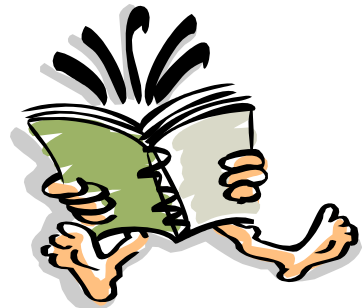


Discrete Structures 2

Chapter 4: Number Theory



Chapter 4: Number Theory

- The Integers and Division.
- Integer Representations.
- Primes.
- Greatest Common Divisors.
- Least Common Multiple.
- Solving Congruences.
- Some of the Applications.

Division (1/15)

DEFINITION

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)

we say that a is a *factor* of b and that b is a *multiple* of a .

notation $a \mid b$ denotes that a divides b .

We write $a \nmid b$ when a does not divide b .

Division (1/15)

DEFINITION

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

Division (2/15)

Example 1

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

Division (2/15)

Example 1 – Solution

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

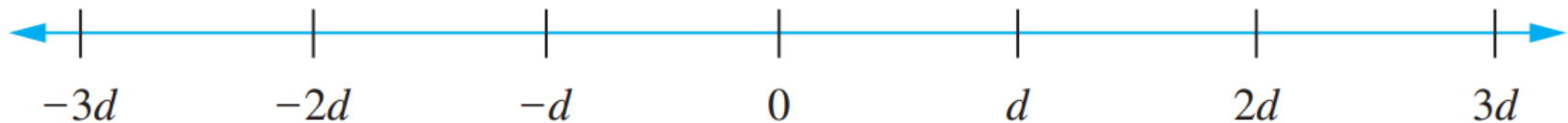
It follows that $3 \nmid 7$, because $7/3$ is not an integer.

$3 \mid 12$ because $12/3 = 4$.

Division (3/15)

Example 2

A number line indicates which integers are divisible by the positive integer d .



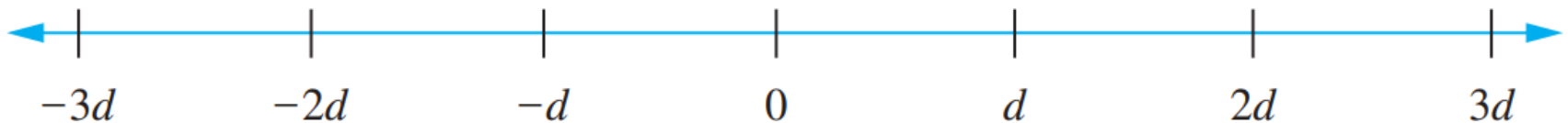
which integers are divisible
by the positive integer d .

Division (4/15)

Example 3

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

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 .



Division (5/15)

THEOREM

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

- (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 $a \mid c$

As a result:

If $a \mid b$ and $a \mid c$, then $a \mid \mathbf{m}b + \mathbf{n}c$ whenever
 \mathbf{m} and \mathbf{n} are integers

Division (6/15)

Examples

- 1) Does 2 divides 4?
- 2) Does 2 divides 8?
- 3) 2 divides $(4 + 8)$?

- 4) Does 2 divides 4?
- 5) Does 2 divides $4 * 5$?
- 6) Does 2 divides $4 * 4$?

- 7) Does 2 divides 4?
- 8) Does 4 divides 16?
- 9) Does 2 divides 16?

Division (7/15)

The Division Algorithm

Let a be an integer and d a positive integer. Then

dividend \rightarrow a
divisor \rightarrow d

$$\frac{a}{d} = \text{quotient } (q) , \quad \text{remainder } (r)$$

with, $0 \leq r < d$

$$a = dq + r$$

The remainder r cannot be negative!

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

$$q = \left\lfloor \frac{a}{d} \right\rfloor$$
$$r = a - qd$$

Division (8/15)

Example 1

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

Division (8/15)

Example 1 – Solution

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

$$q = \lfloor 101/11 \rfloor = \lfloor 9.18 \rfloor = 9,$$

$$r = 101 - (9)(11) = 2$$

Division (8/15)

Example 1 – Solution

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

Solution: We have

$$101 = 11 \cdot 9 + 2.$$

Hence, the quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$,
and the remainder is $2 = 101 \text{ mod } 11$.

Division (9/15)

Example 2

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

Division (9/15)

Example 2 – Solution

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

$$q = \lfloor -11/3 \rfloor = \lfloor -3.6 \rfloor = -4,$$

$$r = -11 - (3)(-4) = 1$$

Division (9/15)

Example 2 – Solution

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

Solution: We have

$$-11 = 3(-4) + 1.$$

Hence, the quotient when -11 is divided by 3 is $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \text{ mod } 3$.

Division (10/15)

Example 3

Evaluate:

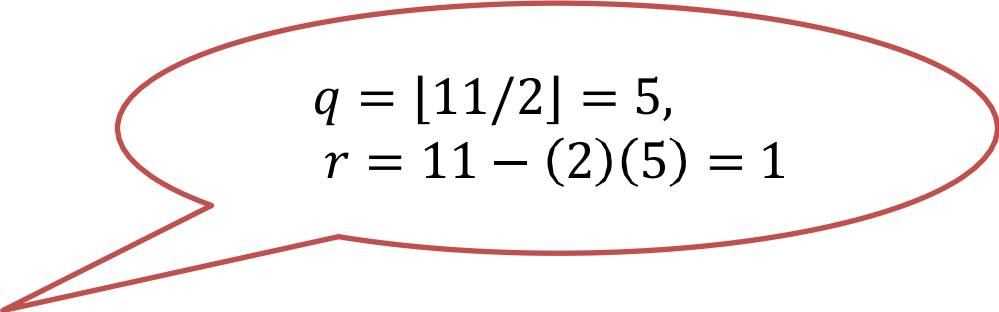
➤ $11 \bmod 2$

➤ $-11 \bmod 2$

Division (10/15)

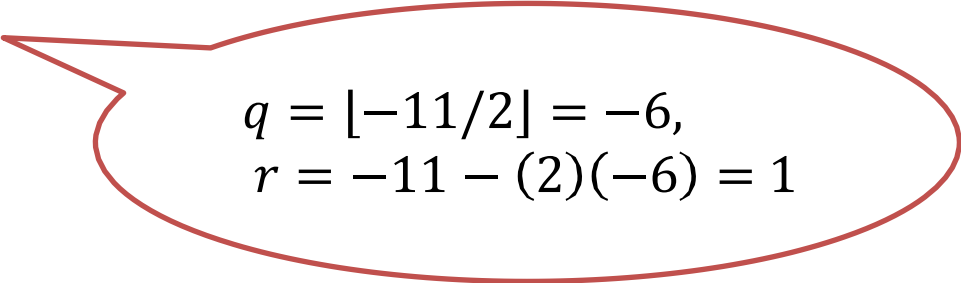
- **Example 3 – Solution**

- **Evaluate:**


$$q = \lfloor 11/2 \rfloor = 5,$$
$$r = 11 - (2)(5) = 1$$

➤ $11 \bmod 2 = 1$

➤ $-11 \bmod 2 = 1$


$$q = \lfloor -11/2 \rfloor = -6,$$
$$r = -11 - (2)(-6) = 1$$

Division (11/15)

