جـامـعـة بنهـــا

كلية الحاسبات والذكاء الإصطناعي

Discrete Mathematics

Lecture 05

Dr. Ahmed Hagag

Faculty of Computers and Artificial Intelligence
Benha University

Spring 2023

Chapter 4: Number Theory

- The Integers and Division.
- Integer Representations.
- Primes.
- Greatest Common Divisors.
- Least Common Multiple.

Division (1/15)

DEFINITION

If a and b are integers with $a \neq 0$,

we say that a *divides* b if there is an integer c such that

$b = ac$. (or equivalently, if $\frac{b}{a}$ is an integer)

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

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

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

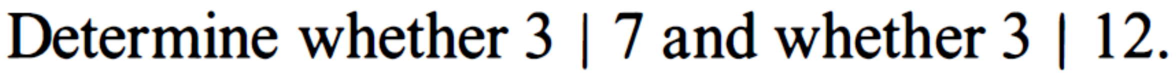
Division (1/15)

DEFINITION

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

Division (2/15)

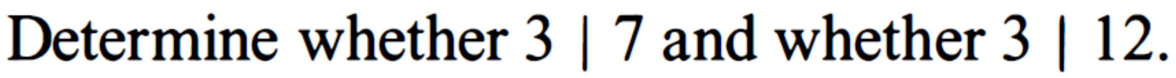
Example 1



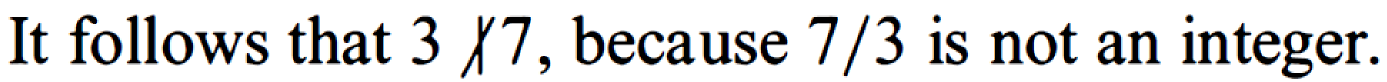
Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Division (2/15)

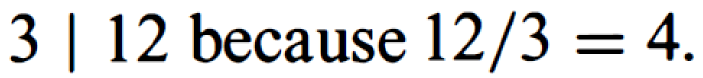
Example 1 – Solution



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



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



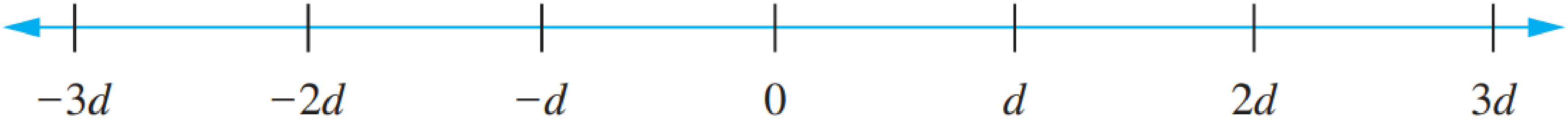
$3 \mid 12$ because $12/3 = 4$.

Division (3/15)

Example 2

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

which integers are divisible by the positive integer d.

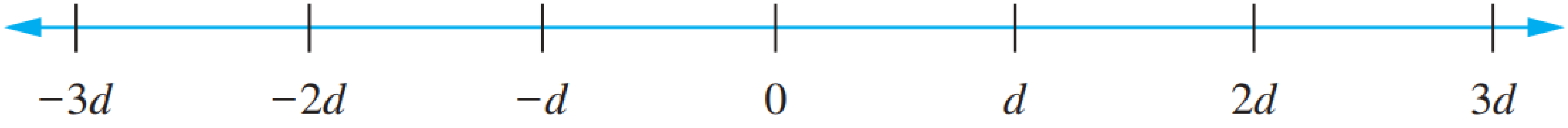


Division (4/15)

Example 3

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

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



Division (5/15)

THEOREM

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

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$

(ii) if $a \mid b$, then $a \mid bc$ for all integers c

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$

As a result:

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

Division (6/15)

Examples

1) Does 2 divdes 4?
2) Does 2 divdes 8?
3) 2 divdes $(4 + 8)$?

4) Does 2 divdes 4?
5) Does 2 divdes $4 \ast 5$?
6) Does 2 divdes $4 \ast 4$?

7) Does 2 divdes 4?
8) Does 4 divdes 16?
9) Does 2 divdes 16?

Division (7/15)

The Division Algorithm

Let $\boldsymbol{a}$ be an integer and $\boldsymbol{d}$ a positive integer. Then

dividend → a

divisor → d

$$\frac{a}{d} = \boxed{quotient\ (q)}\ ,\qquad \boxed{remainder\ (r)}$$

$$with\ ,\ \boxed{0 \le r < d}$$

$$a = dq + r$$

The remainder r cannot be negative!

$$q = a \ \mathbf{div}\ d$$

$$r = a \ \mathbf{mod}\ d$$

$$\boldsymbol{q} = \left\lfloor \frac{\boldsymbol{a}}{\boldsymbol{d}} \right\rfloor$$

$$\boldsymbol{r} = \boldsymbol{a} - \boldsymbol{qd}$$

Division (8/15)

Example 1

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

Division (8/15)

Example 1 – Solution

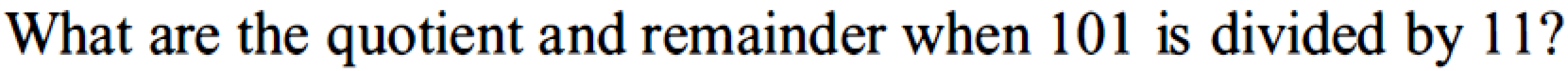
What are the quotient and remainder when 101 is divided by 11?

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

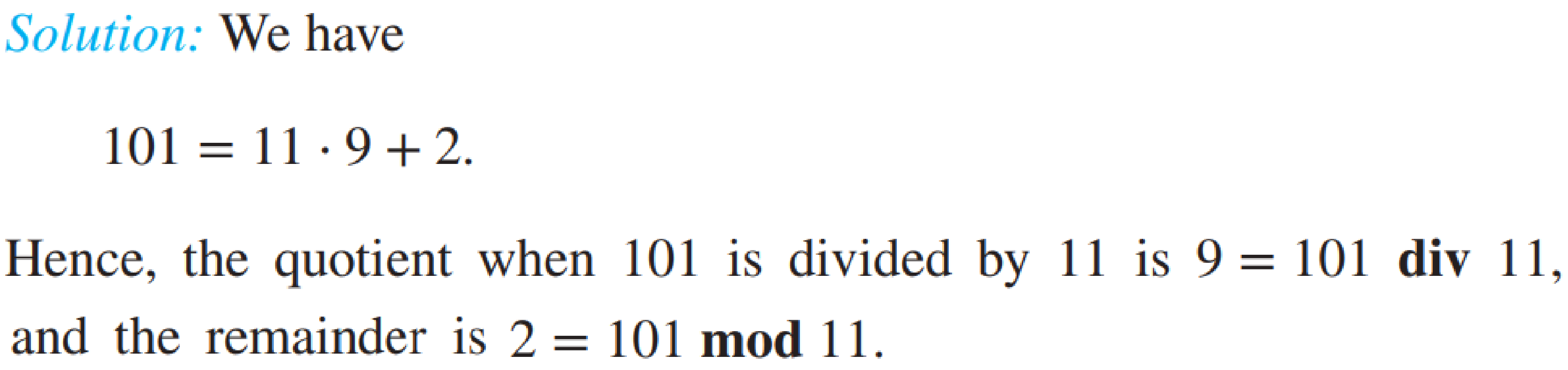
$$r = 101 - (9)(11) = 2$$

Division (8/15)

Example 1 – Solution



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



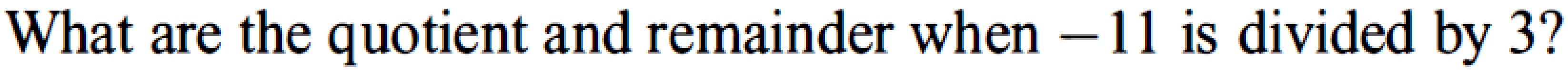
Solution: We have

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

Hence, the quotient when 101 is divided by 11 is $9 = 101$ **div** 11, and the remainder is $2 = 101$ **mod** 11.

