NUMBER THEORY

4.1, 4.3

4.1
Divisibility and Modular Arithmetic

DIVISION ALGORITHM

- The quotient remainder theorem states that when an integer is divided by an integer we get one remainder and quotient.

- The value of remainder will either be 0 or less than to number we are divided with.

THEOREM (Quotient-Remainder Theorem)

- Given any integer n and a positive integer d, there exist unique integers q and r such that

$$n = d \cdot q + r$$

where

$$0 \leq r < d.$$

EXAMPLE

- What is the quotient and remainder when 54 is divided by 4?

- $n =$ 54 and we divide it with 4 i.e. $d = 4$

$$n = d \cdot q + r$$

$$54 = 4 \cdot 13 + 2;$$

Hence,

Quotient = 13 and Remainder = 2

EXAMPLE

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

- $n = -11$ and we divide it with 1 i.e. $d = 3$

$$n = d \cdot q + r$$

$$-11 = 3 \cdot (-4) + 1;$$

Hence,

Quotient $= -4$ and Remainder $= 1$

EXAMPLE

- What is the quotient and remainder when -54 is divided by 4?

- $n = -54$ and we divide it with 4 i.e. $d = 4$

$$n = d \cdot q + r$$

$$-54 = 4 \cdot (-14) + 2;$$

Hence,

Quotient $= -14$ and Remainder $= 2$

EXAMPLE

- What is the quotient and remainder when 54 is divided by 70?

- If we take $n = 54$ and we divide it with 70 i.e. $d = 70$

  Here,

$$\text{divisor} > \text{number}$$

$$n = d \cdot q + r$$

$$54 = 70 \cdot (0) + 54;$$

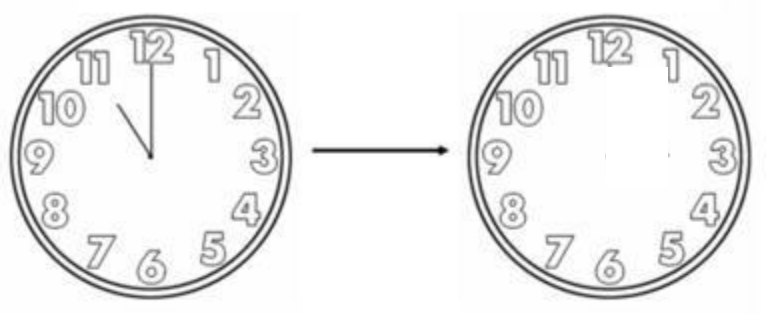
Hence,

Quotient = 0 and Remainder = 54

Divisibility and modular arithmetic

In many applications, we only care about the remainder when an integer is divided by a specific positive integer.

Example: On a 12-hour clock, what time is it when it is 52 hours after 11:00?

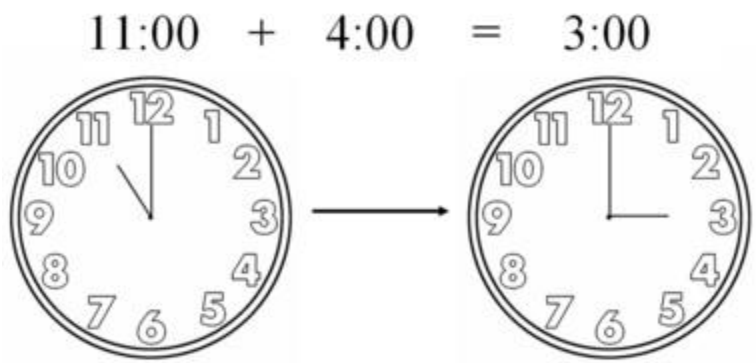


Divisibility and modular arithmetic

In many applications, we only care about the remainder when an integer is divided by a specific positive integer.

Example: On a 12-hour clock, what time is it when it is 52 hours after 11:00?

