Competitive Programming and Mathematics Society

# Mathematics Workshop

## Number Theory Basics

**Smit**

# Table of contents

# Welcome

- This is a very introductory explanation of number theory so if you are already familiar with the theory, expect to see things you already know
- i will try to upload the slides on the website (unswcpmsoc.com) if i figure out how

# Attendance form

# Notation

- We will use more or less standard notation in number theory

# Notation

- We will use more or less standard notation in number theory
- $\mathbb{N}$ is the Natural Numbers, which includes $0$

# Notation

- We will use more or less standard notation in number theory
- $\mathbb{N}$ is the Natural Numbers, which includes $0$
- $\mathbb{Z}$ is the Integers

# Notation

- We will use more or less standard notation in number theory
- $\mathbb{N}$ is the Natural Numbers, which includes $0$
- $\mathbb{Z}$ is the Integers
- $+$, $-$, $\times$ are defined the same way you probably learnt in primary school

# Notation

- We will use more or less standard notation in number theory
- $\mathbb{N}$ is the Natural Numbers, which includes $0$
- $\mathbb{Z}$ is the Integers
- $+$, $-$, $\times$ are defined the same way you probably learnt in primary school
- $a|b$ means there exists an integer $k$ such that $ka = b$

# Notation

- We will use more or less standard notation in number theory
- $\mathbb{N}$ is the Natural Numbers, which includes $0$
- $\mathbb{Z}$ is the Integers
- $+$, $-$, $\times$ are defined the same way you probably learnt in primary school
- $a|b$ means there exists an integer $k$ such that $ka = b$
- $a \equiv b$ in $\mod m$ means that $m|(b-a)$

# Notation

- We will use more or less standard notation in number theory
- $\mathbb{N}$ is the Natural Numbers, which includes $0$
- $\mathbb{Z}$ is the Integers
- $+$, $-$, $\times$ are defined the same way you probably learnt in primary school
- $a|b$ means there exists an integer $k$ such that $ka = b$
- $a \equiv b$ in $\mod m$ means that $m|(b - a)$
- $\mathbb{Z}_m$ is pretty much $\mathbb{Z}$ but with $=$ redefined so that $a = b$ means $a \equiv b$ in $\mod m$

# Advantages of modular spaces

- Working in $\mathbb{Z}_m$ is something you will find yourself doing a lot when solving number theory problems (and competitive maths is full of those)
- Often, the right choice of $\mathbb{Z}_m$ can greatly simplify the problem and allow you to find the solution pretty quickly

# Advantages of modular spaces

- Working in $\mathbb{Z}_m$ is something you will find yourself doing a lot when solving number theory problems (and competitive maths is full of those)
- Often, the right choice of $\mathbb{Z}_m$ can greatly simplify the problem and allow you to find the solution pretty quickly
- Example: Decimal Palindromes are numbers that look the same backwards when written in the decimal base system. Prove that all decimal palindromes with an even number of digits are divisible by 11.

# Prime modular spaces

- A prime modular space is $\mathbb{Z}_p$ where $p$ is some prime number. They are useful because they have (nearly) all the properties that you are used to when working with numbers:

# Prime modular spaces

- A prime modular space is $\mathbb{Z}_p$ where $p$ is some prime number. They are useful because they have (nearly) all the properties that you are used to when working with numbers:
  - $ab = 0$ means that $a = 0$ or $b = 0$

# Prime modular spaces

- A prime modular space is $\mathbb{Z}_p$ where $p$ is some prime number. They are useful because they have (nearly) all the properties that you are used to when working with numbers:
  - $ab = 0$ means that $a = 0$ or $b = 0$
  - for fixed $a \neq 0$ and $b$, there is one and only one $k$ such that $ak = b$.

# Prime modular spaces

- A prime modular space is $\mathbb{Z}_p$ where $p$ is some prime number. They are useful because they have (nearly) all the properties that you are used to when working with numbers:
  - $ab = 0$ means that $a = 0$ or $b = 0$
  - for fixed $a \neq 0$ and $b$, there is one and only one $k$ such that $ak = b$.
- the second property is cool because not even $\mathbb{Z}$ has that property, so in a sense $\mathbb{Z}_p$ is more powerful than $\mathbb{Z}$.

