

# Number Theory and Cryptography

## Chapter 4

With Question/Answer Animations

# Chapter Motivation

- *Number theory* is the part of mathematics devoted to the study of the integers and their properties.
- Key ideas in number theory include divisibility and the primality of integers.
- Representations of integers, including binary and hexadecimal representations, are part of number theory.
- Number theory has long been studied because of the beauty of its ideas, its accessibility, and its wealth of open questions.
- We'll use many ideas developed in Chapter 1 about proof methods and proof strategy in our exploration of number theory.
- Mathematicians have long considered number theory to be pure mathematics, but it has important applications to computer science and cryptography studied in Sections 4.5 and 4.6.



# Chapter Summary

- Divisibility and Modular Arithmetic
- Integer Representations and Algorithms
- Primes and Greatest Common Divisors
- Solving Congruences
- Applications of Congruences
- Cryptography

# Divisibility and Modular Arithmetic

Section 4.1

# Section Summary

- Division ✓
- Division Algorithm ✓
- Modular Arithmetic ✓

$a \mid b$  نقسم  
 $a \nmid b$  لا نقسم  
 $b/a$  مضروب

$a$  قاسم لـ  $b$   
 $b$  مضاعفات  $a$

# Division

قابلية القسمة

**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  $a$ .

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

● If  $a \mid b$ , then  $b/a$  is an integer. إذا كانت  $a$  تقسم  $b$  فإن  $b$  تقبل متبقية على  $a$  دون باقى

● If  $a$  does not divide  $b$ , we write  $a \nmid b$ .

**Example:** Determine whether  $3 \mid 7$  and whether

$3 \mid 12$ .

$$\begin{array}{r} 4 \\ 3 \overline{) 12} \\ \underline{12} \\ 0 \end{array}$$
 $r = 0$   
 $3 \mid 12$



$$\begin{array}{r} 2 \\ 3 \overline{) 7} \\ \underline{6} \\ 1 \end{array}$$
 $r = 1$   
 $3 \nmid 7$

$$\begin{array}{|c|c|c|} \hline 3 & 3 & 1 \\ \hline \end{array}$$
 $3 \nmid 7$

$a$  divides  $b$   
 $a \mid b$

$a$  تقسم  $b$



$7m$

$2 \nmid 7$

2 لا تقسم 7



$8m$

$2 \mid 8$

2 تقسم 8

$a \mid b$   
 $2 \mid 8$

$b$  يقبل القسمة على  $a$  دون باقى  
 $8 \div 2 = 4$        $4 \times 2 = 8$

$a$  تقسم  $b$        $a \mid b$   
 $b$  تقسم  $a$        $b \mid a$

$b \div a = c$

$ca = b$

Proof

اثبات قاعدة 1

If  $\underline{a \mid b}$  and  $\underline{a \mid c}$  then  $a \mid b+c$

①  $(a \mid b) \Rightarrow b = sa$        $(a \mid c) \Rightarrow c = ta$

②  $b = sa$

$b+c = a(t+s)$

$c = ta$

③

$b+c = a(t+s)$

$a \mid b+c$

# 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  $a \mid (b + c)$ ; (i)  $2 \mid 8$  and  $2 \mid 10 \Rightarrow 2 \mid 18$
- ii. If  $a \mid b$ , then  $a \mid bc$  for all integers  $c$ ; (ii)  $2 \mid 8$ ,  $2 \mid (8 \cdot 3) \Rightarrow 2 \mid 24$
- iii. If  $a \mid b$  and  $b \mid c$ , then  $a \mid c$ .  $2 \mid 8$     $8 \mid 40$     $2 \mid 40$

**Proof:** (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,

$$b + c = as + at = a(s + t). \quad \text{Hence, } a \mid (b + c)$$

(Exercises 3 and 4 ask for proofs of parts (ii) and (iii).) ◀

**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.

Can you show how it follows easily from from (ii) and (i) of Theorem 1?

$$2 \mid 4 \quad \text{and} \quad 2 \mid 6 \quad \text{then} \quad 2 \mid n(4) + m(6) \\ 2 \mid 3 \cdot 4 + 2 \cdot 6$$

# Division Algorithm

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

ناجی القسمة

**Division Algorithm:** 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  $a = dq + r$  (proved in Section 5.2).

$$\begin{array}{r} 3 \\ 4 \overline{) 13} \\ \underline{12} \\ 1 \end{array}$$

- $d$  is called the divisor.
- $a$  is called the dividend.
- $q$  is called the quotient.
- $r$  is called the remainder.

مقسوم عليه  
المقسوم  
الناجی  
الباقی

Definitions of Functions  
**div** and **mod**

$$\begin{aligned} \text{الناجی} \quad q &= a \text{ div } d \\ \text{الباقی} \quad r &= a \text{ mod } d \end{aligned}$$

## Examples:

- ① ● What are the quotient and remainder when 101 is divided by 11?

**Solution:** The quotient when 101 is divided by 11 is 9 = 101 **div** 11, and the remainder is 2 = 101 **mod** 11.

$$\begin{aligned} 101 \text{ div } 11 &= 9 \\ 101 \text{ mod } 11 &= 2 \end{aligned}$$

- ② ● What are the quotient and remainder when -11 is divided by 3?

**Solution:** The quotient when -11 is divided by 3 is -4 = -11 **div** 3, and the remainder is 1 = -11 **mod** 3.

$$\begin{aligned} -11 \text{ div } 3 &= -4 \\ -11 \text{ mod } 3 &= 1 \end{aligned}$$



$$\begin{array}{r} q \\ d \overline{) a} \\ \hline r \end{array}$$

$$\begin{array}{r} 5 \\ 5 \overline{) 27} \\ \underline{25} \\ 2 \end{array}$$

$$d = 5$$

$$a = 27$$

$$r = 2$$

$$q = 5$$

$$13 \div 5$$

$$\begin{array}{r} 2 \\ 5 \overline{) 13} \\ \underline{10} \\ 3 \end{array}$$

$$a = dq + r$$

$$r = a - dq$$

$$r = 13 - 2(5) = 13 - 10 = 3$$

الحاسبة

$$\frac{13}{5} = \lfloor 2.6 \rfloor = 2$$

$$r = 13 - 5(2) = 3$$

الباقي  $r$  من  $div$

ال몫  $q$  من  $mod$

الباقي  
الباقي

$$\begin{array}{l} a \div d = q \\ a \bmod d = r \end{array}$$

101 و 11

ما باقي وناتج قسمة

$$\begin{array}{r} 9 \\ 11 \overline{) 101} \\ \underline{99} \\ 2 \end{array}$$

$$a = 101$$

$$d = 11$$

$$q = 9$$

$$r = 2$$

$$q = 101 \div 11 = \lfloor 9.18 \rfloor = 9$$

$$r = a - qd = 101 - 9(11) \\ r = 2$$

-11 و 3

ما باقي وناتج قسمة

$$q = -\frac{11}{3} = \lfloor -3.6 \rfloor = -4$$

$$r = a - qd = -11 - (-4)3 \\ r = 1$$

$$\begin{array}{r} -4 \\ 3 \overline{) -11} \\ \underline{-12} \\ 1 \end{array}$$

$$q = -4$$

$$r = 1$$

## Examples

1) Does 2 divides 4? ✓

$$2 \mid 4 \quad \checkmark$$

2) Does 2 divides 8? ✓

$$2 \mid 8 \quad \checkmark$$

3) 2 divides  $(4 + 8)$ ? ✓

$$2 \mid 12 \quad \checkmark$$

4) Does 2 divides 4?

5) Does 2 divides  $4 * 5$ ?

$$2 \mid 4.5$$

6) Does 2 divides  $4 * 4$ ?

$$2 \mid 4.4$$

7) Does 2 divides 4?

$$2 \mid 4$$

$$4 \mid 8$$

$$2 \mid 16$$

8) Does 4 divides 16?

9) Does 2 divides 16?

Evaluate:

باني قسمة 11 على 2

$$\triangleright \underline{11 \bmod 2 = 1}$$

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

$$\begin{array}{r} 5 \\ 2 \overline{) 11} \\ \underline{10} \\ 1 \end{array}$$

$$r = 1$$

$$\triangleright \underline{-11 \bmod 2 = 1}$$

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

$$\begin{array}{r} -6 \\ 2 \overline{) -11} \\ \underline{-12} \\ 1 \end{array}$$

# 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  $a - b$ .

- 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.
- Two integers are congruent mod  $m$  if and only if they have the same remainder when divided by  $m$ .
- 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 and whether 24 and 14 are congruent modulo 6.  $17 \equiv 5 \pmod{6} \quad ??$   
 $24 \equiv 14 \pmod{6}$

**Solution:**

- $17 \equiv 5 \pmod{6}$  because 6 divides  $17 - 5 = 12$ .  $6 \mid (17-5)$
- $24 \not\equiv 14 \pmod{6}$  since  $24 - 14 = 10$  is not divisible by 6.

$$6 \nmid (24-14)$$
$$6 \nmid (10)$$

جميع الأعداد  
 $16 \bmod 5 = 1$   
 $21 \bmod 5 = 1$   
 $26 \bmod 5 = 1$   
 $31 \bmod 5 = 1$   
 16 و 21 و 26 و 31  
 تتطابق باقي القسمة  
 على العدد 5

$$16 \bmod 5 \equiv 26 \bmod 5$$

$$a \bmod m \equiv b \bmod m$$

$$a - b = 26 - 16 = 10$$

$$5 \mid 10 \checkmark$$

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

لتعبير عن تطابق modulo

$$a \equiv b \pmod{m}$$

$$26 \equiv 16 \pmod{5}$$

$$a \equiv b \pmod{m}$$

$$a \bmod m \equiv b \bmod m$$

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

Example  $17 \equiv 5 \pmod{6} \checkmark$

طريق 1

$$17 \bmod 6 = 5 \bmod 6$$

$$5 = 5$$

$$\begin{array}{r} 2 \\ 6 \overline{) 17} \\ \underline{12} \\ 5 \end{array}$$

$$\begin{array}{r} 0 \\ 6 \overline{) 5} \\ \underline{0} \\ 5 \end{array}$$

طريق 2

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

$$17 - 5 = 12$$

$$6 \mid 12 \checkmark$$

$$24 \not\equiv 14 \pmod{6}$$

$$6 \nmid (24 - 14) \quad \begin{array}{r} 10 \\ 6 \overline{) 10} \\ \underline{6} \\ 4 \end{array}$$

# More on Congruences

**Theorem 4:** Let  $\overset{5}{\underline{m}}$  be a positive integer. The integers  $\overset{16}{\underline{a}}$  and  $\overset{25}{\underline{b}}$  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 the 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  $a \equiv b \pmod{m}$ . ◀

Proof

$$a \equiv b \pmod{m}$$

def of congruence

$$m \mid a - b$$

def of division

$$a - b = km$$

$$\boxed{a = km + b}$$

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

\* 17

$$17 \equiv 5 \pmod{6}$$

✓

$$\begin{array}{l} ? \\ m \mid a - b \\ 6 \mid (17 - 5) \quad 6 \mid 12 \end{array}$$

\* 24

$$24 \not\equiv 5 \pmod{6}$$

$$\begin{array}{l} ? \\ 6 \mid (24 - 5) \quad 6 \mid 19 \quad \times \end{array}$$

Find each of these values.

a)  $(-133 \pmod{23} + 261 \pmod{23}) \pmod{23}$

$$(a \pmod{m} + b \pmod{m}) \pmod{m}$$

$$(a + b) \pmod{m}$$

$$(-133 + 261) \pmod{23}$$

$$128 \pmod{23}$$

$$= 13$$

$$\begin{array}{r} 5 \\ 23 \overline{) 128} \\ \underline{115} \\ 13 \end{array}$$

$r = 13$

$$26 \equiv 16 \pmod{5}$$

$$26 \bmod 5 = 1$$

# The Relationship between $(\bmod m)$ and $\bmod m$ Notations

- The use of “mod” in  $a \equiv b \pmod{m}$  and  $a \bmod m = b$  are different.
- $a \equiv b \pmod{m}$  is a relation on the set of integers. انعام
- In  $a \bmod m = b$ , the notation **mod** denotes a function. دالة
- The relationship between these notations is made clear in this theorem.
- **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  $a \bmod m = b \bmod m$ . (Proof in the exercises)



$$8 \equiv 5 \pmod{3}$$

$$8+2 \equiv 5+2 \pmod{3}$$

$$10 \equiv 7 \pmod{3} \checkmark$$

$$16 \equiv 10 \pmod{3} \checkmark$$

# 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

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

**Proof:**

$$\checkmark b = a + sm \quad d = c + tm \checkmark$$

- 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,

- $$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t) \text{ and } a + c \equiv b + d \pmod{m}$$
- $$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

- 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 from Theorem 5 that

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

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

$$18 \equiv 3 \pmod{5}$$

$$77 \equiv 2 \pmod{5}$$

$$a = b \pmod{m}$$

في حالة اضافة رقم صحيح الى  $a$  ،  $b$   
في حالة ضرب رقم صحيح بـ  $a$  ،  $b$   
تبقى الجملة صحيحة

$$7 = 2 \pmod{5}$$

$$7+3 = 2+3 \pmod{5}$$

✓ نتيجة 3

$$10 = 5 \pmod{5}$$

$$7 = 2 \pmod{5}$$

✓ مثلا ضرب بـ 2

$$14 = 4 \pmod{5}$$

$$a \equiv b \pmod{m}$$

✓

$$c \equiv d \pmod{m}$$

$$a+c \equiv b+d \pmod{m}$$

يكرر جمع هاتين الصيغتين

$$7 = 2 \pmod{5}$$

$$11 = 1 \pmod{5}$$


---


$$18 = 3 \pmod{5}$$

✓ 5/15

✓ يكرر ضرب هاتين

$$7 = 2 \pmod{5}$$

$$11 = 1 \pmod{5}$$


---


$$77 = 2 \pmod{5}$$

5/75

# Algebraic Manipulation of Congruences

الضرب برقم صحيح يحافظ على صحة متطابقة

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

If  $a \equiv b \pmod{m}$  holds then  $\underline{c \cdot a} \equiv \underline{c \cdot b} \pmod{m}$ , where  $c$  is any integer, holds by Theorem 5 with  $d = c$ .

