Fundamentals of Computer Security

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 $\frac{\mathrm{b}}{a}$ 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 ∤ b when a does not divide b.

Remark: We can express a|b using quantifiers as $\exists c\colon\ ac = b$, 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 $0 < dk = n$, or with $0 < \mathrm{k} = \frac{\mathrm{n}}{\mathrm{d}}$.
- 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:

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

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

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

and the remainder is

$$1 = 1001 \bmod 11$$

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, lets 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: $a{\sim}a \qquad \forall a \in S$
2. Symmetric: $a{\sim}b$ implies $\mathrm{b}{\sim}a \quad \forall a, b \in S$
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 $\mathrm{a} \in S$ one defines its equivalence class as the set $\{\mathrm{x} \in S: x{\sim}a\}$

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 $\mathrm{x, y, z} \in \mathbb{R}$:

1. (Reflexivity) $x = x$
2. (Symmetry) if $x = \mathrm{y}$ then $\mathrm{y} = x$,
3. (Transitivity) if $x = \mathrm{y}$ and $\mathrm{y} = \mathrm{z}$ then $x = \mathrm{z}$.

All of these are true!

Divisibility and Modular Arithmetic

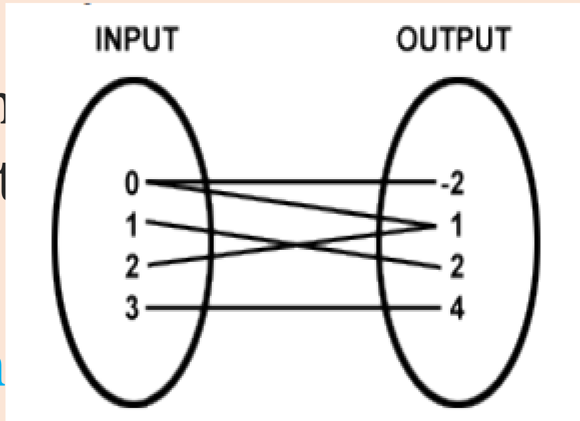
Definition (Congruence)

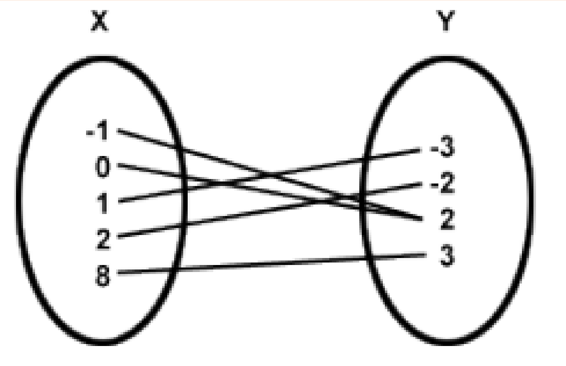
The "congruence" relation is an equivalence relation

- 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 $a \equiv b \ (mod\ m)$ to indicate that a is congruent to b modulo m.
- We say that $a \equiv b \ (mod\ m)$ is a congruence and that m is its modulus (plural moduli).
- If a and b are not congruent modulo m, we write $a \not\equiv b \ (mod\ m)$

Divisibility and Modular Arithmetic

Modular Arithmetic





- Note: Although both
od m) an
ude
"mod", they represent
rent conce
- The first represents
of intege
ond
represents a function

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 $a \equiv b\ (mod\ m)$ if and only if (iff) $\mathrm{a\ mod\ m = b\ mod\ m}$

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 ≡ 5 (mod 6).
- However, because 24 - 14 = 10 is not divisible by 6, we see that 24 ≢ 14 (mod 6).

Divisibility and Modular Arithmetic

Modular Arithmetic

- Note: The concept of congruences was developed by a German mathematician Karl Friedrich Gauss the 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 $\mathrm{a} = \mathrm{b} + \mathrm{km}$

Proof:

⇒ If $a \equiv b(mod\ m),$ 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 $a \equiv b(mod\ m).$

Divisibility and Modular Arithmetic

Modular Arithmetic

Theorem (Proven statement based on previously established statements):

Let m be a positive integer. If $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$, then

$$a + c \equiv b + d(mod\ m)$$

and

$$ac \equiv bd\ (mod\ m)$$

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 $ac \equiv bc \ (mod\ m)$, the congruence $a \equiv b(mod\ m)$ may be false. (You cannot always divide both sides of a congruence by the same number!)
- Similarly, if $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$, the congruence $ac \equiv b(mod\ m)$ 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

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

and

$$a.b \bmod m \equiv \big((a \bmod m).(b \bmod m)\big)\bmod m$$

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 $\{0,1, \dots , \mathrm{m}-1\}$.
- In particular, we define addition of these integers, denoted by $\mathrm{a} +_{\mathrm{m}} \mathrm{b} = (\mathrm{a}+\mathrm{b}) \bmod \mathrm{m}$, 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 $\mathrm{a} \cdot_{\mathrm{m}} \mathrm{b} = (\mathrm{a}.\mathrm{b}) \bmod \mathrm{m}$ where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers.
- The operations $+_{\mathrm{m}}$ and $\cdot_{\mathrm{m}}$ 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 $\{0, \ldots, \mathrm{m}-1\}$, 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 $119 \; mod \; 5 = 4$, 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 $\forall a \neq 0 \in \mathbb{Z}_m$ $is\ m - a\ i.e.$
$$a + (m - a) = (m - a) + a = 0 \; \forall \; a \in \mathbb{Z}_m$$

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

Modular Exponentiation

- In cryptography it is important to be able to find $b^n \mathrm{mod}\, m$ 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 $n = (a_{k-1} \ldots a_1 a_0)_2$, to compute b^n.

Note: $b^n = b^{a_{k-1}.2^{k-1}+\cdots+a_1.2^1+a_0} = b^{a_{k-1}.2^{k-1}} \ldots b^{a_1.2} b^{a_0}$

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

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.

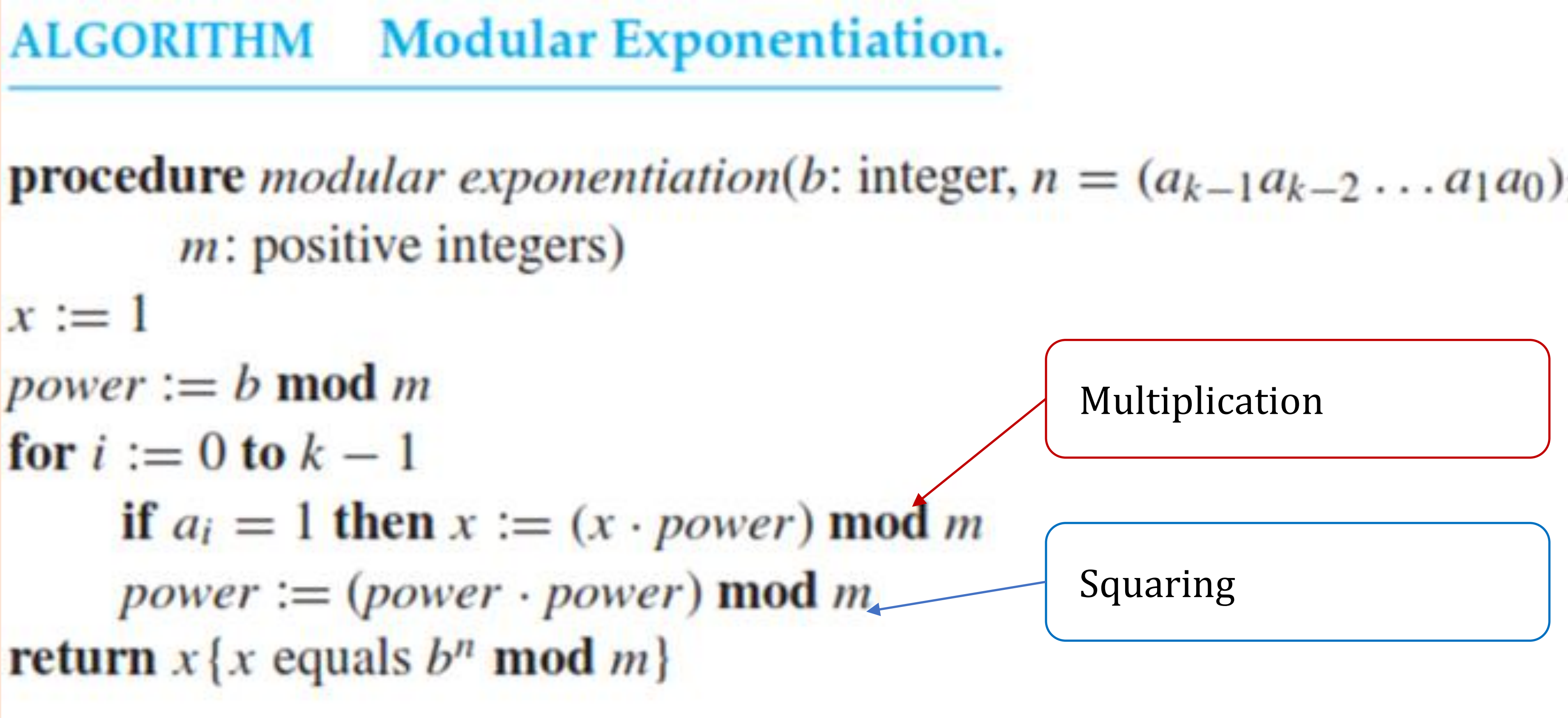
Example:

