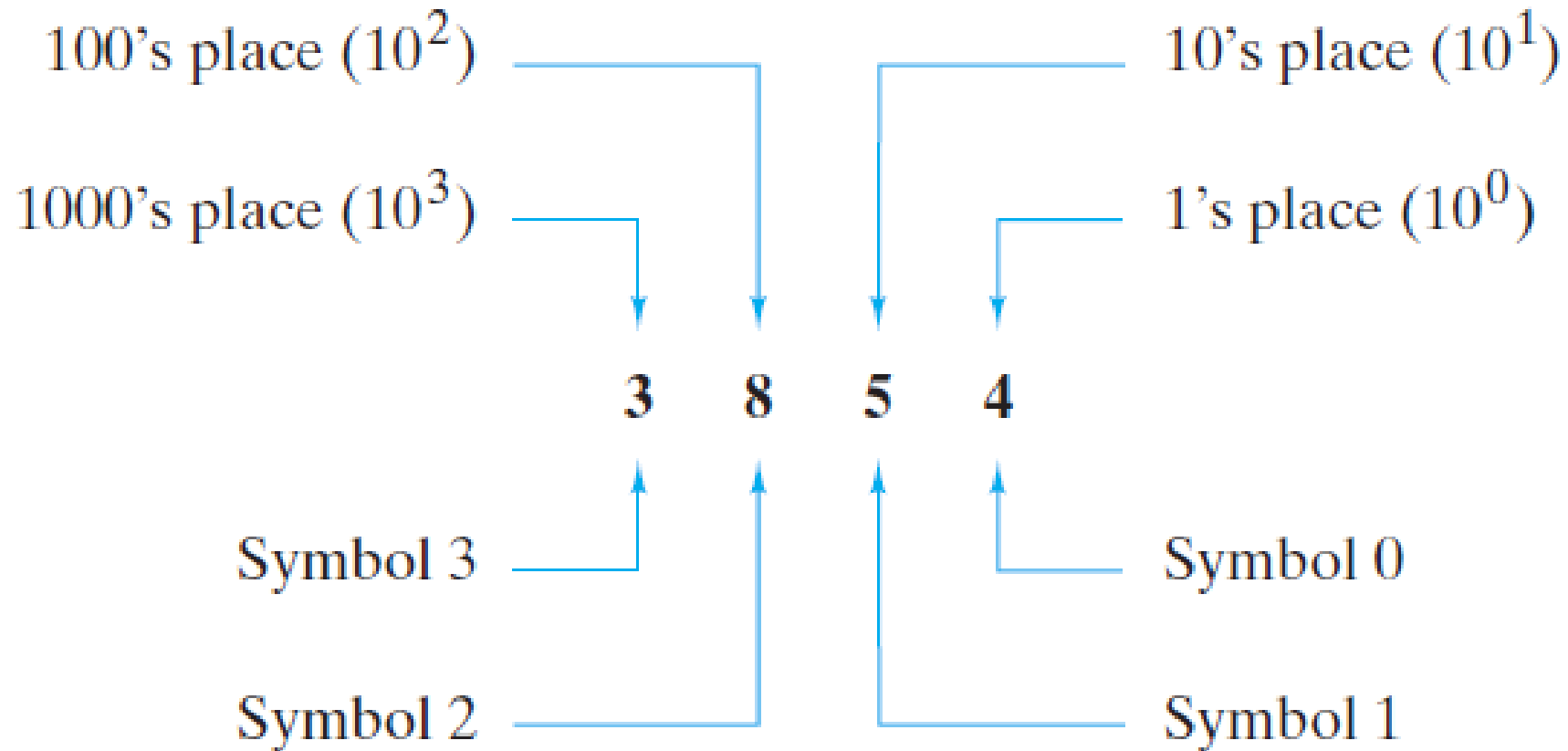
Integer Representations and Algorithms

- A **bit** is a *binary digit*, that is, a 0 or a 1
- The term *digital* refers to the use of the digits 0 and 1
- The **octal number system**, which represents integers using eight symbols,
- In the decimal number system, to represent integers we use the 10 symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9
- In representing an integer, the symbol's position is significant; reading from the right, the first symbol represents the number of 1's, the next symbol the number of 10's, the next symbol the number of 100's, and so on

