1 Day 2

Definition 1. A ring is a commutative ring with unity.

Definition 2. A field is a ring where every non-zero element has a multiplicative inverse

The first ring we'll examine is $\mathbb{Z}$, which is the ring of integers

Definition 3. Let R be a ring, with $a, b \in R$. We say that a divides b if,

$$c * a = b$$

and introduce the following notation,

$$a|b$$

- Transitivity: This satisfies transitivity as, a divides b and b divides c implies that a divides c.
- Note:

$$\begin{aligned} &a|a \\ &a|b \wedge a|(b+c) \implies a|c \\ &a|b \wedge b|a \not\implies a = b \end{aligned}$$

Definition 4. Let $p \in \mathbb{Z}$, p is called prime if $p > 0$ and the divisors of p are 1 and p, with $1 \neq p$

Fact: $\forall n \geq 2,\ \exists\, p_1, \ldots, p_k$, where $p_1, \ldots, p_k$ are prime, such that $n = p_1 p_2 \ldots p_k$

Proof. If n is prime, then we are done.
If n is not prime, then it follows that,

$$\begin{aligned} a|n &\implies n = ab \\ &\implies a, b < n \\ &\implies a = p_1 p_2 \ldots p_k \\ &\implies b = q_1 q_2 \ldots q_k \\ &\implies n = p_1 p_2 \ldots p_k q_1 q_2 \ldots q_k \end{aligned}$$

□

Theorem 1. There are infinitely many primes.

Proof. Assume that there are finitely many primes, $p_1, \ldots, p_k$. Suppose, towards contradiction that we have $n = p_1 p_2 \ldots p_k + 1$. Then there exists a prime $q|n$, but $p_i \neq q$ since every p_i division leaves a remainder. □

An alternative approach can be seen,

Proof.

$$2 < 3 < 5 < 7 < 11 < \ldots < p < \cdots < q < \ldots$$
$$p_1 < p_2 < p_3 < \ldots$$
$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \cdots + \frac{1}{p_k} = \infty$$

Which somehow follows from,

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$$

Beats me. □

Fact: $\forall N \in \mathbb{N}$ there exists a prime p, such that $q - p > N$ where q is the next prime. (We can make this claim about there being a next prime, thanks to the well ordering principle, where any non-empty subset of $\mathbb{N}$ has a smallest element.)
$\iff$ There exist composite numbers (non-primes),

$$n, n+1, \ldots, n+L,\ L \geq N$$
$$(L+1)! + 2, (L+2)! + 3, \ldots, (L+1)! + L, (L+1)! + (L+1)$$

(This baffles me.)
Conjecture: The Twin-prime conjecture suggests that there are infinitely many pairs of primes of the form $p, p+2$

Definition 5. Given $a, b \in \mathbb{Z}$, the Greatest Common Divisor is defined as such,

$$gcd(a, b) := \text{The largest common divisor, thanks goobz}$$

The Euclidean Algorithm is as such,

$$\exists a, b \in \mathbb{Z},\ b \neq 0$$
$$\nexists y, r,\ s.t.\ a = qb + r, 0 \leq r \leq |b|$$

Proof. Without loss of generalty, $b > 0$,

Number line, with b on it

- $\{a - qb : q \in \mathbb{Z}\}$ contains non-negative integers. Looking at the subset of non-negatives, or $\{a - qb | q \in \mathbb{Z},\ a - q \geq 0\}$ we can select a smallest element, thanks to the well ordering principle. We'll call this r, giving

$$a - qb = r$$
$$a = qb + r$$

- Algorithm for finding $gcd(a, b)$,

$$a = q_1 b + r_1$$

if $r_1 = 0$ then $gcd(a, b) = |b|$. If $r_1 \neq 0$, then,

$$b = q_2 r_1 + r_2 r_1 = \dots$$

Apparently, we know this. Great. It has been proven. Libtards(me) owned by facts and logic.

$\square$

Theorem 2.

$$gcd(a, b) = xa + yb, \text{ for some } x, y \in \mathbb{Z}$$

<u>Example:</u>

$$\begin{aligned} gcd(18, 22) = 2 \\ &= x * 18 + y * 22 \\ &= (x + 22) * 18 + (y - 18) * 22 \\ &= 5 * 18 + (-4) * 22 \end{aligned}$$

<u>Fact:</u>

$$a_1, a_2, \dots, a_n \in \mathbb{Z}, \text{where not all are 0}$$

Then,

$$\begin{aligned} gcd(a_1, \dots, a_n) &= x_1 a_1 + \dots + x_n a_n \\ &= gcd(gcd(a_1, \dots, a_{n-1}) a_n) \\ &= min(x_1 a_1 + \dots + x_n a_n | x_1, \dots, x_n \in \mathbb{Z},\ x_1 a_1 + \dots + x_n a_n > 0) \end{aligned}$$