To compute 3^9, we have that $9 = (1001)_2$ so that $3^9 = 3^8 . 3^1$.
By successively squaring, we find that $3^2 = 9, 3^4 = 9^2 = 81$ and $3^8 = 81^2 = 6561$.
Consequently, $3^9 = 3^8 . 3^1 = 6561.3 = 19{,}683$

Try 3^{23}

Modular Exponentiation

Algorithm Exponentiation



ALGORITHM Modular Exponentiation.

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

Multiplication

Squaring

Modular Exponentiation

Algorithm Exponentiation

- The algorithm successively finds $b \; mod \; m, b^2 \; mod \; m, b^4 \; mod \; m, \dots, b^{2^{k-1}} \; mod \; m$ and multiplies together those terms $b^{2^j} mod \; m$ 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 $3^9 mod\ 5$

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

Answer=3

Modular Exponentiation

Algorithm Exponentiation

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

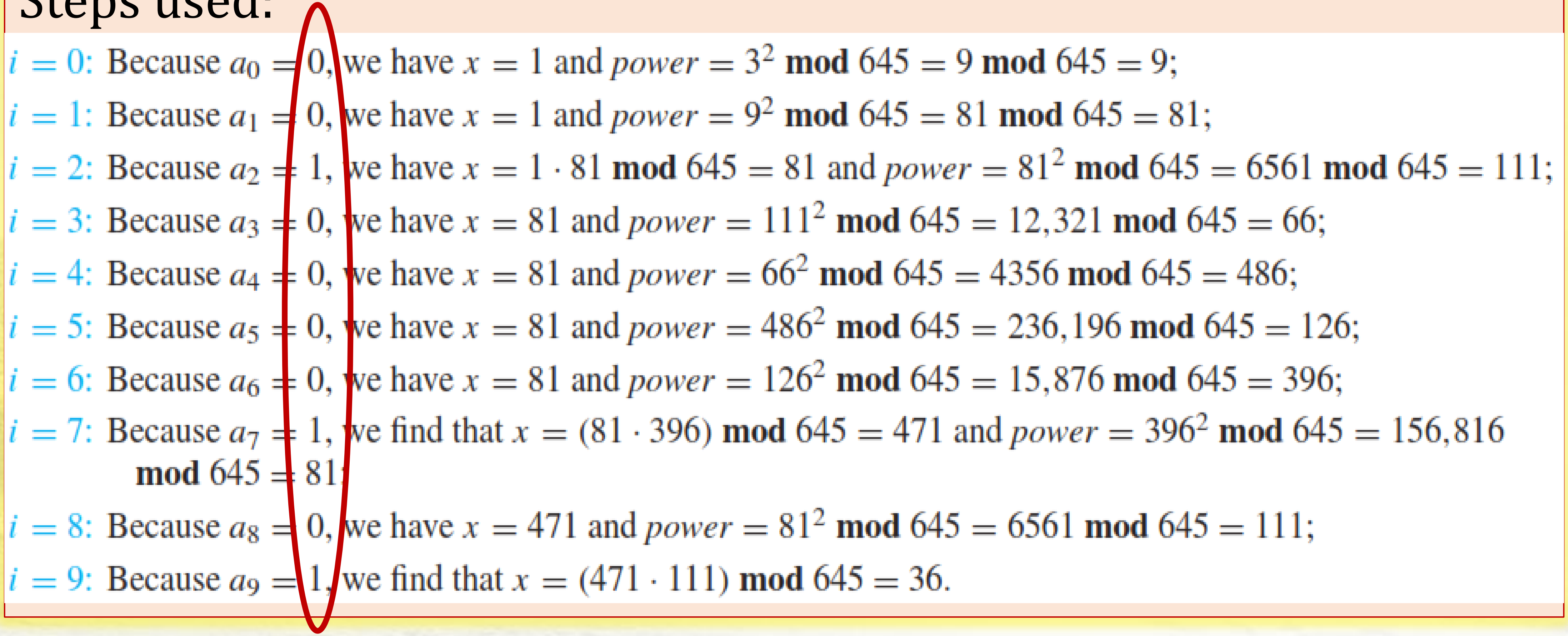
Solution: The algorithm initially sets $\mathrm{x} = 1$ and $\mathrm{power} = 3\ mod\ 645$

- In the computation of $3^{644} mod$, this algorithm determines $3^{2^j} mod\ 645$ for $j = 1,2, \ldots, 9\ \ (k)$ by successively squaring and reducing modulo 645.
- If $\mathrm{a}_j = 1$ (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 $3\ mod\ 645$ and reduces the result $modulo\ \ 645$.

Modular Exponentiation

Algorithm Exponentiation

Steps used:



$i = 0$: Because $a_0 = 0$, we have $x = 1$ and $power = 3^2$ **mod** $645 = 9$ **mod** $645 = 9$;

$i = 1$: Because $a_1 = 0$, we have $x = 1$ and $power = 9^2$ **mod** $645 = 81$ **mod** $645 = 81$;

$i = 2$: Because $a_2 = 1$, we have $x = 1 \cdot 81$ **mod** $645 = 81$ and $power = 81^2$ **mod** $645 = 6561$ **mod** $645 = 111$;

$i = 3$: Because $a_3 = 0$, we have $x = 81$ and $power = 111^2$ **mod** $645 = 12{,}321$ **mod** $645 = 66$;

$i = 4$: Because $a_4 = 0$, we have $x = 81$ and $power = 66^2$ **mod** $645 = 4356$ **mod** $645 = 486$;

$i = 5$: Because $a_5 = 0$, we have $x = 81$ and $power = 486^2$ **mod** $645 = 236{,}196$ **mod** $645 = 126$;

$i = 6$: Because $a_6 = 0$, we have $x = 81$ and $power = 126^2$ **mod** $645 = 15{,}876$ **mod** $645 = 396$;

$i = 7$: Because $a_7 = 1$, we find that $x = (81 \cdot 396)$ **mod** $645 = 471$ and $power = 396^2$ **mod** $645 = 156{,}816$ **mod** $645 = 81$;

$i = 8$: Because $a_8 = 0$, we have $x = 471$ and $power = 81^2$ **mod** $645 = 6561$ **mod** $645 = 111$;

$i = 9$: Because $a_9 = 1$, we find that $x = (471 \cdot 111)$ **mod** $645 = 36$.