إضافة رقم صحيح يحافظ على صحة المتطابقة

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

If  $a \equiv b \pmod{m}$  holds then  $\underline{c + a} \equiv \underline{c + b} \pmod{m}$ , where  $c$  is any integer, holds by Theorem 5 with  $d = c$ .

- Dividing a congruence by an integer does not always produce a valid congruence.

قسمة المتطابقة على عدد صحيح لا يحافظ على صحتها

**Example:** The congruence  $14 \equiv 8 \pmod{6}$  holds. But dividing both sides by 2 does not produce a valid congruence since  $14/2 = 7$  and  $8/2 = 4$ , but  $7 \not\equiv 4 \pmod{6}$ .

See Section 4.3 for conditions when division is ok.

$$\frac{14}{2} \equiv \frac{8}{2} \pmod{6}$$

$$7 \not\equiv 4 \pmod{6}$$

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

- We use the following corollary to Theorem 5 to compute the remainder of the product or sum of two integers when divided by  $m$  from the remainders when each is divided by  $m$ .

**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

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

*(proof in text)*

مناد

# Arithmetic Modulo $m$

**Definitions:** Let  $\mathbf{Z}_m$  be the set of nonnegative integers less than  $m$ :  $\{0, 1, \dots, m-1\}$

- The operation  $+_m$  is defined as  $a +_m b = (a + b) \bmod m$ . This is *addition modulo  $m$* .
- The operation  $\cdot_m$  is defined as  $a \cdot_m b = (a \cdot b) \bmod m$ . This is *multiplication modulo  $m$* .
- Using these operations is said to be doing *arithmetic modulo  $m$* .

**Example:** Find  $7 +_{11} 9$  and  $7 \cdot_{11} 9$ .

**Solution:** Using the definitions above:

- $7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

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

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

طريقة اخرى

$$\begin{aligned} & (a + b) \bmod m \\ & a +_m b \\ & (17 + 5) \bmod 6 \\ & = 17_6 + 5 \end{aligned}$$

# Arithmetic Modulo $m$

- The operations  $+_m$  and  $\cdot_m$  satisfy many of the same properties as ordinary addition and multiplication.
- Closure: If  $a$  and  $b$  belong to  $\mathbb{Z}_m$ , then  $a +_m b$  and  $a \cdot_m b$  belong to  $\mathbb{Z}_m$ .  *$a$  و  $b$  تنتمي الى  $\mathbb{Z}_m$  اذا الجمع احصا ينتميا  $\mathbb{Z}_m$*
- Associativity: If  $a$ ,  $b$ , and  $c$  belong to  $\mathbb{Z}_m$ , then  $(a +_m b) +_m c = a +_m (b +_m c)$  and  $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$ . *تجميعية*
- Commutativity: If  $a$  and  $b$  belong to  $\mathbb{Z}_m$ , then  $a +_m b = b +_m a$  and  $a \cdot_m b = b \cdot_m a$ . *تبديل*
- Identity elements: The elements  $0$  and  $1$  are identity elements for addition and multiplication modulo  $m$ , respectively. *عنصري هوية*
- If  $a$  belongs to  $\mathbb{Z}_m$ , then  $a +_m 0 = a$  and  $a \cdot_m 1 = a$ .

*عنصري هوية الجمع 0*

*عنصري هوية الضرب 1*  
continued →

# Arithmetic Modulo $m$

معكوس عكسي

$$\begin{array}{l} 3 \rightarrow -3 = 0 \\ -5 \rightarrow 5 = 0 \end{array}$$

● 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  $0 +_m 0 = 0$

$$a \Rightarrow m - a$$

● Distributivity: If  $a$ ,  $b$ , and  $c$  belong to  $\mathbf{Z}_m$ , then

$$a +_m (m - a) = 0$$

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

$$\begin{array}{l} 2 \rightarrow \frac{1}{2} \\ \frac{3}{4} \rightarrow \frac{4}{3} \end{array}$$

● Exercises 42-44 ask for proofs of these properties.

● Multiplicative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.

لم يتم ذكره

● (optional) Using the terminology of abstract algebra,  $\mathbf{Z}_m$  with  $+_m$  is a commutative group and  $\mathbf{Z}_m$  with  $+_m$  and  $\cdot_m$  is a commutative ring.

معكوس عكسي



تمثيل الأعداد الصحيحة

# Integer Representations and Algorithms

Section 4.2

# Section Summary

- Integer Representations ✓
  - Base  $b$  Expansions
  - Binary Expansions
  - Octal Expansions
  - Hexadecimal Expansions
- Base Conversion Algorithm
- Algorithms for Integer Operations

$$965 = 5 + 60 + 900 \\ = 5 \times 10^0 + 6 \times 10^1 + 9 \times 10^2$$

حرف تمثيل الأعداد العشرية

# Representations of Integers

- In the modern world, we use decimal, or base 10, notation to represent integers. For 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 bases  $b = \underline{2}$  (binary),  $b = \underline{8}$  (octal), and  $b = \underline{16}$  (hexadecimal) are important for computing and communications
- The ancient Mayans used base 20 and the ancient Babylonians used base 60.

$$(183)_u = 3 \times 4^0 + 8 \times 4^1 + 1 \times 4^2$$

$$n = a_0 \times b^0 + a_1 b^1 + a_2 b^2 \dots$$

# Base $b$ Representations

$$\underline{a_n} \quad \underline{a_3} \quad \underline{a_2} \quad \underline{a_1} \quad \underline{a_0}$$

$b$  الأساس :- عدد صحيح أكبر من 1

- We can use positive integer  $b$  greater than 1 as a base, because of this theorem:

**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:

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

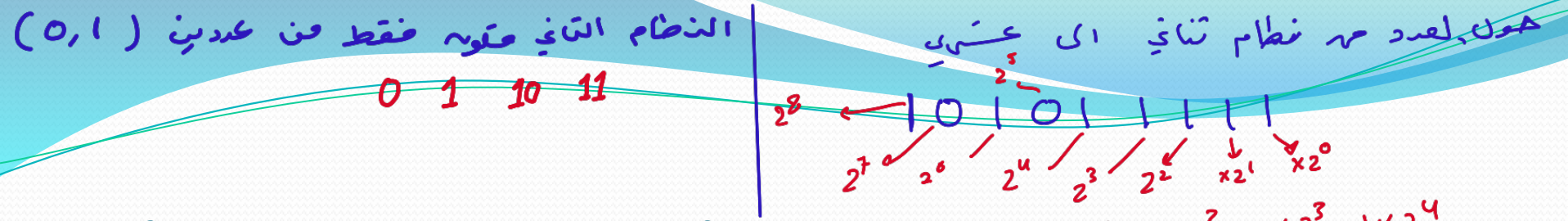
where  $k$  is a nonnegative integer,  $a_0, a_1, \dots, a_k$  are nonnegative integers less than  $b$ , and  $a_k \neq 0$ . The  $a_j, j = 0, \dots, k$  are called the base- $b$  digits of the representation.

(We will prove this using mathematical induction in Section 5.1.)

- 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.

نظام الثمانية (231)<sub>8</sub>  
نظام الثنائي (101)<sub>2</sub>

في النظام العشري لا يكتب رقم (10)



# 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:** What is the decimal expansion of the integer that has  $(1\ 0101\ 1111)_2$  as its binary expansion?

**Solution:**

$$(1\ 0101\ 1111)_2 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 351$$

**Example:** What is the decimal expansion of the integer that has  $(11011)_2$  as its binary expansion?

**Solution:**  $(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 27$

2<sup>4</sup> 2<sup>3</sup> 2<sup>2</sup> 2<sup>1</sup> 2<sup>0</sup>

1 1 0 1 1

$= 1 \times 2^0 + 1 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 + 1 \times 2^4 = 1 + 2 + 0 + 8 + 16 = 27$

ميكو، لنظام الثماني ص ٨ ع ١

0 1 2 3 4 5 6 7 10

# Octal Expansions

مثاني

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

**Example:** What is the decimal expansion of the number with octal expansion  $(7016)_8$ ?  $= 6 \times 8^0 + 1 \times 8^1 + 0 \times 8^2 + 7 \times 8^3$   
 $= 6 + 8 + 0 + 3584$

**Solution:**  $7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$   
 $= 3598$

**Example:** What is the decimal expansion of the number with octal expansion  $(111)_8$ ?

**Solution:**  $1 \cdot 8^2 + 1 \cdot 8^1 + 1 \cdot 8^0 = 64 + 8 + 1 = 73$

$$1 \times 8^0 + 1 \times 8^1 + 1 \times 8^2 = 1 + 8 + 64 = 73$$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

# Hexadecimal Expansions

The hexadecimal expansion needs 16 digits, but our decimal system provides only 10. So letters are used for the additional symbols. 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.

**Example:** What is the decimal expansion of the number with hexadecimal expansion  $(2AE0B)_{16}$  ?

**Solution:**

$$2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627$$

**Example:** What is the decimal expansion of the number with hexadecimal expansion  $(E5)_{16}$  ?

**Solution:**  $14 \cdot 16^1 + 5 \cdot 16^0 = 224 + 5 = 229$

$$\begin{aligned} &= 5 \times 16^0 + E \times 16^1 = 5 + 14 \times 16 \\ &= 5 + 224 \\ &= 229 \end{aligned}$$

$$\rightarrow \cancel{8} \times 16^0 + 0 \times 16^1 + \cancel{E} \times 16^2 + \cancel{A} \times 16^3 + 2 \times 16^4 = 175627$$

11                      14                      10



تحويل الأساس

$$\begin{array}{r} q_0 \\ b \overline{) n} \\ \underline{a_0} \end{array}$$

$$n = bq_0 + a_0$$

# Base Conversion

To construct the base  $b$  expansion of an integer  $n$ :

- Divide  $n$  by  $b$  to obtain a quotient and remainder.

$$\underline{n = bq_0 + a_0} \quad 0 \leq a_0 \leq b$$

- The remainder,  $\underline{a_0}$ , is the rightmost digit in the base  $b$  expansion of  $n$ . Next, divide  $\underline{q_0}$  by  $\underline{b}$ .

$$\underline{q_0 = bq_1 + a_1} \quad 0 \leq a_1 \leq b$$

- The remainder,  $a_1$ , is the second digit from the right in the base  $b$  expansion of  $n$ .

- Continue by successively dividing the quotients by  $b$ , obtaining the additional base  $\underline{b}$  digits as the remainder. The process terminates when the quotient is 0.

توقف العملية عندما يصبح الباقي = 0

continued →

لتحويل أي عدد عشر  $n$  إلى عدد أساسه  $b$

نقسم العدد  $n$  على  $b$

	$\div b$	$r$
$n$	$q_0$	$a_0$
$q_0$	$q_1$	$a_1$
$q_1$	$q_2$	$a_2$
	$\vdots$	$a_3$
	$0$	$a_n$

ثم نكرر الخطوات بـ  $q_0$  على  $b$   
الناتج الأول  $q_0$  على  $b$

ونكرر الخطوات بنصف  
الطريقة حتى نصل  
إلى ناتج  $0$

نكتب العدد الناتج حسب الترتيب التالي  $(a_n a_{n-1} a_{n-2} a_{n-3})_b$

هول الحرقم 25 إلى النظام الثنائي ( $b=2$ )

	$\div 2$	$r$
25	12	1
12	6	0
6	3	0
3	1	1
1	0	1

1 1 0 0 1

$(11001)_2$

# Algorithm: Constructing Base $b$ Expansions

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

*Handwritten notes:* Red arrows point from  $n$  to 25 and from  $b$  to 2. Three red horizontal lines are drawn to the right of the loop body.

