Primes

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

Fundamental Theorem of Arithmetic

Any natural number $n \in \mathbb{N}$ has a factorization into primes that is unique modulo the arrangement of the factors: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ for primes $p_1, p_2, \ldots, p_r$.

canonical factorization: $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$

pf. Let $n \in \mathbb{N}$, $n \geq 2$. If n is prime, done: $n = p$.

If n is composite, then n has a prime, p_1, as its smallest divisor. Keep going: $\Rightarrow n = p_1 p_2 \cdot \ldots \cdot p_r$.

uniqueness: suppose that $p_1 p_2 \cdot \ldots \cdot p_r = q_1 q_2 \cdot \ldots \cdot q_s$.

∎

SIEVE OF ERATOSTHENES

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~

~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~

~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~

41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ ~~53~~

~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ ~~59~~ ~~60~~ 61 ~~62~~ ~~63~~ ~~64~~ ~~65~~

~~66~~ ~~67~~ ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ ~~73~~ ~~74~~ ~~75~~ ~~76~~ ~~77~~ ...

Thm There are infinitely many primes. (Euclid)

pf: Suppose, to the contrary, that there are only finitely many primes, $p_1, p_2, \dots, p_n$. Then define

$$P = p_1 p_2 \cdots p_n + 1.$$

By assumption, P is composite & must have prime divisors. This would force $p_i \mid 1$ for some i, a contradiction. ∎

Thm. (Bertrand / Chebyshev) If $n \geq 2$, there is a prime between n and $2n$.

Corollary: Let p_n be the n^{th} prime. Then $p_n \leq 2^n$.

pf. via induction base: $2 \leq 2$ ✓ IH: $p_n \leq 2^n$ for some n.
Then $2^n \leq p \leq 2^{n+1} \Rightarrow p_{n+1} \leq 2^{n+1}$. ∎