2 Day 3

Theorem 3. Every natural number $n \geq 2$ factors uniquely into primes, or,

$$\begin{aligned} \exists p_1, \dots, p_k\ p_i \neq p_j \forall i, j \text{ (all primes)} \\ \exists a_1, \dots, a_k \\ n = p_1{}_1^a \dots p_k{}_k^a \end{aligned}$$

Moreover if

$$n = {q_1}^{b_1} \dots {q_l}^{b_l}$$

where q_i-primes ($q_i \neq q_j$). Then $k = l$ and there is a permutation,

$$(i_1, \ldots, i_k)\text{of}\{1, \ldots, n\}$$

with

$$a_t = b_i t$$
$$p_t = q_i t$$

2.1 Extension to rings:

Let R be a commutative ring with unity. $p \in R$ is prime. If $p = ab$, the following is implied

- a is invertible in R
- ab is invertible in R

Definition 6. A ring, R is a Unique Factorization Domain (U.F.D) if every $a \in R$ with $a \neq 0$, factors into primes,

$$a = p_1 \ldots p_k$$

and for any other factorization,

$$a = q_1 \ldots q_l$$

we have $k = l$ and, up to enumeration $p_i = u_i q_i$ for some u_i invertible in R

Definition 7. $\mathbb{Z}[i]$ is the smallest ring containing both $\mathbb{Z}$ and i

Proof. Let $\mathbb{Z}_{\geq 0} = \{0, 1, \ldots\}$

$$\bigoplus_{i=1}^{\infty} \mathbb{Z}_{\geq 0} = \{(a_1, a_2, \ldots)|a_i \in \mathbb{Z}_{\geq 0},\ \text{(finitely many are non-zero)}\}$$
$$\alpha, \beta \in \bigoplus_{i=1}^{\infty} \mathbb{Z}_{\geq 0},\ \alpha + \beta = (a_1 + b_1, a_2 + b_2, \ldots)$$

Where $\alpha = (a_1, a_2, \ldots)$ and $\beta = (b_1, b_2, \ldots)$. We can totally order $\bigoplus_{i=1}^{\infty} \mathbb{Z}_{\geq 0}$ i.e. we can introduce a relation with, $\leq$ between the $\bigoplus_{i=1}^{\infty} \mathbb{Z}_{\geq 0}$

1. $\alpha \leq \alpha$
2. $\alpha \leq \beta \ \&\ \beta \leq \alpha \implies \alpha = \beta$
3. $\alpha \leq \gamma \implies \alpha \leq \gamma$
4. $\alpha \leq \beta,\ \forall \gamma,\ \alpha + \gamma \leq \beta + \gamma$
5. $\forall \alpha, \beta,\ \alpha \leq \beta$ or $\beta \leq \alpha$

$$n \cdot m \longmapsto \log(n \cdot m) = \log(n) + \log(m)$$

$$\mathbb{N} \xrightarrow[\log]{\approx} \bigoplus_{i=1}^{\infty} \mathbb{Z}_{\geq 0}$$

$$n \longmapsto (a_1, a_2, \dots, a_k, 0, \dots)$$

$$n = 2^{a_1} 3^{a_2} \dots p^{a_k}$$

Since we've proven existence, now we need to prove uniqueness.

$$a \geq 2$$
$$a = p_1 \dots_k = q_1 \dots q_l$$

Note(Should be separate lemma):

$$p|nm \implies p|n \text{ or } p|m$$

It is easy to show if you assume that p does not divide n, which implies that $gcd(n, p) = 1$, which gives

$$xp + yn = 1$$
$$mxp + ynm = \implies p|m$$

Which, without loss of generality, gives

$$p_1 \dots p_k = q_1 \dots q_l$$

□

3 Day 3

3.1 Modular Arithmetic

$$\mathbb{Z}/n\mathbb{Z}$$

3.1.1 Quotient structures:

1. X is a set, equipped with an equivalence relation $\sim$.

$$X \to X/\sim$$

2. R a ring, $I \in R$, where I is an ideal.

$$R, I \to R/I$$

3. G a group, $H \nabla G$ a normal subgroup

$$G, H \to {}^{G}\!/_{H}$$

Note that 1 specializes to 2 and 3
X, $\sim$ a relation $\equiv$ a set of ordered pairs of elements of X. Notation:

$$x \sim y \equiv (x, y) \text{ is in the set of ordered pairs}$$

Definition 8. $\sim$ is an equivalence relation if the folowing conditions are satisfied

