School of Engineering and Computer Science

Mathematical tools applied to Computer Science

Ch2: Number Theory and Cryptography

Kamel ATTAR
kamel.attar@epita.fr

Week #3 ✦ 24/SEP/2024 ✦
Week #4 ✦ 01/OCT/2024 ✦

Translating back

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 $a \mid b$ denotes that a divides b.We write $a \nmid b$ when a does not divide b.

Example

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

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 $a \mid b$ denotes that a divides b.We write $a \nmid b$ when a does not divide b.

Example

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

Solution

We see that $3 \nmid 7$, because $\frac{7}{3}$ is not an integer. On the other hand, $3 \mid 12$ because $\frac{12}{3} = 4$.

Theorem :

Let a, b and c be integers, where $a \neq 0$. 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 $a \mid c$.

Corollary

If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

✎ Wooclap 1.

① Does 17 divide each of these numbers?

$$a)\ 68 \qquad b)\ 84 \qquad c)\ 357 \qquad d)\ 1001$$

② Prove that if a is an integer other than 0, then

$$a)\ 1 \text{ divides } a. \qquad b)\ a \text{ divides } 0.$$

③ Show that if $a \mid b$ and $b \mid a$, where a and b are integers other than 0, then $a = b$ or $a = -b$.

④ Show that if a, b, c, and d are integers, where $a \neq 0$, such that $a \mid c$ and $b \mid d$, then $ab \mid cd$.

⑤ Show that if a, b, and c are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$.

Theorem : THE 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 $a = dq + r$.

Theorem : THE 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 $a = dq + r$.

$$a = dq + r$$

Divisor: d is called the **divisor**;
Dividend: a is called the **dividend**;
Quotient: q is called the **quotient**;
Remainder: r is called the **remainder**.

Theorem : THE 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 $a = dq + r$.

$$a = dq + r$$

Divisor: d is called the **divisor**;
Dividend: a is called the **dividend**;
Quotient: q is called the **quotient**;
Remainder: r is called the **remainder**.

This notation is used to express the quotient and remainder:

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

Example

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

Example

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

Solution

We have

$$101 = 11 \times 9 + 2$$

Hence, the quotient when 101 is divided by 11 is $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \bmod 11$.

Example

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

Example

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 $-4 = -11 \text{ div } 3$, and the remainder is $1 = -11 \bmod 3$.
Note that the remainder cannot be negative. Consequently, the remainder is not -2, even though

$$-11 = 3(-3) - 2,$$

because $r = -2$ does not satisfy $0 \leq r < 3$.

✎ **Wooclap 2.** What are the quotient and remainder when

a) 19 is divided by 7?

b) -111 is divided by 11?

c) 789 is divided by 23?

d) 1001 is divided by 13?

e) 0 is divided by 19?

f) 3 is divided by 5?

g) -1 is divided by 3?

h) 4 is divided by 1?

Definition (Modular Arithmetic)

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.

Definition (Modular Arithmetic)

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.

Example

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

Definition (Modular Arithmetic)

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.

Example

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

Solution

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

Theorem :

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

$$a \equiv b \pmod{m} \iff a = b + km\,.$$

Theorem :

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

$$a \equiv b \pmod{m} \iff a = b + km\,.$$

Proposition :

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

Theorem :

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

$$a \equiv b \pmod{m} \iff a = b + km\,.$$

Proposition :

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

Example

Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from the previous theorem that $18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$ and that $77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$.

✎ **Wooclap 3.** Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

a. $c \equiv 9a \pmod{13}$
b. $c \equiv 11b \pmod{13}$
c. $c \equiv a + b \pmod{13}$
d. $c \equiv 2a + 3b \pmod{13}$
e. $c \equiv a^2 + b^2 \pmod{13}$
f. $c \equiv a^3 - b^3 \pmod{13}$

✎ **Wooclap 7.** Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

a. $c \equiv 9a \pmod{13}$
b. $c \equiv 11b \pmod{13}$
c. $c \equiv a + b \pmod{13}$
d. $c \equiv 2a + 3b \pmod{13}$
e. $c \equiv a^2 + b^2 \pmod{13}$
f. $c \equiv a^3 - b^3 \pmod{13}$

