Note Title 8/1/2022

Lecture - 3:

Tuesday, 2/8/2022

1st principle of mathematical induction: Let A be a non-empty subset of $\mathbb{N}$. Suppose that (i) $1 \in A$ and (ii) $n \in A \Rightarrow 1+n \in A$.

Then, $A = \mathbb{N}$.

2nd principle of mathematical induction: Let A be a non-empty subset of $\mathbb{N}$. Suppose that (i) $1 \in A$ and (ii) $1, 2, \ldots, n \in A \Rightarrow 1+n \in A$.

Then $A = \mathbb{N}$.

Theorem: The above two principles are equivalent to the well-ordering principle of $\mathbb{N}$.

#

§ <u>Primes</u>: An integer $p > 1$ is called a prime number if there is no divisor d of p satisfying $1 < d < p$ That is, 1 and p are the only positive divisors of p

If an integer $a > 1$ is not a prime, then it is called a composite number.

<u>Theorem 1</u>: If p is a prime, and $p \mid ab$, then $p \mid a$ or $p \mid b$.

More generally, if $p \mid a_1 \cdot a_2 \cdots a_n$, then p divides at least one factor a_i of the product.

<u>Proof</u>: Suppose that $p \nmid a$. Then, $\gcd(a, p) = 1$. Since $p \mid ab$, so $p \mid b$.

If $p \mid a_1 a_2 a_3$, then $p \mid a_1 b_1$, where $b_1 = a_2 a_3$. $\Rightarrow p \mid a_1$ or $p \mid b_1$

If $p \mid b_1$, then $p \mid a_2 a_3$ implies $p \mid a_2$ or $p \mid a_3$. Hence, $p \mid a_i$ for some $i = 1, 2, 3$.

In general, we can use mathematical induction.
So, we assume that the result holds whenever p divides a product with fewer than n factors.

Now, if $p \mid a_1 a_2 \cdots a_n$, we write $p \mid a_1 c$ where $c = a_2 a_3 \cdots a_n$.

Then, $p \mid a_1$ or $p \mid c$. If $p \mid a_1$, we are done.
If $p \mid c$, we apply the induction hypothesis to conclude that $p \mid a_i$ for some $i = 2, 3, \ldots, n$.

Hence, $p \mid a_i$ for some $i = 1, 2, \ldots, n$.

This completes the proof. #

Theorem 2 (Fundamental Theorem of Arithmetic):
Every integer $n > 1$ can be expressed as a product of primes. Also, the factorization of n into primes is unique apart from the order of the prime factors.

Proof: Let $n > 1$. If n is a prime, then the integer itself stands as a product with a single factor. Otherwise, $n = n_1 n_2$, where $1 < n_1 < n$, $1 < n_2 < n$. If n_1 is a prime, then n_1 remains in the factorization. Otherwise, it will factor into, say, $n_3 n_4$ where $1 < n_3 < n_1$ and $1 < n_4 < n_1$. Similarly, we proceed with n_2. This process of writing each composite number that arises as a product of factors must terminate because the factors are smaller than the composite number itself, and each factor is greater than 1.

Thus, we can write n as a product of primes as

$$n = p_1^{a_1} \cdots p_k^{a_k}, \quad \text{where } p_1, \ldots, p_k \text{ are distinct primes, and } a_1, \ldots, a_k \text{ are positive.}$$

We next prove that the factorization of n into product of primes is unique apart from the order of the prime factors.

Suppose that there is an integer n with two different factorizations. Dividing out any primes common to the two reepresentations, we would have an equality of the form

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \longrightarrow (1)$$

where the factors p_i and q_j are primes, not necessarily all distinct and $p_i \neq q_j$ for any i and j.

But this impossible, because $p_1 \mid q_1 q_2 \cdots q_s \Rightarrow p_1 \mid q_j$ for some j (by Theorem 1).

$\Rightarrow p_1 = q_j$ for some j.

This completes the proof. #

Theorem 3 (Euclid): There are infinitely many primes. That is, there is no end to the sequence of primes

$$2, 3, 5, 7, 11, 13, \ldots$$

1st proof: Suppose that there are only finitely many primes, say, $p_1, p_2, \ldots, p_r$. Consider $n = 1 + p_1 p_2 \cdots p_r$.

Since $n > p_i$ for all i, so n is not a prime (as $p_1, \ldots, p_r$ are the only primes)

By Fundamental Theorem of Arithmetic, n has a prime divisor p.

Since $p_1, \ldots, p_r$ are the only primes, so $p = p_j$ for some j.

$\Rightarrow p_j$ divides $1 = n - p_1 p_2 \cdots p_r$, which is a contradiction.

$\therefore$ There are infinitely many primes. #

__2nd proof:__ Fermat's numbers are defined as:

$$F_n = 2^{2^n} + 1, \quad n \geq 1 \qquad F_1 = 5,\ F_2 = 2^4 + 1 = 17$$

$$F_3 = 2^8 + 1 = 257, \ldots$$

We first prove that $\gcd(F_n, F_{n+k}) = 1$ for all $k \geq 1$

(That is, any two distinct Fermat's numbers are co-prime).

Let $m \mid F_n$ and $m \mid F_{n+k}$, where $k \geq 1$.

Put $x = 2^{2^n}$. Then, $\dfrac{F_{n+k} - 2}{F_n} = \dfrac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \dfrac{x^{2^k} - 1}{x + 1}$

$$= x^{2^k - 1} - x^{2^k - 2} + \ldots - 1, \text{ which is an integer.}$$

$\Rightarrow$ F_n divides $F_{n+k} - 2$

Since $m \mid F_n$ and $m \mid F_{n+k}$, so $m \mid 2$.
But Fermat's numbers are odd, and hence $m = 1$.

$\therefore \gcd(F_n, F_{n+k}) = 1$ for all $k \geq 1$.

Now, consider the prime factoreizations of the Fermat's numbers,
Since $\gcd(F_n, F_{n+k}) = 1$, so the prime divisors of F_n and F_{n+k} are all different.

Since there are infinitely many Fermat's number, so there are infinitely many prime numbers.

\#