Division (9/15)

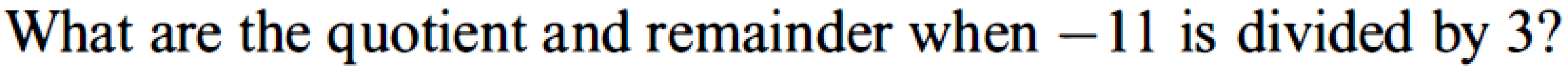
Example 2



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

Division (9/15)

Example 2 – Solution


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

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

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

Division (9/15)

Example 2 – Solution

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

Solution: We have

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

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

Division (10/15)

Example 3

Evaluate:

- $11 \textbf{ mod } 2$

- $-11 \textbf{ mod } 2$

Division (10/15)

Example 3 – Solution

Evaluate:

- $11 \textbf{ mod } 2 = 1$

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

- $-11 \textbf{ mod } 2 = 1$

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

Division (11/15)

Note:

If $\boldsymbol{a \mid b}$, then $\boldsymbol{-a \mid b}$

Example:

$2 \mid 8$

Then

$-2 \mid 8$

Division (12/15)

Example 4

Show that if a is an integer, then 1 | a

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

Division (13/15)

Example 5

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

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

Division (14/15)

Example 6

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

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

Division (15/15)

Example 7

If $\boldsymbol{a} \mid 1$, then $\boldsymbol{a} = \cdots$

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

Modular Arithmetic (1/12)

Introduction (1/3)

In some situations, we care only about the remainder of an integer when it is divided by some specified positive integer. For instance, when we ask what time it will be (on a 24-hour clock) 50 hours from now, we care only about the remainder when 50 plus the current hour is divided by 24. Because we are often interested only in remainders, we have special notations for them.

Example:

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

Answer: $(100 + 2)\ \mathbf{mod}\ 24 = 6$,

Time is $6{:}\,00$

Modular Arithmetic (1/12)

Introduction (2/3)

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

Modular Arithmetic (1/12)

Introduction (3/3)

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

Karl Friedrich Gauss

Modular Arithmetic (2/12)

DEFINITION

a, b are integers and m is a positive integer

a is *congruent* to b *modulo* m

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

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

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

Modular Arithmetic (3/12)

Example 1

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

- 17

- 24

Modular Arithmetic (3/12)

Example 1 – Solution

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

- 17

$17 - 5 = 12, \qquad \frac{12}{6} = 2, \qquad then \quad 17 \equiv 5 \pmod{6}$

- 24

$24 - 5 = 19, \qquad \frac{19}{6} = 3.2, \qquad then \quad 24 \not\equiv 5 \pmod{6}$

Modular Arithmetic (4/12)

Example 2

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

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

Modular Arithmetic (4/12)

Example 2 – Solution

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

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

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

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

Modular Arithmetic (4/12)

Example 2 – Solution

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

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

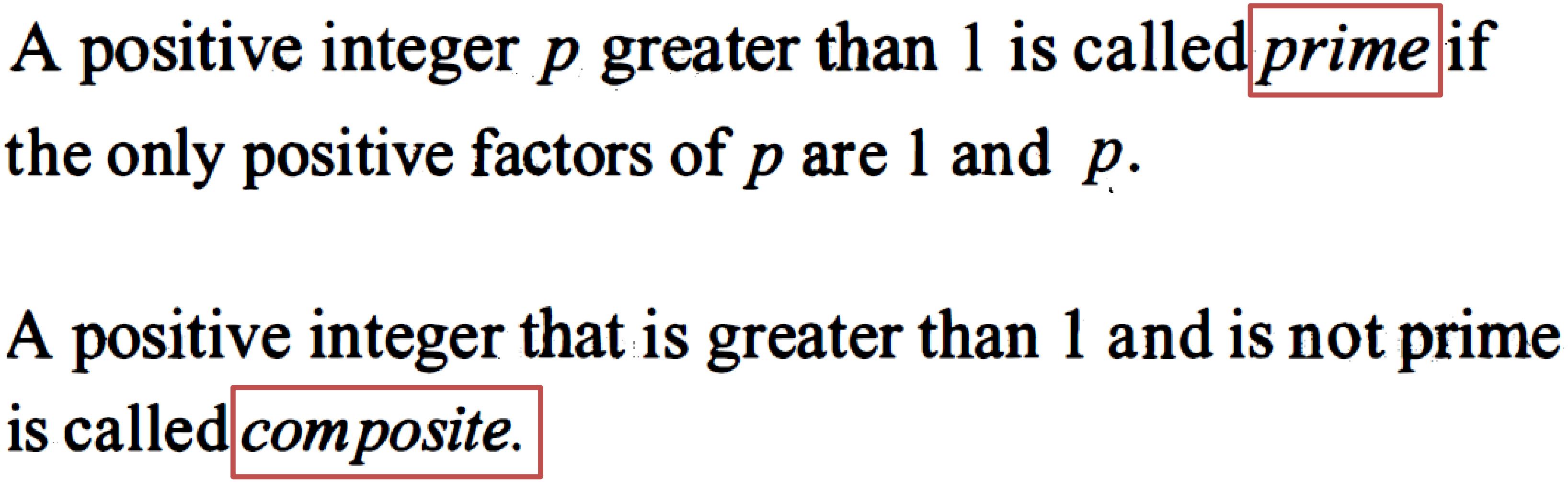
$a = 2 + k * 4,$ k is integer

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

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

Primes (1/9)

Definition



A positive integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p.

A positive integer that is greater than 1 and is not prime is called *composite.*

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

Primes (2/9)

Remark

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

Primes (3/9)

THEOREM 1

THE FUNDAMENTAL THEOREM OF ARITHMETIC

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

Primes (4/9)

THEOREM 2

If n is a composite integer,

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

Example 1: The integer 100 is prime or not ?

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

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

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

Primes (5/9)

Example 2

The integer 101 is prime or not ?

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

$$2 \nmid 101, \qquad 3 \nmid 101\,, \qquad 5 \nmid 101, \qquad \text{and} \quad 7 \nmid 101$$

So, 101 is a prime integer.

Primes (6/9)

Example 3

Find the prime factorization of 100?

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

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

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

Primes (7/9)

Example 4

Find the prime factorization of 1001?