Modular Exponentiation

Algorithm Exponentiation

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

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

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

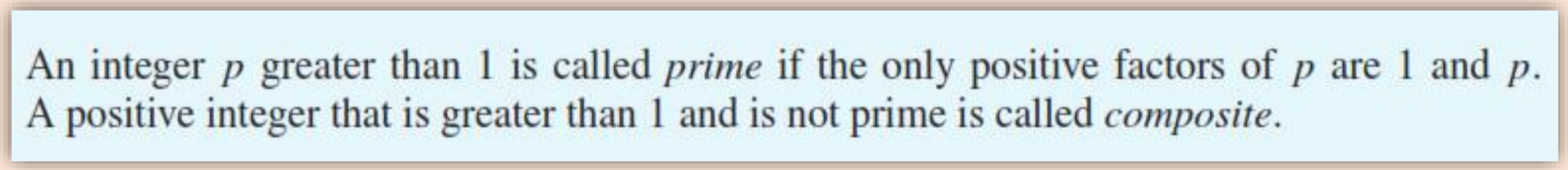
- Primes have become essential in modern cryptographic systems and some of their properties are important in cryptography.
  - For example, finding large primes is essential in modern cryptography.
  - The length of time required to factor large integers into their prime factors is the basis for the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

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

$$641 = 1.641$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3.37$$

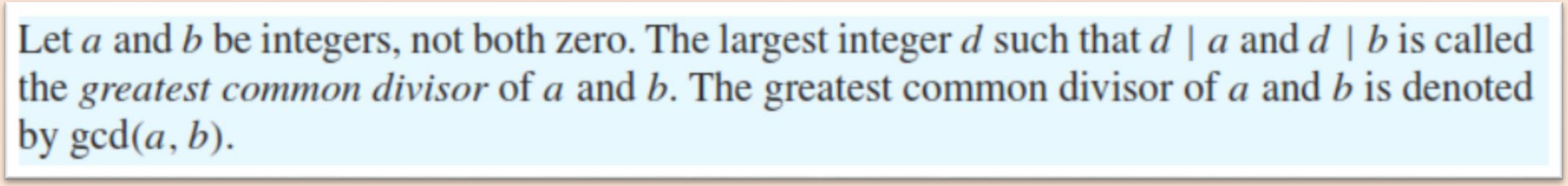
$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$$

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?

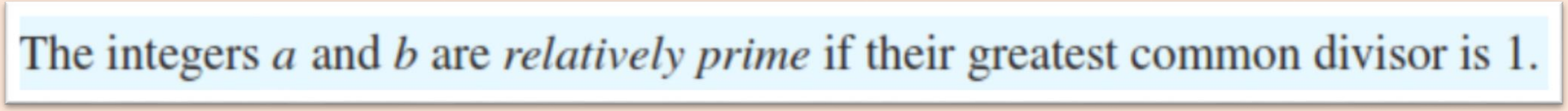
Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, $\gcd(24, 36) = 12$.

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

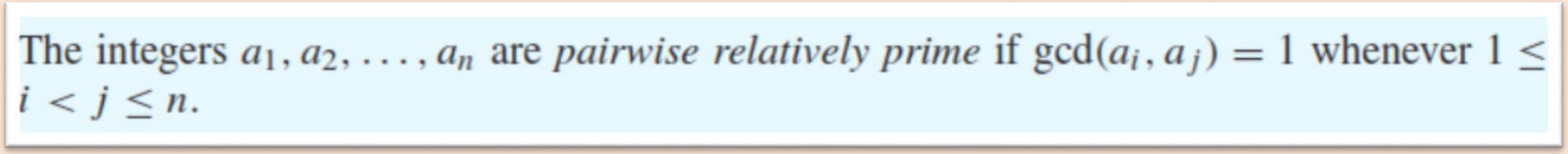


The integers *a* and *b* are *relatively prime* if their greatest common divisor is 1.

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

Primes and Greatest Common Divisors

PAIRWISE PRIME



The integers $a_1, a_2, \ldots, a_n$ 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 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 $\mathrm{b} > \sqrt{n}$, 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.

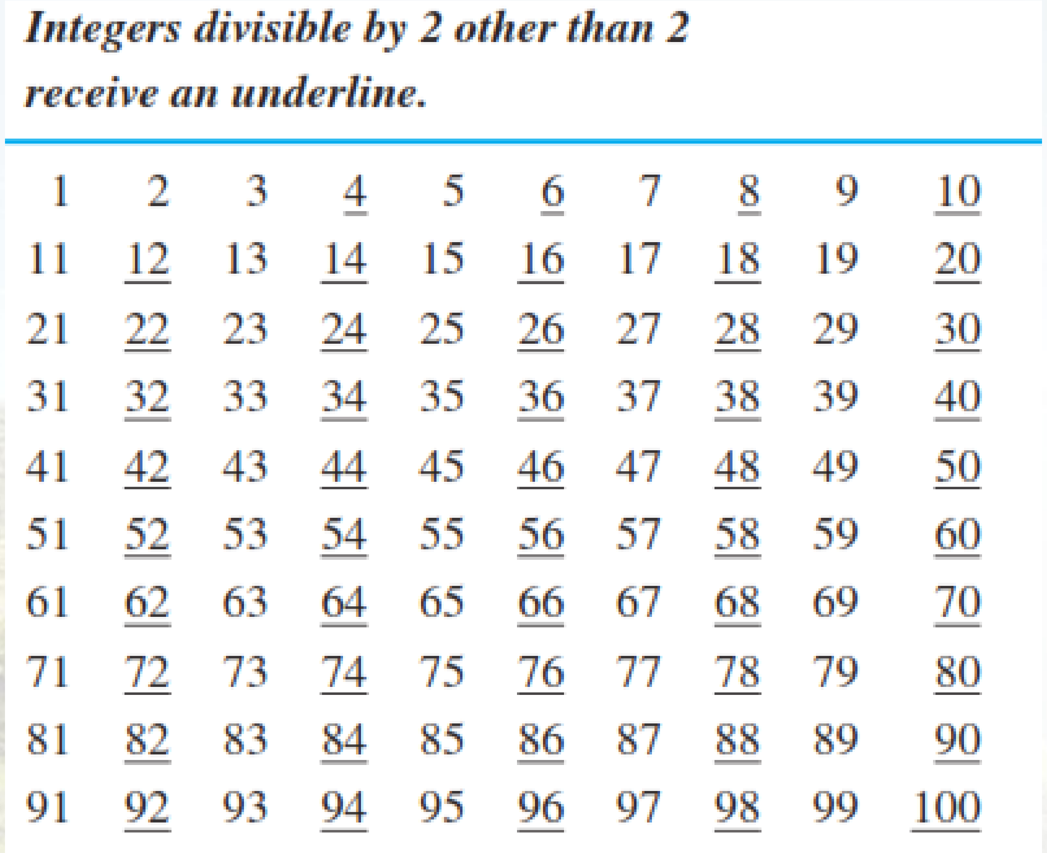
Primality Test

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.

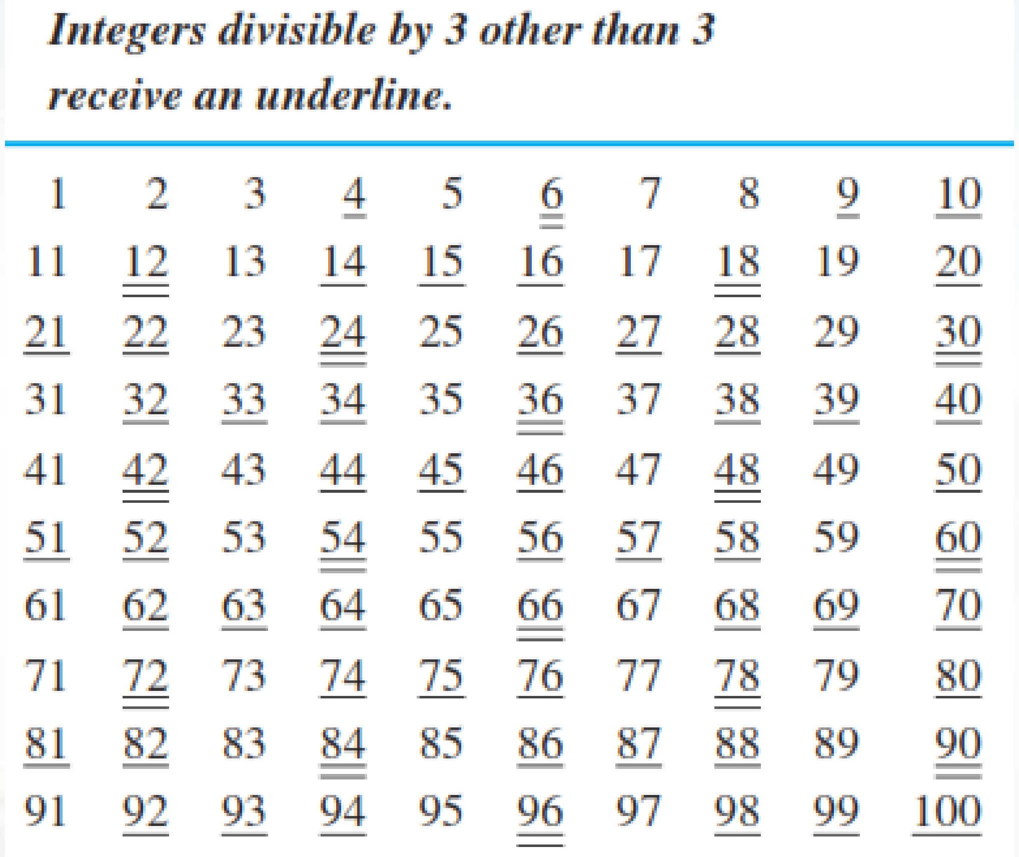
We conclude that the primes less than 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.

