# Number Theory 1

November 10, 2019

# 1 Congruency

Let $n \in \mathbb{N} \backslash \{0\}$. For all $a, b \in \mathbb{Z}$, define

$$a \equiv b (\text{mod n}) \text{ if and only if } n | a - b$$

The relation $\cdots \equiv \cdots (\text{mod } n)$ is an equivalence relation on $\mathbb{Z}$, and so, for all $a \in \mathbb{Z}$, we use $[a]_n$ to denote the equivalence class of $a$. Define

$$\mathbb{Z}/n\mathbb{Z} = \{[a]_n | a \in \mathbb{Z}\}$$

and define $\oplus_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by: for all $a, b \in \mathbb{Z}$,

$$[a]_n \oplus_n [b]_n = [a + b]_n$$

Define $\otimes_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ by: for all $a, b \in \mathbb{Z}$,

$$[a]_n \otimes_n [b]_n = [ab]_n$$

If $n \in \mathbb{N} \backslash \{0\}$, then $(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ is group.

Cayley Table.

## 1.1 Congruency and Group

If $n \in \mathbb{N} \backslash \{0\}$, then $(\mathbb{Z}/n\mathbb{Z}, \oplus_n)$ is abelian with order n. Moreover, $(\mathbb{Z}/n\mathbb{Z}, \oplus_n) = C_n$. $((\mathbb{Z}/n\mathbb{Z}, \oplus_n) = \langle [1]_n \rangle)$

Is $(\mathbb{Z}/n\mathbb{Z}, \otimes_n)$ a group? No.

Let $G_n = \mathbb{Z}/n\mathbb{Z} \backslash \{[0]_n\}$. Is $(G_n, \otimes_n)$ a group? No.

For all $n \in \mathbb{N}$ with $n \geqslant 2$, define

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[k]_n \in \mathbb{Z}/n\mathbb{Z} | (\exists x \in \mathbb{Z})(kx \equiv 1 \text{ (mod n)})\}$$

Let $n \in \mathbb{N}$ with $n \geqslant 2$. Then $((\mathbb{Z}/n\mathbb{Z})^*, \otimes_n)$ is a group.
Proof.

1. $\otimes_n$ is a function from $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ to $(\mathbb{Z}/n\mathbb{Z})^*$
2. $[1]_n$ is the identity element.

3. Since $kx \equiv 1 \pmod{n}$, then the inverse of $[x]_n$ is $[k]_n$.

List the Cayley Table of $((\mathbb{Z}/6\mathbb{Z})^*, \otimes_6)$.

Let $n \in \mathbb{N}$ with $n \geqslant 2$. If $1 < m \leqslant n$ is such that there exists $1 < d \leqslant m$ with $d|m$ and $d|n$, then $[m]_n \notin (\mathbb{Z}/n\mathbb{Z})^*$.

# 2 Greatest Common Divisor

Let $a, b \in \mathbb{Z}$ with $|a| + |b| \neq 0$. We say that $d \in \mathbb{N}$ is the greatest common divisor of $a$ and $b$, and write this element $\gcd(a, b)$, if
(i) $d|a$ and $d|b$,
(ii) and for all $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c|d$.

## 2.1 Linear Diophantine Equations

A linear Diophantine equation in two variables is an equation in the form

$$ax + by = c \text{ where } a, b, c \in \mathbb{Z} \text{ are constants with } |a| + |b| \neq 0$$

A solution is a pair $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ with $ax_0 + by_0 = c$.

## 2.2 Bezout's Lemma

Let $a, b \in \mathbb{Z}$ with $|a| + |b| \neq 0$. Then there exists $x, y \in Z$ such that $\gcd(a, b) = ax + by$.
Proof. Consider

$$S = \{n \in \mathbb{N}\backslash\{0\} | (\exists x, y \in \mathbb{Z})(n = ax + by)\}$$

Let $d \in S$ be the $\leqslant$-least element of $S$. $\gcd(a, b) = d$.

Let $n \in \mathbb{N}$ with $n \geqslant 2$. For all $m \in \mathbb{Z}$,

$$[m]_n \in (\mathbb{Z}/n\mathbb{Z})^* \text{ if and only if } \gcd(m, n) = 1$$

## 2.3 A More General Form of Bezout's Lemma

Let $a_1, a_2, \cdots a_n \in \mathbb{Z}$. Let $d = \gcd(a_1, a_2, \cdots a_n)$. Then there exists $x_1, x_2, \cdots, x_n$ with $|x_1| + |x_2| + \cdots + |x_n| \neq 0$ such that

$$x_1 a_1 + x_2 a_2 + \cdots + x_n a_n = d$$

## 2.4 Multiplicative Inverses

Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}\backslash\{0\}$. If $q, r \in \mathbb{Z}$ with $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Let $n \in \mathbb{N}$ with $n \geqslant 2$. $(\mathbb{Z}/n\mathbb{Z})^* = \{[m]_n | (m < n) \wedge (\gcd(m, n) = 1)\}$

### 2.5 Relatively Prime

Let $a, b \in \mathbb{Z}$ with $|a| + |b| \neq 0$. We say that $a$ and $b$ are relatively prime if $\gcd(a, b) = 1$.