Note:

If $a \mid b$, then $-a \mid b$

Example:

$$2 \mid 8$$

Then

$$-2 \mid 8$$

Division (12/15)

Example 4

Show that if a is an integer, then $1 \mid a$

➤ $q = \lfloor a/1 \rfloor = a$

➤ $(a)(1) = a$, and $r = 0$, so $1 \mid a$

Division (13/15)

Example 5

Show that if a is an integer other than 0, then $a \mid 0$

➤ $q = \lfloor 0/a \rfloor = 0$

➤ $(0)(a) = 0$, and $r = 0$, so $a \mid 0$

Division (14/15)

Example 6

Show that if a is an integer other than 0, then $a \mid a$

➤ $q = \lfloor a/a \rfloor = 1$

➤ $(1)(a) = a$, and $r = 0$, so $a \mid a$

Division (15/15)

Example 7

If $a \mid 1$, then $a = \dots$

- $a = \pm 1$
- $q = \lfloor 1/a \rfloor = \lfloor 1/\pm 1 \rfloor = \pm 1$
- $(\pm 1)(1) = \pm 1$, and $r = 0$, so $a \mid 1$ if $a = \pm 1$

Modular Arithmetic (1/12)

Introduction (1/3)

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.

Example:

What time does a 24-hour clock read 100 hours after it reads 2:00?

Answer: $100 + 2 \bmod 24 = 6$,

Time is 6:00

Modular Arithmetic (1/12)

Introduction (2/3)

We have already introduced the notation $a \bmod m$ to represent the remainder when an integer a is divided by the positive integer m . We now introduce a different, but related, notation that indicates that **two integers have the same remainder when they are divided by the positive integer m .**

Modular Arithmetic (1/12)

Introduction (3/3)

The great German mathematician *Karl Friedrich Gauss* developed the concept of congruences at the end of the eighteenth century. The notion of congruences has played an important role in the development of number theory.



Karl Friedrich Gauss

Modular Arithmetic (2/12)

DEFINITION

a, b are integers and m is a positive integer

a is congruent to b modulo m

$$a \equiv b(\mathbf{mod} \ m) \iff m \text{ divides } a - b$$

$$a \equiv b(\mathbf{mod} \ m) \iff a \mathbf{mod} \ m = b \mathbf{mod} \ m$$

$$a \equiv b(\mathbf{mod} \ m) \iff \text{there is an integer } k \text{ such that } a = b + km$$

Modular Arithmetic (3/12)

Example 1

Decide whether each of these integers is *congruent* to 5 *modulo* 6.

➤ 17

➤ 24

Modular Arithmetic (3/12)

Example 1 – Solution

Decide whether each of these integers is *congruent* to 5 *modulo* 6.

➤ 17

$$17 - 5 = 12, \quad \frac{12}{6} = 2, \quad \text{then} \quad 17 \equiv 5(\text{mod } 6)$$

➤ 24

$$24 - 5 = 19, \quad \frac{19}{6} = 3.2, \quad \text{then} \quad 24 \not\equiv 5(\text{mod } 6)$$

Modular Arithmetic (4/12)

Example 2

List *five* integers that are *congruent* to 2 *modulo* 4.

$a \equiv b(\mathbf{mod} \ m)$ - there is an integer k such that $a = b + km$

Modular Arithmetic (4/12)

Example 2 – Solution

List *five* integers that are *congruent to 2 modulo 4*.

$a \equiv b(\mathbf{mod} \ m)$ - there is an integer k such that $a = b + km$

$a = 2 + k * 4,$ k is integer

- $k = 1 \rightarrow a = 6$
- $k = 2 \rightarrow a = 10$
- $k = 3 \rightarrow a = 14$
- $k = 4 \rightarrow a = 18$
- $k = 5 \rightarrow a = 22$

Modular Arithmetic (4/12)

Example 2 – Solution

List *five* integers that are *congruent* to 2 modulo 4.

$a \equiv b(\text{mod } m)$ - there is an integer k such that $a = b + km$

$a = 2 + k * 4,$ k is integer

- $k = 1 \rightarrow a = 6$
- $k = 2 \rightarrow a = 10$
- $k = 3 \rightarrow a = 14$
- $k = 4 \rightarrow a = 18$
- $k = 5 \rightarrow a = 22$

The set of all integers congruent to an integer a modulo m is called the **congruence class** of a modulo m .

Modular Arithmetic (5/12)

Example 3

List all integers between -100 and 100 that are congruent to -1 modulo 25 .

Modular Arithmetic (5/12)

Example 3 – Solution

List all integers between -100 and 100 that are congruent to -1 modulo 25 .

$$\begin{aligned} a \equiv b(\bmod m) &\Leftrightarrow \text{there is an integer } k \text{ such that } a = b + km \\ a \equiv -1(\bmod 25) &\Leftrightarrow \text{there is an integer } k \text{ such that } a = -1 + 25k \end{aligned}$$

$$100 > a > -100, \quad a \text{ is integer}$$

$$100 > -1 + 25k > -100, \quad k \text{ is integer}$$

$$101 > 25k > -99, \quad k \text{ is integer}$$

$$4.04 > k > -3.96, \quad k \text{ is integer}$$

$$k = 4, 3, 2, 1, 0, -1, -2, -3$$

Modular Arithmetic (5/12)

Example 3 – Solution

List all integers between -100 and 100 that are congruent to -1 modulo 25 .

$$a = -1 + 25k$$

$$k = 4, 3, 2, 1, 0, -1, -2, -3$$

$$\text{➤ } k = -3 \rightarrow a = -76$$

$$\text{➤ } k = -2 \rightarrow a = -51$$

$$\text{➤ } k = -1 \rightarrow a = -26$$

$$\text{➤ } k = 0 \rightarrow a = -1$$

$$\text{➤ } k = 1 \rightarrow a = 24$$

$$\text{➤ } k = 2 \rightarrow a = 49$$

$$\text{➤ } k = 3 \rightarrow a = 74$$

$$\text{➤ } k = 4 \rightarrow a = 99$$

Modular Arithmetic (6/12)

Example 4

Suppose that a is integer,
 $a \equiv 4 \pmod{13}$.

Find the integer c with $0 \leq c \leq 12$ such that $c \equiv 9a \pmod{13}$

Modular Arithmetic (6/12)

Example 4 – Solution

Suppose that a is integer,
 $a \equiv 4 \pmod{13}$.

Find the integer c with $0 \leq c \leq 12$ such that $c \equiv 9a \pmod{13}$

$$a \equiv 4 \pmod{13} \rightarrow a = 4 + k(13) \rightarrow \text{if } k = 0, \text{ then } a = 4$$

$$c \equiv 9a \pmod{13} \rightarrow c \equiv 9(4) \pmod{13}$$

Modular Arithmetic (6/12)

Example 4 – Solution

Suppose that a is integer,
 $a \equiv 4 \pmod{13}$.

