Fundamental Thm of Arithmetic(Factorisation Thm)

Theorem

Every Natural number (> 1) can be expressed as a product of primes.

Proof.

By Induction:
Base Case: $n = 2$, is True as 2 is prime. We can regard the single prime number, p, as a product of primes.
Induction Step: Assume true for $k < n$, show true for n.
If n is prime then we can regard n as a product of just one prime.
If n is composite, then $n = n_1 * n_2$ where $n_1 < n$ and $n_2 < n$.
By Induction, n_1 and n_2 can be expressed as products of primes and since $n = n_1 * n_2$, so also is n a product of primes. □

Fundamental Thm of Arithmetic(Factorisation Thm)

From Euclid's Lemma: If $gcd(a, b) = 1$ (i.e. a and b are relatively prime) and also $a|(b * c)$ then $a|c$.
Recall: From Corollary 1. Euclid's Lemma above:
Let p be a prime. If $p|(b * c)$ then either $p|b$ or $p|c$.
Since p is prime and assume $p \not| b$, then $gcd(p, b) = 1$.
From Euclid's Lemma, $p|c$.

Corollary 4. Euclid's Lemma: If p and $p_1, p_2, \ldots p_n$ are primes and $p|p_1 * p_2 \cdots * p_n$ then $p = p_k$ some $1 \leq k \leq n$.
Proof:
From Euclid's Lemma: $p|p_1$ or $p|p_2 * p_3 \cdots * p_n$. If $p|p_1$ then $p = p_1$. If $p \not| p_1$ then $p|p_2 * \cdots * p_n$. Again by Euclid's Lemma: $p = p_2$ or $p|p_3 * \cdots * p_n$. Hence, by continued application of Euclid's Lemma, $p = p_k$ for some $1 \leq k \leq n$.

Fundamental Thm of Arithmetic(Factorisation Thm)

Theorem

Unique Factorisation Thm

The representation of a natural number (>1) as a product of primes is unique apart from the ordering of the primes. We can fix an ordering by the size of the primes.

Proof.

If n is prime then it is considered a product of primes, i.e. 'a unique product of one prime'.
Assume $n = p_1 * p_2 * \cdots * p_j$ and also $n = q_1 * q_2 * \cdots * q_k$ where the $p_1, p_2, \ldots, p_j$ and $q_1, q_2, \ldots, q_k$ are prime. So as to fix an order, assume $p_1 \le p_2 \le \cdots \le p_j$ and $q_1 \le q_2 \le \cdots \le q_k$. We show $j = k$ and $p_i = q_i$ for $1 \le i \le j$.

$\square$

Fundamental Thm of Arithmetic(Factorisation Thm)

Proof.

By Induction on n.
$n = 2$. True, as 2 is a unique product of one prime.
Induction step: $n > 2$.
If n is prime, then n is 'a unique product of one prime' .
If n is composite then $1 < j$ and $1 < k$. By Corollary 1. Euclid's Lemma, $p_1 = q_r$ some r and $q_1 = p_s$ some s. Since $p_1 \leq p_s = q_1 \leq q_r = p_1$ i.e. $p_1 \leq q_1 \leq p_1$ then $p_1 = q_1$. Then $1 < \frac{n}{p_1} < n$, and also $\frac{n}{p_1} = p_2 * \cdots * p_j = q_2 * \cdots * q_k$. By induction, $j = k$ and $p_i = q_i$, $2 \leq i \leq j$. Hence $j = k$ and $p_i = q_i$ for $1 \leq i \leq j$. $\square$

Fundamental Thm of Arithmetic(Factorisation Thm)

Theorem

Fundamental Theorem of Arithmetic *(Factorisation Thm)*
A positive integer, n, can be factorised uniquely into powers of primes.

$$n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$$

i.e.

$$n = (* i \mid 0 < i \ : \ p_i^{\alpha_i})$$

where p_i *is the* i^{th} *prime and* $p_1 < p_2 < \ldots$

Prime representaton (Decomposition) of n

We can order the primes as:
$primes = 2, 3, 5, 7, 11, 13, \ldots$ i.e.
for primes, p_k: $p_1 = 2$, $p_2 = 3$ etc.
We can can decompose a number, n, into prime factors.
For example, $n = 12250$.

$$\begin{aligned} 12250 &= 2^1 * 3^0 * 5^3 * 7^2 * 11^0 \ldots \\ &= 2^1 * 3^0 * 5^3 * 7^2 * (*i \mid 4 < i \; : \; p_i^0) \end{aligned}$$

Exercise: Find the prime factors of 10101.

Least Common Multiple, lcm

In the current context, read $x|y$ as 'y is a multiple of x'

Definition

$l = lcm(a, b)$ iff $(l > 0)$
1. $a|l$ and $b|l$ **i.e.** l is a common multiple of of a and b
2. If $a|m$ and $b|m$ then $l \leq m$. **i.e.** l is the least common multiple

Alternative Definition:

Definition

$l = lcm(a, b)$ iff $(l > 0)$
1. $a|l$ and $b|l$ **i.e.** l is a common multiple of of a and b
2. If $a|m$ and $b|m$ then $l|m$. **i.e.** any common multiple of a and b is a multiple of l.

Calculating lcm(a,b)

Definition

$$lcm(x, y) = \frac{x * y}{gcd(x, y)}$$

Example

Find lcm(54,12).

