Primes

Defn An integer $p > 1$ is **prime** iff the only divisors of p are 1 and itself.

Formally: $\text{Prime}(p) = (p > 1) \wedge \left(\neg\left(\exists a, b : \mathbb{Z}.\ ab = p \wedge a \neq p \wedge b \neq p\right)\right)$

$\text{Prime}(p) = (p > 1) \wedge \left(\neg\, \exists n : \mathbb{N}.\ (n > 1) \wedge (n < p) \wedge (n \mid p)\right)$

$\text{Prime}(p) = (p > 1) \wedge \left(\forall d : \mathbb{N}.\ (d \mid p) \longrightarrow (d = 1) \vee (d = p)\right)$.

Ex. $2, 3, 5, 7 \ldots$ are prime. 6 is not prime since $2 \cdot 3 = 6$.

A number > 1 which is **not** prime is called Composite.

Note: 1 is neither prime nor composite!

Thm (Fundamental Theorem of Arithmetic) Every positive integer can be factored into a product of zero or more primes. (Note: a product of zero primes is 1.) Moreover, this product of primes is unique if the primes are listed from smallest to biggest.

Proof — later (needs induction).

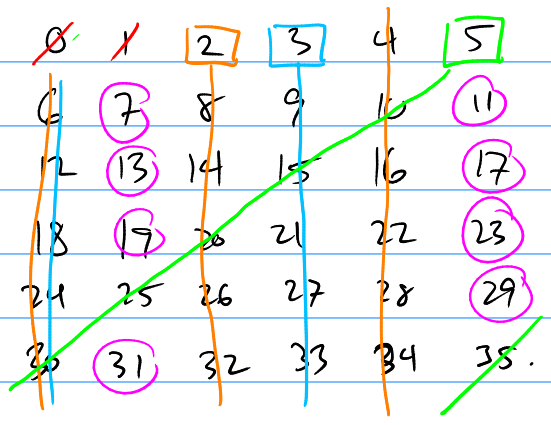
Thm If n is composite, then it has a prime divisor $\leq \sqrt{n}$.

$\forall n : \mathbb{Z}^+.\ \text{Composite}(n) \longrightarrow \exists p : \mathbb{Z}^+.\ \text{Prime}(p) \wedge (p \mid n) \wedge (p \leq \sqrt{n})$.

Proof. Let n be an arbitrary positive integer and suppose n is composite. Then there must exist a, b such that $ab = n$ and $1 < a, b < n$.

- If a and b are both $> \sqrt{n}$, then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is not possible since $ab = n$.
- Therefore one of a or b must be $\leq \sqrt{n}$. Suppose it is $a \leq \sqrt{n}$. We know that $a | n$ since $ab = n$. However, we don't know whether a is prime. But by the FTA, a is a product of primes; let p be one of them. Then $p \leq a \leq \sqrt{n}$ and $p | a | n$, and therefore p is a prime whose existence we wanted to show.

Sieve of Eratosthenes



Thm There are infinitely many prime numbers.

Proof. By contradiction. Suppose there are only finitely many primes $p_1, p_2, \ldots, p_k$. Consider

$$Q = p_1 p_2 p_3 \cdots p_k + 1.$$

Q cannot be divisible by any of the primes since it would give a remainder of 1.

But the FTA tells us Q is a product of primes, none of which are on our list — this is a contradiction.

Biggest known prime is $2^{82589933} - 1$.