# 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

# Division

**Definition**: If $a$ and $b$ are integers with $a \neq 0$, then $a$ *divides* $b$ if there exists *an integer* $c$ such that $b = ac$.

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

**Example**: Determine whether $3 \mid 7$ and whether $3 \mid 12$.

# Properties of Divisibility

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

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

**Proof**: (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,

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

(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?

# 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.

**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).

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

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

q = a **div** d
r = a **mod** d

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

q = a **div** d
r = a **mod** d

# Division Algorithm

**Examples:**

- 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** $11$.

- 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 $3$.

# 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

$$a \not\equiv b \pmod{m}$$

# 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 $a - b$.

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

**Solution**:

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

# More on Congruences

**Theorem** 4: Let m be a positive integer. The integers *$a$ and $b$ are congruent modulo $m$* <u>if and only if</u> 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 $a \equiv b \pmod{m}$. ◀

# The Relationship between $(\text{mod } m)$ and $\textbf{mod } m$ Notations

- The use of "mod" in $a \equiv b \pmod{m}$ and $a \textbf{ mod } m = b$ are different.
  - $a \equiv b \pmod{m}$ is a relation on the set of integers.
  - In $a \textbf{ mod } m = b$, the notation **mod** denotes a function.
- 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 $a \equiv b \pmod{m}$ <u>if and only if</u> $a \text{ mod } m = b \text{ mod } m$. (*Proof in the exercises*)

# 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**:

- Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 4 there are integers $s$ and $t$ with $b = a + sm$ and $d = c + tm$.
- Therefore,
  - $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
  - $b\,d = (a + sm)\,(c + tm) = ac + m(at + cs + stm)$.
- Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

# Congruences of Sums and Products

**Theorem** 5: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

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

**Example:** Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 5 that

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

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

# Algebraic Manipulation of Congruences

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

  If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where $c$ is any integer (*holds by Theorem 5 with $d = c$*).
- Adding an integer to both sides of a valid congruence preserves validity.

  If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, 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.

# Algebraic Manipulation of Congruences

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

**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.)

# Computing the **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

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

and

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

(*proof in text*)

# Arithmetic Modulo *m*

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

- The operation $+_m$ is defined as $a +_m b = (a + b)$ **mod** $m$. This is *addition modulo m*.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b)$ **mod** $m$. 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:

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

# 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 $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.
  - Associativity: If $a$, $b$, and $c$ belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
  - Commutativity: If $a$ and $b$ belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
  - Identity elements: The elements 0 and 1 are identity elements for addition and multiplication modulo $m$, respectively.
    - If $a$ belongs to $\mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

*continued →*

# Arithmetic Modulo *m*

- 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 $0 +_m 0 = 0$
- Distributivity: If $a$, $b$, and $c$ belong to $\mathbf{Z}_m$, then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.
- Multiplicative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.
  - Note that modular multiplicative inverse a is b if a*b = 1 (mod m), where b is in {1,2, … , m-1}
  - Ex: 4 is modulo 11 inverse of 3, since 3*4=12=1 (mod 11)

# 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

# Representations of Integers

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

# Base $b$ Representations

- 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:

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

  where $k$ is a nonnegative integer, $a_0, a_1, \ldots.\ a_k$ are nonnegative integers less than $b$, and $a_k \neq 0$. The $a_j$, $j = 0,\ldots,k$ 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 $(a_k a_{k-1} \ldots. a_1 a_0)_b$.
- We usually omit the subscript 10 for base 10 expansions.

# Binary Expansions

Most computers represent integers and do arithmetic with binary (base 2) expansions of integers. In these expansions, the only digits used are 0 and 1.

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

**Solution**:

$(1\ 0101\ 1111)_2 = 1\cdot2^8 + 0\cdot2^7 + 1\cdot2^6 + 0\cdot2^5 + 1\cdot2^4 + 1\cdot2^3 + 1\cdot2^2 + 1\cdot2^1 + 1\cdot2^0 = 351.$

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

**Solution**: $(11011)_2 = 1\cdot2^4 + 1\cdot2^3 + 0\cdot2^2 + 1\cdot2^1 + 1\cdot2^0 = 27.$

# Octal Expansions

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 $(7016)_8$ ?

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

# Hexadecimal Expansions

The hexadecimal expansion needs 16 digits, 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**:

$$2\cdot16^4 + 10\cdot16^3 + 14\cdot16^2 + 0\cdot16^1 + 11\cdot16^0 = 175627$$

# Base Conversion

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

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

  $n = bq_0 + a_0 \quad 0 \leq a_0 \leq b$
- The remainder, $a_0$ , is the rightmost digit in the base $b$ expansion of $n$. Next, divide $q_0$ by $b$.

  $q_0 = bq_1 + a_1 \quad 0 \leq a_1 \leq b$
- 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 $b$ digits as the remainder. The process terminates when the quotient is $0$.

