Primes

Defn An integer $p > 1$ is prime iff the only factors of p are 1 and p. That is, if $a | p$ then $a = 1$ ✓ $a = p$.

Note 1 is not considered prime.

Ex. $2, 3, 5, 7, \ldots$

Theorem (Fundamental Theorem of Arithmetic) —
Every positive integer can be written as the product of zero or more primes. The product is unique as long as you don't care about order.

Note: product of zero primes is 1!

Eg. $6 = 2 \times 3 = 3 \times 2$.

Proof that every $n \in \mathbb{Z}^+$ can be written as a product of primes.

Proof by strong induction.

- $n = 1$, product of zero primes. ✓
- Let $n \geq 2$, and suppose that every positive integer $< n$ can be written as a product of primes

Either n is prime or not.

- If it is prime, done. ✓
- If not, by definition, there must be some $1 < a < n$ which is a divisor of n.

  Let $b = n/a$, then $n = ab$.

  $1 < b < n$. By assumption, a and b can be written as a product of primes, hence so can $n = ab$.

Theorem If n is composite (ie not prime), it has a prime divisor which is $\leq \sqrt{n}$.

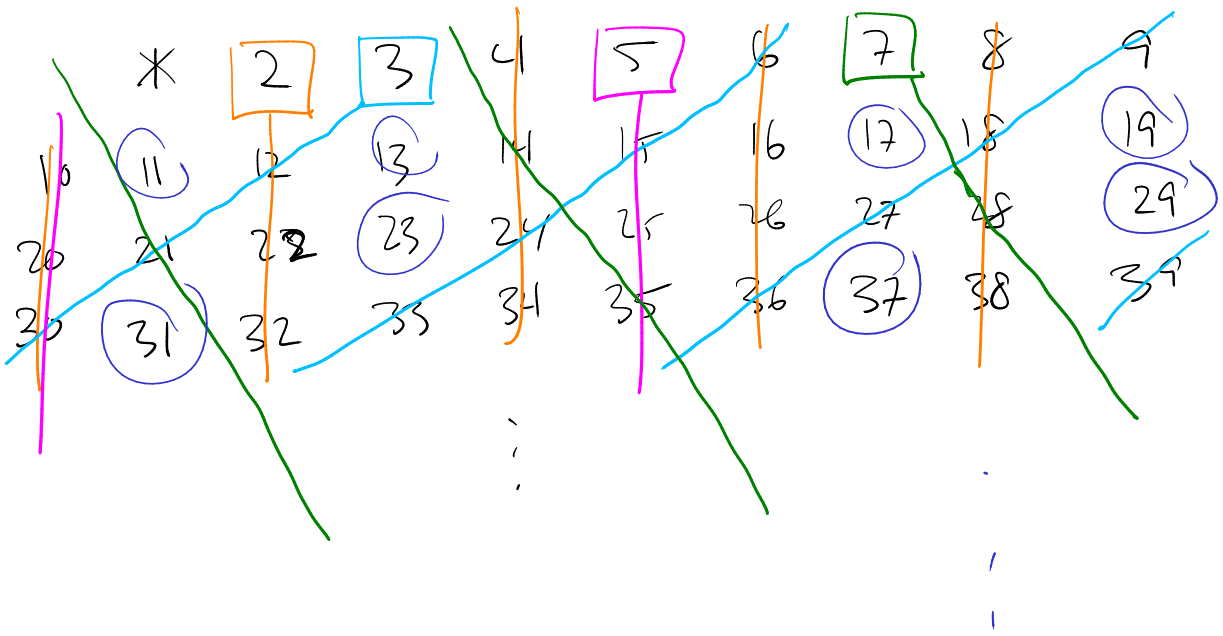
Proof. Suppose n is composite, then there must exist a divisor $1 < a < n$, and hence also $1 < b < n$ such that $n = ab$. At least one of a, b must be $\leq \sqrt{n}$, since if both were $> \sqrt{n}$, then $ab > n$.

Suppose $a \leq \sqrt{n}$. a might not be prime, but, by the FTA, a can be written as a product of primes, so there must be some prime $p \mid a$.

then $p \mid a$ and $a \mid n \Rightarrow p \mid n$

$p \leq a$ and $a \leq \sqrt{n} \Rightarrow p \leq \sqrt{n}$.

Sieve of Eratosthenes



Theorem There are infinitely many primes.

Proof: Take any finite set of primes $p_1, p_2, \ldots, p_n$.

Consider $Q = p_1 p_2 \cdots p_n + 1$. By the FTA, Q can be written as a product of primes, say $q \mid Q$ is one such prime.

Note $p_1 \nmid Q$ because $Q \equiv_{p_1} 1$.

$p_2 \nmid Q$ " $Q \equiv_{p_2} 1$.

etc.

Hence q is not one of $p_1 \cdots p_n$.

So there are always more primes!

Divisibility tests

Test for divisibility by 3: add all digits.

e.g. $136,974,217 \longrightarrow 40 \longrightarrow 4$.

↳ not div. by 3.

$$n = 10^k d_k + 10^{k-1} d_{k-1} + \dots + 10 d_1 + d_0.$$

Now $10 \equiv_3 1$.

Hence $10^k \equiv_3 1^k \equiv_3 1$.

So

$$10^k d_k + 10^{k-1} d_{k-1} + \dots + 10 d_1 + d_0$$

$$\equiv_3 d_k + d_{k-1} + \dots + d_1 + d_0.$$