CPMSoc Number Theory Workshop

March 16, 2022

"Prime numbers have always fascinated mathematicians, professional and amateur alike. They appear among the integers, seemingly at random, and yet not quite: there seems to be some order or pattern, just a little below the surface, just a little out of reach."

— Underwood Dudley

1 Preliminaries

1.1 Pre-Requisites

1. Modular Arithmetic
2. Divisibility
3. Primality and Coprimality
4. Should have/be done/doing MATH1081 (if not that's fine too)

Note: The above pre-requisites have been addressed in the first number theory workshop. You can find it on the CPMSoc website :). Do go through that before reading the following notes.

1.2 Notation

1. $\mathbb{N} = \{1, 2, 3 \cdots\}$
2. $\mathbb{P}_n = \{p \in \mathbb{P} : p|n,\ n \in \mathbb{N}\}$
3. Any problem in the problem section that is starred (*) is a standard theorem as well and therefore is highly recommended to be learnt.

2 Euclid's Proof

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: There are infinitely many primes!

Proof. We proceed by assuming that there are finitely many primes

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

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. □

3 Fermat's Little Theorem and Generalizations

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

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

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

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

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

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

□

3.2 Euler's Totient Theorem

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 $\varphi(1) = 1$.

Note: the elements in $\left\{ a \in \mathbb{Z}_n : \gcd(a, n) = 1 \right\}$ are also called units.

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.

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

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

Proof. We simply use the inclusion-exclusion principle to arrive at,

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

. □

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.

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

Note: For proving that there are $\varphi(n)$ elements in each $\varphi(m)$ columns, consider each element modulo n and try to map it to all integers from 0 to $n-1$.

□

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 $n \in \mathbb{N}$, and $\varphi : \mathbb{N} \to \mathbb{N}$,

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

Note: We see that if $n = p$ then $\varphi(p) = p - 1$, and hence the above turns into Fermat's.

Proof.
Consider the set of units modulo n

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

where $1 \leq x_i \leq m-1$, $\gcd(x_i, n) = 1$ 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

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

□

4 Problems

4.1 Introductory Problems

1. Give an example of 20 consecutive numbers being composite.
2. Prove the claim : If one wishes to find prime factor of $n \in \mathbb{N}$, then they should check divisibility against all prime factors up to $\lfloor \sqrt{n} \rfloor$.
3. Find n such that $2^n | 3^{1024} - 1$.
4. Let $p \geq 7$ be a prime. Prove that the number

   $$\underbrace{11\cdots1}_{(p-1)1's}$$

   is divisible by p.
5. Determine with proof whether following is an integer or not :

   $$\sqrt{1976^{1977} + 1978^{1979}}.$$

6. Prove that for $m, n \in \mathbb{N}$

   $$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn},$$

   whenever $\gcd(m, n) = 1$.

4.2 Intermediate Problems

1. (IMO 2005) Consider the sequence $\left\{a_1, a_2, \cdots\right\}$ defined by

   $$a_n = 2^n + 3^n + 6^n - 1$$

   for all positive integers n. Determine all positive integers that are relatively prime to every term of the sequence.

2. Determine the last three digits of the number

$$2003^{2002^{2001}}.$$

3. (Simon Marais 2021) Define the sequence of integers $a_1, a_2, \cdots$ by $a_1 = 1$ and

$$a_{n+1} = (n + 1 - \gcd(a_n, n)) \times a_n$$

for all integers ≥ 1. Prove that $\frac{a_{n+1}}{a_n} = n \iff n \in \mathbb{P}$ or $n = 1$.

4. Give an example of 11 consecutive positive integers the sum of whose squares is a perfect square.

5. (Wilson's Theorem)* A natural number $n > 1$ is prime $\iff$

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

Hint: Consider the polynomial $g(x) = (x-1)(x-2)\cdots(x-(p-1))$.