*continued* →

# Base Conversion

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

**Solution**: Successively dividing by 8 gives:

- $12345 = 8 \cdot 1543 + 1$
- $1543 = 8 \cdot 192 + 7$
- $192 = 8 \cdot 24 + 0$
- $24 = 8 \cdot 3 + 0$
- $3 = 8 \cdot 0 + 3$

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

# Comparison of Hexadecimal, Octal, and Binary Representations

**TABLE 1** Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

| Decimal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Hexadecimal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| Octal | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| Binary | 0 | 1 | 10 | 11 | 100 | 101 | 110 | 111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |

Initial 0s are not shown

Each octal digit corresponds to a block of 3 binary digits.
Each hexadecimal digit corresponds to a block of 4 binary digits.
So, conversion between binary, octal, and hexadecimal is easy.

# Conversion Between Binary, Octal, and Hexadecimal Expansions

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

**Solution**:

- 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 $(3EBC)_{16}$.

# 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 $(a_{n-1}, a_{n-2}, \ldots, a_0)_2$ and $(b_{n-1}, b_{n-2}, \ldots, b_0)_2$, 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($s_0, s_1, \ldots, s_n$){the binary expansion of the sum is $(s_n, s_{n-1}, \ldots, s_0)_2$}

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

# 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 $(a_{n-1}, a_{n-2}, \ldots, a_0)_2$ and $(b_{n-1}, b_{n-2}, \ldots, b_0)_2$, respectively}
for $j := 0$ to $n - 1$
    if $b_j = 1$ then $c_j = a$ shifted $j$ places
    else $c_j := 0$
{$c_0, c_1, \ldots, c_{n-1}$ 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 $O(n^2)$.

# Binary Modular Exponentiation

- In cryptography, it is important to be able to find $b^n$ **mod** $m$ efficiently, where $b$, $n$, and $m$ are large integers.
- Use the binary expansion of $n$ *(the exponent)*, $n = (a_{k-1},\ldots,a_1,a_0)_2$, to compute $b^n$.

  Note that:

  [redacted]

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

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

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

*continued* →

# Binary Modular Exponentiation Algorithm

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

procedure *modular exponentiation*($b$: integer, $n = (a_{k-1}a_{k-2}\ldots a_1a_0)_2$ , $m$: positive integers)
$x := 1$
power := b **mod** m
for $i := 0$ to $k - 1$
  if $a_i = 1$ then $x := (x \cdot \mathit{power})$ mod $m$
  $\mathit{power} := (\mathit{power} \cdot \mathit{power})$ mod $m$
return $x$ {$x$ equals $b^n$ mod $m$ }

Go over this algorithm using b=3, n=5 , m=8

Also check the Solution in Example 12 from the Book

# 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

# Primes

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

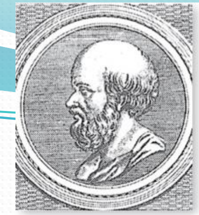
**Example**: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

# The Fundamental Theorem of Arithmetic

**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**:

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



Erastothenes
(276-194 B.C.)

# The Sieve of Erastosthenes

- The *Sieve of Erastosthenes* 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.
  a. Delete all the integers, other than 2, divisible by 2.
  b. Delete all the integers, other than 3, divisible by 3.
  c. Next, delete all the integers, other than 5, divisible by 5.
  d. Next, delete all the integers, other than 7, divisible by 7.
  e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

{2,3,5,7,11,15,1719,23,29,31,37,41,43,47,53,

59,61,67,71,73,79,83,89, 97}

*continued →*

# The Sieve of Erastosthenes

**TABLE 1** **The Sieve of Eratosthenes.**

*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 |

*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 |

*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 |

*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 |

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 $b \leq \sqrt{n}$.

*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 $i$.

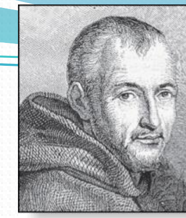

Euclid
(325 B.C.E. – 265 B.C.E.)

# Infinitude of Primes

Theorem: There are infinitely many primes. (Euclid)

**Proof**: Assume finitely many primes: $p_1, p_2, \ldots.., p_n$

- Let $q = p_1p_2\cdots p_n + 1$
- Either $q$ is prime or by the fundamental theorem of arithmetic it is a product of primes.
  - But none of the primes $p_j$ divides $q$ since if $p_j \mid q$, then $p_j$ divides $q - p_1p_2\cdots p_n = 1$ .
  - Hence, there is a prime not on the list $p_1, p_2, \ldots.., p_n$. It is either $q$, or if $q$ is composite, it is a prime factor of $q$. This contradicts the assumption that $p_1, p_2, \ldots.., p_n$ are all the primes.
- Consequently, there are infinitely many primes.



Marin Mersenne
(1588-1648)

# Mersene Primes

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

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$ , and $2^7 - 1 = 127$ are Mersene primes.
- $2^{11} - 1 = 2047$ is not a Mersene prime since $2047 = 23 \cdot 89$.
- There is an efficient test for determining if $2^p - 1$ is prime.
- The largest known prime numbers are Mersene primes.
- As of mid 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/

# 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 $x$.

  **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 $x/\ln x$.
  - The odds that a randomly selected positive integer less than $n$ is prime are approximately $(n/\ln n)/n = 1/\ln n$.

