

Fundamentals of Computer Security

A scenic landscape featuring a large body of water, possibly a fjord or a wide river, surrounded by green, rocky hills. The sky is a deep blue with wispy white clouds. The sun is visible on the right side of the image, creating a bright reflection on the water's surface. The overall atmosphere is serene and natural.

Lecture 3

Number Theory and Cryptography (Modular Arithmetic)

"Only those who have the patience to do simple things perfectly will acquire the skills to do difficult things easily" James J. Corbett

Introduction to Number Theory

- The part of mathematics devoted to the study of the set of integers and their properties is known as **Number Theory**.

Introduction to Number Theory

- Number theory plays an essentially role both in
 1. Classical cryptography, first used thousands of years ago
 2. Modern cryptography, which plays an essential role in electronic communication.
- **Note:** Number theory, once considered the purest of subjects, has become an essential tool in providing computer and Internet security.

Divisibility and Modular Arithmetic

- Division of an integer by a positive integer produces a **quotient** and a **remainder**.
- Working with these remainders leads to modular arithmetic, which plays an important role in mathematics which is used throughout computer science.
- Important applications of modular arithmetic include
 1. Generating pseudorandom numbers
 2. Constructing check digits (for error detection)
 3. Encrypting messages

Divisibility and Modular Arithmetic

Definition (**Division**)

- If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer.
- When a divides b we say that a is a factor or divisor of b , and that b is a multiple of a . The notation $a|b$ denotes that a divides b . We write $a \nmid b$ when a does not divide b .

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

Divisibility and Modular Arithmetic

Definition (**Division**): Example

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

Solution:

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

Divisibility and Modular Arithmetic

Basic Properties of Divisibility

- Let $a, b, c \in \mathbb{Z}$ (integers), where $a \neq 0$. Then
 1. If $a|b$ and $a|c$, then $a|(b + c)$
 2. If $a|b$, then $a|bc \ \forall c \in \mathbb{Z}$
 3. If $a|b$ and $b|c$, then $a|c$

Divisibility and Modular Arithmetic

Proof (1)

Suppose that $a|b$ and $a|c$. Then, from the definition of divisibility, it follows that there are integers s and t with $b = as$ and $c = at$.

Hence,

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

Hence $a|(b + c)$

Divisibility and Modular Arithmetic

The Division Algorithm

- When an integer is divided by a positive integer, there is a **quotient** and a **remainder**, as per the division algorithm below.

Definition(Division Algorithm)

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

Divisibility and Modular Arithmetic

The Division Algorithm

- In the equality $a = dq + r$ for the division algorithm, d is called the **divisor**, a is called the **dividend**, q is called the **quotient**, and r is called the **remainder**.
- The notations used to express the quotient and remainder are:

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

Divisibility and Modular Arithmetic

The Division Algorithm

Remark: Note that both $a \operatorname{div} d$ and $a \bmod d$ for a fixed d are functions on the set of integers.

- Furthermore, when a is an integer and d is a positive integer, we have

$$a \operatorname{div} d = \frac{a}{d}$$

and

$$a \bmod d = a - d$$

Divisibility and Modular Arithmetic

The Division Algorithm

Example: What are the quotient and remainder when 1002 is divided by 11?

Solution: We have $1001 = 11 \cdot 91 + 1$

- Hence, the quotient when 1001 is divided by 11 is

$$91 = 1001 \operatorname{div} 11$$

and the remainder is

$$1 = 1001 \operatorname{mod} 11$$

Divisibility and Modular Arithmetic

Modular Arithmetic

- In some situations we care only about the remainder of an integer when it is divided by some specified positive integer.

Divisibility and Modular Arithmetic

- Before discussing congruences, let's review the definition and basic properties of equivalence relations

Equivalence Relations: This is a relationship on a set

- Let S be a set. A binary relation \sim on S is called an **equivalence relation** if it is

1. **Reflexive:** $a \sim a \quad \forall a \in S$
2. **Symmetric:** $a \sim b$ implies $b \sim a \quad \forall a, b \in S$
3. **Transitive:** $a \sim b$ and $b \sim c$ implies $a \sim c \quad \forall a, b, c \in S$

If \sim is an equivalence relation on S , then for $a \in S$ one defines its equivalence class as the set $\{x \in S : x \sim a\}$

Divisibility and Modular Arithmetic

Equivalence Relations

Example:

- The relation “is equal to”, denoted “=”, is an equivalence relation on the set of real numbers since for any $x, y, z \in \mathbb{R}$:
 1. (Reflexivity) $x = x$
 2. (Symmetry) if $x = y$ then $y = x$,
 3. (Transitivity) if $x = y$ and $y = z$ then $x = z$.

