# Number Theory and Divisibility Issues

Maya Koreth and Dania Rustom

MIT PRIMES Circle

2022

# What is Number Theory?

Number Theory is the study of the properties and relationships of numbers. In this presentation, we will explore:

- Divisibility and Congruence Relations
- Euclidean Algorithm
- Modular Arithmetic
- Primitive Roots

# Introductions and Definitions

## Definition (Divisibility Symbols)

If $ax = b$ for any integer $x$, then we say that $\boldsymbol{a}$ divides $\boldsymbol{b}$, or $\boldsymbol{a|b}$. Conversely, if $\boldsymbol{ax \neq b}$, then $\boldsymbol{a}$ does not divide $\boldsymbol{b}$, or $\boldsymbol{a \nmid b}$.

## Definition (Prime Numbers)

If an integer $p$ has no divisor other than 1 and itself, it is called a **prime number.** Otherwise, it is a **composite number.** Examples of prime numbers: 2, 3, 5, and 7; examples of composite numbers: 4, 6, 8, and 9.

## Definition (Coprime)

We say that $a$ and $b$ are **relatively prime** in case (a,b) = 1. The fact that (a,b) = 1 can also be expressed by saying that $a$ and $b$ are coprime, or saying $a$ is prime to $b$.

# Greatest Common Divisor

**Theorem (Definition)**

*The greatest common divisor $g$ of $b$ and $c$ can be characterized in the following two ways:*

1. *It is the least positive value of $bx + cy$ where $x$ and $y$ range over all integers.*
2. *It is the positive common divisor of $b$ and $c$ which is divisible by every common divisor.*

# Euclidean Algorithm

The Euclidean algorithm is a way to find the greatest common divisor of two positive integers, $a$ and $b$.

## Example

Find the greatest common divisor of 6409 and 42823:

$$42823 = 6 \cdot 6409 + 4369$$

$$6409 = 1 \cdot 4369 + 2040$$

$$4369 = 2 \cdot 2040 + 289$$

$$2040 = 7 \cdot 289 + 17$$

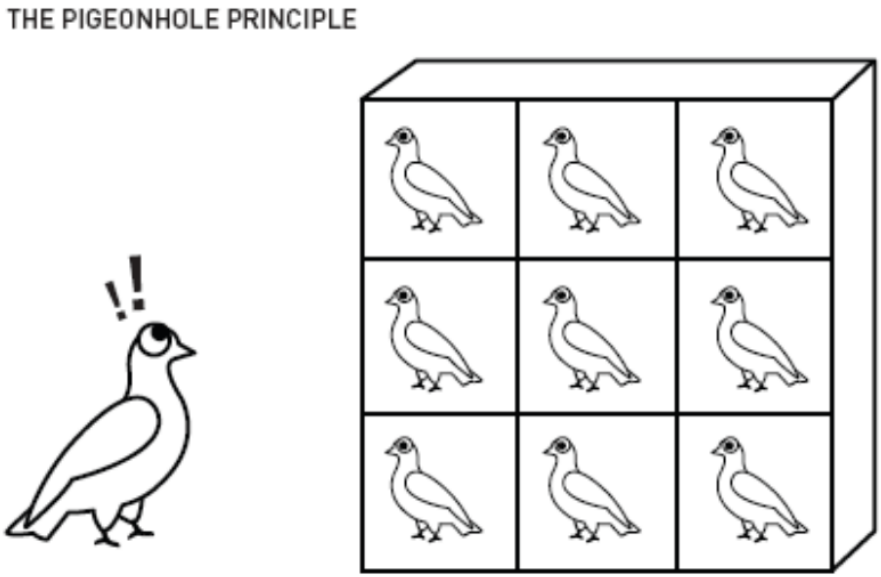
$$289 = 17 \cdot 17 + 0$$

Thus the greatest common divisor is 17

# Pigeonhole Principle

**Theorem**

*If $n+1$ elements are placed into $n$ sets, then at least one of the sets contains two or more elements.*



# Posa Problem

**Theorem**

*If one chooses more than n numbers from the set* $\{1, 2, 3, ..., 2n\}$*, then two of them are relatively prime.*

# Posa Problem

**Theorem**

*If one chooses more than n numbers from the set* $\{1, 2, 3, ..., 2n\}$*, then two of them are relatively prime.*

**Example**

We can start by using a smaller example, with $n = 3$. Then, we have the numbers:

$$\{1, 2, 3, 4, 5, 6\}$$

If we choose $n + 1$ numbers from this set, we can see that 1 and 5 are coprime to all other numbers. This forces us to choose the remaining four numbers, $\{2, 3, 4, 6\}$, but even in this set, 2 and 3 are coprime. Thus, at least two numbers will always be coprime in this set. But how do we prove this?

