Primes and GCD

**Def.** A positive integer \( p \) greater that 1 is called **prime** if the only positive factors of \( p \) are 1 and \( p \), otherwise it is called **composite**.

In symbolic logic notation:

For \( p \in \mathbb{Z}, p > 1 \), if \( ((a \mid p) \rightarrow (a = 1 \lor a = p)) \), then \( p \) is prime.

**Example:** The first 10 primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29

**Theorem** THE FUNDAMENTAL THEOREM OF ARITHMETIC

Every positive integer can be written uniquely as the product of primes, where the prime factors are written in order of increasing size. (Here, a product can have zero, one, or more than one prime factor.)

**Examples:**

1. \( 100 = 2^2 \cdot 5^2 \)
2. \( 1024 = 2^{10} \)
3. \( 840 = \) __________

**Theorem** There are infinitely many primes (Euclid’s proof).

Proof.
Number of primes and their distribution
Let $\pi(x)$ be the number of primes less than or equal to $x$. For instance $\pi(2) = 1$, $\pi(11) = 5$, $\pi(29) = 10$.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$\pi(x)$</th>
<th>$x/\ln(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>1,000</td>
<td>168</td>
<td>145</td>
</tr>
<tr>
<td>10,000</td>
<td>1,229</td>
<td>1,086</td>
</tr>
<tr>
<td>100,000</td>
<td>9,592</td>
<td></td>
</tr>
<tr>
<td>1,000,000</td>
<td>78,498</td>
<td>72,838</td>
</tr>
<tr>
<td>10,000,000</td>
<td>664,579</td>
<td></td>
</tr>
<tr>
<td>100,000,000</td>
<td>5,761,455</td>
<td></td>
</tr>
<tr>
<td>1,000,000,000</td>
<td>50,847,534</td>
<td></td>
</tr>
<tr>
<td>10,000,000,000</td>
<td>455,052,511</td>
<td></td>
</tr>
<tr>
<td>100,000,000,000</td>
<td>4,118,054,813</td>
<td></td>
</tr>
<tr>
<td>1,000,000,000,000</td>
<td>37,607,912,018</td>
<td></td>
</tr>
<tr>
<td>10,000,000,000,000</td>
<td>346,065,536,839</td>
<td></td>
</tr>
<tr>
<td>100,000,000,000,000</td>
<td>3,204,941,750,802</td>
<td></td>
</tr>
<tr>
<td>1,000,000,000,000,000</td>
<td>29,844,570,422,669</td>
<td></td>
</tr>
<tr>
<td>10,000,000,000,000,000</td>
<td>279,238,341,033,925</td>
<td></td>
</tr>
<tr>
<td>100,000,000,000,000,000</td>
<td>2,623,557,157,654,233</td>
<td></td>
</tr>
<tr>
<td>1,000,000,000,000,000,000</td>
<td>24,739,954,287,740,860</td>
<td></td>
</tr>
<tr>
<td>10,000,000,000,000,000,000</td>
<td>234,057,667,276,344,607</td>
<td></td>
</tr>
<tr>
<td>100,000,000,000,000,000,000</td>
<td>2,220,819,602,560,918,840</td>
<td></td>
</tr>
<tr>
<td>1,000,000,000,000,000,000,000</td>
<td>21,127,269,486,018,731,928</td>
<td></td>
</tr>
<tr>
<td>10,000,000,000,000,000,000,000,000</td>
<td>201,467,286,689,315,906,290</td>
<td></td>
</tr>
<tr>
<td>100,000,000,000,000,000,000,000,000,000</td>
<td>1,925,320,391,606,803,968,923</td>
<td></td>
</tr>
</tbody>
</table>

The Prime Number Theorem (1896)
The ratio of $\pi(x)$ and $x/\ln(x)$ approaches 1 as $x$ grows without bound.

This implies that $\pi(x) \approx x/\ln(x)$ for large $x$.

