Competitive
Programming and
Mathematics
Society

Number Theory

Sarthak Sahoo and Gordon Ye

Welcome

- All workshops shall be 2 hours long.
- The notes of the contents in the workshops shall be provided on the CPMSoc website.
- Each workshop will have an accompanying problem set, which can be found in the notes.
- There will be workshops on odd numbered weeks from week 5 on wards (That's this week).
- Hope you enjoy yourselves and feel free to ask questions during the workshops ☺.

Competitive Mathematics

- Well known competitions such as Putnam, IMC, SMMC.
- 6 hours contest, 3 hours per half.
- Having first year uni knowledge is a prerequisite.
- Challenging problems that are slightly different from typical uni exams.
- Have fun solving!

Table of contents

Notation

CPMSOC

1. $\mathbb{N} = \left\{1, 2, 3 \cdots\right\}$
2. $\mathbb{P} = \left\{\text{set of all primes}\right\}$
3. $\mathbb{P}_n = \left\{p \in \mathbb{P} : p \middle| n,\ n \in \mathbb{N}\right\}$

Revision

CPMSOC

Example

Let p be a prime number. Prove that there are infinitely many multiples of p whose last ten digits are all distinct.

Revision

CPMSOC

Example

Let p be a prime number. Prove that there are infinitely many multiples of p whose last ten digits are all distinct.

- The answer for $p = 2$ and $p = 5$ becomes obvious after some thought.

Revision

Example

Let p be a prime number. Prove that there are infinitely many multiples of p whose last ten digits are all distinct.

- The answer for $p = 2$ and $p = 5$ becomes obvious after some thought.
- Consider $p, 2p, 3p, ...999999999p$. We will prove that those numbers produces $10^{10} - 1$ different terminating sequences.

Revision

CPMSOC

Example

Let p be a prime number. Prove that there are infinitely many multiples of p whose last ten digits are all distinct.

- The answer for $p = 2$ and $p = 5$ becomes obvious after some thought.
- Consider $p, 2p, 3p, ...999999999p$. We will prove that those numbers produces $10^{10} - 1$ different terminating sequences.
- We will prove the above by proving any two numbers within the sequence have a difference that is not divisible by 10^{10}. Let's arbitrarily pick mp and np, where $1 \leq m, n \leq 999999999$.

Revision

Example

Let p be a prime number. Prove that there are infinitely many multiples of p whose last ten digits are all distinct.

- The answer for $p = 2$ and $p = 5$ becomes obvious after some thought.
- Consider $p, 2p, 3p, ...999999999p$. We will prove that those numbers produces $10^{10} - 1$ different terminating sequences.
- We will prove the above by proving any two numbers within the sequence have a difference that is not divisible by 10^{10}. Let's arbitrarily pick mp and np, where $1 \leq m, n \leq 999999999$.
- Since p is coprime to 10^{10} and $m - n$ does not divide 10^{10}, $p(m - n)$ is not divisible by 10^{10}.

Euclid's Gem

There are infinitely many primes! A fact that seems intuitively obvious, yet we shall present a proof (or rather we shall present Euclid's proof). Before proceeding to the proof we present a lemma.

Lemma (Fundamental Theorem of Arithmetic)

Every positive integer $n > 1$ can be written as the product of primes uniquely up to ordering.

Euclid's Gem

There are infinitely many primes! A fact that seems intuitively obvious, yet we shall present a proof (or rather we shall present Euclid's proof). Before proceeding to the proof we present a lemma.

Lemma (Fundamental Theorem of Arithmetic)

Every positive integer $n > 1$ can be written as the product of primes uniquely up to ordering.

Theorem (Infinitude of Primes)

There are infinitely many primes!

Euclid's Gem

CPMSOC

Arc CLUBS SUPPORTED BY Arc INDEPENDENTLY RUN

Proof.

