MATH 145 NOTES
(FALL 2023 UNIVERSITY OF WATERLOO)

Ray Hang
Taught by Professor Jason P. Bell

December 13, 2023

Contents

Chapter 1

Proofs

Lecture 1: Introduction to MATH145 - Abstract Algebra

1.1 Introduction

Remark. A mathematical proof has two parts: “Discovery” and “Proving”.

Think of it generally as you lay your foundations and rough work in the discovery phase and then translate that work into a rigorous proof in the proving phase.

Definition 1.1 (Basic form of a proof)**.** A proof has a baseline form of “If p, then q”, where p and q are mathematical statements.

Note. Somewhat counterintuitively, we find that if p is always false then the statement “If p, then q” is always vacuously true.

Explanation. If p is never true then it does not matter what q is.

Example 1.1. A statement such as “If humans are fish, then dogs are cats” is always literally true as humans are not fish and thus it does not matter whether dogs are cats.

p	q	“If p, then q”
True	True	True
True	False	False
False	True	True
False	False	True

Table 1.1: Truth Table of Proofs

p	q	$p \wedge q$	$p \vee q$	"If p, then q"	$\neg p$	$\neg p \vee q$
True	True	True	True	True	False	True
True	False	True	False	False	False	False
False	True	True	False	True	True	True
False	False	False	False	True	True	True

Table 1.2: Truth Table of Various Statements

Example 1.2 (Proof Example 1: Parity). Here is an example of the processes of discovery and proving for the proof of the following theorem.

Theorem 1.1 (Parity). If $n \in \mathbb{Z}$ is even, then $n+1$ is odd.

Discovery: We see that p is "$n \in \mathbb{Z}$ is even" and q is "$n+1$ is odd".

We note the following definitions of odd and even integers:

Definition 1.2 (Even Integers). An integer n is even if and only if $\exists k \in \mathbb{Z}$ such that $n = 2 \cdot k$.

Definition 1.3 (Odd Integers). An integer n is odd if and only if $\exists k \in \mathbb{Z}$ such that $n = 2 \cdot k + 1$.

Now we start the proof.

Proof. (Parity) We assume that n is an even integer (this is our assumption of the hypothesis p).

By the definition of even integers that $\forall n$, $\exists k \in \mathbb{Z}$ such that $n = 2k$.

Thus, $n+1 = 2k+1$, which by the definition of odd integers is an odd integer, as desired. □

1.2 Proof by Contradiction

Example 1.3 (Proof Example 2: Irrationality of $\sqrt{2}$). Here is a second example, this time using a method called "proof by contradiction":

Theorem 1.2 (Irrationality of $\sqrt{2}$). $\sqrt{2}$ is irrational.

Definition 1.4 (Rationality). A number $\alpha \in \mathbb{R}$ is rational if $\alpha = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$. It is generally also accepted that a and b are coprime; that they have no common factors.

Corollary 1.1 (Irrationality). A number $\beta \in \mathbb{R}$ is irrational if it is not rational.

Proof. Assume that $\sqrt{2}$ is rational, i.e. that $\sqrt{2} = \frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$.

Thus,

$$\begin{aligned}
\sqrt{2} &= \frac{a}{b} \\
\Rightarrow 2 &= \frac{a^2}{b^2} \\
\Rightarrow 2b^2 &= a^2 \\
\Rightarrow a^2 &\text{ is even} \\
\Rightarrow 2b^2 &= (2k)^2, k \in \mathbb{Z} \\
\Rightarrow 2b^2 &= 4k^2 \\
\Rightarrow b^2 &= 2k^2 \\
\Rightarrow b^2 &\text{ is even}
\end{aligned}$$

Thus, both a and b are even, which is a contradiction as they are assumed to be coprime. Thus, by contradiction, $\sqrt{2}$ is irrational. □

Chapter 2

Rings

2.1 Axioms

Lecture 2: Axioms in $\mathbb{Z}$

Definition 2.1 (Additive Axioms). We define the addition axioms as follows:

A(i) Addition is commutative, that is, $\forall x, y \in \mathbb{Z}, x + y = y + x$

A(ii) Addition is associative, that is, $\forall x, y, z \in \mathbb{Z}, (x + y) + z = x + (y + z)$

A(iii) There exists an additive identity, that is, $\exists 0 \in \mathbb{Z}$ such that $\forall x \in \mathbb{Z}, (x + 0) = x$.

A(iv) There exists additive inverses, that is, $\forall x \in \mathbb{Z}, \exists - x \in \mathbb{Z}$ such that $x + (-x) = 0$

Theorem 2.1 (Cancelling). Let $x, y, z \in \mathbb{Z}$. Then $x + z = y + z \Rightarrow x = y$.

Proof. Let x, y, z be arbitrary numbers and assume $x + z = y + z$

Since $x + z = y + z$ we have $(x + z) + (-z) = (y + z) + (-z)$

By A(ii), we have $x + (z + (-z)) = y + (z + (-z))$

By A(iv), we have $x + 0 = y + 0$

By A(iii), we have $x = y$, as desired. □

Definition 2.2 (Multiplicative Axioms). We define the multiplication axioms as follows:

M(i) Multiplication is commutative, that is, $\forall x, y \in \mathbb{Z}, x \cdot y = y \cdot x$

M(ii) Multiplication is associative, that is, $\forall x, y, z \in \mathbb{Z}, (x \cdot y) \cdot z = x \cdot (y \cdot z)$

M(iii) There exists a multiplicative identity, that is, $\exists 1 \in \mathbb{Z}$ such that $\forall x \in \mathbb{Z}, (x \cdot 1) = x$

Definition 2.3 (Distributive Property). $\forall x, y, z \in \mathbb{Z}, (x + y) \cdot z = x \cdot z + y \cdot z \wedge z \cdot (x + y) = z \cdot x + z \cdot y$

Theorem 2.2 (Properties of 0). $\forall x \in \mathbb{Z}, x \cdot 0 = 0 \cdot x = 0$

Proof. By M(i), it is sufficient to prove that $0 \cdot x = 0 \ \forall x \in \mathbb{Z}$

Let x be an arbitrary integer.

Then,

$$\begin{aligned} 0 \cdot x &= (0+0) \cdot x && \text{A(iii)} \\ \Rightarrow 0 \cdot x &= 0 \cdot x + 0 \cdot x && \text{Distributive Property} \\ \Rightarrow 0 \cdot x + 0 &= 0 \cdot x + 0 \cdot x && \text{A(iii)} \end{aligned}$$

By cancelling $0 \cdot x$ from both sides, we obtain that $0 \cdot x = 0$, as desired. □

Theorem 2.3 (Parity of Negatives). $(-1) \cdot (-1) = 1$

Proof.

$$\begin{aligned} (-1) \cdot 0 &= 0 && \text{Theorem 2.2} \\ \Rightarrow (1 + (-1)) \cdot (-1) &= 0 && \text{A(iii)} \\ \Rightarrow 1 \cdot (-1) + (-1) \cdot (-1) &= 0 && \text{Distributive Property} \\ \Rightarrow (-1) + (-1) \cdot (-1) &= 0 && \text{M(iii)} \\ \Rightarrow 1 + (-1) + (-1) \cdot (-1) &= 1 && \text{Cancelling} \\ \Rightarrow 0 + (-1) \cdot (-1) &= 1 && \text{A(iv)} \\ \Rightarrow (-1) \cdot (-1) &= 1 && \text{A(iii)} \end{aligned}$$

□

Lecture 3: More about the axioms

Corollary 2.1. From the axioms, we can derive the following properties:

(i) $x \in \mathbb{Z} \wedge y + x = x + y = y \ \forall y \in \mathbb{Z} \Leftrightarrow x = 0$

(ii) $x \in \mathbb{Z} \wedge y \cdot x = x \cdot y = y \ \forall y \in \mathbb{Z} \Leftrightarrow x = 1$

(iii) $x, y, z \in \mathbb{Z} \wedge x + y = y + x = 0 \wedge x + z = z + x = 0 \Rightarrow y = z = -x$

Proof. ((i)) $y + x = y \Rightarrow y + x = y + 0 \Rightarrow x = 0$ via A(iii) □

Proof. ((ii)) WLOG, assume $y = 1$. Then $1 \cdot x = x \cdot 1 = 1 \Rightarrow x = 1$ via M(iii) □

Proof. ((iii)) $x + y = 0 = x + z \Rightarrow x + y = x + z \Rightarrow y = z$ by Cancelling. □

2.2 Introduction to Rings

Definition 2.4 (Rings). A ring R is a non-empty set with binary operations addition and multiplication such that the axioms A(i), A(ii), A(iii), A(iv), M(ii), M(iii), and the Distributive Property holds.

Corollary 2.2 (Commutative Rings). If a ring R is such that M(i) also holds, then it is known as a "Commutative Ring".

Lecture 4: Properties of Rings

Definition 2.5 (Units). Let R be a ring.

$r_1, r_2 \in R$ are units of $R \Leftrightarrow r_1 \cdot r_2 = r_2 \cdot r_1 = 1$

Definition 2.6 (Idempotents). Let R be a ring.

$r \in R$ is an idempotent in $R \Leftrightarrow r^2 = r$

Example 2.1. Idempotents and Units of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$

	Idempotents	Units
$\mathbb{Z}$	0, 1	-1, 1
$\mathbb{Q}$	0, 1	$\mathbb{Q} \setminus \{0\}$
$\mathbb{R}$	0, 1	$\mathbb{R} \setminus \{0\}$

Table 2.1: Idempotents and Units of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Example 2.2. Let $R = \mathbb{Z}^2$.

The units of R are: (1, 1), (1, -1), (-1, 1), (-1, -1)

The idempotents of R are: (1, 1), (0, 0), (1, 0), (0, 1)

Definition 2.7 (Integral Domains). A ring R is an integral domain if it is commutative and if

$$\forall r_1, r_2 \in R, r_1 \cdot r_2 = 0 \Rightarrow r_1 = 0 \lor r_2 = 0$$

Theorem 2.4 (Idempotents of Integral Domains). Let R be an integral domain. Then the only idempotents of R are 0 and 1.

2.3 Ordered Rings

Definition 2.8 (Order Axioms). We define the order axioms $<$ and $>$ in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ as follows:

O(i) $\forall x, y \in \mathbb{R}$, exactly one of $x < y, x = y, x > y$ is true.

O(ii) $\forall x, y, z \in \mathbb{R}, x > y \Rightarrow x + z > y + z$

O(iii) $\forall x, y, z \in \mathbb{R}, x > y \land z > 0 \Rightarrow x \cdot z > y \cdot z$

O(iv) $\forall x, y, z \in \mathbb{R}, x > y \land z < 0 \Rightarrow x \cdot z < y \cdot z$

O(v) $\forall x, y, z \in \mathbb{R}, x < y \land y < z \Rightarrow x < z$

Lecture 5: More about Order

Definition 2.9 (Ordered Rings)**.** A commutative ring R is ordered if all of the order axioms hold for elements within the ring.

Theorem 2.5 (Ordered Rings are Integral Domains)**.** An ordered ring R is an integral domain.

Proof. Suppose that $r_1, r_2 \in R \land r_1 \cdot r_2 = 0 \land r_1 \neq 0$. Assume WLOG that $r_1 > 0$.

If $r_2 > 0, r_1 \cdot r_2 > 0$. If $r_2 < 0, r_1 \cdot r_2 < 0$. Thus, by exhaustion, if $r_1 \cdot r_2 = 0 \land r_1 \neq 0, r_2 = 0$. □

2.4 Boolean Rings

Definition 2.10 (Boolean Ring)**.** If you have a boolean B in a ring $P(B)$:

(i) Addition: $\forall b_1, b_2 \in B, b_1 + b_2 = (b_1 \setminus b_2) \cup (b_2 \setminus b_1)$

(ii) Multiplication: $\forall b_1, b_2 \in B, b_1 \cdot b_2 = b_1 \cap b_2$

(iii) Additive Identity: $\varnothing$

(iv) Multiplicative identity: B

Question. Can a boolean ring be ordered?

Answer. Only if $|B| = 1$.

Proof. (Boolean rings are not ordered) We have the following facts:

(i) An ordered ring is an integral domain.

(ii) The only idempotents in an integral domain on $\mathbb{R}$ are 1 and 0

(iii) In a boolean ring, everything is an idempotent.

These □

Theorem 2.6 (Jacobson's Theorem of Commutativity)**.** A ring R is commutative if $\exists n \in \mathbb{Z} > 1$ such that $\forall r \in R, r^n = r$

Lecture 6: Induction and the Well-Ordering Principle

Definition 2.11 (Principle of Mathematical Induction)**.** Let $P(1), P(2), \ldots$ be mathematical statements.

If $P(1)$ is true and $\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1)$, then $P(n)$ is true $\forall n \in \mathbb{N}$.

Corollary 2.3 (Principle of Strong Mathematical Induction)**.** If $P(1)$ is true and $\forall k \in \mathbb{N}, P(i)$ is true $\forall i \in \{1, 2, \ldots, k\} \Rightarrow P(k+1)$ is true, then $P(n)$ is true $\forall n \in \mathbb{N}$.

Definition 2.12 (Well-ordered)**.** We say that a non-empty set S is well-ordered if every non-empty subset has a least element.

Definition 2.13 (Well-Ordering Principle). Every non-empty subset of the positive integers is well-ordered.

Exercise 2.1. Prove that the principle of mathematical induction implies the well-ordering principle and vice versa.

Lecture 7: Units

Definition 2.14 (R[[x]]). We define $R[[x]]$ with an integer domain R such that

$$R[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i, a \in R \right\}$$

$$\left(\sum a_i x^i\right) + \left(\sum b_i x^i\right) = \sum \left(a_i + b_i\right) x^i$$

$$\left(\sum a_i x^i\right) \cdot \left(\sum b_i x^i\right) = \sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_i \right) x^n$$

Theorem 2.7 (Idempotency of units). If $r \in R$ is a unit of R, then r^n is a unit $\forall n \in \mathbb{N}$.

Lemma 2.1 (Unit multiplication). If $r_1, r_2 \in R$ are units of R, then $r_1 \cdot r_2$ is also a unit of R.

Definition 2.15 (Pell's Equation).

$$x^2 - 2y^2 = \pm 1$$

Example 2.3 (Using Pell's Equation). We begin with a lemma.

Lemma 2.2. $a + b\sqrt{2}$ is a unit of $\mathbb{Z}[2] \Leftrightarrow a^2 - 2b^2 = \pm 1$

Proof. ($\Rightarrow$) Suppose $a + b\sqrt{2}$ is a unit. Then, there exists c, d such that $(a + b\sqrt{2})(c + d\sqrt{2}) = 1$.

Do some expansion and simplification magic, and you obtain $ac + 2bd) + \sqrt{2}(ad + bc) = 1 + 0\sqrt{2}$

Thus, $ac + 2bd = 1, ad + bc = 0$

Additionally, as $(a - b\sqrt{2})(c - d\sqrt{2}) = ac + 2bd - \sqrt{2}(ad + bc) = 1$, we get

$$\begin{aligned}(a + b\sqrt{2})(c + d\sqrt{2})(a - b\sqrt{2})(c - d\sqrt{2}) = 1 \\ \Rightarrow (a^2 - 2b^2)(c^2 - 2d^2) = 1 \\ \Rightarrow a^2 - 2b^2 = \pm 1, c^2 - 2d^2 = \pm 1\end{aligned}$$

As desired. □

Proof. ($\Leftarrow$) If $a^2 - 2b^2 = \pm 1$, then $(a + \sqrt{2}b)(a - \sqrt{2}b) = \pm 1 \Rightarrow a + b\sqrt{2}$ is a unit. □

Theorem 2.8 (Units of $\mathbb{Z}[\sqrt{2}]$)**.** All units of $\mathbb{Z}[\sqrt{2}]$ are of the set $\{\pm(\sqrt{2}+1)^j : j \in \mathbb{Z}\}$

Lemma 2.3. Let u be a unit of $\mathbb{Z}[\sqrt{2}]$ and suppose that $1 \leq u \leq \sqrt{2}+1$. Then $u = 1$, or $u = \sqrt{2}+1$.

Proof. Let $u = a + b\sqrt{2} \Rightarrow a^2 - 2b^2 = \pm 1 \Rightarrow u^{-1} = a - b\sqrt{2}, u^{-1} = -a + b\sqrt{2}$.

$(\sqrt{2}+1)^{-1} \leq u \leq 1 \Rightarrow 1 \leq a + b\sqrt{2} \leq \sqrt{2}+1 \Rightarrow \sqrt{2} \leq u + u^{-1} \leq \sqrt{2}+2$

Case 1: $u = a + b\sqrt{2}, u^{-1} = a - b\sqrt{2}$

$1 < \sqrt{2} \leq 2a \leq 2 + 2\sqrt{2} < 4 \Rightarrow a = 1 \Rightarrow b = 0 \Rightarrow u = 1$

Case 2: $u = a + b\sqrt{2}, u^{-1} = -a + b\sqrt{2}$

$\sqrt{2} \leq 2b\sqrt{2} \leq 2 + \sqrt{2} \Rightarrow \frac{1}{2} \leq b \leq \frac{1}{\sqrt{2}+\frac{1}{2}} \Rightarrow b = 1 \Rightarrow a = \pm 1 \Rightarrow u = \sqrt{2}+1$ □

Proof. (Theorem 2.8) If u is a unit of $\mathbb{Z}[\sqrt{2}] \wedge u \geq 1 \Rightarrow u = (\sqrt{2}+1)^j, j \geq 1$

Let $S = \{j \in \mathbb{N} : (\sqrt{2}+1)^j > u\}$

By Well-Ordering Principle, there exists a smallest $k \in S$ such that $(\sqrt{2}+1)^{k-1} \leq u \leq (\sqrt{2}+1)^k \Rightarrow 1 \leq u(\sqrt{2}-1)^{k-1} < \sqrt{2}+1 \Rightarrow 1 \leq u \leq \sqrt{2}+1$

By Lemma 2.3, $u = 1 \Rightarrow u = (\sqrt{2}+1)^{k-1}$

To finish this proof, let u be a unit of $\mathbb{Z}[\sqrt{2}]$.

If $u \geq 1$ then $u = (\sqrt{2}+1)^j, j \geq 0$

If $0 < u < 1$ then $u^{-1} > 1 \Rightarrow u^{-1} = (\sqrt{2}+1)^j \Rightarrow u = (\sqrt{2}+1)^{-j}$

If $u < 0 \Rightarrow -u > 0 \Rightarrow -u = (\sqrt{2}+1)^j$

Thus, every unit is in $\{\pm(\sqrt{2}+1)^j : j \in \mathbb{Z}\}$ and thus everything in the set is a unit. □

Lecture 8: Pascal's Triangle

Theorem 2.9 (Binomial Coefficients)**.** $\binom{n}{k}$ is the number of ways of selecting k element subsets from a set of size n.

Proof. We assume WLOG that our n element set is the set $\{1, 2, \ldots, n\}$.

Note that if we want to select k elements from this set, we have n ways to select the first element.

After this, we have $n-1$ ways of selecting the next element. In total, we thus have $n(n-1)(n-2)\cdots(n-k+1)$ ways of selecting k distinct elements from the set.

Notice that if $i_1 < \cdots < i_k$ are k elements of the set, we have $k!$ ways of rearranging these elements.

Thus, each set of size k is counted $k!$ times, and thus we have $\frac{n(n-1)\cdots(n-k+1)}{k!}$ ways of selecting our set of k elements from the superset.

With some fiddling around, we see that this is equivalent to $\frac{n!}{(n-k)!k!}$, as desired. □

Theorem 2.10 (Pascal's Identity)**.** $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

Proof. Proof is trivial by simply using the formula for the choose function. □

Chapter 3

Primes and Factorization

3.1 Primes

Lecture 9: Infinitude of Primes

Theorem 3.1 (Units of $\mathbb{Z}$)**.** The only units of $\mathbb{Z}$ are ± 1.

Proof. Since $1 \cdot 1 = -1 \cdot -1 = 1$, we see that they are units of $\mathbb{Z}$

Conversely, if z is a unit of $\mathbb{Z}$, then $znew0$.

Observer that $-z$ is a unit.

Assume WLOG that $z > 0 \Rightarrow z \geq 1$.

By assumption, $\exists x \in \mathbb{Z}$ such that $x \cdot z = 1$

$z \geq 1 \Rightarrow x \geq 1$.

If $z \neq 1, z \geq 2 \Rightarrow x \cdot z \geq x \cdot 2 \geq 1 \cdot 2 = 2$, but $x \cdot z = 1$, leading to a contradiction.

Thus, the only units of $\mathbb{Z}$ are ± 1, as desired. □

Notation. Given $z_1, z_2 \in \mathbb{Z}$, we write $z_1 \mid z_2 \Leftrightarrow \ \exists k \in \mathbb{Z}$ such that $z_2 = k \cdot z_1$.