# Prime modular spaces

- A prime modular space is $\mathbb{Z}_p$ where $p$ is some prime number. They are useful because they have (nearly) all the properties that you are used to when working with numbers:
  - $ab = 0$ means that $a = 0$ or $b = 0$
  - for fixed $a \neq 0$ and $b$, there is one and only one $k$ such that $ak = b$.
- the second property is cool because not even $\mathbb{Z}$ has that property, so in a sense $\mathbb{Z}_p$ is more powerful than $\mathbb{Z}$.
- practice: find $n \in \mathbb{Z}_7$ such that $4n = 3$

# Bezout's identity

- For any pair of integers $p$, $q$ there exist two integers $a$, $b$ (called Bezout coefficients) such that:

$$ap + bq = \gcd(p, q)$$

# Bezout's identity

- For any pair of integers $p$, $q$ there exist two integers $a$, $b$ (called Bezout coefficients) such that:

$$ap + bq = \gcd(p, q)$$

- An obvious special case is if $p$ and $q$ are coprime, in which case the RHS is $1$.

# Inverses

- If we fix some modulo $m$ and choose some $a$ coprime to $m$ then Bezout tells us there exist $a^{-1}$ and $k$ such that:

$$aa^{-1} + km = 1$$

ie

$$aa^{-1} = 1$$

in $\mathbb{Z}_m$. We call $a^{-1}$ the "inverse" or "reciprocal" to $a \in \mathbb{Z}_m$.

# Inverses

- If we fix some modulo $m$ and choose some $a$ coprime to $m$ then Bezout tells us there exist $a^{-1}$ and $k$ such that:

$$aa^{-1} + km = 1$$

ie

$$aa^{-1} = 1$$

in $\mathbb{Z}_m$. We call $a^{-1}$ the "inverse" or "reciprocal" to $a \in \mathbb{Z}_m$.

- if it exists, $a^{-1}$ is unique within $\mathbb{Z}_m$.

# Inverses

- If we fix some modulo $m$ and choose some $a$ coprime to $m$ then Bezout tells us there exist $a^{-1}$ and $k$ such that:

$$aa^{-1} + km = 1$$

  ie

$$aa^{-1} = 1$$

  in $\mathbb{Z}_m$. We call $a^{-1}$ the "inverse" or "reciprocal" to $a \in \mathbb{Z}_m$.
- if it exists, $a^{-1}$ is unique within $\mathbb{Z}_m$.
- if $m$ is prime then $a$ being coprime to $m$ is equivalent to $a \neq 0$ in $\mathbb{Z}_m$, so any nonzero number has an inverse

# Inverses

- If we fix some modulo $m$ and choose some $a$ coprime to $m$ then Bezout tells us there exist $a^{-1}$ and $k$ such that:

$$aa^{-1} + km = 1$$

  ie

$$aa^{-1} = 1$$

  in $\mathbb{Z}_m$. We call $a^{-1}$ the "inverse" or "reciprocal" to $a \in \mathbb{Z}_m$.
- if it exists, $a^{-1}$ is unique within $\mathbb{Z}_m$.
- if $m$ is prime then $a$ being coprime to $m$ is equivalent to $a \neq 0$ in $\mathbb{Z}_m$, so any nonzero number has an inverse
- This number is very analogous to what $\frac{1}{x}$ is to $x$ in like the rationals or the reals, we can take the analogy a step further and define division: $\frac{a}{b} = ab^{-1}$.

# Inverses

- If we fix some modulo $m$ and choose some $a$ coprime to $m$ then Bezout tells us there exist $a^{-1}$ and $k$ such that:

$$aa^{-1} + km = 1$$

  ie

$$aa^{-1} = 1$$

  in $\mathbb{Z}_m$. We call $a^{-1}$ the "inverse" or "reciprocal" to $a \in \mathbb{Z}_m$.
- if it exists, $a^{-1}$ is unique within $\mathbb{Z}_m$.
- if $m$ is prime then $a$ being coprime to $m$ is equivalent to $a \neq 0$ in $\mathbb{Z}_m$, so any nonzero number has an inverse
- This number is very analogous to what $\frac{1}{x}$ is to $x$ in like the rationals or the reals, we can take the analogy a step further and define division: $\frac{a}{b} = ab^{-1}$.
- This surprisingly satisfies pretty much every property you might expect division to have!

# Powers

Let's consider how powers work in $\mathbb{Z}_p$ where $p$ is prime

# Powers

Let's consider how powers work in $\mathbb{Z}_p$ where $p$ is prime

- Fixing some nonzero $a \in \mathbb{Z}_p$, consider a graph whose vertices are members or $\mathbb{Z}_p$ and every arrow is of the form $x \to ax$.

# Powers

Let's consider how powers work in $\mathbb{Z}_p$ where $p$ is prime

- Fixing some nonzero $a \in \mathbb{Z}_p$, consider a graph whose vertices are members or $\mathbb{Z}_p$ and every arrow is of the form $x \to ax$.
- $\mathbb{Z}_p$ is finite in size so there can be no infinite chains of arrows, ie every chain must loop back to itself.

