Primes!

Note, for any $n \in \mathbb{N}$, $1 | n$, since $1 \times n = n$. Also, $n | n$, since $n \times 1 = n$. These are "trivial divisors".

Defn An integer $p > 1$ is <u>prime</u> iff it has no nontrivial divisors, that is,

$$Prime(p) \equiv (p > 1) \wedge (\forall d : \mathbb{N}.\ (1 < d < n) \rightarrow d \nmid n).$$

Ex.

- 2 is prime
- 3 is prime $(2 \nmid 3)$.
- 4 is not prime $(2 | 4)$.
- 5 prime
- 6 not prime $(2 | 6)$
- 7 prime $(2 \nmid 7,\ 3 \nmid 7,\ 4 \nmid 7,\ 5 \nmid 7,\ 6 \nmid 7)$

Defn Integers > 1 that are not prime are called <u>composite</u>.

ie. n is composite if it has at least one nontrivial divisor $d | n$. (This means there is some k such that $dk = n$, so also $k | n$.)

Notice 0 and 1 are neither prime nor composite!

- 0 is multiplicative annihilator
- 1 is multiplicative identity.

- 1 is the "building block" of $\mathbb{N}$ under addition.
- primes are the "building blocks" of $\mathbb{N}$ under multiplication.

Theorem Fundamental Theorem of Arithmetic

① Every positive integer $n \geq 1$ is equal to a product of zero or more primes, known as its prime factorization. ② The product is unique "up to reordering" (ie. if sorted from smallest to biggest).

Proof of existence (①). Via strong induction.

Base case: $n=1$ is equal to a product of zero primes.

Let $k \geq 1$ be arbitrary, and suppose that every number $\leq k$ is equal to a product of primes. We must show this for $k+1$.

If $k+1$ is prime, then it is equal to a "product" of just one prime.

Otherwise, if it is composite, then $k+1 = ab$ for some $1 < a, b < k+1$. Since $a \leq k$ and $b \leq k$, by ind. hyp. they are both equal to a product of primes. Hence so is $k+1 = ab$.

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

Formally: $\forall n : \mathbb{N}.\ \text{Composite}(n) \rightarrow \exists d : \mathbb{N}.\ \text{Prime}(d) \wedge (d \leq \sqrt{n}) \wedge (d \mid n)$.

Proof: Let n be arbitrary and suppose it is composite, that is, there exist a, b such that $n = ab$ and $1 < a, b < n$. If both were $> \sqrt{n}$, then their product would be $ab > n$. But $ab = n$, so it cannot be the case that both are $> \sqrt{n}$; one must be $\leq \sqrt{n}$.

Suppose $a \leq \sqrt{n}$. By the Fundamental Theorem of Arithmetic, a is equal to a product of primes. Choose one of them and call it p. Then

① p is prime
② $p \leq a \leq \sqrt{n}$ so $p \leq \sqrt{n}$
③ $p \mid a$ and $a \mid n$ so $p \mid n$.

Hence p is the number claimed to exist.

Hence, if we don't find any prime divisors of n which are $\leq \sqrt{n}$, then n must be prime.

Sieve of Eratosthenes