✎ **Wooclap 8.** Evaluate these quantities.

a. $13 \bmod 3$ b. $-97 \bmod 11$ c. $155 \bmod 19$ d. $-221 \bmod 23$

✎ **Wooclap 11.** Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

a. $c \equiv 9a \pmod{13}$
b. $c \equiv 11b \pmod{13}$
c. $c \equiv a + b \pmod{13}$
d. $c \equiv 2a + 3b \pmod{13}$
e. $c \equiv a^2 + b^2 \pmod{13}$
f. $c \equiv a^3 - b^3 \pmod{13}$

✎ **Wooclap 12.** Evaluate these quantities.

a. $13 \bmod 3$ b. $-97 \bmod 11$ c. $155 \bmod 19$ d. $-221 \bmod 23$

✎ **Wooclap 13.** Find the integer a such that

a. $a \equiv -15 \pmod{23}$ and $-26 \leq a \leq 0$
b. $a \equiv 24 \pmod{29}$ and $-15 \leq a \leq 15$
c. $c \equiv 99 \pmod{21}$ and $100 \leq a \leq 140$

✎ **Wooclap 15.** Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

a. $c \equiv 9a \pmod{13}$
b. $c \equiv 11b \pmod{13}$
c. $c \equiv a + b \pmod{13}$
d. $c \equiv 2a + 3b \pmod{13}$
e. $c \equiv a^2 + b^2 \pmod{13}$
f. $c \equiv a^3 - b^3 \pmod{13}$

✎ **Wooclap 16.** Evaluate these quantities.

a. $13 \bmod 3$ b. $-97 \bmod 11$ c. $155 \bmod 19$ d. $-221 \bmod 23$

✎ **Wooclap 17.** Find the integer a such that

a. $a \equiv -15 \pmod{23}$ and $-26 \leq a \leq 0$
b. $a \equiv 24 \pmod{29}$ and $-15 \leq a \leq 15$
c. $c \equiv 99 \pmod{21}$ and $100 \leq a \leq 140$

✎ **Wooclap 18.** Decide whether each of these integers is congruent to 5 modulo 17.

a. 80 b. 103 c. -29 d. -122.

Definition (Primes)

An integer p greater than 1 is called prime if the only positive factors of p are 1 and p (meaning that p can be divisible only by 1 and itself).

Definition (Primes)

An integer p greater than 1 is called prime if the only positive factors of p are 1 and p (meaning that p can be divisible only by 1 and itself).

- A positive integer that is greater than 1 and is not prime is called composite.
- The integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$.

Definition (Primes)

An integer p greater than 1 is called prime if the only positive factors of p are 1 and p (meaning that p can be divisible only by 1 and itself).

- A positive integer that is greater than 1 and is not prime is called composite.
- The integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$.

Example

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.

Theorem : 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 where the prime factors are written in order of nondecreasing size.

Theorem : 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 where the prime factors are written in order of nondecreasing size.

Example

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

$$\begin{aligned} 100 &= 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2, \\ 641 &= 641, \\ 999 &= 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37, \\ 1024 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}. \end{aligned}$$

Theorem :

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

Theorem :

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

Example

Show that 101 is prime.

Theorem :

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

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.

Theorem :

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

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.

✎ **Wooclap 22.** Determine whether each of these integers is prime.

$a)\ 21$ $b)\ 29$ $c)\ 71$ $d)\ 97$ $e)\ 111$ $f)\ 143$.

Example

Find the prime factorization of $\mathbf{7007}$.

We are tasked with finding the prime factorization of $\mathbf{7007}$.

- **Step 1: Dividing by Small Primes**
  We begin by checking if $\mathbf{7007}$ is divisible by small primes such as $\mathbf{2}$, $\mathbf{3}$, $\mathbf{5}$, and so on.

Example

Find the prime factorization of $\mathbf{7007}$.

We are tasked with finding the prime factorization of $\mathbf{7007}$.

