Integers and Division

Shirley Chu

De La Salle University

Nov 10, 2011

Division

Definition

If a and b are integers and $a \neq 0$, we say *a divides b* if there is an integer c such that $b = ac$.

Notations: $a|b$, $a \not| b$

Example: Determine whether $3|51$ and whether $3|52$.

Division

Theorem

Let a, b, c be integers. Then

a) *if $a|b$ and $a|c$, then $a|(b+c)$;*

b) *if $a|b$, then $a|bc$ for all integers c.*

c) *if $a|b$ and $b|c$, then $a|c$.*

Corollary:

1. If a, b, c are integers, such that $a|b$ and $a|c$, then $a|(mb+nc)$.

The Division Algorithm

Theorem

Let a be an integer and d be a positive integer. Then there are unique integers q and r, where $0 \leq r < d$, such that $a = dq + r$.

$$a = dq + r$$

dividend

divisor

quotient

remainder

Examples

1. What are the quotient and remainder when 101 is divided by 15?
2. What are the quotient and remainder when -11 is divided by 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 $a - b$.

Notations: $a \equiv b \bmod m$, $a \not\equiv b \bmod m$

Example:
Determine whether 17 is congruent to 5 modulo 6.
Determine whether 24 and 17 are congruent modulo 12.

Theorems

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 $a = b + km$.

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

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

Prime

Definition

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

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

Fundamental Theorem of Arithmetic

Theorem

Every positive 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: Give the prime factorization of 100, 625, 1919.

Theorem

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

Greatest Common Divisor

Definition

Let a and b be integers and not both zero. The largest integer d such that $d|a$ and $d|b$ is called *greatest common divisor of a and b*.

Notation: $\gcd(a, b)$.

Example: What is the greatest common divisor of 75 and 325?

GCD

Definition

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

Example: Determine whether 17 and 22 are relatively prime?

Definition

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: Which numbers less than 15 are pairwise relatively prime with 15?

Least Common Multiple

Definition

The *least common multiple of a and b*, where a and b are positive integers, is the smallest positive integer that is divisible by both a and b.

Notation: $\operatorname{lcm}(a, b)$

Primes and GCD, LCM

Prime factorization can be used to find the GCD and LCM of two or more integers.
Let a and b be positive integers, and p_j be primes $(1 \leq j \leq n)$ where

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \\ b &= p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n} \end{aligned}$$

$$\begin{aligned} \gcd(a, b) &= p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)} \\ \operatorname{lcm}(a, b) &= p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \ldots p_n^{\max(a_n, b_n)} \end{aligned}$$

GCD and LCM

Theorem

Let a and b be positive integers. Then

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

.

Euclidean Algorithm

Lemma

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

Example: Find $\gcd(65, 24)$.

$65 = 24(2) + 17$

$24 = 17(1) + 7$

$17 = 7(2) + 3$

$7 = 3(2) + 1$

$3 = 1(3) + 0$

$\boxed{\gcd(65, 24) = 1}$

References

[Rosen, 2007] Kenneth Rosen.
Discrete Mathematics and Its Applications 7^{th} edition, 2007