# Powers

Let's consider how powers work in $\mathbb{Z}_p$ where $p$ is prime

- Fixing some nonzero $a \in \mathbb{Z}_p$, consider a graph whose vertices are members or $\mathbb{Z}_p$ and every arrow is of the form $x \to ax$.
- $\mathbb{Z}_p$ is finite in size so there can be no infinite chains of arrows, ie every chain must loop back to itself.
- $a$ is invertible so every vertex must have exactly one arrow pointing towards it, means the graph can be decomposed into disconnected cycles

# Powers

Let's consider how powers work in $\mathbb{Z}_p$ where $p$ is prime

- Fixing some nonzero $a \in \mathbb{Z}_p$, consider a graph whose vertices are members or $\mathbb{Z}_p$ and every arrow is of the form $x \to ax$.
- $\mathbb{Z}_p$ is finite in size so there can be no infinite chains of arrows, ie every chain must loop back to itself.
- $a$ is invertible so every vertex must have exactly one arrow pointing towards it, means the graph can be decomposed into disconnected cycles
- other than the $0$ self-cycle, every other cycle must be the same size

# Powers

Let's consider how powers work in $\mathbb{Z}_p$ where $p$ is prime

- Fixing some nonzero $a \in \mathbb{Z}_p$, consider a graph whose vertices are members or $\mathbb{Z}_p$ and every arrow is of the form $x \to ax$.
- $\mathbb{Z}_p$ is finite in size so there can be no infinite chains of arrows, ie every chain must loop back to itself.
- $a$ is invertible so every vertex must have exactly one arrow pointing towards it, means the graph can be decomposed into disconnected cycles
- other than the $0$ self-cycle, every other cycle must be the same size
- every cycle is of size $C$ where $p - 1 \mid C$

# Fermat's Little Theorem

- for any prime $p$ and any integer $a$, $a^p - a \mid p$.

# Fermat's Little Theorem

- for any prime $p$ and any integer $a$, $a^p - a \mid p$.
- the proof relies on the fact that for any nonzero $a \in \mathbb{Z}_p$, $a^{p-1} = 1$.

# Fermat's Little Theorem

- for any prime $p$ and any integer $a$, $a^p - a \mid p$.
- the proof relies on the fact that for any nonzero $a \in \mathbb{Z}_p$, $a^{p-1} = 1$.
- More generally if $m$ and $n$ differ by a multiple of $p - 1$, then $a^m = a^n$
- example: what is the remainder of $4^{119}$ when divided by $11$?

# Totient Theorem

- we can generalise this result to non-prime $m \in \mathbb{Z}$ in general, by only considering members of $\mathbb{Z}_m$ coprime to $m$.
- define $\phi(m)$ as the number of such integers (this was $p - 1$ for prime $p$)
- by the same argument as with Fermat's Little Theorem above, we get

$$a^{\phi(m)} = 1$$

  for any $a$ coprime to $m$.
- this is all well and good, but how do we even know what $\phi(m)$ even is?

# Chinese Remainder Theorem

- Given two coprime numbers $p$ and $q$, if you know the remainders of $x$ when divided by $p$ and $q$, you know the remainder of $x$ when divided by $pq$.

# Chinese Remainder Theorem

- Given two coprime numbers $p$ and $q$, if you know the remainders of $x$ when divided by $p$ and $q$, you know the remainder of $x$ when divided by $pq$.
- This is essentially a function of the form:

$$\mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_{pq}$$

# Chinese Remainder Theorem

- Given two coprime numbers $p$ and $q$, if you know the remainders of $x$ when divided by $p$ and $q$, you know the remainder of $x$ when divided by $pq$.
- This is essentially a function of the form:

$$\mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_{pq}$$

- Note that the converse is pretty easy. If an integer is of the form $r + kpq$, then the remainders with respect to $p$ and $q$ are $r$ as a member of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ respectively.

# Chinese Remainder Theorem

- Given two coprime numbers $p$ and $q$, if you know the remainders of $x$ when divided by $p$ and $q$, you know the remainder of $x$ when divided by $pq$.
- This is essentially a function of the form:

$$\mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_{pq}$$

- Note that the converse is pretty easy. If an integer is of the form $r + kpq$, then the remainders with respect to $p$ and $q$ are $r$ as a member of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ respectively.
- Example: Consider $5 \in \mathbb{Z}_6$. Then it translates to $1 \in \mathbb{Z}_2$ and $2 \in \mathbb{Z}_3$.