Find the integer c with $0 \leq c \leq 12$ such that $c \equiv 9a \pmod{13}$

$$a \equiv 4 \pmod{13} \rightarrow a = 4 + k(13) \rightarrow \text{if } k = 0, \text{ then } a = 4$$

$$c \equiv 9a \pmod{13} \rightarrow c \equiv 9(4) \pmod{13}$$

$$c = 36 \bmod 13 = 10$$

Modular Arithmetic (7/12)

THEOREM

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

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

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

Example

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

Modular Arithmetic (7/12)

THEOREM

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

If $a \equiv b(\mathbf{mod} \ m)$ and $c \equiv d(\mathbf{mod} \ m)$, then

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

Example

$$7 \equiv 2 (\mathbf{mod} \ 5) \text{ and } 11 \equiv 1 (\mathbf{mod} \ 5)$$

$$(7 + 11) \equiv (2 + 1)(\mathbf{mod} \ 5)$$

$$(7 * 11) \equiv (2 * 1)(\mathbf{mod} \ 5)$$

Modular Arithmetic (8/12)

COROLLARY 1

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

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

Modular Arithmetic (9/12)

Example 5

Find the following value.

$$(-133 \bmod 23 + 261 \bmod 23) \bmod 23$$

Modular Arithmetic (9/12)

Example 5 – Solution

Find the following value.

$$(-133 \bmod 23 + 261 \bmod 23) \bmod 23$$

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

$$(-133 + 261) \bmod 23 = (128) \bmod 23 = 13$$

Modular Arithmetic (10/12)

COROLLARY 2 (1/2)

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

$$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

$$(a)^2 \bmod m = ((a \bmod m)(a \bmod m)) \bmod m$$

$$(a)^4 \bmod m = ((a^2 \bmod m)(a^2 \bmod m)) \bmod m$$

...

Modular Arithmetic (10/12)

COROLLARY 2 (1/2)

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

$$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

$$(a)^2 \bmod m = ((a \bmod m)(a \bmod m)) \bmod m$$

$$(a)^4 \bmod m = ((a^2 \bmod m)(a^2 \bmod m)) \bmod m$$

...

If the power is a power of 2:

Then we use: $a^1, a^2, a^4, a^8, \dots$ where $a^4 = a^2 \cdot a^2$ and so on.

Modular Arithmetic (10/12)

COROLLARY 2 (2/2)

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

$$(a)^{11} \bmod m = \underline{\hspace{10em}}$$

...

If the power is not a power of 2:

- 1 Convert the power to binary. ($11 = 1011 = 2^0 + 2^1 + 2^3 = 1 + 2 + 8$)
- 2 Then we use a^1, a^2, a^8 and so on.

$$(a)^{11} \bmod m = (a^1 \cdot a^2 \cdot a^8) \bmod m$$

Where $a^2 = a \cdot a$ and $a^8 = a^4 \cdot a^4 = (a^2 \cdot a^2) \cdot (a^2 \cdot a^2)$

Modular Arithmetic (11/12)

Example 6

Find the following value.

$$(3^4 \bmod 17)^2 \bmod 11$$

Modular Arithmetic (11/12)

Example 6 – Solution

Find the following value.

$$(3^4 \bmod 17)^2 \bmod 11$$

The power is a power of 2:

We will first evaluate $3^1 \bmod 17 = 3 \bmod 17 = 3$

Second, $3^2 \bmod 17 = (3 \bmod 17)(3 \bmod 17) \bmod 17 = 9 \bmod 17 = 9$

Third, $3^4 \bmod 17 = (3^2 \bmod 17)(3^2 \bmod 17) \bmod 17 = 81 \bmod 17 = 13$

So, $(3^4 \bmod 17)^2 \bmod 11 = (13)^2 \bmod 11$

Finally, $(13)^2 \bmod 11 = (13 \bmod 11)(13 \bmod 11) \bmod 11 = 4 \bmod 11 = 4$

Modular Arithmetic (12/12)

Example 7

Find the following value.

$$5^{11} \bmod 12$$

Modular Arithmetic (12/12)

Example 7 – Solution (1/2)

Find the following value.

$$5^{\boxed{11}} \bmod 12$$

The power is NOT a power of 2:

We will first the power to binary ($11 = 1011 = 2^0 + 2^1 + 2^3 = 1 + 2 + 8$)

Then we use $5^1, 5^2, 5^8$ and so on. And $(5^{11} \bmod 12) = (5^1 \cdot 5^2 \cdot 5^8) \bmod 12$

Modular Arithmetic (12/12)

Example 7 – Solution (1/2)

Find the following value.

$$(5^{11} \bmod 12) = (5^1 \cdot 5^2 \cdot 5^8) \bmod 12$$

We will first evaluate $5^1 \bmod 12 = 5 \bmod 12 = 5$

Second, $5^2 \bmod 12 = (5 \bmod 12)(5 \bmod 12) \bmod 12 = 25 \bmod 12 = 1$

Third, $5^4 \bmod 12 = (5^2 \bmod 12)(5^2 \bmod 12) \bmod 12 = 1 \bmod 12 = 1$

Fourth, $5^8 \bmod 12 = (5^4 \bmod 12)(5^4 \bmod 12) \bmod 12 = 1 \bmod 12 = 1$

Finally,

$$(5^{11} \bmod 12) = (5^1 \cdot 5^2 \cdot 5^8) \bmod 12 = (5 \cdot 1 \cdot 1) \bmod 12 = 5 \bmod 12 = 5$$

Integer Representations (1/6)

Introduction

Integers can be expressed using any integer greater than one as a base. we commonly use decimal (base 10), representations, binary (base 2), octal (base 8), and hexadecimal (base 16) representations are often used, especially in computer science.

Integer Representations (2/6)

THEOREM: base b expansion of n

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

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

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 base b expansion of n is denoted by $(a_k a_{k-1} \dots a_1 a_0)_b$

For instance, $(983)_{10}$ represents $9 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0 = 983$

(base 10), or **decimal expansions**

Integer Representations (3/6)

Decimal Expansions

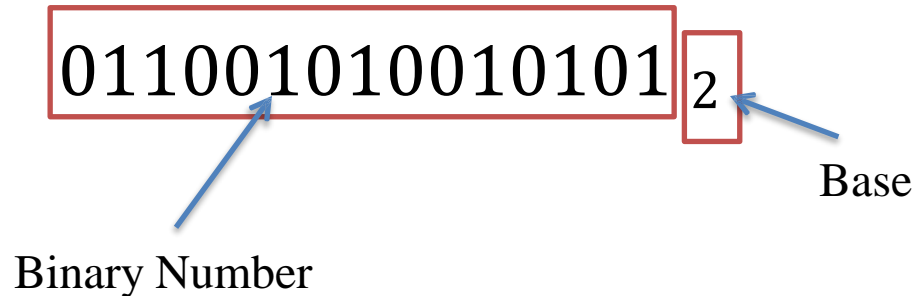
- The decimal numbering system has **10 digits**; (0,1, ..., 9)
- Base ($b = 10$).
- Examples:
 - 12234_{10}
 - 30.44_{10}
 - 1100_{10}
 - 7789_{10}

Integer Representations (3/6)

Binary Expansions (1/3)

In particular, computers usually use binary notation (with 2 as the base) when carrying out arithmetic. In binary notation each digit is either a **0** or a **1**. In other words, the binary expansion of an integer is just a bit string.