1. $x \sim x$
2. $x \sim y \implies y \sim x$
3. $x \sim y \sim z \implies x \sim z$

- Example: Discrete equivalence relationship, $x \sim y \iff x = y$
- Example: $\forall x, y,\ x \sim y$

Definition 9. 1. $(x, \sim)$ is an equivalence relation. $x \in X$ the equivalence class of x denoted $\hat{x}$ is the set of y with $x \sim y$

2. X breaks up into the (non-overlapping) equivalence class.

$$z \in \overline{x} \cap \overline{y}$$

CIRCLE WITH OTHER CIRCLES IN IT

Definition 10.

$${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \text{ (the set of equivalence classes)}$$

With the set of equivalence classes as $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

$$n \in \mathbb{N} = \{1, 2, \ldots\}$$
$$a \sim b \equiv a = b(modn) \iff n|a - b$$

1. There is an equivalence relation
2. $a, a', b, b' \in \mathbb{Z}$

$$\begin{aligned} \overline{a} &= \overline{a}' \\ \overline{b} &= \overline{b}' \\ \implies \overline{a+b} = \overline{a'+b'} \implies \overline{ab} &= \overline{a'b'} \end{aligned}$$

To show $\overline{a+b} = \overline{a'+b'}$,

$$\begin{aligned} n&|(a+b)-(a'+b') \\ n&|(a-a')+(b-b') \end{aligned}$$

To show $\overline{ab} = \overline{a'b'}$

$$\begin{aligned} n&|(ab-a'b') \\ ab-ab'&+ab'-a'b' \\ n&|a(b-b')+(a-a')b' \end{aligned}$$

$$\begin{aligned} \overline{0} &= n\mathbb{Z} \\ \overline{1} &= 1+n\mathbb{Z} \\ \overline{2} &= 2+n\mathbb{Z} \\ &\vdots \\ \overline{n-1} &= (n-1)+n \end{aligned}$$

Definition 11. ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ is a ring w.r.t,

$$\begin{aligned} \overline{a}\cdot\overline{b} &\equiv \overline{ab} \\ \overline{a}+\overline{b} &\equiv \overline{a+b} \end{aligned}$$

1.

$$\begin{aligned} (\overline{a}+\overline{b})+\overline{c} &= \overline{a}+(\overline{b}+\overline{c}) \\ (\overline{a}+\overline{b})+\overline{c} &= \overline{a+b}+\overline{c} = \overline{(a+b)+c} \\ \overline{a}+(\overline{b}+\overline{c}) &= \overline{a}+\overline{b+a} = \overline{a+(b+c)} \end{aligned}$$

2.

$$(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})$$

3.

$$\overline{a} = \overline{a}+\overline{0} = \overline{0}+\overline{a} = \overline{a}$$

4.

$$\overline{a}+\overline{x} = \overline{0} \iff \overline{x} = \overline{-a}$$

5.

$$\overline{a} + \overline{b} = \overline{b} + \overline{c} = \overline{a+b}$$

6.

$$\begin{aligned} \overline{a}(\overline{b} + \overline{b}) &= \overline{a}\overline{b+c} \\ &= \overline{a(b+c)} \\ &= \overline{ab+ac} \\ &= \overline{ab} + \overline{ac} \\ &= \overline{a}\overline{b} + \overline{ac} \end{aligned}$$

7.

$$\overline{1} \cdot \overline{a} = \overline{1 \cdot a} = \overline{a}$$

Theorem 4. <u>(This should be a proposition)</u> $\mathbb{Z}/_{/}n\mathbb{Z}$ is a field if and only if $n = p$ where p is prime.

Theorem 5. <u>(This should be a proposition)</u> F is a field if F has no zero-divisors, or

$$\begin{aligned} ab &= 0 \\ \implies a &= 0 \text{ or } b = 0 \end{aligned}$$

Proof. Assume $ab = 0$ and $a \neq 0$

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

$\square$

Theorem 6. <u>This should be a fact, also it confuses me</u> For every p (a prime), and $n \in \mathbb{N}$, there is a <u>unique</u> field of size p^n,

$$\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n} \text{ if } m|n$$

4 Day 4

$$\begin{aligned} \mathbb{Z}/_{n\mathbb{Z}} &= \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\} \\ a \sim b &\iff a = bmod(n) \end{aligned}$$

$\mathbb{Z}/_{n\mathbb{Z}}$ is a ring wrt,

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a} \cdot \overline{b} &= \overline{ab} \end{aligned}$$

- $\overline{0}$ 0-element
- $\overline{1}$ is 1 in $\mathbb{Z}/n\mathbb{Z}$

Theorem 7. $\mathbb{Z}/n\mathbb{Z}$ is a field if and only f $n = p$ where p is prime.