Answer: 52 **mod** 12 = 4 ⇒ 11:00 + 4 hrs = 15:00
⇒ 15:00 **mod** 12 = 3:00



Example: What day of the week will it be 100 days from today?

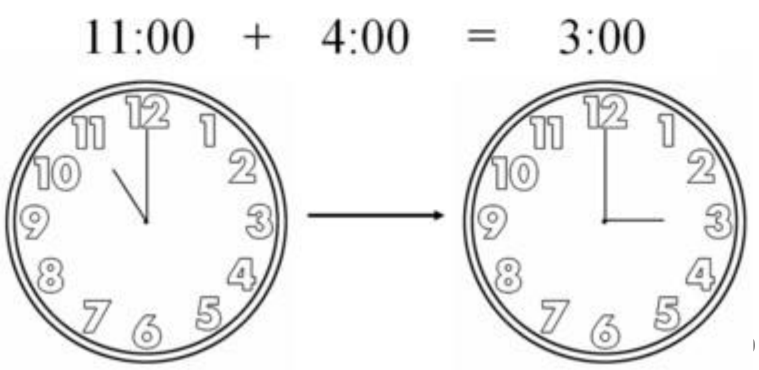
Answer:

Divisibility and modular arithmetic

In many applications, we only care about the remainder when an integer is divided by a specific positive integer.

Example: On a 12-hour clock, what time is it when it is 52 hours after 11:00?

Answer: 52 **mod** 12 = 4 ⇒ 11:00 + 4 hrs = 15:00 ⇒ 15:00 **mod** 12 = 3:00



Example: What day of the week will it be 100 days from today?

Answer: 100 **mod** 7 = 2

Congruence Relation

Definition: If a and b are integers and m is a positive integer, then a is *congruent* to *b modulo m* if m divides $a - b$.

- The notation $a \equiv b \pmod{m}$ says that a is congruent to b modulo m.
- We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus*.
- Two integers are congruent mod m if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write

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

Congruence Relation

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

Solution:

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

Examine that 38 mod 5 = 3 and 13 mod 5 = 3, then it can be written that $38 \equiv 13 \pmod 5$.

Pronounce: 38 is congruent with 13 in modulo 5.

Congruence examples

Example:

- $17 \equiv 2 \pmod 3$

  → 3 divides $17-2 = 15$ without remainder
- $-7 \equiv 15 \pmod{11}$

  → 11 divides $-7-15 = -22$ without remainder
- $12 \not\equiv 2 \pmod 7$

  → 7 cannot divide $12-2 = 10$
- $-7 \not\equiv 15 \pmod 3$

  → 3 cannot divide $-7-15 = -22$

Congruence Theorem 1 & 2

1- **Congruence and Divisibility**

Suppose a and b are integers and $m > 0$.
If m divides $a - b$ without remainder, then $a \equiv b \pmod{m}$.

OR

a≡b(modn) if and only if n|a−b

2- Theorem 2: **Congruence and Equality**

$a \equiv b \pmod{m}$ can be written as $a = b + km$ (k integer).

1- $3x \equiv 5 \pmod{7}$ theorem2: $a=b+kn$ for some integer k

$3x=5+7k$ divide with 3 on both sides

$x=(5+7K)/3$ find min value of k of 3 multiple

$=(5+7.1)/3$

$=12/3$

$x=4$

Solve the following linear congruence equations.

(a) $3x \equiv 5 \pmod 7$

Answer: $x = 4$ since $3 \cdot 4 = 12 = 5 \pmod 7$.

(b) $5x \equiv 4 \pmod 7$

Answer: $x = 5$ since $5 \cdot 5 = 25 = 4 \pmod 7$.

(c) $2x \equiv 1 \pmod 7$

Answer: $x = 4$ since $2 \cdot 1 = 8 = 1 \pmod 7$.

(d) $6x \equiv 3 \pmod 7$

Answer: $x = 4$ since $6 \cdot 4 = 24 = 3 \pmod 7$.