Or, in simpler terms, the first number divide second number WOOO

Definition 3.1 (Prime Numbers)**.** We say that a number $p \in \mathbb{Z}$ is a prime number if it is not a unit and if $\forall z \in \mathbb{Z}, z \mid p \Rightarrow z = \pm 1 \vee z = \pm p$.

Lemma 3.1 (At least one prime factor)**.** Let $n > 1$ be a positive integer. Then, n has at least one prime factor.

Proof. Suppose that this is not true.

Let $S = \{n \in \mathbb{N} : n > 1\}$ and the lemma does not hold on n.

By assumption, $S \neq \varnothing$.

By the Well-Ordering Principle, there exists a smallest element $m \in S$.

m cannot be prime by definition, and thus $m = ab, a, b > 0, a, b \neq 1, m > a, b$

Notice that $a < m$ and thus $a \notin S$.

Thus, a has a prime factor p.

However, $m = a \cdot b = kpb$ and thus m has a prime factor p which is a contradiction. □

Theorem 3.2 (Euclid's Theorem)**.** There are infinitely many prime numbers.

Proof. Suppose that this is false. This is, there are primes $p_1, \ldots, p_k$ for some finite number k.

Let $M = p_1 \cdots p_k + 1$. By Lemma 3.1, M has at least one prime factor $p > 1$ such that $p \mid M$.

However, the only primes are in the set $\{p_1, \ldots, p_k\}$.

Therefore, $p \in \{p_1, \ldots, p_k\}$.

Thus, $p \mid p_1 \cdots p_k$.

Thus, $p \mid M - p_1 \cdots p_k \Rightarrow p \mid 1 \Rightarrow p$ is a unit and thus not prime, and thus we obtain a contradiction. □

Corollary 3.1. We can apply the same logic to primes of the form $4k + 3$.

3.2 Euclidean Algorithm

Definition 3.2 (Common Divisor)**.** Given $a, b \in \mathbb{N}$, we say that $d \in \mathbb{N}$ is a common divisor of a and b if $d \mid a$ and $d \mid b$.

Lecture 10: Euclidean Algorithm

Definition 3.3 (Base Euclidean Algorithm)**.** For two positive integers a, b, this lets us compute an integer $d = \gcd(a, b)$.

WLOG, let $a \geq b$. Then, there exists $q \in \mathbb{N}, r \in \{0, 1, \ldots, b-1\}$ such that $a = bq + r$.

Repeat this process with $(a, b) \rightarrow (b, r)$ until $r = 0$. Then, $q = b$

Lecture 11: Extended Euclidean Algorithm

Example 3.1. $a = 92,\ b = 21$:

Input: $a, b \in \mathbb{N}$ such that $a > b$

Output: $d \in \mathbb{N},\ d \in \mathbb{N}$

$d = \gcd(a, b) \land d = as + bt$

Step 1: Let $a_1 = a, s_1 = 1, t_1 = 0 \Rightarrow p_1 = (a_1, s_1, t_1)$

$a_2 = b, s_2 = 0, t_2 = 1 \Rightarrow p_2 = (a_2, s_2, t_2)$

Step 2: Use the division algorithm to write $a_1 = q_2 a_2 + r_2, r_2 \in \{0, \ldots, a_2 - 1\}$

If $r_2 = 0$ stop and output $(d, s, t) = (a_2, s_2, t_2)$

Otherwise, let $a_3 = r_2 = a_1 - q_2 a_2, let s_2 = s_1 - q_2 s_2, t_2 = t_1 - q_2 t_2$

and let $p_3 = (a_3, s_3, t_3)$ and go to Step 3.

Step 3: Write $a_2 = q_3 a_3 + r_3$ with $r_3 \in \{0, \ldots, a_3 - 1\}$

If $r_3 = 0$, stop and output $(d, s, t) = (a_3, s_3, t_3)$

Otherwise, let

$$
\begin{aligned}
a_4 = a_2 - q_3 a_3 = r_3, \qquad & (3.1)\\
s_4 = s_2 - q_3 s_3, \qquad & (3.2)\\
t_4 = t_2 - q_3 t_3 \qquad & (3.3)
\end{aligned}
$$

Step 4: Write $a_3 = q_4 a_4 + r_4, r_4 \in \{0, 1, \ldots, a_x - 1\}$

If $r_4 = 0$, stop and output $(d, s, t) = (a_4, s_4, t_4)$

Otherwise, let $a_5 = a_3 - q_4 a_4, s_5 = s_3 - q_4 s_4, t_5 = t_3 - q_4 t_4$

In general, for step *i*: Write $a_{i-1} = q_i a_i + r_i, r_i \in \{0, \ldots, a_{i-1}\}$

If $r_i = 0$, stop and output $(d, s, t) = (a_i, s_i, t_i)$.

Otherwise, let $a_{i+1} = a_{i-1} - q_i a_i, s_{i+1} = s_{i-1} - q_i s_i, t_{i+1} = t_{i-1} - q_i t_i$ and $p_{i+1} = (a_{i+1}, s_{i+1}, t_{i+1},)$

Thus, we see in the example given:

p_1	92	1	0
p_2	21	0	1
p_3	8	1	-4
p_4	5	-2	9
p_5	3	3	-13
	2	-5	22
	1	8	-35

Lemma 3.2 (Termination of the Algorithm). $\forall i \geq 1$, if $a_i \neq 0$, then $a_i > a_{i+1}$

Proof. Notice $a_1 = a, a_2 = b \wedge a > b$ by assumption, so the claim is true when $i = 1$.

Now suppose the claim holds for some $i = 1, \ldots, k-1$ with $k \geq 2$ and suppose that $a_k \neq 0$.

Then $a_{k+1} = a_{k-1} - q_k a_k = r_k$, where $r_k \in \{0, \ldots, a_{k-1}\}$ is the remainder when we divide a_k into a_{k-1}.

So $a_{k+1} = r_k < a_k$. So the claim holds when $i = k$ and thus by induction the result follows. □

Corollary 3.2. EEA Terminates

Proof. Let $S = \{a_i : a_i \neq 0\}$

Notice $a_1 = a \wedge a_2 = b$ are in S so $S \neq \emptyset$

By the WOP $\exists$ a smallest element of $S = a_M$

Notice $a_m > a_{m+1}$ by Lemma 11.1, and thus by minimality of $a_m, a_{m+1} \notin S$

So $a_{m+1} = 0 \Rightarrow$ the algorithm terminates. □

Lemma 3.3 (GCD equivalence)**.** $\forall i \geq 1$ such that $a_i \neq 0$, $\gcd(a_i, a_{i+1}) = \gcd(a, b)$

Proof. Base Case: $i = 1, \gcd(a_1, a_2) = \gcd(a, b)$

Now suppose that the claim is true for $i = 1, \ldots, k-1$ with $k \geq 2 \wedge a_k \neq 0$.

Then $a_{k+1} = a_{k-1} - q_k a_k = r_k$

So $\gcd(a_{k-1, a_k}) = \gcd(a_k, a_{k+1})$ by Lemma 11.1

But by the inductive hypothesis, $\gcd(a_{k-1}, a_k) = \gcd(a, b)$, so $\gcd(a_k, a_{k+1}) = \gcd(a, b)$, as desired. □

Corollary 3.3. If EEA outputs (d, s, t), then $d = \gcd(a, b)$

Proof. Since (d, s, t) is the output, $\exists m \geq 1$ such that $d = a_m, s = s_m, t = t_m \wedge a_{m+1} = 0$.

But by Lemma **??**, $\gcd(a, b) = \gcd(a_m, a_{m+1}) = \gcd(d, 0) = d$ □

Lemma 3.4 (d = sa + tb)**.** For $i \geq 1$, if $a_i \neq 0$ then $a_i = s_i a + t_i b$

Proof. Base Cases: $i = 1 \Rightarrow a_1 = a, s_1 = 1, t_1 = 0 \wedge i = 2 \Rightarrow a_2 = b, s_2 = 0, t_2 = 1$ Now suppose that the claim holds for $i = 1, \ldots, k, k \geq 2$ and consider $i = k+1$

Then, $a_{k+1} = (a_{k-1} - q_k a_k) = (s_{k-1} a + t_{k-1} b) - q_k (s_k a + t_k b)$ by the inductive hypothesis

$= a(a_{k-1} - q_k s_k) + b(t_{k-1} - t_k q_k) = a s_{k+1} + b t_{k+1}$ and the result follows by induction. □

Corollary 3.4. $d = sa + tb$

Proof. EEA says that $\exists m$ such that $(d, s, t) = (a_m, s_m, t_m)$. By Lemma **??**, $a_m = s_m a + t_m b \Rightarrow d = sa + tb$ □

Corollary 3.5. Let p be prime. If $p \mid ab, a, b \in \mathbb{N}$, then $p \mid a \vee p \mid b$

Proof. We'll prove the contrapositive: If a and $p \nmid b$ then $p \nmid ab$.

If $p \nmid a \Rightarrow \gcd(a, p) = 1$ and $p \nmid b \Rightarrow \gcd(b, p) = 1$.

By the EEA, $\exists$ such that $1 = pst$ at and $\exists x, y$ such that $1 = px + by \Rightarrow 1 = (ps + at)(px + by) = p^2 sx + psby + pxat + abxy = p(sxp + sby + xat) + ab(xy) \Rightarrow \exists m, n$ such that $1 = pm + abn$. □

Lecture 12: Euclid's Algorithm Extended Pt. 2

3.3 Euclid's Lemma

Lemma 3.5 (Euclid's Lemma Defined)**.** If p is prime and $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

Proof. By contrapositive, suppose that $p \nmid a \wedge p \nmid b$,

Then $\gcd(p, a) = \gcd(p, b) = 1 \because p$ is prime.

Thus, by EEA, $\exists s, t \in \mathbb{Z}$ such that $ps + at = 1$

and $\exists x, y \in \mathbb{Z}$ such that $px + by = 1$

Multiplying those two equations gives $(ps + at)(px + by) = 1 \Rightarrow p^2sx + psby + pxat + abty = 1$

$\Rightarrow p(psx + sby + xat) + (ab)(ty) = 1$

This means that if $d \mid p \wedge d \mid ab \Rightarrow d \mid p(psx + sby + xat) + ab(ty) \Rightarrow p \mid 1$

Thus, the gcd of p and ab must be $1 \Rightarrow p \nmid ab$.

The result thus follows by taking the contrapositive: $p \mid ab \Rightarrow p \mid$ or $p \mid b$. □

Note. For the ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

Then, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

Corollary 3.6. Of Euclid's Lemma: let p be prime. If $p \mid a_1 \cdots a_n \wedge n \in \mathbb{N} \Rightarrow \ \exists i \in \{1, \dots, n\}$ such that $p \mid a_i$.

Proof. Induction on n.

When $n = 1$, the claim is immediate.

So now let $k \geq 2$ and assume that the claim holds for $n < k$.

Now consider the case when $n = k$.

So, $p \mid a_1 \cdots a_k$

Let $a = (a_1 \cdots a_{k-1})$ and $b = a_k$

So $p \mid ab$ and thus by Euclid's Lemma $p \mid a$ or $p \mid b$.

If $p \mid b$ then $p \mid a_k$ so we can take $i = k$, and we're done.

On the other hand, if $p \mid a \Rightarrow p \mid a_1 a_2 \cdots a_{k-1}$

and so by the inductive hypothesis, $\ \exists i \in \{1, \dots, k-1\}$ such that $p \mid a_i$

Hence, the claim holds in both cases, so the result follows by induction. □

3.4 Unique Factorization

Theorem 3.3 (Fundamental Theorem of Arithmetic). Let $n \geq 2$ be a natural number.

(i) n has a factorization into primes.

(ii) This factorization is unique; i.e., if $n = p_1 \cdots p_s = q_1 \cdots q_k$ where $p_1, \dots, q_k$ are primes, then $s = t \wedge q_1, \dots, q_k$ is a rearrangement of $p_1, \dots p_s$.

We first show that every $n \in \mathbb{N}$ has at least one factorization into primes. To do this, let $S = \{n \in \mathbb{N} : n \geq 2 \wedge n$ does not have a factorization into primes.$\}$

Proof. Proof of *(i)*.

If $S = \varnothing$, then *(i)* is true, so we may assume towards a contradiction that $S \neq \varnothing$.

Then, S has a smallest element due to the WOP.

Let m denote this smallest element. Notice that m cannot be prime.

Thus, $m = ab$ with $1 < a, b < m$ for some $a, b \in \mathbb{N}$.

Since $2 \leq a, b, m$, we know that $a, b \notin S$ and so we have $a = p_1 \cdots p_s, b = q_1 \cdots q_k$ for some primes p_i, q_j.

But now $m = ab = p_1 \cdots p_s q_1 \cdots q_k$ so m factors into primes, which is a contradiction $\Rightarrow S = \varnothing$ and i is true. □

Proof. We let $P(n)$: n has a unique prime factorization be the proposition.

Base Case: $P(1) : 2$ is a trivial case.

Inductive Hypothesis: We assume, for some arbitrary $k \in \mathbb{N}$ strictly greater than 2, that $P(i)$ is true $\forall i \in \{1, 2, \ldots, k-1\}$.

Inductive Step:

Suppose that $k = p_1 \cdots p_s = q_1 \cdots q_k$ is two factorizations of k into primes.

Notice that $k = p_1(p_2 \cdots p_s)$ So $p_1 \mid k \because k = q_1 \cdots q_t \Rightarrow p_1 \mid q_1 \cdots q_t$.

So, by the EEA, $\exists i$ such that $p_1 \mid q_i$ and since p_1 and q_i are primes, this gives that $q_i = p_1$.

After reindexing, we may assume that $i = 1$ and $p_1 = q_1$.

So now $k = p_1(p_2 \cdots p_s) = q_1(q_2 \cdots q_k) = p_1(p_2 \cdots q_k)$.

Because $\mathbb{Z}$ is an integral domain, this means that $m = p_2 \cdots p_s = q_2 \cdots q_k$.

Notice that $m = \frac{k}{p_1} < k$.

By the inductive hypothesis, m factors into primes uniquely, so $s - 1 = t - 1 \Rightarrow s = t$ and $p_2, \cdots, p_s$ is a rearrangement of $q_2, \cdots, q_t \Rightarrow s = t \wedge p_1, \cdots, p_s$ is a rearrangement of $q_1, \cdots q_t \because q_1 = p_1$ and thus the results follows by induction. □

Lemma 3.6 (Extension of Euclid's Lemma). If p is prime and $1 \leq k < p$, then $p \nmid k!$

Proof. If $p \mid k! \Rightarrow p \mid 1 \cdot 2 \cdots k \Rightarrow \exists i \in \{1, \ldots, k\}$ such that $p \mid i$ and this is impossible $\because 0 < i < p$. □

Note. $p \mid \binom{p}{k}, k = 1, 2, \ldots, p-1 \because p \mid p!$ and $\frac{p!}{k!(p-k)!} = \binom{p}{k} \Rightarrow p \mid k!(p-k)!\binom{p}{k} \Rightarrow p \mid \binom{p}{k}$.

Lecture 13: Fundamental Theorem of Arithmetic

Definition 3.4 (The Fundamental Theorem of Arithmetic). $n \geq 2$.

If $p_1, \ldots, p_k$ are all the primes that divide n, $\exists i_1, \ldots, i_k \in \mathbb{N}$

such that $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k} \wedge i_1, \ldots, i_k$ are uniquely determined.

Example 3.2. $n = 120 = 2^3 3^1 5^1$

Proposition 3.1. Let $D = \{d \in \mathbb{N} : d \mid n\}$ ("the set of divisors of n")

If $n = p_q^{i_1} \cdots p_k^{i_k}$ then $D(n) = \{p_i^{j_k} \cdots p_k^{j_k} : 0 \leq j_1 \leq i_1, \ldots, 0 \leq j_k \leq i_k\}$

Proof. If $d = p_1^{j_1} \cdots p_k^{j_k}$ with $0 \leq j_1 \leq i_1, \ldots, 0 \leq j_k \leq i_k$ then $n = d(p_1^{i_1 - k_1} \cdots p_k^{i_k - j_k})$ and so $d \in D(n)$.

So, $\{p_i^{j_i} \cdots p_k^{j_k} : 0 \leq j_1 \leq i_1, \ldots, 0 \leq j_k \leq i_k\} \subseteq D(n)$

Next, we'll show the reverse containment.

Let $d \in D(n)$. Then $\exists a \in \mathbb{N}$ such that $d \cdot a = n$

By the FTA, we can write that $d = q_1^{s_1} \cdots q_r^{s_r}, a = l_1^{t_1} \cdots l_m^{t_m}$ and thus $n = d \cdot a = q_1^{s_1} \cdots q_r^{s_r} l_1^{t_1} \cdots l_m^{t_m}$, where q, l are primes.

Example: $120 = 4 \cdot 30 = (2^2) \cdot (2^1 3^1 5^1)$

Since $n = p_1^{i_1} \cdots p_k^{i_k} = q_1^{s_1} \cdots q_r^{s_r} l_1^{t_1} \cdots l_m^{t_m}$, by unique factorization, we have a factor $q_i^{s_i}, i \geq 1$ and $l_i^{t_i}$.

So all of the prime factors of d and a are from $\{p_1, \ldots p_k\}$ so $d = p_q^{j_1} \cdots p_k^{j_k}$ and $a = p_1^{u_1} \cdots p_k^{u_k}$

And thus by the FTA, $i_1 = j_1 + u_1, \ldots, i_k = j_k + u_k$.

Since $u_1, \ldots, u_k \geq 0 \wedge j_1, \ldots, j_k \geq 0$, we see that $0 \leq j_1 \leq i_1, \ldots, 0 \leq j_k \leq i_k$ and so $d = p_1^{j_1} \cdots p_k^{j_k}$.

Thus, $D(n) \subseteq \{p_1^{j_1} \cdots p_k^{j_k} : 0 \leq j_1 \leq i_1, \ldots, 0 \leq j_k \leq i_k\}$ and the result follows. □

Definition 3.5 (GCD Formula). Let $p_1, \ldots, p_k$ be pairwise distinct primes and suppose that $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, b = p_1^{\beta_1} \cdots p_k^{\beta_k}$

Example: $a = 120 = 2^3 3^1 5^1, b = 140 = 2^2 5^1 7^1$

Thus, $\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)}$

Proof. $p^{\min(\alpha_i, \beta_i)} \mid p^{\alpha_i}, p^{\beta_i}, \because \min(\alpha_i, \beta_i) \leq \alpha_i, \beta_i$

Thus, it is a common divisor of a and b.

On the other hand, we showed that if $d \mid a$, then $d = p_1^{j_1} \cdots p_k^{j_k} \Rightarrow 0 \leq j_k \leq \alpha_k$

Similarly, if $d \mid b$, then $0 \leq j_k \leq \beta_k$.

Thus, if $d \mid a \wedge d \mid b \Rightarrow 0 \leq j_1 \leq \min(\alpha_1, \beta_1), \ldots$

Thus, any other divisor would be less than $p_1^{\min(\alpha_1, \beta_1)} \cdots p_k^{\min(\alpha_k, \beta_k)}$, and thus, it must be the GCD. □

Chapter 4

Equivalence Relations

4.1 Introduction

Definition 4.1 (Equivalence)**.** We'll say that a relation $\sim$ on X, a set, is an equivalence relation if the following holds:

(i) $\forall x \in X, x \sim x$ (reflexivity)

(ii) $\forall x, y \in X$, if $x \sim y$ then $y \sim x$ (symmetry)

(iii) $\forall x, y, z \in X$, if $x \sim y \wedge y \sim z$, then $x \sim z$ (transitivity)

Example 4.1. Let $m \in \mathbb{N}, m \geq 2$.

We put an equivalence relation $\sim$ on $\mathbb{Z}$ where $x \sim y$ if $x - y$ is a multiple of m.

$m = 4 \Rightarrow 1 \sim 5, 2 \sim 10, 17 \sim -3, 1 \nsim 4$

Is this reflexive? $x - x = 0 = 0 \cdot m \rightarrow$ yes.

Is this symmetric? $x \sim y \Leftrightarrow m \mid (x - y) \Leftrightarrow m \mid (y - x) \Leftrightarrow y \sim x$

Is this transitive? $x \sim y \wedge y \sim z \Rightarrow \ \exists a, b$ such that $y - x = ma \wedge z - y = mb \Rightarrow z - x = m(a + b)$

Note. Notation: We write $x \equiv y \pmod m$ if $x - y$ is a multiple of m.

Given $a \in \mathbb{Z}$, we let $[a]_m = \{b \in \mathbb{Z} : b \equiv a \pmod m\}$, this is called the equivalence class of $a \pmod m$.