- $q$  represents the quotient obtained by successive divisions by  $b$ , starting with  $q = n$ .
- The digits in the base  $b$  expansion are the remainders of the division given by  $q \bmod b$ . *الموافي*
- The algorithm terminates when  $q = 0$  is reached.

# Base Conversion

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

**Solution:** Successively dividing by 8 gives:  $\div 8$

●  $12345 = 8 \cdot 1543 + 1$

●  $1543 = 8 \cdot 192 + 7$

●  $192 = 8 \cdot 24 + 0$

●  $24 = 8 \cdot 3 + 0$

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

$$\begin{array}{r} 24 \\ 8 \overline{) 192} \\ \underline{16} \phantom{0} \\ 32 \\ \underline{32} \\ 0 \end{array}$$

gives:  $\div 8$

		mod
12345	1543	1
1543	192	7
192	24	0
24	3	0
3	0	3

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

$$\begin{array}{ccccc} \underline{3} & \underline{0} & \underline{0} & \underline{7} & \underline{1} \\ (30071)_8 \end{array}$$

# 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. — — — —
- So, conversion between binary, octal, and hexadecimal is easy.

## Conversion of binary to decimal ( base 2 to base 10)

Example: convert  $(1011)_2$  to its decimal equivalent

$$= 2^0 \times 1 + 2^1 \times 1 + 2^2 \times 0 + 2^3 \times 1 = 11$$

Example2: convert  $(1000100)_2$  to its decimal equivalent

$$2^0 \times 0 + 2^1 \times 0 + 2^2 \times 1 + 2^3 \times 0 + 2^4 \times 0 + 2^5 \times 0 + 2^6 \times 1 = 68$$

## Conversion of decimal to binary ( base 10 to base 2)

Example: convert  $(68)_{10}$  to binary

86	34	0
34	17	0
17	8	1
8	4	0
4	2	0
2	1	0
1	0	1

$(1000100)_2$

Answer = 1 0 0 0 1 0 0

## Octal Number System

- 1 octal digit is equivalent to 3 bits — — —
- Octal numbers are 0 to 7.
- Numbers are expressed as powers of 8.

### Conversion of octal to decimal ( base 8 to base 10)

Example: convert  $(632)_8$  to decimal

$$2 \times 8^0 + 3 \times 8^1 + 6 \times 8^2 = (410)_{10}$$

### Conversion of decimal to octal ( base 10 to base 8)

Example: convert  $(177)_{10}$  to octal equivalent  $\div 8$

177	22	1
22	2	6
2	0	2

$$\begin{array}{r} 2 \\ 8 \overline{) 22} \\ \underline{16} \\ 6 \end{array}$$

$$(261)_8$$



# Hexadecimal Number System

- 1 hex digit is equivalent to 4 bits. — — — —

- Numbers are 0,1,2.....8,9, A, B, C, D, E, F.

B is 11, E is 14

- Numbers are expressed as powers of 16.

- $16^0 = 1$ ,  $16^1 = 16$ ,  $16^2 = 256$ ,  $16^3 = 4096$ ,  $16^4 = 65536$ , ...

## Conversion of hex to decimal ( base 16 to base 10)

Example: convert  $(F4C)_{16}$  to decimal

$$= \overset{12}{\cancel{C}} \times 16^0 + 4 \times 16^1 + \overset{15}{\cancel{F}} \times 16^2$$
$$12 + 4 \times 16 + 15 \times 256 =$$

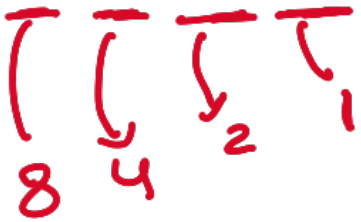
## Conversion of decimal to hex ( base 10 to base 16)

Example: convert  $(4768)_{10}$  to hex.  $\div 16$

4768	298	0
298	18	<del>10</del> A
18	1	2
1	0	1

$(12A0)_{16}$

# Conversion Between Binary, Octal, and Hexadecimal Expansions



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

**Solution:**

$$\begin{array}{cccccc} 11 & 1110 & 1011 & 1100 & & \\ \hline 011 & 111 & 010 & 111 & 100 & \\ 3 & 7 & 2 & 7 & 4 & \end{array} = (37274)_8$$

- To convert to octal, we group the digits into blocks of three  $(011\ 111\ 010\ 111\ 100)_2$ , adding initial 0s as needed. The blocks from left to right correspond to the digits 3, 7, 2, 7, and 4. Hence, the solution is  $(37274)_8$ .
- To convert to hexadecimal, we group the digits into blocks of four  $(0011\ 1110\ 1011\ 1100)_2$ , adding initial 0s as needed. The blocks from left to right correspond to the digits 3, E, B, and C. Hence, the solution is  $(3EBC)_{16}$ .

$$\begin{array}{cccc} 0011 & 1110 & 1011 & 1100 \\ \hline 0011 & 1110 & 1011 & 1100 \\ 3 & 14 & 11 & 12 \\ 3 & E & B & C \end{array} = (3EBC)_{16}$$

## From Binary to Octal

Starting at the binary point and working left, separate the bits into groups of **three** and replace each group with the corresponding **octal** digit.

$$\underline{0}\underline{1000}\underline{1011}_2 = \overset{\text{2}}{010} \overset{\text{1}}{001} \overset{\text{21}}{011} = 213_8$$

2    1    3

## From Binary to Hexadecimal

Starting at the binary point and working left, separate the bits into groups of **four** and replace each group with the corresponding **hexadecimal** digit.

$$\underline{1000}\underline{1011}_2 = \overset{\text{8}}{1000} \overset{\text{8 21}}{1011} = 8\text{B}_{16}$$

8    ~~8~~  
B

## From Octal to Binary

Replace each **octal** digit with the corresponding **3-bit** binary string.

$$213_8 = 010 \ 001 \ 011 = 10001011_2$$

0 1 0    0 0 1    0 1 1

## From Hexadecimal to Binary

Replace each **hexadecimal** digit with the corresponding **4-bit** binary string.

$$8\text{B}_{16} = 1000 \ 1011 = 10001011_2$$

1 0 0 0    1 0 1 1

جميع الاعداد في النظام الثنائي

# Binary Addition of Integers

- Algorithms for performing operations with integers using their binary expansions are important as computer chips work with binary numbers. Each digit is called a bit.

```
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  $n - 1$ 
     $d := \lfloor (a_j + b_j + c) / 2 \rfloor$ 
     $s_j := a_j + b_j + c - 2d$ 
     $c := d$ 
 $s_n := c$ 
return  $(s_0, s_1, \dots, s_n)$  {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  $O(n)$ .

# Binary Addition

$$\begin{array}{r} 0 \\ + 0 \\ \hline 0 \end{array} \quad \begin{array}{r} 0 \\ + 1 \\ \hline 1 \end{array} \quad \begin{array}{r} 1 \\ + 1 \\ \hline 10 \end{array} \quad \begin{array}{r} 1 \\ + 1 \\ \hline 11 \end{array}$$

$$\begin{array}{r} 110 + 111 \\ \hline 1101 \end{array}$$

$(1101)_2$

$$\begin{array}{r} a_j \dots a_2 a_1 a_0 \\ a_j \dots b_2 b_1 b_0 \\ \hline s_j \dots s_2 s_1 s_0 \end{array}$$

$$s_j = a_j + b_j + c - 2d$$

$$\begin{array}{r} a \\ + b \\ \hline s \end{array}$$

$a_j$	$b_j$	$c$	$d$	$s_j$
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

حزب الخلافة السنية


$$\begin{array}{r} 110 \\ \times 101 \\ \hline 110 \\ 0000 \\ 11000 \\ \hline 11110 \end{array}$$

ضرب الاعداد في النظام الثنائي

# Binary Multiplication of Integers

- Algorithm for computing the product of two  $n$  bit 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  $c_j = a$  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  $n - 1$ 
     $p := p + c_j$ 
return  $p$  { $p$  is the value of  $ab$ }
```



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

$$b^n \bmod m$$

$$2^3 \bmod 5$$

$$8 \bmod 5 = 3$$

$$\frac{1}{5} \sqrt[5]{8} = \frac{1}{5} \sqrt[5]{3^5} = \frac{1}{5} \cdot 3 = \frac{3}{5}$$

# 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:  $b^n = b^{a_{k-1} \cdot 2^{k-1} + \dots + a_1 \cdot 2 + a_0} = b^{a_{k-1} \cdot 2^{k-1}} \dots b^{a_1 \cdot 2} \cdot b^{a_0}$   
حساب توان به کمک سیستم دودویی  
برای محاسبه توان، ما توانهای کوچکتر را محاسبه میکنیم و آنها را در هم ضرب میکنیم.
- Therefore, to compute  $b^n$ , we need only compute the values of  $b$ ,  $b^2$ ,  $(b^2)^2 = b^4$ ,  $(b^4)^2 = b^8$ , ...,  $b^{2^k}$  and then multiply the terms  $b^{2^j}$  in this list, where  $a_j = 1$ .

3<sup>11</sup> | 11 → binary

11	5	1
5	2	1
2	1	0
1	0	1

1011

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

**Solution:** Note that  $11 = (1011)_2$  so that  $3^{11} = 3^8 \cdot 3^2 \cdot 3^1 = ((3^2)^2)^2 \cdot 3^2 \cdot 3^1 = (9^2)^2 \cdot 9 \cdot 3 = (81)^2 \cdot 9 \cdot 3 = 6561 \cdot 9 \cdot 3 = 117,147$ .

$$3^{(1011)_2} = 3^8 \cdot 3^2 \cdot 3^1 = ((3^2)^2)^2 \cdot 3^2 \cdot 3^1 = 117147$$

continued →



$$2^7 = 2^{(111)} = 2^4 \cdot 2^2 \cdot 2^1 = 16 \times 8 = 128$$

$$\begin{array}{r|rr} 7 & 3 & 1 \\ 3 & 1 & 1 \\ \hline 1 & 0 & 1 \end{array} \quad \underline{\quad} \quad \underline{\quad} \quad \underline{\quad}$$

# Binary Modular Exponentiation Algorithm

$$\overline{8} \quad \overline{4} \quad \overline{2} \quad \overline{1}$$

- The algorithm successively finds  $b \bmod m$ ,  $b^2 \bmod m$ ,  $b^4 \bmod m$ , ...,  $b^{2^{k-1}} \bmod m$ , and multiplies together the terms  $b^{2^j}$  where  $a_j = 1$ .

$$b^1 \cdot b^2 \cdot b^4 \cdot b^8 \Rightarrow b^{2^{k-1}}$$

**procedure** modular exponentiation ( $b$ : integer,  $n = (a_{k-1}a_{k-2}\dots a_1a_0)_2$ ,  $m$ : positive integers)

$x := 1$

$\text{power} := \underline{b \bmod m}$

**for**  $i := 0$  to  $k - 1$

**if**  $a_i = 1$  **then**  $\underline{x} := (\underline{x} \cdot \underline{\text{power}}) \bmod m$

$\underline{\text{power}} := (\underline{\text{power}} \cdot \underline{\text{power}}) \bmod m$

**return**  $x$  {  $x$  equals  $b^n \bmod m$  }

$$2^3 \bmod 4$$

تبدیل بیت  
n

تبدیل بیت  
m

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

الوقت المستغرق لحساب  $b^n \bmod m$  يعتمد على عدد البتات

الاعداد الأولية

GCD  
القاسم المشترك الأكبر

# Primes and Greatest Common Divisors

Section 4.3

# Section Summary

- Prime Numbers and their Properties
- Conjectures and Open Problems About Primes
- Greatest Common Divisors and Least Common Multiples
- The Euclidian Algorithm
- gcds as Linear Combinations

