On Primes and Irreducibles: Aren't they the same?

Jake Fulford

Department of Mathematics
The University of Virginia

Directed Reading Program, Spring 2023

Motivation

- $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n} = \infty$, density of integers is 100% inside the integers.
- $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, density of squares is 0% inside the integers.
- Does $\displaystyle\sum_{p} \frac{1}{p}$ converge?
- We need unique factorization to answer this question.

Basic Number Theory

Question

How do we define factorization within the integers?

Definition (Divisibility)

a divides b, denoted $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = ac$.

Important Properties

- $a \mid b \implies |a| \leq |b|$
- $a \mid b$ and $a \mid c \implies a \mid bn + cm$ for all $n, m \in \mathbb{Z}$

Primes and Irreducibles

Definition (Prime)

$p \in \mathbb{Z}$ is prime if

$$p \mid ab \implies p \mid a \quad \text{or} \quad p \mid b.$$

Definition (Irreducible)

$p \in \mathbb{Z}$ is irreducible if

$$p = ab \implies a = \pm 1 \quad \text{or} \quad b = \pm 1.$$

Prime $\implies$ Irreducible

Claim

Every prime is irreducible.

Proof

- Suppose p is prime and $p = ab$.
- Then $p \mid ab$, by defintion, $p \mid a$ or $p \mid b$.
- WLOG, suppose $p \mid a$, then $a = pc$ for some $c \in \mathbb{Z}$.
- Then $p = ab = (pc)b = p(cb)$

$$\cancel{p} = \cancel{p}cb \implies 1 = cb$$

- Therefore $c = \pm 1$ and $b = \pm 1$, so p is irreducible. $\square$

Remark

This argument is valid for **any** integral domain, not just $\mathbb{Z}$.

Irreducible $\implies$ Prime?

Question

Are all irreducibles also prime?

Answer

Not always... for example, in $\mathbb{Z}[\sqrt{6}]$,

$$2 \text{ is irreducible} \quad \text{and} \quad 2 \mid 6 = \sqrt{6} \times \sqrt{6} \quad \text{but} \quad 2 \nmid \sqrt{6}$$

However

In $\mathbb{Z}$, yes! To prove this, we need:

1. Euclidean Division Algorithm
2. Greatest Common Divisor (GCD)
3. Euclid's Lemma

1. Division Algorithm

Claim

For any positive $a, b \in \mathbb{Z}$, there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < b.$$

Proof

- Let $S = \{a - qb \geq 0 \mid q \in \mathbb{Z}\}$.
- S is nonempty because $a - 0b \in S \subseteq \mathbb{N}$.
- By the **well-ordering principle**, S has a least element r.
- Then $r = a - qb$ for some $q \in \mathbb{Z}$, so $a = qb + r$
- Suppose $r \geq b$, then

  $$\min(S) = r > r - b = a - (q+1)b \in S \quad !!!$$

  Therefore $r < b$.
- Uniqueness follows from the condition $0 \leq r < b$. $\square$

2. Greatest Common Divisor

Definition

The **greatest common divisor** of $a, b \in \mathbb{Z}$ is the largest integer d such that $d \mid a$ and $d \mid b$.

Claim (Bezout's Identity)

$\gcd(m, n)$ is the minimum positive $\mathbb{Z}$-linear combination of m, n:

$$\gcd(m, n) = \min(\{am + bn > 0 \mid m, n \in \mathbb{Z}\}).$$

Proof (Sketch)

- Let $S = \{am + bn > 0 \mid m, n \in \mathbb{Z}\} \neq \emptyset$ (because $a^2 + b^2 \in S$).
- By the well-ordering principle, S has a least element d.
- $d \mid a$ and $d \mid b$ by **division algorithm** (use minimality of d).
- If $d' \mid a$, $d' \mid b$, then $d' \mid am + bn = d \implies d' \leq d$. $\square$

3. Euclid's Lemma

Defintion (coprime)

Two integers a, b are **coprime** if $\gcd(a, b) = 1$.

Remark

Irreducibles are coprime to all other integers.