Example:



Integer Representations (3/6)

Binary Expansions (2/3)

- The binary numbering system has **2 digits**; (0, 1).
- Base ($b = 2$).
- Examples:
 - 011001010010101_2 (Integer)
 - 11001.101_2 (Not Integer)
 - 021100_2 ✖

Integer Representations (3/6)

Binary Expansions (3/3)

Example:

What is the decimal expansion of the integer that has $(1\ 0101)_2$ as its binary expansion?

$(1\ 0101)_2$ represents $1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 21$

$(1\ 0101)_2 = (21)_{10}$

Integer Representations (4/6)

Octal and Hexadecimal Expansions

In particular, computers usually use octal (base 8) or hexadecimal (base 16) notation when expressing characters, such as letters or digits. In fact, we can use any integer greater than 1 as the base when expressing integers.

Integer Representations (5/6)

Octal Expansions

Usually, the octal digits used are $(0, 1, 2, 3, 4, 5, 6, 7)$ with base $(b = 8)$.

Example:

What is the decimal expansion of the integer that has $(7016)_8$ as its octal expansion?

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

$(7016)_8 = (3598)_{10}$

Integer Representations (6/6)

Hexadecimal Expansions (1/3)

Sixteen different digits are required for hexadecimal expansions. Usually, the hexadecimal digits used are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F, where the letters A through F represent the digits corresponding to the numbers 10 through 15 (in decimal notation).

Integer Representations (6/6)

Hexadecimal Expansions (2/3)

- The hexadecimal numbering system has **16 digits**; (**0,1, ..., 9,A, B, C, D, E, F**)
- Base ($b = 16$).
- The letters A, B, C, D, E, F are used to represent the values 10, 11, 12, 13, 14, 15, respectively.
- Examples:
 - $11A3034_{16}$
 - $770F1_{16}$
 - 6689011_{16}

Integer Representations (6/6)

Hexadecimal Expansions (3/3)

A	B	C	D	E	F
10	11	12	13	14	15

Example:

What is the decimal expansion of the integer that has $(2AE0B)_{16}$ as its hexadecimal expansion?

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

$$(2AE0B)_{16} = (175\ 627)_{10}$$

Base Conversion (1/7)

Binary to Decimal Conversion (1/3)

- The decimal value of a binary number is computed by summing the result of multiplying each of its digits by the base 2 raised to a power determined by the digit position.
- Example1: (011010_2)

0	1	1	0	1	0
2^5	2^4	2^3	2^2	2^1	2^0



$$\begin{aligned} &= 0 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 \\ &= 0 \quad + 16 \quad + 8 \quad + 0 \quad + 2 \quad + 0 \quad = 26 \end{aligned}$$

Base Conversion (1/7)

Binary to Decimal Conversion (1/3)

- The decimal value of a binary number is computed by summing the result of multiplying each of its digits by the base 2 raised to a power determined by the digit position.
- Example1: (011010_2)

0	1	1	0	1	0
2^5	2^4	2^3	2^2	2^1	2^0



$$\begin{aligned} &= 0 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 \\ &= 0 + 16 + 8 + 0 + 2 + 0 = 26 \end{aligned}$$

$$011010_2 = 26_{10}$$

Base Conversion (1/7)

Binary to Decimal Conversion (2/3)

- Example2: (10011_2)

Base Conversion (1/7)

Binary to Decimal Conversion (2/3)

- Example2: (10011_2)

1	0	0	1	1
2^4	2^3	2^2	2^1	2^0



$$\begin{aligned} &= 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 \\ &= 16 + 0 + 0 + 2 + 1 = 19 \end{aligned}$$

$$10011_2 = 19_{10}$$

Base Conversion (1/7)

Binary to Decimal Conversion (3/3)

- Example3: (10001.101_2)

1	0	0	0	1	.	1	0	1
2^4	2^3	2^2	2^1	2^0		2^{-1}	2^{-2}	2^{-3}



$$\begin{aligned} &= 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 + 1 \times 2^{-1} + 0 \times 2^{-2} + 1 \times 2^{-3} \\ &= 16 + 0 + 0 + 0 + 1 + 0.5 + 0 + 0.125 \\ &= 17.625 \end{aligned}$$

$$10001.101_2 = 17.625_{10}$$

Base Conversion (2/7)

Decimal to Binary Conversion (1/2)

- Example1: (75_{10})

$$\begin{array}{r|l} \div & \\ 75 & 2 \quad \mathbf{1} \\ \hline 37 & \end{array}$$

Base Conversion (2/7)

Decimal to Binary Conversion (1/2)

- Example1: (75_{10})

	÷		
75		2	1
37		2	1
18			

Base Conversion (2/7)

Decimal to Binary Conversion (1/2)

- Example1: (75_{10})

\div		
75	2	1
37	2	1
18	2	0
9		

Base Conversion (2/7)

Decimal to Binary Conversion (1/2)

- Example1: (75_{10})

	÷		
75		2	1
37		2	1
18		2	0
9		2	1
4			

Base Conversion (2/7)

Decimal to Binary Conversion (1/2)

- Example1: (75_{10})

	÷		
75		2	1
37		2	1
18		2	0
9		2	1
4		2	0
2			

Base Conversion (2/7)

Decimal to Binary Conversion (1/2)

- Example1: (75_{10})

	÷		
75		2	1
37		2	1
18		2	0
9		2	1
4		2	0
2		2	0
1			

Base Conversion (2/7)

Decimal to Binary Conversion (1/2)

- Example1: (75_{10})

\div		
75	2	1
37	2	1
18	2	0
9	2	1
4	2	0
2	2	0
1	2	1
0		

Base Conversion (2/7)

Decimal to Binary Conversion (1/2)

- Example1: $(75_{10}) = (1001011_2)$

	÷			
75	2	1		
37	2	1		
18	2	0		
9	2	1		
4	2	0		
2	2	0		
1	2	1		
0				

1	0	0	1	0	1	1
---	---	---	---	---	---	---

Base Conversion (2/7)

Decimal to Binary Conversion (2/2)

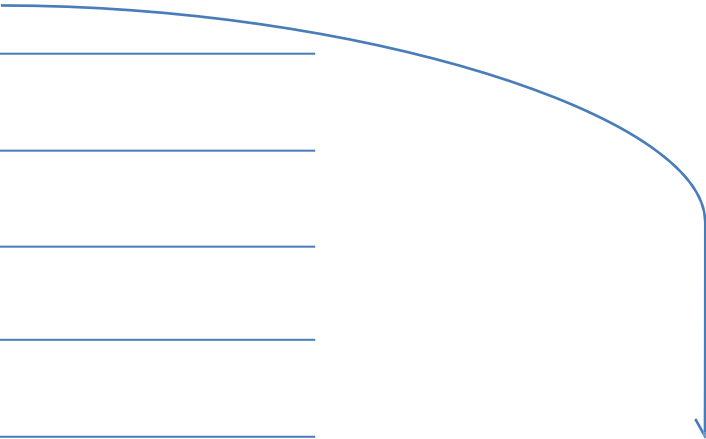
- Example2: (25_{10})