# Generating Primes

- The problem of generating large primes is of both theoretical and practical interest.
- 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 $1,2,\ldots, 40$. 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 $n$.

# Greatest Common Divisor

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

One can find greatest common divisors of small numbers by inspection.

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

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

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

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

# Greatest Common Divisor

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

**Example**: 17 and 22

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

**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.

# Finding the Greatest Common Divisor Using Prime Factorizations

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

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

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

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

- 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:** $120 = 2^3 \cdot 3 \cdot 5$ $\quad 500 = 2^2 \cdot 5^3$

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

- 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.

# Least Common Multiple

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

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

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

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

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

- 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

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

# Euclidean Algorithm

Euclid
(325 B.C.E. – 265 B.C.E.)

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

**Example**: Find gcd(91, 287): Divide 287 by 91

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

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

*continued* →

# Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

```
procedure gcd(a, b: positive integers)
x := a
y := b
while   y ≠ 0
      r := x mod y
      x := y
      y := r
return x {gcd(a,b) is x}
```

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

# Correctness of Euclidean Algorithm

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

**Proof**:

- Suppose that $d$ divides both $a$ and $b$. Then $d$ also divides $a - bq = r$ (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, $\gcd(a,b) = \gcd(b,r)$. ◀

# Correctness of Euclidean Algorithm

- Suppose that a and b are positive integers with $a \geq b$.
  Let $r_0 = a$ and $r_1 = b$.
  Successive applications of the division algorithm yields:

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

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

Étienne Bézout
(1730-1783)

# 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)

**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*.

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

# 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 2nd equation into the 1st 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 Euclidian 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.

# 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 $a \mid c$.

**Proof**: Read from the book.

Lemma 3: If p is prime and $p \mid a_1a_2 \cdots a_n$, then $p \mid a_i$ for some i.

(*proof uses mathematical induction; see Exercise* 64 *of Section* 5.1)

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

# Uniqueness of Prime Factorization

- We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique.

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

$n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots p_t$.

- 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 divides , for some $k$, contradicting the assumption that and are distinct primes.

$p_{i_1}$ $q_{j_k}$

$p_{i_1}$ $q_{j_k}$

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

# 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).
- But dividing by an integer relatively prime to the modulus does produce a valid congruence:

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

**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, $a \equiv b \pmod{m}$. ◀

# 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

# Linear Congruences

**Definition**: A congruence of the form

$$ax \equiv b(\bmod m),$$

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

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

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

**Example**: $5$ is an inverse of $3$ modulo $7$ since $5 \cdot 3 = 15 \equiv 1 (\bmod 7)$

- 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 $x$.

# 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 $sa \equiv 1 \pmod{m}$
- Consequently, $s$ is an inverse of $a$ modulo $m$.
- The uniqueness of the inverse is Exercise 7.

# Finding Inverses

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

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

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

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

# Finding Inverses

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

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

$42620 = 45 \cdot 101 + 75$
$101 = 1 \cdot 75 + 26$
$75 = 2 \cdot 26 + 23$
$26 = 1 \cdot 23 + 3$
$23 = 7 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1$

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

Working Backwards:

$1 = 3 - 1 \cdot 2$
$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$
$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$
$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$
$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$
$\quad = 26 \cdot 101 - 35 \cdot 75$
$1 = 26 \cdot 101 - 35 \cdot (42620 - 45 \cdot 101)$
$\quad = -35 \cdot 42620 + 1601 \cdot 101$

Bézout coefficients : $-35$ and $1601$

1601 is an inverse of 101 modulo 42620

# Using Inverses to Solve Congruences

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

**Example**: What are the solutions of the congruence $3x \equiv 4(\bmod 7)$.

**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

$$-2 \cdot 3x \equiv -2 \cdot 4(\bmod 7).$$

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 $x \equiv 6 \pmod 7$. By Theorem $5$ of Section $4.1$, it follows that $3x \equiv 3 \cdot 6 = 18 \equiv 4(\bmod 7)$ which shows that all such $x$ satisfy the congruence.

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

# 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 $a^p \equiv a \pmod{p}$

(*proof outlined in Exercise* 19)

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

**Example**: Find $7^{222}$ **mod** 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, $7^{222}$ **mod** $11 = 5$.

# Pseudoprimes

- 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.

  $341 = 11 \cdot 31$

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

# Pseudoprimes

- Given a positive integer $n$, such that $2^{n-1} \equiv 1 \pmod{n}$:
  - If $n$ does not satisfy the congruence, it is composite.
  - 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 $b$.
  - For example, among the positive integers less than $10^{10}$ there are $455{,}052{,}512$ primes, but only $14{,}884$ pseudoprimes to the base $2$.