# Posa Problem

**Theorem**

*If one chooses more than n numbers from the set* $\{1, 2, 3, ..., 2n\}$*, then two of them are relatively prime.*

**Proof.**

First prove that two consecutive integers are always coprime. Denote two integers as $n$ and $n+1$. Then let

$$\gcd(n, n+1) = g$$

where $g$ is a natural number. By definition, $g|n$ and $g|(n+1)$, which means that

$$g|((n+1) - n) = 1$$

Thus, the $\gcd(n, n+1) = 1$. □

# Posa Problem Continued

**Theorem**

*If one chooses more than n numbers from the set* $\{1, 2, 3, ..., 2n\}$*, then two of them are relatively prime.*

**Proof continued.**

To pick more than $n$ numbers from the set (i.e more than half), there will always be at least two numbers that are consecutive by the pigeonhole principle. Since consecutive numbers are always coprime, the proof is completed. □

# Congruences and Modulo

## Definition (Modular Congruency)

If a non-zero integer $m$ divides $a - b$, we say that a is congruent to b modulo m and write $\boldsymbol{a \equiv b \pmod{m}}$. If $\boldsymbol{m \nmid (a - b)}$, then we say that a is not congruent to b modulo m, which is written as $\boldsymbol{a \not\equiv b \pmod{m}}$.

## Definition (Modulus)

Modulus m, an assumed positive integer, is the **idea of taking an integer m and cutting it off at a specified point.** For example:

## Example

$$10 \pmod 3$$

$$10 = 3(3) + 1$$

$$10 \equiv 1 \pmod 3$$

# CRT Example

## Theorem (Chinese Remainder Theorem)

*Guarantees that a solution exists within a set of congruences, as long as the modulus values of each congruence are coprime.*

## Example

$$x \equiv 1 \pmod 4, \quad x \equiv 0 \pmod 3, \quad x \equiv 5 \pmod 7$$

$$m = m_1 * m_2 * m_3 = 84$$

$$\frac{m}{m_1} = 21, 21 \cdot a_1 \equiv 1 \pmod 4, a_1 = 5$$

$$\frac{m}{m_2} = 28, 28 \cdot a_2 \equiv 1 \pmod 3, a_2 = 9$$

$$\frac{m}{m_1} = 12, 12 \cdot a_3 \equiv 1 \pmod 7, a_3 = 3$$

$$x = (21 \cdot 5 \cdot 1) + (28 \cdot 9 \cdot 0) + (12 \cdot 3 \cdot 5)$$

$$x \equiv 285 \pmod{84} \equiv 33 \pmod{84}$$

# Euler's Totient Function

**Definition**

The number $\phi(m)$ is the **number of positive integers less than or equal to m that are relatively prime to m.**

**Example**

Finding $\phi(9)$: The numbers coprime to 9 are $1, 2, 4, 5, 7, 8$. This means that $\phi(9) = 6$.

# Primitive Roots

## Definition (Primitive Roots)

If $a$ belongs to the exponent $\phi(m)$ modulo m, then $a$ is called a **primitive root modulo m.**

## Theorem

*If p is a prime, then there exist $\phi(p-1)$ primitive roots modulo p. The only integers having primitive roots are $p^e$, $2p^e$, 1, 2, and 4, with p an odd prime.*

# Primitive Roots

## Definition (Primitive Roots)

If $a$ belongs to the exponent $\phi(m)$ modulo m, then $a$ is called a **primitive root modulo m.**

## Theorem

*If p is a prime, then there exist $\phi(p-1)$ primitive roots modulo p. The only integers having primitive roots are $p^e$, $2p^e$, 1, 2, and 4, with p an odd prime.*

## Example

Find the primitive root of the prime 5

$$a^{\phi(5)} \equiv 1 \pmod 5$$

$$a^4 \equiv 1 \pmod 5$$

$$a^2 \equiv -1 \pmod 5$$

$$a \equiv 2 \pmod 5, a \equiv 3 \pmod 5$$

# References and Acknowledgements

Acknowledgements: We would like to thank Mary Stelow and Marisa Gaetz as well as everyone at PRIMES Circle for making this program possible. A special thank you to our mentor, Ariana Park, for guiding us throughout these months and always being there to help us.


Ivan Niven, Herbert S. Zuckerman, *An Introduction to the Theory of Numbers (4th Edition).*


Gabriel D. Carroll, *Combinatorial Number Theory*

Thank you! Any questions?