Base Conversion (2/7)

Decimal to Binary Conversion (2/2)

- Example2: (25_{10})

25	2	1
12	2	0
6	2	0
3	2	1
1	2	1
0		



11001

Base Conversion (3/7)

Binary and Hexadecimal Equivalents

Hexadecimal Digits and Its Decimal and Binary Equivalents										
Hex	Decimal	Binary		Hex	Decimal	Binary				
0	0	0000		8	8	1000				
1	1	0001		9	9	1001				
2	2	0010		A	10	1010				
3	3	0011		B	11	1011				
4	4	0100		C	12	1100				
5	5	0101		D	13	1101				
6	6	0110		E	14	1110				
7	7	0111		F	15	1111				
Conversion Between Binary and Hexadecimal										
Example:										
5		C		A		← Hexadecimal				
0	1	0	1	1	1	0	0	1	0	← Binary

Base Conversion (4/7)

Binary and Hexadecimal Equivalents – Example1

Convert from Hexadecimal to Binary

C40E₁₆

C	4	0	E

Base Conversion (4/7)

Binary and Hexadecimal Equivalents – Example1

Convert from Hexadecimal to Binary

C40E₁₆

C	4	0	E
12	4	0	14

Base Conversion (4/7)

Binary and Hexadecimal Equivalents – Example1

Convert from Hexadecimal to Binary

C40E₁₆

C	4	0	E
12	4	0	14
1100	0100	0000	1110

1100010000001110₂

Base Conversion (5/7)

Binary and Hexadecimal Equivalents – Example2

Convert from Hexadecimal to Binary
$10A7_{16}$

Base Conversion (5/7)

Binary and Hexadecimal Equivalents – Example2

Convert from Hexadecimal to Binary

10A7₁₆

1	0	A	7
1	0	10	7
0001	0000	1010	0111

1000010100111₂

Base Conversion (6/7)

Binary and Hexadecimal Equivalents – Example3

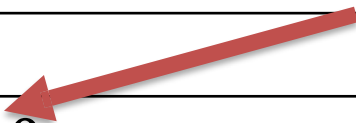
Convert from Binary to Hexadecimal
1101100001011100 ₂

Base Conversion (6/7)

Binary and Hexadecimal Equivalents – Example3

Convert from Binary to Hexadecimal

1101 1000 0101 1100₂



1101	1000	0101	1100

Base Conversion (6/7)

Binary and Hexadecimal Equivalents – Example3

Convert from Binary to Hexadecimal

1101 1000 0101 1100₂



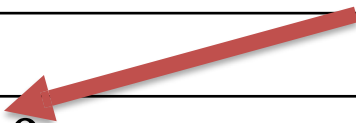
1101	1000	0101	1100
13	8	5	12

Base Conversion (6/7)

Binary and Hexadecimal Equivalents – Example3

Convert from Binary to Hexadecimal

1101 1000 0101 1100₂



1101	1000	0101	1100
13	8	5	12
D	8	5	C

D85C₁₆

Base Conversion (7/7)

ALGORITHM 1 Constructing Base b Expansions.

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 the base b expansion of $n\}$

Addition Algorithm (1/2)

Addition in Binary (1/3)

- How to add two binary numbers?

$$0 + 0 = 0$$

$$0 + 1 = 1$$

$$1 + 0 = 1$$

$$1 + 1 = 0 \rightarrow 1$$

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example1:

$$101100 + 11010$$

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example1:

101100

+

11010

0

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example1:

101100

+

11010

10

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example1:

101**1**00

+

11**0**10

110

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example 1:

$$\begin{array}{r} 1 \\ 101100 \\ + \\ 11010 \\ \hline 0110 \end{array}$$

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example 1:

$$\begin{array}{r} 1 \\ + \\ 10\textcolor{red}{1}100 \\ \hline 1 \qquad + \\ 1\textcolor{red}{1}010 \\ \hline 0110 \end{array}$$

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example 1:

$$\begin{array}{r} 1 \\ 101100 \\ --- \\ 1 \quad + \\ \quad + \\ 11010 \\ ----- \\ 00110 \end{array}$$

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example 1:

$$\begin{array}{r} 11 \\ + \\ 101100 \\ \hline 0 \end{array} + \begin{array}{r} 11010 \\ \hline 00110 \end{array}$$

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example 1:

A binary addition diagram. The first number, 101100, is positioned above a dashed line. A blue '1' is placed above the first number, indicating a carry. The second number, 11010, is positioned below the first number and to the right of the dashed line. A red '0' is placed above the second number, indicating a carry. A red dashed arrow points from the red '0' down to the first number. A plus sign '+' is placed to the right of the second number. Below the dashed line, the result 000110 is shown.

$$\begin{array}{r} 1 \\ 101100 \\ --- \\ 0 \quad 11010 \\ + \\ \hline 000110 \end{array}$$

Addition Algorithm (1/2)

Addition in Binary (2/3)

- Example 1:

A diagram illustrating binary addition. The first number, 101100, is aligned above the second number, 11010. A plus sign (+) is placed to the right of the second number. A horizontal dashed line separates the addends from the sum. The sum, 1000110, is written below the dashed line. A blue '1' is positioned above the first number, with a vertical dashed red arrow pointing down from it to the first column of the sum, indicating a carry.

$$\begin{array}{r} 1 \\ 101100 \\ + 11010 \\ \hline 1000110 \end{array}$$

Addition Algorithm (1/2)

Addition in Binary (3/3)

- Example2:

$$\begin{array}{r} 11 \\ 11110 \\ 1100 \\ \hline 101010 \end{array} +$$

Addition Algorithm (2/2)

ALGORITHM 2 Addition of Integers.

procedure *add*(*a*, *b*: positive integers)

{ the binary expansions of *a* and *b* are $(a_{n-1}a_{n-2} \dots a_1a_0)_2$
and $(b_{n-1}b_{n-2} \dots b_1b_0)_2$, respectively }

c := 0

for *j* := 0 **to** *n* − 1

d := $\lfloor (a_j + b_j + c)/2 \rfloor$

*s*_{*j*} := $a_j + b_j + c - 2d$

c := *d*

*s*_{*n*} := *c*

return (*s*₀, *s*₁, ..., *s*_{*n*}) { the binary expansion of the sum is $(s_ns_{n-1} \dots s_0)_2$ }

Multiplication Algorithm (1/3)

Multiplication in Binary

Consider the multiplication of two n -bit integers a and b . The conventional algorithm (used when multiplying with pencil and paper) works as follows. Using the distributive law, we see that

$$\begin{aligned} ab &= a(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1}) \\ &= a(b_0 2^0) + a(b_1 2^1) + \cdots + a(b_{n-1} 2^{n-1}). \end{aligned}$$

We can compute ab using this equation. We first note that $ab_j = a$ if $b_j = 1$ and $ab_j = 0$ if $b_j = 0$. Each time we multiply a term by 2, we shift its binary expansion one place to the left and add a zero at the tail end of the expansion. Finally, we obtain ab by adding the n integers $ab_j 2^j$, $j = 0, 1, 2, \dots, n - 1$.