Claim

$$\gcd(a, n) = 1 \quad \text{and} \quad n \mid ab \implies n \mid b$$

Proof

- By **Bezout's Identity**, $\exists m, k \in \mathbb{Z}$ such that $nm + ak = 1$.
- Then $b = bnm + abk = bnm + nk = n(bm + k)$.
- Thus $n \mid b$. $\square$

Finally: Irreducibles $\implies$ Prime

Proof

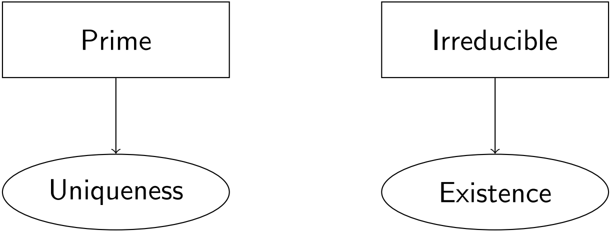
- Suppose p is irreducible and $p \mid ab$. WTS $p \mid a$ or $p \mid b$.
- To this end, suppose $p \nmid a$.
- Then p is coprime to a.
- Thus $p \mid b$ by Euclid's Lemma. $\square$

Why do we care that prime $\iff$ irreducible?

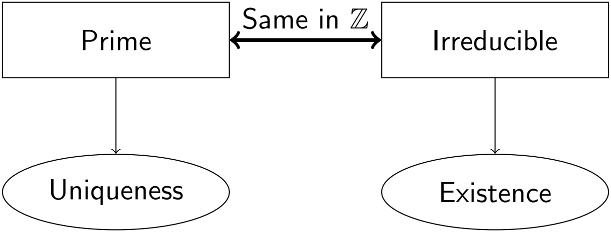
Prime

Irreducible

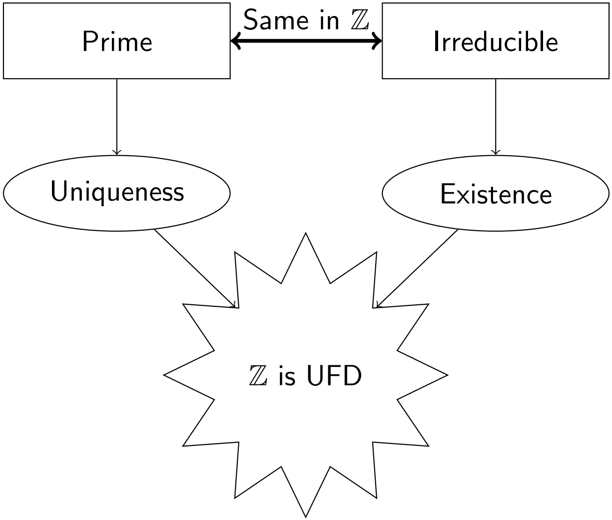
Why do we care that prime $\iff$ irreducible?



Why do we care that prime $\iff$ irreducible?



Why do we care that prime $\iff$ irreducible?



Existence of Irreducible Factorizations

Claim

Every integer has a factorization into irreducibles.

Proof (Contradiction)

- Suppose $S = \{\text{natural numbers without a factorization}\} \neq \emptyset$.
- By the well-ordering principle, set $n = \min(S)$.
- n is not irreducible, so n has some **nontrivial** factorization:

$$n = ab \text{ for some } a, b \in \mathbb{Z}.$$

- $a, b \notin S$ because $a, b < n$ and $n = \min(S)$.
- Thus $a = p_1 \dots p_s$ and $b = q_1 \dots q_t$ for irreducibles p_i, q_i.
- So $n = p_1 \dots p_s q_1 \dots q_t$ is a factorization of n. !!!
- Therefore n has a factorization into irreducibles. $\square$

Uniqueness of Prime Factorizations

Claim

If a prime factorization exists, then it is unique.

Proof

- Suppose $p_1 \dots p_s = q_1 \dots q_t$ are two prime factorizations of n.
- Then $p_1 \mid q_1 \dots q_t$.
- Then $p_1 \mid q_i$ for some i by definition of prime.
- WLOG: $i = 1$ (formally, we permute the indices).
- Then $p_1 = q_1$ because p_1 and q_1 are irreducible.
- Then $p_2 \dots p_s = q_2 \dots q_t$.
- Iterate to show that $s = t$ and $p_i = q_i$ for all i. $\square$

$\mathbb{Z}$ is a UFD

Definition (Unique Factorization Domain)

A **unique factorization domain** is an integral domain in which every nonzero element can be written as a product of primes, and this factorization is unique up to order and multiplication by units.