Theorem 4.1 (Fermat's Little Theorem)**.** Let p be prime and let $a \in \mathbb{Z}$. Then,

$$a^p \equiv a \pmod p$$

Example 4.2. $p = 2 : a^2 - a = a(a - 1) = a \pmod 2$

$p = 5 : p$ prime $\Rightarrow p \mid \binom{p}{k}$ for $1 \leq k \leq p - 1$

Why? $\rightarrow \binom{p}{k} k!(p - k)! = p!$

Proof. Notice it suffices to prove that $a^p \equiv a \pmod p$ for $a \in \mathbb{N}$.

We prove this by induction on a. The base case is when $a = 1 \Rightarrow 1^p = 1 \equiv 1 \pmod p$.

Now suppose that the claim holds for an arbitrary $n \geq 1$ and consider the case $n+1$.

Then $(n+1)^p = \binom{p}{0}n^p + \cdots + \binom{p}{p}1 = \binom{p}{0}n^p + p \cdot s + \binom{p}{p}1, s \in \mathbb{Z}$

$= n^p + 1 + p \cdot s \equiv n^p + 1 \pmod p \equiv n + 1 \pmod p$ by the inductive hypothesis. The result follows. □

Lecture 14: Binary Relations

Definition 4.2 (Introduction). A binary relation R on a set S is a subset of $S \times S$

We write sRt if $(s,t) \in R \subseteq S \times T$

We write $\neg xRy$ if $(x, y \notin R)$, thus $x \not\leq y$

Definition 4.3 (Binary Rotation). A binary rotation $\sim$ on X is an equivalence relation if it is

(i) reflexive: $x \sim x \; \forall x$

(ii) symmetric: $x \sim y \Rightarrow y \sim x \; \forall x, y \in X$

(iii) transitive: $x \sim y \wedge y \sim z \Rightarrow x \sim z \; \forall x, y, z \in X$

Example 4.3. If $m \geq 2$ is an integer, we have an equivalence relation $\sim$ on $\mathbb{Z}$

$x \sim y \Leftrightarrow m \mid (x - y)$

We thus write that $x \equiv y \pmod m$

Lemma 4.1. Let $m \geq 2$

If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are integers and $a_i \equiv b_i \pmod m$ for $i = 1, \ldots, m$,

then $a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod m$ and $a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod m$

Proof. We prove this by induction on n

When $n = 1$, the claim is immediately true.

Now suppose the claim holds when $n < k$ for some $k \geq 2$.

We consider the case when $n = k$

Then, $a_1 + a_2 + \cdots + a_{k-1} \equiv b_1 + \cdots + b_{k-1} \pmod m$ and $a_1 \cdots a_{k-1} \equiv b_1 \cdots b_{k-1}$ by the inductive hypothesis.

Thus, $a_1 + \ldots a_{k-1} - (b_1 + \cdots + b_{k-1}) = mc, c \in \mathbb{Z}$ and $a_1 \cdots a_{k-1} - b_1 \cdots b_{k-1} = md, d \in \mathbb{Z}$

By assumption, $a_k - b_k = me, e \in \mathbb{N}$

Thus, $a_1 + \cdots + a_k = (a_1 + \cdots + a_{k-1}) + a_k = b_1 + \cdots + b_{k-1} + mc + a_k$

$= b_1 + \cdots + b_{k-1} + mc + b_k + me = b_1 + \cdots + b_k + m(c+e)$

$\Rightarrow (a_1 + \cdots + a_k) - (b_1 + .. + b_k) = m(c+e)$, so $a_1 + \cdots + a_k \equiv b_1 + \cdots + b_k \pmod m$

Consider $a_1 \cdots a_k = (a_1 \cdots a_{k-1})a_k = (b_1 \cdots b_{k-1} + md)(b_k + me) = b_1 \cdots b_k + m(\text{things})$

Thus, $a_1 \cdots a_k - b_1 \cdots b_k \equiv 0 \pmod{m}$, as desired. □

Definition 4.4 (Equivalence Classes)**.** If X is a set with an equivalence relation $\sim$, X is partitioned into equivalence classes. Thus, for $x \in X, [x]_\sim = \{y \in X : x \sim y\}$

Example 4.4. If $m = 5$ and $\sim \equiv \pmod{m}$, then $x \equiv y \pmod{m} \Leftrightarrow$ x and y have the same remainder when we divide by m.

Note. We let $[X]_\sim = \{y \in \mathbb{Z} : y \equiv x \pmod{m}\}$

$[3]_5 = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$

The ring $\frac{\mathbb{Z}}{m\mathbb{Z}} = \mathbb{Z} \pmod{m\mathbb{Z}}$, is a ring with elements $[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m$

Note. Addition: $[i]_m + [j]_m = [i+j]_m$. Example: $[3]_5 + [3]_5 = [6]_5 = [1]_5$

Multiplication: $[i]_m[j]_m = [ij]_m$. Example: $[4]_5[4]_5 = [16]_5 = [1]_5$

Proof. We show that addition and multiplication are well-defined.

First, notice that if $[a_1]_m = [b_1]_m \Leftrightarrow a_1 b_1 \pmod{m}$

Then $[a_1 + a_2]_m = [b_1 + b_2]_m \wedge [a_1 a_2]_m = [b_1 b_2]_m$

Thus, $\frac{\mathbb{Z}}{m\mathbb{Z}}$ has binary operators addition and multiplication, and the additive and multiplicative identity. □

Exercise 4.1. Show that the ring axioms hold.

Lecture 15: Quotient Rings

Definition 4.5 (Definition of a Quotient Ring)**.** Let $m \in \mathbb{N}$.

Then, $|\mathbb{Z}/m\mathbb{Z}| = m$ and $\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$

Proof. Let $[n]_m$ be an element of $\mathbb{Z}/m\mathbb{Z}$.

By the division algorithm,

$$\begin{aligned} n &= qm + r \text{for some } q \in \mathbb{Z}, r \in \{0, 1, \ldots, m-1\} \\ &\Rightarrow n - r \text{is a multiple of m} \\ &\Rightarrow n \equiv r \pmod{m} \end{aligned}$$

So, $[n]_m = [r]_m$, which means that $\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$

Notice if $0 \leq i, j < m \wedge i \neq j$ then $-(m-1) < i - j < (m-1)$

So, $\therefore i - j \neq 0$ we see $m \nmid (i - j)$

Hence, $i \not\equiv j \pmod{m} \Rightarrow [i]_m \neq [j]_m$

So, $[0]_m, \ldots, [m-1]_m$ are pairwise distinct and so $|\mathbb{Z}/m\mathbb{Z}| = m$ □

Note. We also said that $\mathbb{Z}/m\mathbb{Z}$ is a ring, with binary operations such that:

Addition: $[a]_m + [b]_m = [a+b]_m$

Multiplication: $[a]_m[b]_m = [ab]_m$

And respective identities $0 = [0]_m$ and $1 = [1]_m$

When is $\mathbb{Z}/m\mathbb{Z}$ an integral domain when $m \geq 2$?

Theorem 4.2 (Theorem 4.2)**.** $\mathbb{Z}/m\mathbb{Z}$ is an integral domain $\Leftrightarrow$ m is prime.

Proof. First, if m is not prime, then $m = ab$ with $1 < a, b < m$.

But now, $0 < a, b < m$, thus implying that $[a]_m \neq [0]_m$ and $[b]_m \neq [0]_m$

But then, $[a]_m[b]_m = [ab]_m = [m]_m = [0]_m \Rightarrow \mathbb{Z}/m\mathbb{Z}$ is not an integral domain if m is not prime.

Thus, the first direction follows from the contrapositive.

Now suppose that $m = p$ is prime and that $[a]_p[b]_p = [0]_p$.

Notice that $[a]_p[b]_p = [ab]_p$ and that if $[a]_p[b]_p = [0]_p$, then $p \mid ab$.

By Euclid's Lemma (Lemma **??**), $p \mid a$ or $p \mid b$ => $[a]_p = [0]_p$ or $[b]_p = [0]_p$ and thus $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. □

Chapter 5

Fields

5.1 Introduction

Definition 5.1 (Rings and Fields)**.** A ring R is a field if

(i) R is commutative

(ii) $\forall a \in R$, if $a \neq 0$ then a is a unit

Example 5.1. $\mathbb{Z}$ is not a field because 2 is not a unit.

$\mathbb{Q}$ is a field because every single thing has a reciprocal other than 0.

$\mathbb{R}$ is a field because everything has an inverse other than 0.

5.2 Integral Domains

Proposition 5.1 (Integral Domains and Fields)**.** Let F be a field. Then, F is an integral domain.

Proof. Suppose that $a, b \in F$ and $ab = 0$

If $a \neq 0$ then it has an inverse a^{-1}

So, $a^{-1}(ab) = 0 \Rightarrow 1 \cdot b = 0 \Rightarrow b = 0$

Thus, $a = 0$ or $b = 0$ and thus F is an integral domain. □

Note. Fields $\subset$ Integral Domains $\subseteq$ Commutative Rings $\subset$ Rings

Theorem 5.1 (Finite Integral Domains)**.** Let R be a finite integral domain. Thus, R is a field.

Note. If X is a finite set and $f : X \to X$ is a function from X to X, then f is one to one $\Leftrightarrow$ f is onto.

Why? Let $x_1, \ldots, x_n$ denote the elements of X.

Notice that if $f : X \to X$ is 1 to 1, then $f(x_1), f(x_2), \ldots, f(x_n)$ are pairwise distinct. Thi sis because if $f(x_1) = f(x_j) \Rightarrow x_i = x_j$ meaning that f is not 1 to 1, a contradiction.

Proof. So $f(x_1), \ldots, f(x_n)$ are n distinct elements of X, and since $|X| = n$ we see that $\{f(x_1), \ldots, f(x_n)\} = X$ so f is onto. □

Exercise 5.1. Can you do the converse?

Proof. Proof of theorem **??**:

Let $r \in R$ be non-zero.

We make a map $f : R \to R$ given by $f(x) = rx$.

We claim that f is one to one. To see this, notice that if $f(a) = f(b)$, then $ra = rb \Rightarrow r(a - b) = 0$

Because R is an integral domain and $r \neq 0$, therefore $a - b = 0 \Rightarrow a = b$, and thus f is one to one.

Because R is finite, thus f is also onto from the note above.

So, $\exists x \in R$s.t. $f(x) = 1 \Rightarrow rx = 1 = xr$ and thus r is a unit.

Thus, condition *(ii)* is satisfied and R is thus a field, as desired. □

Corollary 5.1. If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof. $|\mathbb{Z}/p\mathbb{Z}| = p < \infty$ and $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. □

Note. In Assignment 4: p is prime and $p \nmid a \Rightarrow \exists x$ such that $p \mid (ax - 1) \Rightarrow [a]_p \neq [0]_p \Rightarrow \exists x$ such that $[a]_p[x]_p = [1]_p \Rightarrow [ax - 1]_p = [0]_p$

Chapter 6

Linear Diophantine Equations

6.1 Introduction

Definition 6.1. An equation of the form $a_1x_1 + \cdots a_nx_n = b$ where $a_1, \dots, a_n, b \in \mathbb{Z}$ and $x_1, \dots x_n$ are unknowns.

The goal of this is to find the integer solutions to said equation.

Example 6.1. $12x_1 + 5x_2 + 7x_3 = 81$

So how do we find the solution?

We start with a simple case: $n = 2$

Example 6.2. $ax + by = c, a, b, c, \in \mathbb{Z}$

Theorem 6.1 (Solution for n = 2)**.** The equation $ax + by = c$ has an integer solution $\Leftrightarrow \gcd(a, b) \mid c$

Remark. $-5x - 13y = 7$ is the same as $5(-x) + 13(-y) = 7$, thus you can treat the variables as positive WLOG and find the negative inverse of the solutions to find the other equation.

Proof. WLOG, assume $a, b > 0$

Then by the EEA, $\exists s, t \in \mathbb{Z}$ such that $as + bt = d, d = \gcd(a, b)$

So if $d \mid c, c = dc_0$ for some $c_0 \in \mathbb{Z} \Rightarrow a(sc_0) + b(tc_0) = (as + bt)c_0 = dc_0 = c$

So we have a solution.

Conversely, if $ax + by = c$ has an integer solution $(x, y) = (x_0, y_0)$ and if $d = \gcd(a, b)$ then $\because d \mid a \wedge d \mid b \Rightarrow d \mid (ax_0 + by_0) \Rightarrow d \mid c$ as desired. □

Lecture 16: Linear Diophantine Equations Continued

Recap. A linear Diophantine equation is one of the form $ax + by = c, a, b, c \in \mathbb{Z}$

This equation has an integer solution $\Leftrightarrow \gcd(a, b) \mid c$

If $a = b = 0, \gcd(0, 0) = 0$

If $a = 0 \wedge b \neq 0 \Rightarrow \gcd(a, b) = \gcd(0, b) = |b| \Rightarrow 0x + by = c$ thus has an integer solution $\Leftrightarrow |b| \mid c$. Vice versa if $b = 0, a \neq 0$.

If $a, b \neq 0$, we can assume WLOG that $a, b > 0$

6.2 Finding Solutions

Theorem 6.2 (Solution Set). Suppose we have a linear Diophantine equation

$$ax + by = c, (a, b) \neq (0, 0)$$

and let $d = \gcd(a, b)$

Then, if this equation has a solution $(x_0, y_0) \in \mathbb{Z}^2$, then the set of integer solutions S is given by

$$\left\{(x, y) : \exists m \in \mathbb{Z}, x = x_0 + \frac{b}{d}m, y = y_0 - \frac{a}{d}m\right\}$$

Remark. If you want to prove two sets are the same, you must first prove that the first set is contained in the first set, then prove that the second set is contained in the second set. This is similar to an if and only if proof.

Proof. Let

$$S = \left\{(x, y) \in \mathbb{Z}^2 : ax + by = c\right\}$$

and let

$$T = \left\{(x, y) : \exists m \in \mathbb{Z}, x = x_0 + \frac{b}{d}m, y = y_0 - \frac{a}{d}m\right\}$$

We first prove that $T \subseteq S$

Let $(x, y) \in T$. Then, by definition, $\exists m \in \mathbb{Z}$ such that $x = x_0 + \frac{b}{d}m, y = y_0 - \frac{a}{d}m$

Notice that $ax + by = a(x_0 + \frac{b}{d}m) + b(y_0 - \frac{a}{d}m) = ax_0 + \frac{ab}{d}m + by_0 - \frac{ba}{d}m = ax_0 + by_0 = c$

Thus, $(x, y) \in S \Rightarrow T \subset S$

Now we will show that $S \subseteq T$

Let $(x, y) \in S$. Thus, $x, y \in \mathbb{Z} \wedge ax + by = c$.

$\because ax_0 + by_0 = c, \therefore$ subtracting the two equations yields

$$\begin{aligned} a(x - x_0) + b(y - y_0) &= 0 \\ \Rightarrow a(x - x_0) &= -b(b - y_0) \\ \Rightarrow \left(\frac{a}{d}\right)(x - x_0) &= -\left(\frac{b}{d}\right)(y - y_0) \end{aligned}$$

Notice that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}\gcd(a, b) = 1$

Thus, $\left(\frac{a}{d}\right) \mid -\left(\frac{b}{d}\right)(y - y_0)$

Recall that if $\alpha, \beta, \gamma \in \mathbb{Z}, \alpha, \beta, \gamma \neq 0 \wedge \alpha \mid \beta\gamma \wedge \gcd(\alpha, \beta) = 1 \Rightarrow \alpha \mid \gamma$ by the fundamental theorem of arithmetic.

Thus, since $\gcd\left(\frac{a}{d}, -\frac{b}{d}\right) = 1 \Rightarrow \frac{a}{d} \mid y - y_0 \Rightarrow \; \exists m \in \mathbb{Z}$ such that $y - y_0 = \frac{a}{d}m$

Substituting this into the last line gives us $\frac{a}{d}(x - x_0) = -\frac{b}{d}\frac{a}{d}m \Rightarrow x - x_0 = -\frac{b}{d}m$

Thus, we get the set $x = x_0 - \frac{b}{d}m$ and $y = y_0 + \frac{a}{d}m \Rightarrow (x, y) \in T \Rightarrow S \subseteq T$.

Thus, we have proven that $S \subseteq T \wedge T \subseteq S \Rightarrow S = T$, as desired. □

Theorem 6.3 (General Case). Now we prove the general case:

$$a_1x_1 + \cdots + a_nx_n = b, a_1, \ldots, a_n, b \in \mathbb{Z}$$

Has an integer solution $\Leftrightarrow \gcd(a_1, \ldots a_n) \mid b$

Proof. Let $a_1, \ldots, a_n \in \mathbb{Z}, \neq 0$

We define $\gcd(a_1, \ldots a_n)$ to be the largest integer $d > 0$ such that $d \mid a_1, \ldots d \mid a_n$ □

Theorem 6.4 (General Case Defined). Let $n \in \mathbb{N} \wedge a_1, \ldots a_n \neq 0$

Then, $d = \gcd(a_1, \ldots a_n) \Leftrightarrow d \mid a_1, \ldots, d \mid a_n \wedge \exists m_1, \ldots, m_n \in \mathbb{Z}$ such that $d = m_1a_1 + \cdots m_na_n \wedge d > 0$

Proof. We prove this by induction on n.

When $n = 1, \gcd(a_1) = |a_1|$

Notice if $d = a_1m_1 \wedge d \mid a_1 \wedge d > 0 \Rightarrow d = |a_1| \because d = a_1m_1 \wedge a_1 = dm_1$

Now suppose that the result holds whenever $n < k$, where $k \geq 2$ and we consider the case when $n = k$. Let

Let $r = \gcd(a_1, \ldots, a_{k-1})$, let $e = \gcd(r, a_k), d = \gcd(a_1, \ldots, a_k)$

We claim that $e = d$. To see this, observe that $e \mid r \wedge e \mid a_k$

By the induction hypothesis, $r = m_1a_1 + \cdots + m_{k-1}a_{k-1}$ for some $m_1, \ldots m_{k-1} \in \mathbb{Z}$

Then, $e \mid a_1, \ldots e \mid a_{k-1} \wedge e \mid a_k \Rightarrow e \mid d$

Conversely, d is the gcd of $a_1, \ldots, a_n$

So, $d \mid (m_1a_1 + \cdots + m_{k-1}a_{k-1}) \Rightarrow d \mid r \wedge d \mid a_k \Rightarrow d \mid e$

Thus, $d \mid e \wedge e \mid d \Rightarrow |d| = e$

$e, d > 0 \Rightarrow e = d$

By the EEA, $e = sr + ta_k$ for some $s, t \in \mathbb{Z}$

$= s(m_1a_1 + \cdots + m_{k-1}a_{k-1} + ta_k = (sm_1)a_1 + \cdots + (sm_{k-1})a_{k-1} + ta_k)$

So we can write $d = e$ as an integer combination of $a_1, \ldots, a_k$ and suppose that $b \in \mathbb{Z}$ satisfies $b \mid a_1, \ldots, b \mid a_k, b = m_1a_1 + \cdots m_ka_k, b > 0$. We claim that $b = d$.

To see that $b = d$, notice that $d =$ integer combination because b divides every integer combination $\Rightarrow b \mid d$ and similarly $d \mid b$ and so $|d| = b \Rightarrow b = d$ □

Lecture 17: More LDE

Recap.

$$d = \gcd(a_1, \ldots, a_n), a_i \neq 0$$

If and only if the following hold:

$d > 0$

((ii) $d \mid a_1, \ldots, d \mid a_n$

(iii) $\exists m_1, \ldots, m_n \in \mathbb{Z}$ such that $d = a_1 m_1 + \cdots + a_n m_n$

Corollary 6.1. The linear Diophantine equation

$$a_1 x_1 + \cdots a_n x_n = b$$

with $a_1, \ldots, a_n$ as nonzero integers, $b \in \mathbb{Z}$, has an integer solution IF AND ONLY IF $\gcd(a_1, \ldots, a_n) \mid b$.

Proof. We first prove the forward statement.

Suppose that $\exists x_1, \ldots, x_n \in \mathbb{Z}$ such that $a_1 x_1 + \cdots a_n x_n = b$, and let $d = \gcd(a_1, \ldots, a_n)$, then $d \mid a_1, d \mid a_2, \ldots, a \mid a_n$ and thus $\exists a'_1, \ldots, a'_n \in \mathbb{Z}$ such that

$$\begin{aligned} a_1 &= da'_1 \\ a_2 &= da'_2 \\ &\vdots \\ a_n &= da'_n \end{aligned}$$

So

$$\begin{aligned} b &= a_1 x_1 + \cdots a_n x_n \\ &= da'_1 x_1 + da'_2 x_2 + \cdots + da'_n x_n \\ &= d(a'_1 x_1 + \cdots + a'_n x_n) \end{aligned}$$

And thus $d \mid b$.

We now prove the backward statement.

Suppose that $d \mid b$.