Primality Test



Integers divisible by 2 other than 2 receive an underline.

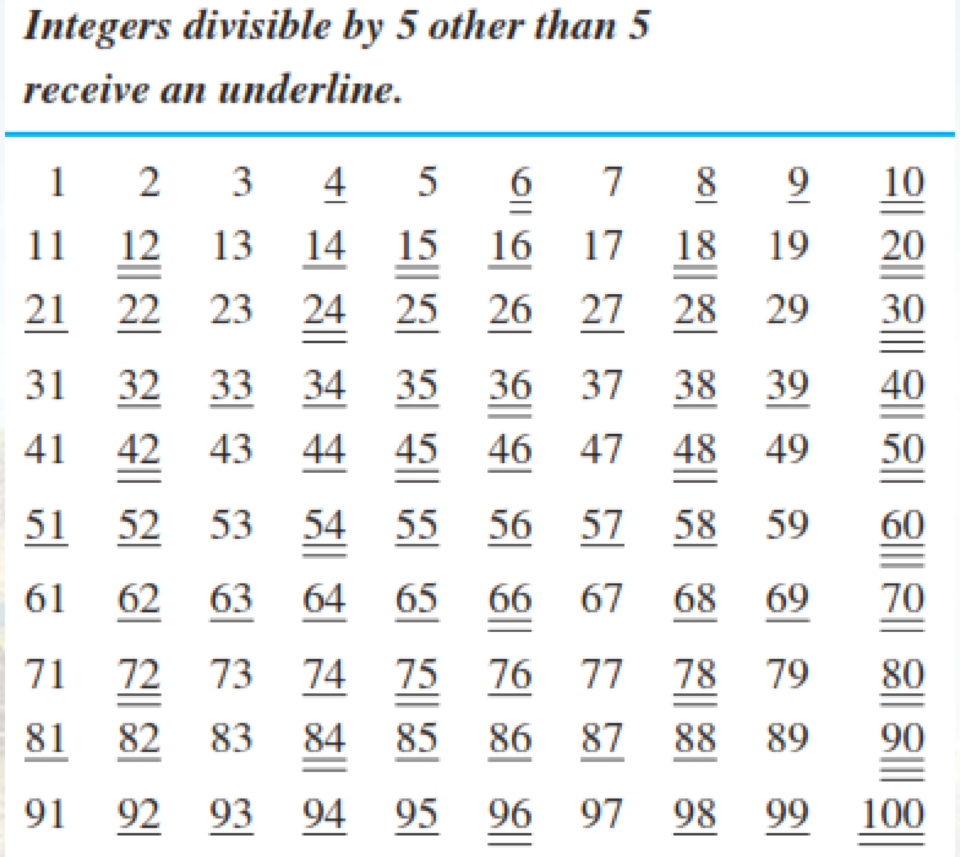
1	2	3	$\underline{4}$	5	$\underline{6}$	7	$\underline{8}$	9	$\underline{10}$
11	$\underline{12}$	13	$\underline{14}$	15	$\underline{16}$	17	$\underline{18}$	19	$\underline{20}$
21	$\underline{22}$	23	$\underline{24}$	25	$\underline{26}$	27	$\underline{28}$	29	$\underline{30}$
31	$\underline{32}$	33	$\underline{34}$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



Integers divisible by 3 other than 3 receive an underline.

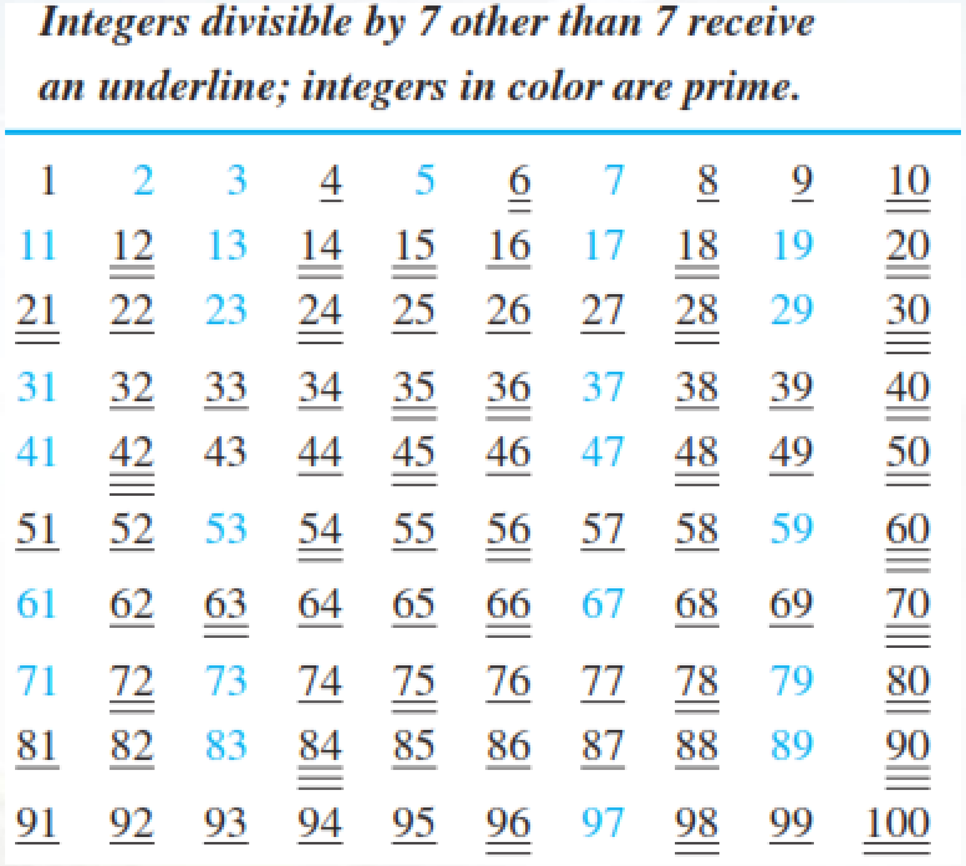
1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	8	$\underline{9}$	$\underline{10}$
11	$\underline{\underline{12}}$	13	$\underline{14}$	$\underline{15}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{20}$
$\underline{21}$	$\underline{22}$	23	$\underline{\underline{24}}$	25	$\underline{26}$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

Primality Test



Integers divisible by 5 other than 5 receive an underline.

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



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

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

Primality Test

THE INFINITUDE OF PRIMES

- It has long been known that there are infinitely many primes.
- This means that whenever $p_1, p_2, \ldots, p_n$ 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, $p_1, p_2, \ldots, p_n$.
- Let $Q = p_1 \, p_2 \; \ldots \; p_n + 1$
- 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 $Q - p_1 \, p_2 \; \ldots \; p_n = 1$
- Hence, there is a prime not in the list $p_1, p_2, \ldots, p_n$. 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 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

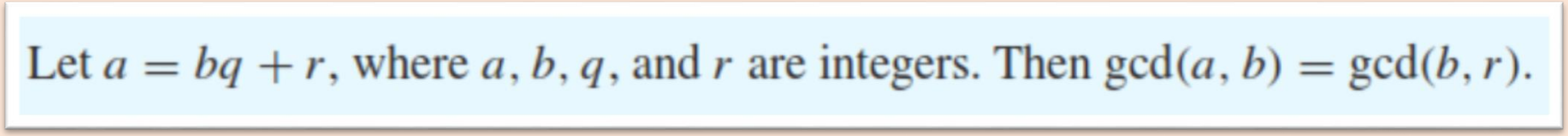
- Any divisor of 91 and 287 must also be a divisor of $287 - 91 \cdot 3 = 14$.
- Also, any divisor of 91 and 14 must also be a divisor of $287 = 91 \cdot 3 + 14$.
- Hence, the greatest common divisor of 91 and 287 is the same as the greatest common divisor of 91 and 14.
- This means that the problem 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 · 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 · 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

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) \\ = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