➤ Example

$$3854 = 3 \cdot 10^3 + 8 \cdot 10^2 + 5 \cdot 10^1 + 4 \cdot 10^0$$

Integer Representations and Algorithms

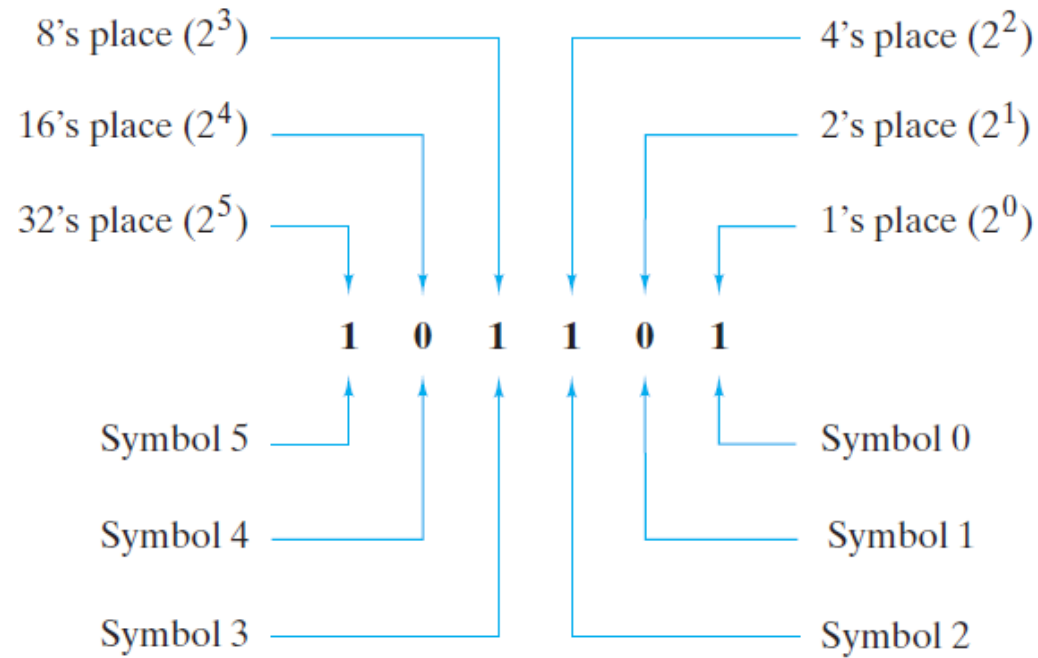


The Decimal number system

Integer Representations and Algorithms

In the binary (base 2) number system, to represent integers we need only two symbols, 0 and 1