$gcd(54, 12) = gcd(12, 6) = 6$

$\therefore$

$$lcm(54, 12) = \frac{54 * 12}{6} = 54 * \frac{12}{6} = 54 * 2 = 108$$

Finding gcd and lcm using Prime representation

Finding gcd and lcm using Prime representation

Let $a = (*i \mid 0 < i \; : \; p_i^{\alpha_i})$ and $b = (*i \mid 0 < i \; : \; p_i^{\beta_i})$ then

$$gcd(a, b) = (*i \mid 0 < i \; : \; p_i^{min(\alpha_i, \beta_i)})$$

and

$$lcm(a, b) = (*i \mid 0 < i \; : \; p_i^{max(\alpha_i, \beta_i)})$$

Example

Find gcd(54,12) and lcm(54,12)
$54 = 2^1 * 3^3$ and $12 = 2^2 * 3^1$

$$\begin{aligned} gcd(54,12) &= 2^{min(1,2)} * 3^{min(3.1)} \\ &= 2^1 * 3^1 \\ &= 6 \end{aligned}$$

Also

$$\begin{aligned} lcm(54,12) &= 2^{max(1,2)} * 3^{max(3.1)} \\ &= 2^2 * 3^3 \\ &= 4 * 27 \\ &= 108 \end{aligned}$$

Calculating *gcd* and *lcm* using the Factorisation Theorem is not efficient.
Consider $gcd(1147, 851)$.
$851 = 23 * 37 = 23^1 * 31^0 * 37^1$
$1147 = 31 * 37 = 23^0 * 31^1 * 37^1$

$$\begin{aligned} gcd(1147, 851) &= 23^{min(0,1)} * 31^{min(1,0)} * 37^{min(1,1)} \\ &= 37 \end{aligned}$$

$$\begin{aligned} lcm(1147, 851) &= 23^{max(0,1)} * 31^{max(1,0)} * 37^{max(1,1)} \\ &= 26381 \end{aligned}$$

Properties of *gcd* and *lcm*

So that the properties are more readable, an infix version of *gcd* and *lcm* can be used i.e. use "$a\ gcd\ b$" instead of "$gcd(a, b)$" and use "$a\ lcm\ b$" instead "$lcm(a, b)$",

gcd	Associativity	$a\ gcd\ (b\ gcd\ c) = (a\ gcd\ b)\ gcd\ c$
	Commutativity	$a\ gcd\ b = b\ gcd\ a$
	Idempotent	$a\ gcd\ a = a$
	Distributivity	$a\ gcd\ (b\ lcm\ c) = (a\ gcd\ b)\ lcm\ (a\ gcd\ c)$
lcm	Associativity	$a\ lcm\ (b\ lcm\ c) = (a\ lcm\ b)\ lcm\ c$
	Commutativity	$a\ lcm\ b = b\ lcm\ a$
	Idempotent	$a\ lcm\ a = a$
	Distributivity	$a\ lcm\ (b\ gcd\ c) = (a\ lcm\ b)\ gcd\ (a\ lcm\ c)$

Divisors of 6

Consider the set, D, of divisors of 6 i.e. $D = \{1, 2, 3, 6\}$.
The operations *gcd* and *lcm* are closed on this set in that if $a, b \in D$ then $(a\, gcd\, b) \in D$ and $(a\, lcm\, b) \in D$.
The *identity* element for *gcd* is 6 as for $a \in D$, $(a\, gcd\, 6) = (6\, gcd\, a) = a$.
The *identity* element for *lcm* is 1 as for $a \in D$, $(a\, lcm\, 1) = (1\, lcm\, a) = a$.
Also, for $a \in D$, $a\, gcd\, 1 = 1$ and $a\, lcm\, 6 = 6$.

Correspondence: D and Pow({0,1})

The Powerset of $\{0,1\}$ is the subsets of $\{0,1\}$, i.e.
$Pow(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$ where $\emptyset$ is the empty set.

$\cup$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\emptyset$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0,1\}$	$\{0,1\}$
$\{1\}$	$\{1\}$	$\{0,1\}$	$\{1\}$	$\{0,1\}$
$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$

lcm	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

$D \sim Pow(\{0,1\})$

Matching:

x	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$m(x)$	1	2	3	6

$\cap$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{0\}$	$\emptyset$	$\{0\}$	$\emptyset$	$\{0\}$
$\{1\}$	$\emptyset$	$\emptyset$	$\{1\}$	$\{1\}$
$\{0,1\}$	$\emptyset$	$\{0\}$	$\{1\}$	$\{0,1\}$

gcd	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

From tables:

$m(x \cup y) = m(x)\, lcm\, m(y)$ e.g.

$m(\{0,1\}) = m(\{0\} \cup \{1\}) = m(\{0\})\, lcm\, m(\{1\}) = 2\, lcm\, 3 = 6$

$m(x \cap y) = m(x)\, gcd\, m(y)$

e.g. $m(\emptyset) = m(\{0\} \cap \{1\}) = m(\{0\})\, gcd\, m(\{1\}) = 2\, gcd\, 3 = 1$

Boolean Algebra

A Boolean Algebra consists of a set of elements, B, with 2 special elements, 0 and 1 together with the binary operations $\cap$, $\cup$ and the unary operator, $'$, satisfying the following axioms:

$0' = 1$	$1' = 0$
$p \cap 0 = 0$	$p \cup 1 = 1$
$p \cap 1 = p$	$p \cup 0 = p$
$p \cap p' = 0$	$p \cup p' = 1$
$(p')' = p$	
$p \cap p = p$	$p \cup p = p$

Boolean Axioms Cont'd

$(p \cap q)' = p' \cup q'$	$(p \cup q)' = p' \cap q'$
$p \cap q = q \cap p$	$p \cup q = q \cup p$
$p \cap (q \cap r) = (p \cap q) \cap r$	$p \cup (q \cup r) = (p \cup q) \cup r$
$p \cap (q \cup r) = (p \cap q) \cup (p \cap r)$	$p \cup (q \cap r) = (p \cup q) \cap (p \cup r)$