Prime :- يقسم فقط على نفسه وعلى 1  
Composite : يقسم على أكثر من ذلك

الأعداد الأولية

# Primes

2, 3, 5, 7, 11, 13, 17, 19, 23, 29

**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, but 9 is composite because it is divisible by 3.

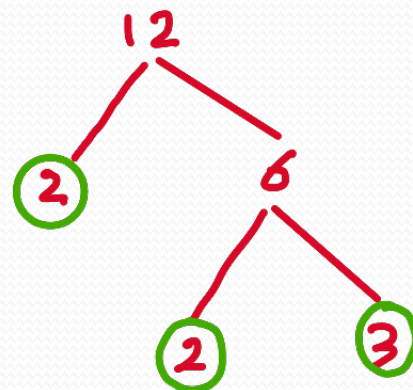
# The Fundamental Theorem of Arithmetic

ای عدد موجب اکبر من واحد یکن کتابة می سکتان  
حاصل ضربا عدد ۴، لا عدد الا و لیه

**Theorem:** Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

## Examples:

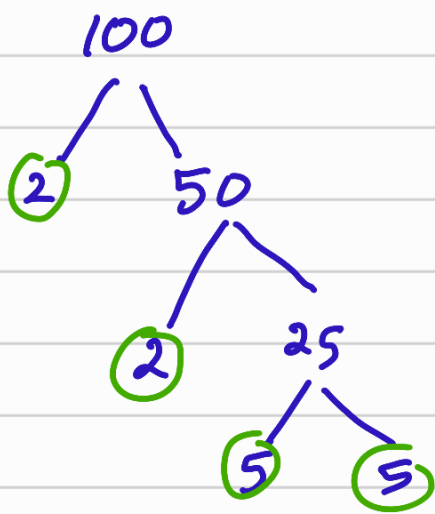
- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $641 = 641$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$



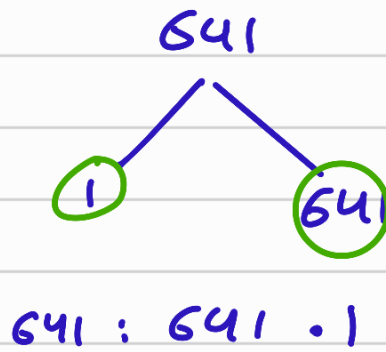
$$12 = 2 \cdot 2 \cdot 3$$

$$12 = 2^2 \cdot 3$$

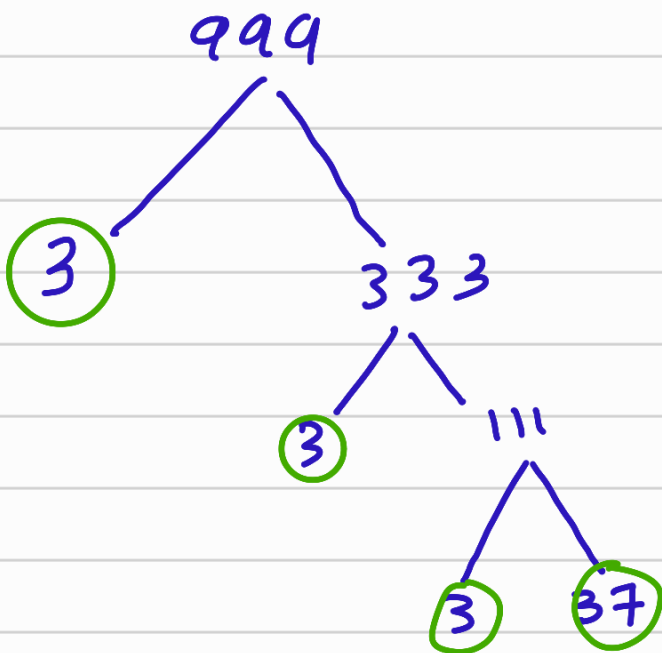
Write the number as product of  
Prime numbers



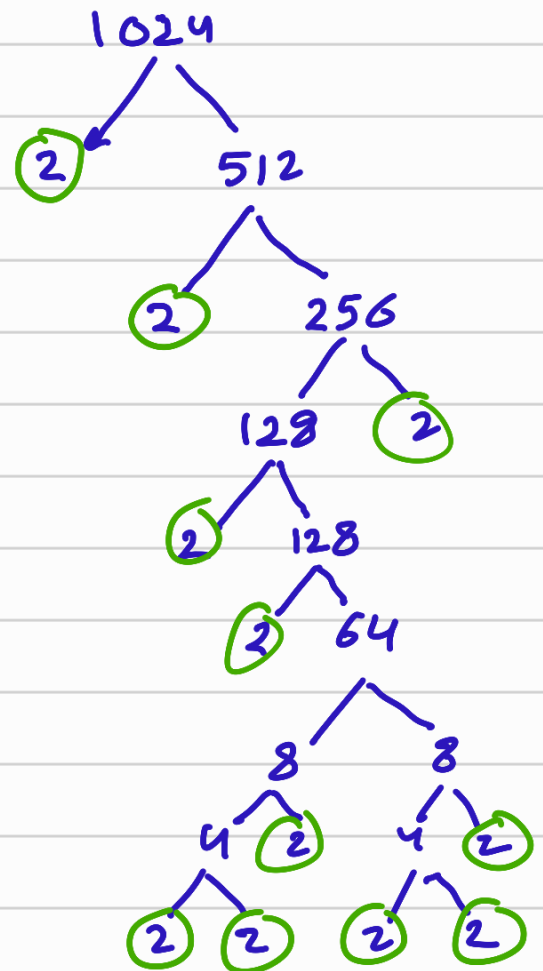
$$100 : 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$$



$$641 : 641 \cdot 1$$



$$\begin{aligned} 999 &= 3 \cdot 3 \cdot 3 \cdot 37 \\ &= 3^3 \cdot 37 \end{aligned}$$



$$1024 = 2^{10}$$



Eratosthenes  
(276-194 B.C.)

عزبالي

# The Sieve of Eratosthenes

تستخدم هذه الطريقة لمعرفة الأعداد الأولية التي لا تتجاوز عدد معين

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.

امسح كل الأعداد الأولية أقل من 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}

جميع الأعداد الأولية  
أقل من 100

continued →



# The Sieve of Eratosthenes

TABLE 1 The Sieve of Eratosthenes.

Integers divisible by 2 other than 2  
receive an underline.

حذف كل الأرقام التي تقسم على 2 عدا 2

1	2	3	4	5	6	7	8	9	10
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>

① حذف جميع الأعداد الأقل من العدد المطلوب

Integers divisible by 3 other than 3

receive an underline.

حذف كل الأرقام التي تقسم على 3 عدا 3

1	2	3	4	5	6	7	8	9	10
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>	<u>27</u>	<u>28</u>	29	<u>30</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>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</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>	65	<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>
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>	95	<u>96</u>	97	<u>98</u>	99	<u>100</u>

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

To see this, note that if  $n = ab$ , then  $a \leq \sqrt{n}$  or  $b \leq \sqrt{n}$ .

طريقة قسمه تجريبية وتعتبر غير فعالة. وهو صافي الأعداد الأولية

Trial division, a very inefficient method of determining if a number  $n$  is prime, is to try every integer  $i \leq \sqrt{n}$  and see if  $n$  is divisible by  $i$ .

تبدأ من العدد الأولي يجب تجريب جميع الأعداد التي تكون أقل من  $\sqrt{n}$

Integers divisible by 5 other than 5  
receive an underline.

حذف كل الأرقام التي تقسم على 5 عدا 5

1	2	3	4	5	6	7	8	9	10
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
<u>21</u>	<u>22</u>	23	<u>24</u>	<u>25</u>	<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>
41	<u>42</u>	43	<u>44</u>	<u>45</u>	<u>46</u>	47	<u>48</u>	49	<u>50</u>
<u>51</u>	<u>52</u>	53	<u>54</u>	<u>55</u>	<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>
71	<u>72</u>	73	<u>74</u>	<u>75</u>	<u>76</u>	77	<u>78</u>	79	<u>80</u>
<u>81</u>	<u>82</u>	83	<u>84</u>	<u>85</u>	<u>86</u>	<u>87</u>	<u>88</u>	89	<u>90</u>
91	<u>92</u>	93	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	99	<u>100</u>

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

حذف كل الأرقام التي تقسم على 7 عدا 7

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

حذف جميع الأعداد الأقل من العدد الأولي

عدد صال العدد 49 هو عدد اوي

$$n = 49$$

$$\sqrt{n} = \sqrt{49} = 7$$

2, 3, 4, 5, 6, (7) ✓  
X X X X X

ليس عدد اوي لان لديه عامل هو 7

$$49 : 1, 7, 49$$

\* اثبات ان صال عدد لانها في حلة عدد الاوليه

① افترض ان صال عدد محدد من الاعداد الاوليه

$$p_1, p_2, p_3, \dots, p_n$$

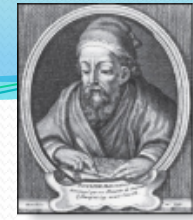
② استاء عدد جديد  $q$  (حاصل ضرب جميع الاعداد الاوليه زائد واحد)

$$q = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$$

③ نفحص العدد  $q$  هل هو اوي او مركب  
له اذا كان عدد اوي فان ذلك يتناقض  
له اذا كان عدد مركب فيحتاج ان يقسم  
على احد الاعداد في القائمة بدون باقى  
وهذا لا يحدث لان صال باقى

④ الشك في صال عدد اوي ليس له لقائه المحددة  
التي فرضنا وهذا العدد ممكن ان يكون  $p_{n+1}$  او  
عدد اوي اخر

⑤ الفرضه القائله ان الاعداد الاوليه محدودة غير صحيحة اذا بوجه  
عدد لانها في حلة الاعداد الاوليه



Euclid

(325 B.C.E. – 265 B.C.E.)

# Infinitude of Primes

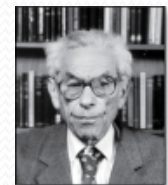
هناك عدد لا نهائي من الاعداد الأولية

**Theorem:** There are infinitely many primes. (Euclid)

**Proof:** <sup>١</sup> Assume <sup>٢</sup> finitely many primes:  $p_1, p_2, \dots, p_n$

- ② ● Let  $q = p_1 p_2 \dots p_n + 1$
- ③ ● Either  $q$  is prime or by the fundamental theorem of arithmetic it is a product of primes.
  - But none of the primes  $p_j$  divides  $q$  since if  $\underline{p_j} \mid \underline{q}$ , then  $\underline{p_j}$  divides  $q - p_1 p_2 \dots p_n = 1$ .
  - 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. ميتا قص
- ننتهي Consequently, there are infinitely many primes.

This proof was given by Euclid *The Elements*. The proof is considered to be one of the most beautiful in all mathematics. It is the first proof in *The Book*, inspired by the famous mathematician Paul Erdős' imagined collection of perfect proofs maintained by God.



Paul Erdős  
(1913-1996)



Marin Mersenne  
(1588-1648)

الاعداد ميرسيني الاولى

# Mersene Primes

مبنى كتابه الاعداد الاولى على صوره  $2^p - 1$

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

- $2^2 - 1 = 3$ ,  $2^3 - 1 = 7$ ,  $2^5 - 1 = 31$ , and  $2^7 - 1 = 127$  are Mersene primes. في بعض الاصناف تقضي لفاحده اعداد غير اولية
- $2^{11} - 1 = 2047$  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 2011, 47 Mersene primes were known, the largest is  $2^{43,112,609} - 1$ , which has nearly 13 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/>



مترجم بحثي يهـ خ  
اي ايجاد ارقام ميرسيني  
الاولية

2, 3, 5, 7, 11, 17, 19, 23, 29

توزيع الأعداد الأولية

# Distribution of Primes

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

**Prime Number Theorem**: The ratio of the number of primes not exceeding  $x$  and  $x/\ln x$  approaches 1 as  $x$  grows without bound. ( $\ln x$  is the natural logarithm of  $x$ )

- The theorem tells us that the number of primes not exceeding  $x$ , can be approximated by  $x/\ln x$ . ما احتمال اختيار عدد أو كـ أقل من  $10 = \frac{1}{2.3}$
- The odds that a randomly selected positive integer less than  $n$  is prime are approximately  $(n/\ln n)/n = 1/\ln n$ .

حاصل الأعداد الأولية الأقل من  $100 = \frac{100}{2.3} = 21.7$  الخمسة 25  
الاحتمال اختيار عدد أو كـ أقل من عدد معين  $\frac{1}{\ln n}$



# Primes and Arithmetic Progressions

(optional)

الاحمار الاوليه والسلاسل الحسابيه

- Euclid's proof that there are infinitely many primes can be easily adapted to show that there are infinitely many primes in the following  $4k + 3$ ,  $k = 1, 2, \dots$  (See Exercise 55) سلسلة تقري اعداد اوليه  $3k+4$
- In the 19<sup>th</sup> century G. Lejuenne Dirchlet showed that every arithmetic progression  $ka + b$ ,  $k = 1, 2, \dots$ , where  $a$  and  $b$  have no common factor greater than 1 contains infinitely many primes. (The proof is beyond the scope of the text.) دسرتليه: اي سلسلة  $ka+b$  بشرط  $a$  و  $b$  ليس بينهما قاسم مشترك يقبل عدد لا نهائي من الاعداد الاوليه
- 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.