We proceed by assuming that there are finitely many primes

$$\mathbb{P} = \left\{p_1, p_2, \cdots, p_n\right\},$$

we do not bother ourselves with the ordering of the elements in the set of primes denoted by $\mathbb{P}$.

Consider the following:

$$n = p_1 \cdots p_n + 1,$$

the above leaves a remainder of 1 when divided by each of the primes in the set $\mathbb{P}$,i.e, its not divisible by any prime in $\mathbb{P}$. However by the **FTA** n must be divisible by a prime $p_{n+1} \notin \mathbb{P}$, which is a contradiction since we assumed the set of all primes is finite. Hence $\mathbb{P}$ must be infinite. ■

Fermat's Little Theorem

Fermat's little theorem can be really use full in considering $a^k \pmod n$, and is a fundamental theorem in elementary number theory.
The theorem tells us how to treat powers of an integer modulo a natural number. And is essential for building up understanding of divisibility between different forms of numbers.
Before proceeding to proving Fermat's Little Theorem, we prove a little lemma,

Lemma

If p is a prime then,

$$(a+b)^p \equiv a^p + b^p \pmod p,$$

where $a, b \in \mathbb{Z}$.

Fermat's Little Theorem

CPMSOC

Arc CLUBS SUPPORTED BY Arc INDEPENDENTLY RUN

Proof.

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + pM, \ M \in \mathbb{Z}.$$

∎

Fermat's Little Theorem

CPMSOC

Arc CLUBS SUPPORTED BY Arc INDEPENDENTLY RUN

Proof.

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + pM, \;\; M \in \mathbb{Z}.$$

■

Corollary

***Corollary**: For $p \in \mathbb{P}$ (Induction),*

$$\left(\sum_{1 \le i \le n} a_i\right)^p \equiv \sum_{1 \le i \le n} a_i^p \pmod{p},$$

where $a_i \in \mathbb{Z}, \forall i$.

Fermat's Little Theorem

CPMSOC

Theorem (Fermat's Little Theorem)

For $a \in \mathbb{Z}$ *and* $p \in \mathbb{P}$ *such that* $\gcd(a, p) = 1$ *we have,*

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

Fermat's Little Theorem

CPMSOC

Arc CLUBS SUPPORTED BY Arc INDEPENDENTLY RUN

Theorem (Fermat's Little Theorem)

For $a \in \mathbb{Z}$ *and* $p \in \mathbb{P}$ *such that* $\gcd(a, p) = 1$ *we have,*

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

Proof.

Note that for $\gcd(a, p) = 1,\ a, p \in \mathbb{N}$,

$$a^p \equiv (\overbrace{1 + 1 + \cdots + 1}^{a \text{ times}})^p \equiv (\overbrace{1 + 1 + \cdots + 1}^{a \text{ times}}) \equiv a \pmod{p}$$

■

Euler's Totient Function

One generalization of Fermat's Little Theorem is what's known as Euler's Totient Theorem. Euler's Totient Theorem is naturally motivated through a specific counting problem. The Euler's $\varphi(n)$ counts the number of integers k such that $\gcd(k, n) = 1, k \in \mathbb{Z}/n\mathbb{Z}$.

The precise formulation is; for $n \in \mathbb{N} - \{1\}$

$$\varphi(n) = \left|\left\{a \in \mathbb{Z}_n : \gcd(a, n) = 1\right\}\right|,$$

we can define or check through the definition that $\varphi(1) = 1$.

Euler's Totient Function

One generalization of Fermat's Little Theorem is what's known as Euler's Totient Theorem. Euler's Totient Theorem is naturally motivated through a specific counting problem. The Euler's $\varphi(n)$ counts the number of integers k such that $\gcd(k,n) = 1, k \in \mathbb{Z}/n\mathbb{Z}$.

The precise formulation is; for $n \in \mathbb{N} - \{1\}$

$$\varphi(n) = \left|\left\{a \in \mathbb{Z}_n : \gcd(a,n) = 1\right\}\right|,$$

we can define or check through the definition that $\varphi(1) = 1$.