- **Step 1: Dividing by Small Primes**
  We begin by checking if $\mathbf{7007}$ is divisible by small primes such as $\mathbf{2}$, $\mathbf{3}$, $\mathbf{5}$, and so on.

  Check divisibility by 2: Since $\mathbf{7007}$ is odd, it is not divisible by $\mathbf{2}$.

Example

Find the prime factorization of $\mathbf{7007}$.

We are tasked with finding the prime factorization of $\mathbf{7007}$.

- **Step 1: Dividing by Small Primes**
  We begin by checking if $\mathbf{7007}$ is divisible by small primes such as $\mathbf{2}$, $\mathbf{3}$, $\mathbf{5}$, and so on.

  Check divisibility by 2: Since $\mathbf{7007}$ is odd, it is not divisible by $\mathbf{2}$.

  Check divisibility by 3: The sum of the digits of $\mathbf{7007}$ is:

  $$\mathbf{7 + 0 + 0 + 7 = 14}$$

  Since $\mathbf{14}$ is not divisible by $\mathbf{3}$, $\mathbf{7007}$ is not divisible by $\mathbf{3}$.

Example

Find the prime factorization of $\mathbf{7007}$.

We are tasked with finding the prime factorization of $\mathbf{7007}$.

- **Step 1: Dividing by Small Primes**
  We begin by checking if $\mathbf{7007}$ is divisible by small primes such as $\mathbf{2}$, $\mathbf{3}$, $\mathbf{5}$, and so on.

  Check divisibility by 2: Since $\mathbf{7007}$ is odd, it is not divisible by $\mathbf{2}$.

  Check divisibility by 3: The sum of the digits of $\mathbf{7007}$ is:

  $$\mathbf{7 + 0 + 0 + 7 = 14}$$

  Since $\mathbf{14}$ is not divisible by $\mathbf{3}$, $\mathbf{7007}$ is not divisible by $\mathbf{3}$.

  Check divisibility by 5: The last digit of $\mathbf{7007}$ is $\mathbf{7}$, so it is not divisible by $\mathbf{5}$.

Example

Find the prime factorization of $\mathbf{7007}$.

We are tasked with finding the prime factorization of $\mathbf{7007}$.

- **Step 1: Dividing by Small Primes**
  We begin by checking if $\mathbf{7007}$ is divisible by small primes such as $\mathbf{2}$, $\mathbf{3}$, $\mathbf{5}$, and so on.

  Check divisibility by 2: Since $\mathbf{7007}$ is odd, it is not divisible by $\mathbf{2}$.

  Check divisibility by 3: The sum of the digits of $\mathbf{7007}$ is:

  $$\mathbf{7 + 0 + 0 + 7 = 14}$$

  Since $\mathbf{14}$ is not divisible by $\mathbf{3}$, $\mathbf{7007}$ is not divisible by $\mathbf{3}$.

  Check divisibility by 5: The last digit of $\mathbf{7007}$ is $\mathbf{7}$, so it is not divisible by $\mathbf{5}$.

  Check divisibility by 7: We divide $\mathbf{7007}$ by $\mathbf{7}$:

  $$\mathbf{7007 \div 7 = 1001}$$

  Thus, $\mathbf{7007 = 7 \times 1001}$.

- **Step 2: Prime Factorization of 1001**

  Next, we find the prime factorization of $\mathbf{1001}$. We again check for divisibility by small primes.

- **Step 2: Prime Factorization of 1001**

  Next, we find the prime factorization of $\mathbf{1001}$. We again check for divisibility by small primes.

  Check divisibility by 7: We divide $\mathbf{1001}$ by $\mathbf{7}$:

  $$\mathbf{1001 \div 7 = 143}$$

  Thus, $\mathbf{1001 = 7 \times 143}$, and we now need to factor $\mathbf{143}$.

Step 2: Prime Factorization of 1001

Next, we find the prime factorization of $\mathbf{1001}$. We again check for divisibility by small primes.