Theorem:3

$a \bmod m = r$ can also be written as $a \equiv r \pmod{m}$.

Example:

- $23 \bmod 5 = 3 \rightarrow 23 \equiv 3 \pmod{5}$
- $14 \bmod 8 = 6 \rightarrow 14 \equiv 6 \pmod{8}$
- $-41 \bmod 9 = 4 \rightarrow -41 \equiv 4 \pmod{9}$
- $-39 \bmod 13 = 0 \rightarrow -39 \equiv 0 \pmod{13}$

Theorem:4 & 5

Congruence and Arithmetic:

Suppose m is a positive integer.

If $a \equiv b \pmod{m}$ and c is an arbitrary integer, then

- $(a + c) \equiv (b + c) \pmod{m}$
- $ac \equiv bc \pmod{m}$
- $a^p \equiv b^p \pmod{m}$, p non-negative

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

- $(a + c) \equiv (b + d) \pmod{m}$
- $ac \equiv bd \pmod{m}$

Therorem:4 & 5 Example

Example:

Suppose $17 \equiv 2 \pmod 3$ and $10 \equiv 4 \pmod 3$, then according to the Congruence Theorem,

- $17 + 5 \equiv 2 + 5 \pmod 3 \quad \Leftrightarrow \quad 22 \equiv 7 \pmod 3$
- $17 \cdot 5 \equiv 2 \cdot 5 \pmod 3 \quad \Leftrightarrow \quad 85 \equiv 10 \pmod 3$
- $17 + 10 \equiv 2 + 4 \pmod 3 \quad \Leftrightarrow \quad 27 \equiv 6 \pmod 3$
- $17 \cdot 10 \equiv 2 \cdot 4 \pmod 3 \quad \Leftrightarrow \quad 170 \equiv 8 \pmod 3$

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

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod 5$$
$$77 = 7 \;\; 11 \equiv 2 + 1 = 3 \pmod 5$$

NOTE:

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

Example: The congruence $14 \equiv 8 \pmod 6$ holds. But dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod 6$.

Arithmetic Modulo m

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

- The operation $+_m$ is defined as $a +_m b = (a + b)$ **mod** m. This is *addition modulo m*.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (ab)$ **mod** m. This is *multiplication modulo m*.
- Using these operations is said to be doing *arithmetic modulo m*.

Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Using the definitions above:

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

4.3
Primes and Greatest Common Divisor

Primes Numbers

A positive integer *p* (*p* > 1) is called a **prime number** if its divisors are only 1 and *p*.

For example, 23 is a prime number, because it can only be divided by 1 and 23 to get no remainder.

Numbers which are not prime numbers are called **composite numbers**.

For example, 20 is a composite number, because 20 is divisible by 2, 4, 5, and 10, besides by 1 and 20 itself.

Relatively Prime

Two integers a and b are said to be **relatively prime** if they do not have any common factors other than 1, or, $GCD(a,b) = 1$.

Example:

- 20 and 3 are relatively prime, since $GCD(20,3) = 1$.
- 7 and 11 are relatively prime, since $GCD(7,11) = 1$.
- 20 and 5 are not relatively prime, since $GCD(20,5) = 5 \neq 1$.

If a and b are relatively prime, then there exist integers m and n such that $ma + nb = 1$.

Example:

- 20 and 3 are relatively prime because $GCD(20,3) = 1$, so that it can be written that $2 \cdot 20 + (-13) \cdot 3 = 1$ ($m = 2$, $n = -13$).
- 20 and 5 are not relatively prime because $GCD(20,5) \neq 1$, and thus 20 and 5 cannot be written in the form of $m \cdot 20 + n \cdot 5 = 1$.

Greatest Common Divisor

Suppose *a* and *b* are non-zero integers. The **Greatest Common Divisor** (**GCD**) of *a* and *b* is the greatest possible integer *d* such that $d \mid a$ and $d \mid b$.

In this case, it can be written as GCD(*a*,*b*) = *d*.

Example: Determine GCD(45,36) !

