we defined:

A positive integer is prime if it has only $\mathbf{1}$ and itself as its positive divisors.

Primes: $2, 3, 5, 7, 11, \ldots$

Theorem (F.T.A)

Every positive integer can be expressed uniquely (up to order) as a product of (zero or more) primes.
"up to order" means order does not count, i.e. 2.3 and 3.2 are the same prime factorization of 6.

- "zero or more" means
  
  - zero factors: 1 (empty product)
  - one factor: 2, 3, 5, ... (primes)
  - more factors: 4, 6, 8, ... (composites)

Ex: 100 = 2 · 2 · 5 · 5
1356 = 2 · 2 · 3 · 113
1357 = 23 · 59
17 = 17 (prime)
1 = 1 (empty product)
Thus

but \( n \neq 1 \) be composite. Then \( n \)
has a prime factor \( p \) satisfying
\( p \leq \sqrt{n} \).

Corollary (contra-positive)

If \( n > 1 \) is not divisible by any
prime \( p \leq \sqrt{n} \), then \( n \) is prime.

Example: is 113 prime?

2 \( \not| \) 113, 3 \( \not| \) 113, 5 \( \not| \) 113, 7 \( \not| \) 113.

\( 11^2 = 121 > 113 \), \( \therefore 11 > \sqrt{113} \), so we
need not check 11 \( \not| \) 113. Conclude
113 is prime.
Proof: 

since \( n \) is composite, there exist integers \( a, b \) st.

\[ 1 < a < n, \quad 1 < b < n \quad \text{st.} \quad ab = n \]

Assume (to set a -\( \times \)) that both

\[ a > \sqrt{n} \quad \text{and} \quad b > \sqrt{n} \]

Then

\[ n = ab > \sqrt{n} \cdot \sqrt{n} \]

\[ \therefore n > n \quad \therefore \times \]

This -\( \times \) shows either \( a \leq \sqrt{n} \) or

\( b \leq \sqrt{n} \). For definiteness say \( a \leq \sqrt{n} \).

If \( a \) is prime we're done

since \( a \mid n \).

If \( a \) is
composite, it has a prime divisor
\[ p \mid a \] (by F.T.A.), so \[ p \mid n \]
and \[ p \leq a \leq \sqrt{n} \].

Then (Euclid)
The set of prime numbers is infinite.

Proof:
Assume there are only finitely many primes, say \( n \) of them,
\[ p_1, p_2, p_3, \ldots, p_n \]
let \( m = (p_1p_2p_3\ldots p_n) + 1 \).

By the FTA, there exists a prime \( q \in \{ p_1, p_2, \ldots, p_n \} \) s.t. \( q | m \).

(since \( m > 1 \)). But also

\[
q \mid (p_1p_2\ldots p_n)
\]

so we have

\[
q \mid [m - (p_1p_2\ldots p_n)]
\]

\[
\Rightarrow q \mid 1
\]

This is impossible since 1 has no prime factors. This -X shows our assumption was false.

\( \therefore \) the set of primes is infinite. \( \therefore \)
**Defn:** \( a, b \in \mathbb{Z} \Rightarrow f \), The **Greatest Common Divisor** of \( a \) and \( b \) is the largest \( d \in \mathbb{Z}^+ \) such that \( d \mid a \) and \( d \mid b \).

**Ex.** \( \text{GCD}(12, 18) = 6 \)

\[\{1, 2, 3, 4, 6, 12\} \cap \{1, 2, 3, 6, 9, 18\} = \{1, 3, 6\}\]

**Ex.** \( \text{GCD}(13, 44) = 1 \)

\[\{1, 13\} \cap \{1, 2, 4, 11, 44\} = \{1\}\]

**Defn:** \( a, b \in \mathbb{Z} \Rightarrow f \), are said to be **relatively prime** if \( f \text{ GCD}(a, b) = 1 \).

Equivalently: \( a, b \) have no prime factors in common.
- \( \gcd(a, a) = a \)
- \( \gcd(p, a) = 1 \) if \( p \nmid a \)
- \( \gcd(p, a) = p \) if \( p \mid a \)