Proposition 1. No field has 0-divisors ($ab = 0$ implies $a = 0$ or $b = 0$). Proof was supplied last class

Note: R is a ring, therefore

$$0 \cdot r = 0$$
$$(-a)b = a(-b) = -(ab)$$

0 and 1 are unique.

Proof. p does not divide a if and only if $gcd(a, p) = 1$.

$$\exists x, y \in \mathbb{Z},\ xa + yp = 1$$
$$\overline{xa + yp} = \overline{1}$$
$$\overline{x} \cdot \overline{a} + \underbrace{\overline{y} \cdot \overline{p}}_{\text{cancels out for some reason}} = \overline{1}$$
$$\overline{x} \cdot \overline{a} = \overline{1}$$
$$\implies \mathbb{Z}/n\mathbb{Z},\ \text{ a field}$$

Assume n is not a prime, where

$$n = ab,\ \text{ with }\ a, b > 1$$
$$\overline{n} = \overline{a} \cdot \overline{b}$$
$$\overline{0} = \overline{a} \cdot \overline{b}$$

$\implies \mathbb{Z}/n\mathbb{Z}$ has 0-divisors because $\overline{a}, \overline{b} \neq 0$, thus the previous proposition is proven. □

Definition 12. Given a ring R, we use the notation, R^* to indicate that it has invertible elements. Furthermore, we observe that R^* is an abelian group w.r.t. product.

Theorem 8. (This should be a corrolary). p is a prime.

$$(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$$

Theorem 9. (Also a corrolary)
$\forall a \in \mathbb{Z}$ p does not divide a.

$$a^{p-1} = 1 mod(p)$$

Example:

$$p = 3,\ a = 16$$
$$16^2 = 1 mod(3)$$

Proposition 2. G is a finite group.

$$\forall x \in G,\ x^{|G|} = 1$$
$$\overline{a}^{p-1} = \overline{1}$$
$$a^{p-1} = 1 mod(p)$$

Alternative proof of Corrolary 2,

Proof.

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)$$
$$x \mapsto ax mod(p)$$

Assume $ax = ay mod(p)$. We want to show,

$$x = y$$
$$\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y}$$
$$\overline{a}(\overline{x} - \overline{y}) = 0$$
$$\overline{x} - \overline{y} = 0$$

Somehow, we move on to,

$$\overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \ldots (\overline{p-1}) = (\overline{a \cdot 1}) \cdot (\overline{a \cdot 2}) \cdot \ldots (\overline{a \cdot (p-1)})$$
$$\overline{(p-1)}! = (\overline{a})^(p-1) \cdot \overline{(p-1)}!$$
$$\overline{(p-1)} = \overline{z} \neq 0$$
$$\overline{z} = (\overline{a})^{p-1} \cdot \overline{z}$$
$$\overline{z} - \overline{a}^{p-1} \cdot \overline{z} = 0$$
$$\overline{z}(\overline{1} - \overline{a}^{p-1}) = 0$$

□

4.1 Primality test

n Pick a coprime with n, check whether $a^{n-1} = 1 mod(n)$, if they are not equal, then n is not prime. Plus some other easily checked conditions. This also somehow implies a fast algorithm for testing natural numbers for primality.
Unfortunately (hahaha what? is there anything more unfortunate than the previous factoid? in any case, I continue, with regret).

$$\exists n \in \mathbb{N}$$
$$a^{n-1} = 1 mod(n)$$

for every a with $gcd(a, n) = 1$. Sick.

Definition 13.

$$\varphi(n) = |\{i : 1 \leq i \leq n-1,\ gcd(i,n) = 1\}|$$
$$\varphi(p) = p - 1$$
$$\varphi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k})$$

$p_1, \dots, p_k$ are the prime factors of n

Theorem 10.

$$a \in N,\ gcd(a,n) = 1$$
$$a^{\varphi(n)} = 1 mod(n)$$

Proposition 3. (Should be an idea. Utter shrapnel of an idea, but an idea nonetheless)

$$(\mathbb{Z}/_{n\mathbb{Z}}) = \{\bar{i} : 1 \leq i \leq n-1,\ gcd(i,n) = 1\}$$

Theorem 11. (Should be a lemma)

$$\varphi(ab) = \varphi(a)\varphi(b)$$

if $a, b \in \mathbb{N}$ with $gcd(a,b) = 1$

$$n = p_1^{d_1} \dots p_k^{d_k} \varphi(p^d) =$$

Yes, that lemma ends there. That's it. No more lemmas.