Check divisibility by 7: We divide $\mathbf{1001}$ by $\mathbf{7}$:

$$\mathbf{1001 \div 7 = 143}$$

Thus, $\mathbf{1001 = 7 \times 143}$, and we now need to factor $\mathbf{143}$.

Check divisibility of $\mathbf{143}$ by small primes:

$\mathbf{143}$ is odd, so it is not divisible by $\mathbf{2}$.
The sum of the digits of $\mathbf{143}$ is $\mathbf{1 + 4 + 3 = 8}$, which is not divisible by $\mathbf{3}$.
The last digit of $\mathbf{143}$ is $\mathbf{3}$, so it is not divisible by $\mathbf{5}$.

Step 2: Prime Factorization of 1001

Next, we find the prime factorization of $\mathbf{1001}$. We again check for divisibility by small primes.

Check divisibility by 7: We divide $\mathbf{1001}$ by $\mathbf{7}$:

$$\mathbf{1001 \div 7 = 143}$$

Thus, $\mathbf{1001 = 7 \times 143}$, and we now need to factor $\mathbf{143}$.

Check divisibility of $\mathbf{143}$ by small primes:

$\mathbf{143}$ is odd, so it is not divisible by $\mathbf{2}$.
The sum of the digits of $\mathbf{143}$ is $\mathbf{1 + 4 + 3 = 8}$, which is not divisible by $\mathbf{3}$.
The last digit of $\mathbf{143}$ is $\mathbf{3}$, so it is not divisible by $\mathbf{5}$.

Check divisibility by 11: The alternating sum of the digits of $\mathbf{143}$ is:

$$\mathbf{1 - 4 + 3 = 0}$$

Since $\mathbf{0}$ is divisible by $\mathbf{11}$, $\mathbf{143}$ is divisible by $\mathbf{11}$. We divide:

$$\mathbf{143 \div 11 = 13}$$

Thus, $\mathbf{143 = 11 \times 13}$.

Step 3: Conclusion

We have factored $\mathbf{7007}$ as:

$$\mathbf{7007 = 7 \times 1001 = 7 \times 7 \times 143 = 7 \times 7 \times 11 \times 13}$$

Therefore, the prime factorization of $\mathbf{7007}$ is:

$$\mathbf{7007 = 7^2 \times 11 \times 13}$$

✎ **Wooclap 23.** Find the prime factorization of each of these integers.

$a)$ 88 $b)$ 126 $c)$ 729 $d)$ 1001 $e)$ 1111 $f)$ 909.090

✎ **Wooclap 24.** Find the prime factorization of $10!$.

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

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

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

Integers divisible by 2, 3, 5 and 7 highlighted with different colors

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

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 .

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 $\gcd(a, b)$.

Example

What is the greatest common divisor of 24 and 36?

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 $\gcd(a, b)$.

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?

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

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

Theorem :

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

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

Theorem :

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

✎ Wooclap 28.

1. Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.
2. Which positive integers less than 30 are relatively prime to 30?

Theorem : Another way to find the greatest common divisor

Suppose that the prime factorizations of the positive integers a and b are

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

where each exponent is a nonnegative integer. Then $\gcd(a, b)$ is given by

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

Theorem : Another way to find the greatest common divisor

Suppose that the prime factorizations of the positive integers a and b are

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

where each exponent is a nonnegative integer. Then $\gcd(a, b)$ is given by

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

Example

Because the prime factorizations of 120 and 500 are $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, the greatest common divisor is

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

Definition

The least *common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\text{lcm}(a, b)$.

Definition

The least *common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\text{lcm}(a, b)$.

Theorem :

Suppose that the prime factorizations of the positive integers a and b are

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

where each exponent is a nonnegative integer. Then $\text{lcm}(a, b)$ is given by

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

Example

What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

Example

What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

Solution

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

Example

What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

Solution

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

Theorem :

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

Theorem :

1. If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.
2. If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.
3. Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

✎ **Wooclap 29.** What are the greatest common divisors of these pairs of integers? and What is the least common multiple of each pair ?

a. $3^7 \cdot 5^3 \cdot 7^3$; $2^{11} \cdot 3^5 \cdot 5^9$
b. $11 \cdot 13 \cdot 17$; $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$
c. 23^{31} ; 23^{17}
d. $41 \cdot 43 \cdot 53$; $41 \cdot 43 \cdot 53$
e. $3^{13} \cdot 5^{17}$; $2^{12} \cdot 7^{21}$
f. 1111 ; 0

Lemma

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

Lemma

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

Proof: We will show now how Euclidean algorithm is used to find $gcd(a, b)$.