- 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:

$$
\begin{aligned}
662 &= 414 \cdot 1 + 248 \\
414 &= 248 \cdot 1 + 166 \\
248 &= 166 \cdot 1 + 82 \\
166 &= 82 \cdot 2 + 2 \\
82 &= 2 \cdot 41 + 0.
\end{aligned}
$$

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

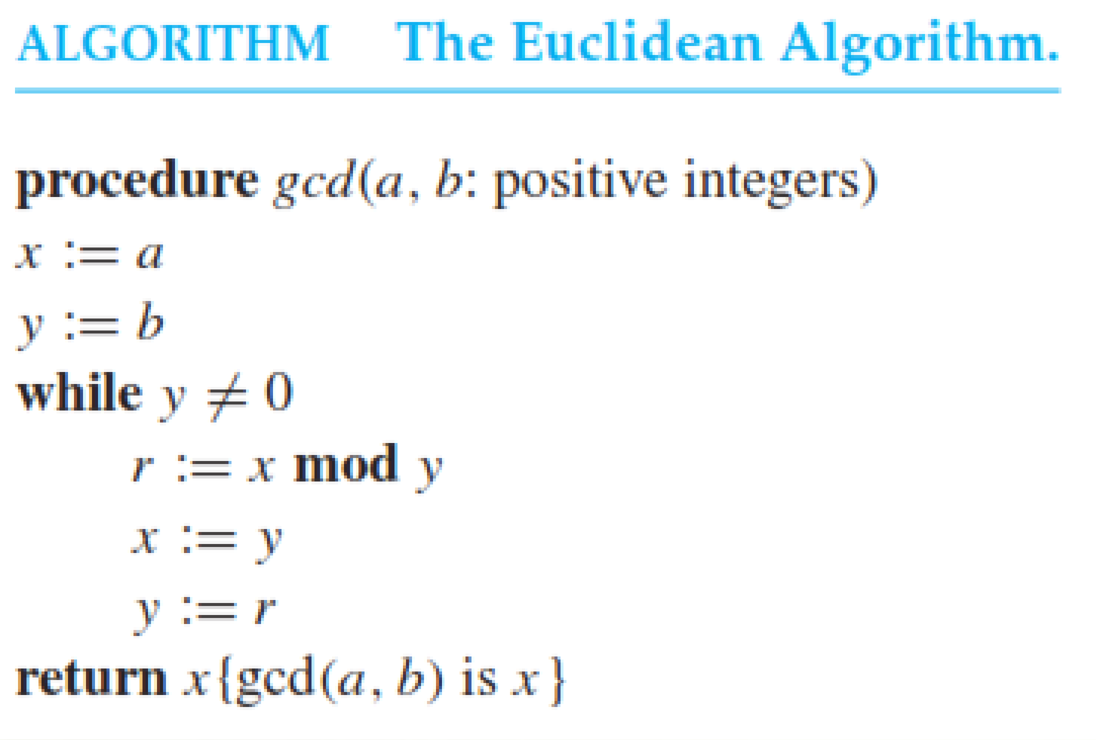
Example: d=gcd(1970,1066)

1970	=	1	×	1066	+	904
1066	=	1	×	904	+	162
904	=	5	×	162	+	94
16						
9						
6						
26	=	1	×	16	+	10
16	=	1	×	10	+	6
10	=	1	×	6	+	4
6	=	1	×	4	+	2
4	=	2	×	2	+	0

$\boldsymbol{d = gcd(1066, 904)}$
$\boldsymbol{d = gcd(904, 162)}$
$\boldsymbol{d = gcd(162, 94)}$
$\boldsymbol{d = gcd(94, 68)}$
$\boldsymbol{d = gcd(10, 6)}$
$\boldsymbol{d = gcd(6, 4)}$
$\boldsymbol{d = gcd(4, 2)}$
$\boldsymbol{d = 2}$

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

EUCLIDEAN ALGORITHM



ALGORITHM The Euclidean Algorithm.

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

Basic Notions of Finite Fields

The set of natural numbers is $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$, and the set of integers is $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Definition 1 (Divides). If $a, b \in \mathbb{Z}$, we say that a divides b, written $a | b$, if $ac = b$ for some $c \in \mathbb{Z}$. In this case, we say a is a divisor of b. We say that a does not divide b, written $a \nmid b$, if there is no $c \in \mathbb{Z}$ such that $ac = b$.

For example, we have $2 | 6$ and $-3 | 15$. Also, all integers divide 0, and 0 divides only 0. However, 3 does not divide 7 in $\mathbb{Z}$.

Definition 2 (Prime and Composite). An integer $n > 1$ is prime if the only positive divisors of n are 1 and n. We call n composite if n is not prime.

Basic Notions of Finite Fields

Definition 3(Group). A group is a set $\mathbb{G}$ equipped with a binary operation $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}$ and an identity element $1 \in \mathbb{G}$ such that:
1. $\forall a, b \in \mathbb{G}$, we have $(ab)c = a(bc)$.
2. For each a $\in \mathbb{G}$, we have a $.1 = 1. a = a$, and there exists b $\in \mathbb{G}$ such that a$b = 1$.

Definition 4 (Abelian Group). An abelian group is a group $\mathbb{G}$ such that $ab = ba, \forall a, b \in \mathbb{G}$.

Basic Notions of Finite Fields

Definition 5 (Ring). A ring $\mathbb{R}$ is a set equipped with binary operations × and +and elements $0,1 \in \mathbb{R}$ such that $\mathbb{R}$ is an abelian group under +, and $\forall a, b, c \in \mathbb{R}$ we have,

- a $.1 = 1. a = a$
- $(ab)c = a(bc)$
- a(b $+ c) = ab + bc$

If, in addition, $ab = ba, \forall a, b \in \mathbb{R}$, then we call $\mathbb{R}$ a commutative ring.

Basic Notions of Finite Fields

Definition 6 (Integers Modulo n). The ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n is the set of equivalence classes of integers modulo n. It is equipped with its natural ring structure:

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (\mathrm{a} + \mathrm{b}) + \mathrm{n}\mathbb{Z}$$

$$(a + n\mathbb{Z}).(b + n\mathbb{Z}) = (\mathrm{a}.\mathrm{b}) + \mathrm{n}\mathbb{Z}$$

Example

$$\mathbb{Z}/3\mathbb{Z}=\{\{\dots, -3,0,3, \dots\}, \{\dots, -2,1,4, \dots\}, \{\dots, -1,2,5, \dots\}\}$$

Basic Notions of Finite Fields

Modulo 7 Example

The elements in each column are congruent to each other modulo 7

…						
-21	-20	-19	-18	-17	-16	-15
-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	**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
…						

Basic Notions of Finite Fields

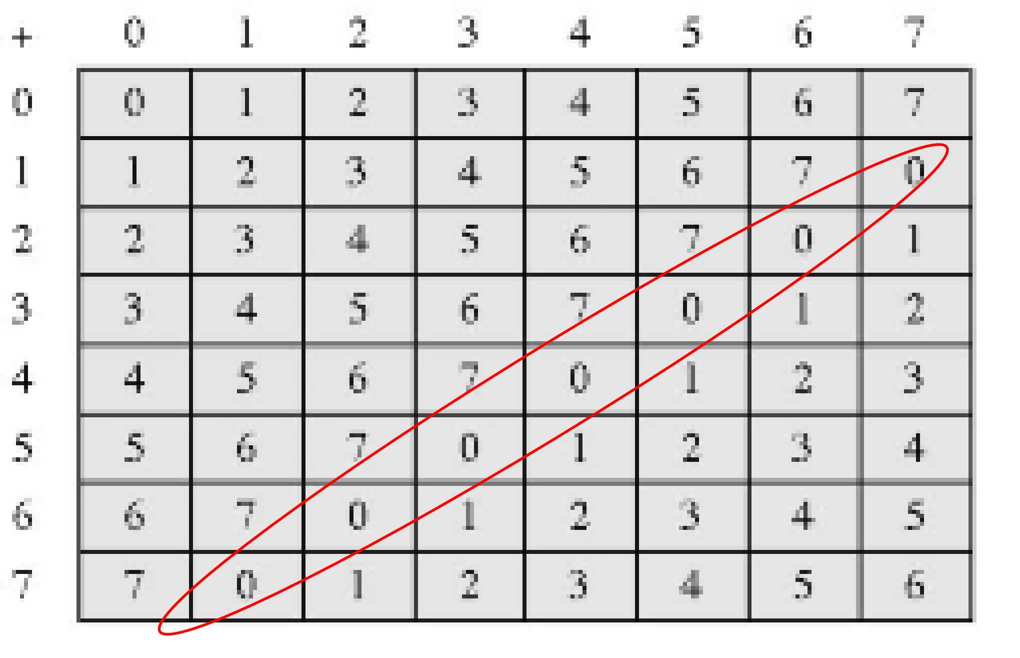
Definition 7 (Field). A field $\mathbb{K}$ is a ring such that for every nonzero element $a \in \mathbb{K}$ there is an element b $\in \mathbb{K}$ such that $ab = 1$. For example, if p is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field .