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

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

$\sqrt{13}$ are $2, 3$

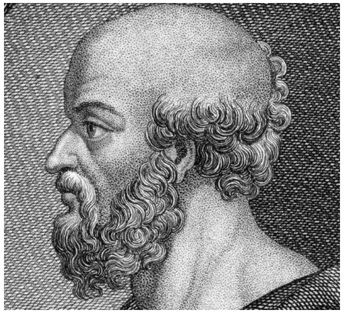
$$\left(\begin{array}{c|c} 1001 & 7 \\ 143 & 11 \\ 13 & 13 \\ 1 & \end{array}\right)$$

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

Primes (8/9)

The Sieve of Eratosthenes (1/6)

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



Eratosthenes
Greek

Primes (8/9)

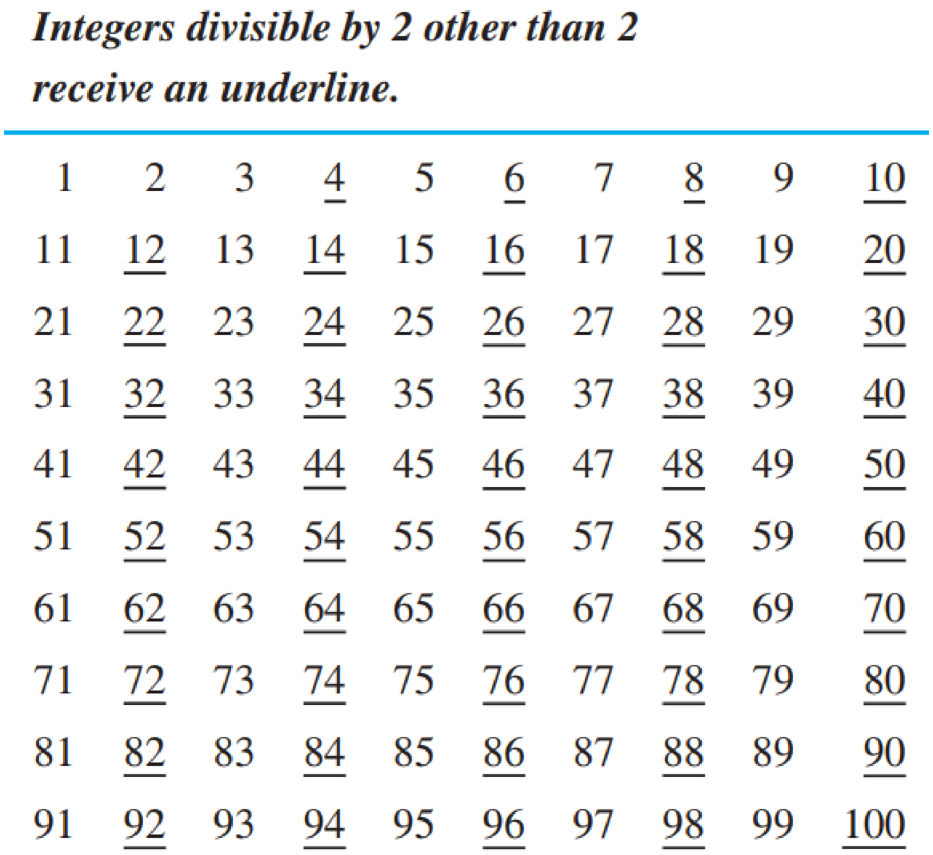
The Sieve of Eratosthenes (2/6)

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

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

Primes (8/9)

The Sieve of Eratosthenes (3/6)

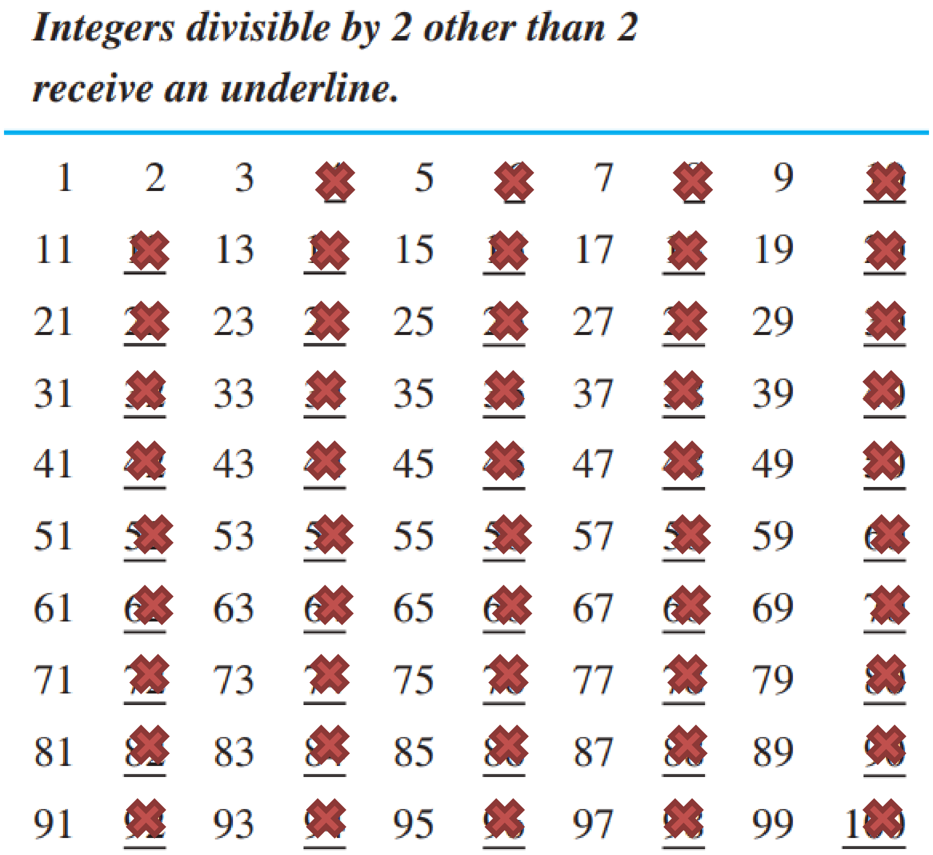


Integers divisible by 2 other than 2 receive an underline.

1	2	3	$\underline{4}$	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	$\underline{100}$

Primes (8/9)

The Sieve of Eratosthenes (3/6)



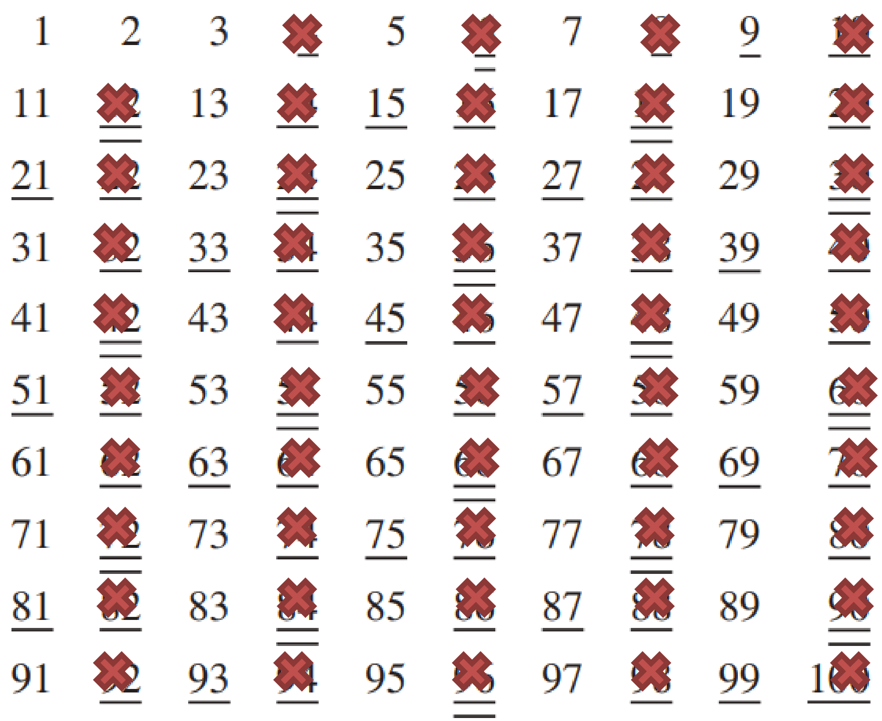
Integers divisible by 2 other than 2 receive an underline.

