Number Theory: Integers, Division, Prime Number

Discrete Math Team
Outline

- Integer and Division
- Primes
- GCD (Great Common Divisor)
- LCM (least Common Multiple)
Division

Definition: if $a$ and $b$ are integers ($a \neq 0$), $a$ divides $b$ if $\exists c$ such that $b = ac$.

When $a$ divides $b$, we say that $a$ is a factor of $b$ and that $b$ is a multiple of $a$.

Notation:
- $a \mid b : a$ divides $b$ ($a$ habis membagi $b$; $b$ habis dibagi $a$)
- $a \nmid b : a$ does not divide $b$ ($a$ tidak habis membagi $b$; $b$ tidak habis dibagi $a$)

Example:
- $3 \mid 7$?  $3 \mid 12$?
- $3 \nmid 7$ since $7/3$ is not an integer
- $3 \mid 12$ because $12/3 = 4$
Theorem 1

Let $a$, $b$, and $c$ be integers, then:

- If $a$ divides $b$ and $a$ divides $c$, then $a$ divides $(b + c)$
- If $a$ divides $b$, then $a$ divides $bc$ for all integers $c$
- If $a$ divides $b$ and $b$ divides $c$, then $a$ divides $c$

Proof:

- If $a$ divides $b$ and $a$ divides $c$, then $a$ divides $(b + c)$
  - $b = ma$ and $c = na$
  - $b + c = ma + na = (m + n)a$
  - $b + c = (m + n)a$
  - So, $a$ divides $(b + c)$
Proof

- If $a | b$, then $a | bc$ for all integers $c$
  - $b = ma$, $bc = (ma)c = (mc)a$
  - $bc = (mc)a$
  - So, $a | bc$

- If $a | b$ and $b | c$, then $a | c$
  - $b = ma$, $c = pb = p(ma) = (pm)a$
  - $c = (pm)a$
  - So, $a | c$
Corollary 1

- $a | b$ and $a | c \implies a | mb + nc$

Proof:
- $b = pa$
- $c = qa$
- $mb = (mp)a$
- $nc = (nq)a$
- $mb + nc = (mp + nq)a$
- So, $a | mb + nc$
Division Algorithm

- **Theorem 2**: Let $a$ be an integer and $d$ a positive integer. Then there exist unique integers $q$ and $r$, with $0 \leq r < d$, such that $a = dq + r$.

- **Definition**
  - $q = a \text{ div } d; q = \text{quotient}$, $d = \text{divisor}$, $a = \text{dividend}$
  - $r = a \text{ mod } d; r = \text{remainder}$
Division Algorithm Examples

What are the quotient and remainder when 101 is divided by 11?
- \[101 = 11 \cdot 9 + 2\]
- The quotient is: \[9 = 101 \div 11\]
- The remainder is: \[2 = 101 \mod 11\]

What are the quotient and remainder when -11 is divided by 3?
- \[-11 = 3 (-4) + 1\]
- The quotient is: \[-4 = -11 \div 3\]
- The remainder is: \[1 = -11 \mod 3\]
- Note: the remainder can’t be negative
- \[-11 = 3 (-3) – 2 \Rightarrow r = -2\] doesn’t satisfy \[0 \leq r < 3\]
Modular Arithmetic

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

- **Notation**:
  - $a \equiv b \pmod{m}$; $a$ is congruent to $b$ modulo $m$
  - $a \not\equiv b \pmod{m}$; $a$ and $b$ are not congruent to modulo $m$

- **Theorem 3**:
  - $a \equiv b \pmod{m}$ iff $a \mod m = b \mod m$.

- **Example**:
  - $17 \equiv 12 \mod 5$, $17 \mod 5 = 2$, $12 \mod 5 = 2$
  - $-3 \equiv 17 \mod 10$, $-3 \mod 10 = 7$, $17 \mod 10 = 7$
Modular Arithmetic

Theorem 4:
Let $m$ be a positive integer, $a \equiv b \pmod{m}$ iff $\exists k$ such that $a = b + km$.