Then $b = db'$

We show that $\exists m_1, \ldots, m_n \in \mathbb{Z}$ such that $a_1 m)1 + \cdots + a_n m_n = d$

Multiplying both sides by b' yields that $a_1(m_1 b') + \cdots + a_n(m_n b') = db = b$.

Thus, letting $x_1 = m_1 b', \ldots, x_n = m_n b'$, we see that $a_1 x_1 + s a_n x_n = b$, as desired. □

Example 6.3. Show that $216x + 100y + 75z = 6$, has an integer solution and find one.

Step 1: Use the EEA to find the gcd of the first two numbers:

216	1	0
100	0	1
16	1	-2
4	-6	13
0		

So, $\gcd(216, 100) = 4 \Rightarrow 4 = 216(-6) + 100(13)$

Step 2: Use EEA to find $\gcd(4, 75)$

75	1	0
4	0	1
3	1	-18
1	-1	19
0		

Thus, $1 = 4(19) + 75(-1)$

Step 3: Use the expression from Step 1, substitute it into the expression above.

$$\begin{aligned} 1 &= (216(-6) + 100(13))(19) + 75(-1) \\ 1 &= 216(-114) + 100(247) + 75(-1) \end{aligned}$$

Step 4: Multiply by 6.

$$\begin{aligned} 6 &= 216(-114 \cdot 6) + 100(247 \cdot 6) + 75(-6) \\ 6 &= 216(-684) + 100(1482) + 75(-6) \end{aligned}$$

Thus, $(x, y, z) = (-684, 1482, -6)$.

6.3 Solving Linear Diophantine Equations mod m

Here we have $a_1, \dots, a_n$ as nonzero integers, $x_1, \dots, x_n$ as variables, and $b \in \mathbb{Z}$.

We want to consider the equation

$$a_1x_1 + \cdots a_nx_n \equiv b \pmod{m}$$

Notice that the equation has an integer solution $(x_1, \dots, x_n) \in \mathbb{Z}^n \Leftrightarrow\ \exists m_1, \dots, m_n \in \mathbb{Z}$ such that

$$\begin{aligned} &a_1m_1 + \cdots a_nm_n \equiv b \pmod{m} \\ &\Leftrightarrow m \mid (a_1m_1 + \cdots a_nm_n - b) \\ &\Leftrightarrow a_1m_1 + \cdots a_nm_n - b = mj \text{ for some } j \in \mathbb{Z} \\ &\Leftrightarrow\ \exists m_1, \dots m_n, j \in \mathbb{Z} \end{aligned}$$

And that $a_1m_1 + \cdots a_nm_n + m(-j) = b \Leftrightarrow a_1x_1 + \cdots a_nx_n + mx_{n+1} = b$ has an integer solution.

$\Leftrightarrow \gcd(a_1, \dots, a_n, m) \mid b$.

Theorem 6.5 (Solutions of a modular Linear Diophantine Equation)**.** The equation

$$a_1x_1 + \cdots a_nx_n \equiv b \pmod{m}$$

has an integer solution if and only if $\gcd(a_1, \dots, a_n, m) \mid b$

Theorem 6.6 (Sun-tzu's Theorem)**.** First, we define some things:

Definition 6.2. Let $a, b \in \mathbb{Z}$ be nonzero.

We say that a and b are coprime if $\gcd(a, b) = 1$.

Given $m_1, \ldots, m_n$ as nonzero integers, we say that they are pairwise coprime if $\gcd(m_i, m_j) = 1, i \neq j$

Let $m_1, \ldots, m_n$ be nonzero pairwise coprime integers and let $a_1, a_2, \ldots a_n \in \mathbb{Z}$.

Then the system of equations

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Has a solution and has a unique solution in $\{0, 1, \ldots, m_1, \ldots, m_n - 1\}$

Proof. To prove this, we let

$$M_i = \prod_{j \neq i} m_j = m_1 \cdot m_2 \cdots m_{i-1} m_{i+1} \cdots m_n$$

for $i = 1, \ldots n$

Lemma 6.1. $\gcd(m_i, M_i) = 1$ for $i = 1, \ldots, n$

Proof. Suppose the opposite. Then $\gcd(m_i, M_i) = d > 1$

Thus d has a prime factor p and so $p \mid m_i$, $p \mid M_i$

$M_i = \prod_{j \neq i} m_j$

since $p \mid \prod_{j \neq i} m_j$ then by EUclid's lemma, p divides one of the terms of the product, and thus $p \mid m_j, j \neq i$ and so $p \mid m_i \wedge p \mid m_j$ but this is impossible because they are coprime, and thus by contradiction the result follows. □

By the EEA, $\exists x_i, y_i \in \mathbb{Z}$ such that $x_i m_i + y_i M_i = 1$

Notice that $y_i M_i = \begin{cases} 1 \pmod{m_k}, & \text{if } i = k; \\ 0 \pmod{m_k}, & \text{otherwise.} \end{cases}$

Proof. $y_1 M_i \equiv 1 \pmod{m_i} \Rightarrow y_i M_i - 1 = m_i(-x_i)$

$m_1 \mid y_i M_i - 1 \Rightarrow y_i M_i \equiv 1 \pmod{m_i} \Rightarrow M_i \equiv 0 \pmod{m_i}, j \neq i$ □

Now let $x = a_1 y_1 M_1 + \cdots + a_n y_n M_n$

Notice that $\pmod{m_1}$

$$\begin{aligned} x &\equiv a_1y_1M_1 + \cdots a_ny_nM_n \pmod{m_1} \\ &\equiv a_1 \cdot 1 + a_2 \cdot 0 + \cdots + a_n \cdot 0 \pmod{m_1} \\ &\equiv a_1 \pmod{m_1} \end{aligned}$$

Similarly, if we look $\pmod{m_i}$, we get that $x \equiv a_i \pmod{m_i}$ for $i = 1, \ldots, n$ and thus we have a solution, as desired.

□

Lecture 18: Sunzi's Theorem

We figured out his name is not indeed Sun-Tzu but indeed is Sun-Zi.

Theorem 6.7 (Sunzi's Theorem)**.** Let $m1, \ldots, m_n$ be pairwise coprime integers and let $a_1, \ldots a_n \in \mathbb{Z}$.

Then,

(i) $\exists$ an $x \in \mathbb{Z}$ such that $x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_n \pmod{m_n}$

(ii) The solution is unique (m_1d) $M := m_1 \cdots m_n$. In particular, $\exists$ a unique solution $x_0 \in \{0, 1, \ldots, M-1\}$

Lemma 6.2. Let $m_1, \ldots, m_n$ be pairwise coprime.

Then, $x \equiv 0 \pmod{m_1} \wedge x \equiv 0 \pmod{m_2}, \ldots, x \equiv 0 \pmod{m_n} \Leftrightarrow x \equiv 0 \pmod{M}$

Proof. Backwards proof:

Notice that if $x \equiv 0 \pmod{M}$ then $M \mid x \Rightarrow m_i \mid x \; \forall i \in \{1, \ldots, n\}, \because M = m_1 \cdots m_n$
$\Rightarrow x \equiv 0 \pmod{m_i} \; \forall i$

Forwards proof:

We prove this by induction on n. When $n = 1$, the proof is obvious.

Now suppose that the claim holds whenever $n < k, k \geq 2$.

We consider the case when $n = k$.

So, we assume that $x \equiv 0 \pmod{m_1}, \ldots, x \equiv 0 \pmod{m_k}$

So, by the induction hypothesis, since $x \equiv 0 \pmod{m_1}, \ldots, x \equiv 0 \pmod{m_{k-1}}$, we have $x \equiv 0 \pmod{m_1 \cdots m_{k-1}}$

And we know that $x \equiv 0 \pmod{m_k}$ by assumption.

Last time, we showed that $\gcd(m_1 \cdots m_{k-1}, m_k) = 1$

So, by the EEA, $\exists s, t \in \mathbb{Z}$ such that $sm_1 \cdots m_{k-1} + tm_k = 1$

Since $x \equiv 0 \pmod{m_1 \cdots m_{k-1}} \Rightarrow \exists a \in \mathbb{Z}$ such that $x = m_1 \cdots m_{k-1}a$

If we multiply both sides by a, then we get that $sm_1 \cdots m_{k-1}a + tm_ka = a \Rightarrow sx + tm_ka = a$

Since $m_k \mid x \wedge m_k \mid tm_ka \Rightarrow m_k \mid a \Rightarrow x = m_1 \cdots m_kb, b \in \mathbb{Z} = Mb$

So, $M \mid x \Rightarrow x \equiv 0 \pmod{M}$,, and the result follows by induction. □

Theorem 6.8 (Sunzi's Theorem (Uniqueness)). By what we proved above, $\exists$ a solution $x \equiv a_1 \pmod{m_1}, \dots x \equiv a_n \pmod{m_n}$. Now we state that this solution is unique $\pmod{M}$.

Proof. Suppose that $x, y \in \mathbb{Z}$ are two solutions.

Then $x \equiv y \pmod{m_1}, \dots x \equiv y \pmod{m_n}$ by transitivity of congruency.

Thus, $x - y \equiv 0 \pmod{m_1}, \dots, x - y \equiv 0 \pmod{m_n}$

By our Lemma, this means that $x - y \equiv 0 \pmod{M} \Rightarrow x \equiv y \pmod{M} \Rightarrow$ there is a unique solution $\pmod{M}$. □

Chapter 7

Groups

7.1 Introduction

Example 7.1. Let R be a ring. Then, R^* = the set of units of R. Then, R^* is a group.

Definition 7.1 (Definition of a Group). A group is a set G with a binary operation $\cdot$ such that all of the following hold:

1. (associativity) $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. (identity) $\exists e \in G$ such that $\forall a \in G, a \cdot e = e \cdot a = a$
3. (inverses) $\forall x \in G,\ \exists y \in G$ such that $x \cdot y = y \cdot x = e$

Remark. If $x \cdot y = y \cdot x = e$, we say that y is the inverse of x and write $y = x^{-1}$

Remark. Inverses are unique;
$y \cdot x = x \cdot y = e \wedge z \cdot x = x \cdot z = e \Rightarrow y = y \cdot e = y \cdot (x \cdot z) = (y \cdot x) \cdot z = e \cdot z = z \Rightarrow y = z$

Remark. When the binary operation is equivalent to multiplication, we often write the identity as "1" and when it's equivalent to addition, we write the identity as "0".

Remark. If G is a group and $a \cdot b = b \cdot a\ \forall a, b \in G$, then G is called an "abelian" group.

Example 7.2. If R is a ring, then R is an abelian group with operation $+$ and $e = 0$.

Example 7.3. If F is a field, then:

(i) F is an abelian group with $+$ and $e = 0$

(ii) F_0 is an abelian group with $\cdot$ and $e = 1$

(iii) $\forall x, y, z \in F, x \cdot (y + z) = x \cdot y + x \cdot z$

Example 7.4. Imagine a regular, non-distortable hexagon. Notice that we have some symmetries:

(i) r: a reflection about the y-axis.

(ii) ρ : rotation 60° clockwise.

(iii) $r\rho r = \rho^{-1}$: a rotation 60° counter clockwise.

The symmetries of a regular hexagon form a group.

Proposition 7.1. All symmetries of a regular n-gon are given tby the set

$$\{\rho^i : i = 0, \dots, n-1\} \cup \{\rho^i \cdot r : i = 0, \dots, n-1\}$$

Where ρ is a rotation by $\left(\frac{360}{n}\right)^\circ$ clockwise, and r is a reflection about the y-axis.

Lecture 19: Groups Continued

7.2 Types of Groups

Recap. A group G is a set with a binary operator $\cdot \Rightarrow (G, \cdot)$.

(i) $\cdot$ is associative.

(ii) There exists an identity $e \in G$ such that $e \cdot x = x \cdot e = x \ \forall x \in G$

(iii) $\forall x \in G \ \exists x^{-1} \in G \Rightarrow x \cdot x^{-1} = x^{-1} \cdot x = e$

If $\forall x, y \in G, x \cdot y = y \cdot x$, then G is an "Abelian" group.

Theorem 7.1 (Idempotents and Abelians). If $(G, \cdot)$ is a group and $x \cdot x = e \ \forall x \in G$ then G is Abelian.

Proof. Let $x, y \in G$. Then $x \cdot y \in G \Rightarrow (x \cdot y) \cdot (x \cdot y) = e \Rightarrow x \cdot (y \cdot x \cdot y) = e$
$\Rightarrow (x \cdot x) \cdot (y \cdot x \cdot y) = x \cdot e \Rightarrow e \cdot (y \cdot x \cdot y) = x \Rightarrow y \cdot x \cdot y = x \Rightarrow y \cdot x \cdot y \cdot y = x \cdot y \Rightarrow y \cdot x = x \cdot y$ □

Definition 7.2 (Dihedral Groups). D_n = a group of size $2n$.

As a set,

$$D_n = \{1, \rho, \rho^2, \dots, \rho^{n-1}\} \cup \{\tau, \rho\tau, \rho^2\tau, \dots, \rho^{n-1}\tau\}$$

With binary operator $\cdot$

$$\rho^i \rho^j = \begin{cases} p^{i+j}, & \text{if } i + j \leq n-1; \\ p^{i+j-n}, & \text{otherwise.} \end{cases}$$

$$\rho^i \rho^j \tau = \begin{cases} p^{i+j}\tau, & \text{if } i + j \leq n-1; \\ p^{i+j-n}\tau, & \text{otherwise.} \end{cases}$$

$$\rho^i \tau \cdot \rho^j = \begin{cases} \rho^{i-j}\tau, & \text{if } i \geq j; \\ \rho^{i-j+n}\tau, & \text{otherwise.} \end{cases}$$

$$\rho^i \tau \cdot \rho^j \tau = \begin{cases} \rho^{i-j}, & \text{if } i \geq j; \\ \rho^{i-j+n}, & \text{otherwise.} \end{cases}$$

To visualise, imagine τ as a reflection about the y axis of a regular n-gon centred at the origin, while ρ is one rotation clockwise conforming to rotational symmetry.

For example, for a hexagon, label each vertex as $[n]_6$

Then τ :

$$\begin{aligned}[0]_6 &\to [0]_6\\ [1]_6 &\to [5]_6\\ [2]_6 &\to [4]_6\\ [3]_6 &\to [3]_6\\ [4]_6 &\to [2]_6\\ [5]_6 &\to [1]_6\end{aligned}$$

And ρ :

$$\begin{aligned}[0]_6 &\to [1]_6\\ [1]_6 &\to [2]_6\\ [2]_6 &\to [3]_6\\ [3]_6 &\to [4]_6\\ [4]_6 &\to [5]_6\\ [5]_6 &\to [0]_6\end{aligned}$$

$\rho \circ \tau([x]_6) = \rho([-x]_6) = [-x+1]_6$

$\tau \circ \rho^5([x]_6) = \tau([x+5]_6) = [-x-5]_6 = [-x+1]_6$

Remark. There are exactly $2n$ rigid symmetries of a regular n-gon.

Definition 7.3 (Symmetric Groups)**.** Let X be a set and let $S_X = \{f : X \to X : f \text{ is 1-1 and onto}\}$

$f1-1: \ \forall a, b \in X, f(a) = f(b) \Rightarrow a = b$

f onto: $\ \forall y \in X \ \exists x \in X \Rightarrow f(x) = y$

Thus, $(S_X, \circ)$ is a group.

Lecture 20: More about Groups

7.3 Subgroups and Cosets

Recap. A Group $G, \cdot$ is a set and an associated binary operator such that

(i) $\cdot$ is associative

(ii) $\exists 1 \in G, \ \forall x \in G \to 1 \cdot x = x \cdot 1 = x$

(iii) $\forall x \in G \ \exists x^{-1} \in G$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$

Remark. H is a subgroup of G if it is closed under $\cdot$; i.e. $\forall h_1, h_2 \in H, h_1 \cdot h_2 \in H \wedge 1 \in H \wedge \; \forall h \in H, h^{-1} \in H$

Example 7.5. Let G be a finite group and let $a \in G$. Notice that $\exists$ a smallest positive integer d such that $a^d = 1$.

Why? Since G is finite, by the Pigeonhole Principle, $\exists i > j$ positive integers such that $a^i = a^j \Rightarrow a^i \cdot a^{-j} = a^j \cdot a^{-j} \Rightarrow a^{i-j} = 1$

And so there exists $m \in \mathbb{N}$ such that $a^m = 1$ and exists a smallest $d \in \mathbb{N}$ such that $a^d = 1$

Let $H = \{1, a, a^2, \ldots, a^{d-1}\} \subseteq G$

We claim that H is a subset of G, i.e. for $a^i, a^j \in H$

$$a^i \cdot a^j = \begin{cases} a^{i+j}, & \text{if } i+j < d; \\ a^{i+j-d}, & \text{otherwise.} \end{cases}$$

If $i + j \geq d$, write $i + j = i + j - d + d \Rightarrow a^{i+j} = a^{i+j-d} \cdot a^d = a^{i+j-d}$

Example 7.6. $d = 5, a^5 = 1$

Thus, $H = \{1, a, a^2, a^3, a^4\}$

$a^1 \cdot a^2 = a^3, a^3 \cdot a^4 = a^7 = a^2 \cdot a^5 = a^2$

Notice that $a^i \cdot a^{d-i} = a^d = 1$ and so H is closed under taking inverses, and thus H is a subgroup of G, and H is what is known as a "cyclic" subgroup of H.

Definition 7.4 (Cyclic Subgroups)**.** A group H is cyclic, then $\exists a \in H$ such that every element of H is a power of a.

Notation. R^* is the group of the units of the ring R.

Example 7.7. $(\mathbb{Z}/5\mathbb{Z})^*$.

$\mathbb{Z}/5\mathbb{Z} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

$(\mathbb{Z}/5\mathbb{Z})^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ because $[0]_5$ does not have an inverse.

if $a = [4]_5$ then $\{[1]_5, [4]_5\}$ is the subgroup.

letting $a = [2]_5$ shows that $(\mathbb{Z}/5\mathbb{Z})^*$ is a cyclic group.

Definition 7.5 (Cosets)**.** Let G be a group and let H be a subgroup.

Then if $a \in G$, we define $Ha = \{ha : h \in H\}$ as a "right coset" of G.

Similarly if $a \in G$, we define $aH = \{ah : h \in H\}$ as a "left coset" of G.

Example 7.8. Let $G = (\mathbb{Z}/5\mathbb{Z})^*\{[1]_5, [2]_5, [3]_5, [4]_5\}$ and $H = \{[1]_5, [4]_5\}$

What are the right cosets of H in G?

Let $a = [1]_5 \Rightarrow Ha = H \cdot [1]_5 = H$

Let $a = [2]_5 \Rightarrow Ha = H \cdot [2]_5 = \{[2]_5, [3]_5\}$

Let $a = [3]_5 \Rightarrow Ha = \{[2]_5, [3]_5\}$

Let $a = [4]_5 \Rightarrow Ha = \{[1]_5, [4]_5\} = H$

$\{[2]_5, [3]_5\}, \{[1]_5, [4]_5\}$ are "distinct subgroups" of G

Lemma 7.1 (Distinct Subgroups). Let G be a group and let H be a subgroup. If $a, b \in G$ then either $Ha = Hb$ or $Ha \cap Hb = \varnothing$

Proof. If $Ha \cap Hb = \varnothing$, then there is nothing to prove, so we assume that $Ha \cap Hb \neq \varnothing$ and so $\exists h_1, h_2 \in H$ such that $h_1 a = h_1 b$

Claim 7.1. Notice if $h \in H$ then we claim $H \cdot h = H$.

Proof. To see this, notice that $H \cdot h = \{x \cdot h : x \in H\} \subseteq H$ as H is closed under $\cdot$

Notice also that if $x \in H$ then $x = (x \cdot h^{-1}) \cdot h$

$\because x \in H \wedge h \in H \Rightarrow x \cdot h^{-1} \in H \Rightarrow x \in H \Rightarrow H \subseteq H \cdot h)$ □

Now, $H \cdot a = (H \cdot h_1) \cdot a = H \cdot (h_1 \cdot a) = H \cdot (h_2 \cdot b) \equiv (H \cdot h_2) \cdot b = H \cdot b$ □

Note. Notice we can put an equivalence relation of G, $\sim$ using H

$$a \sim b \Leftrightarrow Ha = Hb \Leftrightarrow \ \exists h_1 \in H, h_2 \in H \to h_1 a = h_2 b$$

Reflexivity: $Ha = Hb \Rightarrow a \sim a$

Symmetric: $a \sim b \Leftrightarrow Ha = Hb \Rightarrow Hb = Ha \Rightarrow b \sim a$

Transitivity: $a \sim b \wedge b \sim a \Rightarrow Ha = Hb \wedge Hb = Hc \Rightarrow Ha = Hc \Rightarrow a \sim c$

Remark. Recall that when you have an equivalence relation on a set X, the relation partitions X into disjoint subsets; namely the equivalence classes.