- 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

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

- Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots > 0$ cannot contain more than a terms.
- Furthermore,it follows from Lemma that

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

- Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

Example

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

Example

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

solution

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

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

Cryptography is the discipline focused on techniques for secure communication, allowing the transmission of information in a manner that protects it from unauthorized access. It plays a crucial role in ensuring data privacy and integrity across various applications, such as secure messaging, online banking, and e-commerce.

(a) The **sender** is the individual or system that intends to transmit a message to a **receiver**, who is the intended recipient of that message.
(b) The **adversary** is any entity attempting to intercept, alter, or otherwise compromise the message being sent, thus posing a threat to confidentiality and security.
(c) In **private key cryptography** (also known as symmetric cryptography), the sender and receiver share a secret key before communication begins. This key is used to both encrypt and decrypt messages, requiring secure management to prevent unauthorized access.
(d) In **public key cryptography** (asymmetric cryptography), the encryption process uses two keys: a public key that can be shared openly and a private key that is kept secret. The public key is used to encrypt messages, while the corresponding private key is used to decrypt them, allowing secure communication without needing to share the secret key beforehand.
(e) The original, unencrypted message is referred to as the **plaintext**. It is the information that the sender wishes to transmit securely.
(f) The transformed message, which is no longer readable without the proper key, is called the **ciphertext**. It results from applying a cryptographic algorithm to the plaintext.
(g) A **Caesar cipher** is a type of substitution cipher in which each letter in the plaintext is shifted by a fixed number of positions down or up the alphabet. For example, a shift of 3 would convert the letter 'A' to 'D', 'B' to 'E', and so on. This cipher is named after Julius Caesar, who reportedly used it to communicate with his generals.
(h) Cryptographic protocols, such as the **Diffie-Hellman key exchange** and the **RSA algorithm**, provide secure methods for exchanging keys and encrypting messages. These protocols are foundational to modern secure communications.

Definition (Caesar Cipher)

The **Caesar cipher** is a simple substitution cipher where each letter in the plaintext is shifted by a fixed number of positions down the alphabet. Mathematically, to represent the Caesar cipher, we first map each letter of the alphabet to an element of the set

$$\mathbb{Z}_{26} = \{X \in \mathbb{Z} : 0 \leq X \leq 25\}, \qquad A = 0, B = 1, \cdots, Z = 25.$$

Caesar's encryption method can be modeled by a function f that maps an integer p (representing a letter) to another integer $f(p)$, where $0 \leq p \leq 25$. The encryption rule is given by the formula:

$$f(p) \equiv (p + 3) \bmod 26.$$

Here, the number 3 represents the fixed shift, meaning each letter is shifted 3 places forward in the alphabet.

Definition (Caesar Cipher)

The **Caesar cipher** is a simple substitution cipher where each letter in the plaintext is shifted by a fixed number of positions down the alphabet. Mathematically, to represent the Caesar cipher, we first map each letter of the alphabet to an element of the set

$$\mathbb{Z}_{26} = \{X \in \mathbb{Z} : 0 \leq X \leq 25\}, \qquad A = 0,\ B = 1,\ \cdots,\ Z = 25.$$

Caesar's encryption method can be modeled by a function f that maps an integer p (representing a letter) to another integer $f(p)$, where $0 \leq p \leq 25$. The encryption rule is given by the formula:

$$f(p) \equiv (p + 3) \bmod 26.$$

Here, the number 3 represents the fixed shift, meaning each letter is shifted 3 places forward in the alphabet.