All of these are true!

Divisibility and Modular Arithmetic

Definition (Congruence)

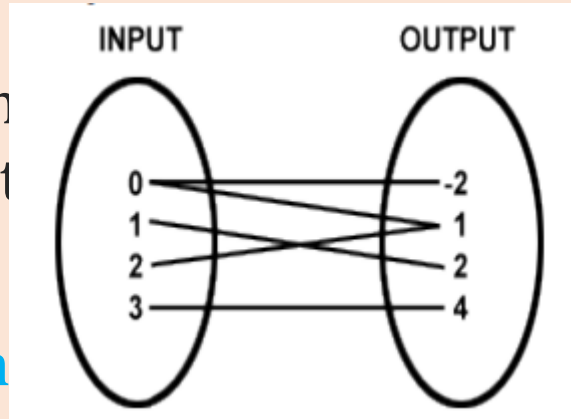
The “congruence” relation is an equivalence relation

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

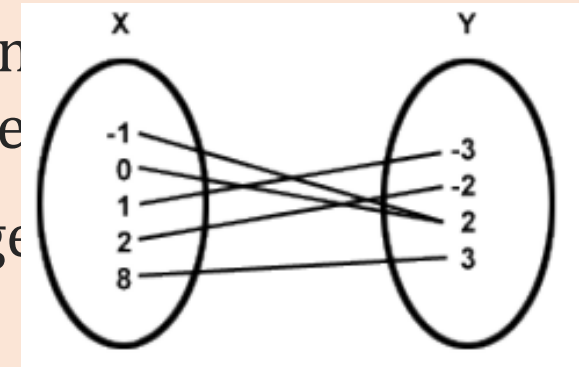
Divisibility and Modular Arithmetic

Modular Arithmetic

- Note: Although both “**mod**”, they represent
- The first represents represents a **function**



($\text{mod } m$) and
represent concepts
of integers



ude
ond

Relation: A relation is a set of inputs and outputs, often written as ordered pairs (input, output).

Function: A function is a relation in which each input x (domain) has only one output y (range).

Divisibility and Modular Arithmetic

Modular Arithmetic

- Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if (iff) $a \bmod m = b \bmod m$

Example

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

Solution: (by definition of congruency)

- Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod{6}$.
- However, because $24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$.

Divisibility and Modular Arithmetic

Modular Arithmetic

- **Note:** The concept of congruences was developed by a German mathematician **Karl Friedrich Gauss** at the end of the eighteenth century.
- This notion of congruences has played an important role in the development of number theory.

Divisibility and Modular Arithmetic

Modular Arithmetic

Theorem (Proven statement based on previously established statements): Let m be a positive integer. The integers a and b are congruent modulo m iff there is an integer k such that $a = b + km$

Proof:

→ If $a \equiv b \pmod{m}$, by the definition of congruence, we know that $m \mid (a - b)$. This means that there is an integer k such that $a - b = km$, so that $a = b + km$.

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

Divisibility and Modular Arithmetic

Modular Arithmetic

Theorem (Proven statement based on previously established statements):

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

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

and

$$ac \equiv bd \pmod{m}$$

Divisibility and Modular Arithmetic

Modular Arithmetic

Examples

Because $5 \equiv 7 \pmod{2}$ and $11 \equiv 17 \pmod{2}$, it follows from “Theorem” that

$$(16 = 5 + 11) \equiv (7 + 17 = 24) \equiv 0 \pmod{2}$$

and that

$$55 = 5 \cdot 11 \equiv 7 \cdot 17 = 119 \equiv 1 \pmod{2}$$

Divisibility and Modular Arithmetic

Modular Arithmetic

Caution!

- We must be careful working with congruences.
- Some properties we may expect to be true are not valid.
- For example, if $ac \equiv bc \pmod{m}$, the congruence $a \equiv b \pmod{m}$ may be false. (You cannot always divide both sides of a congruence by the same number!)
- Similarly, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, the congruence $ac \equiv bd \pmod{m}$ may be false.