If G is a group and $H \leq G$ and $\sim$ is $a \sim b \Leftrightarrow Ha = Hb$, what are our equivalence classes?

Answer: The equivalence classes are the distinct right cosets of G.

Notice that $a \sim b \Leftrightarrow Ha = Hb \Leftrightarrow Ha \cap Hb \neq \varnothing \Leftrightarrow \ \exists h_1 \in H_1 \ \exists h_2 \in H$ such that $h_1 a = h_2 b \Leftrightarrow \ \exists h_1 \in H, \ \exists h_2 \in H$ such that $a = (h_1^{-1} h_2) b$.

So $a \sim b \Rightarrow a \in Hb$

Conversely, if $h \in H$ then $hb \sim b$ because $H(hb) = (Hh)b = Hb$

And so $[b] = \{a \in H : Ha = Hb\} = Hb$

Corollary 7.1. Let G be a finite group and let H be a subgroup.

Then G is a disjoint union of cosets $Ha_1 \cup Ha_2 \cup \cdots \cup Ha_d$

What is the size of Ha?

Lemma 7.2. IfG is a group and $H \leq G$ then $|Ha| = |H|$

Proof. Consider the map $f : H \to Ha$

Then $f(h) = ha$

By definition of Ha this is onto. □

Lecture 21: Even more about groups

7.4 Order and Euler's Totient Function

Recap. If you have a group G, and a subgroup $H \leq G$, then H has right cosets $a \in G$ such that $H \cdot a = \{h \cdot a : h \in H\}$ and left cosets $a \cdot H = \{a \cdot h : h \in H\}$

It also has an equivalence relation $\sim$ if, for $x, y \in G$,

$$\begin{aligned} x \sim y &\Leftrightarrow Hx = Hy \\ &\Leftrightarrow \ \exists h_1, h_2 \in H \text{ such that } h_1 x = h_2 y \\ &\Leftrightarrow \ \exists h \in H \text{ such that } h \cdot x = y \end{aligned}$$

It can be said that equivalence classes are cosets Ha

Additionally, we showed that $|Ha| = |H| \ \forall a \in G$ (right cosets have the same size as the group). As a consequence, we get the following corollary:

Notation. The common terminology for the "size" of a group is the "order" of said group.

Corollary 7.2 (Lagrange's Theorem)**.** If G is a finite group and H is a subgroup of G, then $|H| \mid |G|$

Proof. We know that G is a disjoint union of right cosets:

$$G = Ha_1 \dot\cup Ha_2 \dot\cup \cdots \dot\cup Ha_k \text{ for some } k \geq 1$$

Thus,

$$\begin{aligned} |G| &= |Ha_1| + |Ha_2| + \cdots + |Ha_k| \\ &= |H| + |H| + \cdots + |H| \\ &= k \cdot |H| \end{aligned}$$

And thus $|H| \mid |G|$. □

We also looked at a special type of group:

Let G be a finite group and let $a \in G$. We say that $\exists$ a smallest $n \in \mathbb{N}$ such that $a^n = 1$

Why? By the Pigeonhole Principle, $\exists i, j \in \mathbb{N}, i < j$, such that $a^i = a^j \Rightarrow a^{-i} \cdot a^i = a^{-i} \cdot a^j \Rightarrow 1 = a^{j-i}$

We call this value n the "order" of a, which is also the size of the subgroup

$$H = \{1, a, a^2, \ldots, a^{n-1}\}$$

This is because $a^i \cdot a^j = \begin{cases} a^{i+j}, & \text{if } i+j \leq n-1; \\ a^{i+j-n}, & \text{otherwise.} \end{cases}$

H is also what is known as a "cyclic" group.

By Lagrange's Theorem, $|H| \mid |G|$ and thus $n \mid |G|$ i.e. the order of a divides the order of G. This leads to the corollary:

Corollary 7.3 (Cyclic Order)**.** If G is a finite group and $a \in G$ then

$$a^{|G|} = 1$$

Proof. Let n denote the order of a. Then, by Lagrange's Theorem, $n \mid |G|$, and thus $\exists k \in \mathbb{N}$ such that $a|G| = n \cdot k$.

So, $a^{|G|} = a^{n \cdot k} = (a^n)^k = 1^k = 1$ □

Corollary 7.4. Let p be prime and let $a \in \mathbb{Z}$ be coprime with p; i.e., $\gcd(a, p) = 1$.

$$a^{p-1} \equiv 1 \pmod p$$

Proof. Let $G = (\mathbb{Z}/p\mathbb{Z})^*$, i.e. the units group of $\mathbb{Z}/p\mathbb{Z}$

Then, $|G| = p - 1$ as we get rid of 0. I.e, $G = \{[1]_p, \ldots, [p-1]_p\}$

Since $p \nmid a$, $[a]_p \neq [0]_p$ and thus $[a]_p \in G$. So,

$$\begin{aligned} [a]_p^G &= [1]_p \Rightarrow \\ [a]_p^{p-1} &= [1]_p \Rightarrow \\ [a^{p-1}]_p &= [1]_p \Rightarrow \\ a^{p-1} &\equiv 1 \pmod p \end{aligned}$$

□

Definition 7.6 (Euler's Totient Function)**.** The function:

$$\phi(n) \coloneqq |(\mathbb{Z}/n\mathbb{Z})^*|$$

Lemma 7.3. For $n \in \mathbb{N}$, $\phi(n) = |\{j \in \{0, 1, \ldots, n-1\} : \gcd(j, n) = 1\}|$

Example 7.9. $\phi(6) = |\{j \in \{0, 1, 2, 3, 4, 5\} : \gcd(j, 6) = 1\}| = 2 = \phi(2)\phi(3)$

Proof. We claim that $[i]_n \in (\mathbb{Z}/n\mathbb{Z})^* \Leftrightarrow \gcd(i, n) = 1$.

Notice.

$$\begin{aligned}\gcd(i,n)=1 &\Rightarrow\ \exists s,t\in\mathbb{Z}\text{ such that } si+tn=1 \text{ by the EEA}\\ &\Rightarrow [s]_n[i]_n+[t]_n[n]_n=[1]_n\\ &\Rightarrow [s]_n[i]_n=[1]_n\\ &\Rightarrow [i]_n \text{ is a unit}\end{aligned}$$

Then, $\exists s\in\mathbb{Z}$ such that

$$\begin{aligned}&[s]_n\cdot[i]_n=[1]_n\\ &\Rightarrow si\equiv 1 \pmod n\\ &\Rightarrow si=1+n\cdot t \text{ for some } t\in\mathbb{Z}\\ &\Rightarrow si-nt=1 \text{ for some } t\in\mathbb{Z}\\ &\Rightarrow \gcd(i,n)=1\end{aligned}$$

Now, $\mathbb{Z}/n\mathbb{Z}=\{[0]_n,\dots[n-1]_n\}$ and so $(\mathbb{Z}/n\mathbb{Z})^*=\{[j]_n:\gcd(j,n)=1, 0\le j<n\}$

and so, $|(\mathbb{Z}/n\mathbb{Z})^*|=|\{j\in\{0,\dots,n-1\}:\gcd(j,n)=1\}|$ □

Corollary 7.5 (Euler-Fermat Theorem)**.** Let $n\in\mathbb{N}$ and let $a\in\mathbb{Z}$.

If $\gcd(a,n)=1$,

$$a^{\phi(n)}\equiv 1 \pmod n$$

Notice. This is a generalisation of Fermat's Little Theorem. Take $n=p$ where p is prime, then if $gcd(a,p)=1$, $a^{\phi(p)}==1 \pmod p \Rightarrow a^{p-1}\equiv 1 \pmod p$

Proof. Let $G=(\mathbb{Z}/n\mathbb{Z})^*),\Rightarrow |G|=\phi(n)$

If $\gcd(a,n)=1\Rightarrow [a]_n\in(\mathbb{Z}/n\mathbb{Z})^*$

And thus from our corollary,

$[a]_n^{\phi(n)}=[1]_n\Rightarrow[a^{\phi(n)}]_n=[1]_n\Rightarrow a^{\phi(n)}\equiv 1 \pmod n$ □

Example 7.10. $n=20\Rightarrow\phi(20)=$

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

Alternatively, $20=2^2\cdot 5^1\Rightarrow$

$\mathbb{Z}/20\mathbb{Z}\simeq\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\Rightarrow(\mathbb{Z}/20\mathbb{Z})^*\simeq(\mathbb{Z}/4\mathbb{Z})^*\times(\mathbb{Z}/5\mathbb{Z})^*$

Corollary 7.6. If $[a]_{20}\in(\mathbb{Z}/20\mathbb{Z})^*\Rightarrow[a]_{20}^8=[1]_{20}$

Exercise 7.1. Show for A6 that $[a]_{20}^4=[1]_{20}$

Definition 7.7 (Normal Subgroups)**.** Let H be a subgroup of group G, and let $a \in G$.

H is a normal subgroup of G if $\forall a \in G, Ha = aH$

Recap. If G is abelian and $H \leq G$ then H is normal in G.

Theorem 7.2 (Wilson's Theorem)**.** Let p be prime. Then, $(p-1)! \equiv -1 \pmod{p}$

Proof. Let G be a finite abelian group, or

$$G = \{g_1, g_2, \dots, g_n\}, n = |G|$$

Observation. In a group, we can pair off elements with their inverses, i.e. $x \leftrightarrow x^{-1}$

Problem. When does x get paired with itself?

Solution. When $x = x^{-1} \Leftrightarrow x^2 = 1 \Leftrightarrow$ order of x is $1, 2$.

Take $G = \{g_1, \dots, g_n\}$ and break it into two parts:

(i) $\{x_1, x_1^{-1}\} \cup \{x_2, x_2^{-1}\} \cup \dots \cup \{x_k, x_k^{-1}\}, x_i \neq x_i^{-1}$

(ii) $\{y_1, y_2, \dots, y_l\}, y_i = y_i^{-1}$

Consider the product $g_1 g_2 \cdots g_n = x_i x_i^{-1} \cdots x_k x_k^{-1} \cdots y_1 \cdots y_l = y_1 \cdots y_l$

Theorem 7.3. If G is a finite abelian group and let $G = g_1, \dots, g_n$

Then $g_1 \cdots g_n = y_1 \cdots y_l$ where y_i are elements of G that are their own inverses.

So now, let $G = (\mathbb{Z}/p\mathbb{Z})^*$

If $[x]_p = [x]_p^{-1} \Leftrightarrow [x]_p^2 = [1]_p \Leftrightarrow [x^2]_p = [1]_p \Leftrightarrow [x-1]_p \cdot [x+1]_p = [0]_p$.

Since $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, then this means that either $[x]_p = [1]_p$ or $[x]_p = [-1]_p = [p-1]_p$.

Thus, $G = \{[1]_p, \dots, [p-1]_p\}$. Take the product of all of the elements of G.

$= [1]_p \cdots [p-1]_p = [1]_p \cdot [-1]_p \Rightarrow [(p-1)!]_p = [-1]_p \Rightarrow (p-1)! \equiv -1 \pmod{p}$ □

Lecture 22: Even more more about groups, beginning of crypto

Recap. We covered Wilson's Theorem (Theorem ??); i.e. if p is a prime number then $(p-1)! \equiv -1 \pmod{p}$

We proved it by showing that in a field $\mathbb{Z}/p\mathbb{Z}$ the expression $x^2 - 1$ only has two roots: $x = [1]_p, [-1]_p$

Because of this,

$$\begin{aligned}&x^2 - [1]_p = 0\\ &\Leftrightarrow x - [1]_p = 0, x + [1]_p = 0 \text{ because it is an integral domain}\\ &\Leftrightarrow x = [1]_p, [-1]_p\end{aligned}$$

So, in $(\mathbb{Z}/p\mathbb{Z})^*$, we notice that $x = x^{-1} \Leftrightarrow x^2 = 1 \Leftrightarrow x = [1]_p, [-1]_p$

Additionally, we see that if G is a finite abelian group with elements $g_1, \ldots, g_n$ and $y_1, \ldots y_r$ are the elements of G such that $y_i = y_i^{-1}$, then $g_1 g_2 \cdots g_n = y_1 \cdots y_r$

And so in $(\mathbb{Z}/p\mathbb{Z})^*$, we see that $[1]_p[2]_p \cdots [p-1]_p = [1]_p \cdot [p-1]_p$ and the result follows.

Example 7.11. Let G be the group of "orientation-preserving symmetries" of a regular hexagon.

$$G = \{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$$

$$1 \cdot \rho \cdot \rho^2 \cdot \rho^3 \cdot \rho^4 \cdot \rho^5 = \rho^{15} = \rho^3$$

We also took a look at the Euler-Fermat Theorem.

Lemma 7.4 (Order of p^n prime quotient function)**.** Let p be prime.

Then, $|(\mathbb{Z}/p^n\mathbb{Z})^*| = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$

Proof. There are p^n elements $g \in 1, \ldots, p^n$. Of those elements, the ones where $\gcd(p^n, g) \neq 1$ are of the form $p * k, k \in 1, 2, \ldots, p^{n-1}$, and thus there are $k = p^{n-1}$ elements that do not satisfy the totient function, meaning there are $p^n - p^{n-1}$ elements. □

Example 7.12. Let p be 25 as an example. We see that the order is $25 - \frac{25}{5} = 20$

In general, for $n = p_1^{i_1} \cdots p_k^{i_k}$,

$$\phi(n) = \phi(p_1^{i_1}) \cdots \phi(p_k^{i_k}) = p_1^{i_1}(1 - p\frac{1}{p_1}) \cdots p_k^{i_k}(1 - \frac{1}{p_k}) = n \prod_{p|n}(1 - \frac{1}{p})$$

Chapter 8

Encryption

8.1 Introduction

Prior to 1977, we did not have very secure encryption methods.

Example 8.1. Caesar Cipher: shift each letter by a number of letters to the right.

Example 8.2. Text to binary string: Example -> 256 chars

"DOG" -> 01 ... 10 ... 1 ... 1

Where each character becomes an 8-bit binary number.

8.2 RSA

Problem. We want to send and receive messages without others being able to figure it out.

Solution. RSA encoding:

Suppose Alice and Bob want to talk to each other without Eve eavesdropping.

Step 1: Alice picks two **large** primes p and q and multiplies them together to get $N = p \cdot q$.

Notice. $\phi(N) = \phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$

This is the order of $(\mathbb{Z}/pq\mathbb{Z})^*$

Step 2: Alice picks a number $r \in \mathbb{N}$ such that $\gcd(r, N) = 1$

Step 3: Alice publishes (N, r) as her public key.

Step 4: Alice computes a positive integer e such that $re \equiv 1 \pmod{(p-1)(q-1)}$

We can use the EEA to find $s, t \in \mathbb{Z}$ such that $rs + t\phi(N) = 1$

If $s > 0$ take $e = s$; if $s < 0 \Rightarrow r(s + \phi(N)k) + \phi(N)(t - rk) = 1$, pick a k large enough such that $s + \phi(N)k > 0$ and take $e = k$.

Thus, (N, e) becomes Alice's private key.

Now, for the process of **encryption**:

Let us say that Bob wants to send Alice a message M.

Step 1: Convert M to integers that are between 0 and $N-1$. WLOG, assume Bob wants to send an integer M between 0 and $N-1$.

Step 2: Bob computes $M^r \pmod N$ and sends it to Alice. r is from Alice's public key.

That is Bob's encrypted message.

Alice **decrypts** it.

She takes Bob's message $M' := M^r \pmod N$ and computes $(M')^e \pmod N$

Lemma 8.1 (Decryption). We claim that this is the original message M

Proof.

$$(M')^e \equiv (M^r)^e \pmod N \equiv M^{re} \pmod N$$

But $re \equiv 1 \pmod{\phi(N)}$ and so $re = 1 + \phi(N)y$ for some $y \in \mathbb{N}$

So,

$$\begin{aligned} M^{re} &\equiv M^{1+\phi(N)y} \pmod N \\ &\equiv M^1 \cdot (M^{\phi(N)})^y \pmod N \end{aligned}$$

Case 1: If $\gcd(M,N) = 1$, then $M^{\phi(N)} \equiv 1 \pmod N$ by Euler-Fermat

In this case, $M^{re} \equiv M^1 \cdot 1^y \pmod N \equiv M \pmod N$

Case 2: If $\gcd(M,N) \neq 1 \Rightarrow \gcd(M,N) = \{p, q, pq\}$

If $p \mid M \wedge q \nmid M$, then $(M')^e \equiv M^{re} \equiv 0 \pmod p$

and $(M')^e \equiv M^{re} \equiv M^{1+\phi(N)y} \pmod q \equiv M \pmod p$ by Fermat's Little Theorem.

And so, $(M')^e \equiv M \pmod p \wedge (M')^e \equiv M \pmod q \Rightarrow (M')^e \equiv M \pmod{pq}$ by Sun-zi's theorem. □

Lecture 23: RSA continued

Question. Why is

$$(M')^e \equiv M \pmod N$$

Answer. Look $\pmod p$:

Case 1: $p \mid M$

If $p \mid M \Rightarrow (M')^e = M^{re} \equiv 0 \pmod p \wedge M \equiv 0 \pmod p$, so $M^{re} \equiv M \pmod p$

Case 2: $p \nmid M$

$$\begin{aligned}(M')^e &= (M^r)^e\\ &= M^{re}\\ &= M^{1+(p-1)(q-1)y}\\ &= M \cdot (M^{p-1})^{(q-1)y}\\ &\equiv M \cdot 1^{(q-1)y} \pmod{p} \text{ by FLT}\\ &\equiv M \pmod{p}\end{aligned}$$

So in either case, $(M')^e \equiv M \pmod{p}$

Similar,ly, $(M')^e \equiv M \pmod{q}$
$\Rightarrow p \mid (M')^e - M \wedge q \mid (M')^e - M$
$\Rightarrow pq \mid (M')^e - M \Rightarrow (M')^e \equiv M \pmod{pq}$ by Sun-Zi's Theorem.

Problem (Discrete Log Problem)**.** Let there be a finite group G, and an element $g \in G$. Compute $g^n := y$. Given g, y, what is n?

Example 8.3. Given the group $(\mathbb{Z}/59\mathbb{Z})^*$, then $[2]_{59}^x = [27]_{59}$. Find x.

It is very easy to compute $[2]_{59}^x$. Let $x = 50 = 32 + 16 + 2$. Simply multiply the corresponding multiples of $[2]_{59}^{2n}$ as required.

If you have a very long string, and a very long key as long as the string that you're encrypting, then you will not be able to decrypt the string without the key.

Definition 8.1 (Diffe-Helman key exchange)**.** Let there be an element $g \in G$, where the order $|G| = n$ is large. Let two parties have an agreed-upon rule for converting elements $g \in G$ into keys.

Party 1 picks a number a such that $\gcd(a, n) = 1$ and computes $g^a \in G$ and sends it to party 2.

Party 2 picks a number b such that $\gcd(b, n) = 1$ and computes $g^b \in G$ and sends it to party 1.

Example 8.4. Party 1 knows: G, n, g, a, g^a, g^b

Party 2 knows: G, n, g, b, g^a, g^b

An eavesdropper knows: G, n, g, g^a, g^b

Party 1 can compute: $(g^b)^a = g^{ab} \in G$, which is the key.

Party 2 can compute: $(g^a)^b = g^{ab} \in G$, which is the key.

The eavesdropper does not know a or b, in which case the Discrete Log Problem makes it exponentially difficult to figure out the key.

It is thus easy to generate new keys, but very difficult to figure them out without knowing a or b.

8.3 O Notation

Notation. We have $\mathcal{O}$ as "Big O",

o as “Little O”

$\sim$ as “asymptotic to”

Definition 8.2 (Big O). $f(n) = \mathcal{O}(g(n))$ if $\exists c > 0$ such that $f(n) < Cg(n)$ $\forall n$ as n becomes large.

Definition 8.3 (Little O). $f(n) = o(g(n))$ if $\frac{f(n)}{g(n)} \to o$ as $n \to \infty$.

Definition 8.4 (Asymptotic). $f(n) \sim g(n)$ if $\frac{f(n)}{g(n)} \to 1$

Example 8.5. In $(0, \infty)$:

$\mathbb{R}_{>0}$: $(\log x)^3 = o(x^{\frac{1}{100}})$

$\mathbb{N}$: $2^n = o(n!)$ (because $n! \sim \frac{n^n}{e^n}\sqrt{2\pi n}$ (Stirling's Formula))

$\mathbb{R}_{>0}$: $\sin x + 2 = \mathcal{O}(1)$

Lecture 24: Polynomials

8.4 Polynomials

Example 8.6. Let us say you pick a number m such that $0 \leq m < 2^n$. Let $n = 4, m = 11$.

We try to guess this number.

First, we ask if the number $= 0 \pmod 2$. Because it is not, we write our guess as ___1, in binary representation.