# Chinese Remainder Theorem

- Given two coprime numbers $p$ and $q$, if you know the remainders of $x$ when divided by $p$ and $q$, you know the remainder of $x$ when divided by $pq$.
- This is essentially a function of the form:

$$\mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_{pq}$$

- Note that the converse is pretty easy. If an integer is of the form $r + kpq$, then the remainders with respect to $p$ and $q$ are $r$ as a member of $\mathbb{Z}_p$ and $\mathbb{Z}_q$ respectively.
- Example: Consider $5 \in \mathbb{Z}_6$. Then it translates to $1 \in \mathbb{Z}_2$ and $2 \in \mathbb{Z}_3$.
- We shall show this function is invertible, thereby showing the CRT.

# The more general case

- If we have a number of mutually coprime integers $n_1, n_2, n_3, \ldots n_i$ then we can string together applications of the two-integer CRT to get:

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_i} \to \mathbb{Z}_{n_1 n_2} \times \cdots \times \mathbb{Z}_{n_i} \to \cdots \to \mathbb{Z}_{n_1 n_2 \ldots n_i}$$

giving the more general result of the CRT.

# Using CRT to find invertible elements

- Consider coprime $p$ and $q$. Every invertible element of $\mathbb{Z}_pq$ corresponds to a pair of invertible elements in $\mathbb{Z}_p$ and $\mathbb{Z}_q$.

# Using CRT to find invertible elements

- Consider coprime $p$ and $q$. Every invertible element of $\mathbb{Z}_pq$ corresponds to a pair of invertible elements in $\mathbb{Z}_p$ and $\mathbb{Z}_q$.
- This means that if $\mathbb{Z}_p$ has $\phi(p)$ invertible elements and $\mathbb{Z}_q$ has $\phi(q)$ invertible elements, then the number of invertible elements in $\mathbb{Z}_{pq}$ $\phi(pq)$ must be the product $\phi(p)\phi(q)$.

# Using CRT to find invertible elements

- Consider coprime $p$ and $q$. Every invertible element of $\mathbb{Z}_pq$ corresponds to a pair of invertible elements in $\mathbb{Z}_p$ and $\mathbb{Z}_q$.
- This means that if $\mathbb{Z}_p$ has $\phi(p)$ invertible elements and $\mathbb{Z}_q$ has $\phi(q)$ invertible elements, then the number of invertible elements in $\mathbb{Z}_{pq}$ $\phi(pq)$ must be the product $\phi(p)\phi(q)$.
- $\phi$ is multiplicative for coprime numbers

# A formula for Totient Function

- Every positive integer has a factorisation into prime powers

$$x = {p_1}^{n_1} {p_2}^{n_2} \dots {p_i}^{n_i}$$

# A formula for Totient Function

- Every positive integer has a factorisation into prime powers

$$x = {p_1}^{n_1} {p_2}^{n_2} \dots {p_i}^{n_i}$$

- Powers of distinct primes are coprime, so CRT applies and

$$\phi(x) = \phi(p_1)^{n_1} \phi(p_2)^{n_2} \dots \phi(p_i)^{n_i}$$

# A formula for Totient Function

- Every positive integer has a factorisation into prime powers

$$x = {p_1}^{n_1} {p_2}^{n_2} \dots {p_i}^{n_i}$$

- Powers of distinct primes are coprime, so CRT applies and

$$\phi(x) = \phi(p_1)^{n_1} \phi(p_2)^{n_2} \dots \phi(p_i)^{n_i}$$

- Now all that is left is finding the totient function for an arbitary prime power $p^n$.

# A formula for Totient Function

- Every positive integer has a factorisation into prime powers

$$x = {p_1}^{n_1} {p_2}^{n_2} \dots {p_i}^{n_i}$$

- Powers of distinct primes are coprime, so CRT applies and

$$\phi(x) = \phi(p_1)^{n_1} \phi(p_2)^{n_2} \dots \phi(p_i)^{n_i}$$

- Now all that is left is finding the totient function for an arbitary prime power $p^n$.

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

# Where to from here?

- Number Theory is one of the oldest branches of mathematics, and a LOT of theorems have been discovered, this workshop barely scratches the surface
- Every new theorem you learn is a new tool in your toolbox, allowing you to make a quicker logical leap when solving competitive maths questions
- Some interesting avenues in number theory to explore are:
  - Fibonacci numbers, eg Cassini's identity, Catalan's identity, d'Ocagne's identity, etc
  - Diophantine Equations
  - Base systems
  - Recreational number theory, for the more casual mathematics enthusiasts
  - More formal number theory such as Algebraic Number Theory and Analytic Number Theory
  - Applications in cryptography

# Attendance form :D

# Further events

Please join us for the Dynamic Programming Workshop tomorrow (Also $\frac{\tau}{2}$ day!!)