Proof:
- If $a \equiv b \pmod{m}$, then $m \mid (a - b)$.
- This means that $\exists k$ such that $a - b = km$, so that $a = b + km$.
- Conversely, if $\exists k$ such that $a = b + km$, then $km = a - b$.
- Hence, $m$ divides $a - b$, so that $a \equiv b \pmod{m}$.
Theorem 5:
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 $ac \equiv bd \pmod{m}$

Proof:
Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, there are integers $s$ and $t$ with
- $b = a + sm$
- $d = c + tm$. Hence:
- $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$
- $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$
Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$
Corollary 2

Let $m$ be a positive integer, $a$ and $b$ be integers. Then:

- $(a + b) \mod m \equiv ((a \mod m) + (b \mod m)) \mod m$
- $ab \equiv (a \mod m)(b \mod m) \mod m$

Proof:

By the definitions of mod $m$ and congruence modulo $m$, we know that $a \equiv (a \mod m)(\mod m)$ and $b \equiv (b \mod m)(\mod m)$

Hence theorem 5 tells us that:

- $(a + b) \mod m \equiv ((a \mod m) + (b \mod m)) \mod m$
- $ab \equiv (a \mod m)(b \mod m) \mod m$
Caesar Cipher

- Alphabet to number: \(a \sim 0, \ b \sim 1, \ldots, \ z \sim 25\).

- Encryption: \(f(p) = (p + k) \mod 26\).

- Decryption: \(f^{-1}(p) = (p - k) \mod 26\).
  - Caesar used \(k = 3\).

- This is called a substitution cipher
  - You are substituting one letter with another.
Caesar Cipher Example

- Encrypt “go cavaliers”
  - Translate to numbers: g = 6, o = 14, etc.
    - Full sequence: 6, 14, 2, 0, 21, 0, 11, 8, 4, 17, 18
  - Apply the cipher to each number: \( f(6) = 9, f(14) = 17 \), etc.
    - Full sequence: 9, 17, 5, 3, 24, 3, 14, 11, 7, 20, 21
  - Convert the numbers back to letters: 9 = j, 17 = r, etc.
    - Full sequence: jr wfdydolhuv

- Decrypt “jr fdydolhuv”
  - Translate to numbers: j = 9, r = 17, etc.
    - Full sequence: 9, 17, 5, 3, 24, 3, 14, 11, 7, 20, 21
  - Apply the cipher to each number: \( f^{-1}(9) = 6, f^{-1}(17) = 14 \), etc.
    - Full sequence: 6, 14, 2, 0, 21, 0, 11, 8, 4, 17, 18
  - Convert the numbers back to letters: 6 = g, 14 = 0, etc.
    - Full sequence: go cavaliers
Caesar Cipher Example

- Encrypt “MEET YOU IN THE PARK”
  - Translate to numbers:
    - Full sequence: 12, 4, 4, 19, 24, 14, 20, 8, 13, 19, 7, 4, 15, 0, 17, 10
  - Apply the cipher to each number:
    - Full sequence: 15, 7, 7, 22, 1, 7, 23, 11, 16, 22, 10, 7, 18, 3, 20, 13
  - Convert the numbers back to letters:
    - Full sequence: PHHW BRX LQ WKH SDUN
Caesar Cipher Example

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

Solution:

- First, note that 10 represents K, then using the encryption function specified, it follows that \( f(10) = (7 \cdot 10 + 3) \mod 26 = 21 \)
- Because 21 represents V, K is replaced by V in the encrypted message.
Prime Numbers

- **Definition**: A positive integer $p$ is prime if the only positive factors of $p$ are 1 and $p$
  - If there are other factors, it is composite
  - Note that 1 is not prime!
  - It’s not composite either – it’s in its own class

- **Definition**: An integer $n$ is composite if and only if there exists an integer $a$ such that $a \mid n$ and $1 < a < n$
Fundamental theorem of arithmetic

- Every positive integer greater than 1 can be uniquely written as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size.

