

Divides

Given integers a and b we say a divides b and write $a|b$ provided there exists an integer q such that $aq = b$.

Examples

- Does 3 divide 6?
- Does -3 divide 6?
- Does 7 divide 15?
- Does 5 divide 0?
- Does 0 divide 3?
- Does 0 divide 0?

Note $a|b$ is a statement, a/b is a number.

Properties of divides

- If $a|b$ and $b|a$, then $a|a$
- If $a|b$ and $b|c$ then $a|c$.
- (Two-out-of-three rule)
If $x = y + z$ and k divides two of x, y , or z , then k divides the third.

The Division Algorithm

Let a and b be integers with $b \neq 0$, then there exist unique integers q and r such that

$$a = bq + r \text{ and } |b| > r \geq 0.$$

Examples:

- $a = 16$ and $b = 3$
- $a = 16$ and $b = 4$
- $a = -16$ and $b = 5$
- $a = 16$ and $b = 32$

Idea behind why division algorithm is true

Existence of quotient and remainder for $a, b > 0$.

Idea: reduce to a smaller case.

If $0 < a < b$, then $a = b \cdot 0 + a$ works.

Otherwise, suppose we know quotient and remainder for $a - b$;
say

$$a - b = b(q') + r.$$

Then $a = b(q' + 1) + r$ gives quotient $q = q' + 1$ and remainder r .

Can make this into a rigorous induction proof—but inductive thinking (i.e. reducing to a previous case is the more important point).

Uniqueness

Suppose $a = bq + r$ and $a = bu + s$ where $0 \leq r, s < b$.

Subtracting gives: $b(q - u) = s - r$.

LHS is multiple of b . RHS lies in $(-b, b)$.

So $s - r = 0$. That is, $s = r$.

Now equate two equations to get $bq = bu$, and hence $q = u$.

Prime numbers

An integer n is prime provided $n > 0$, and n has exactly two positive divisors.

- 1?
- 2?
- 3?
- 4?

Importance of primes

Fundamental Theorem of Arithmetic

Every positive integer is a product of primes.

Proof. By strong induction.

1 is the product of 0 primes

Suppose true for all integers less than n .

If n is prime, n is the product of a single prime and we are done.

Otherwise, $n = ab$ for some integers a and b with $1 < a, b < n$. Since a is a product of primes and b is a product of primes, so is $n = ab$. ■

Can actually show that up to re-ordering of the primes, there is just one way to write a given positive integer as a product of primes.

Only a finite number of primes are known!

Largest known is: $242,643,801-1$, a 12,837,064 digit number;
7.05 megabytes to store digits

Primes are valuable—they are used in providing secure communication (Cryptography)

Infinite of primes

There exist an infinite number of primes.

Proof. Suppose not. List them as p_1, p_2, \dots, p_k .

Consider $n = p_1 p_2 \cdots p_k + 1$.

Any prime divisor of n would divide 1 (by the 2 out of 3 rule).
But a prime can't divide 1; so we have a contradiction. ■

Prime Number Theorem

If $\pi(n)$ denotes the number of primes less than or equal to n , then

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\ln n} = 1.$$

I.e. for n large, $\pi(n)$ is approximately $n/(\ln n)$

First conjectured by Legendre in 1796.

Proven by Hadamard & Poussin in 1896

More elementary proof in 1949 by Erdős.

Euclid's Lemma

Let p be a prime and a and b be integers. Then $p|ab \Rightarrow p|a$ or $p|b$.

Sketch of proof in case a and b positive.

If $p|a$ done. Otherwise use the Division Algorithm to write $a = pq + r$ for some $0 < r < p$.

$p|ab \Rightarrow pk = ab$ for some integer k

Substitution give $pk = (pq + r)b = pqb + rb$.

By 2-out-of-3 rule, $p|rb$.

We've reduced to a smaller case $r < b$. So $p|b$. ■

Integers mod n

Let n be a positive integer.

Define $a \equiv b \pmod{n}$ provided n divides $(b - a)$.

Examples: $3 \equiv 5 \pmod{2}$; $13 \equiv 5 \pmod{4}$

Write $a = r \pmod{n}$, where r is the remainder when a is divided by n .

Examples:

The integers mod n , denoted \mathbb{Z}_n , consists of the numbers $0, 1, \dots, n - 1$, and the operations $+$ and $*$ where $a + b$ is $a + b \pmod{n}$, and $a * b$ is $a \cdot b \pmod{n}$.

Examples:

Can show that these operations make \mathbb{Z}_n into a commutative ring (additive identity 0, multiplicative identity 1).

\mathbb{Z}_n arise in many applications (e.g. coding theory, cryptography, data compression).

Properties of mod arithmetic

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a \equiv b \pmod{n}$ and $ac \equiv bd \pmod{n}$

Consequences

$$10^n \pmod{9}$$

$$x \equiv \text{sum of digits} \pmod{9}$$

$$10^n \pmod{11}$$

$$x \equiv \text{to alternation sum of digits} \pmod{11}$$

Properties of the integers

- Commutative ring ($+$ is associative, commutative, has an identity and every element has an additive inverse; $*$ is associative, commutative, and has an identity; $*$ distributes over addition)
- The positive integers have the well-ordering property (i.e. every nonempty subset of positive integers has a smallest element)
- Is an integral domain; i.e. in addition to $*$ being commutative we have that $ab = 0$ implies $a = 0$ or $b = 0$.

Being an integral domain is critical.

E..g. Solve $x^2 - 3x + 2 = 0$ over the integers;

Reduce to $(x - 2)(x - 1) = 0$.

Since \mathbb{Z} is an integral domain, $x - 2 = 0$ or $x - 1 = 0$.

Thus $x = 2$ or $x = 1$.

Examples of commutative rings that aren't domains

- Subsets of X with Δ and \cap
Additive identity is \emptyset ; $A \cap B = \emptyset$ does not imply that $A = \emptyset$ or $B = \emptyset$.

- Integers mod 6.

Question: for which n is \mathbb{Z}_n an integral domain?

Exploration:

$n = 2?$

$n = 3$

$n = 4?$

$n = 5$

$n = 6? \dots$

Characteristic

Given a commutative ring and integer n , we can define $n \cdot 1$ to be the sum of n 1's.

Two things can happen: either for every positive integer n , $n \cdot 1$ is nonzero or there is a positive integer n such that $n \cdot 1 = 0$. In former case, R contains $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$ which is a copy of the integers. (Example: $\mathbb{R}[x]$). Say R has characteristic 0.

In the latter, by WOP there is a smallest positive integer n with $n \cdot 1 = 0$. We call the smallest such n the characteristic of R .

Examples.

Integral domains

We claim n is prime? If not, $n = ab$ for some $1 < a, b < n$.
So $(a \cdot 1) = (b \cdot 1) = (ab) \cdot 1 = 0$. Since in integral domain,
either $a \cdot 1 = 0$ or $b \cdot 1 = 0$, contrary to the minimality of n .

Upshot: characteristic for integral domain is necessarily a prime.