بعل اردوس لكل عدد صحيح

موجب  $n$  يوجد سلسله حسابيه بطول  $n$   
تتكون با تكامل من اعداد اوليه



Terence Tao  
(Born 1975)

نظريات الأعداد الأولية

# Generating Primes

- The problem of generating large primes is of both theoretical and practical interest.
- We will see (in Section 4.6) that finding large primes with hundreds of digits is important in cryptography.
- So far, no useful closed formula that always produces primes has been found. There is no simple function  $f(n)$  such that  $f(n)$  is prime for all positive integers  $n$ .
- But  $f(n) = n^2 - n + 41$  is prime for all integers 1, 2, ..., 40. Because of this, we might conjecture that  $f(n)$  is prime for all positive integers  $n$ . But  $f(41) = 41^2$  is not prime.
- More generally, there is no polynomial with integer coefficients such that  $f(n)$  is prime for all positive integers  $n$ . (See supplementary Exercise 23.)
- Fortunately, we can generate large integers which are almost certainly primes. See Chapter 7.



المسائل حول الأعداد الأولية

# Conjectures about Primes

- Even though primes have been studied extensively for centuries, many conjectures about them are unresolved, including:
- **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.  
 $1^2 + 1 = 2$   
 $2^2 + 1 = 5$   
 $4^2 + 1 = 17$   
 $6^2 + 1 = 37$
- **There are infinitely many primes of the form  $n^2 + 1$** , where  $n$  is a positive integer. But it has been shown that there are infinitely many primes of the form  $n^2 + 1$ , where  $n$  is a positive integer or the product of at most two primes.
- **The Twin Prime Conjecture** The twin prime conjecture is that 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 mid 2011) consists of numbers  $65,516,468,355 \cdot 23^{33,333} \pm 1$  which have 100,355 decimal digits.  
(1) فرضية جولدباخ :- جميع الأعداد الزوجية التي أكبر من 2 هي ناتج جمع عددين أوليين  
(2) هناك عدد لا نهائي من الأعداد الأولية يمكن صياغتها بصيغة  $(n^2 + 1)$   
(3) فرضية التوأم

# القاسم المشترك الأكبر Greatest Common Divisor (gcd)

**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  $\gcd(a, b)$ .

العدد  $\gcd$  هو أكبر عدد يقسم كل واحد من العددين  $a, b$

➤ We can find greatest common divisors of small numbers by inspection.

**Example:** What is the greatest common divisor of 24 and 36?

**Solution:**  $\gcd(24, 36) = 12$

$\gcd = 12$   
24: 2, 4, 6, 8, 3, 12, 24

**Example:** What is the greatest common divisor of 17 and 22?

36: 2, 4, 6, 9, 12, 18, 36

**Solution:**  $\gcd(17, 22) = 1$

17: 17, 1  
22: 2, 22, 1, 22  
 $\gcd = 1$

10: 1, 2, 5, 10  
17: 1, 17

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

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

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



جامعة أم القرى  
UMM AL-QURA UNIVERSITY

## Greatest Common Divisor (gcd)

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

**Example:** 17 and 22 relatively prime  $\gcd = 1$

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

**Example:** Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

**Solution:** Because  $\gcd(10, 17) = 1$ ,  $\gcd(10, 21) = 1$ , and  $\gcd(17, 21) = 1$ , 10, 17, and 21 are pairwise relatively prime.

**Example:** Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

**Solution:** Because  $\gcd(10, 24) = 2$ , 10, 19, and 24 are not pairwise relatively prime.

Pairwise relatively prime

# Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of  $a$  and  $b$  are:

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

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

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

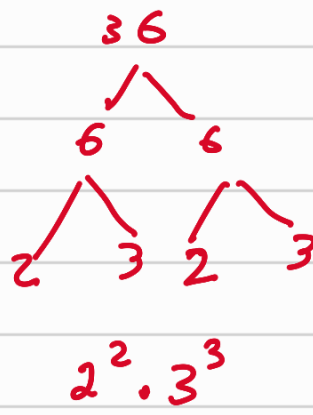
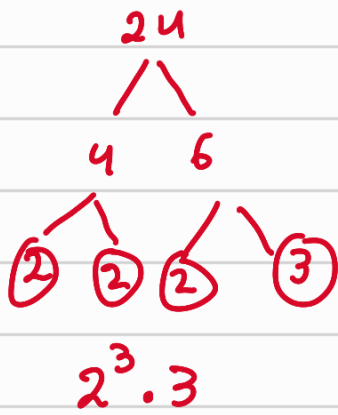
- This formula is valid since the integer on the right (of the equals sign) divides both  $a$  and  $b$ . No larger integer can divide both  $a$  and  $b$ .

**Example:**  $\underline{120} = 2^3 \cdot 3 \cdot 5$      $\underline{500} = 2^2 \cdot 5^3$

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

طريقة غير فعالة

- 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.



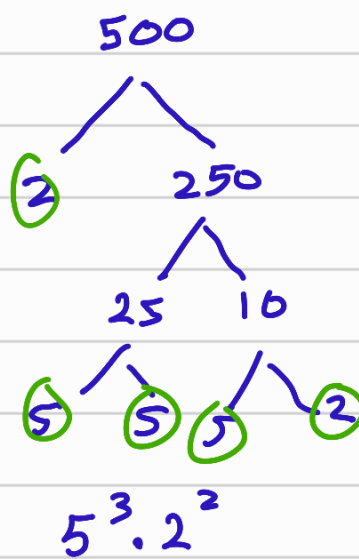
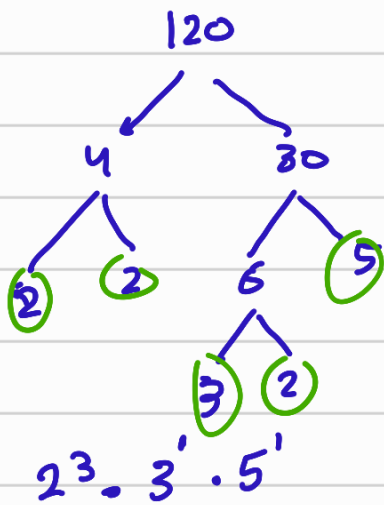
$$24 = 2^3 \cdot 3^1$$

$$36 : 2^2 \cdot 3^2$$


---


$$: 2^2 \cdot 3^1 = 12$$

$$GCD = 12$$



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

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


---


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

20

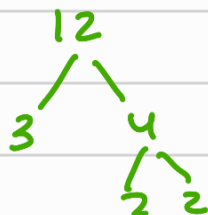
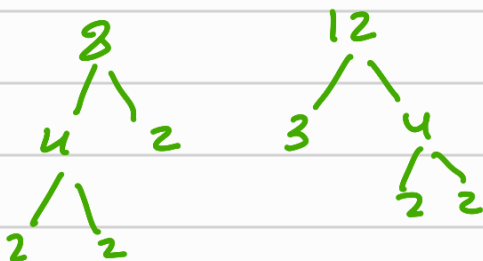
Find LCM for (2, 3)

2 : 2, 4, 6, 8, 10

3 : 3, 6, 9, 12

LCM = 6

Find LCM for (8, 12)



$$LCM = 2^3 \cdot 3$$

$$= 24$$

نویس 5

حاصل ضرب ای کدرین = GCD x LCM

$ab = GCD \times LCM$

(LCM = 24) المدين 8, 12

gcd

$$\frac{8 \times 12}{24} = gcd = 4$$

# صغاف صتره الاعداد

## Least Common Multiple (lcm)

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

اصغر رقم عليه القسمة في  $a$  و  $b$

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

بالتحليل للعوامل

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

This number is divided by both  $a$  and  $b$  and no smaller number is divided by  $a$  and  $b$ .

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

$$2^4 \cdot 3^5 \cdot 7^2$$

- The greatest common divisor and the least common multiple of two integers are related by:

**Theorem 5:** Let  $a$  and  $b$  be positive integers. Then  $ab = \text{gcd}(a, b) \cdot \text{lcm}(a, b)$

# الخوارزمية الإقليدية كتاب لاف Euclidean Algorithm

طريقة فعالة

- 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  $\gcd(b,c)$  when  $a > b$  and  $c$  is the remainder when  $a$  is divided by  $b$ .

$a > b$

**Example:** Find  $\gcd(91, 287)$ :

- $287 = 91 \cdot 3 + 14$  Divide 287 by 91
- $91 = 14 \cdot 6 + 7$  Divide 91 by 14
- $14 = 7 \cdot 2 + 0$  Divide 14 by 7  
Stopping condition

فنتيجه  $a$  على  $b$  وينتج باقي  $c \text{ mod } c$   
نكرر هذه العملية يصبح الرقم الجدير هو  $b$   
وننتيجه على  $c$  ونكرر العملية  
حتى نحصل على  $\gcd$

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$



# Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd( $a, b$ : positive integers)
```