We then ask if it is $= 1 \pmod 4$. Because it is not, we write our guess as __11.

We then ask $= 3 \pmod 8$. Because it is, we write our guess as _011.

We then ask if it is $= 3 \pmod{16}$. Because it is not, we write our guess as 1011, which is 11's binary expansion.

Remark. We need n bits of information to distinguish numbers from 0 to $2^n - 1$, inclusive.

In general, n can be described with about $\log_2 n$ bits. So, if we are doing a computation involving an integer n and we want to measure its complexity, we measure it as a function of $\log_2 n$.

In particular, if our computation requires $\mathcal{O}((\log n)^d)$ steps for some $d \in \mathbb{N}$, then we say it can be performed in polynomial time.

We say that it is exponential if, for large n, $\exists C > 1$ such that it requires at least $C^{\log n} = e^{\log n \log c} = n^{\log c}$ steps.

Remark. Addition, multiplication, and exponentiation can all be done in polynomial time.

Remark. There is a prime test called the AKS algorithm that tests if a number is prime in polynomial time.

Let R be a ring. We let $R[x]$ denote the set of elements of the form $r_0 + r_1x + \cdots + r_nx^n, n \geq 0, x^0 = 1, r_1, \ldots, r_n \in R$.

Example 8.7. If $R = \mathbb{Z}$, then $2 + 3x + 5x^3 = 2 + 3x + 0x^2 + 5x^3 + 0x^4$

We call $R[x]$ the ring of polynomials with coefficients in R.

Notice that $R[x]$ is a ring.

Addition: $(a_0 + a_1x + \cdots = a_nx^n) + (b_0 + b_2x + \cdots + b_nx^n) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$. $0 = 0 + 0x + \cdots + 0x^n$. We trivially see that it is associated and commutative.

Multiplication: $(a_0 + a_1x + cdots + a_mx^m) \cdot (b_0 + b_1x + \cdots + b_nx^n) = a_0b_0 + (a_0b_1 = a_1b_0)x + \cdots + (a_mb_{n-1} + a_{m-1}b_n)^{m+n-1} + a_mb_nx^{m+n}$

In general, we have

$$(\sum_{c=0}^{m} a_1x^i) \cdot (\sum_{j=0}^{n} b_jx^i) = \sum_{k=0}^{m+n} c_kx^k, \text{ where } c_k = \sum_{i+j=k} a_ib_j$$

Theorem 8.1 (Commutativity of R[x]).] $R[x]$ is commutative $\Leftrightarrow$ R is commutative.

Proof. If $R[x]$ is commutative and $a, b \in R$. Then $a \cdot b = b \cdot a$, since a, b can be regarded as constant polynomials. So, R is commutative.

Next, if R is commutative and $p(x), g(x) \in R[x]$, we write that $p(x) = a_0 + a_1x + \cdots = a_mx^m$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n$

Then, $p(x)q(x) = (a_0 + a_1 + \cdots = a_mx^m)(b_0 + b_1x + \cdots + b_nx^n) = \sum_{k=0}^{n+m} (\sum_{i+j=k} a_ib_i)x^k = q(X)p(x)$ □

Definition 8.5 (Degree). Let $p(x) \in R[x]$ be a polynomial. If $p(x) = 0$, we define $\deg(p(x)) = -\infty$.

If $p(x) \neq 0$ then we write $p(x) = a_0 + a_1x + \cdots + a_nx^n, a_n \neq 0$, we define $deg(p(x)) = n$.

Lemma 8.2. Let R be an integral domain, then $\deg(p(x)q(X) = \deg(p(x)) + \deg(q(x))$, where $-\infty + n = -\infty, -\infty + -\infty = -\infty$

Proof. If p or q is 0 then the result is immediate. Thus, we assume that p and q are non-zero.

We write

$$p(x) = a_0 + a_1x + \cdots + a_mx^m, a_m \neq 0, m = \deg(p)$$
$$q(x) = b_0 + b_1x + \cdots + b_nx^n, b_n \neq 0, n = \deg(q)$$

$p(x)q(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + \cdots + a_mb_nx^{m+n}$. $\because R$ is an integral domain and $a_m, b_n \neq 0$, we see that $a_m \cdot b_n \neq 0$ and so $m + n = \deg(p(x)q(X)), m + n = \deg(p) + \deg(q)$ □

Notice. If $R = \mathbb{Z}/6\mathbb{Z}$,

$$\begin{aligned} p(x) &= [1]_6 + [2]_6 x \\ q(x) &= [1]_6 + [3]_6 x \\ p(x)q(x) &= [1]_6 + [5]_6 x \end{aligned}$$

We are going to look at $R = F$, where F is a field.

Theorem 8.2. Let $n \geq 3$. If $p(x), g(x), r(x)$ are coprime polynomials and are not constant, then $p(x)^n + q(x)^n \neq r(x)^n$ in the field $\mathbb{C}[x]$.

Chapter 9

Polynomials

9.1 Division

Lecture 25: Division of Polynomials

Notation. Let R be a ring. Then, $R[x]$ is a ring of polynomials with coefficients in R

Recap. $\deg(p(x)) = n, p(x) \neq 0, p(x) = a_n x^n + \cdots + a_0, a_n \neq 0$

$\deg(0) = -\infty$.

$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ if R is an integral domain.

Theorem 9.1. Let F be a field, then $F[x]^* = F^*$.

Proof. We show that $F[x]^* \subseteq F^* \wedge F^* \subseteq F[x]^*$

To see that $F^* \subseteq F[x]^*$, let $\alpha \in F^* = F \setminus 0$. Then $\exists \beta \in F^*$ such that $\alpha\beta = \beta\alpha 1$.

Then, this holds in $F[x] \Rightarrow \alpha \in F[x]^*$.

To see that $F[x]^* \subseteq F^*$, let $p(x) \in F[x]^*$ and let $q(x) \in F[x]^*$ be its inverse. Thus, $p(x)q(x) = 1$.

Taking the degree, we see that $\deg(p(x)q(x)) = \deg(1) \Rightarrow \deg(p(x)) + \deg(q(x)) = 0 \Rightarrow \deg(p(x)) = \deg(p(x)) = 0$

So, $p(x) = \alpha \in F^*, q(x) = \beta \in F^* \Rightarrow F[x]^* \subseteq F^*$ □

Note. Comparison between $F[x]$ and $\mathbb{Z}$:

$F[x]$	$\mathbb{Z}$
0	0
F^*	± 1 units
$\deg(p(x))$	$\lvert n \rvert$ size
irreducible	prime
reducible	composite

Definition 9.1 (Reducible polynomial). Let $p(x) \neq 0 \in F[x]$

We say that $p(x)$ is reducible if $\exists a(x), b(x)$ of deg ≥ 1 such that $p(x) = a(x)b(x)$.

If $\deg(p(x)) \geq 1 \wedge p(x))is$ not reducible, then $p(x)$ is irreducible.

Example 9.1. Consider $F = \mathbb{Z}/2\mathbb{Z}$. Then $F[x] = \mathbb{Z}/2\mathbb{Z}[x]$. Which are reducible?

(i) $[1]_2x^2 = ([1]_2x)([1]_2x)$

(ii) $[1]_2x^2 + [1]_2x = ([1]_2x)([1]_2x + [1]_2)$

(iii) $[1]_2x^2 + [1]_2 = ([1]_2x + [1]_2)^2$

(iv) $[1]_2x^2 + [1]_2x + [1]_2$ is irreducible.

Why is *(iv)* irreducible?

If it were reducible, then there would exists $a, b \in \mathbb{Z}/2\mathbb{Z}$ such that

$$\begin{aligned}[1]_2x^2 + [1]_2x + [1]_2 &= ([1]_2x + a)([1]_2x + b)\\ &= [1]_2x^2 + bx + ax + ab\\ &= [1]_2x^2 + (a+b)x + ab\end{aligned}$$

Compare the coefficients:

(i) $[1]_2 = ab$

(ii) $[1]_2 = a + b$

There is no solution to this system of equations in $\mathbb{Z}/2\mathbb{Z}$.

Observation. Using the division algorithm, input $b(x), a(x) \in F[x], a(x), b(x) \neq 0$.

Output $q(x), r(x) \in F[x]$ such that

(i) $a(x) = q(x)b(x) + r(x)$

(ii) $\deg(r(x)) < \deg(b(x))$

(iii) $q(x), r(x)$ are unique with regard to *(i)* and *(ii)*

This is long division of polynomials.

Definition 9.2 (Division Algorithm). For any $a, b, b \neq 0$, $a = bq + r$.

Proof. We prove the division algorithm holds in fields with polynomials.

Let $a(x), b(x) \in F[x], a(x), b(x) \neq 0$

We prove this via induction on $\deg(a(x))$

Base Case: $\deg(a(x)) = 0$ so $a(x)$ is constant $c \neq 0$. Thus, $q(x) = \frac{b(x)}{c}, r(x) = 0$
$\Rightarrow b(x) = q(x)a(x) + r(x)$

Induction Hypothesis: Let $d \in \mathbb{N}$ and assume the claim holds whenever $\deg(a(x)) < d$ and consider the case when $\deg(a(x)) = d$

Case I: If $d < \deg(b(x))$, take $q(X) = 0, r(x) = a(x)$

Case II: If $d \geq \deg(b(x))$, let $\deg(b(x)) = m \leq d$

So, $b(x) = b_m x^m + \cdots, a(x) = a_d x^d + \cdots, b_m, a_m \neq 0$

Let $\widetilde{a}(x) = a(x) - (\frac{a_d}{b_m})x^{d-m}b(x) = (a_d x^d + \text{lower degree terms}) - (\frac{a_d}{b_m}x^{d-m})(b_m x^m + \text{lower degree terms})$

$\widetilde{a}(x)$ is a polynomial of a degree $< d$, and thus by the induction hypothesis, the claim holds if $\widetilde{a}(x) \neq 0$.

If $\widetilde{a}(x) = 0$ then that means that $b(x)$ divides cleanly into $a(x)$, which means the claim holds regardless.

Thus, *(i)* and *(ii)* hold by induction. □

Lecture 26: More about the division of polynomials

Recap. Using the division algorithm, let $b(x), a(x) \in F[x], b(x) \neq 0$.

Then, $\exists q(x), r(x) \in F[x]$ such that $a(x) = q(x)b(x) + r(x)$ s,t, $\deg(r(x)) < \deg(b(x))$ and that $q(x), r(x)$ are unique.

Last time, we proved the uniqueness of $q(x)$ and $r(x)$:

Suppose we have $q_1(x), q_2(x), r_1(x), r_2(x) \in F[x]$ such that $a(x) = q_1(x)b(x) + r_1(x) + q_2(x)b(x) + r_2(x); \deg(r_1(x)), \deg(r_2(x)) < \deg(b(x))$.

Thus,

$$q_1(x)b(x) + r_1(x) = a(x) \tag{9.1}$$
$$q_2(x)b(x) + r_2(x) = a(x) \tag{9.2}$$

Subtracting the two, we get $(q_1(x) - q_2(x))b(x) + r_1(x) - r_2(x) = 0$

Since $\deg(r_1(x)), \deg(r_2(x)) < \deg(b(x)) \Rightarrow \deg(r_1(x) - r_2(x)) < \deg(b(x))$

$r_1(x) - r_2(x) = -(q_1(x) - q_2(x))b(x)$. $\deg(b(x)) > \deg(r_1(x) - r_2(x)) = \deg((q_1(x) - q_2(x))b(x)) = \deg(q_1(x) - q_2(x)) + \deg(b(x)) \Rightarrow 0 > \deg(q_1(x) - q_2(x)) \Rightarrow q_1(x) - q_2(x) = 0 \Rightarrow r_1(x) - r_2(x) = 0$

And thus we have demonstrated uniqueness. □

Definition 9.3 (Divisors of polynomials). $p(x) \mid q(x)$ in $F[x]$ if $\exists a(x) \in F[x]$ such that $q(x) = a(x)p(x)$.

Definition 9.4 (Monic Polynomials). Let $p(x) \in F[x]$ be non-zero. We say that $p(x)$ is monic if $p(X) = x^n +$ lower degree terms, $n \geq 0$

Definition 9.5 (GCD of polynomials). Let $a(x), b(x) \in F[x]$ be polynomials. We define $\gcd(a(x), b(x))$ to be the largest degree monic polynomial that divides $a(x)$ and $b(x)$ if $a(x), b(x) \neq 0$.

If $a(x) = 0, b(x) \neq 0, \gcd(a(x), b(x)) = c^{-1}b(x)$ where c is the leading coefficient of $b(x)$.

Similarly, if $a(x) \neq 0, b(x) = 0, \gcd(a(x), b(x)) = c^{-1}a(x)$ where c is the leading coefficient of $a(x)$.

If $a(x) = b(x) = 0, \gcd(a(x), b(x)) = 0$

With this, we can create an EEA for polynomials.

Example 9.2. (i) Find the gcd, $d(x), a(x) = x^4 + x^3 + 9x + 9, b(x) = x^3 - x^2 - 3x - 1$

(ii) Find $s(x), t(x) \in F[x]$ such that $d(x) = a(x)s(x) + b(x)t(x)$

Step 1 is to divide $a(x)$ by $b(x)$.

Step 2 is to divide $b(x)$ by $r_1(x)$.

Step 3 is to divide $r_1(x) by r_2(x)$

Repeat until you get 0.

x^4+x^3+9x+9	1	0
x^3-x^2-3x-1	0	1
$5x^2+16x+11$	1	$-x-2$
$\frac{206x}{25}+\frac{206}{25}$	$\frac{-x}{5}+\frac{21}{25}$	$\frac{x^2}{5}-\frac{11x}{25}-\frac{17}{25}$
$x+1$	$\left(\frac{-x}{5}+\frac{21}{25}\right)\frac{25}{206}$	$\left(\frac{x^2}{5}-\frac{11x}{25}-\frac{17}{25}\right)\frac{25}{206}$
0		

Table 9.1: EEA on the example above

Observation. We can do the same things in $F[x]$ that we can do in $\mathbb{Z}$:

(i) $|n| \sim \deg(p(x))$

(ii) prime $\sim$ irreducible

(iii) composite $\sim$ reducible

(iv) units $= \{\pm 1\} \sim$ units $= F^*$

As a consequence of this, we also have Euclid's Lemma for polynomials:

Lemma 9.1 (Euclid's Lemma for Polynomials). If $p(x) \in F[x]$ is irreducible and $p(x) \mid a(x)b(x)$ then $p(x) \mid a(x)$ or $p(x) \mid b(x)$

Proof. The proof is the same as in the integers. □

Lemma 9.2 (Divisibility). If $p(x)$ is irreducible and $p(x) \nmid a(x)$ then $\gcd(p(x), a(x)) = 1$

Proof. The proof is the same as in the integers. □

Lecture 27: EEA for Polynomials in a Field, Continued

Recap. Last time we covered the EEA for polynomials:

We input $a(x), b(x)$ with $b(x)$ non-zero and we get a monic polynomial $d(x) = \gcd(a(x), b(x))$ as output.

Because of this, we know that $\exists s(x), t(x) \in F[x]$ such that $d(x) = s(x)a(x) + t(x)b(X)$, and that additionally that $e(x) \mid a(X) \wedge e(X) \mid b(x) \Rightarrow e(x) \mid d(x)$

Just line in $\mathbb{Z}$, if $p(x)$ is irreducible and monic, then $\gcd(a(x), p(x)) = \begin{cases} p(x), & \text{if } p(x) \mid a(x); \\ 1, & \text{otherwise.} \end{cases}$

Definition 9.6 (Unique Factorization of a Polynomial). If $a(x) \in F[x]$ is non-zero, then $a(x) = Cx^n +$ lower degree terms, $C \neq 0$.

Suppose that $a(x) = C \cdot p_1(x)p_2(x)\cdots p_s(x) = C \cdot q_1(x)\cdots q_t(x)$ where $p_i(x), q_i(x)$ are monic and irreducible.

Then $s = t$ and after reordering, $p_1(x) = q_1(x), \ldots, p_s(x) = p_t(x)$.

Proof. We prove this by induction of $\deg(a(x))$. Since $a(x) \neq 0, \deg(a(x)) \geq 0$

Base Case: $\deg(a(x)) = 0 \Rightarrow a(x) = C \Rightarrow s = t = 0$, meaning it is true.

Suppose that the claim holds whenever $\deg(a(x)) < n$ and consider the case when $\deg(a(x)) = n$.

Now observe that $p_s(x) \mid C \cdot q_1(x)\cdots q_s(x)$.

By the generalisation of Euclid's lemma, $\exists i$ such that $p_s(x) \mid q_i(x)$ After reordering the indices, we may assume that $i = t$ so that $p_s(x) \mid q_t(x)$. Because $p_s(x), q_t(x)$ are both monic and irreducible, this implies that $p_s(x) = q_t(x)$.

So, $a(x) = Cp_1(x)\cdots p_{s-1}(x)p_s(x) = Cq_1(x)\cdots q_{t-1}(x)q_t(x)$

Let $b(x) = \frac{a(x)}{p_s(x)} = Cp_1(x)\cdots p_{s-1}(x) = Cq_1(x)\cdots q_{t-1}(x)$. Notice that $\deg(b(x)) < \deg(a(x)) = n$ and thus by the induction hypothesis, $s - 1 = t - 1 \Rightarrow s = t$ and thus the result follows by induction. □

Theorem 9.2 (Existence of Factorization of a Polynomial)**.** There always is a factorization of $a(x) = Cx^n+$ lower degree terms as $C\cdot$ a product of monic irreducible polynomials. This is, $a(x) = C \cdot p_1(x)\cdots p_s(x)$.

Proof. Suppose towards a contradiction that this is not true and let

$$S = \{\deg(a(x)) : a(x) \text{ cannot be factored}\}$$

By assumption, $S \neq \varnothing$ and so by the Well-Ordering Principle, $\exists$ a smallest element $d \in S$.

Then by the definition of S, $\exists a(x) = Cx^d$ + lower deg terms that cannot be factored into irreducible polynomials.

If $d = 0, a(x) = C \Rightarrow d > 0$

Case 1: $a(x)$ is irreducible. Let $p(x) = \frac{a(x)}{C} = x^d + \ldots$ which is irreducible.

Case 2: $a(x)$ is reducible. Thus $a(x) = b(x)c(x)$ with $1 \leq \deg(b(x)), \deg(c(x)) < d = \deg(a(x))$.

By minimality of $d, \deg(b(x)), \deg(c(x)) \notin S$. So $b(x), c(X)$ factor. Say $b(x) = C_1 \cdot p_1(x)\cdots p_s(x), c(x) = C_2 q_1(x)\cdots q_t(x), p_i(x), q_j(x)$ are monic and irreducible. Then $b(x)c(x) = Cp_1(x)\cdots p_q(x)\cdot q_1(x)\cdots q_t(x)$ but this contradicts our choice of $a(x)$ and thus the result follows. □

Lecture 28: More stuff

Theorem 9.3 (Fermat's Last Theorem for $\mathbb{R}[x]$)**.** Let $a(x), b(x), c(x)$ be pairwise coprime polynomials and let $n \geq 3$.

If $a(x)^n + b(x)^n = c(x)^n$, then $a(x), b(x), c(x)$ are constants.

Notice that this does not hold in every field.

Example 9.3. $F = \mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$

$$\begin{aligned}(1+x)^5 &= 1+5x+10x^2+10x^3+5x^4+x^5\\ &= 1+x^5\\ &= 1^5+x^5\end{aligned}$$

Definition 9.7 (Characteristics)**.** Let R be a ring. If $\nexists n \in \mathbb{N}$ such that $1+1+\cdots+1$ (n times) $=0$, then we say that R has a characteristic 0.

Otherwise, $\exists$ a smallest $d \in \mathbb{N}$ .s.t $1+1+\cdots+1$ (d times) $=0$ and we say that R is of characteristic d.

Example 9.4. What is the characteristic of

(*i*) $\mathbb{Z}$?0

(*ii*) $\mathbb{Z}/5\mathbb{Z}$?5

(*iii*) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$?6

(*iv*) $\mathbb{R}$?0

(*v*) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.2\mathbb{Z}$?2

Theorem 9.4. Let F be a field. Then, the characteristic of F is either 0 or a prime number p.

Proof. If $\text{char}(F)=0$ there is nothing to prove, so we assume that F has a positive characteristic $n \geq 2$.

If n is prime, there is nothing to prove.

So WLOG we assume that n is composite, i.e. $n = a \cdot b, 1 < a, b < n$.

