III. Number Theory

A. Natural Numbers : $\mathbb{N} := \{0, 1, 2, 3, \dots\}$

1. Peano Axioms (1889)

i. $0 \in \mathbb{N}$

ii. If $n \in \mathbb{N}$, then $S(n) \in \mathbb{N}$

(Successor function $S(n) = n+1$)

iii. $\forall n \in \mathbb{N}$, $0 \neq S(n)$

iv. $\forall m, n \in \mathbb{N}$, if $m \neq n$, then $S(m) \neq S(n)$

v. If $A \subseteq \mathbb{N}$ with $0 \in A$ and $\forall x \in A$, $S(x) \in A$, then $A = \mathbb{N}$.

Def: The Zero : 0

The Unit : 1

Primes : 2, 3, 5, 7, 11, 13, ...

Composites : 4, 6, 8, 10, 12, ...

Thm : $\exists$ countably infinitely many primes.

(Euclid) Pf (Contradiction): Suppose there are only finitely many primes: $\{p_1, p_2, \dots, p_n\}$. Consider $p_1 p_2 \cdots p_n + 1$. Since $p_j \nmid 1$ $\forall j$, $1 \le j \le n$, then $p_j \nmid (p_1 p_2 \cdots p_n + 1)$. Thus $p_1 p_2 \cdots p_n + 1$ is relatively prime compared to $\{p_1, p_2, \dots, p_n\}$. So either $p_1 p_2 \cdots p_n + 1$ is prime or $p_1 p_2 \cdots p_n + 1$ is composite but not on our list, making our list of primes incomplete. $(\rightarrow\leftarrow)$

Notation: $a \nmid b$ = "a does not divide b", ex) $3 \nmid 1$

(Goldbach 1730) Pf: Consider the Fermat numbers.

$F_n := 2^{2^n} + 1 \quad \forall n \in \mathbb{N}$

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$,

$F_4 = 65,537$,

$F_5 = 4294967297 = 641 \times 6700417$.

Lemma: $\prod_{k=0}^{n-1} F_k = F_n - 2 \quad \forall n \in \mathbb{Z}^+$

Pf (Induction):

1) For $n = 1$, we need $\prod_{k=0}^{1-1} F_k = F_0 = F_1 - 2$. ✓

2) Now Suppose $\prod_{k=0}^{n-1} F_k = F_n - 2$ and show that $\prod_{k=0}^{n} F_k = F_{n+1} - 2$.

Inductive Assumption

Notice that $\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) F_n$

$= (F_n - 2) F_n = \left(2^{2^n} - 2\right)\left(2^{2^n} + 1\right)$

To be continued...