In Base 2: $101101_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$



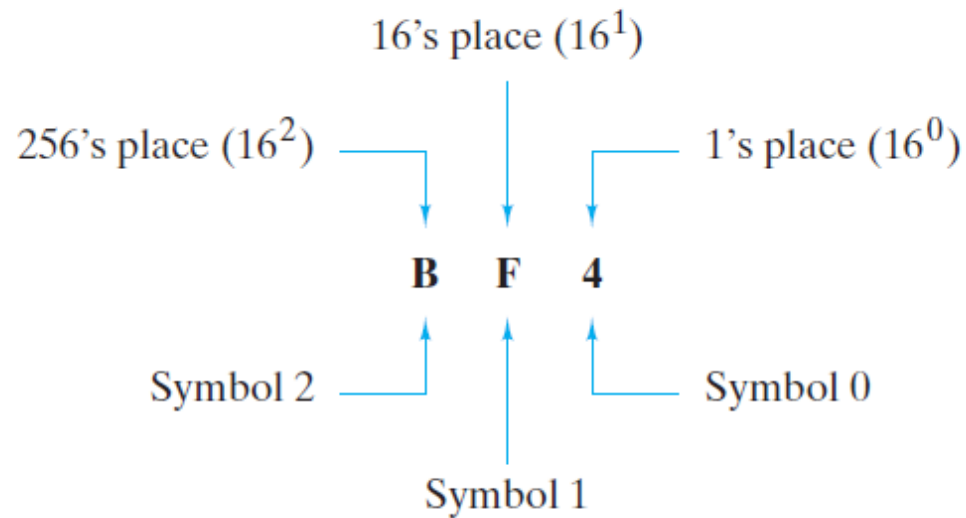
The Binary number system

Integer Representations and Algorithms

In the hexadecimal number system, to represent integers we use the symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F

The symbols A–F are interpreted as decimal 10–15

$$\text{B4F} = 11 \cdot 16^2 + 4 \cdot 16^1 + 15 \cdot 16^0$$



The Hexadecimal number system

Prime and Composite

- An integer greater than 1 whose only positive divisors are itself and 1 is called ***prime*** An integer greater than 1 that is not prime is called ***composite***
- The integer 23 is prime because its only divisors are itself and 1X The integer 34 is composite because it is divisible by 17, which is neither 1 nor 34

A positive integer n greater than 1 is composite if and only if n has a divisor d satisfying $2 \leq d \leq \sqrt{n}$.

Primes and Greatest Common Divisors

- Every integer greater than 1 is divisible by at least two integers, because a positive integer is divisible by 1 and by itself. Positive integers that have exactly two different positive integer factors are called **primes**.

DEFINITION 1

An 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*.

Remark: The integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$.

Determine whether each of these integers is prime

a) 21 b) 29

c) 71 d) 97

e) 111 f) 143

Find the prime factorization of each of these integers

a) 88 b) 126 c) 729

d) 1001 e) 1111 f) 909,090

Greatest Common Divisor

The largest integer that divides both of two integers is called the **greatest common divisor** of these integers.

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b . The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

What is the greatest common divisor of 24 and 36?

The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12X Hence, $\gcd(24, 36) = 12$ X

What is the greatest common divisor of 17 and 22?

The integers 17 and 22 have no positive common divisors other than 1, so that $\gcd(17, 22) = 1$ X

The integers a and b are *relatively prime* if their greatest common divisor is 1.

Greatest Common Divisor

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

Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Because $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, and $\gcd(17, 21) = 1$, we conclude that 10, 17, and 21 are pairwise relatively prime.

Because $\gcd(10, 24) = 2 > 1$, we see that 10, 19, and 24 are not pairwise relatively prime.

Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers 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, and where all primes occurring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then $\gcd(a, b)$ is given by

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

Find GCD of 120 and 500 using prime factorization

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

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

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

Prime factorizations can also be used to find the **least common multiple** of two integers.

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

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

What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

Solution: We have

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

THEOREM 5

Let a and b be positive integers. Then

$$ab = \text{gcd}(a, b) \cdot \text{lcm}(a, b).$$

Exercise

Which positive integers less than 12 are relatively prime to 12?

Which positive integers less than 30 are relatively prime to 30?

Determine whether the integers in each of these sets are pairwise relatively prime.

- a) 21, 34, 55 b) 14, 17, 85
- c) 25, 41, 49, 64 d) 17, 18, 19, 23

Determine whether the integers in each of these sets are pairwise relatively prime.

- a) 11, 15, 19 b) 14, 15, 21
- c) 12, 17, 31, 37 d) 7, 8, 9, 11

We call a positive integer **perfect** if it equals the sum of its positive divisors other than itself.

