Day 19 - Topics in Number Theory #4: Infinitude of Primes, Euclid's Theorem

Definitions

- RECALL: A natural number n is **prime** if it has exactly two distinct positive divisors, 1 and n. A natural number is **composite** if it is not prime.
- FACT: A number $n > 1$ is **composite** if an only if $n = ab$ for some natural numbers $a, b < n$.

Theorem NT 3.1: Every natural number >1 is either prime or divisible by a prime.

Theorem NT 3.2 (**Euclid's Theorem**). There are infinitely many primes.

Theorem NT 3.3 (**Fundamental Theorem of Arithmetic**). Every natural number >1 is either prime or can be written as a unique product of primes.

Theorem NT 3.3 (**Fundamental Theorem of Arithmetic - MORE DETAIL**). Every natural number $n > 1$ has a unique prime factorization. That is, *n* has a prime factorization (`can be written as a prime or product of primes'), and if $n = p_1 p_2 p_3 ... p_k$ and $n = q_1 q_2 q_3 ... q_l$ are two prime factorizations of *n*, then $k = l$ and the primes p_i and q_i are the same, except they may be in a different order.

<u>Prop.</u> There are infinitely many primes.

<u>Proof</u> <u>(Contradiction)</u>. Suppose there are finitely many primes, n many for some $n \in \mathbb{N}$.
let $p_1, p_2, p_3, p_4, \dots, p_n$ be all the primes.

let $S = p_1 p_2 p_3 p_4 \cdots p_n + 1$

<u>claim:</u> $p_1 \nmid S$.

<u>proof of claim:</u> let $d = p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n$

So $S = p_1 d + 1$ note $d \in \mathbb{Z}$ by closure.

thus S has a remainder of 1 when

divided by p_i, thus $p_i \nmid S$ $\square$

<u>claim</u> for any i, $1 \le i \le n$, we have $p_i \nmid S$.

<u>proof of claim</u>. let p_i be one of the primes
let e = the product of all primes except p_i, $e \in \mathbb{Z}$ by closure.

then $S = p_i \cdot e + 1$

Does $p_i \mid p_i \cdot e$? Yes.

$p_i \cdot e = p_i \cdot (\underbrace{\text{an integer}}_{e})$

$p_i = 5$
$e = 6$
$5 \mid 30$?
$30 = 5 \cdot 6$

thus S has a remainder of 1 when divided by p_i
so $p_i \nmid S$. $\square$

Is S prime itself? FACT: NOPE.

$2 \cdot 3 \cdot 5 + 1 = 6 \cdot 5 + 1 = \underline{31}$ is prime.

$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 210 + 1 = 211$ is prime

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 =$ ______ is prime.

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = \underline{30031}$ is it prime?
$= 59 \cdot 509$
NO

Recall Fact: S is either prime, or divisible by a prime.
In either case there is a

In either case, there is a prime number that is not on our list $p_1, p_2, \ldots, p_n$.
This is a contradiction, we assumed that our list included all primes. $\square$

Theorem (fundamental theorem of arithmetic). Every natural number $n > 1$ can be written as a unique product of primes.

Note: two parts, existence and uniqueness

Part 1 claim: every natural number $n > 1$ is either prime or can be written as a product of primes.

proof (contradiction). Suppose there exist natural numbers that are not prime and cannot be written as a product of primes.
let $S = \{n \in \mathbb{N} \mid n$ is not prime and n cannot be written as a product of primes$\}$
let m be the smallest member of S.
What facts do we know about m?

$m \in \mathbb{N}$ (therefore $m \in \mathbb{Z}$)
m is not prime.
m is not a product of prime
} because $m \in S$.

so $m = ab$ for some natural numbers $a, b < m$.

case 1: both a, b are prime
then $m = a \cdot b$ is a product of primes, contradiction.

case 2: at least one of them is not prime.
(OR "one of them is composite")

WLOG suppose a is composite.
note that a can't be written as a product of primes, because if so we could use that to write m as a product of primes,

$m = a \cdot b$

which would give a contradiction.

Then $a \in S$ because it's not prime and can't be written as a product of primes,

"cannot be written as a product of primes"

contradiction since $a < m$ and m is smallest member of S

$\square$

part 2 uniqueness claim: the prime factorization of a natural number is unique:

Strategy: $S = \{n \in \mathbb{N} \mid n \text{ has more than one different prime factorization}\}$

let m = smallest member of S.

$m \to p_1 p_2 p_3 \cdots p_n$

two factorizations

$m \to q_1 q_2 \cdots q_m$ $\quad p, q \in$ Primes.

Strategy: eliminate one factor, find a smaller member of S.

$\square$