```
   $x := a$ 
```

```
   $y := b$ 
```

```
  while  $y \neq 0$ 
```

```
     $r := x \bmod y$ 
```

```
     $x := y$ 
```

```
     $y := r$ 
```

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

12, 8

$x = 12$

$y = 8$

$r = 12 \bmod 8$

$x = y$   
 $y = r$

- In Section 5.3, we'll see that the time complexity of the algorithm is  $O(\log b)$ , where  $a > b$ .



# Euclidean Algorithm to find GCD

- خطوات
- ① نقسم العدد الأكبر على العدد الأصغر
  - ② نقسم العدد الأصغر على باقي القسمة
  - ③ نكرر العملية حتى نصل إلى باقي قدر يساوي صفر
  - ④ GCD يكون هو آخر رقم قسمتها عليه

Find GCD for (8, 12)

$$12 \div 8 \Rightarrow 12 = 8 \cdot 1 + 4$$

$$8 \div 4 \Rightarrow 8 = 4 \cdot 2 + \boxed{0}$$

$$\begin{array}{r} 1 \\ 8 \overline{) 12} \\ \underline{8} \phantom{0} \\ 4 \phantom{0} \\ 8 \phantom{0} \\ \underline{8} \\ 0 \end{array}$$

GCD = 4 آخر رقم قسمتها عليه

Find GCD 91, 287

$$\begin{array}{r} 3 \\ 91 \overline{) 287} \\ \underline{273} \phantom{0} \\ 14 \phantom{0} \end{array}$$

$$\begin{array}{r} 6 \\ 14 \overline{) 91} \\ \underline{84} \phantom{0} \\ 7 \phantom{0} \end{array}$$

$$\begin{array}{r} 2 \\ 7 \overline{) 14} \\ \underline{14} \\ \boxed{0} \end{array}$$

آخر رقم قسمتها عليه 7

$$287 = 3 \times 91 + 14$$

$$91 = 6 \times 14 + 7$$

$$14 = 2 \times 7 + 0$$

$$\text{GCD}(91, 287) = 7$$

$$\text{GCD}(91, 14) = 7$$

$$\text{GCD}(14, 7) = 7$$

# Correctness of Euclidean Algorithm

$$a = bq + r$$

$$\begin{array}{r} q_0 \\ \overline{a} \\ b \end{array} \quad \begin{array}{r} q_1 \\ \overline{b} \\ r \end{array}$$

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

اثبات **Proof:**

- ✓ Suppose that  $d$  divides both  $a$  and  $b$ . Then  $d$  also divides  $a - bq = r$  (by Theorem 1 of Section 4.1). Hence, any common divisor of  $a$  and  $b$  must also be any 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  $a$  and  $b$  must also be a common divisor of  $b$  and  $r$ .
- Therefore,  $\gcd(a, b) = \gcd(b, r)$ .

اي قاسم مشترك بين  $a$  و  $b$  سيكون  
أي قاسم مشترك بين  $b$  و  $r$   
أي قاسم مشترك بين  $a$  و  $b$  سيكون  
أي قاسم مشترك بين  $b$  و  $r$

# Correctness of Euclidean Algorithm

$$\begin{array}{c} \begin{array}{c} q_0 \\ b \overline{) a} \\ \hline r_0 \end{array} \quad \begin{array}{c} q_1 \\ r_0 \overline{) b} \\ \hline r_1 \end{array} \quad \begin{array}{c} q_2 \\ r_1 \overline{) r_0} \\ \hline r_2 \end{array} \quad \begin{array}{c} q_3 \\ r_2 \overline{) r_1} \\ \hline r_3 \end{array} \end{array}$$

$$a = q_0 b + r_0$$

$$b = r_0 q_1 + r_1$$

$$r_0 = r_1 q_2 + r_2$$

- 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:

القسمة المتتالية  
تنتج الباقى المتتالية

$$r_0 = r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1,$$

$$r_1 = r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2,$$

$\vdots$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1},$$

$$r_{n-1} = r_n q_n.$$

- Eventually, a remainder of zero occurs in the sequence of terms:  $a = r_0 > r_1 > r_2 > \dots \geq 0$ . The sequence can't contain more than  $a$  terms.
- By Lemma 1  
 $\gcd(\underline{a}, \underline{b}) = \gcd(r_0, r_1) = \dots = \gcd(\underline{r_{n-1}}, \underline{r_n}) = \gcd(r_n, 0) = r_n$ .
- Hence the greatest common divisor is the last nonzero remainder in the sequence of divisions.





# gcds as Linear Combinations

**Bézout's Theorem:** If  $a$  and  $b$  are positive integers, then there exist integers  $s$  and  $t$  such that  $\gcd(a,b) = sa + tb$ .  
(proof in exercises of Section 5.2)

مصادله  
بیژو

**Definition:** 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  $b$ . The equation  $\gcd(a,b) = sa + tb$  is called Bézout's identity.

ضرایب  
بیژو

مصادله بیژو

By Bézout's Theorem, the gcd of integers  $a$  and  $b$  can be expressed in the form  $sa + tb$  where  $s$  and  $t$  are integers. This is a linear combination with integer coefficients of  $a$  and  $b$ .

●  $\gcd(6,14) = (-2) \cdot 6 + 1 \cdot 14$

$$\begin{array}{r} 2 \\ 6 \overline{) 14} \\ \underline{12} \\ 2 \end{array}$$

$$\begin{array}{r} 3 \\ (2) \overline{) 6} \\ \underline{6} \\ 0 \end{array}$$

$GCD = 2$

$$2 = sa + tb$$

$$2 = s(14) + t(6) = 1(14) - 2(6)$$

$s \uparrow$

$t \uparrow$

## الحواصم المتراكمة كتركيبات خطية

نغزیه بیزد :- اذا كان لدينا عددین صحیحین  $a$  و  $b$

فانه يمكن كتابه  $\boxed{GCD}$  لهما في شكل ترکیب

خطي

$$Gcd(a, b) = Sa + tb$$

معادله بیزد

ارقام توانین و سها معادلات بیزد

$$GCD = 5 \quad \text{خطی} \quad 15, 25$$

$$5 = S \cdot 15 + t \cdot 25$$

$$S = 2$$

$$t = -1$$

$$5 = 2 \times 15 - 1 \times 25$$

خطوات كتابه  $GCD$  في شكل ترکیب خطي

① حسب  $GCD$  بالطريقة الاقليدية بالتفضيل مع كتابه كل معادلة

② خطیه كتابه المعادلات بالتكامل  $\dots = 8$

③ لغرض في المعادلات لتقويض  $Working\ backward$

④ تبسيط اخر معادلة للمعقول في شكل معادلة

$$GCD = Sa + tb$$

بیزد

# Finding gcds as Linear Combinations

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

**Solution:** First use the Euclidean algorithm to show  $\gcd(252, 198) = 18$

- i.  $252 = 1 \cdot 198 + 54$
- ii.  $198 = 3 \cdot 54 + 36$
- iii.  $54 = 1 \cdot 36 + 18$
- iv.  $36 = 2 \cdot 18$

● Now working backwards, from iii and i above

- $18 = 54 - 1 \cdot 36$

- $36 = 198 - 3 \cdot 54$

● Substituting the 2<sup>nd</sup> equation into the 1<sup>st</sup> yields:

- $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$

● Substituting  $54 = 252 - 1 \cdot 198$  (from i)) yields:

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

● This method illustrated above is a two pass method. It first uses the Euclidean algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers. A one pass method, called the extended Euclidean algorithm, is developed in the exercises.

Express  $\gcd(25, 15) = \underline{5}$  as linear combination of  $\textcircled{25}, \textcircled{15}$

① حساب لـ  $\gcd$  بالتقسيد

$$\begin{array}{r} 1 \\ 15 \overline{) 25} \\ \underline{15} \\ 10 \end{array} \quad \begin{array}{r} 1 \\ 10 \overline{) 15} \\ \underline{10} \\ 5 \end{array} \quad \begin{array}{r} \textcircled{5} \\ \textcircled{5} \overline{) 10} \\ \underline{10} \\ 0 \end{array}$$

①

$$\begin{aligned} 25 &= 15 \times 1 + 10 \\ 15 &= 10 \times 1 + 5 \\ 10 &= 5 \times 2 + 0 \end{aligned}$$

②

$$\begin{aligned} 10 &= 25 - 15 \times 1 \\ 5 &= 15 - \textcircled{10} \times 1 \end{aligned}$$

③ التحويل الكاف

$$5 = 15 - (25 - 15 \times 1) \times 1$$

④ تبسيط

$$5 = 1 \times 15 - 25 + 15 \times 1$$

$$5 = -1 \times \textcircled{25} + 2 \times \textcircled{15}$$

$$5 = s a + t b$$

$$s = -1$$

$$t = 2$$

Express  $\gcd(252, 198) = 18$  as linear

combination of  $252, 198$

①

$$\begin{array}{r} 1 \\ 198 \overline{) 252} \\ \underline{198} \\ 54 \end{array}$$

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

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

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

$$36 = 18 \times 2 + 0$$

$$\begin{array}{r} 3 \\ 54 \overline{) 198} \\ \underline{162} \\ 36 \end{array}$$

$$\begin{array}{r} 1 \\ 36 \overline{) 54} \\ \underline{36} \\ 18 \end{array}$$

$$\begin{array}{r} 2 \\ 18 \overline{) 36} \\ \underline{36} \\ 0 \end{array}$$

$$(54) = 252 - 198 \times 1 \quad (2)$$

$$(36) = 198 - 54 \times 3$$

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

$$18 = 54 - (198 - 54 \times 3) \quad (3)$$

$$18 = \underline{54} - 198 + \underline{54 \times 3}$$

$$18 = 54 \times 4 - 198$$

$$18 = 4(252 - 198) - 198$$

$$18 = 4 \times 252 - 4 \times 198 - 198 \times 1$$

$$18 = 4 \times \boxed{252} - 5 \times \boxed{198}$$

$$s = 4$$

$$t = -5$$



نتائج نظرية بيزو

$\gcd(a, b) = 1$

# Consequences of Bézout's Theorem

**Lemma 2:** If  $a$ ,  $b$ , and  $c$  are positive integers such that  $\gcd(a, b) = 1$  and  $a \mid bc$ , then  $a \mid c$ . 4 28

**Proof:** Assume  $\gcd(a, b) = 1$  and  $a \mid bc$

● Since  $\gcd(a, b) = 1$ , by Bézout's Theorem there are integers  $s$  and  $t$  such that  $sa + tb = 1$ .  $sca + tcb = c$

● Multiplying both sides of the equation by  $c$ , yields  $sac + tbc = c$ .  $a \mid cbt$

● From Theorem 1 of Section 4.1:

$a \mid tbc$  (part ii) and  $a$  divides  $sac + tbc$  since  $a \mid sac$  and  $a \mid tbc$  (part i)

● We conclude  $a \mid c$ , since  $sac + tbc = c$ .

**Lemma 3:** If  $p$  is prime and  $p \mid a_1 a_2 \cdots a_n$ , then  $p \mid a_i$  for some  $i$ .  
(proof uses mathematical induction; see Exercise 64 of Section 5.1)

قاعدة حصر لا تنبأت مرزانية التحليل المبري

● Lemma 3 is crucial in the proof of the uniqueness of prime factorizations.

5 4 5  
a b c

5/20

الترتيب  $\gcd = 1$   $a \mid bc \Rightarrow a \mid c$  5/5 ✓

$$12 = 2^2 \cdot 3$$

مزدانیہ التحليل الاولی

# Uniqueness of Prime Factorization

- We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique (This part of the fundamental theorem of arithmetic. The other part, which asserts that every positive integer has a prime factorization into primes, will be proved in Section 5.2.)

**Proof:** (by contradiction) Suppose that the positive integer  $n$  can be written as a product of primes in two distinct ways:

فرضنا ان العدد  $n$  له تحليلين مختلفين

$$n = p_1 p_2 \cdots p_s \text{ and } n = q_1 q_2 \cdots q_t$$

- Remove all common primes from the factorizations to get

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

- By Lemma 3, it follows that  $p_{i_1}$  divides  $q_{j_k}$ , for some  $k$ , contradicting the assumption that  $p_{i_1}$  and  $q_{j_k}$  are distinct primes.

فمن العددين وصدر ناتج يحافظ الفرضيه سابقه

- Hence, there can be at most one factorization of  $n$  into primes in nondecreasing order.

نتيج ان هناك تحليل اولی واحد كذا لاكثر



$$a \equiv b \pmod{m}$$

$$ca \equiv cb \pmod{m}$$

$$m \mid ca - bc$$

# Dividing Congruences by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1). تمه المتطابقة على عدد ثابت لا يعطي دأى فيه صحيح
  - But dividing by an integer relatively prime to the modulus does produce a valid congruence: ما لسته على عدد ادري  $\gcd(m, c) = 1$
- Theorem 7:** Let  $m$  be a positive integer and let  $a$ ,  $b$ , and  $c$  be integers. If  $ac \equiv bc \pmod{m}$  and  $\gcd(c, m) = 1$ , then  $a \equiv b \pmod{m}$ . عند السته على  $c$  يحصل على قاعدة صحيح يؤتي قاعدة صحيح
- Proof:** Since  $ac \equiv bc \pmod{m}$ ,  $m \mid ac - bc = c(a - b)$  by Lemma 2 and the fact that  $\gcd(c, m) = 1$ , it follows that  $m \mid a - b$ . Hence,  $a \equiv b \pmod{m}$ . ◀

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

# Solving Congruences

Section 4.4

# Section Summary

- Linear Congruences ✓
- The Chinese Remainder Theorem
- Computer Arithmetic with Large Integers (*not currently included in slides, see text*)
- Fermat's Little Theorem
- Pseudoprimes
- Primitive Roots and Discrete Logarithms

