

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.

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

If every prime divisor of a is less than p , then (since we are in a smaller case) $a|k$. But then $p(\frac{k}{a}) = b$, $p|b$.

Otherwise $a \geq p$.

If $p|a$ done.

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

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

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

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

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

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

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 integral domains

- The integers
- Rings of polynomials: $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$.
- Gaussian integers: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
- Extension rings. Fix d to be a non-square and $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ under usual addition and multiplication.

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.

Field of quotients

Given an integral domain D we can define a new object called the field of fractions of D .

The elements are all ordered pairs (p, q) where $p \in D$, $q \in D$ and $q \neq 0$.

We say (p, q) is equivalent to (p', q') provided $pq' = p'q$.

Can show: if (p, q) is equivalent to (p', q') and (r, s) is equivalent to (r', s') , then

$(ps + qr, qs)$ is equivalent to $(p's' + q'r', q's')$ and (pq, rs) is equivalent to $(p'q', r's')$

This gives us well-defined operations:

$$(p, q) + (r, s) = (ps + qr, qs)$$

$$(p, q) * (r, s) = (pr, qs)$$

In fact, this makes the field of quotients into a commutative ring (additive identity $(0, 1)$, multiplicative identity $(1, 1)$) in which every nonzero has a multiplicative inverse.

Examples:

Field of quotients of the integers is essentially the rationals

Field of quotients of the real polynomials is the rational functions