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,

$$a|b = c$$

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

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,

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

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:

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

Then,

$$\begin{aligned} gcd(a_1,\ldots,a_n) &= x_1a_1 + \cdots + x_na_n \\ gcd(a_1,\ldots,a_n) &= gcd(gcd(a_1,\ldots,a_{n-1})a_n) \\ &= min(x_1a_1 + \cdots + x_na_n | x_1,\ldots,x_n \in \mathbb{Z},\ x_1a_1 + \cdots + x_na_n > 0) \end{aligned}$$