Definition 8 (Finite Field). Fields with a finite number of elements

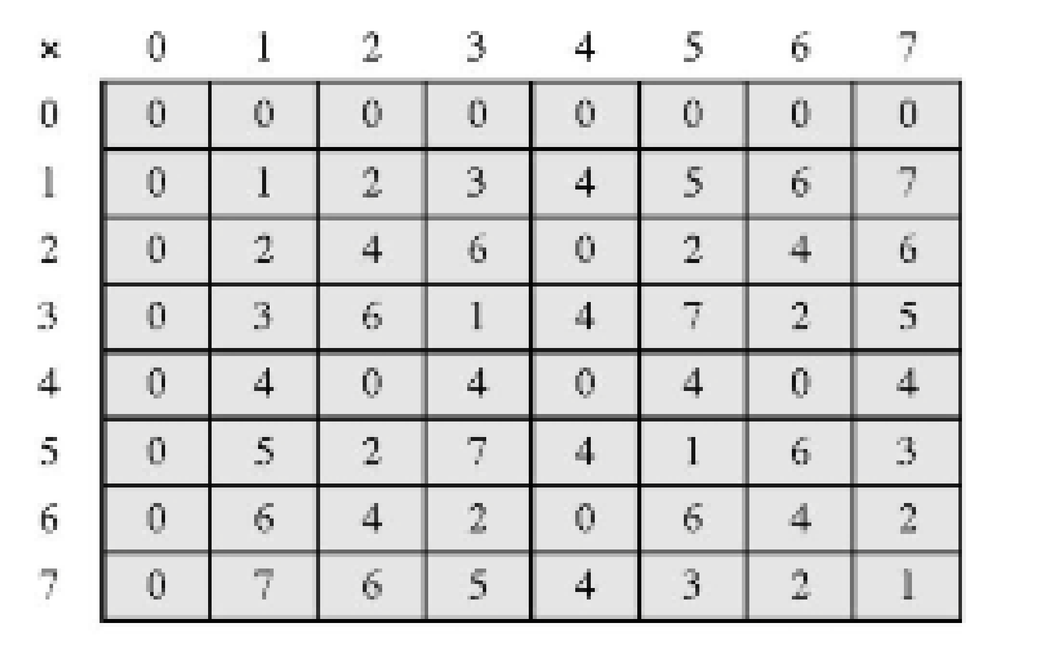
It can be proved that if a field is finite then it has p elements, for some prime number p.

- We also say that it has order p
- We denote $\mathrm{GF}(p^n)$ – GF stands for Galois field
- For $n = 1$ we have $\mathrm{GF}(p)$ which is $\mathbb{Z}_p$
  - If p is prime, then any element in $\mathbb{Z}_p$ has a multiplicative inverse
- For $n > 1$ the field has a different structure

Basic Notions of Finite Fields: Modulo 8 Example/ Arithmetic modulo 8



+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6



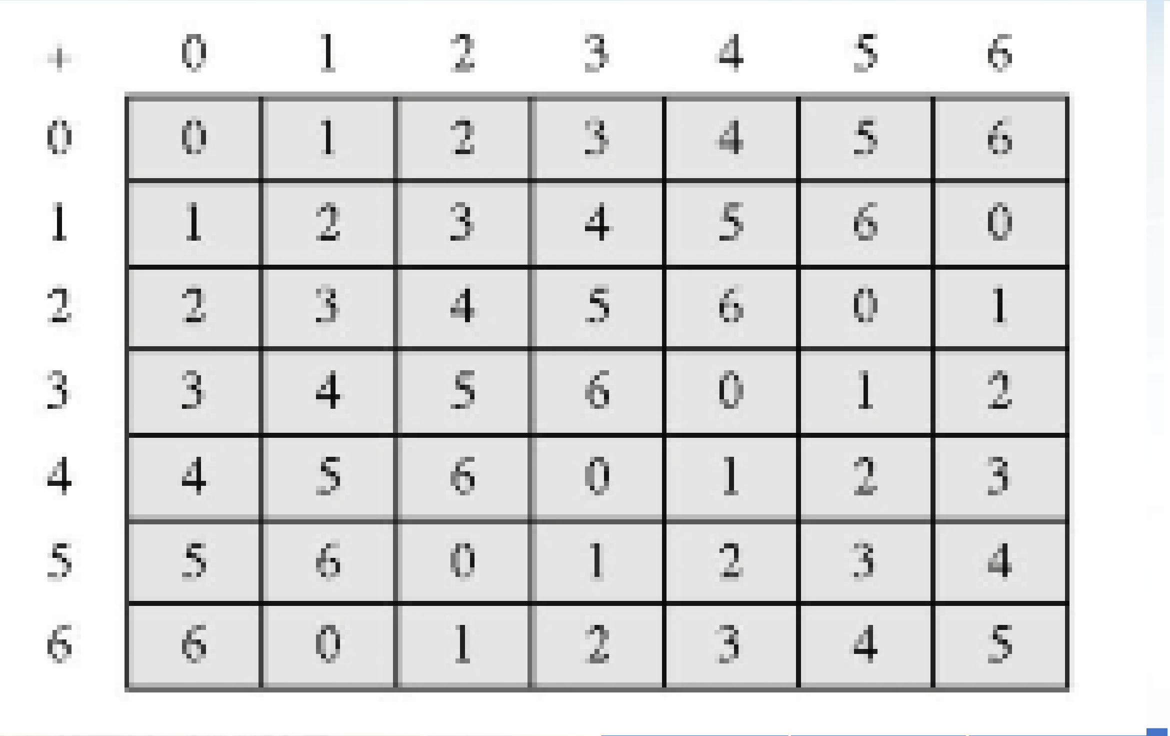
×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Field ?

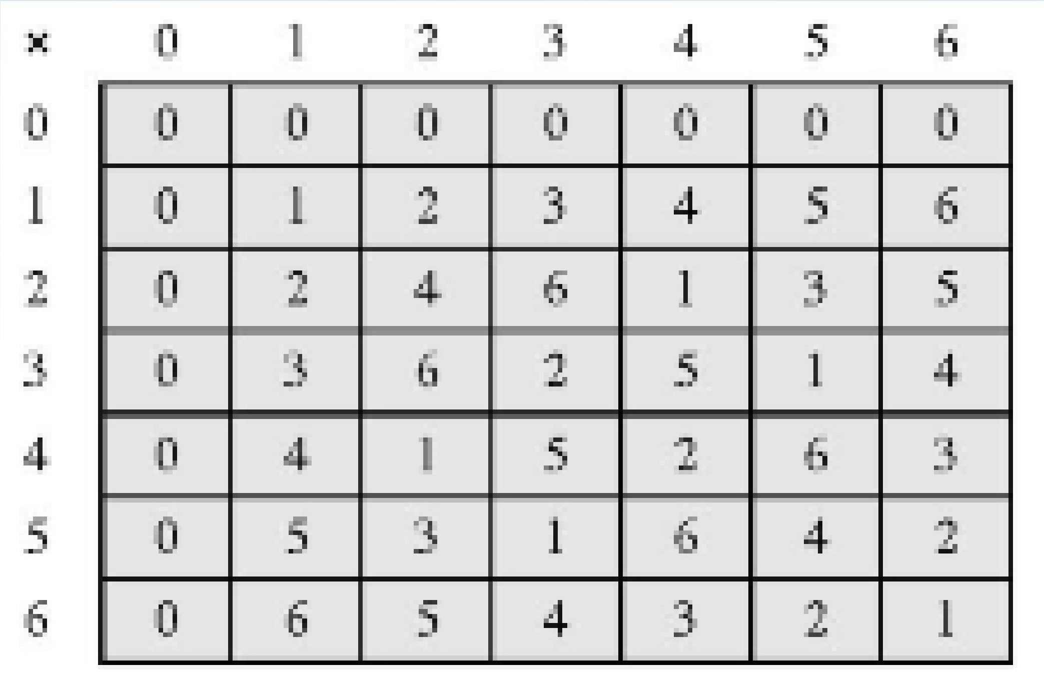
w	0	1	2	3	4	5	6	7
$-w$	0	7	6	5	4	3	2	1
w^{-1}	–	1	–	3	–	5	–	7

This is not a field!