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

Primes (8/9)

The Sieve of Eratosthenes (4/6)

Integers divisible by 3 other than 3 receive an underline.

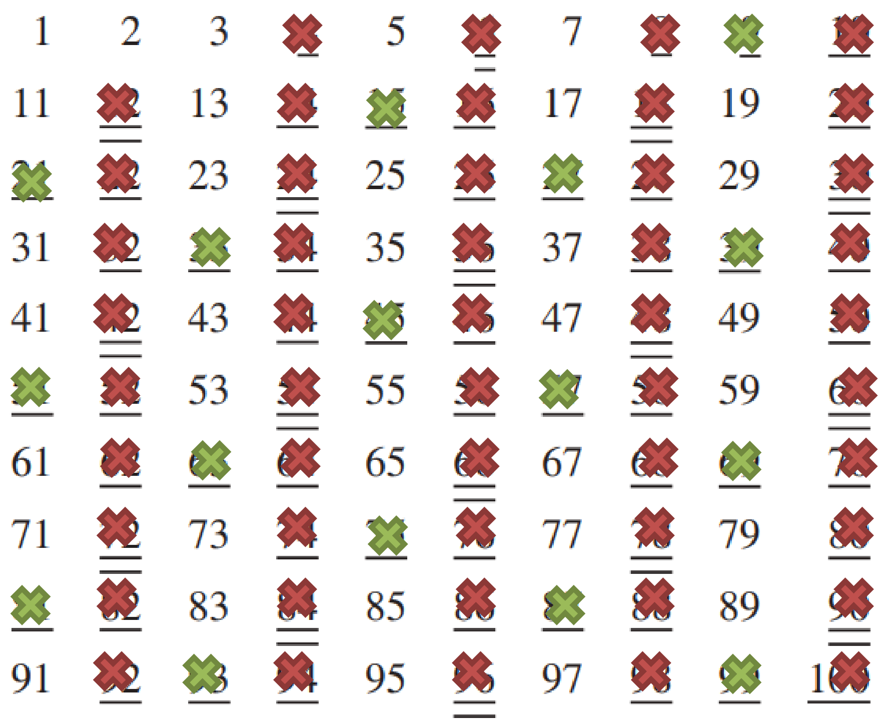


1	2	3	$\xcancel{\underline{4}}$	5	$\xcancel{\underline{\underline{6}}}$	7	$\xcancel{\underline{8}}$	$\underline{9}$	$\xcancel{\underline{10}}$
11	$\xcancel{\underline{\underline{12}}}$	13	$\xcancel{\underline{14}}$	$\underline{15}$	$\xcancel{\underline{16}}$	17	$\xcancel{\underline{\underline{18}}}$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

Primes (8/9)

The Sieve of Eratosthenes (4/6)

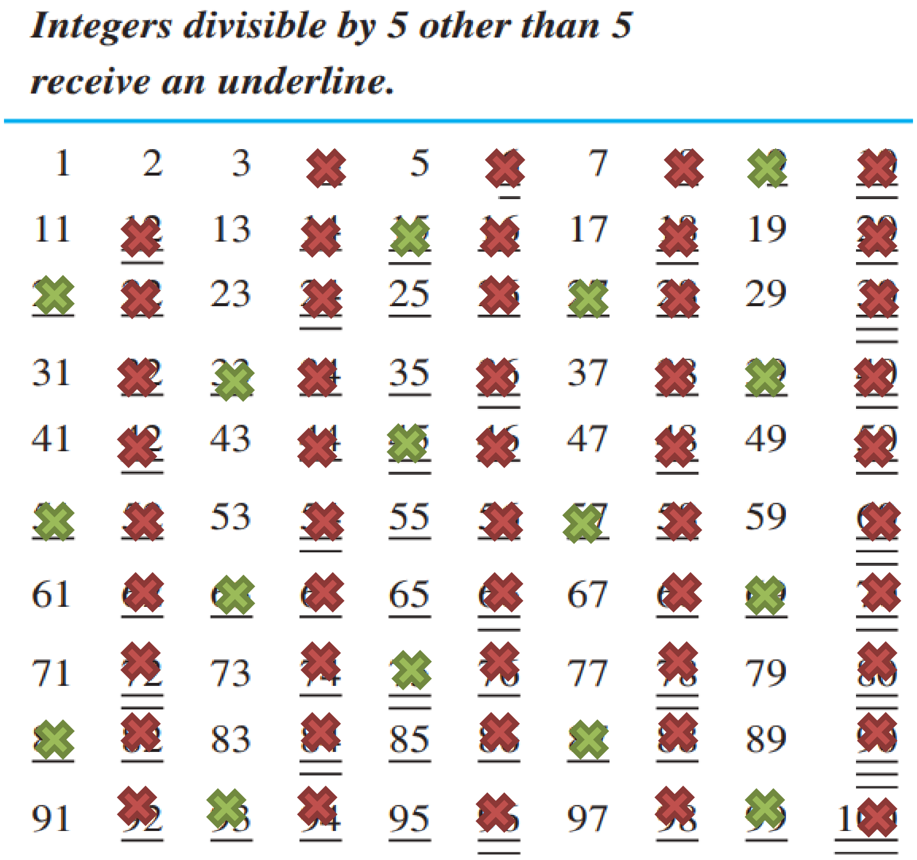
Integers divisible by 3 other than 3 receive an underline.



1	2	3	❌	5	❌	7	❌	❎	❌
11	❌	13	❌	❎	❌	17	❌	19	❌
❎	❌	23	❌	25	❌	❎	❌	29	❌
31	❌	❎	❌	35	❌	37	❌	❎	❌
41	❌	43	❌	❎	❌	47	❌	49	❌
❎	❌	53	❌	55	❌	❎	❌	59	❌
61	❌	❎	❌	65	❌	67	❌	❎	❌
71	❌	73	❌	❎	❌	77	❌	79	❌
❎	❌	83	❌	85	❌	❎	❌	89	❌
91	❌	❎	❌	95	❌	97	❌	❎	❌

Primes (8/9)

The Sieve of Eratosthenes (5/6)