Multiplication Algorithm (2/3)

Multiplication in Binary – Example

Multiplying $(110)_2$ and $(101)_2$.

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

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

and

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

add $(110)_2$, $(0000)_2$, and $(11000)_2$.

$$\begin{array}{r} 110 \\ \times 101 \\ \hline 110 \\ 000 \\ 110 \\ \hline 11110 \end{array}$$

Multiplication Algorithm (3/3)

ALGORITHM 3 Multiplication of Integers.

```
procedure multiply( $a, b$ : positive integers)
{ the binary expansions of  $a$  and  $b$  are  $(a_{n-1}a_{n-2} \dots a_1a_0)_2$ 
  and  $(b_{n-1}b_{n-2} \dots b_1b_0)_2$ , respectively }
for  $j := 0$  to  $n - 1$ 
    if  $b_j = 1$  then  $c_j := a$  shifted  $j$  places
    else  $c_j := 0$ 
{  $c_0, c_1, \dots, c_{n-1}$  are the partial products }
 $p := 0$ 
for  $j := 0$  to  $n - 1$ 
     $p := \text{add}(p, c_j)$ 
return  $p$  {  $p$  is the value of  $ab$  }
```

Primes (1/9)

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*.

Ex: The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3.

Primes (2/9)

Remark

The integer 1 is not prime, because it has only one positive factor. Note also that an integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$

Primes (3/9)

THEOREM 1

THE FUNDAMENTAL THEOREM OF ARITHMETIC

Every integer greater than 1 can be written *uniquely as a prime or as the product of two or more primes.*

Primes (4/9)

THEOREM 2

If n is a composite integer,

then n has a prime divisor less than or equal to \sqrt{n} .

Example 1: The integer 100 is prime or not ?

The prime numbers $\leq \sqrt{100}$ are 2, 3, 5, and 7

$$2|100, \quad \text{and} \quad 5|100$$

So, 100 is not a prime integer. 100 is a composite integer.

Primes (5/9)

Example 2

The integer 101 is prime or not ?

The prime numbers $\leq \sqrt{101}$ are 2, 3, 5, and 7

$2 \nmid 101$, $3 \nmid 101$, $5 \nmid 101$, and $7 \nmid 101$

So, 101 is a prime integer.

Primes (6/9)

Example 3

Find the prime factorization of 100?

The prime numbers $\leq \sqrt{100}$ are 2, 3, 5, and 7

$$\left(\begin{array}{c|c} 100 & 2 \\ 50 & 2 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array} \right)$$

$$\begin{aligned} 100 &= 2 \cdot 2 \cdot 5 \cdot 5 \\ &= 2^2 \cdot 5^2 \end{aligned}$$

Primes (7/9)

Example 4

Find the prime factorization of 1001?

The prime numbers $\leq \sqrt{1001}$ are 2, 3, 5, 7, 11, 13, 17, 19, 23 ...

$\sqrt{143}$ are 2, 3, 5, 7, 11

$\sqrt{13}$ are 2, 3

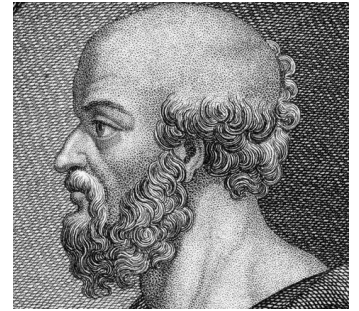
$$\left(\begin{array}{c|c} 1001 & 7 \\ 143 & 11 \\ 13 & 13 \\ 1 & \end{array} \right)$$

$$1001 = 7 \cdot 11 \cdot 13$$

Primes (8/9)

The Sieve of Eratosthenes (1/6)

In mathematics, the sieve of Eratosthenes is an ancient algorithm for finding all prime numbers up to any given limit.



Eratosthenes
Greek

Primes (8/9)

The Sieve of Eratosthenes (2/6)

Is used to find all primes not exceeding a specified positive integer. For instance, the following procedure is used to find the primes not exceeding 100. Note that composite integers not exceeding 100 must have a prime factor not exceeding $10 = \sqrt{100}$.

The prime numbers $\leq \sqrt{100}$ are 2, 3, 5, and 7

Primes (8/9)

The Sieve of Eratosthenes (3/6)

*Integers divisible by 2 other than 2
receive an underline.*

1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	9	<u>10</u>
11	<u>12</u>	13	<u>14</u>	15	<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>
31	<u>32</u>	33	<u>34</u>	35	<u>36</u>	37	<u>38</u>	39	<u>40</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>
61	<u>62</u>	63	<u>64</u>	65	<u>66</u>	67	<u>68</u>	69	<u>70</u>
71	<u>72</u>	73	<u>74</u>	75	<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>
91	<u>92</u>	93	<u>94</u>	95	<u>96</u>	97	<u>98</u>	99	<u>100</u>

Primes (8/9)

The Sieve of Eratosthenes (3/6)

*Integers divisible by 2 other than 2
receive an underline.*

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

Primes (8/9)

The Sieve of Eratosthenes (4/6)

*Integers divisible by 3 other than 3
receive an underline.*

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

Primes (8/9)

The Sieve of Eratosthenes (4/6)

*Integers divisible by 3 other than 3
receive an underline.*

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

Primes (8/9)

The Sieve of Eratosthenes (5/6)

*Integers divisible by 5 other than 5
receive an underline.*

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

Primes (8/9)

The Sieve of Eratosthenes (5/6)

*Integers divisible by 5 other than 5
receive an underline.*

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

Primes (8/9)

The Sieve of Eratosthenes (6/6)

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

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

Primes (8/9)

The Sieve of Eratosthenes (6/6)

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

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

Primes (9/9)

	2	3	4	5	6	7	8	9	10	Prime numbers			
11	12	13	14	15	16	17	18	19	20	2	3	5	7
21	22	23	24	25	26	27	28	29	30	11	13	17	19
31	32	33	34	35	36	37	38	39	40	23	29	31	37
41	42	43	44	45	46	47	48	49	50	41	43	47	53
51	52	53	54	55	56	57	58	59	60	59	61	67	71
61	62	63	64	65	66	67	68	69	70	73	79	83	89
71	72	73	74	75	76	77	78	79	80	97	101	103	107
81	82	83	84	85	86	87	88	89	90	109	113		
91	92	93	94	95	96	97	98	99	100				
101	102	103	104	105	106	107	108	109	110				
111	112	113	114	115	116	117	118	119	120				

Greatest Common Divisors (1/5)

DEFINITION “gcd” (1/2)

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 .

is denoted by $\gcd(a, b)$.

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

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

Greatest Common Divisors (1/5)

DEFINITION “gcd” (2/2)

For 12 and 18, what is the greatest common factor?

We have four common factors {1, 2, 3, 6}

The greatest one is {6}.

Greatest Common Divisors (2/5)

Example 1

What is the greatest common divisor of 24 and 36?