## 3 Eulers Totient Function

**Eulers Totient Function**, denoted $\varphi$, is the function defined on all $n \in \mathbb{N}$ with $n \geqslant 2$ by

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$$

In other words, $\varphi(n)$ is the number of $0 < m < n$ such that $m$ and $n$ are relatively prime.

If $p \in \mathbb{N}$ is prime, then $\varphi(p) = p - 1$.

### 3.1 Eulers Theorem

Let $a, n \in \mathbb{N}$ with $n \geqslant 2$ and $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1(\text{mod } n)$.

### 3.2 Fermats Little Theorem

If $a, p \in \mathbb{N}$, $p$ is prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1(\text{mod } p)$

### 3.3 Eulers Product Formula

$$\varphi(n) = n \cdot \prod_{p \in A} (1 - \frac{1}{p})$$

where $A$ is the set of distinct primes that divide $n$.

## 4 Corollary of Bezout's Lemma

Let $a, b \in \mathbb{Z}$ with $|a| + |b| \neq 0$. Then $\gcd(a, b) = 1$ if and only if there exists a solution to the Diophantine equation $ax + by = 1$.

Let$a, b \in \mathbb{Z}$ with $|a| + |b| \neq 0$. If $\gcd(a, b) =$ d, then

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

$\sqrt{2}$ is irrational.

Let $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$. If $a|c$ and $b|c$, then $ab|c$.

(Euclids Lemma)Let $a, b, c\mathbb{Z}$ with $\gcd(a, b) = 1$. If $a|bc$, then $a|c$.

Let $p \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If $p$ is prime and $p|ab$, then $p|a$ or $p|b$.

## 5 Fundamental Theorem of Arithmetic

Let $p \in \mathbb{N}$ be prime. If $a_1, \cdots, a_n$ Z and $p|a_1 \cdots a_n$, then there exists 1 k n such that $p|a_k$ .

Let $p, q_1, ..., q_n \in \mathbb{N}$ be primes. If $p|q_1 \cdots q_n$, then there exists $1 \leqslant k \leqslant n$ such that $p = q_k$.

(Fundamental Theorem of Arithmetic) If $n \in \mathbb{N}$ with $n \geqslant 2$, then $n$ can be uniquely factored into a product of primes.

## 6 Exercise

1. Let $a, b, p, m \in \mathbb{Z}^+$. If $p^a \equiv 1 (\text{mod } m)$, $p^b \equiv 1 (\text{mod } m)$, $d$ =gcd$(a, b)$, show that $p^d \equiv 1(\text{mod } m)$.
(Hint. Bezouts Lemma.)

2. Let $p, m \in \mathbb{Z}^+$. If $a$ is the least positive integer such that $p^a \equiv 1(\text{mod } m)$, than for any $b \in \mathbb{Z}^+$, if $p^b \equiv 1(\text{mod } m)$, then $a|b$.
(Hint. Use the conclusion of problem 1.)

3. Here is a proof of Fermats Little Theorem. Consider the set $S = \{a, 2a, \cdots, (p-1)a\}$. For any $ma, na$ in S, there doesn't exist $ma \equiv na$. (Why?) Therefore

$$S \text{ mod } p = \{0 \leqslant k \leqslant p-1 | ma \equiv k (\text{mod } p), ma \in S\} = \{1, 2, \cdots, p-1\}$$

Then,

$$a \cdot 2a \cdots (p-1)a \equiv (p-1)!(\text{mod } p)$$

which implies $a^{p-1}(p-1)! \equiv (p-1)!$ (mod $p$). Since gcd($(p-1)!, p$)=1, then $a^{p-1} \equiv 1$ (mod $p$).
Use the same method to prove Eulers Theorem. (Consider $S = \{ka | \gcd(k, n) = 1, 1 \leqslant k \leqslant n\}$).

4. Let $S_n = 1^n + 2^n + \cdots + (n-1)^n$. Find all $n \geqslant 2$, such that $n|S_n$. (Answer. $n$ is odd.)

5. Show that there exists infinite pairs of positive integers $(a,b,c)$ $(a,b,c > 2019)$ such that

$$a|bc-1, \quad b|ac+1, \quad c|ab+1.$$

(Hint. Let $c = ab+1$. $(a,b,c) = (k, k+1, k^2+k+1)$)

6. Let $k \in \mathbb{Z}^+$ and $k \geqslant 2$. Let $a, b \in \mathbb{Z}$ and $ab \neq 0$, $a+b$ is odd. If there exists $x, y \in \mathbb{Z}$, $0 < |x-y| \leqslant 2$ such that $a^k x - b^k y = a - b$. Show that $|a-b| = d^k$, where $d = \gcd(a,b)$.

7. We define a sequence $\{a_n\}$:

1. $a_i \in \mathbb{Z}^+$
2. $a_{n+1}$ is the least number such that $a_{n+1}$ and $\sum_{i=1}^{n} a_i$ are relatively prime, and $a_{n+1} \notin \{a_1, a_2, \cdots, a_n\}$

Show that every $a \in \mathbb{Z}^+$ can be found in this sequence $\{a_n\}$.