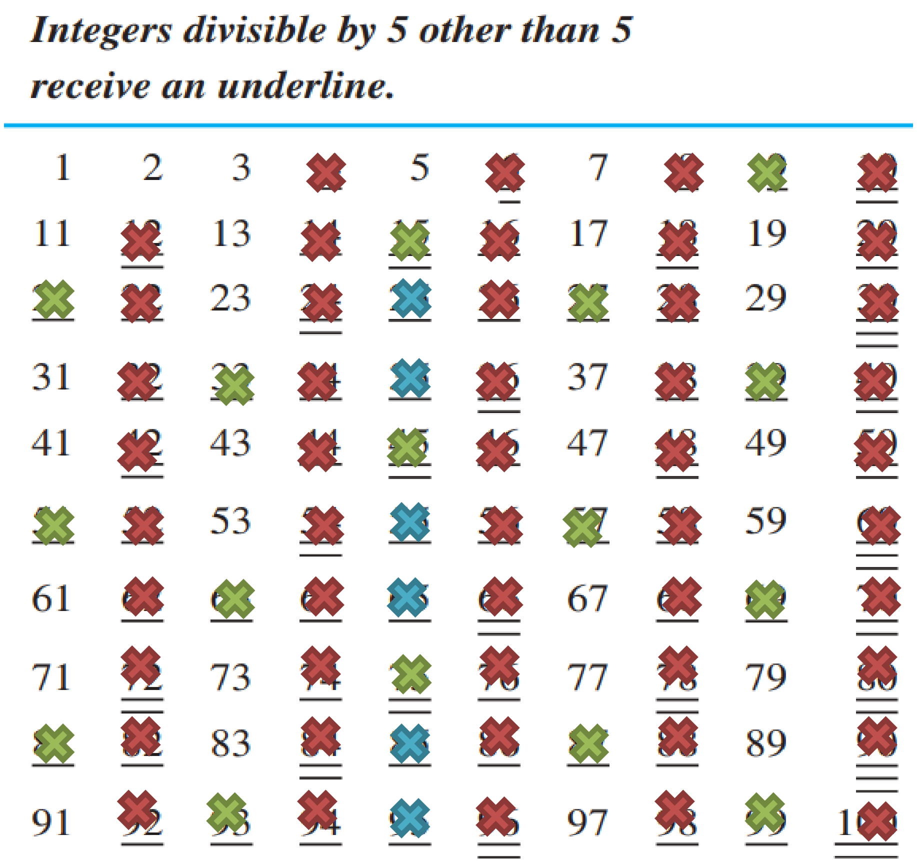


Integers divisible by 5 other than 5 receive an underline.

1	2	3	❌	5	❌	7	❌	❎	❌
11	❌	13	❌	❎	❌	17	❌	19	❌
❎	❌	23	❌	25	❌	❎	❌	29	❌
31	❌	❎	❌	35	❌	37	❌	❎	❌
41	❌	43	❌	❎	❌	47	❌	49	❌
❎	❌	53	❌	55	❌	❎	❌	59	❌
61	❌	❎	❌	65	❌	67	❌	❎	❌
71	❌	73	❌	❎	❌	77	❌	79	❌
❎	❌	83	❌	85	❌	❎	❌	89	❌
91	❌	❎	❌	95	❌	97	❌	❎	❌

Primes (8/9)

The Sieve of Eratosthenes (5/6)

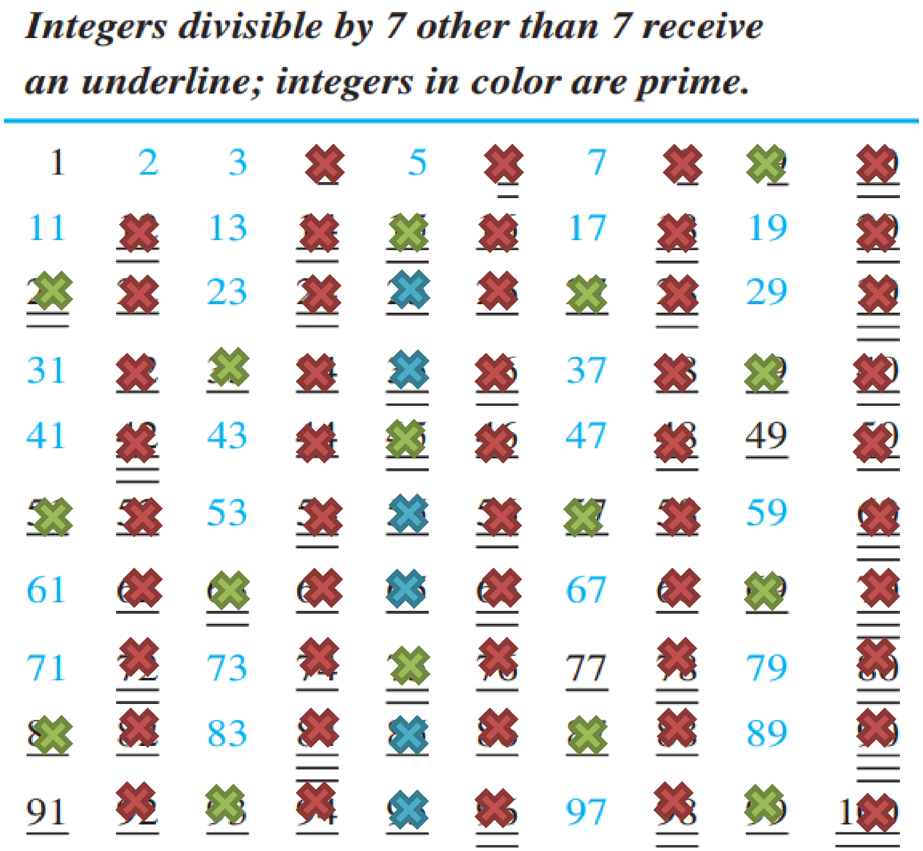


Integers divisible by 5 other than 5 receive an underline.

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

Primes (8/9)

The Sieve of Eratosthenes (6/6)

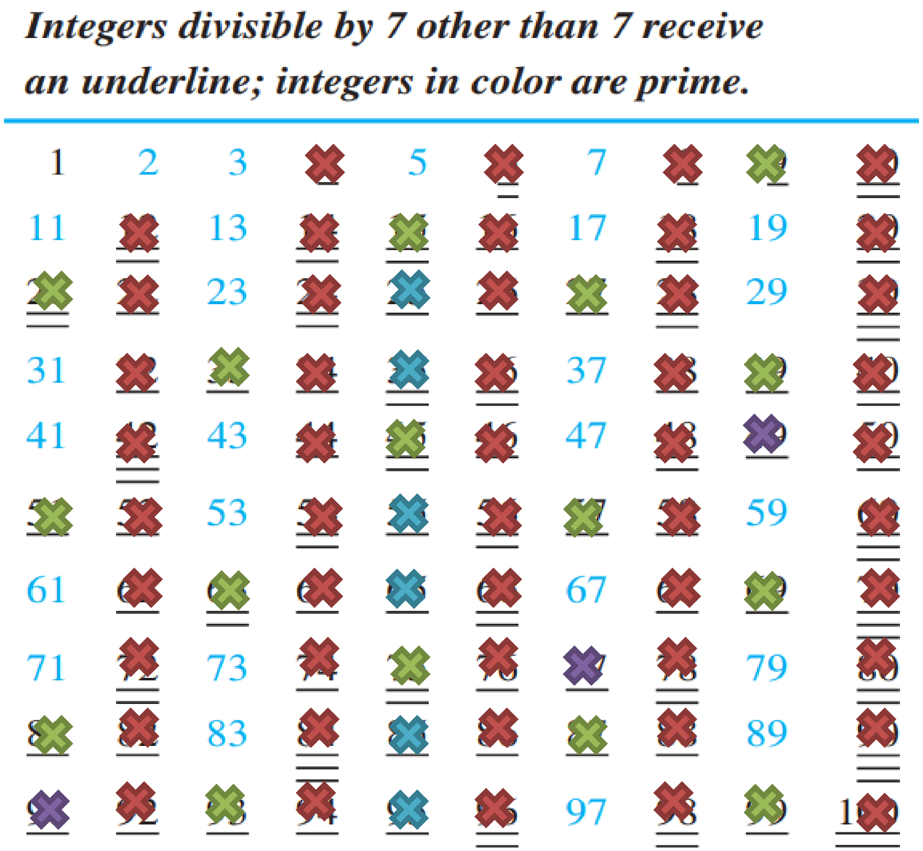


Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	✖	5	✖	7	✖	✖	✖
11	✖	13	✖	✖	✖	17	✖	19	✖
✖	✖	23	✖	✖	✖	✖	✖	29	✖
31	✖	✖	✖	✖	✖	37	✖	✖	✖
41	✖	43	✖	✖	✖	47	✖	49	✖
✖	✖	53	✖	✖	✖	✖	✖	59	✖
61	✖	✖	✖	✖	✖	67	✖	✖	✖
71	✖	73	✖	✖	✖	77	✖	79	✖
✖	✖	83	✖	✖	✖	✖	✖	89	✖
91	✖	✖	✖	✖	✖	97	✖	✖	1✖

