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 $p \in Z, p > 1$, if $((a \mid p) \rightarrow (a = 1 \vee a = p))$, 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.
Proof.

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 **<u>greatest common divisor of *a* and *b*</u>**. 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 $500 = 2^2 \cdot 5^3$,
$\gcd(120,500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20$.

Def. The **<u>least common multiple</u>** 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 lcm*(a,b)*.

Examples:
1. 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
$$ab = \gcd(a,b) \cdot \mathrm{lcm}(a,b).$$
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
$$\mathrm{lcm}(a,b) = p_1^{\max(n_1,k_1)} p_2^{\max(n_2,k_2)} p_3^{\max(n_3,k_3)} \cdots p_m^{\max(n_m,k_m)}.$$

By substitution, properties of exponents, and commutativity,
$$\gcd(a,b) \cdot \mathrm{lcm}(a,b) = p_1^{\min(n_1,k_1)} p_2^{\min(n_2,k_2)} \cdots p_m^{\min(n_m,k_m)} \cdot p_1^{\max(n_1,k_1)} p_2^{\max(n_2,k_2)} \cdots p_m^{\max(n_m,k_m)}$$

$$= p_1^{\min(n_1,k_1)+\max(n_1,k_1)} p_2^{\min(n_2,k_2)+\max(n_2,k_2)} \cdots p_m^{\min(n_m,k_m)+\max(n_m,k_m)}$$
$$= p_1^{n_1+k_1} p_2^{n_2+k_2} \cdots p_m^{n_m+k_m}$$
$$= p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_m^{n_m} \cdot p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_m^{k_m}$$
$$= ab$$