Divisibility and Modular Arithmetic

Modular Arithmetic

Corollary(statement that follows readily from a previous statement)

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

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

and

$$a \cdot b \bmod m \equiv ((a \bmod m) \cdot (b \bmod m)) \bmod m$$

Divisibility and Modular Arithmetic

Arithmetic Modulo m

- We can define arithmetic operations on \mathbb{Z}_m , the set of non-negative integers less than m , that is, the set $\{0, 1, \dots, m - 1\}$.
- In particular, we define addition of these integers, denoted by $a +_m b = (a + b) \bmod m$, where the addition on the right-hand side of this equation is the ordinary addition of integers, and we define multiplication of these integers, by $a \cdot_m b = (a \cdot b) \bmod m$ where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers.
- The operations $+_m$ and \cdot_m are called “**addition modulo m** ” and “**multiplication modulo m** ” and when we use these operations, we are said to be doing **arithmetic modulo m** .

Modular Arithmetic

Definition (**Arithmetic modulo m**): \mathbb{Z}_m defined to be the set $\{0, \dots, m - 1\}$, equipped with two operations, $+$ and \times .

- Addition and multiplication in \mathbb{Z}_m work exactly like real addition and multiplication, except that the results are reduced modulo m .
- For example, suppose we want to compute 17×7 in \mathbb{Z}_5 .
- As integers, we have $17 \times 7 = 119$.
- To reduce 119 *modulo* 5, we just perform ordinary long division: $119 = 23 \times 5 + 4$, so $119 \bmod 5 = 4$, and hence $17 \times 7 = 4$ in \mathbb{Z}_5 .

Modular Arithmetic: Addition

- These definitions of addition and multiplication satisfy most of the familiar rules of arithmetic.

Properties of modular arithmetic, without proof

1. Addition is **closed**, i.e. $\forall a, b \in \mathbb{Z}_m, a + b \in \mathbb{Z}_m$
2. Addition is **commutative**, i.e. $\forall a, b \in \mathbb{Z}_m, (a + b) = (b + a)$.
3. Addition is **associative**, i.e.
$$\forall a, b, c \in \mathbb{Z}_m, (a + b) + c = a + (b + c)$$
4. 0 is an **additive identity**, i.e. $\forall a, a + 0 = 0 + a = a$
5. The **additive inverse** of any $\forall a \neq 0 \in \mathbb{Z}_m$ is $m - a$ i.e.
$$a + (m - a) = (m - a) + a = 0 \quad \forall a \in \mathbb{Z}_m$$

Modular Arithmetic: Multiplication

1. Multiplication is **closed**, i.e.

$$\forall a, b \in \mathbb{Z}_m, ab \in \mathbb{Z}_m$$

2. Multiplication is **commutative**, i.e.

$$\forall a, b \in \mathbb{Z}_m, ab = ba$$

3. Multiplication is **associative**, i.e.

$$\forall a, b, c \in \mathbb{Z}_m, (ab)c = a(bc)$$

4. 1 is a **multiplicative identity**, i.e.

$$\forall a \in \mathbb{Z}_m, a \times 1 = 1 \times a = a$$

5. Multiplication **distributes** over addition, i.e.

$$\forall a, b, c \in \mathbb{Z}_m, (a + b)c = (ac) + (bc) \text{ and } a(b + c) = (ab) + (ac)$$

Modular Exponentiation

- In cryptography it is important to be able to find $b^n \bmod m$ efficiently where b, n and m large integer. It is impractical to first compute b^n and then find its remainder when divided by m because b^n will be a huge number.
- Instead, we can use an algorithm that employs the binary expansion of the exponent n .
- Basic idea is how to use the binary expansion of n say $n = (a_{k-1} \dots a_1 a_0)_2$, to compute b^n .

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

- This shows that to compute b^n , we need only compute the values of $b, b^2, (b^2)^2 = b^4, (b^4)^2 = b^8, \dots, b^{2^k}$.

Modular Exponentiation

- Once we have these values, we multiply the terms b^{2^j} in this list, where $a_j = 1$. (For efficiency, after multiplying by each term, we reduce the result modulo m .) This gives us b^n .

Example:

To compute 3^9 , we have that $9 = (1001)_2$ so that $3^9 = 3^8 \cdot 3^1$.

By successively squaring, we find that $3^2 = 9$, $3^4 = 9^2 = 81$ and $3^8 = 81^2 = 6561$.

Consequently, $3^9 = 3^8 \cdot 3^1 = 6561 \cdot 3 = 19,683$

Try 3^{23}

Modular Exponentiation

Algorithm Exponentiation

ALGORITHM Modular Exponentiation.