Largest known prime number
$2^{43,112,609} - 1$ by S. Yates (2009) note that is has 12978189 digits
**Theorem**  If $n$ is a composite integer, then $n$ has a prime divisor less than or equal to $\sqrt{n}$.  

**Proof:**

---

**Example:** Show that 101 is prime.

---

**Goldback’s Conjecture (1742)**
Every even integer greater than two is the sum of two primes.

---

**GCD**

**Def.** Let $a$ and $b$ be integers, not both zero. The largest integer $d$ such that $d|a$ and $d|b$ is called the greatest common divisor of $a$ and $b$. The greatest common divisor of $a$ and $b$ is denoted by $\gcd(a,b)$.

**Examples:**

1. The $\gcd(24,36) = 12$
2. The $\gcd(17,22) = 1$

One way to find the GCD of $a$ and $b$ is to use the prime factorizations of these integers.
Example: Find the $\gcd(120, 500)$.
Solution:
Since $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, 
$\gcd(120, 500) = 2^\min(3,2) \cdot 3^\min(1,0) \cdot 5^\min(1,3) = 2^2 \cdot 3^0 \cdot 5^1 = 20$.

Repeated use of the division algorithm provides another method for finding the gcd of two integers, it is called the Euclidean algorithm.

Example: Find the gcd of 414 and 662 using the Euclidean algorithm.

\[
\begin{align*}
662 &= 414 \cdot 1 + 248 \\
414 &= 248 \cdot 1 + 166 \\
248 &= 166 \cdot 1 + 82 \\
166 &= 82 \cdot 2 + 0 \\
82 &= 2 \cdot 41 + 0
\end{align*}
\]

The Euclidean Algorithm is a consequence of Lemma 1 p. 228

Lemma 1: Let $a = bq + r$, where $a$, $b$, $q$, and $r$ are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Proof in text p. 228.

Def. The least common multiple of the positive integers $a$ and $b$ is the smallest positive integer that is divisible by both $a$ and $b$. The least common multiple of $a$ and $b$ is denoted by $\text{lcm}(a, b)$.

Examples:
1. $\text{lcm}(12, 18) = 36$.
2. Find the lcm of $2^3 3^5 7^2$ and $2^4 3^3$.
3. Find the gcd of $2^3 3^5 7^2$ and $2^4 3^3$. 
**Theorem** Let $a$ and $b$ be positive integers. Then

$$ab = \gcd(a,b) \cdot \lcm(a,b).$$

**Proof:** By the Fundamental Theorem of Arithmetic, $a = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_m^{n_m}$ and $b = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_m^{k_m}$, where some of the $n_i$ and $k_i$ are possibly zero.

The formulae for $\gcd$ and $\lcm$ are as follows:

\[
\gcd(a,b) = p_1^{\min(n_1,k_1)} p_2^{\min(n_2,k_2)} p_3^{\min(n_3,k_3)} \cdots p_m^{\min(n_m,k_m)}
\]

and

\[
\lcm(a,b) = p_1^{\max(n_1,k_1)} p_2^{\max(n_2,k_2)} p_3^{\max(n_3,k_3)} \cdots p_m^{\max(n_m,k_m)}.
\]

By substitution, properties of exponents, and commutativity,

\[
\gcd(a,b) \cdot \lcm(a,b) = p_1^{\min(n_1,k_1)} p_2^{\min(n_2,k_2)} \cdots p_m^{\min(n_m,k_m)} \cdot p_1^{\max(n_1,k_1)} p_2^{\max(n_2,k_2)} \cdots p_m^{\max(n_m,k_m)}
\]

\[
= p_1^{\min(n_1,k_1) + \max(n_1,k_1)} p_2^{\min(n_2,k_2) + \max(n_2,k_2)} \cdots p_m^{\min(n_m,k_m) + \max(n_m,k_m)}
\]

\[
= p_1^{n_1 + k_1} p_2^{n_2 + k_2} \cdots p_m^{n_m + k_m}
\]

\[
= p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_m^{n_m} \cdot p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_m^{k_m}
\]

\[
= ab
\]