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

Greatest Common Divisors (2/5)

Example 1

What is the greatest common divisor of 24 and 36?

$\sqrt{24}$ are 2, 3

$\sqrt{36}$ are 2, 3, 5

$$\left(\begin{array}{c|c} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array} \right) = 2^3 \cdot 3$$

$$\left(\begin{array}{c|c} 36 & 2 \\ 18 & 2 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array} \right) = 2^2 \cdot 3^2$$

$$\gcd(24, 36) = 2^2 \cdot 3 = 12$$

Greatest Common Divisors (3/5)

Example 2

What is the $\gcd(120, 500)$?

$\sqrt{120}$ are 2, 3, 5, 7

$\sqrt{500}$ are 2, 3, 5, 7, 11, 13, 17, 19

$$\left(\begin{array}{c|c} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \right) = 2^3 \cdot 3 \cdot 5$$

$$\left(\begin{array}{c|c} 500 & 2 \\ 250 & 2 \\ 125 & 5 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array} \right) = 2^2 \cdot 5^3$$

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

Greatest Common Divisors (4/5)

DEFINITION 1

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

Is 17 and 22 are relatively prime?

Greatest Common Divisors (4/5)

DEFINITION 1

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

Is 17 and 22 are relatively prime? (Yes)

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

Greatest Common Divisors (5/5)

DEFINITION 2

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

Greatest Common Divisors (5/5)

DEFINITION 2

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 . Example:

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

Solution:

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.

Least Common Multiple (1/5)

DEFINITION “lcm”

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 $\text{lcm}(a, b)$.

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

Least Common Multiple (2/5)

Example 1

What is the $\text{lcm}(24, 36)$?

$\sqrt{24}$ are 2, 3

$\sqrt{36}$ are 2, 3, 5

$$\left(\begin{array}{c|c} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array} \right) = 2^3 \cdot 3$$

$$\left(\begin{array}{c|c} 36 & 2 \\ 18 & 2 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array} \right) = 2^2 \cdot 3^2$$

$$\text{lcm}(24, 36) = 2^3 \cdot 3^2 = 72$$

Least Common Multiple (3/5)

Example 2

What is the $\text{lcm}(120, 500)$?

$\sqrt{120}$ are 2, 3, 5, 7

$\sqrt{500}$ are 2, 3, 5, 7, 11, 13, 17, 19

$$\left(\begin{array}{c|c} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \right) = 2^3 \cdot 3 \cdot 5$$

$$\left(\begin{array}{c|c} 500 & 2 \\ 250 & 2 \\ 125 & 5 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array} \right) = 2^2 \cdot 5^3$$

$$\text{lcm}(120, 500) = 2^3 \cdot 3^1 \cdot 5^3 = 3000$$

Least Common Multiple (4/5)

THEOREM

Let a and b be positive integers. Then

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

Least Common Multiple (5/5)

Example 3

What are the **gcd(120, 500)** and **lcm(120, 500)** ?

$\sqrt{120}$ are 2, 3, 5, 7

$\sqrt{500}$ are 2, 3, 5, 7, 11, 13, 17, 19

$$\left(\begin{array}{c|c} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \right) = 2^3 \cdot 3 \cdot 5$$

$$\left(\begin{array}{c|c} 500 & 2 \\ 250 & 2 \\ 125 & 5 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array} \right) = 2^2 \cdot 5^3$$

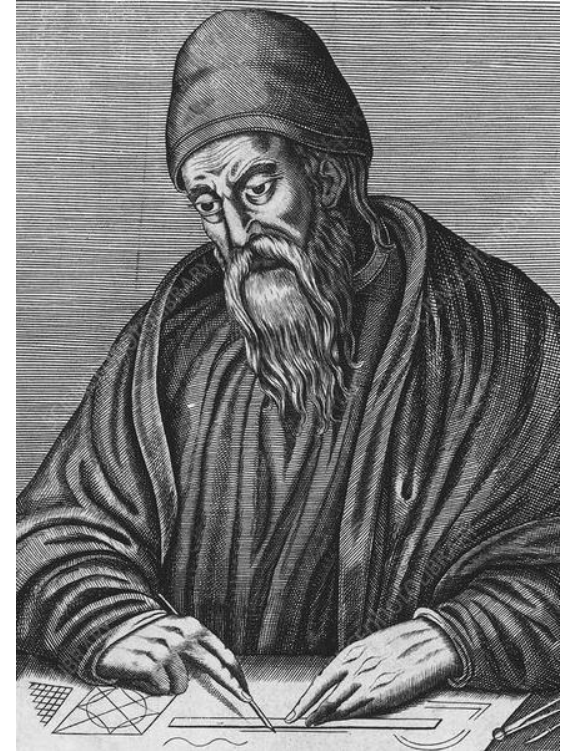
$$\text{lcm}(120, 500) = 2^3 \cdot 3^1 \cdot 5^3 = 3000$$

$$\text{gcd}(120, 500) = \frac{120 * 500}{3000} = 20$$

Methods of Finding The gcd (1/6)

The Euclidean 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. It is named after the ancient Greek mathematician **Euclid**, who included a description of this algorithm in his book “*The Elements*.”



Euclid

Methods of Finding The gcd (1/6)

The Euclidean Algorithm

The Euclidean algorithm is based on the following result about *greatest common divisors* and the *division algorithm*.

Let $a = bq + r$, where a , b , q , and r are integers.

Then $\gcd(a, b) = \gcd(b, r)$.

If $r = 0$, then $\gcd(a, b) = b$

Methods of Finding The gcd (2/6)

Example 1

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

Methods of Finding The gcd (2/6)

Example 1

b

a

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

Methods of Finding The gcd (2/6)

Example 1 – Solution

b

a

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

Successive uses of the division algorithm give: $a = bq + r$

$$662 = 414 \cdot 1 + 248 \quad \rightarrow \quad 662/414 \rightarrow q = 1 \quad \text{and} \quad r = 248$$

Methods of Finding The gcd (2/6)

Example 1 – Solution

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

Successive uses of the division algorithm give: $a = bq + r$

$$662 = 414 \cdot 1 + 248 \quad \rightarrow \quad 662/414 \rightarrow q = 1 \quad \text{and} \quad r = 248$$

$$\gcd(a, b) = \gcd(b, r)$$

$$\gcd(662, 414) = \gcd(414, 248)$$

Methods of Finding The gcd (2/6)

Example 1 – Solution

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

Successive uses of the division algorithm give: $a = bq + r$

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

$$\rightarrow 662/414 \rightarrow q = 1 \text{ and } r = 248$$

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

Methods of Finding The gcd (2/6)

Example 1 – Solution

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

Successive uses of the division algorithm give: $a = bq + r$

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

$$\rightarrow 662/414 \rightarrow q = 1 \text{ and } r = 248$$

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

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

Methods of Finding The gcd (2/6)

Example 1 – Solution

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

Successive uses of the division algorithm give: $a = bq + r$

$$662 = 414 \cdot 1 + 248 \quad \rightarrow \quad 662/414 \rightarrow q = 1 \quad \text{and} \quad r = 248$$