The notation $\mathbb{Z}_n$ refers to the set of integers $\{0, 1, \ldots, n-1\}$. When we write $x \in \mathbb{Z}_n$, we mean that x is a variable that can take any value from this set. In the context of the Caesar cipher, $\mathbb{Z}_{26}$ is used because there are 26 letters in the alphabet.

Definition (Caesar Cipher)

The **Caesar cipher** is a simple substitution cipher where each letter in the plaintext is shifted by a fixed number of positions down the alphabet. Mathematically, to represent the Caesar cipher, we first map each letter of the alphabet to an element of the set

$$\mathbb{Z}_{26} = \{X \in \mathbb{Z} : 0 \leq X \leq 25\}, \qquad A = 0,\ B = 1,\ \cdots,\ Z = 25.$$

Caesar's encryption method can be modeled by a function f that maps an integer p (representing a letter) to another integer $f(p)$, where $0 \leq p \leq 25$. The encryption rule is given by the formula:

$$f(p) \equiv (p + 3) \bmod 26.$$

Here, the number 3 represents the fixed shift, meaning each letter is shifted 3 places forward in the alphabet.

Example

If the plaintext is "HELLO", and we apply a Caesar shift of 3:
H (7) becomes K (10), E (4) becomes H (7), L (11) becomes O (14),
L (11) becomes O (14), O (14) becomes R (17).
The resulting ciphertext is "KHOOR".

Example

What is the secret message produced from the message

"MEET YOU IN THE PARK"

Using the Caesar cipher?

Example

What is the secret message produced from the message

"MEET YOU IN THE PARK"

Using the Caesar cipher?

Solution

First replace the letters in the message with numbers. This produces

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3) \bmod 26$. This gives

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating this back to letters produces the encrypted message

"PHHW BRX LQ WKH SDUN."

Definition (Decrypting the Caesar Cipher)

To recover the original message from a message encrypted using the Caesar cipher, we use the inverse function f^{-1} of the encryption function f.

$$\begin{array}{rccl} f^{-1} & : & \mathbb{Z}_{26} & \to & \text{mod } 26 \\ & & p & \mapsto & f^{-1}(p) = (p-3) \text{ mod } 26 \end{array}$$

Definition (Decrypting the Caesar Cipher)

To recover the original message from a message encrypted using the Caesar cipher, we use the inverse function f^{-1} of the encryption function f.

$$\begin{array}{rccl} f^{-1} & : & \mathbb{Z}_{26} & \to & \text{mod } 26 \\ & & p & \mapsto & f^{-1}(p) = (p-3) \text{ mod } 26 \end{array}$$

- The Caesar cipher can be generalized to a broader class of ciphers. Instead of shifting each letter by a fixed value of 3, we can shift by an arbitrary integer k.

Definition (Decrypting the Caesar Cipher)

To recover the original message from a message encrypted using the Caesar cipher, we use the inverse function f^{-1} of the encryption function f.

$$\begin{array}{rccl} f^{-1} & : & \mathbb{Z}_{26} & \to & \text{mod } 26 \\ & & p & \mapsto & f^{-1}(p) = (p-3) \text{ mod } 26 \end{array}$$

- The Caesar cipher can be generalized to a broader class of ciphers. Instead of shifting each letter by a fixed value of 3, we can shift by an arbitrary integer k.
- In this case, the encryption function becomes:

$$f(p) = (p+k) \text{ mod } 26\,,$$

where k is the key that determines the shift. This generalized version is known as the *shift cipher* or *Caesar shift*.

Definition (Decrypting the Caesar Cipher)

To recover the original message from a message encrypted using the Caesar cipher, we use the inverse function f^{-1} of the encryption function f.

$$\begin{array}{rccl} f^{-1} & : & \mathbb{Z}_{26} & \to & \text{mod } 26 \\ & & p & \mapsto & f^{-1}(p) = (p-3) \text{ mod } 26 \end{array}$$

- The Caesar cipher can be generalized to a broader class of ciphers. Instead of shifting each letter by a fixed value of 3, we can shift by an arbitrary integer k.
- In this case, the encryption function becomes:

$$f(p) = (p+k) \text{ mod } 26\,,$$

where k is the key that determines the shift. This generalized version is known as the *shift cipher* or *Caesar shift*.