- a) Show that 6 and 28 are perfect.
- b) Show that $2^{p-1}(2^p - 1)$ is a perfect number when $2^p - 1$ is prime.

What are the greatest common divisors of these pairs of integers?

- a) $2^2 \cdot 3^3 \cdot 5^5, 2^5 \cdot 3^3 \cdot 5^2$
- b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$
- c) 17, 17^{17} d) $2^2 \cdot 7, 5^3 \cdot 13$
- e) 0, 5 f) $2 \cdot 3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5 \cdot 7$

If the product of two integers is $2^7 3^8 5^2 7^{11}$ and their greatest common divisor is $2^3 3^4 5$, what is their least common multiple?

Euclidian Algorithm

Computing the greatest common divisor of two integers directly from the prime factorizations of these integers is inefficient. The reason is that it is time-consuming to find prime factorizations. We will give a more efficient method of finding the greatest common divisor, called the **Euclidean algorithm**.

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

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

$$662 = 414 \cdot 1 + 248$$

$$414 = 248 \cdot 1 + 166$$

$$248 = 166 \cdot 1 + 82$$

$$166 = 82 \cdot 2 + 2$$

$$82 = 2 \cdot 41.$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

Exercise

Use the Euclidean algorithm to find

- | | |
|--------------------------|----------------------------|
| a) $\gcd(1, 5)$. | b) $\gcd(100, 101)$. |
| c) $\gcd(123, 277)$. | d) $\gcd(1529, 14039)$. |
| e) $\gcd(1529, 14038)$. | f) $\gcd(11111, 111111)$. |

Use the Euclidean algorithm to find

- | | |
|-------------------------|---------------------------|
| a) $\gcd(12, 18)$. | b) $\gcd(111, 201)$. |
| c) $\gcd(1001, 1331)$. | d) $\gcd(12345, 54321)$. |
| e) $\gcd(1000, 5040)$. | f) $\gcd(9888, 6060)$. |

How many divisions are required to find $\gcd(21, 34)$ using the Euclidean algorithm?

How many divisions are required to find $\gcd(34, 55)$ using the Euclidean algorithm?

Extended Euclidian

BÉZOUT'S THEOREM If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

If a and b are positive integers, then integers s and t such that $\gcd(a, b) = sa + tb$ are called *Bézout coefficients* of a and b (after Étienne Bézout, a French mathematician of the eighteenth century). Also, the equation $\gcd(a, b) = sa + tb$ is called *Bézout's identity*.

We will describe an algorithm called the **extended Euclidean algorithm**, which can be used to express $\gcd(a, b)$ as a linear combination of a and b using a single pass through the steps of the Euclidean algorithm/

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

To show that $\gcd(252, 198) = 18$, the Euclidean algorithm uses these divisions:

$$252 = 1 \cdot 198 + 54$$

$$198 = 3 \cdot 54 + 36$$

$$54 = 1 \cdot 36 + 18$$

$$36 = 2 \cdot 18$$

Using the next-to-last division (the third division), we can express $\gcd(252, 198) = 18$ as a linear combination of 54 and 36. We find that

$$18 = 54 - 1 \cdot 36$$

The second division tells us that

$$36 = 198 - 3 \cdot 54$$

Substituting this expression for 36 into the previous equation, we can express 18 as a linear

Combination of 54 and 198, We have

$$18 = 54 - 1 \cdot 36$$

$$54 - 1 \cdot (198 - 3 \cdot 54)$$

$$4 \cdot 54 - 1 \cdot 198$$

The first division tells us that :

$$54 = 252 - 1 \cdot 198$$

Substituting this expression for 54 into the previous equation, we can express 18 as a linear combination of 252 and 198. We conclude that

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198,$$

Exercise: express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

a) 10, 11

b) 21, 44

c) 36, 48

d) 34, 55

e) 117, 213

f) 0, 223

g) 123, 2347

h) 3454, 4666

i) 9999, 11111

Use the extended Euclidean algorithm to express $\gcd(26, 91)$ as a linear combination of 26 and 91.