Divisors of 45: 1, 3, 5, 9, 15, 45.

Divisors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36.

Common divisors of 45 and 36 are 1, 3, 9.

For the enumeration above, it can be concluded that GCD(45,36) = 9.

Greatest Common Divisor and Least Common Multiple GCD, LCM

BY USING PRIME FACTORIZATION:

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

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

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

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

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

The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

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

Greatest Common Divisor

Suppose m and n are integer, $n > 0$, such that $m = nq + r$, $0 \le r < n$. Then GCD(m,n) = GCD(n,r).

Example:

Take the value m = 66, n = 18,

66 = 18·3 + 12

then GCD(66,18) = GCD(18,12) = 6.

Linear Congruence

The linear congruence is in the form of:

$$ax \equiv b \pmod{m},$$

where $m > 0$, a and b are arbitrary integers, and x is any integer.

The solution can be found in the way:

$$ax = b + km \rightarrow x = (b + km) / \mathrm{a}$$

Try each value of $k = 0, 1, 2, \ldots$ and $k = -1, -2, \ldots$ that delivers integer value for x.

Linear Congruence example

Example:
Determine the solutions for $4x \equiv 3 \pmod 9$!

$4x \equiv 3 \pmod 9 \rightarrow x = (3 + k \cdot 9) / 4$

$k = 0 \rightarrow x = (3 + 0 \cdot 9) / 4 = 3/4$ $\rightarrow$ not a solution

$k = 1 \rightarrow x = (3 + 1 \cdot 9) / 4 = 3$ $\rightarrow$ **a solution**

$k = 2 \rightarrow x = (3 + 2 \cdot 9) / 4 = 21/4$ $\rightarrow$ not a solution

$k = 3, k = 4$ $\rightarrow$ no solution

$k = 5 \rightarrow x = (3 + 5 \cdot 9) / 4 = 12$ $\rightarrow$ **a solution**

…

$k = -1 \rightarrow x = (3 - 1 \cdot 9) / 4 = -6/4$ $\rightarrow$ not a solution

$k = -2 \rightarrow x = (3 - 2 \cdot 9) / 4 = -15/4$ $\rightarrow$ not a solution

$k = -3 \rightarrow x = (3 - 3 \cdot 9) / 4 = -6$ $\rightarrow$ **a solution**

…

$k = -7 \rightarrow x = (3 - 7 \cdot 9) / 4 = -15$ $\rightarrow$ **a solution**

…

The set of solutions is: $\{3, 12, \ldots, -6, -15, \ldots\}$.

Linear Congruence cont..

Example:
Determine the solutions for $2x \equiv 3 \pmod 4$!

$$2x \equiv 3 \pmod 4 \rightarrow x = (3 + k \cdot 4) / 2$$

Because $k \cdot 4$ is always an even number, then $3 + k \cdot 4$ will always be an odd number.
If an odd number is divided by 2, then the result will be a decimal number (never be an integer).
Thus, there is **no value** of x that can be the solution of $2x \equiv 3 \pmod 4$.

Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

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}

Assignment: Implement this algorithm.

Euclidean algorithm

The Euclidian algorithm is an **efficient** method for computing the greatest common divisor of two integers. It is based on the idea that gcd(a,b) is equal to gcd(a,c) when $a > b$ and c is the remainder when a is divided by b.

Example: Find gcd(287, 91):

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

Stopping condition

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

Euclidean algorithm

Example:

Take m = 80, n = 12, so the condition that $m \geq n$ is fulfilled.

$80 = 12 \cdot 6 + 8$

$12 = 8 \cdot 1 + 4$

$8 = 4 \cdot 2 + 0$

$n = 0 \rightarrow m = 4$ is the last non-zero remainder

GCD(80,12) = 4; **Finish**.