Primes (8/9)

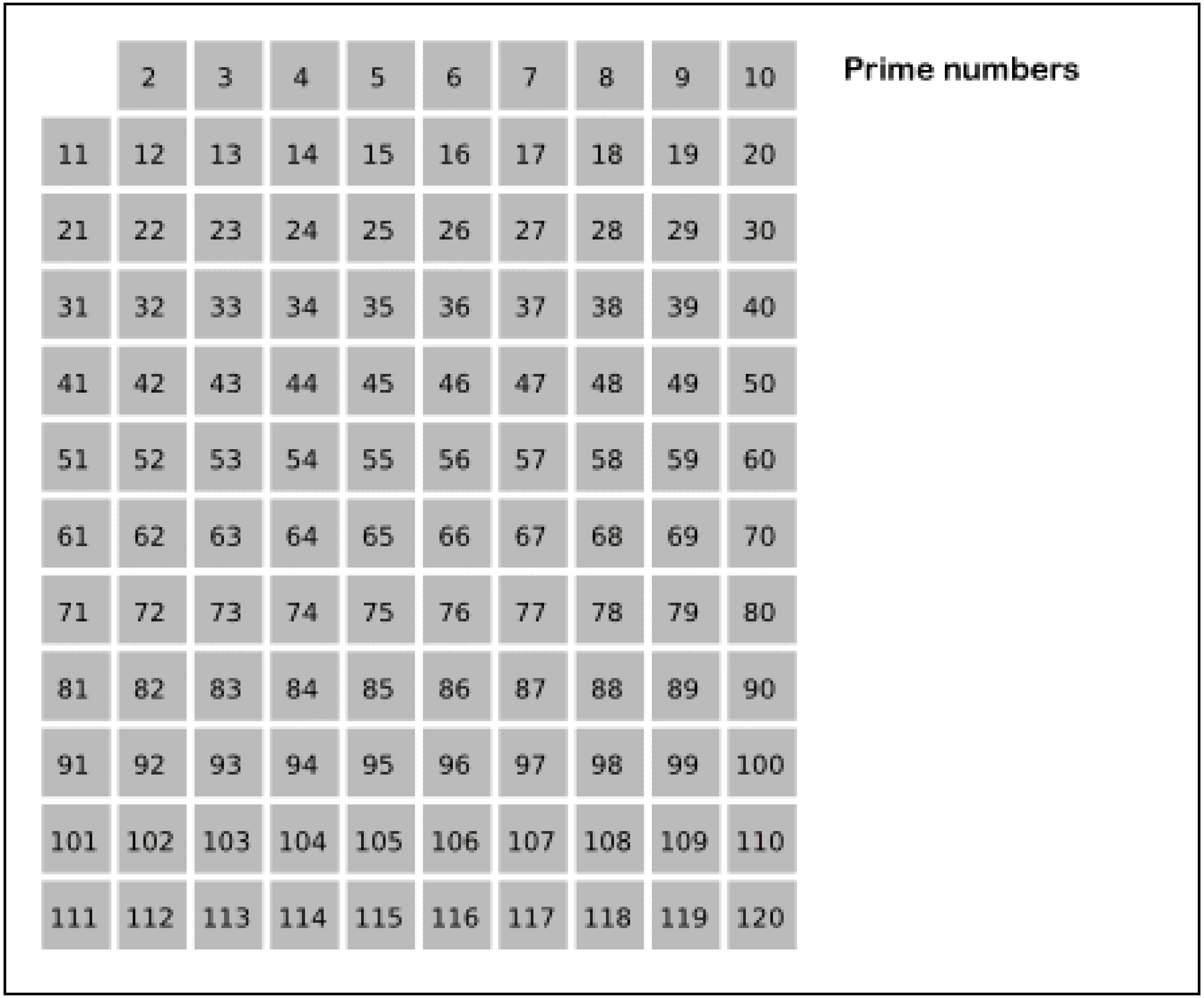
The Sieve of Eratosthenes (6/6)



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

1	2	3	✖	5	✖	7	✖	✖	✖
11	✖	13	✖	✖	✖	17	✖	19	✖
✖	✖	23	✖	✖	✖	✖	✖	29	✖
31	✖	✖	✖	✖	✖	37	✖	✖	✖
41	✖	43	✖	✖	✖	47	✖	✖	✖
✖	✖	53	✖	✖	✖	✖	✖	59	✖
61	✖	✖	✖	✖	✖	67	✖	✖	✖
71	✖	73	✖	✖	✖	✖	✖	79	✖
✖	✖	83	✖	✖	✖	✖	✖	89	✖
✖	✖	✖	✖	✖	✖	97	✖	✖	✖

Primes (9/9)



	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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Prime numbers

Greatest Common Divisors (1/5)

DEFINITION "gcd" (1/2)

Let a and b be integers, not both zero.

The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b.

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

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

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

Greatest Common Divisors (1/5)

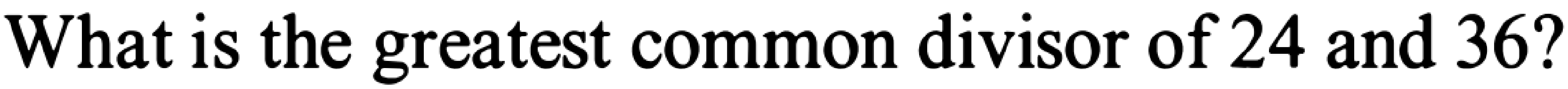
DEFINITION “gcd” (2/2)

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

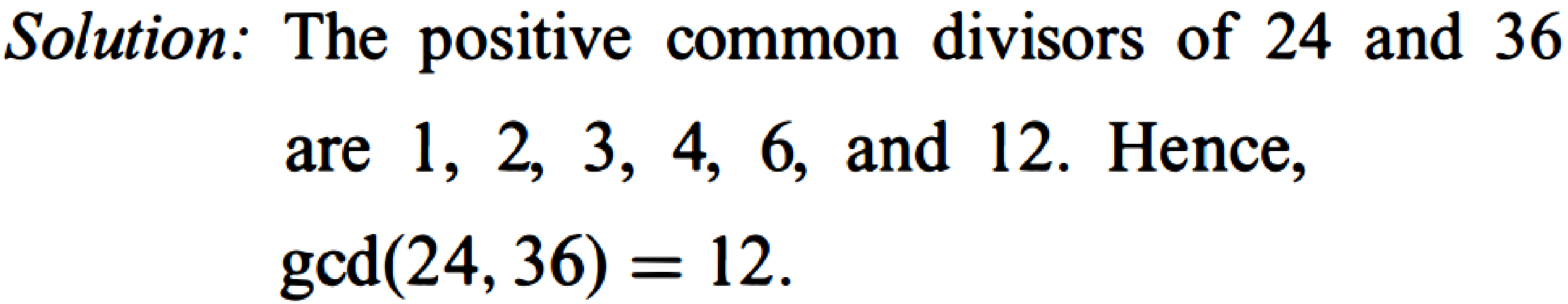
We have four common factors $\{1, 2, 3, 6\}$
The greatest one is $\{6\}$.