Basic Notions of Finite Fields: Modulo 7 Example/ Arithmetic modulo 7

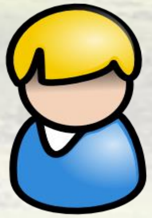


+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5



×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Field



?

w	0	1	2	3	4	5	6
$-w$	0	6	5	4	3	2	1
w^{-1}	–	1	4	5	2	3	6

This is a field!

GCD and Linear Combinations

- The greatest common divisor of two integers a and b can be expressed in the form $sa + tb$, where s and t are integers.
- In other words, $\gcd(a, b)$ can be expressed as a linear combination with integer coefficients of a and b. For example, $\gcd(6, 14) = 2$, and $2 = (-2) \cdot 6 + 1 \cdot 14.$

GCD and Linear Combinations

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

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

GCD and Linear Combinations

- The method proceeds by working backward through the divisions of the Euclidean algorithm, so this method requires a forward pass and a backward pass through the steps of the Euclidean algorithm.
- The algorithm used is called the **extended Euclidean algorithm:** used to express gcd(a, b) as a linear combination of a and b using a single pass through the steps of the Euclidean algorithm;

GCD and Linear Combinations

Finding the multiplicative inverse in $\mathbb{Z}_p$

- Given an element q, how do we calculate q^{-1}?
- **Euclid's Algorithm to compute** $\gcd(a, b)$: $\text{Euclid}(a, b)$
  - If $b = 0$ then return a
  - Else return $Euclid(b, a \, mod \; b)$
- Result: if $d = gcd(a, b):$, then there are integers x, y such that

$$d = ax + by$$

- Consequence: if $\gcd(a, b) = 1$, then there are integers x, y such that

$$ax + by = 1$$

GCD and Linear Combinations

So, $ax \equiv 1(\, mod\ b)$, i.e., $x = a^{-1}\ mod\ b$

Question: How do we calculate x for given a, b?

Idea: run Euclid’s algorithm in such a way as to compute not only d, but also x and y

GCD and Linear Combinations

Definition (Euler's Totient Function: $\varphi(n)$):

For $n \in \mathbb{N}$, let $\varphi\,(n) = \#\{a \in \mathbb{N}: a \leq n\; and\; \gcd(a, n) = 1\}$

How many numbers there are between 1 and $n - 1$ that are relatively prime to n.

- Example

$$\begin{aligned}\varphi(1) &= \#\{1\} = 1\\ \varphi(2) &= \#\{1\} = 1\\ \varphi(5) &= \#\{1, 2, 3, 4\} = 4\\ \varphi(12) &= \#\{1,5,7,11\} = 4\end{aligned}$$

- Also, if p is any prime number then $\varphi\,(p) = \#\{1,2, \dots, p - 1\} = p - 1$

GCD and Linear Combinations

Definition (Fermat’s Little Theorem)

- If p is prime and a is an integer not divisible by p , then

$$a^{p-1} \equiv 1(mod\ p): x^{\varphi(n)} \equiv 1(mod\ n)$$

- Furthermore, for every integer a we have

$$a^{p} \equiv 1(mod\ p)$$

- Fermats little theorem tells us that if $\mathrm{a} \in \mathbb{Z}_{\mathrm{p}}$, then $\mathrm{a}^{\mathrm{p}-1} = 1$ in $\mathbb{Z}_{\mathrm{p}}$
- Its extremely useful in computing remainders modulo p of large powers of integers.

GCD and Linear Combinations

Example: Find $7^{222} mod\ 11$

Solution: We can use Fermat's little theorem to evaluate 7^{222}mod 11

- Rather than using fast modular exponentiation algorithm.
- By Fermat's little theorem, we know that $7^{10} \equiv 1(\mathrm{mod}\ 11)$, so is $7^{10k} \equiv 1(\mathrm{mod}\ 1)\forall \mathrm{k} \in \mathbb{Z}$. To take advantage of the last congruence, we divide the exponent 222 by 10 to get $222 = 22.10 + 2$
- Hence $7^{222} = 7^{22.10+2} = (7^{10})^{22} 7^{2} = (1)^{22}.\,49 \equiv 5(\mathrm{mod}\ 11)$
- It follows that $7^{222}\mathrm{mod}\ 11 = 5$

Solving Inverses

Quickly computing inverses and huge powers

- Aim: Solve the equation $ax \equiv 1 \ (mod\ n)$ when we know it has a solution, and how to efficiently compute $a^m \ (mod\ n)$
- These algorithms are of fundamental importance to the cryptographic algorithms of public key cryptography

Solving Inverses

- How can we Solve $ax \equiv 1\ (mod\ n)$?
- Suppose $a, n\ \in \mathbb{N}$ with $\gcd(a, n)\ =\ 1$. Then from before, the equation $ax\ \equiv\ 1\ (mod\ n)$ has a unique solution. How can we find it?
- Proposition: (Extended Euclidean Representation). Suppose $a, b\ \in \mathbb{Z}$

and let g $= \gcd(a, b)$. Then there exists $\exists x, y\ \in \mathbb{Z}$ such that $ax\ +\ by\ =\ g$.

Solving Inverses

Example

- Suppose $a = 5$ and $b = 7$. Compute $\gcd(5, 7)$ are as follows. Here we underline certain numbers, because it clarifies the subsequent back substitution we will use to find x and y.

$\underline{7}$	$=$	1	$.$	$\underline{5}$	$+$	$\underline{2}$	$\Rightarrow \mathbf{2 = 1.7 - 1.5}$
$\underline{5}$	$=$	2	$.$	$\underline{2}$	$+$	$\underline{1}$	$\Rightarrow \mathbf{1 = 1.5 - 2.2}$ $\mathbf{1 = 1.5 - 2.(1.7 - 1.5\ )}$ $\mathbf{1 = 1.5 - 2.7 + 2.5}$ $\mathbf{1 = 3.5 - 2.7}$

Solving Inverses

- Example 2. Suppose $a = 130$ and $b = 61$. Compute gcd(130,61) are as follows.

130	=	2	.	61	+	8	$\Longrightarrow 8 = 1.130 - 2.61$
61	=	7	.	8	+	5	$\Longrightarrow 5 = -7.130 + 15.61$
8	=	1	.	5	+	3	$\Longrightarrow 3 = 8.130 - 17.61$
5	=	1	.	3	+	2	$\Longrightarrow 2 = -15.130 + 32.61$
3	=	1	.	2	+	1	$\Longrightarrow 1 = 23.130 - 49.61$
2	=	1	.	2	+	0	

Solving Inverses

- Example 2. Suppose $a = 130$ and $b = 61$. Compute gcd(130,61) are as follows.

Thus $x = 23$ and $y = -49$ is a solution to $130x + 61y = 1$

Solving Inverses

$\underline{130}$	=	2	.	$\underline{61}$	+	$\underline{8}$	$\Rightarrow 8 = 1.\,130 - 2.\,61$
$\underline{61}$	=	7	.	$\underline{8}$	+	$\underline{5}$	$\Rightarrow 5 = 1.61 - 7.8$ $= 1.61 - 7.(1.130 - 2.61\,)$ $= 1.61 - 7.130 + 14.61$ $= -7.\,130 + 15.\,61$
$\underline{8}$	=	1	.	$\underline{5}$	+	$\underline{3}$	$\Rightarrow 3 = 1.8 - 1.5$ $= 1.(1.130 - 2.61) - 1.(-7.130 + 15.61\,)$ $= 1.130 - 2.61 + 7.130 - 15.61$ $= 8.\,130 - 17.\,61$
$\underline{5}$	=	1	.	$\underline{3}$	+	$\underline{2}$	$\Rightarrow 2 = 1.5 - 1.3$ $= 1.(-7.130 + 15.61\,) - 1.(8.130 - 17.61\,)$ $= -7.130 + 15.61 \; - 8.130 + 17.61$ $= -15.\,130 + 32.\,61$
$\underline{3}$	=	1	.	$\underline{2}$	+	$\underline{1}$	$\Rightarrow 1 = 1.3 - 1.2$ $= 1.(8.130 - 17.61) - 1.(-15.130 + 32.61)$ $= 8.130 - 17.61 + 15.130 - 32.61$ $= 8.130 - 17.61 + 15.130 - 32.61$ $= 23.\,130 - 49.\,61$

Solving Inverses

Algorithm (Inverse Modulo n). Suppose a and n are integers and $\gcd(a, n) = 1$. This algorithm finds an x such that $ax \equiv 1 \ (mod\ n)$ as follows,

- [Compute Extended GCD] Use this algorithm to compute integers x and y such that $ax + ny = \gcd(a, n) = 1$
- [Finished] Output x.