We present two important lemmas, that are not only important on their own but also are precursors of a method to proving an explicit formulation of Euler's Totient function.

Euler's Totient Function

CPMSOC

Lemma

For $p \in \mathbb{P}$ *and* $a \in \mathbb{N}$,

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

Euler's Totient Function

CPMSOC

Lemma

For $p \in \mathbb{P}$ and $a \in \mathbb{N}$,

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

Proof.

Two of them actually, the first one is to simply count the set $\varphi(p^a) = \left|\left\{b \in \mathbb{Z}_{p^a} : \gcd(b, p^a) = 1\right\}\right| = \left|\left\{p, 2p, \cdots, p^2, p^2 + p, \cdots, \right\}\right|$. Or use the inclusion-exclusion principle,

$$\varphi(p^a) = p^a - \left|\left\{b : 1 \leq b \leq p^a, p|b\right\}\right| = p^a - \frac{p^a}{p}$$

. ∎

Lemma

If $m, n \in \mathbb{N}$ *and* $\gcd(m, n) = 1$ *, then*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

This makes φ *multiplicative.*

Proof.

Consider the following matrix:

$$\Phi = \begin{pmatrix} 1 & 2 & \cdots & m \\ m+1 & m+2 & \cdots & 2m \\ \vdots & \vdots & \ddots & \vdots \\ m(n-1)+1 & m(n-1)+1 & \cdots & mn \end{pmatrix},$$

there are $\varphi(mn)$ numbers in the matrix above that are relatively prime to mn.

However, note that there are also $\varphi(m)$ columns containing containing those elements in the table that are relatively prime to m. Then we take note that there are $\varphi(n)$ elements in each $\varphi(m)$ columns that are relatively prime to n, therefore there are $\varphi(m)\varphi(n)$ elements that are co-prime to mn.

$$\therefore \varphi(mn) = \varphi(m)\varphi(n).$$

∎

Euler's Theorem

CPMSOC

Theorem

Let $\varphi : \mathbb{N} \to \mathbb{N}$ *then,*

$$\varphi(n) = n \prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p}\right).$$

Proof.

This is a corollary of the two **Lemmas** presented above. ■

Euler's Theorem

CPMSOC

Theorem

Let $\varphi : \mathbb{N} \to \mathbb{N}$ *then,*

$$\varphi(n) = n \prod_{p \in \mathbb{P}_n} \left(1 - \frac{1}{p}\right).$$

Proof.

This is a corollary of the two **Lemmas** presented above. ■

Theorem (Euler's Theorem)

If $n \in \mathbb{N}$, $gcd(a, n) = 1$ *and* $\varphi : \mathbb{N} \to \mathbb{N}$,

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

Proof.

Consider the set of units modulo n

$$R = \left\{x_1, x_2, \cdots, x_{\varphi(n)}\right\},$$

where $1 \leq x_i \leq n - 1$, $\gcd(x_i, n) = 1$ and all the x_i are distinct. We consider the left coset ,

$$aR = \left\{ax_1, \cdots, ax_{\varphi(n)}\right\}.$$

Since multiplying by a is a bijection we have that $aR = R$, therefore we have that

$$\prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} (ax_i) \pmod{n}, \iff a^{\varphi(n)} \equiv 1 \pmod{n}$$

∎

Example Problems

CPMSOC

1. if $a \equiv b \pmod{n}$, show that $a^n \equiv b^n \pmod{n^2}$.
2. Let a and b be positive integers. Prove that

$$\gcd(n^a - 1, n^b - 1) = n^{\gcd(a,b)} - 1.$$

3. Let n be an integer greater than 2. Prove that among the fractions

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n},$$

an even number are irreducible.

4. Determine the respective last digit (unit digit) of the numbers

$$3^{1001} 7^{1002} 13^{1003}, \quad \underbrace{7^{7^{\cdot^{\cdot^{7}}}}}_{1001\ 7's}.$$