$n \cdot 1 = (1+1+\cdots+1)$ (n times) $= (1+1+\cdots+1$ (a times) $)(1+1+\cdots+1$ (b times) $)$

Since $n = \text{char}(F), 0 < a, b < n$, we see that this $\neq 0$ meaning that $n \neq 0$

This gives a contradiction as n was defined to be the characteristic of F. □

Remark. When $n=2$, there are counterexamples such as

$$\begin{aligned}(x^2-1)^2+(2x)^2 &= x^4-2x^2+1+4x^2\\ &= x^4+2x^2+1\\ &= (x^2+1)^2\end{aligned}$$

Lemma 9.3. Let $u(x), v(x)$ be nonzero polynomials in $\mathbb{R}[x]$ and suppose that $u'(x)v(x)-v'(x)u(x)=0$

Then $\exists \lambda \in \mathbb{R}$ such that $u(x)=\lambda v(x)$

Thus $(\frac{u(x)}{v(x)})' = \frac{v(x)u'(x)-u(x)v'(x)}{v(x)^2} = 0 \Rightarrow \frac{u(x)}{v(x)} = \lambda \Rightarrow u(x) = \lambda v(x)$

Exercise 9.1. $u(x), b(x), w(x) \in \mathbb{R}[x], u(x) \neq 0, \gcd(u(x), v(x)) = 1 \wedge u(x) \mid v(x)w(x) \Rightarrow u(x) \mid w(x)$

Proof. (Proof of Fermat's Last Theorem for $\mathbb{R}[x]$] Suppose that $n \geq 3$, $a(x)^n + b(x)^n = c(x)^n$. WLOG we assume that $a(x), b(x), c(x) \neq 0$. So, if $\pi(x)$ is an irreducible factor of a(x):

$$\begin{aligned}
&\pi(x) \mid a(X) \\
\Rightarrow\ &\pi(x) \mid a(X)^n \\
\Rightarrow\ &\pi(x) \mid c(x)^n \Rightarrow \pi(x) && \mid c(x) \\
\Rightarrow\ &a(x) \text{ has no prime factors, so } a(x) \in \mathbb{R}
\end{aligned}$$

Similarly, $c(x) \in \mathbb{R}$

Consider the equation

$$a(x)^n + b(x)^n = c(x)^n \tag{9.3}$$
$$na(x)^{n-1}a'(x) + nb(x)^{n-1}b'(x) = nc(x)^{n-1}c'(x) \tag{9.4}$$

Multiplying (17.3) by $na'(x)$ and (17.4) by $a(x)$ and subtracting, we get that

$$na(x)^n a'(x) + nb(x)^n a'(x) = nc(x)^n a'(x) \tag{9.5}$$
$$na(x)^n a'(x) + nb(x)^{n-1}a(x)b'(x) = nc(x)^{n-1}a(x)c'(x) \tag{9.6}$$
$$nb(x)^{n-1}\left[b(x)a'(x) - a(x)b'(x)\right] = nc(x)^{n-1}\left[c(x)a'(x) - a(x)c'(x)\right] \tag{9.7}$$
$$\Rightarrow b(x)^{n-1}\left[b(x)a'(x) - a(x)b'(x)\right] = c(x)^{n-1}\left[c(x)a'(x) - a(x)c'(x)\right] \tag{9.8}$$
$$a(x)^{n-1}\left[a(x)b'(x) - b(x)a'(x)\right] = c(x)^{n-1}\left[c(x)b'(x) - b(x)c'(x)\right] \tag{9.9}$$

(17.8) $\Rightarrow b(x)^{n-1}c(x)^{n-1}\left[c(x)a'(x) - a(x)c'(x)\right] \wedge c(x)^{n-1} \mid b(x)^{n-1}\left[b(x)a'(x) - a(x)b'(x)\right]$

(17.9) $\Rightarrow a(x)^{n-1} \mid c(x)^{n-1}\left[c(x)b'(x) - b(x)c'(x)\right]$

Since $\gcd(b(x), c(x)) = 1 \Rightarrow \gcd(b(x)^{n-1}, c(x)^{n01}) = 1$

And so $b(x)^{n-1} \mid [c(x)a'(x) - a(x)c'(x)]$

Similarly, $c(x)^{n-1} \mid [b(x)a'(x) - a(x)b'(x)] \wedge a(x)^{n-1} \mid [c(x)b'(x) - b(x)c'(x)]$

Case I: If $c(x)a'(x) - a(x)c'(x) = 0$

By our lemma, we get that $c(x) = \lambda a(x), \lambda \in \mathbb{R} \setminus \varnothing$

But $\gcd(a(x), c(x)) = 1$ meaning that $a(x), c(x) \in \mathbb{R} \Rightarrow b(x) \in \mathbb{R}$

Similarly, if $b(x)a'(x) - a(x)b'(x) = 0 \vee c(x)b'(x) - b(x)c'(x) = 0$ we get a constant solution.

Case II: $c(x)a'(x) - a(x)c'(x) \neq 0 \wedge b(x)a'(x) - a(x)b'(x) \neq 0 \wedge c(X)b'(x) - b(x)c'(x) \neq 0$

We see that $c(x)a'(x) - a(x)c'(x) \neq 0 \Rightarrow b(x)^{n-1} \mid c(x)a'(x) - a(x)c'(x)$

We see that $\deg(b(x)^{n-1}) \leq \deg(c(x)a'(x) - a(x)c'(x)) \Rightarrow (n-1)\deg(b(x)) \leq \deg(c(x)) + \deg(a(x)) - 1$

So, we get

$$(n-1)\deg(b(x)) \leq \deg(c(x)) + \deg(a(x)) - 1 \tag{9.10}$$
$$(n-1)\deg(c(x)) \leq \deg(b(x)) + \deg(a(x)) - 1 \tag{9.11}$$
$$(n-1)\deg(a(x)) \leq \deg(b(x)) + \deg(c(x)) - 1 \tag{9.12}$$
$$\tag{9.13}$$

Adding them all up, we get

$$(n-1)\left[\deg(a(x))+\deg(b(x))+\deg(c(x))\right] \le 2\left[\deg(a(x))+\deg(b(x))+\deg(c(x))\right]-3,$$

a contradiction, as $2\left[\deg(a(x))+\deg(b(x))+\deg(c(x))\right] \not\le 2\left[\deg(a(x))+\deg(b(x))+\deg(c(x))\right]-3$ □

Lecture 29: Congruency of Polynomials

9.2 Equivalence Classes in Polynomials

Similarly to numbers, we can say that polynomials are congruent

Definition 9.8 (Congruency of Polynomials). We say that $a(x) \equiv b(x) \pmod{p(x)} \Leftrightarrow \exists c(x)$ such that $p(x) = c(x)a(x) + b(x)$

Notice. (i) It is reflexive: $a(x) \equiv a(x) \pmod{p(x)}$

(ii) It is symmetric: $a(x) \equiv b(x) \pmod{p(x)} \Rightarrow b(x) \equiv a(x) \pmod{p(x)}$

(iii) It is transitive: $a(x) \equiv b(x) \pmod{p(x)} \wedge b(x) \equiv c(x) \pmod{p(x)} \Rightarrow a(x) \equiv c(x) \pmod{p(x)}$

Let $[a(x)]_{p(x)} = \{b(x) \in F[x] : b(x) \equiv a(x) \pmod{p(x)}\}$

$[3]_5 = \{\dots, -2, 3, 8, 13, \dots\}$

$[x+1]_{x^2+x+1} = \{\dots, x+1, x^2+2x+2, x^3+x^2+2x+1, \dots\}$

Notation. Let $p(x) \neq 0 \in F[x]$.

We let $f[x]/p(x)$ denote the set of equivalence classes in $F[x]$ with regard to the equivalence relation $\equiv \pmod{p(x)}$.

$\mathbb{Z} \mapsto F[x]$

$\mathbb{Z}/m\mathbb{Z} \mapsto F[x]/p(X)$

Theorem 9.5. As a set,

$$F[x]/p(x) = \{[r(x)]_{p(x)} : \deg(r(x)) < \deg(p(x))\}$$

Furthermore, if $\deg(r_1(x)), \deg(r_2(x)) < \deg(p(x))$ then $[r_1(x)]_{p(x)} = [r_2(x)]_{p(x)} \Leftrightarrow r_1(x) = r_2(x)$

Proof. Notice by the division algorithm, if $a(x) \in F[x]$, then $\exists a(1), r(x) \in F[x], \deg(r(x)) < \deg(p(x))$ such that $a(x) = q(x)p(x) + r(x) \Rightarrow a(x) - r(x) = p(x)q(x) \Rightarrow a(x) \equiv r(x) \pmod{p(x)}$

And so, $[a(x)]_{p(x)} = [r(x)]_{p(x)}$

Next suppose that $\deg(r_1(x)), \deg(r_2(x)) < \deg(p(x))$

Then $[r_1(x)]_{p(X)} = [r_2(x)]_{p(x)} \Leftrightarrow r_1(x) \equiv r_2(x) \pmod{p(x)} \Leftrightarrow p(x) \mid (r_1(x) - r_2(x)) \Leftrightarrow r_1(x) - r_2(x) = 0 \Leftrightarrow r_1(x) = r_2(x)$ □

View $F[x]/p(x)$ as a ring.

Similarly to the integers, we have the lemma:

Lemma 9.4. Let $0 \neq p(x) \in F[x]$ and $a_1(x), \ldots, a_n(x), b(x), \ldots b_n(x) \in F[x]$

$$\begin{aligned} a_1(x) &\equiv b_1(x) \pmod{p(x)} \\ \wedge a_2(x) &\equiv b_2(x) \pmod{p(x)} \\ &\vdots \\ \wedge a_n(x) &\equiv b_n(x) \pmod{p(x)} \end{aligned}$$

means that

(*i*) $a_1(x) + a_2(x) + \cdots a_n(x) \equiv b_1(x) + b_2(x) + \cdots + b_n(x) \pmod{p(x)}$

(*ii*) $a_1(x)a_2(x)\cdots a_n(x) \equiv b_1(x)b_2(x)\cdots b_n(x) \pmod{p(x)}$

Exercise 9.2. Prove the lemma.

We thus see that this allows us to write $F[x]/p(x)$ "F[x] mod p(x)" as a ring:

Addition: $[a(x)]_{p(x)} + [b(x)]_{p(x)} = [a(x) + b(x)]_{p(x)}$

Multiplication: $[a(x)]_{p(x)} \cdot [b(x)]_{p(x)} = [a(x)b(x)]_{p(x)}$

$0 = [0]_{p(x)}, 1 = [1]_{p(x)}$

Question. Why is this well-defined?

Answer. Uf $[a_1(x)]_{p(x)} = [b_1(x)]_{p(x)} \wedge [a_2(x)]_{p(x)} = [b_2(x)]_{p(x)}$

Then $a_1(x) \equiv b_1(x) \pmod{p(x)} \wedge a_2(x) \equiv b_2(x) \pmod{p(x)}$

Which implies that $[a_1(x) + a_2(x)]_{p(x)} = [b_1(x) + b_2(x)]_{p(x)} \wedge [a_1(x)a_2(x)]_{p(x)} = [b_1(x)b_2(x)]_{p(x)}$

So, $[a_1(x)]_{p(x)} + [a_2(x)]_{p(x)} = [b_1(x)]_{p(x)} + [b_2(x)]_{p(x)}$, and similarly for multiplication.

Notation. $\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\} \cong \mathbb{F}_2 = \{0, 1\}$

Question. What is $\mathbb{F}_2[x]/(x^2 + x + 1)$ as a ring?

Answer. As a set, it is $\{[r(x)]_{x^2+x+1} : \deg(r(x)) < 2\} = \{[0]_{x^2+x+1}, [1]_{x^2+x+1}, [x + 0]_{x^2+x+1}, [x + 1]_{x^2+x+1}\}$

Lecture 30: I was sick

Chapter 10

Complex Numbers

10.1 Introduction

Lecture 31: More about complex numbers

Recap. $r(\cos(\theta) + i\sin(\theta) = re^{i\theta}) = a + bi, r = \sqrt{a^2 + b^2}$

Solve for θ using the inverse trigonometric functions.

$e^{i\theta} + e^{i\psi} = e^{i\theta+\psi} \Rightarrow (\cos(\theta) + i\sin(\theta))(\cos(\psi) + i\sin(\psi)) = \cos(\theta + \psi) + i\sin(\theta + \psi)$

From this we can derive the sine and cosine addition identities. All trigonometric identities can be derived similarly.

$1 = e^{i\theta}e^{-i\theta} = (\cos(\theta) + i\sin(\theta))(\cos(-\theta) + i\sin(-\theta)) = \cos^2(\theta) + \sin^2(\theta)$

Definition 10.1 (The Unit Circle)**.** Let $S' = \{e^{i\theta} : \theta \in [0, 2\pi)\}$

This is the unit circle, and is an abelian group under multiplication.

Theorem 10.1 (De Moivre's Formula)**.** For $n \in \mathbb{N}, (\cos(\theta) + i\sin(\theta))^n = e^{in\theta} = \cos(n\theta) + i\sin(n\theta)$

By the binomial theorem, we also have
$(\binom{n}{0}(\cos(\theta))^n - \binom{n}{2}(\cos(\theta))^{n-2}(\sin(\theta))^2 + \binom{n}{4}(\cos(\theta))^{n-4}(\sin(\theta))^4 - \cdots)$
$+ i(\binom{n}{1}(\cos(\theta))^{n-1}(\sin(\theta)) - \binom{n}{3}(\cos(\theta))^{n-3}(\sin(\theta))^3 + \cdots)$

Note. Comparing the real and imaginary parts of the formulas, we get that

$$\cos(n\theta) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} (\cos(\theta))^{n-2j}(-1)^j \binom{n}{2j}(\sin(\theta))^{2j}$$

$$\sin(n\theta) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{1+2j}(\cos(\theta))^{n-1-2j}(\sin(\theta))^{1+2j}(-1)^j$$

We write $\cos(n\theta) = T_n(\cos(\theta)), T_n(x) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} x^{n-2j}(-1)^j \binom{n}{2j}(1 - x^2)^j$

This is known as the n-th Chebyshev polynomial.

Question. What are the roots of $x^n - 1 = 0$ in $\mathbb{C}$?

Answer. $e^{2\pi ij/n}$ is a root for $j = 0, 1, \ldots, n-1$

Definition 10.2 (Roots of Unity)**.** A number $Z \in \mathbb{C}$ that satisfies $z^n - 1 = 0$ is called an n-th root of unity and if n is the smallest positive number such that $z^n = 1$, we call z a primitive n-th root of unity.

Definition 10.3 (Algebraically Closed)**.** A field F is called algebraically closed if, whenever $\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in F[x]$ is a non-constant polynomial, we can factor it completely into linear terms over F.

Example 10.1. $\mathbb{R}$ is not algebraically closed: $x^2 + 1$

$\mathbb{Q}$ is not algebraically closed

$\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$ is not algebraically closed.

In general, $\mathbb{F}_p$ is not algebraically closed, p prime.

$\mathbb{C}$ is algebraically closed, i.e. if $p(z) \in \mathbb{C}[z]$ is non-constant then $\exists c \in \mathbb{C} \Rightarrow p(c) = 0$

Lecture 32: More with the Fundamental Theorem of Algebra

Note. From the Fundamental Theorem of Algebra, we have:

Let $p(z) \in \mathbb{C}[z]$ be a non-constant polynomial. Then $\exists c \in \mathbb{C}$ such that $p(c) = 0$.

We derive the following corollary from it:

Corollary 10.1 (Unique Factorization of Polynomials in $\mathbb{C}$)**.** Then $\exists C \in \mathbb{C}, c_1, \ldots, c_n \in \mathbb{C}$ such that $p(z) = C(z - c_1)(z - c_2) \cdots (z - c_n)$

Proof. We prove this using induction on n.

Base case: $n = 1 \Rightarrow p(z) = Cz + c_1 = C(z + \frac{c_1}{C})$

Assume this holds whenever $n < d$ and consider $p(z)$ of degree d.

By the FTA, $\exists c_1 \in \mathbb{C}$ such that $p(c_1) = 0$ and we claim that this means that $z - c_1 \mid p(z)$.

To see this, we use the division algorithm to see that $\exists q(z)$ of degree $d - 1$ and $r \in \mathbb{C}$ such that $p(z) = (z - c_1)q(z) + r$. Plugging in $z = c_1$, we get that the LHS $= 0$, so RHS $= 0$, and thus $r = 0$.

And so $p(z) = (z - c_1)q(z)$. Since $\deg(q(z)) = d - 1 < d$, the induction hypothesis holds, and the result follows by induction. □

We now want to prove that all polynomials have roots:

Our strategy:

(i) Let $p(z) \in \mathbb{C}[z]$ be non-constant and show that $|p(z)|$ achieves a global minimum at some point $z = c$.

(ii) Make a change of variables and assume $c = 0$

(iii) Show that $p(0) = 0$

Proof. (Of (i)) Let $p(z) = c_0 + c_1 z + \cdots + c_{n-1}z^{d-1} + c_d z^d$

Notice we assume WLOG that $c_d = 1$ by scaling, and assume $c_0 \neq 0$.

Let $M = \max(1, |c_0|, |c_1|, \ldots, |c_{d-1}|)$

Consider $|p(z)|$when $|z| > 2Md$:

$$\begin{aligned}
|p(z)| &= |z^d + c_{d-1}z^{d-1} + \cdots + c_1 z + c_0| \\
&\geq |z^d| - |c_{d-1}z^{d-1} + \cdots + c_1 z + c_0| \\
&\geq |z|^d - |c_{d-1}z^{d-1}| - \cdots - |c_1 z| - |c_0| \\
&= |z|^d - |c_{d-1}||z|^{d-1} - \cdots - |c_1||z| - |c_0| \\
&\geq |z|^d - M|z|^{d-1} - M|z|^{d-2} - \cdots - M|z| - M \\
&\geq |z|^d - M|z|^{d-1} - \cdots - M|z|^{d-1} && \because |z| \geq 1 \\
&= |z|^d - dM|z|^{d-1} \\
&= |z|^{d-1}(|z| - dM) \\
&> |z|^{d-1} \cdot dM && \because |z| > 2dM \\
&\geq dM && \because |z| \geq 1 \\
&\geq |p(0)| = |c_0|
\end{aligned}$$

This means that $|p(z)| > |p(0)|$

By the Extreme Value Theorem, $|p(z)|$ achieves a minimum at some point $z = c$ in the closed, bounded set $\{z \in \mathbb{C} : |z| \leq 2Md\}$

Notice that c is a global minimum. To see this, notice that if $|z| \leq 2Md \Rightarrow |p(z)| \geq |p(c)|$ by definition, and vice versa as we showed if $|z| > 2Md$ □

For (ii), we simply let $x = z - c$, making $|p(x)|$ has a global minimum at $x = 0 \Rightarrow z = c$

We thus write $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + c_d x^d$ and WLOG assume $a_0 = 1 \neq 0$

Thus, write $p(x) = 1 + a_k x^k + \cdots + a_d x^d, a_k \neq 0$

Remark. If $z \neq 0 \in \mathbb{C}$, the equation $x^k = z$ has exactly k solutions.

Proof. Write $z = re^{i\theta}, r > 0, \theta \in [0, 2\pi]$

$y := r^{\frac{1}{k}} \cdot e^{\frac{i\theta}{r}}, y^k = z$

Notice that $ye^{\frac{2\pi ij}{k}}$ is a solution, $j = 0, 1, \ldots k - 1$ □

Now pick $y_0 \in \mathbb{C}$ such that $y_0^k = -\overline{a_k} \in \mathbb{C}$

Consider $p(y_0 t), t \to 0^+$

$$\begin{aligned}
p(y_0 t) &= 1 + a_k + y_0^k t^k + a_{k+1}y_0^{k+1}t^{k+1} + \cdots + a_d y_0^d t^d \\
&= 1 + a_k(-\overline{a_k})t^k + a_{k+1}y_0^{k+1}t^{k+1} + \cdots + a_d y_0^d t^d \\
&= 1 - |a_k|^2 t^k + b_{k+1}t^{k+1} + \cdots + b_d t^d
\end{aligned}$$

And we see that this becomes slightly less than one as $t \to 0^+$

We write $\frac{p(y_0 t) - 1}{t^k} = -|a_k|^2 + b_{k+1}t^1 + \cdots + b_d t^{d-k} \to -|a_k|^2 < 0, t \to 0^+$

So for t sufficiently close to 0 and positive, $|\varepsilon(t)| < \frac{|a_k|^2}{2}$

This implies that for t sufficiently small and positive, we get that

$$\begin{aligned}|p(y_0t)| &= |1 - |a_k|^2t^k + t^k\varepsilon(t)| \\ &\leq |1 - |a_k|^2t^k| + |t^k\varepsilon(t)| \\ &= 1 - |a_k|^2t^k + \frac{|a_k|^2}{2}t^k \\ &= 1 - \frac{|a_k|^2}{2}t^k < 1 = |p(0)|\end{aligned}$$

10.2 Finite Fields

Lecture 33: Finite Fields

Theorem 10.2 (Size of Finite Fields). Every finite field has size p^n for some prime p and some $n \geq 1$.