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

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

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

$$82 = 2 \cdot 41 + 0$$

Methods of Finding The gcd (2/6)

Example 1 – Solution

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

Successive uses of the division algorithm give: $a = bq + r$

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

$$\rightarrow 662/414 \rightarrow q = 1 \text{ and } r = 248$$

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

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

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

$$82 = 2 \cdot 41 + 0$$

If $r = 0$, then $\gcd(a, b) = b$

$$\gcd(82, 2) = 2$$

$$\gcd(662, 414) = \gcd(82, 2) = 2$$

Methods of Finding The gcd (2/6)

Example 1 – Solution

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

We can summarize these steps in tabular form

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	662	414	1	248
1	414	248	1	166
2	248	166	1	82
3	166	82	2	2
4	82	2	41	0

$$r_0 = a \quad r_1 = b$$

Methods of Finding The gcd (3/6)

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b: \text{positive integers})$

$x := a$

$y := b$

while $y \neq 0$

$r := x \bmod y$

$x := y$

$y := r$

return $x \{gcd(a, b) \text{ is } x\}$

Methods of Finding The gcd (4/6)

BEZOUT'S THEOREM

$\gcd(a, b)$ can be expressed as a **linear combination**

If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$ is called Bezout *identity*.

s and t are called *Bezout coefficients* of a and b .



ETIENNE BEZOUT
France

Methods of Finding The gcd (5/6)

$$\gcd(a, b) = sa + tb$$

Extended Euclidean Algorithm

To find the *Beyzout coefficients* of a and b (i.e., s and t), called extended Euclidean algorithm,

we set $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, and $t_1 = 1$ and let

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

for $j = 2, 3, \dots, n$, where the q_j are the quotients in the divisions used when the Euclidean algorithm finds $\gcd(a, b)$.

The desired *Beyzout coefficients* are the values of s_n and t_n

Methods of Finding The gcd (6/6)

Example 2

$$\gcd(a, b) = sa + tb$$

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	252	198	1	54
1	198	54	3	36
2	54	36	1	18
3	36	18	2	0

Using Euclidean algorithm

If $r = 0$, then $\gcd(a, b) = b$

$$\gcd(36, 18) = 18$$

$$\gcd(252, 198) = \gcd(36, 18) = 18$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54		
1	198	54	3	36		
2	54	36	1	18		
3	36	18	2	0		
4						

$$\begin{array}{ll} s_0 = 1 & s_1 = 0 \\ t_0 = 0 & t_1 = 1 \end{array}$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18		
3	36	18	2	0		
4						

$$\begin{array}{ll} s_0 = 1 & s_1 = 0 \\ t_0 = 0 & t_1 = 1 \end{array}$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18		
3	36	18	2	0		
4						

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$s_j = s_{j-2} - q_{j-1}s_{j-1}$$

$$s_2 = s_0 - q_1s_1$$

$$s_2 = 1 - 0 = 1$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	
3	36	18	2	0		
4						

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$s_j = s_{j-2} - q_{j-1}s_{j-1}$$

$$s_2 = s_0 - q_1s_1$$

$$s_2 = 1 - 0 = 1$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	
3	36	18	2	0		
4						

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$t_j = t_{j-2} - q_{j-1}t_{j-1}$$

$$t_2 = t_0 - q_1t_1$$

$$t_2 = 0 - 1 = -1$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0		
4						

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$t_j = t_{j-2} - q_{j-1}t_{j-1}$$

$$t_2 = t_0 - q_1t_1$$

$$t_2 = 0 - 1 = -1$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0		
4						

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$s_j = s_{j-2} - q_{j-1}s_{j-1}$$

$$s_3 = s_1 - q_2s_2$$

$$s_3 = 0 - 3 = -3$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	
4						

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$s_j = s_{j-2} - q_{j-1}s_{j-1}$$

$$s_3 = s_1 - q_2s_2$$

$$s_3 = 0 - 3 = -3$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	
4						

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$t_j = t_{j-2} - q_{j-1}t_{j-1}$$

$$t_3 = t_1 - q_2t_2$$

$$t_3 = 1 - (-3) = 4$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
4						

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$t_j = t_{j-2} - q_{j-1}t_{j-1}$$

$$t_3 = t_1 - q_2t_2$$

$$t_3 = 1 - (-3) = 4$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
4						

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$s_j = s_{j-2} - q_{j-1}s_{j-1}$$

$$s_4 = s_2 - q_3s_3$$

$$s_4 = 1 - (-3) = 4$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
4					4	

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$s_j = s_{j-2} - q_{j-1}s_{j-1}$$

$$s_4 = s_2 - q_3s_3$$

$$s_4 = 1 - (-3) = 4$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
4					4	

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$t_j = t_{j-2} - q_{j-1}t_{j-1}$$

$$t_4 = t_2 - q_3t_3$$

$$t_4 = -1 - (4) = -5$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
4					4	-5

$$\begin{aligned} s_0 &= 1 & s_1 &= 0 \\ t_0 &= 0 & t_1 &= 1 \end{aligned}$$

$$\begin{aligned} t_j &= t_{j-2} - q_{j-1}t_{j-1} \\ t_4 &= t_2 - q_3t_3 \\ t_4 &= -1 - (4) = -5 \end{aligned}$$

Methods of Finding The gcd (6/6)

$$\gcd(a, b) = sa + tb$$

Example 2 – Solution

$$s_j = s_{j-2} - q_{j-1}s_{j-1} \quad \text{and} \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198 using the extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
4					4	-5

The Bezout coefficients of a and b are:

$$s_4 = 4 \quad \text{and} \quad t_4 = -5$$

Then:

$$\begin{aligned} \gcd(252, 198) \\ = (4)(252) + (-5)(198) \end{aligned}$$

Applications (1/4)

1. Hashing Functions
2. Pseudorandom Numbers
3. Cryptography
- ...

Applications (2/4)

1. Hashing Functions

$$h(k) = k \bmod m$$

Find the memory locations assigned by the hashing function $h(k) = k \bmod 111$ to the records of customers with Social Security numbers 064212848 and 037149212.

Solution: The record of the customer with Social Security number 064212848 is assigned to memory location 14, because

$$h(064212848) = 064212848 \bmod 111 = 14.$$

Similarly, because

$$h(037149212) = 037149212 \bmod 111 = 65,$$

the record of the customer with Social Security number 037149212 is assigned to memory location 65.



Applications (3/4)

2. Pseudorandom Numbers

linear congruential method

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

modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.

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

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

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

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

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

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

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

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

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

Applications (4/4)

3. Cryptography

m is the number of elements in the language used.

Classical Cryptography

$$f(p) = (p + k) \bmod m.$$

Encryption

$$f^{-1}(p) = (p - k) \bmod m.$$

k is called a **key**

Decryption

Solution: To encrypt the message “STOP GLOBAL WARMING” we first translate each letter to the corresponding element of \mathbf{Z}_{26} . This produces the string

18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6.

We now apply the shift $f(p) = (p + 11) \bmod 26$ to each number in this string. We obtain

3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.

Translating this last string back to letters, we obtain the ciphertext “DEZA RWZMLW HLCX-TYR.”