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

Multiplication

Squaring

Modular Exponentiation

Algorithm Exponentiation

- The algorithm successively finds $b \bmod m, b^2 \bmod m, b^4 \bmod m, \dots, b^{2^{k-1}} \bmod m$ and multiplies together those terms $b^{2^j} \bmod m$ where $a_j = 1$, finding the remainder of the product when divided by m after each multiplication.
- Note: In this algorithm provides the most efficient algorithm available to compute values of the “**mod**” function.

Modular Exponentiation

Algorithm Exponentiation

Example 1: Use “Algorithm Exponentiation” to find $3^9 \bmod 5$

Solution: The algorithm initially sets $x = 1$ and $\text{power} = 3 \bmod 5$

Answer=3

Modular Exponentiation

Algorithm Exponentiation

Example 2: Use “Algorithm Exponentiation” to find $3^{644} \bmod 645$

Solution: The algorithm initially sets $x = 1$ and $\text{power} = 3 \bmod 645$

- In the computation of $3^{644} \bmod$, this algorithm determines $3^{2^j} \bmod 645$ for $j = 1, 2, \dots, 9$ (k) by successively squaring and reducing modulo 645.
- If $a_j = 1$ (where a_j is the bit in the j^{th} position in the binary expansion of 644, which is (1010000100), it multiplies the current value of x by $3 \bmod 645$ and reduces the result modulo 645.

Modular Exponentiation

Algorithm Exponentiation

Steps used:

- $i = 0$: Because $a_0 = 0$, we have $x = 1$ and $power = 3^2 \bmod 645 = 9 \bmod 645 = 9$;
- $i = 1$: Because $a_1 = 0$, we have $x = 1$ and $power = 9^2 \bmod 645 = 81 \bmod 645 = 81$;
- $i = 2$: Because $a_2 = 1$, we have $x = 1 \cdot 81 \bmod 645 = 81$ and $power = 81^2 \bmod 645 = 6561 \bmod 645 = 111$;
- $i = 3$: Because $a_3 = 0$, we have $x = 81$ and $power = 111^2 \bmod 645 = 12,321 \bmod 645 = 66$;
- $i = 4$: Because $a_4 = 0$, we have $x = 81$ and $power = 66^2 \bmod 645 = 4356 \bmod 645 = 486$;
- $i = 5$: Because $a_5 = 0$, we have $x = 81$ and $power = 486^2 \bmod 645 = 236,196 \bmod 645 = 126$;
- $i = 6$: Because $a_6 = 0$, we have $x = 81$ and $power = 126^2 \bmod 645 = 15,876 \bmod 645 = 396$;
- $i = 7$: Because $a_7 = 1$, we find that $x = (81 \cdot 396) \bmod 645 = 471$ and $power = 396^2 \bmod 645 = 156,816 \bmod 645 = 81$;
- $i = 8$: Because $a_8 = 0$, we have $x = 471$ and $power = 81^2 \bmod 645 = 6561 \bmod 645 = 111$;
- $i = 9$: Because $a_9 = 1$, we find that $x = (471 \cdot 111) \bmod 645 = 36$.

Modular Exponentiation

Algorithm Exponentiation

- The Algorithm produces the result $3^{644} \bmod 645 = 36$

Time Complexity: It is quite efficient because it uses $O((\log m)^2, \log n)$ bit operations to find $b^n \bmod m$

Primes and Greatest Common Divisors

Introduction

- An important concept based on divisibility is that of a prime number.
- A prime is an integer greater than 1 that is divisible by no positive integers other than 1 and itself.
- Thousands of years ago it was known that there are infinitely many primes; the proof of this fact, found in the works of Euclid, is famous for its elegance and beauty.

Primes and Greatest Common Divisors

Introduction

- Primes have become essential in modern cryptographic systems and some of their properties are important in cryptography.
 - For example, finding large primes is essential in modern cryptography.
 - The length of time required to factor large integers into their prime factors is the basis for the strength of some important modern cryptographic systems.

Primes and Greatest Common Divisors

PRIMES

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

Definition

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

Primes and Greatest Common Divisors

PRIMES

The Fundamental Theorem of Arithmetic: Every integer greater than 1 ($\forall a \in \mathbb{Z} > 1$) 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 non-decreasing size.