Use the extended Euclidean algorithm to express $\gcd(252, 356)$ as a linear combination of 252 and 356.

Use the extended Euclidean algorithm to express $\gcd(144, 89)$ as a linear combination of 144 and 89.

Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) is a mathematical theorem that deals with solving systems of congruences. It provides a way to reconstruct an integer from its remainders when divided by several pairwise coprime (relatively prime) moduli. In simpler terms, it allows us to find a unique solution to a set of congruences given certain conditions.

Suppose we have a system of congruences:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

$$x \equiv a_n \pmod{m_n}$$

where the moduli m_1, m_2, \dots, m_n are pairwise coprime (i.e., they have no common factors other than 1), and a_1, a_2, \dots, a_n are the corresponding remainders.

The CRT states that there exists a unique solution x modulo $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$, such that for each i , $x \equiv a_i \pmod{m_i}$.

The formula to find this solution is given by:

$$x = (a_1 * M_1 * y_1 + a_2 * M_2 * y_2 + \dots + a_n * M_n * y_n) \pmod{M}$$

where:

$$M_i = M / m_i$$

y_i is the modular inverse of M_i modulo m_i , meaning $M_i * y_i \equiv 1 \pmod{m_i}$

Example of the Chinese Remainder Theorem

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

Here,

the moduli 3, 5, and 7 are pairwise coprime.

Step 1: Calculate the product of the moduli ($M = 3 \cdot 5 \cdot 7 = 105$).

Calculate the values of M_1, M_2, M_3 :

$$M_1 = M / 3 = 105 / 3 = 35$$

$$M_2 = M / 5 = 105 / 5 = 21$$

$$M_3 = M / 7 = 105 / 7 = 15$$

Modular inverse y_1, y_2, y_3 , for each M_i

$$y_1 \equiv 35^{-1} \pmod{3} \equiv 2 \pmod{3}$$

$$y_2 \equiv 21^{-1} \pmod{5} \equiv 1 \pmod{5}$$

$$y_3 \equiv 15^{-1} \pmod{7} \equiv 1 \pmod{7}$$

Now, Compute values of each variables into formula.

$$x = (a_1 * M_1 * y_1 + a_2 * M_2 * y_2 + \dots + a_n * M_n * y_n) \pmod{M}$$

$$x = (2 * 35 * 2 + 3 * 21 * 1 + 2 * 15 * 1) \pmod{105}$$

$$x = (140 + 63 + 30) \pmod{105}$$

$$x = 233 \pmod{105}$$

$$x = 23$$

Pseudorandom Numbers

Randomly chosen numbers are often needed for computer simulations. Different methods have been devised for generating numbers that have properties of randomly chosen numbers. Because numbers generated by systematic methods are not truly random, they are called **pseudorandom numbers**.

The most commonly used procedure for generating pseudorandom numbers is the **linear congruential method**. We choose four integers: the **modulus** m , **multiplier** a , **increment** c , and **seed** x_0 , with $2 \leq a < m$, $0 \leq c < m$, and $0 \leq x_0 < m$. We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n , by successively using the recursively defined function

- $x_{n+1} = (ax_n + c) \bmod m$.

Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.

$$x_{n+1} = (ax_n + c) \bmod m.$$

$$x_{n+1} = (7x_n + 4) \bmod 9.$$

$$x_1 = 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,$$

$$x_2 = 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,$$

$$x_3 = 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,$$

$$x_4 = 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,$$

$$x_5 = 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,$$

$$x_6 = 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,$$

$$x_7 = 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = 4 \bmod 9 = 4,$$

$$x_8 = 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,$$

$$x_9 = 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.$$

Because $x_9 = x_0$ and because each term depends only on the previous term, we see that the sequence

3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, ...

is generated. This sequence contains nine different numbers before repeating.

