# Number Theory

TSS Math Club

March 2023

# 1 Integers

## 1.1 Division with Remainder

### 1.1.1 Example

Find the quotient and remainder when 102 is divided 5.

### 1.1.2 Example

Find the quotient and remainder when 213 is divided 7.

## 1.2 Divisibility

### 1.2.1 Definition

### 1.2.2 Notation

$a|b$

### 1.2.3 Theorems

- $a|b$ and $b|c \implies a|c$
- $a|b \implies a|cb$
- $a|b$ and $a|c \implies a|mb + nc$

## 1.3 GCD and LCM

### 1.3.1 Defnition

- GCD:
- LCM:

### 1.3.2 Notations

- GCD:
- LCM:

### 1.3.3 Example

- (10,5)= [10,5]=
- (3,2)= [3,2]=
- (0,n)= [0,n]=
- (n,1)= [n,1]=

### 1.3.4 Theorem

If $(a, b) = d$, then $(a/d, b/d) = 1$
Proof:

### 1.3.5 Theorem

If $a = bq + r$, then $(a, b) = (b, r)$
Proof:

### 1.3.6 Euclidean Algorithm

#### 1.3.7 Theorem

If$(a, b) = d$, then exist integers $x, y$ such that

$$ax + by = d$$

Proof:

#### 1.3.8 Corollary

If $d|ab$ and $(d, a) = 1$, then $d|b$
Proof:

### 1.4 Primes and UFD

#### 1.4.1 Primes

Definition:

#### 1.4.2 Lemma

If $n$ is composite, the there is a divider $d$ such that $d \leq n^{\frac{1}{2}}$
Proof:

#### 1.4.3 Lemma

If $n$ is composite, the there is a prime divider $p$ such that $p \leq n^{\frac{1}{2}}$

#### 1.4.4 Euclid's Lemma

If $p$ is a prime and $p|ab$ then $p|a$ or $p|b$.
Proof:

#### 1.4.5 Extended Euclid's Lemma 1

If $p$ is a prime and $p|a_1 a_2 ... a_n$ then $p|a_i$.

#### 1.4.6 Extended Euclid's Lemma 2

If $p$ and $q_i$ are primes and $p|q_1 q_2 ... q_n$ then $p = q_i$.

#### 1.4.7 $\mathbb{Z}$ is UFD (Unique Factorization Domain)

Any positive integer can be written as a product of primes in one and only one way.
Proof:

#### 1.4.8 GCD and LCM in Terms of Factorization

#### 1.4.9 Theorem

$(a, b)[a, b] = ab$

#### 1.4.10 Theorem

Number of divisor $d(n) =$

# 2 Diophantine Equations

## 2.1 Definition

## 2.2 Use Divisibility

#### 2.2.1 Example

Given $x, y$ are integers and $xy = 30$, find ordered pair $(x, y)$.

### 2.2.2 Example

Given $x, y$ are integers and

$$y = \frac{x^3 + 7x - 10}{x + 3},$$

find ordered pair $(x, y)$.

### 2.2.3 Simon's Favourite Factoring Trick

Given $x, y$ are integers and

$$3x + xy + 3y + 31 = 0,$$

find ordered pair $(x, y)$.

## 2.3 Solve Linear Diophantine Equations

### 2.3.1 Definition

Solve $ax + by = c$ for integers $x, y$.

### 2.3.2 Theorem

For the equation above, if $(a, b)|c$, then there are infinite number of solutions. If $(a, b) \nmid c$, then there is no solution.

### 2.3.3 Example

Solve $3x + 4y = 10$.

### 2.3.4 Example

Solve $8x + 4y = 6$.

#### 2.3.5 Example

Solve $6x + 9y = 24$.

# 3 Congruences and Modulo

## 3.1 Definition

If $a$ is congruent to $b$ modulo $m$ ($a \equiv b\ (m)$) or ($a \equiv b \pmod{m}$), then $m|a - b$.

## 3.2 Congruences and Remainder

#### 3.2.1 Theorem

Every integer is congruent $m$ to exactly one of $0, 1, ..., m - 1$.