Example

The prime factorizations of 100, 641, 999, and 1024 are given by

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

$$641 = 1.641$$

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

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

Primes and Greatest Common Divisors

GCD

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

Definition

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

Primes and Greatest Common Divisors

GCD

- The greatest common divisor of two integers, both non zero, exists because the set of common divisors of these integers is **nonempty** and **finite**.
- The simplest way to find the greatest common divisor of two integers is to find all the positive common divisors of both integers and then take the largest divisor.

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

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

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

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

Primes and Greatest Common Divisors

RELATIVELY PRIME

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

- The integers 17 and 22 are relatively prime, because $\gcd(17, 22) = 1$.

Primes and Greatest Common Divisors

PAIRWISE PRIME

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

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

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

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

Primality Test

- It is often important to show that a given integer is prime.
- For instance, in cryptology large primes are used in some methods for making messages secret.
- One procedure for showing that an integer is prime is based on the following observation.

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

Primality Test

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

Proof

- If n is composite, by definition of a composite, we know that it has a factor a with $1 < a < n$. Hence by definition of a factor of a positive integer, we have $n = ab$ where b is a positive integer greater than 1.
- To proof by contradiction, we need to show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$
- If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > n$
- But $ab = n$, which is contradiction!
- Hence $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Primality Test

TRIAL DIVISION

- From above theorem, it follows that an integer is prime if it is not divisible by any prime less than or equal to its square root.
- This leads to the brute-force algorithm known as **trial division**.
- To use trial division we divide n by all primes not exceeding \sqrt{n} and conclude that n is prime if it is not divisible by any of these primes.

Example: Show that 101 is prime.

Solution: The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime.

Primality Test

TRIAL DIVISION

Example: Find the prime factorization of 7007.

- **Solution:** To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with $7007/7 = 1001$. Next, divide 1001 by successive primes, beginning with 7.
- It is immediately seen that 7 also divides 1001, because $1001/7 = 143$. Continue by dividing 143 by successive primes, beginning with 7. Although 7 does not divide 143, 11 does divide 143, and $143/11 = 13$. Because 13 is prime, the procedure is completed. It follows that $7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$. Consequently, the prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$.

Primality Test

Note:

1. Prime numbers were studied in ancient times for philosophical reasons.
2. Today, there are highly practical reasons for their study.
 - In particular, large primes play a crucial role in cryptography.

Primality Test

The Sieve of Eratosthenes

- The sieve of Eratosthenes is used to find all primes not exceeding a specified positive integer.
- For instance, the following procedure is used to find the primes not exceeding 100.

We conclude that the primes less than 100 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, and 97.

Primality Test

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

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

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

1	2	3	<u>4</u>	5	<u>6</u>	7	8	<u>9</u>	<u>10</u>
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
<u>21</u>	<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>
<u>51</u>	<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>
<u>81</u>	<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>	<u>99</u>	<u>100</u>

Primality Test

Integers divisible by 5 other than 5 receive an underline.

1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	<u>9</u>	<u>10</u>
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
<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>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>

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

1	2	3	<u>4</u>	5	<u>6</u>	7	<u>8</u>	<u>9</u>	<u>10</u>
11	<u>12</u>	13	<u>14</u>	<u>15</u>	<u>16</u>	17	<u>18</u>	19	<u>20</u>
<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>	<u>49</u>	<u>50</u>
51	<u>52</u>	53	<u>54</u>	<u>55</u>	<u>56</u>	<u>57</u>	<u>58</u>	59	<u>60</u>
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>	<u>77</u>	<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>
<u>91</u>	<u>92</u>	<u>93</u>	<u>94</u>	<u>95</u>	<u>96</u>	97	<u>98</u>	<u>99</u>	<u>100</u>

Primality Test

THE INFINITUDE OF PRIMES

- It has long been known that there are infinitely many primes.
- This means that whenever p_1, p_2, \dots, p_n are the n smallest primes, we know there is a larger prime not listed. We will prove this fact using a proof given by Euclid

Infinitude of Primes

Theorem: There are infinitely many primes.

Proof: We will prove this theorem using a **proof by contradiction**.

- We assume that there are only finitely many primes, p_1, p_2, \dots, p_n .
- Let $Q = p_1 p_2 \dots p_n + 1$
- By the fundamental theorem of arithmetic, Q is prime or else it can be written as the product of two or more primes.
- However, none of the primes p_j divides Q , for if $p_j | Q$ then p_j divides $Q - p_1 p_2 \dots p_n = 1$
- Hence, there is a prime not in the list p_1, p_2, \dots, p_n . This prime is either Q , if it is prime, or a prime factor of Q .
- This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes.

