CMSC 250H - UPF, Primality in Domains, Relations

March 4, 2026

Last Lecture

Theorem

$\sqrt{7}$ is irrational

Proof.

We use unique factorization. Assume $\sqrt{7}$ is rational. Then, we can write

$$\sqrt{7} = \frac{a}{b} \implies 7b^2 = a^2$$

for coprime integers a and b. Let $p_1 p_2 \dots p_k$ be the prime factors of either a or b. That is:

$$a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$
$$b = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$$

Last Lecture

Theorem

$\sqrt{7}$ is irrational

Proof.

We substitute the prime factors in

$$7 \cdot (p_1^{b_1} p_2^{b_2} \dots p_k^{b_k})^2 = (p_1^{a_1} p_2^{a_2} \dots p_k^{a_k})^2 \implies$$

$$7 \cdot p_1^{2b_1} p_2^{2b_2} \dots p_k^{2b_k} = p_1^{2a_1} p_2^{2a_2} \dots p_k^{2a_k}$$

Let $p_i = 7$. Observe the exponent of p_i on the right hands side and left hand side:

$$2b_i + 1 \quad \text{and} \quad 2a_i$$

One is odd and one is even. This contradicts unique factorization. □

Last Lecture

Showing primality in $\mathbb{D} = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

Lemma

The norm of an element $x \in \mathbb{D}$ is never 2, that is

$$N(x) \neq 2$$

for all $x \in \mathbb{D}$

Proof.

We know $x = a + b\sqrt{-5}$ for $a, b \in \mathbb{Z}$. So

$$N(x) = a^2 + 5b^2$$

$N(x) \neq 2$

Proof.

Take the equation mod 5

$$a^2 + 5b^2 \pmod 5 \equiv a^2 \pmod 5$$

So we need $a^2 \equiv 2 \pmod 5$. Consider the squares mod 5. Then

$$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1$$

No square ever is 2! So $N(x)$ cannot never be 2. □

Back to Primality in $\mathbb{D}$

Theorem

2 is prime in $\mathbb{D}$

Proof.

If 2 is composite in D then we write $2 = xy$ for some $x, y \in \mathbb{D}$.
Taking the norm

$$N(2) = N(xy) = N(x)N(y)$$

Recall $N(2) = 2^2 + 0 \cdot 5 = 4$. So, either

1. $N(x)$ and $N(y)$ is 2 – not possible by Lemma
2. One of $N(x)$ and $N(y)$ is 1, the other is 4.

So it must be prime. □

Similar procedure for 3.

General Procedure

Goal

Prove a prime p in $\mathbb{N}$ is prime in $\mathbb{D}$

Idea

Write p as a factor of 2 elements

$$p = x \cdot y$$

with $x, y \in \mathbb{D}$. Since $x, y \in \mathbb{D}$, we have

$$x = a + b\sqrt{-5} \quad \text{and} \quad y = c + d\sqrt{-5}$$

for integers a, b, c, d.

General Procedure

Goal

Prove a prime p in $\mathbb{N}$ is prime in $\mathbb{D}$

Idea

Take the norm

$$N(p) = p^2 = N(x)N(y) = (a^2 + 5b^2)(c^2 + 5b^2)$$

Check $0 \leq a, b, c, d \leq p$ that satisfy the equation. Check to see if $a + b\sqrt{-5}$ is a unit. If there is a satisfying a, b, c, d such that this is not the case, then it is not prime.

Primes are Infinite

Proof.

Assume to the contrary that they are finite. Then we can order them $p_1, p_2, \ldots, p_k$. Consider the product, N, of all primes plus 1:

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$$

If N is prime, then we have just found a prime that was not in our previous list of all primes, a contradiction.
If N is composite, then it has a prime factor, say p_N. However, $p_N \neq p_i$ for all $1 \leq i \leq k$, since dividing N by any p_i results in a remainder of 1. So p_N must be a prime that is not on our list, a contradiction.
In either case, we show that the primes must be infinite. □

Relations

In math, there is an endless number of ways two entities can be related to each other

1. $6 \in \mathbb{Z}$
2. $6 < 10$
3. $X \subseteq Y$
4. $5 \equiv 1 \mod 2$
5. $3 \nmid 8$

We have a symbol in between two mathematical objects. This symbol is called a relation.

Relations

Definition

A relation $R \subseteq A \times A$. We often say $(x, y) \in R$ or use the notation xRy.

The elements of A are paired together in R if $x \sim y$ (x is related to y). An example: for $A = \{1, 2, 3, 4\}$ consider

$$R = \{(1,2), (1,3), (1,4), (1,5), (2,3), (2,4), (2,5), (3,4), (3,5), (4,5)\}$$

What mathematical relation does this set represent?

Properties of Relations

1. A relation is **reflexive** if xRx (or equivalently $(x, x) \in R$) for all $a \in A$
2. A relation is **symmetric** if xRy implies yRx for al $x, y \in A$
3. A relation is **transitive** if when xRy and yRz, then xRz for all $x, y, z \in A$

Equivalence Relations and Equivalence Classes

Definition

A relation R is an equivalence relation if it is reflexive, symmetric, and transitive.

Definition

Suppose R is an equivalence relation on a set A. Given an element $a \in A$, the equivalence class containing a is the subset

$$\{x \in A : xRa\}$$

of A consisting of all elements of A that relate to a. We sometimes denote it $[a]$

Example

Is $\geq$ an equivalence relation on $\mathbb{Z}$?

Example

Is $\geq$ an equivalence relation on $\mathbb{Z}$?

Answer: No, it is not symmetric since if $x \geq y$, it could be that $y \ngeq x$

Example

How about mod 5 on $\mathbb{Z}$?

Answer: Yes! The modular operation itself is an equivalence relation! We call the equivalence classes of modular arithmetic, **residue classes**, since they represent the remainder for integer division

Equivalence Classes

Theorem

Let R be an equivalence relation on the set A. Then, for elements $a, b \in A$, $[a] = [b]$ if and only if aRb.

Try proving it yourself! Remember this is a **bi-implication** so we need to prove both directions of the statement.

Equivalence Classes

Proof.

i) $[a] = [b] \implies aRb$

Since we know that $a \in [a]$ and $b \in [b]$, since $[a] = [b]$, then $a \in [b]$ and $b \in [b]$. So aRb, and bRa.

ii) $aRb \implies [a] = [b]$

Suppose $c \in [a]$. Then we know that cRa. Since aRb and R is an equivalence relation, by transitivity cRb. But, then that means every element $c \in [a]$ is contained in $[b]$. Hence, $[a] \subseteq [b]$. The same argument can be used to show $[b] \subseteq [a]$, establishing $[a] = [b]$ □

Partition

Definition

A partition of a set A is a set of subsets $\{A_i : A_i \subseteq A\}$ of A that union to form A, with each element being in one unique subset. That is

$$\bigcup_i A_i = A \quad \text{with} \quad A_i \cap A_j = \emptyset$$

for all $i < j$

Example: For $A = \{1, 2, 3, 4, 5\}$

$$A_1 = \{1\}, A_2 = \{4, 5\}, A_3 = \{2, 3\}$$

is partition of A of size 3.

Equivalence Classes and Partitions

Theorem

The equivalence classes of an equivalence relation, R, on a set A, form a partition of A.

Proof.

Exercise for you! Not too bad. Need to show two things:

1. $A = \bigcup_{a \in A} [a]$
2. For any $a \neq b$, $[a] \cap [b] = \emptyset$