#### 3.2.2 Theorem

$a \equiv b\ (m)$ iff $a$ and $b$ leave the same remainder on division by $m$.

## 3.3 Operations under modulo

#### 3.3.1 Lemma

- $a \equiv a\ (m)$.
- If $a \equiv b\ (m)$, then $b \equiv a\ (m)$.
- If $a \equiv b\ (m)$ and $c \equiv d\ (m)$, then $a + b \equiv c + d\ (m)$.
- If $a \equiv b\ (m)$ and $c \equiv d\ (m)$, then $ab \equiv cd\ (m)$.

### 3.3.2 Theorem

If $ac \equiv bc\ (m)$ and $(c, m) = 1$, then $a \equiv b\ (m)$

### 3.3.3 Theorem

If $ac \equiv bc\ (m)$ and $(c, m) = d$, then $a \equiv b\ (m/d)$

## 3.4 Problems

### 3.4.1 Problem

Find the least residue of 1492 (mod 4), (mod 10), (mod 101).

### 3.4.2 Problem

Solve $2x \equiv 4\ (6)$.

### 3.4.3 Problem

Prove $m^2 \equiv$ 0 or 1 (4)

### 3.4.4 Problem

Solve $m^2 + n^2 = 1023$

### 3.4.5 Problem

Show every integer is congruent to (mod 9) to the sum of its digits.

# 4 Linear Congruences

We will try to solve the linear equation $ax \equiv b \pmod{m}$ in this section.

## 4.1 General Theory

### 4.1.1 Theorem

If $(a, m) \nmid b$, then $ax \equiv b$ $(m)$ has no solutions.

### 4.1.2 Theorem

If $(a, m) \nmid 1$, then $ax \equiv b$ $(m)$ has exactly one solution mod $m$.

### 4.1.3 Theorem

If $(a, m) \nmid d$, then $ax \equiv b$ $(m)$ has exactly one solution mod $m/d$.

## 4.2 Problems

### 4.2.1 Problem

Solve $2x \equiv 1$ $(17)$

### 4.2.2 Problem

Solve $3x \equiv 1$ $(17)$

### 4.2.3 Problem

Solve $15x + 16y = 17$

### 4.3 Chinese Remainder Theorem (CRT)

If the $n_i$ are pairwise coprime, and if $a_1, ..., a_k$ are any integers, then the system

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has one solution mod $N = n_1 n_2 ... n_k$.

#### 4.3.1 Example

Solve:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ 4x &\equiv 3 \pmod 5 \end{aligned}$$

#### 4.3.2 Problem

Find the remainder when divided by 10 of the following:

$$4^{4^{4^{4^{4^{4^{4^{\cdot^{\cdot^{\cdot^{4}}}}}}}}}}$$

(There are 2023 4's in total).

## 5 Wilson's, Fermat's, Euler's Theorems

### 5.1 Wilson's Theorem

A natural number $n > 1$ is a prime number if and only if the product of all the positive integers less than n is one less than a multiple of $n$ or

$$(n-1)! \equiv -1 \pmod{n}.$$

### 5.2 Fermat's Little Theorem

If $a$ is not divisible by the prime $p$, then

$$a^{p-1} \equiv 1 \pmod p$$

### 5.2.1 Example

What is the least residue of $1945^8 \pmod 7$

### 5.2.2 Example

What is the least residue of $2025^{22} \pmod{11}$

## 5.3 Euler's Theorem

### 5.3.1 Euler's Totient Function

Euler's totient function $\varphi(n)$ counts the positive integers up to a given integer $n$ that are relatively prime to $n$.

### 5.3.2 Example

Find $\varphi(24)$

### 5.3.3 Euler's Totient Function is Multiplicative

If $(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.

### 5.3.4 Example

Find $\varphi(2)$, $\varphi(5)$, $\varphi(10)$.

### 5.3.5 Euler's Totient Function for $p^n$

$\varphi(p^n) = p^n - p^{n-1}$

### 5.3.6 Euler's Totient Function General Formula

### 5.3.7 Euler's Theorem

If $(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

### 5.3.8 Example

What is the least residue of $2023^{41} \pmod{100}$