Greatest Common Divisors (2/5)

Example 1



What is the greatest common divisor of 24 and 36?



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

Greatest Common Divisors (2/5)

Example 1

What is the greatest common divisor of 24 and 36?

$\sqrt{24}$ are $2, 3$

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

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

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

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

Greatest Common Divisors (3/5)

Example 2

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

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

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

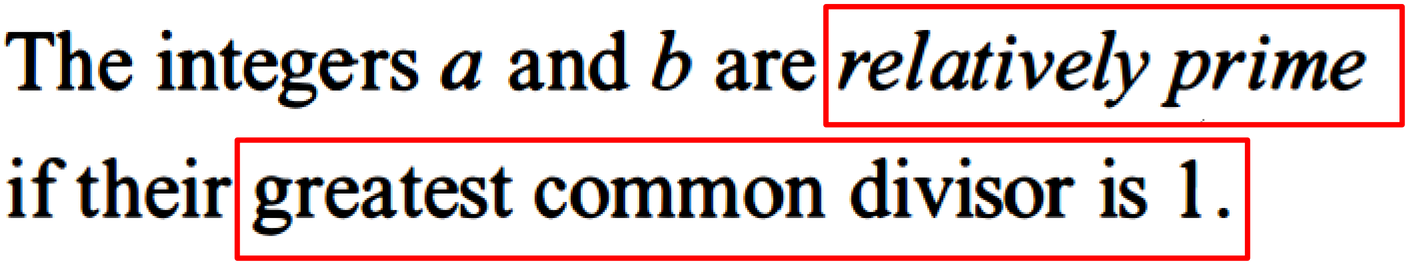
$$\left(\begin{array}{c|c} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}\right) = 2^3 \cdot 3 \cdot 5$$

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

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

Greatest Common Divisors (4/5)

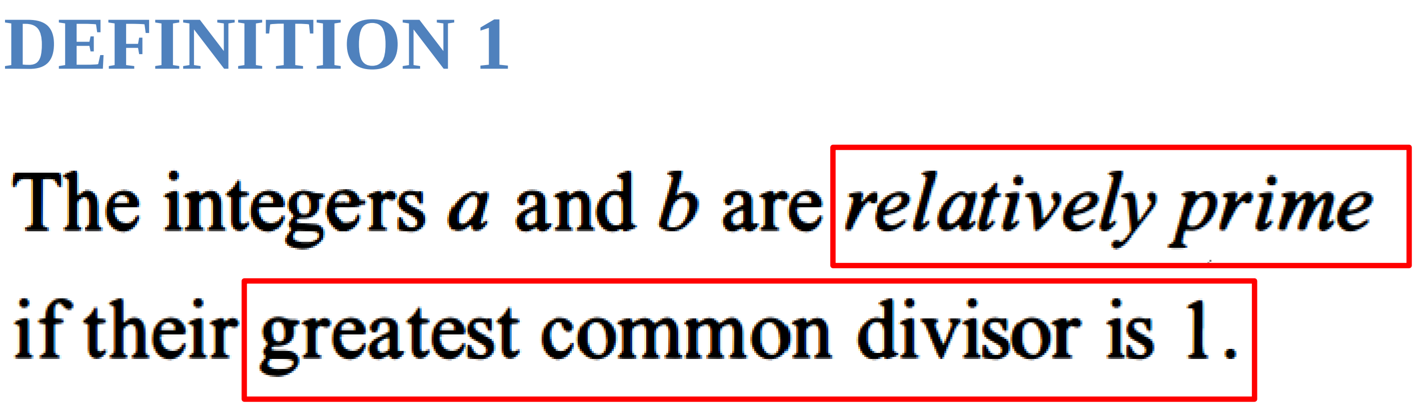
DEFINITION 1



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

Is 17 and 22 are relatively prime?

Greatest Common Divisors (4/5)



DEFINITION 1

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

Is 17 and 22 are relatively prime? (Yes)

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

Greatest Common Divisors (5/5)

DEFINITION 2

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

Greatest Common Divisors (5/5)

DEFINITION 2

The integers $a_1, a_2, \ldots, a_n$ 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.

Least Common Multiple (1/5)

DEFINITION “lcm”

The *least common multiple* of the positive integers a and b

is the smallest positive integer that

is divisible by both a and b.

The least common multiple of a and b is denoted by lcm(a, b).

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

Least Common Multiple (2/5)

Example 1

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

$\sqrt{24}$ are $2, 3$

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

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

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

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

Least Common Multiple (3/5)

Example 2

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

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

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

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

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

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

Least Common Multiple (4/5)

THEOREM

Let a and b be positive integers. Then

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

Least Common Multiple (5/5)

Example 3

What are the $\mathbf{gcd}(\mathbf{120},\mathbf{500})$ and $\mathbf{lcm}(\mathbf{120},\mathbf{500})$?

$\sqrt{120}$ are $2,3,5,7$ $\sqrt{500}$ are $2,3,5,7,11,13,17,19$

$$\left(\begin{array}{c|c} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}\right) = 2^3 \cdot 3 \cdot 5 \qquad \left(\begin{array}{c|c} 500 & 2 \\ 250 & 2 \\ 125 & 5 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}\right) = 2^2 \cdot 5^3$$

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

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

Applications (1/4)

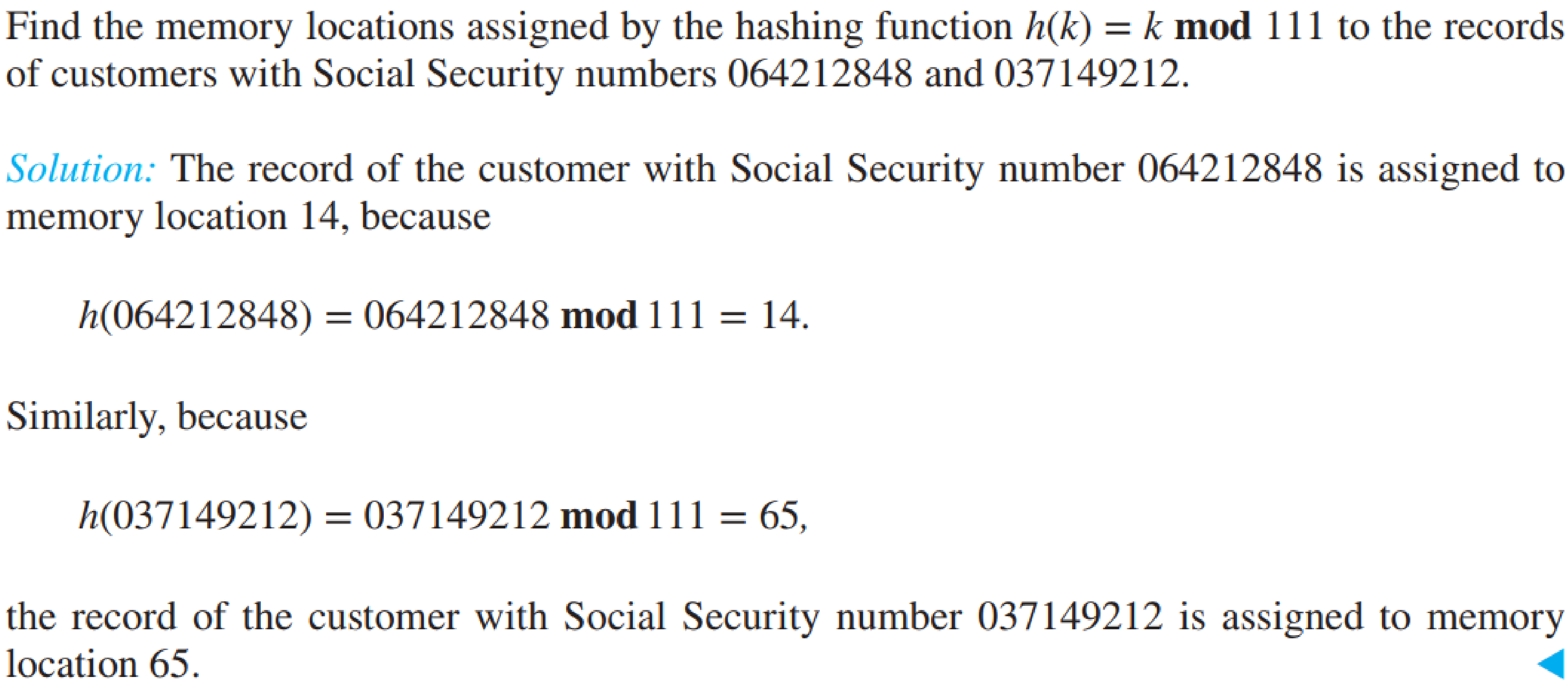
1. Hashing Functions
2. Pseudorandom Numbers
3. Cryptography

