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:

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

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.

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

Which somehow follows from,

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

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),

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

(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.

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

Example:

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

Fact:

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

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,

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

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,

$$a = p_1 \dots p_k$$

and for any other factorization,

$$a = q_1 \dots q_l$$

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 $\mathbb{Z}_{\geq 0} = \{0, 1, \dots\}$

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

Where $\alpha = (a_1, a_2, \dots)$ and $\beta = (b_1, b_2, \dots)$. 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 $\beta \leq \alpha$

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

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

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

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

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

$$a \geq 2$$
$$a = p_1 \ldots_k = q_1 \ldots q_l$$

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

$$p_1 \ldots p_k = q_1 \ldots q_l$$

$\square$