Infinitude of Primes

Mersenne primes

- Because there are infinitely many primes, given any positive integer there are primes greater than this integer.
- There is an ongoing quest to discover larger and larger prime numbers; for almost all the last 300 years, the largest prime known has been an integer of the special form $2^p - 1$ where p is also prime.
- Note that $2^n - 1$ cannot be prime when n is not prime;
- Such primes are called Mersenne primes.

Infinitude of Primes

Mersenne primes

Examples:

- The numbers $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ and $2^7 - 1 = 127$ are Mersenne primes
- While $2^{11} - 1 = 2047$ is not a Mersenne prime because $2047 = 23 \cdot 89$.

Prime Number Distribution

- How many primes are less than a positive number x ?
- This question interested mathematicians for many years; in the late 18th century, mathematicians produced large tables of prime numbers to gather **evidence concerning the distribution of primes**.
- Using this evidence, the great mathematicians of the day, including Gauss and Legendre, came up (without proof), the following theorem .

THE 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 .)

EUCLIDEAN ALGORITHM

Introduction

- Computing the greatest common divisor of two integers directly from the prime factorizations of these integers is inefficient.
- The reason is that it is time-consuming to find prime factorizations.
- We need a more efficient method of finding the greatest common divisor, called the **Euclidean algorithm**.
- Before describing the Euclidean algorithm, we will show how it is used to find $\text{gcd}(91, 287)$.
- First, divide 287, the larger of the two integers, by 91, the smaller, to obtain $287 = 91 \cdot 3 + 14$.

EUCLIDEAN ALGORITHM

- Any divisor of 91 and 287 must also be a divisor of $287 - 91 \cdot 3 = 14$.
- Also, any divisor of 91 and 14 must also be a divisor of $287 = 91 \cdot 3 + 14$.
- Hence, the greatest common divisor of 91 and 287 is the same as the greatest common divisor of 91 and 14.
- This means that the problem of finding $\gcd(91, 287)$ has been reduced to the problem of finding $\gcd(91, 14)$.
- Next, divide 91 by 14 to obtain $91 = 14 \cdot 6 + 7$.

EUCLIDEAN ALGORITHM

- Because any common divisor of 91 and 14 also divides $91 - 14 \cdot 6 = 7$ and any common divisor of 14 and 7 divides 91, it follows that $\gcd(91, 14) = \gcd(14, 7)$.
- Continue by dividing 14 by 7, to obtain $14 = 7 \cdot 2$.
- Because 7 divides 14, it follows that $\gcd(14, 7) = 7$.
- Furthermore, because $\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$, the original problem has been solved.

EUCLIDEAN ALGORITHM

- How the Euclidean algorithm works generally.
- Use successive divisions to reduce the problem of finding the greatest common divisor of two positive integers to the same problem with smaller integers, until one of the integers is zero.

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

EUCLIDEAN ALGORITHM

- Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

$$r_0 = r_1 q_1 + r_2 \qquad 0 \leq r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 < r_2$$

•

•

•

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

$$r_{n-1} = r_n q_n + 0.$$

EUCLIDEAN ALGORITHM

- Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms.
- Furthermore, it follows that
$$\begin{aligned}\gcd(a, b) &= \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) \\ &= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n\end{aligned}$$
- Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

EUCLIDEAN ALGORITHM

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

Solution: Successive uses of the division algorithm give:

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

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

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

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

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

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

Example: $d = \gcd(1970, 1066)$

1970	=	1	×	1066	+	904
1066	=	1	×	904	+	162
904	=	5	×	162	+	94
162	=	1	×	94	+	68
94	=	1	×	68	+	26
68	=	1	×	26	+	16
26	=	1	×	16	+	10
16	=	1	×	10	+	6
10	=	1	×	6	+	4
6	=	1	×	4	+	2
4	=	2	×	2	+	0

$$d = \gcd(1066, 904)$$

$$d = \gcd(904, 162)$$

$$d = \gcd(162, 94)$$

$$d = \gcd(94, 68)$$

Result: $\gcd(1970, 1066) = 2$, i.e., the last nonzero residue in the above computation

$$d = \gcd(68, 26)$$

$$d = \gcd(26, 16)$$

$$d = \gcd(16, 10)$$

$$d = 2$$

EUCLIDEAN ALGORITHM

ALGORITHM The Euclidean Algorithm.

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

$x := a$

$y := b$

while $y \neq 0$

$r := x \bmod y$

$x := y$

$y := r$

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