23

$$ax \equiv b \pmod{m}$$

$$2x \equiv 1 \pmod{5}$$

نجر ب  $x=2$  خافي

$$4 \equiv 1 \pmod{5} \quad x$$

نجر ب  $x=3$

$$6 \equiv 1 \pmod{5}$$

اول حل هو  $x=3$

$$-7 \quad -2 \quad \boxed{3} \quad 8 \quad 13$$

# Linear Congruences

**Definition:** A congruence of the form

$$ax \equiv b \pmod{m},$$

where  $m$  is a positive integer,  $a$  and  $b$  are integers, and  $x$  is a variable, is called a *linear congruence*.

جميع فيه  $x$  بحفة الخطابة

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

$$\bar{a}a \equiv 1 \pmod{m}$$

**Definition:** An integer  $\bar{a}$  such that  $\bar{a}a \equiv 1 \pmod{m}$  is said to be an inverse of  $a$  modulo  $m$ .

مدرس

**Example:** 5 is an inverse of 3 modulo 7 since  $5 \cdot 3 = 15 \equiv 1 \pmod{7}$

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

$\bar{a}$  عدد نجر ب  $a$

بنت يكون ناتج قسمه

$$1 = m \text{ و } a\bar{a}$$

$$15 = 1 \pmod{7}$$

# Inverse of $a$ modulo $m$

- The following theorem guarantees that an inverse of  $a$  modulo  $m$  exists whenever  $a$  and  $m$  are relatively prime. Two integers  $a$  and  $b$  are relatively prime when  $\gcd(a, b) = 1$ .

**Theorem 1:** If  $a$  and  $m$  are relatively prime integers and  $m > 1$ , then an inverse of  $a$  modulo  $m$  exists. Furthermore, this inverse is unique modulo  $m$ . (This means that there is a unique positive integer  $\bar{a}$  less than  $m$  that is an inverse of  $a$  modulo  $m$  and every other inverse of  $a$  modulo  $m$  is congruent to  $\bar{a}$  modulo  $m$ .)

**Proof:** Since  $\gcd(a, m) = 1$ , by Theorem 6 of Section 4.3, there are integers  $s$  and  $t$  such that  $sa + tm = 1$ .

- Hence,  $sa + tm \equiv 1 \pmod{m}$ .
- Since  $tm \equiv 0 \pmod{m}$ , it follows that  $sa \equiv 1 \pmod{m}$   $1 = sa + tm$
- Consequently,  $s$  is an inverse of  $a$  modulo  $m$ .
- The uniqueness of the inverse is Exercise 7.





$$3\bar{a} = 1 \pmod{5}$$

② ضرب

$$6 = 1 \pmod{5}$$

$$\begin{array}{r} 1 \\ 5 \overline{) 6} \\ \underline{5} \\ 1 \end{array} \checkmark$$

↑ 6

$$2\bar{a} = 1 \pmod{11}$$

$$\bar{a} = 2 \times$$

$$\bar{a} = 3 \times$$

⋮

$$\bar{a} = 6 \checkmark$$

$$5\bar{a} = 1 \pmod{10}$$

$$10 \div 10 = 1 \quad r=0$$

$$15 \div 10 = 1 \quad r=5$$

$$20 \div 10 = 2 \quad r=0$$

هذه  
القيمة  
مطلوبة

عندما تكون القيمة الصغرى كما  
لوحه مكتوب

عندما  $GCD \neq 1$  ليس لها حلول



# Finding Inverses

- The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

$$\begin{array}{r} 2 \\ 3 \overline{) 7} \\ \underline{6} \\ 1 \end{array}$$

**Example:** Find an inverse of 3 modulo 7.

**Solution:** Because  $\gcd(3,7) = 1$ , by Theorem 1, an inverse of 3 modulo 7 exists.

$$7 = 3 \times 2 + 1$$

- Using the Euclidian algorithm:  $7 = 2 \cdot 3 + 1$ .

$$1 = 1 \times \boxed{7} - \boxed{3} \times 2$$

- From this equation, we get  $-2 \cdot 3 + 1 \cdot 7 = 1$ , and see that  $-2$  and 1 are Bézout coefficients of 3 and 7.

$$\text{Inverse} = -2$$

- Hence,  $-2$  is an inverse of 3 modulo 7.

- Also every integer congruent to  $-2$  modulo 7 is an inverse of 3 modulo 7, i.e., 5,  $-9$ , 12, etc.

$$\begin{array}{ccccccc} & & & \boxed{5} & & & \\ & & \swarrow & \uparrow & \searrow & \swarrow & \\ -7 & & -2 & & 5 & & 12 \end{array}$$

$$\text{Inverse} = 5$$

# Finding Inverses

**Example:** Find an inverse of 101 modulo 4620.

**Solution:** First use the Euclidian algorithm to show that  $\gcd(101, 4620) = 1$ .

Working Backwards:

$$42620 = 45 \cdot 101 + 75$$

$$101 = 1 \cdot 75 + 26$$

$$75 = 2 \cdot 26 + 23$$

$$26 = 1 \cdot 23 + 3$$

$$23 = 7 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

$$1 = 3 - 1 \cdot 2$$

$$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$

$$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$

$$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$$

$$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$$

$$= 26 \cdot 101 - 35 \cdot 75$$

$$1 = 26 \cdot 101 - 35 \cdot (42620 - 45 \cdot 101)$$

$$= -35 \cdot 42620 + 1601 \cdot 101$$

Since the last nonzero remainder is 1,  
 $\gcd(101, 4260) = 1$

Bézout coefficients :  $-35$  and  $1601$

1601 is an inverse of  
101 modulo 42620

# Find the multiplicative inverse of 15 mod 26

① نتدی ان  $1 = \text{GCD}$  حساب  
Euclidean Algorithm  
بجی صفی و کتابی کر شد  
= 1, 10

$$26 = 15 \times 1 + 11$$

$$15 = 11 \times 1 + 4$$

$$11 = 4 \times 2 + 3$$

$$4 = 3 \times 1 + 1$$

$$3 = 3 \times 1 + 0$$

$$11 = 26 \times 1 - 15 \times 1$$

$$4 = 15 \times 1 - 11 \times 1$$

$$3 = 11 \times 1 - 4 \times 2$$

$$1 = 4 \times 1 - (3) \times 1$$

② حساب معلات سیزد  
کتابی اکارا = بلالہ ر  
الغویض الکافی

inverse  
= 7

$$1 = 4 \times 1 - 11 \times 1 + 4 \times 2$$

$$1 = 4 \times 3 - 11 \times 1$$

$$1 = 3(15 \times 1 - 11 \times 1) - 11 \times 1$$

$$1 = 15 \times 3 - 11 \times 3 - 11 \times 1$$

$$1 = 15 \times 3 - 11 \times 4$$

$$1 = 15 \times 3 - 4(26 \times 1 - 15 \times 1)$$

$$1 = 15 \times 3 - 26 \times 4 + 15 \times 4$$

$$1 = 15 \times 7 - 26 \times 4$$

## Finding Inverses

**Example:** Find an inverse of 101 modulo 4620.

**Solution:** First use the Euclidian algorithm to show that  $\gcd(101, 4620) = 1$ .

$$4620 = 101 \times 45 + 75$$

$$101 = 75 \times 1 + 26$$

$$75 = 26 \times 2 + 23$$

$$26 = 23 \times 1 + 3$$

$$23 = 3 \times 7 + 2$$

$$3 = 2 \times 1 + 1$$

$$2 = 1 \times 2 + 0$$

$$75 = 4620 \times 1 - 101 \times 45$$

$$26 = 101 \times 1 - 75 \times 1$$

$$23 = 75 \times 1 - 26 \times 2$$

$$3 = 26 \times 1 - 23 \times 1$$

$$2 = 23 \times 1 - 3 \times 7$$

$$1 = 3 \times 1 - 2 \times 1$$

$$1 = 3 \times 1 - 2 \times 1 + 3 \times 7 \Rightarrow 1 = 3 \times 8 - 2 \times 1$$

$$1 = 26 \times 8 - 23 \times 8 - 23 \times 1 \Rightarrow 1 = 26 \times 8 - 9 \times 23$$

$$1 = 26 \times 8 - 75 \times 9 + 18 \times 26 \Rightarrow 1 = 28 \times 26 - 75 \times 9$$

$$1 = 26(101 \times 1 - 75 \times 1) - 75 \times 9 \Rightarrow 1 = 26 \times 101 - 75 \times 35$$

$$1 = 26 \times 101 - 35(4620 \times 1 - 101 \times 45)$$

$$1 = \underline{26 \times 101} - 35 \times 4620 + \underline{1575 \times 101}$$

$$1 = 1601 \times 101 - 35 \times 4620$$

$$\text{Inverse} = 1601$$

Solve the linear congruency

$$15x \equiv 8 \pmod{26}$$

① نتایج آن  $(\text{GCD})(a, m)$  و آنکه یوکل

②  $\bar{a}$  کب

③ یوکل اعداد  $\bar{a}$   $\Rightarrow$

$$ax \equiv b \pmod{m}$$

$$a\bar{a} = 1$$

$$x = \bar{a}b \pmod{m} \quad ④$$

اگر یوکل آن یوکل  
عدد یوکل اصل  $m$

$$15x \equiv 8 \pmod{26}$$

$$\text{GCD}(15, 26) = 1$$

$$\text{inverse of } 15 \text{ modulo } 26 = 7$$

$$x = 8 \times 7 \pmod{26}$$

$$x = 56 \pmod{26}$$

$$x = 56 \xrightarrow{-26} 30 \xrightarrow{-26} 4 \xrightarrow{-22} -22$$

$$\boxed{x = 4}$$

# Using Inverses to Solve Congruences

- We can solve the congruence  $ax \equiv b \pmod{m}$  by multiplying both sides by  $\bar{a}$ .

**Example:** What are the solutions of the congruence  $3x \equiv 4 \pmod{7}$ .

**Solution:** We found that  $-2$  is an inverse of  $3$  modulo  $7$  (two slides back). We multiply both sides of the congruence by  $-2$  giving

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}.$$

Because  $-6 \equiv 1 \pmod{7}$  and  $-8 \equiv 6 \pmod{7}$ , it follows that if  $x$  is a solution, then  $x \equiv -8 \equiv 6 \pmod{7}$

We need to determine if every  $x$  with  $x \equiv 6 \pmod{7}$  is a solution. Assume that  $x \equiv \underline{6} \pmod{7}$ . By Theorem 5 of Section 4.1, it follows that  $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod{7}$  which shows that all such  $x$  satisfy the congruence.

The solutions are the integers  $x$  such that  $x \equiv 6 \pmod{7}$ , namely,  $6, 13, 20 \dots$  and  $-1, -8, -15, \dots$

$$\underline{3}x = 4 \pmod{\underline{7}}$$

$$\text{GCD}(3, 7) = 1$$

$$7 = 3 \times 2 + 1$$

$$3 = 3 \times 1 + 0$$

$$1 = 7 \times 1 - 3 \times 2$$

$$\text{inverse} = -2$$

$$3x = 4 \pmod{7}$$

$$x = -8 \pmod{7}$$

$$x = -8$$

$$x = 6$$



$$x = 6 \pmod{7}$$



# The Chinese Remainder Theorem

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

البوانى  
الصينى  
بالنظام  
نقطة  
كل نظام  
مطابق

# The Chinese Remainder Theorem

**Theorem 2:** (*The Chinese Remainder Theorem*) Let  $m_1, m_2, \dots, m_n$  be pairwise relatively prime positive integers greater than one and  $a_1, a_2, \dots, a_n$  arbitrary integers. Then the system

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

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

.

.

.

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

has a unique solution modulo  $m = m_1 m_2 \cdots m_n$ .

(That is, there is a solution  $x$  with  $0 \leq x < m$  and all other solutions are congruent modulo  $m$  to this solution.)

● **Proof:** We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo  $m$  is Exercise 30.

*continued* →

# The Chinese Remainder Theorem

To construct a solution first let  $M_k = m/m_k$  for  $k = 1, 2, \dots, n$  and  $m = m_1 m_2 \cdots m_n$ .

Since  $\gcd(m_k, M_k) = 1$ , by Theorem 1, there is an integer  $y_k$ , an inverse of  $M_k$  modulo  $m_k$ , such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

Note that because  $M_j \equiv 0 \pmod{m_k}$  whenever  $j \neq k$ , all terms except the  $k$ th term in this sum are congruent to 0 modulo  $m_k$ .

Because  $M_k y_k \equiv 1 \pmod{m_k}$ , we see that  $x \equiv \underline{a_k M_k y_k} \equiv a_k \pmod{m_k}$ , for  $k = 1, 2, \dots, n$ .

Hence,  $x$  is a simultaneous solution to the  $n$  congruences.

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

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

.

.

.

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



# Chinese Remainder Theorem

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

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

$$x \equiv a_3 \pmod{m_3}$$

$$m = m_1 m_2 m_3 \dots$$

$a_i$	$M_k$	$y_i$	$a_i M_k y_i$
$a_1$	$m/m_1$		
$a_2$	$m/m_2$		
$a_3$	$m/m_3$		
$\vdots$			

$$M_k y_i \equiv 1 \pmod{m_i}$$

$$x \equiv \sum a_i M_k y_i \pmod{m}$$

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

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

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

$$m = 3 \times 5 \times 7 = 105$$

$a_i$	$M_k$	$y_i$	$a_i M_k y_i$
2	35	2	140
3	21	1	63
2	15	1	30
			<u>233</u>

$$35 y_i \equiv 1 \pmod{3}$$

$$35 = 11 \times 3 + 2 \quad \left| \quad 2 = 35 \times 1 - 11 \times 3 \right.$$

$$3 = 2 \times 1 + 1 \quad \left| \quad 1 = 3 \times 1 - 2 \times 1 \right.$$

$$2 = 2 \times 1 + 0$$

$$1 = 3 \times 1 - 35 \times 1 + 11 \times 3$$

$$1 = 12 \times 3 - 1 \times 35$$

$$y = -1 \bigcup_{+3} 2$$

$$x = \cancel{233}^{23} \pmod{105}$$

$$\begin{array}{ccc} 233 & 128 & 23 \\ \text{---} & \text{---} & \\ 105 & 105 & \end{array}$$