EUCLIDEAN ALGORITHM

- Use the Euclidean algorithm to find $\gcd(330, 156)$

- Divide 330 by 156: (By Quotient-Remainder Theorem)

  This gives $330 = 156 \cdot 2 + 18$
- Divide 156 by 18:

  This gives $156 = 18 \cdot 8 + 12$
- Divide 18 by 12:

  This gives $18 = 12 \cdot 1 + 6$
- Divide 12 by 6:

  This gives $12 = 6 \cdot 2 + 0$

Hence $\gcd(330, 156) = 6$ because 6 is last nonzero remainder

STEPS INVOLVING IN FINDING OUT gcd(330, 156)

- Note that:

  Step 1: we divide 330 by 156

  Step 2: we divide 156 by 18

  Step 3: we divide 18 by 12

  Step 4: we divide 12 by 6

LEMMA

- If a and b are any integers with $b \neq 0$ and q and r are nonnegative integers such that

$$a = q \cdot d + r$$

then

$$\gcd(a,b) = \gcd(b,r)$$

EXAMPLE

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

Successive uses of the division algorithm give:

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

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

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

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

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

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

EXAMPLE

- Find the greatest common divisor of 252 and 198 using the Euclidean algorithm.

Successive uses of the division algorithm give:

$$252 = 198 \cdot 1 + 54$$

$$198 = 54 \cdot 3 + 36$$

$$54 = 36 \cdot 1 + 18$$

$$36 = 18 \cdot 2 + 0$$

- Hence, $\gcd(252, 198) = 18$, because 18 is last nonzero remainder

Linear Combination

GCD(a,b) can be expressed as a *linear combination* of a and b with the multiplying coefficients that can be freely chosen.

Example:
GCD(80,12) = 4, then $4 = (-1)\cdot 80 + (7)\cdot 12$, where –1 and 7 are coefficients that can be freely chosen.

Suppose a and b are positive integers, then there exist integers m and n such that GCD(a,b) = $ma + nb$.

Linear Combinations Example: 1

Example:
Express GCD(312,70) = 2 as the linear combination of 312 and 70!

Applying Euclidean Algorithm:

$312 = 4\cdot 70 + 32$ (1)

$70 = 2\cdot 32 + 6$ (2)

$32 = 5\cdot 6 + 2$ (3)

$6 = 3\cdot 2 + 0$ (4)

Thus, GDC(312,70) = 2

Rearrange (3) to

$2 = 32 - 5\cdot 6$ (5)

Rearrange (2) to

$6 = 70 - 2\cdot 32$ (6)

Insert (6) to (5) so that

$$\begin{aligned} 2 &= 32 - 5\cdot(70 - 2\cdot 32) \\ &= 1\cdot 32 - 5\cdot 70 + 10\cdot 32 \\ &= 11\cdot 32 - 5\cdot 70 \qquad (7) \end{aligned}$$

Rearrange (1) to

$32 = 312 - 4\cdot 70$ (8)

Insert(8) to (7) so that

$$\begin{aligned} 2 &= 11\cdot 32 - 5\cdot 70 \\ &= 11\cdot(312 - 4\cdot 70) - 5\cdot 70 \\ &= 11\cdot 312 - 49\cdot 70 \end{aligned}$$

Thus, GCD(312, 70) = 2

$= 11\cdot 312 - 49\cdot 70$

Linear Combinations Example: 2

Finding gcds as Linear Combinations

Example: Express $\gcd(252,198) = 18$ as a linear combination of 252 and 198.

Solution: First use the Euclidean algorithm to show $\gcd(252,198) = 18$

i. $252 = 1 \cdot 198 + 54$
ii. $198 = 3 \cdot 54 + 36$
iii. $54 = 1 \cdot 36 + 18$
iv. $36 = 2 \cdot 18$

- Now working backwards, from iii and i above
  - $18 = 54 - 1 \cdot 36$
  - $36 = 198 - 3 \cdot 54$
- Substituting the 2nd equation into the 1st yields:
  - $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
- Substituting $54 = 252 - 1 \cdot 198$ (from i)) yields:
  - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$