Proof. Reduce $ax + ny = 1$ modulo n to see that x satisfies $ax \equiv 1 \ (mod\ n)$

Solving Inverses

Algorithm (Inverse Modulo n). Suppose a and n are integers and $\gcd(a, n) = 1$. This algorithm finds an x such that $ax \equiv 1 \ (mod\ n)$ as follows,

- ❖ [Compute Extended GCD] Use this algorithm to compute integers x and y such that $ax + ny = \gcd(a, n) = 1$
- ❖ [Finished] Output x.

Proof. Reduce $ax + ny = 1$ modulo n to see that x satisfies $ax \equiv 1 \ (mod\ n)$

Example . Solve $17x \equiv 1 \ (mod\ 61)$. First, we use Algorithm (Extended Euclid) to find x, y such that $17x + 61y = 1$:

Solving Inverses

$\underline{61}$	$=$	3	.	$\underline{17}$	$+$	$\underline{10}$	$\Rightarrow 10 = 1.61 - 3.17$
$\underline{17}$	$=$	1	.	$\underline{10}$	$+$	$\underline{7}$	$\Rightarrow 7 = 1.17 - 1.10$ $= 1.17 - 1.(1.61 - 3.17)$ $= 1.17 - 1.61 + 3.17$ $= -1.61 + 4.17$
$\underline{10}$	$=$	1	.	$\underline{7}$	$+$	$\underline{3}$	$\Rightarrow 3 = 1.10 - 1.7$ $= 1.(1.61 - 3.17) - 1.(-1.61 + 4.17)$ $= 1.61 - 3.17 + 1.61 - 4.17$ $= 2.61 - 7.17$
$\underline{7}$	$=$	2	.	$\underline{3}$	$+$	$\underline{1}$	$\Rightarrow 1 = 1.7 - 2.3$ $= 1.(-1.61 + 4.17) - 2.(2.61 - 7.17)$ $= -1.61 + 4.17 - 4.61 + 14.17$ $= -5.61 + 18.17$
$\underline{3}$	$=$	3	.	$\underline{1}$	$+$	$\underline{0}$	

Solving Inverses

Thus $17 \cdot 18 + 61.(-5) = 1$ so $x = 18$ is a solution to $17x \equiv 1(mod\ 61)$.

Try $91x \equiv 1\ (mod\ 101)$

Appendix: Modular Arithmetic (Revisited)

Consider the set of integers: fix a positive integer n

- For any integer a, there exists integers q and r such that $\mathrm{a} = \mathrm{q}n + r$ and r is from 0 to $n - 1$

○ q is the largest integers less than or equal to a/n. also called quotient

○ r is called the residue of a modulo n

○ Define the operator mod: $\mathrm{a\ mod\ n} = r$

○ Define the operator div: $\mathrm{a\ div\ n} = \mathrm{q}$

○ Example:

a) 7 mod 5 = 2, 11 mod 7 =4,

b) -11 mod 7 =3: -11=(-2).7+3

- Congruence modulo n: $\mathrm{a} \equiv \mathrm{b\ mod\ n}$ if $\mathrm{a\ mod\ n} = \mathrm{b\ mod\ n}$

Example:

$a)\ 73 \equiv\ 4\, mod\ 23, 21\ \equiv\ -9\ \equiv\ 1\, mod\ 10$

Appendix: Modular Arithmetic (Revisited)

We can perform ordinary arithmetic (addition, subtraction, multiplication) modulo n

- Useful properties (reduce the computation mod n at any step)

i. (a + b) mod n = ((a mod n) + (b mod n)) mod n

ii. (a – b) mod n = ((a mod n) − (b mod n)) mod n

iii. (a • b) mod n = ((a mod n) • (b mod n)) mod n

- Example: to compute $11^7 mod\ 13$

$$11^2 = 121 = 4\ mod\ 13$$
$$11^4 = 4^2 = 3\ mod\ 13$$
$$11^7 = 4.3.11\ mod\ 13 = 2\ mod\ 13$$

- $(\mathbb{Z}_n, +, \bullet, 0{,}1)$ is a commutative ring, where $\mathbb{Z}_n = \{0{,}1{,}2, \ldots, n-1\}$ and the operations are performed $modulo\ n$

Modular Arithmetic (Revisited)

Careful when performing operations modulo n

If $(\mathrm{a}+\mathrm{b}) \equiv (\mathrm{a}+\mathrm{c}) \bmod n$, then $\mathrm{b} \equiv \mathrm{c} \bmod n$

Not true that if $(\mathrm{a}.\,b) \equiv (\mathrm{a}.\,\mathrm{c}) \bmod n$, then $\mathrm{b} \equiv \mathrm{c} \bmod n$

Example: $(2.1) \equiv (2.5) mod\ 8$ but 1 and 5 are **not congruent modulo 8**

- The implication is true if and only if a is relatively prime to n, i.e., $gcd(a, n) = 1$
- Any such a **has a multiplicative inverse** $a^{-1} modulo\ n$

Proposition (Units). $gcd(a, n) = 1$, then the equation $a\,x \equiv b(mod\ n)$ has a solution, and that solution is unique $modulo\ \ n$.

Modular Arithmetic (Revisited)

A nonzero integer b $divides\ a\ if\ a = mb\ ,\ for\ some\ integer\ m.\ We$ denote it as $b|a$ and we say that b is a $divisor\ of\ a$

Example: Positive divisors of 24 are 1,2,3,4,6,8,12,24

Facts:

i. If $a\,|1$, then $a = 1$ or $a = -1$

ii. If $a\,|b$ and $b\,|a$, then $a = b$ or $a = -b$

iii. If $d|g$ and $d|h$, then $d|(mg + nh)$, for any integers m and n

iv. If $a \equiv b(mod\ n), then\ n|(a - b)$

v. If $a \equiv b(mod\ n)$, then $b \equiv a(mod\ n)$,

vi. If $a \equiv b(mod\ n)$, and $b \equiv c(mod\ n)$, then $a \equiv c(mod\ n)$,

Modular Arithmetic (Revisited)

The positive integer d is the greatest common divisor of integers a and b, denoted $d = \gcd(a, b)$ if

- It is a divisor of both a and b
- Any other divisor of a and b is a divisor of d

Example: $\gcd(8,12) = 4, \gcd(24,60) = 12$

❖ Integers a and b are called *relatively prime if* $\gcd(a, b) = 1$

❖ Computing $\gcd(a, b)$: Euclid’s algorithm

❖ Based on the following fact: $\gcd(a, b)= \gcd(b, a\ mod\ b)$

Euclid's Algorithm to compute $\gcd(a, b)$:$\text{Euclid}(a, b)$

```
• If $b = 0$ then return $a$
• Else return $\text{Euclid}(b, a\ mod\ b)$
```

Note: The algorithm always terminates

Primality Test

Proof

- If n is composite, by the definition of a composite integer, we know that it has a factor a with $1 < \mathrm{a} < n$. Hence, by the definition of a factor of a positive integer, we have $n = ab$, where b is a positive integer greater than 1.
- We will show that $\mathrm{a} \leq \sqrt{n}$ or $\mathrm{b} \leq \sqrt{n}$
- If $\mathrm{a} > \sqrt{n}$ and $\mathrm{b} > \sqrt{n}$, then $\mathrm{ab} > \sqrt{n}. \sqrt{n} = n$ which is a contradiction!
- Consequently, $\mathrm{a} \leq \sqrt{n}$ or $\mathrm{b} \leq \sqrt{n}$.
- Because both a and b are divisors of n, we see that n has a positive divisor not exceeding $\sqrt{n}$
- This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself.
- In either case, n has a prime divisor less than or equal to $\sqrt{n}$