Theorem

$\mathbb{Z}$ is a UFD.

Proof

- $\mathbb{Z}$ is an integral domain.
- Factorization into irreducibles exists.
- Factorization into primes is unique.
- Irreducible $\iff$ prime.
- Therefore $\mathbb{Z}$ is a UFD. $\square$

The Series $\sum \frac{1}{p}$

Theorem

$\displaystyle\sum_{n=1}^{\infty} \frac{1}{n}$ converges if and only if $\displaystyle\sum_{p \text{ prime}} \frac{1}{p}$ converges, in particular,

$$\sum_{p} \frac{1}{p} = \infty.$$

Main Ingredient: The Euler Product

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p}}$$

Remark

This is a **formal** identity because of the LHS diverges.

The Euler Product

Proof Sketch

$$\prod_p \frac{1}{1-\frac{1}{p}} = \prod_p \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots\right) \quad \text{(Geometric Series)}$$

$$= \left(1 + \tfrac{1}{2} + \tfrac{1}{2^2} + \cdots\right)\left(1 + \tfrac{1}{3} + \tfrac{1}{3^2} + \cdots\right)\left(1 + \tfrac{1}{5} + \tfrac{1}{5^2} + \cdots\right)\cdots$$

We can construct any $\frac{1}{n}$ by multiplying out the product.
For example, $540 = 2^2 \times 3^3 \times 5$, which corresponds to

$$\tfrac{1}{540} = \left(1 + \tfrac{1}{2} + \tfrac{1}{2^2} + \cdots\right)\left(1 + \cdots + \tfrac{1}{3^3} + \cdots\right)\left(1 + \tfrac{1}{5} + \cdots\right)\left(1 + \tfrac{1}{7} + \cdots\right)\cdots$$

For every natural n, $\frac{1}{n}$ appears in the expanded product

- at least once by **existence**.
- at most once by **uniqueness**.

Thus, $\displaystyle\prod_p \frac{1}{1-\frac{1}{p}} = \sum_{n=1}^{\infty} \frac{1}{n}$. $\square$

$\sum \frac{1}{p} = \infty$

Proof of $\sum \frac{1}{p}$ divergence

- Apply logarithm to Euler Product

$$\log\left(\sum \frac{1}{n}\right) = \log\left(\prod_p \frac{1}{1-\frac{1}{p}}\right) = -\sum_p \log\left(1-\frac{1}{p}\right)$$

- Plug in Taylor series for $\log(1-x)$ for $|x| < 1$

$$\log\left(\sum \frac{1}{n}\right) = \sum_p \sum_{m=1}^{\infty} \frac{1}{m \times p^m} = \sum_{m=1}^{\infty} \sum_p \frac{1}{m \times p^m}$$

$$= \sum_p \frac{1}{p} + \sum_{m=2}^{\infty} \sum_p \frac{1}{m \times p^m}$$

We want to show that the red series is convergent.

$\sum \frac{1}{p} = \infty$

$$\sum_p \left(\sum_{m=2}^{\infty} \frac{1}{mp^m} \right) \leq \sum_p \left(\sum_{m=2}^{\infty} \frac{1}{p^m} \right) \qquad \text{because} \quad \frac{1}{mp^m} < \frac{1}{p^m}$$

$$= \sum_p \frac{\frac{1}{p^2}}{1 - \frac{1}{p}} \qquad \text{Geometric Series formula}$$

$$= \sum_p \frac{1}{p(p-1)}$$

$$\leq \sum_p \frac{1}{p^2} \qquad \text{because} \quad \frac{1}{p(p-1)} < \frac{1}{p^2}$$

$$\leq \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

Thus, $\log \left(\sum \frac{1}{n} \right) = \sum_p \frac{1}{p} + C.$ □

Thank you!