…

Applications (2/4)

1. Hashing Functions

$$\boxed{h(k) = k \textbf{ mod } m}$$



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

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

$$h(064212848) = 064212848 \textbf{ mod } 111 = 14.$$

Similarly, because

$$h(037149212) = 037149212 \textbf{ mod } 111 = 65,$$

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

Applications (3/4)

2. Pseudorandom Numbers

linear congruential method

$$\boxed{x_{n+1} = (ax_n + c) \mathbf{~mod~} m.}$$

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

$$\begin{aligned}
x_1 &= 7x_0 + 4 \mathbf{~mod~} 9 = 7 \cdot 3 + 4 \mathbf{~mod~} 9 = 25 \mathbf{~mod~} 9 = 7,\\
x_2 &= 7x_1 + 4 \mathbf{~mod~} 9 = 7 \cdot 7 + 4 \mathbf{~mod~} 9 = 53 \mathbf{~mod~} 9 = 8,\\
x_3 &= 7x_2 + 4 \mathbf{~mod~} 9 = 7 \cdot 8 + 4 \mathbf{~mod~} 9 = 60 \mathbf{~mod~} 9 = 6,\\
x_4 &= 7x_3 + 4 \mathbf{~mod~} 9 = 7 \cdot 6 + 4 \mathbf{~mod~} 9 = 46 \mathbf{~mod~} 9 = 1,\\
x_5 &= 7x_4 + 4 \mathbf{~mod~} 9 = 7 \cdot 1 + 4 \mathbf{~mod~} 9 = 11 \mathbf{~mod~} 9 = 2,\\
x_6 &= 7x_5 + 4 \mathbf{~mod~} 9 = 7 \cdot 2 + 4 \mathbf{~mod~} 9 = 18 \mathbf{~mod~} 9 = 0,\\
x_7 &= 7x_6 + 4 \mathbf{~mod~} 9 = 7 \cdot 0 + 4 \mathbf{~mod~} 9 = 4 \mathbf{~mod~} 9 = 4,\\
x_8 &= 7x_7 + 4 \mathbf{~mod~} 9 = 7 \cdot 4 + 4 \mathbf{~mod~} 9 = 32 \mathbf{~mod~} 9 = 5,\\
x_9 &= 7x_8 + 4 \mathbf{~mod~} 9 = 7 \cdot 5 + 4 \mathbf{~mod~} 9 = 39 \mathbf{~mod~} 9 = 3.
\end{aligned}$$

Applications (4/4)

3. Cryptography

m is the number of elements in the language used.

Classical Cryptography

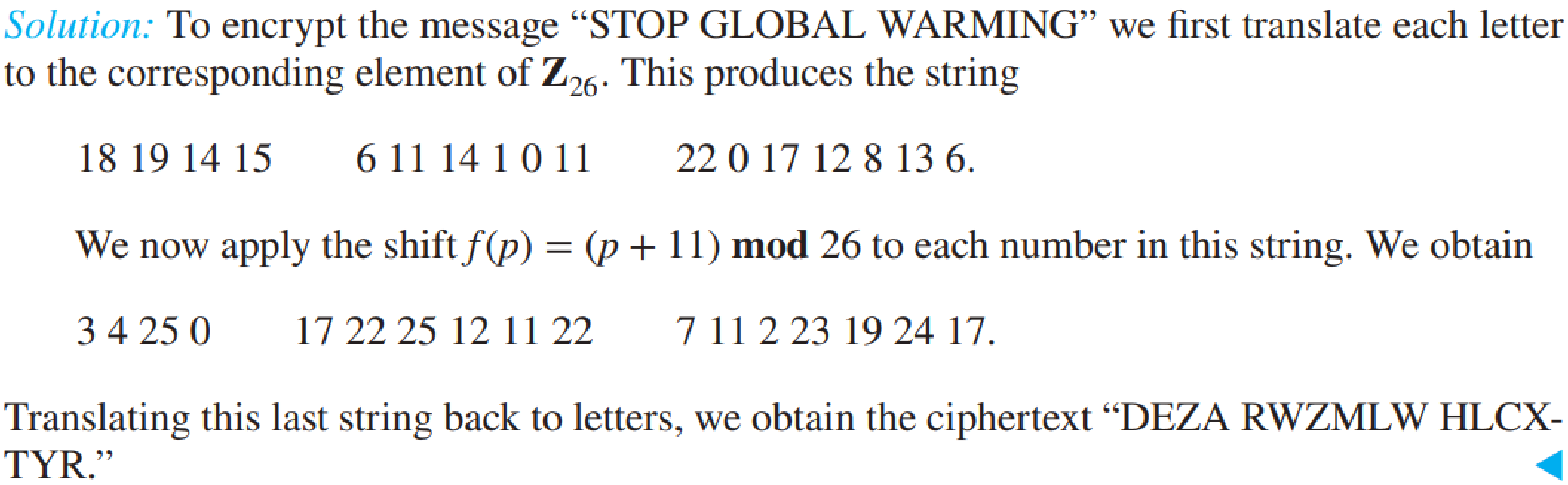
$$f(p) = (p + k) \textbf{ mod } m.$$

Encryption

k is called a **key**

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

Decryption



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

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

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

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

Translating this last string back to letters, we obtain the ciphertext "DEZA RWZMLW HLCXTYR." ◀

Video Lectures

All Lectures: https://www.youtube.com/playlist?list=PLxIvc-MGOs6gZIMVYOOEtUHJmfUquCjwz

Lectures #5: https://www.youtube.com/watch?v=Q-zLpSW3oSU&list=PLxIvc-MGOs6gZIMVYOOEtUHJmfUquCjwz&index=31

https://www.youtube.com/watch?v=3IXnibINWdo&list=PLxIvc-MGOs6gZIMVYOOEtUHJmfUquCjwz&index=32 Up to time 00:21:34

https://www.youtube.com/watch?v=1AZzb2FAVc4&list=PLxIvc-MGOs6gZIMVYOOEtUHJmfUquCjwz&index=34

Thank You

Dr. Ahmed Hagag

ahagag@fci.bu.edu.eg