- Decryption in the shift cipher is performed by reversing the shift, using the formula:

$$f^{-1}(p) = (p-k) \text{ mod } 26.$$

Here, k represents the secret key used for both encryption and decryption.

Example

Encrypt the plaintext message

STOP GLOBAL WARMING

using the shift cipher with shift $k = 11$.

Example

Encrypt the plaintext message

STOP GLOBAL WARMING

using the shift cipher with shift $k = 11$.

Solution

To encrypt the message

STOP GLOBAL WARMING

we first translate each letter to the corresponding element of 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 $f(p) = (p + 11) \bmod 26$ to each number in this string.

Solution

We obtain

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

Translating this last string back to letters, we obtain the cipher text

$$\text{DEZA} \quad \text{RWZMLW} \quad \text{HLCXTYR}$$

Example

Decrypt the cipher text message

LEWLYPLUJL PZ H NYLHA ALHJOLY

that was encrypted with the shift cipher with shift $k = 7$.

Example

Decrypt the cipher text message

LEWLYPLUJL PZ H NYLHA ALHJOLY

that was encrypted with the shift cipher with shift $k = 7$.

Solution

To decrypt the ciphertext

LEWLYPLUJL PZ H NYLHA ALHJOLY

we first translate the letters back to elements of Z_{26}. We obtain

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.

Solution

Next, we shift each of these numbers by $-k = -7$ modulo 26 to obtain

$$4\ 23\ 15\ 4\ 17\ 8\ 4\ 13\ 2\ 4 \quad 8\ 18 \quad 0 \quad 6\ 17\ 4\ 0\ 19 \quad 19\ 4\ 0\ 2\ 7\ 4\ 17.$$

Finally, we translate these numbers back to letters to obtain the plaintext. We obtain

$$\text{EXPERIENCE} \quad \text{IS} \quad \text{A} \quad \text{GREAT} \quad \text{TEACHER.}$$

We can enhance the security of shift ciphers by using a more general function of the form:

$$f(p) = (ap + b) \bmod 26,$$

where a and b are integers, chosen such that f is a bijection (i.e., every input maps to a unique output and vice versa).

We can enhance the security of shift ciphers by using a more general function of the form:

$$f(p) = (ap + b) \bmod 26,$$

where a and b are integers, chosen such that f is a bijection (i.e., every input maps to a unique output and vice versa).

Example

What letter replaces the letter K when the encryption function $f(p) = (7p + 3) \bmod 26$ is used?

We can enhance the security of shift ciphers by using a more general function of the form:

$$f(p) = (ap + b) \bmod 26,$$

where a and b are integers, chosen such that f is a bijection (i.e., every input maps to a unique output and vice versa).

Example

What letter replaces the letter K when the encryption function $f(p) = (7p + 3) \bmod 26$ is used?

Solution

First, recall that K is represented by 10 in the alphabet (where $A = 0, B = 1, \ldots, Z = 25$). Using the given encryption function, we compute:

$$f(10) = (7 \cdot 10 + 3) \bmod 26 = 73 \bmod 26 = 21.$$

Since 21 represents the letter V, the letter K is replaced by V in the encrypted message.

✎ Wooclap 30.

1. Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

   a) $f(p) = (p + 3) \bmod 26$ (the Caesar cipher)
   b) $f(p) = (p + 13) \bmod 26$
   c) $f(p) = (3p + 7) \bmod 26$

2. Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

   a) $f(p) = (p + 14) \bmod 26$
   b) $f(p) = (14p + 21) \bmod 26$
   c) $f(p) = (-7p + 1) \bmod 26$

✎ Wooclap 31.

1. Decrypt these messages that were encrypted using the Caesar cipher.

   a) EOXH MHDQV
   b) WHVW WRGDB
   c) HDW GLP VXP

2. Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10) \bmod 26$.

   a) CEBBOXNOB XYG
   b) LO WI PBSOXN
   c) DSWO PYB PEX