# The Chinese Remainder Theorem

**Example:** Consider the 3 congruences from Sun-Tsu's problem:

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}.$$

- Let  $m = 3 \cdot 5 \cdot 7 = 105$ ,  $M_1 = m/3 = 35$ ,  $M_2 = m/5 = 21$ ,  $M_3 = m/7 = 15$ .
- We see that
  - 2 is an inverse of  $M_1 = 35$  modulo 3 since  $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod{3}$
  - 1 is an inverse of  $M_2 = 21$  modulo 5 since  $21 \equiv 1 \pmod{5}$
  - 1 is an inverse of  $M_3 = 15$  modulo 7 since  $15 \equiv 1 \pmod{7}$
- Hence,

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105} \end{aligned}$$

- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

$$x \equiv 1 \pmod{a} \quad \text{vs} \quad x = at + 1$$

$$\begin{aligned}x &\equiv 1 \pmod{5} \\x &\equiv 2 \pmod{6} \\x &\equiv 3 \pmod{7}\end{aligned}$$

نقوم في المرحله الثانيه

$$x = 5t + 1 \quad \text{--- (1)}$$

$$5t + 1 = 2 \pmod{6}$$

نوز 1, ٢, ٣, ٤, ٥

$$\begin{aligned}6 &= 5 \times 1 + 1 \\1 &= 6 \times 1 - 5 \times 1\end{aligned}$$

$$\begin{aligned}5t &= 1 \pmod{6} \\-1 &= \text{invers}\end{aligned}$$

$$\begin{aligned}t &= -1 \pmod{6} \\t &= 5 \pmod{6}\end{aligned}$$

نقوم في المرحله الثانيه

$$t = 6u + 5 \quad \text{--- (2)}$$

$$x = 5(6u + 5) + 1$$

$$x = 30u + 26$$

نقوم هنا في المرحله الثالثه

$$30u + 26 = 3 \pmod{7}$$

$$30u = -23 \pmod{7}$$

$$30u = 5 \pmod{7}$$

$$\begin{array}{r} 4 \\ 7 \overline{) 30} \\ \underline{28} \\ 2 \end{array}$$

$$-23 \rightarrow -16 \rightarrow -9 \rightarrow -2 \rightarrow 5$$

$$\begin{aligned}30 &= 4 \times 7 + 2 \\4 &= 2 \times 2 + 0\end{aligned}$$

$$2 = 30 \times 1 - 4 \times 7$$

$$u = 5 \pmod{7} \rightarrow u = 7v + 5$$

نقوم u في المرحله x

$$x = 30u + 26$$

$$\begin{aligned}x &= 30(7v + 5) + 26 = 210v + 206 \\x &= 206 \pmod{210}\end{aligned}$$

# حل أنظمة المتباينات باستخدام السبغبدال الخلفى

## Back Substitution

- We can also solve systems of linear congruences with pairwise relatively prime moduli by rewriting a congruence as an equality using Theorem 4 in Section 4.1, substituting the value for the variable into another congruence, and continuing the process until we have worked through all the congruences. This method is known as back substitution.

**Example:** Use the method of back substitution to find all integers  $x$  such that  $x \equiv 1 \pmod{5}$ ,  $x \equiv 2 \pmod{6}$ , and  $x \equiv 3 \pmod{7}$ .

**Solution:** By Theorem 4 in Section 4.1, the first congruence can be rewritten as  $x = 5t + 1$ , where  $t$  is an integer.

- Substituting into the second congruence yields  $5t + 1 \equiv 2 \pmod{6}$ .
- Solving this tells us that  $t \equiv 5 \pmod{6}$ .
- Using Theorem 4 again gives  $t = 6u + 5$  where  $u$  is an integer.
- Substituting this back into  $x = 5t + 1$ , gives  $x = 5(6u + 5) + 1 = 30u + 26$ .
- Inserting this into the third equation gives  $30u + 26 \equiv 3 \pmod{7}$ .
- Solving this congruence tells us that  $u \equiv 6 \pmod{7}$ .
- By Theorem 4,  $u = 7v + 6$ , where  $v$  is an integer.
- Substituting this expression for  $u$  into  $x = 30u + 26$ , tells us that  $x = 30(7v + 6) + 26 = 210v + 206$ .

Translating this back into a congruence we find the solution  $x \equiv 206 \pmod{210}$ .



$$p=5$$

$$a=2$$

$$2^{5-1} = 1 \pmod{5}$$

$$16 = 1 \pmod{5}$$



# Fermat's Little Theorem

Pierre de Fermat  
(1601-1665)

**Theorem 3:** (*Fermat's Little Theorem*) If  $p$  is prime and  $a$  is an integer not divisible by  $p$ , then  $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer  $a$  we have  $\underline{a^p} \equiv a \pmod{p}$   
(proof outlined in Exercise 19)

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^p = a \pmod{p}$$

Fermat's little theorem is useful in computing the remainders modulo  $p$  of large powers of integers.

**Example:** Find  $7^{222} \bmod 11$ .

By Fermat's little theorem, we know that  $7^{10} \equiv 1 \pmod{11}$ , and so  $(7^{10})^k \equiv 1 \pmod{11}$ , for every positive integer  $k$ . Therefore,

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

Hence,  $7^{222} \bmod 11 = 5$ .

$$7^{10} \equiv 1 \pmod{11}$$

$$\begin{array}{r} 4 \\ 11 \overline{) 49} \\ \underline{44} \\ 5 \end{array}$$

$$7^{222} \bmod 11$$

$$7^{220} 7^2 \pmod{11} = (7^{10})^{22} 7^2 \pmod{11} = 49 \pmod{11} = 5 \pmod{11}$$

$$p=3, 5, 7$$

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{Prime}$$

# Pseudoprimes

عند التحقق  $2^{p-1} \equiv 1 \pmod{p}$  هذه القاعدة لعدد أولي، لا، رقم التي ليست أولية، دسمة هذه الأعداد  
Pseudoprime

- By Fermat's little theorem  $n > 2$  is prime, where  $2^{n-1} \equiv 1 \pmod{n}$ .
- But if this congruence holds,  $n$  may not be prime. Composite integers  $n$  such that  $2^{n-1} \equiv 1 \pmod{n}$  are called pseudoprimes to the base 2.

**Example:** The integer 341 is a pseudoprime to the base 2.

$$341 = 11 \cdot 31$$

$$2^{340} \equiv 1 \pmod{341} \text{ (see in Exercise 37)}$$

$$2^{n-1} \equiv 1 \pmod{n}$$

- We can replace 2 by any integer  $b \geq 2$ .

**Definition:** Let  $b$  be a positive integer. If  $n$  is a composite integer, and  $b^{n-1} \equiv 1 \pmod{n}$ , then  $n$  is called a pseudoprime to the base  $b$ .

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

$$\text{Composite } 341 = 11 \times 31$$

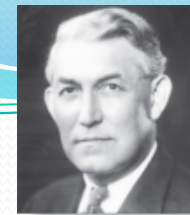
القاعدة انضبطت والعدد غير أولي إذاً العدد 341 شبه أولي

# Pseudoprimes

هذه لفظة تطبق فقط في حالة  
الأرقام الأولية وسبب الإدلة

- Given a positive integer  $n$ , such that  $2^{n-1} \equiv 1 \pmod{n}$ :
  - If  $n$  does not satisfy the congruence, it is composite. غير دي
  - If  $n$  does satisfy the congruence, it is either prime or a pseudoprime to the base 2.
- Doing similar tests with additional bases  $b$ , provides more evidence as to whether  $n$  is prime.
- Among the positive integers not exceeding a positive real number  $x$ , compared to primes, there are relatively few pseudoprimes to the base  $b$ .  
هناك عدد اقل من الأرقام السليمة
- For example, among the positive integers less than  $10^{10}$  there are 455,052,512 primes, but only 14,884 pseudoprimes to the base 2.  
هنا لا يوجد الا ادلة

عدد غير زوجي بحيث  $b^{n-1} \equiv 1 \pmod{n}$  لجميع  $b$  الحد  $\tau$   
 $\gcd(b, n) = 1$



# Carmichael Numbers

## (optional)

Robert Carmichael  
 (1879-1967)

- There are composite integers  $n$  that pass all tests with bases  $b$  such that  $\gcd(b, n) = 1$ .  
**Definition:** A composite integer  $n$  that satisfies the congruence  $b^{n-1} \equiv 1 \pmod{n}$  for all positive integers  $b$  with  $\gcd(b, n) = 1$  is called a *Carmichael* number.
- Example:** The integer 561 is a Carmichael number. To see this:
  - 561 is composite, since  $561 = 3 \cdot 11 \cdot 13$ .
  - If  $\gcd(b, 561) = 1$ , then  $\gcd(b, 3) = 1$ , then  $\gcd(b, 11) = \gcd(b, 17) = 1$ .
  - Using Fermat's Little Theorem:  $b^2 \equiv 1 \pmod{3}$ ,  $b^{10} \equiv 1 \pmod{11}$ ,  $b^{16} \equiv 1 \pmod{17}$ .
  - Then
    - $b^{560} = (b^2)^{280} \equiv 1 \pmod{3}$ ,
    - $b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$ ,
    - $b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$ .
  - It follows (see Exercise 29) that  $b^{560} \equiv 1 \pmod{561}$  for all positive integers  $b$  with  $\gcd(b, 561) = 1$ . Hence, 561 is a Carmichael number.
- Even though there are infinitely many Carmichael numbers, there are other tests (described in the exercises) that form the basis for efficient probabilistic primality testing. (see Chapter 7)

$$\begin{aligned} (b^2)^{280} &= 1 \pmod{3} \quad \checkmark \\ (b^{10})^{56} &= 1 \pmod{11} \\ (b^{16})^{35} &= 1 \pmod{17} \end{aligned}$$

$$17 \times 11 \times 3 = 561 \text{ عدد هو اولي}$$

$$\begin{aligned} 561 &\text{ عدد غير زوجي حقيقى} \\ b^{n-1} &\equiv 1 \pmod{n} \\ \gcd(561, b) &\text{ عدد} \end{aligned}$$

الجذر البدئي

# Primitive Roots

**Definition:** A primitive root modulo a prime  $p$  is an integer  $r$  in  $\mathbb{Z}_p$  such that every nonzero element of  $\mathbb{Z}_p$  is a power of  $r$ .  
يمكن تمثيل أي عدد غير صفري في الأعداد البسيطة كقوة لـ  $r$ .

**Example:** Since every element of  $\mathbb{Z}_{11}$  is a power of 2, 2 is a primitive root of 11.

Powers of 2 modulo 11:  $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^{10} = 2$ .

**Example:** Since not all elements of  $\mathbb{Z}_{11}$  are powers of 3, 3 is not a primitive root of 11.

Powers of 3 modulo 11:  $3^1 = 3, 3^2 = 9, 3^3 = 5, 3^4 = 4, 3^5 = 1$ , and the pattern repeats for higher powers.

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

كل رقم أدنى له جذر بدائي

$$\begin{aligned}
 2^1 &= 2 \pmod{11} \\
 2^2 &= 4 \pmod{11} \\
 2^3 &= 8 \pmod{11} \\
 2^4 &= 5 \pmod{11} \\
 2^5 &= 10 \pmod{11} \\
 2^6 &= 9 \pmod{11} \\
 2^7 &= 7 \pmod{11} \\
 2^8 &= 3 \pmod{11} \\
 2^9 &= 6 \pmod{11} \\
 2^{10} &= 1 \pmod{11}
 \end{aligned}$$

جميع الأعداد من 1 إلى 10  
 يمكن تصنيفها إلى مجموعتين  
 زوجية و فردية  
 mod 11

مخبر 3

$$\begin{aligned}
 3^1 &= 3 \pmod{11} \\
 3^2 &= 9 \pmod{11} \\
 3^3 &= 5 \pmod{11} \\
 3^4 &= 4 \pmod{11} \\
 3^5 &= 1 \pmod{11}
 \end{aligned}$$

في هذا المثال  
 من 1 إلى 10  
 يمكن تصنيفها إلى مجموعتين  
 زوجية و فردية  
 mod 11

الخوارزمية المنفصلة

لدينا عدد أولي  $P$  ، لدينا جذر  $r$  ولدينا عدد  $a$   
 $a \geq 1$  ،  $a \leq P-1$  ،  $a$  و  $P-1$  نساهما

$$\begin{aligned}
 \log_2 100 &= 10 \\
 100 \pmod{15} &= 10
 \end{aligned}$$

$$r^e \pmod{p} = a$$

$$\begin{aligned}
 \log_r a &= e \\
 r^e &= a \pmod{p}
 \end{aligned}$$



الدوئاربية الحنوف

# Discrete Logarithms

Suppose  $p$  is prime and  $r$  is a primitive root modulo  $p$ . If  $a$  is an integer between 1 and  $p - 1$ , that is an element of  $\mathbb{Z}_p$ , there is a unique exponent  $e$  such that  $r^e = a$  in  $\mathbb{Z}_p$ , that is,  $r^e \bmod p = a$ .

**Definition:** Suppose that  $p$  is prime,  $r$  is a primitive root modulo  $p$ , and  $a$  is an integer between 1 and  $p - 1$ , inclusive. If  $r^e \bmod p = a$  and  $1 \leq e \leq p - 1$ , we say that  $e$  is the discrete logarithm of  $a$  modulo  $p$  to the base  $r$  and we write  $\log_r a = e$  (where the prime  $p$  is understood).

**Example 1:** We write  $\log_2 3 = 8$  since the discrete logarithm of 3 modulo 11 to the base 2 is 8 as  $2^8 = 3 \bmod 11$ .  $2^8 = 3 \bmod 11$

**Example 2:** We write  $\log_2 5 = 4$  since the discrete logarithm of 5 modulo 11 to the base 2 is 4 as  $2^4 = 5 \bmod 11$ .

There is no known polynomial time algorithm for computing the discrete logarithm of  $a$  modulo  $p$  to the base  $r$  (when given the prime  $p$ , a root  $r$  modulo  $p$ , and a positive integer  $a \in \mathbb{Z}_p$ ). The problem plays a role in cryptography as will be discussed in Section 4.6.