Moreover $\forall p \in$ primes $\forall n \geq 1 \exists$ a field of size p^n.

Definition 10.4 (Vector Spaces). Let F be a field. An abelian group $(V, +)$ is called an F-vector space if $\exists$ a map $\cdot : F \times V \to V$ (called scalar multiplication) such that

(i) $1 \cdot v = v \forall v \in V, (1 \in F)$

(ii) $(\alpha + \beta) \cdot v = \alpha \cdot v + \cdot v \forall v \in V, \alpha, \beta \in F$

(iii) $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2 \forall \alpha \in F, v_1, v_2 \in V$

(iv) $(\alpha \cdot \beta) \cdot V = \alpha \cdot (\beta \cdot v) \forall \alpha, \beta \in F, \forall v \in V$

Example 10.2. $\mathbb{R}^3 = \{(a_1, a_2, a_3) \because a_1, a_2, a_3 \in \mathbb{R}\}$

$(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$ is an $\mathbb{R}-$vector space.

$\lambda \cdot (a_1, a_2, a_3) = (\lambda a_1, \lambda a_2, \lambda a_3)$

Example 10.3. $\mathbb{C} is an \mathbb{R}$-vector space

$\lambda \in \mathbb{C}, a + bi \in \mathbb{C} \Rightarrow \lambda \cdot (a + bi) = \lambda a + \lambda bi$

In general, if $F \subseteq k$ are both fields and F is a subfield of K, then k is a vector space over F with $\lambda \cdot v = \lambda v$

Definition 10.5 (Linear Independence). Let F be a field and let V be an $F-$vector space.

We say that a subset $S = \{s_1, \ldots, s_n\} \subseteq V$ is F-linearly independent if the only solution to the equation

$$x_1s_1 + x_2s_2 + \cdots + x_ns_n = 0$$

with $x_1, \ldots, x_n \in F$ is $x_1 = x_2 = \cdots = x_n = 0$

Definition 10.6 (Spanning). We say that a set $S = \{s_1, \ldots, s_n\} \subseteq V$ spans V if $\forall v \in V$ we can write $v = \lambda_1 s_1 + \cdots + \lambda_n s_n$ for some $\lambda_1, \ldots, \lambda_n \in F$.

Definition 10.7 (Bases). We say that S is a basis for V if $S \subseteq V$ and S spans V, and S is F-linearly independent.

Theorem 10.3. Let K be a finite field. Then $\exists$ prim p and $n \geq 1$ such that $|K| = p^n$

Proof. Recall that $\text{char}(K) = \{\text{smallest} : 1 + \cdots + 1 = 0\}$ is a prime number if it exists.

So $\exists$ prime p such that $\{0, 1, \ldots, p-1\} \subseteq K$

This means that K is an $\mathbb{F}_p$-vector space.

Claim 10.1. $\exists$ a basis S for K as an $\mathbb{F}_p$-vector space

Proof. Consider all $\mathbb{F}_p$-linearly independent subsets of K and pick $S \subseteq K$of maximal size. $\because K$ is finite, therefore it will exist. □

We now show that S spans K as an $\mathbb{F}_p$-vector space.

To do this, we argue by contradiction: Suppose that S doesn't span K. Then $\exists c \in K$ such that $\nexists$ a solution to the equation $c = x_1 s_1 + \cdots x_n s_n$ with $x_1, \ldots, x_n \in \mathbb{F}_p$ where $S = \{s_1, \ldots, s_n\}$

Now notice that $S \cup \{c\} = \{s_1, \ldots, s_n, c\}$ is $\mathbb{F}_p$-linearly independent because if it is not then $\exists x_1, \ldots, x_n, x_{n+1} \in \mathbb{F}_p$, not all zero, such that $x_1 s_1 + \cdots + x_n s_n + x_{n+1} c = 0$

Notice that if $x_{n+1} = 0$ then we have $x_1 s_1 + \cdots + x_n s_n = 0 \Rightarrow x_1 = \cdots = x_n = 0 \because S = \{s_1, \ldots, s_n\}$ is $\mathbb{F}_p$-linearly independent.

But this contradicts our assumption that not all of them are 0. So, $x_{n+1} \neq 0, x_{n+1} c = -x_1 s_1 - \cdots - x_n s_n$

We thus multiply both sides by x_{n+1}^{-1}

$c = (-x_1 x_{n+1}^{-1}) s_1 + \cdots + (-x_n x_{n+1}^{-1}) s_n$, meaning c is in the span of $\{s_1, \ldots, s_n\} = S$ and thus S spans k as an $\mathbb{F}_p$-vector space, and thus S is a basis for K, which is a contradiction to our assumption.

We now claim that $|K| = |\mathbb{F}_p|^{|S|} = p^n$

To see this, consider the function $f : \mathbb{F}_p \times \mathbb{F}_p \times \cdots \times \mathbb{F}_p \to K$ given by $f((x_1, x_2, \ldots, x_n)) = x_1 s_1 + \cdots + x_n s_n$.

Notice that f is onto because S spans. But f is also one to one because if

$$\begin{aligned}
f((y_1, \ldots, y_n)) &= f((z_1, \ldots, z_n)) \\
&\Rightarrow y_1 s_1 + \cdots y_n s_n = z_1 s_1 + \cdots z_n s_n \\
&\Rightarrow (y_1 - z_1) s_1 + \cdots (y_n - z_n) s_n = 0 \\
&\Rightarrow y_1 - z_1 = \cdots = y_n - z_n = 0 \\
&\Rightarrow y_1 = z_1, \ldots, y_n = z_n \\
&\Rightarrow f \text{ is one to one}
\end{aligned}$$

Thus, $|K| = |\mathbb{F}_p \times \mathbb{F}_p \times \cdots \times \mathbb{F}_p| = p^n$ □

Lecture 34: More on Finite Fields

Theorem 10.4 (Size of a Field). If F is a finite field, then there exists a prime number p and an $n \in \mathbb{N}$ such that $|F| = p^n$

Conversely, for every prime p and every $n \in \mathbb{N}$, there exists a field of size exactly p^n

Notation. If $F \subseteq K$ are both fields, and F is a subfield of K, then we say that K is an extension of F.

Definition 10.8 (Splitting)**.** Let $F \subseteq K$, where K extends F.

We say that $p(x) \in F(x)$ splits over K if there exists $n \geq 1, \lambda_1, \cdots, \lambda_n \in K$ such that $p(x)= C(x-\lambda_1)\cdots(x-\lambda_n)$ for some $C \in K \setminus 0$

Theorem 10.5. Let F be a field and let $p(x) \in F[x]$ be a nonzero polynomial of degree ≥ 1. Then, there exists an extension K of F such that $p(x)$ splits over K.

Recall that if $p(x)$ is irreducible in $F[x]$ then $K = F[x]/p(x)$ is an extension of F and $p(X)$ has a root in K.

Notice. $F \subseteq K \Rightarrow [x]_{p(x)}$ is a root of $p(x)$.

$p(x) = c_0 + c_1 x + \cdots + c_d x^d$

$$\begin{aligned} p([x]_{p(x)}) &= c_0[x]^0_{p(x)} + \cdots + c_d[x]^d_{p(x)} \\ &= [c_0 + c_1 x + \cdots + c_d x^d]_{p(x)} \\ &= [p(x)]_{p(x)} \\ &= [0]_{p(x)} \end{aligned}$$

Proof. (Of Theorem 18.5) We prove this by induction on $\deg(p(x))$

Base Case: $\deg(p(x)) = 1 \Rightarrow p(X) = a(x + \frac{b}{a})$

Thus, $K = F$

Now assume that the claim holds whenever $\deg(p(x)) < n, n \geq 2$

Consider the case when $\deg(p(x)) = n$, we write $p(X) = q(x)a(x)$ with $q(x)$ irreducible and $a(x) \in F[x]$.

Notice that $q(x)$ has a root in $K = fx \setminus q(x)$ which is an extension of F.

$F \subseteq K$ and notice that $a(x)$ has a root a in K. This means that in $K[x]$ we can factor $q(x)$ as $(x-a)q_1(x), q_1(x) \in K[x]$

So $p(x) = (x-a)q_1(x)a(x)$ in $K[x]$

Notice that $\deg(q_1(x)a(x)) = \deg(p(x)) - 1 = n - 1 < n$ and so by the induction hypothesis there is an extension E of K such that $q_1(x)a(x)$ splits.

So in $E[x], q_1(x)a(x) = C(x-\lambda_1)\cdots(x-\lambda_{n-1}) \in E[x] \Rightarrow p(x) = (x-C)q_1(x)a(x) = C(x-\lambda_1)\cdots(x-\lambda_{n-1})(x-c)$. meaning that $p(x)$ splits over E □

Corollary 10.2. Let p be prime and $n \geq 1$, then there exists a field of size p^n.

Proof. Let $F = \mathbb{F}_p = \{0, 1, \ldots, p-1\}$

Consider $x^{p^n} - x \in F[x]$. Let K be an extension of F such that $x^{p^n} - x$ splits over K. Such a K is guaranteed to exist by Theorem 18.5.

Let $E \subseteq K$ be the set of roots of $x^{p^n} - x$

Claim 10.2. E is a field.

Proof. To so that it is a field, it suffices that $E \subseteq K$ is a subfield.

To do this, it suffices to show that

(i) $0, 1, -1 \in E$

(ii) $a, b \in E \Rightarrow a \cdot b \in E, a + b \in E$

(iii) $a \in E \wedge a \neq 0 \Rightarrow a^{-1} \in E$

Remark. If L is a field of $\text{char}(p) > 0$, p is prime, then $(a+b)^p = a^p + b^p \forall a, b \in L$

Proof. $(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p = a^p + b^p$ □

Thus, $(a+b)^{p^2} = (a^p + b^p)^p = a^{p^2} + b^{p^2}$.

Proof. (of (i)) $0^{p^n} - 0 = 0$

$1^{p^n} - 1 = 0$

$(-1)^{p^n} + 1 = 0$ □

Proof. (of (ii)) If $a, b \in E \Rightarrow a^{p^n} - a = 0, b^{p^n} - b = 0$

$\Rightarrow a^{p^n} + b^{p^n} - a - b = 0 \Rightarrow (a+b)^{p^n} - (a+b) = 0 \Rightarrow a + b \in E, (ab)^{p^n} = ab \Rightarrow ab \in E$ □

Proof. (of (iii)) If $a \in E \wedge a \neq 0, a^{p^n} - a = 0 \Rightarrow \frac{1}{a} \in E$ □

If thus follows that $E \subseteq K$ is a subfield and thus E is a field of size $\leq p^n$. □

To show that $|E| = p^n$ we must show that $x^{p^n} - x$ has no repeated roots.

To do this, we use a theorem:

Theorem 10.6. Let $q(x) \in F[x]$. If $\gcd(q(x), q'(x)) = 1$ then $q(x)$ has distinct roots.

$q(x) = x^{p^n} - x \Rightarrow q'(x) = p^n x^{p^{n-1}} - 1 = -1 \Rightarrow \gcd(q(x), q'(x)) = 1$

This means that $q(x)$ has no repeated roots, which means that $\lambda_1, \ldots, \lambda_{p^n}$ are pairwise distinct, which means that $|E| = p^n$, as desired. □

Lecture 35: Wrapping up Finite Fields

Recap. We covered and proved conditionally Theorem 18.5, and also proved that $p(x) = C(x - \lambda_1) \cdots (x - \lambda_n) \in K[x]$ has no repeated roots if and only if $\gcd(p(x), p'(x)) = 1$

For $p(x) = p_0 + p_1 x + \cdots + p_n x^n \in F[x]$, we define $p'(x) = p_1 + 2p_2 x + \cdots + np_n x^{n-1} \in F[x]$

Definition 10.9 (Product Rule). If $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$ Then, $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

Proof.

$$\begin{aligned}
f(x)g(x) &= \left(\sum_{i=0}^{m} a_1x^i\right)\left(\sum_{j=0}^{n} b_jx^j\right) \\
&= \sum_{i=0}^{m}\sum_{j=0}^{n} a_ib_jx^{i+j} \\
(f(x)g(x))' &= \sum_{i=0}^{m}\sum_{j=0}^{n}(i+j)a_ib_jx^{i+j-1} \\
&= \left(\sum_{i=0}^{m}\sum_{j=0}^{n} ia_ib_jx^{i+j-1}\right) + \left(\sum_{i=0}^{m}\sum_{j=0}^{n} ja_ib_jx^{i+j-1}\right) \\
&= \sum_{i=0}^{m} ia_ix^{i-1}\sum_{j=0}^{n} b_jx^j + \sum_{i=0}^{m} a_ix^i\sum_{j=0}^{n} jb_jx^{j-1} \\
&= f'(x)g(x) + f(x)g'(x)
\end{aligned}$$

□

Proof. (Repeated Roots) Suppose that $p(x)$ has a repeated root. Then, $\exists\lambda$ such that $p(x) = (x-\lambda)^2q(x)$

Thus, $p'(x) = 2(x-\lambda)^2q(x) + (x-\lambda)^2q'(x) = (x-\lambda)(2q(x) + (x-\lambda)q'(x))$

And so $p(\lambda) = 0, p'(\lambda) = 0$ and thus $\gcd(p(x), p'(x)) \neq 1$

Now we show the other direction.

Suppose that $\gcd(p(x), p'(x)) \neq 1$. Then $\exists \gcd d(x)$ of deg ≥ 1

By definition, $d(x) \mid p(x) \wedge d(x) \mid p'(x)$ and since $p(x)$ splits by assumption, so thus $d(x)$ and thus $\exists\lambda$ in our field such that $(x-\lambda) \mid p(x) \wedge (x-\lambda) \mid p'(x)$.

Now we write $p(x) = (x-\lambda)q(x) \Rightarrow p'(x) = q(x) + (x-\lambda)q'(x)$

By assumption, $(x-\lambda) \mid p'(x) \Rightarrow (x-\lambda) \mid q(x) \Rightarrow p(x) = (x-\lambda)(x-\lambda)r(x)$ □

Chapter 11

Extracurricular!

Definition 11.1 (Division Rings)**.** A division ring D is a ring satisfying all the field axioms except for possibly the axiom stating that multiplication is commutative.

$\{\text{Fields}\} \subseteq \{\text{Division Rings}\}$

Definition 11.2 (Quaternions)**.** As a set, they are given by

$$\mathbb{H} = \{\alpha \cdot 1 + \beta \cdot i + \gamma \cdot j + \xi \cdot k : \alpha\beta, \gamma, \xi \in \mathbb{R}\}$$

$+(a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k) = (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k$

$i^2 = j^2 = k^2 = -1, ij = -ji = k$

Definition 11.3 (Adjoint)**.** Given $z = \alpha + \beta i + \gamma j + \xi k$ we define $Z^* = \alpha - \beta i - \gamma j - \xi kalpha$ as the adjoint of Z.

Theorem 11.1. For $u, v \in \mathbb{H}$

(i) $(u^*)^* = u$

(ii) $(uv)^* = v^* u^*$

(iii) $N(u) := uu^* \in [0, \infty)$

$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$

Lecture 36: The Final Lecture

Note. 5 questions, 10 points each. Entire exam out of 50 marks.

Question 1: 5 short answer questions, with 2 points each.

Question 2: 5 t/f questions, with 2 points each. Just like midterm, 1 point for correctness, 1 point for justification.

Question 3: Number Theory; linear Diophantine equations, Sun-Zi's Theorem, EEA, unique factorization, Wilson & Fermat, etc. 2 + 2 + 2 + 4 marks.

Question 4: Fields. a) Complex Numbers (4 marks), b), c) Finite Fields (6 marks) <- "You should be

> able to get 2 marks very quickly if you understand the assignments"
>
> Question 5: Groups. a) (3 marks), b) (2 marks), c) (5 marks), c) is hardest.
>
> Bonus: Groups (2 points), marked harshly.
>
> There is no RSA or key-exchanging, but time complexity is fair game.
>
> No tutorial content, except possibly on the bonus question. You are allowed to use it.

$k = \mathbb{F}_3[x]/p(x), p(x) = x^3 + ax + bx + c$ and is irreducible.

$|k| = \{[a\alpha x^2 + \beta x + \gamma]_{p(x)} : \alpha, \beta, \gamma \in \mathbb{F}_3\}$

$p(0) = 0 \Leftrightarrow c = 0, \Rightarrow$ we need $c \neq 0 . p(1) = 0 \Leftrightarrow 1 + a + b + c = 0 \Rightarrow$ we need $1 + a + b + c \neq 0$. $p(-1) = 0 \Leftrightarrow -1 + a - b + c = 0 \Rightarrow -1 + a - b + c \neq 0 \Rightarrow c = 1, 2 + a + b \neq 0, a - b \neq 0 \Rightarrow c = 1, a = 0, b = 2$

$\mathbb{F}_3[x]/(x^3 + 2x + 1)$

Definition 11.4 (Algebraic Numbers). A number $\alpha \in \mathbb{C}$ is algebraic if there exists a nonzero polynomial $p(x) \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$

Definition 11.5 (Transcendental Numbers). A number $\alpha \in \mathbb{C}$ is transcendental if it is not algebraic.

Theorem 11.2 (Liouville's Theorem). The number $\alpha := \frac{1}{10^1} + \frac{1}{10^2} + \frac{1}{10^6} + \frac{1}{10^{24}} + \frac{1}{10^{120}} + \cdots = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.

Lemma 11.1. Let $p(x) = c_0 + c_1 x + \cdots + c_d x^d \in \mathbb{Z}[x]$ and suppose that $\frac{a}{b} \in \mathbb{Q}, a, b \in \mathbb{Z}, b > 0$ and then suppose either $p(\frac{a}{b}) = 0$ or $|p(\frac{a}{b})| > \frac{1}{b^d}$

Proof. $p(\frac{a}{b}) = c_0 + c_1(\frac{a}{b}) + \cdots + c_d(\frac{a}{b})^d = \frac{c_0 b^d + c_1 a b^{d-1} + \cdots + c_d a^d}{b^d} = \frac{A}{b^d}, A \neq 0 \in \mathbb{Z}$

Then $|p(\frac{a}{b})| = |\frac{A}{b^d}| \geq \frac{1}{b^d}$ □

Proof. (Liouville's Theorem) Suppose towards a contradiction that α is not transcendental.

Then there exists a nonzero polynomial $p(x)$ such that $p(\alpha) = 0$

Let $\alpha_n = \frac{1}{10^1} + \cdots + \frac{1}{10^{n!}}$

Then $\alpha_n = \frac{A_n}{10^{n!}}$ for some $A_n \in \mathbb{N}$

Notice that $p(\alpha_n) \neq 0$ for all sufficiently large $n \in \mathbb{N}$.

Use the lemma. $|p(\alpha_n)| \geq \frac{1}{10^{n!d}}$, so this holds for all sufficiently large n.

Notice $|\alpha - \alpha_n| = |\sum_{i=1}^{\infty} \frac{1}{10^{i!}} - \sum_{i=0}^{n} \frac{1}{10^{i!}}| = \sum_{i=n+1}^{\infty} \frac{1}{10^{i!}} = \frac{1}{10^{(n+1)!}} + \cdots \leq \frac{1}{10^{(n+1)!}} + \frac{1}{2 \cdot 10^{(n+1)!}} + \cdots = \frac{2}{10^{(n+1)!}}$

So $0 < |\alpha - \alpha_n| \leq \frac{2}{10^{(n+1)!}}$

Let $M = \max_{\{x : |x - \alpha| \leq 1\}} |p'(x)|, |\alpha_n - \alpha| \leq 1 \forall n \geq 1$

So for sufficiently large $n, p(\alpha_n) \neq 0$ and so $\frac{1}{10^{n! \cdot d}} \leq |p(\alpha_n)| \forall n$ sufficiently large.

By the MVT, $|\frac{p(\alpha)-p(\alpha_n)}{-\alpha_n}| = |p'(c)| \leq M$ for some $c \in (\alpha_n, \alpha)$

$\Rightarrow |p(\alpha) - p(\alpha_n)| \leq M|\alpha - \alpha_n| \leq \frac{2M}{10^{(n+1)!}} \Rightarrow |p(\alpha_n)| \leq \frac{2M}{10^{(n+1)!}}$

So if we combine these inequalities, $\frac{1}{10^{n!\cdot d}} \leq |p(\alpha_n)| \leq \frac{2M}{10^{(n+1)!}}$ for all sufficiently large n

$\Rightarrow \frac{1}{10^{n!\cdot d}} \leq \frac{2M}{10^{(n+1)!}} \forall n$ sufficiently large

$\Rightarrow 1 \leq \frac{2M\cdot 10^{n!\cdot d}}{10^{(n+1)!}} = \frac{2M}{10^{n!(n+1-d)}} \to 0$ which is a contradiction, the final one of this course. □