- Examples
  - $100 = 2 \times 2 \times 5 \times 5$
  - $182 = 2 \times 7 \times 13$
  - $29820 = 2 \times 2 \times 3 \times 5 \times 7 \times 71$
Composite Factors

- If $n$ is a composite integer, then $n$ has a prime divisor less than or equal to the square root of $n$. 
Showing a number is prime

Show that 113 is prime

Solution

- The only prime factors less than $\sqrt{113} = 10.63$ are 2, 3, 5, and 7
- Neither of these divide 113 evenly
- Thus, by the fundamental theorem of arithmetic, 113 must be prime
Showing a number is composite

Show that 899 is prime

Solution
- Divide 899 by successively larger primes (up to $\sqrt{899} = 29.98$), starting with 2
- We find that 29 and 31 divide 899
Primes are infinite

- Theorem (by Euclid): There are infinitely many prime numbers

- Proof by contradiction
- Assume there are a finite number of primes
- List them as follows: $p_1, p_2, ..., p_n$.
- Consider the number $q = p_1 p_2 ... p_n + 1$
  - This number is not divisible by any of the listed primes
    - If we divided $p_i$ into $q$, there would result a remainder of 1
  - We must conclude that $q$ is a prime number, not among the primes listed above
    - This contradicts our assumption that all primes are in the list $p_1, p_2, ..., p_n$. 
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
  - Rephrased: the number of prime numbers less than $x$ is approximately $x/\ln(x)$
  - Rephrased: the chance of an number $x$ being a prime number is $1/\ln(x)$

- Consider 200 digit prime numbers
  - $\ln (10^{200}) \approx 460$
  - The chance of a 200 digit number being prime is $1/460$
  - If we only choose odd numbers, the chance is $2/460 = 1/230$
Greatest common divisor

- The greatest common divisor of two integers $a$ and $b$ is the largest integer $d$ such that $d \mid a$ and $d \mid b$
- Denoted by $\text{gcd} \ (a, b)$

Examples
- $\text{gcd} \ (24, 36) = 12$
- $\text{gcd} \ (17, 22) = 1$
- $\text{gcd} \ (100, 17) = 1$
Relative primes

- Two numbers are relatively prime if they don’t have any common factors (other than 1)
- Rephrased: $a$ and $b$ are relatively prime if $\gcd(a, b) = 1$

- $\gcd(25, 39) = 1$, so 25 and 39 are relatively prime
Pairwise relative prime

- A set of integers $a_1$, $a_2$, ... $a_n$ are pairwise relatively prime if, for all pairs of numbers, they are relatively prime.
  - Formally: The integers $a_1$, $a_2$, ... $a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

- Example: are 10, 17, and 21 pairwise relatively prime?
  - $\gcd(10, 17) = 1$, $\gcd(17, 21) = 1$, and $\gcd(21, 10) = 1$
  - Thus, they are pairwise relatively prime.

- Example: are 10, 19, and 24 pairwise relatively prime?
  - Since $\gcd(10, 24) \neq 1$, they are not.
More on gcd’s

- Given two numbers \( a \) and \( b \), rewrite them as:
  \[
a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}
  \]

- Example: gcd \((120, 500)\)
  - \(120 = 2^3 \times 3 \times 5 = 2^3 \times 3^1 \times 5^1\)
  - \(500 = 2^2 \times 5^3 = 2^2 \times 3^0 \times 5^3\)

- Then compute the gcd by the following formula:
  \[
gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}
  \]

- Example: gcd \((120, 500)\) = \(2^{\min(3, 2)} 3^{\min(1, 0)} 5^{\min(1, 3)} = 2^2 3^0 5^1 = 20\)
Least common multiple

- The least common multiple of the positive integers \(a\) and \(b\) is the smallest positive integer that is divisible by both \(a\) and \(b\).
  - Denoted by \(\text{lcm}(a, b)\)
  - \(\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}\)

- Example: \(\text{lcm}(10, 25) = 50\)
- What is \(\text{lcm}(95256, 432)\)?
  - \(95256 = 2^33^57^2; 432 = 2^43^3\)
  - \(\text{lcm}(2^33^57^2, 2^43^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^43^57^2 = 190512\)
lcm and gcd theorem

- Let \(a\) and \(b\) be positive integers. Then \(ab = \text{gcd}(a, b) \times \text{lcm}(a, b)\)

- Example: \(\text{gcd}(10, 25) = 5, \text{lcm}(10, 25) = 50\)
  - \(10 \times 25 = 5 \times 50\)

- Example: \(\text{gcd}(95256, 432) = 216, \text{lcm}(95256, 432) = 190512\)
  - \(95256 \times 432 = 216 \times 190512\)