Integer Arithmetic

Important Property of $\times$ in $\mathbb{Z}$: $ab = 0 \Rightarrow a = 0$ or $b = 0$

Cancellation Law Given $a, b, c \in \mathbb{Z}$, $c \neq 0$

$$ac = bc \Rightarrow a = b$$

Proof $ac = bc \Rightarrow ac - bc = 0 \Rightarrow (a-b)c = 0$

$\Rightarrow a - b = 0 \Rightarrow a = 0$

$c \neq 0$

$\square$

a is a factor/divisor of b

Definition

Given $a, b \in \mathbb{Z}$, we write $a \mid b$ if $\exists\, c \in \mathbb{Z}$ such that $b = ac$. A <u>factorization</u> of b is any breakdown

$$b = a_1 \cdot a_2 \cdots a_n \text{ where } a_i \in \mathbb{Z}.$$

The only factors of 1 are ± 1.

Definition $p \in \mathbb{N}$ is <u>prime</u> if $p > 1$ and $\forall\, x \in \mathbb{N}$, $x \mid p \Rightarrow x = 1$ or $x = p$. If not we say p is <u>composite</u>.

highest common factor

Definition Given $a, b \in \mathbb{Z}$, $HCF(a,b) \in \mathbb{N}$ is the largest common factor of a and b.

a, b coprime $\Leftrightarrow HCF(a,b) = 1$

E.g. $HCF(15, 7) = 1$, $HCF(36, 21) = 3$

Proposition Given $a, b, m \in \mathbb{Z}$

$m \mid a$ and $m \mid b \Rightarrow m \mid HCF(a,b)$

Remainder Theorem

There exists unique

Given $n \in \mathbb{Z}, m \in \mathbb{N}$, $\exists!\ q, r \in \mathbb{Z}$ such that

- $n = qm + r$ called the remainder n modulo m
- $0 \leq r < m$

Theorem Given $a, b \in \mathbb{Z}$, $\exists\ u, v \in \mathbb{Z}$ such that

$ua + vb = HCF(a,b)$.

In fact $\exists\ u, v \in \mathbb{Z}$ such that $ua + vb = 1$

$\Leftrightarrow$ a, b coprime.

Euclid's Lemma Let $p \in \mathbb{N}$ be prime and $a, b \in \mathbb{Z}$

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b$$

Fundamental Theorem of Arithmetic

Every $a \in \mathbb{N}$, $a > 1$ can be written as a product of primes

$$a = p_1 p_2 \cdots p_r$$

Such a factorization is unique up to reordering.

Remark We'll prove these results in much greater generality later in the course.

FTOA $\Rightarrow$ Every $a \in \mathbb{Q}$, $a \neq 1$ can be written uniquely in form $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, p_i distinct primes, $\alpha_i \in \mathbb{Z} \setminus \{0\}$.

<u>Theorem</u> There are infinitely many prime numbers.

<u>Proof</u> Assume not and $\{p_1, \dots p_n\}$ is a complete list of distinct primes.

Let $c = p_1 \cdots p_n + 1$

$\Rightarrow$ $c \in \mathbb{N}$ and $c > 1$

$\Rightarrow$ After perhaps reordering $p_1 \mid c$

$\Rightarrow$ $p_1 d = p_1 \cdots p_n + 1$ for some $d \in \mathbb{N}$

$\Rightarrow$ $p_1 (d - p_2 \cdots p_n) = 1$ $\Rightarrow$ $p_1 \mid 1$. Contradiction.

$\square$

<u>Modular Arithmetic</u>

Fix $m \in \mathbb{N}$

<u>Definition</u> We say $a, b \in \mathbb{Z}$ are <u>congruent modulo m</u>, if they have the same remainder modulo m. We write $a \equiv b \bmod m$ $(\Leftrightarrow m \mid (b-a))$

remainders are unique

Remainder classes partition $\mathbb{Z}$ $\Rightarrow$ congruence modulo m is equivalence relation.

$\mathbb{Z}/m\mathbb{Z} :=$ Equivalence classes modulo m.

$\mathbb{Z}/m\mathbb{Z} = \{[0],[1],\dots,[m-1]\}$

$\Rightarrow \quad |\mathbb{Z}/m\mathbb{Z}| = m$ finite

<u>Important Exercise</u> $\forall\, a, a', b, b' \in \mathbb{Z}$

$[a] = [a']$, $[b] = [b'] \Rightarrow$ $[a+b] = [a'+b']$ and $[ab] = [a'b']$

<u>Example</u> $m = 3$, $a = 4$, $a' = 7$, $b = 2$, $b' = -1$

$a+b = 6$, $a'+b' = 3$ and $[6] = [3] = [0]$

$ab = 8$, $a'b' = -7$ and $[8] = [2] = [-7]$

<u>Definition</u> We define $+$ and $\times$ on $\mathbb{Z}/m\mathbb{Z}$ as follows:

- Given $[a],[b] \in \mathbb{Z}/m\mathbb{Z}$, $[a]+[b] := [a+b]$
- Given $[a],[b] \in \mathbb{Z}/m\mathbb{Z}$, $[a]\times[b] := [ab]$

Independent of choice of equivalence class representative by above Fact.

$(\mathbb{Z}/m\mathbb{Z}, +, \times)$ shares many properties with $(\mathbb{Z}, +, \times)$.

For example, $[0]$ behaves like 0 and $[1]$ behaves like 1.

There are important differences though,

- $$\underbrace{[1] + [1] + \dots + [1]}_{m \text{ times}} = [m] = [0]$$

- If $m = ab$, $a, b \in \mathbb{N}$, $a, b < m$ (ie m composite)

$\Rightarrow$ $[a], [b] \neq [0]$.

However $[a] \times [b] = [ab] = [m] = [0]$

non-zero terms can multiply to give zero.

- If $p \in \mathbb{N}$ prime, $a \in \mathbb{Z}$

  $[a] \neq [0] \iff p \nmid a \iff HCF(a, p) = 1$

  $\iff \exists\, u, v \in \mathbb{Z}$ such that $ua + vp = 1$

  $\iff \exists\, [u] \in \mathbb{Z}/p\mathbb{Z}$ such that $[u] \times [a] = [1]$

We say $[u]$ is a multiplicative inverse of $[a]$.

<u>Conclusion</u> : $p \in \mathbb{N}$ prime $\Rightarrow$ Every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse.

Not true for $\mathbb{Z}$

True for $\mathbb{Q}$