Can extend notion of \( \gcd \) to case where one of \( a, b \) is zero, but not both:

\( \gcd(a, 0) = a \)

Ex

\[ \gcd(13, 44) = 1 \]
\[ \gcd(12, 25) = 1 \]
\[ \gcd(27, 104) = 1 \]
Let \( a, b \in \mathbb{Z} - \{0\} \). Let the primes that divide at least one of \( a - b \) be listed:

\[ p_1, p_2, \ldots, p_n, \]

so that

\[ a = p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n} \quad (x_i \geq 0, 1 \leq i \leq n) \]

\[ b = p_1^{y_1} p_2^{y_2} \cdots p_n^{y_n} \quad (y_i \geq 0, 1 \leq i \leq n) \]

Then

\[ \text{GCD}(a, b) = p_1^{\min(x_1, y_1)} p_2^{\min(x_2, y_2)} \cdots p_n^{\min(x_n, y_n)}. \]

Proof: See text...
Defn

Let \(a, b \in \mathbb{Z}\). The \textbf{Least Common Multiple (LCM)} of \(a\) and \(b\) is the smallest (positive) \(m\) such that both \(a | m\) and \(b | m\).

\textit{notation:} \(m = \text{LCM}(a, b)\).

\[\text{Then}\]

Let \(a = p_1^{x_1} p_2^{x_2} \cdots p_n^{x_n}\) and \(b = p_1^{y_1} p_2^{y_2} \cdots p_n^{y_n}\) as before. \text{Then}

\[\text{LCM}(a, b) = p_1^{\max(x_1, y_1)} p_2^{\max(x_2, y_2)} \cdots p_n^{\max(x_n, y_n)}\]

\textit{Proof: exercise.}
\[ a \cdot b = \gcd(a, b) \cdot \text{LCM}(a, b) \]

**Proof:** \[ x + y = \min(x, y) + \max(x, y). \]

**Exercise:** Fill in details.

---

**Euclidean Algorithm**

Example: \[ \gcd(198, 84) = 6 \]

\[
\begin{align*}
198 &= 2 \cdot 84 + 30 \\
84 &= 2 \cdot 30 + 24 \\
30 &= 1 \cdot 24 + 6 \\
24 &= 4 \cdot 6 + 0
\end{align*}
\]
Ex: \( \text{GCD}(235, 56) = 1 \)

\[ 235 = 4 \cdot 56 + 11 \]
\[ 56 = 5 \cdot 11 + 1 \]
\[ 11 = 11 \cdot 1 + 0 \]

Lemma:

\[ a, b, q, r \in \mathbb{Z} \text{ and } a = q \cdot b + r, \]

then \( \text{GCD}(a, b) = \text{GCD}(b, r) \).

Proof:

\[ d | a \text{ and } d | b \text{ then } d | (a - qb) \]
\[ d | r \]
\[ d | b \text{ and } d | r \]

\[ \therefore \text{com. divisors of } a, b \leq \text{com. divisors of } b, r \]
Also if $d \mid b$ and $d \mid r$, then $d \mid (4b+r)$, \(\therefore d \mid a\) \(\therefore d \mid a\) and $d \mid b$.

\(\therefore\) \text{GCD of } a, b, r = \text{GCD of } b, r$.

Thus

\(\{\text{GCD of } a, b, r = \text{GCD of } b, r\}$

\(\therefore\) \text{GCD}(a, b) = \text{GCD}(b, r)$. 

///
Recall:

- \[ a \equiv b \pmod{m} \quad \text{if} \quad m \mid (a-b) \]

Example:

- \[ a \equiv b \pmod{m} \quad \text{and} \quad c \equiv d \pmod{m} \]
  \[ \implies a+c \equiv b+d \pmod{m} \]

Proof:

\[ a \equiv b \pmod{m} \implies m \mid (a-b) \]
\[ c \equiv d \pmod{m} \implies m \mid (c-d) \]

\[ \therefore m \mid (a-b)+(c-d) \]
\[ \therefore m \mid (a+c)-(b+d) \]
\[ \therefore a+c \equiv b+d \pmod{m}. \]