Greatest Common Divisor (gcd)

Greatest Common Divisor (gcd).
The **Greatest Common Divisor** (gcd) is also known as the highest common factor (hcf).
Example:
A fraction is in its lowest form $\frac{a}{b}$, when $gcd(a, b) = 1$, i.e. the greatest common divisor is 1.
Example:
$gcd(16, 24) = 8$ as 8 is the greatest common divisor (highest common factor) of 16 and 24.

gcd definition

gcd(a,b)

The positive integer, g, is the gcd (greatest common divisor) of integers a and b
i.e. $g = gcd(a, b)$ iff
1) $g|a$ and $g|b$ **i.e.** g is a common divisor of a and b
2) If $h|a$ and $h|b$ then $h \leq g$ **i.e.** g is the greatest common divisor.

Relatively Prime

If $gcd(a, b) = 1$ then a and b are **relatively prime**.
i.e. a and b have no non-trivial (i.e. $\neq 1$ or $\neq -1$) common factors.
e.g. 4 and 9 are relatively prime.

Finding gcd(a,b)

For $a \geq 0 \wedge b > 0$, we have from Euclid's Remainder Theorem (some unique q and r):

$$a = b * q + r \ \wedge \ 0 \leq r < b$$

Let $g = gcd(a, b)$, then $g|a$ and $g|b$ and so $g|(a - b * q)$
tf: since $r = a - b * q$ then $g|r$.
Show $g = gcd(b, r)$
Pf:
1) $g|b$ and also $g|r$
2) Let $h|b$ and $h|r$, Show $h \leq g$.
Pf: Assume $h > g$, then since $h|b$ and $h|r$
$h|(b * q + r)$ **but** $a = b * q + r$ **tf**. $h|a$
but then $h|a$ and $h|b$ and so h is a divisor of a and b greater than g, contradicting that g is the greatest divisor of a and b.

Finding gcd(a,b) Cont'd

Example: Find $gcd(72, 15)$

From Euclid's Remainder Thm: $a = b * q + r \ \wedge \ 0 \leq r < b$
$72 = 15 * 4 + 12$
$\therefore gcd(72, 15) = gcd(15, 12)$
$15 = 12 * 1 + 3$
$\therefore gcd(15, 12) = gcd(12, 3)$
$12 = 3 * 4 + 0$
$\therefore gcd(12, 3) = 3$ as $3|12$ and $3|3$
From above, $gcd(72, 15) = gcd(15, 12) = gcd(12, 3) = 3$

GCD Properties

Properties of gcd

1. $gcd(a, b) = gcd(b, a \, mod \, b)$.
2. $gcd(a, b) = gcd(b, a)$
3. $gcd(k * b, b) = b$
4. $gcd(a, 0) = a$ as $a|a$ and $a|0$.

Example: Find $gcd(72, 15)$ more briefly,

$gcd(72, 15)$
$= gcd(15, \ 72 \, mod \, 15)$
$= gcd(15, 12)$
$= gcd(12, 3)$
$= 3, \ as \, 3|12$.

a*x+b*y=1

Question:
Given a 5 litre jar and a 13 litre jar can we get exactly 1 litre in one of them by filling and refilling the jars from a bigger container.
Can we find integers x and y such that

$$5 * x + 13 * y = 1$$

Solution:
Let $x = -5$ and $y = 2$ to get

$$5 * (-5) + 13 * 2 = 1$$

5L	0	5	0	5	0	3	3	5	0	5	0	5	0
13L	13	8	8	3	3	0	13	11	11	6	6	1	1

In effect, the 13L jar is filled twice and the 5L jar is emptied 5 times.

Question:
Can we find integers x and y such that

$$6 * x + 14 * y = 1$$

Solution:
No Solution!

a*x+b*y=gcd(a,b)

In general, we can find integers x and y such that:

$$a * x + b * y = gcd(a, b)$$

In particular, if $gcd(a, b) = 1$, i.e. a and b are **relatively prime**, then we can find we can find integers x and y such that:

$$a * x + b * y = 1$$

An equation such as $a * x + b * y = g$ is a linear *Diophantine Equation*. If g is a multiple of the $gcd(a, b)$ then there is a solution.

Multiplicative Inverse. Solve $a *_n x = 1$

(Recall: $a *_n x = (a * x)\ mod\ n$)
If we can find x and y such that $a * x - n * y = 1$ then
$a *_n x = 1$
as from Euclid's Remainder Theorem:
$a * x - n * y = (a * x)\ mod\ n$, for some y.
If $a *_n x = 1$ then
x is the inverse of a .
If a and n are relatively prime (i.e. $gcd(a, n) = 1$) then a has an inverse in $\mathbb{Z}_n$.

In Summary

An element $a \in \mathbb{Z}_n$ has an inverse, x,
iff $a * x - n * y = 1$, for some y.
iff $gcd(a, n) = 1$.

Inverse Example

Let the number, a, be a remainder on division by n, i.e. $a \in \{0, 1, \ldots n-1\}$. Assuming $gcd(a, n) = 1$, the number, a, has a multiplicative inverse, x, $mod\, n$, iff $a * x \equiv_n 1$ i.e.
iff $a * x - n * y = 1$, for some y. The equation, $a * x - n * y = 1$, has a solution iff $gcd(a, n) = 1$.
With $a = 3$ and $n = 10$, we have $gcd(3, 10) = 1$ and so 3 and 10 are relatively prime. Find $x < 10$ and y such that $3 * x - 10 * y = 1$.
Checking the multiples, $3, 3 * 2, 3 * 3, 3 * 4$ up to $3 * 9$, i.e. check $3 * k$ for $k \in \{1, 2, \ldots 9\}$ we find that $3 * 7 - 10 * 2 = 1$ i.e.
$3 * 7 \equiv_{10} 1$ i.e.
7 is the multiplicative inverse of 3, $mod\, 10$.

Proof a*x+b*y=gcd(a,b)

Theorem

Given $a, b \in \mathbb{N}$ *show there exists* $x, y \in \mathbb{Z}$ *such that*

$$a * x + b * y = gcd(a, b)$$

Proof (by induction on b)

Base case: $b = 0$.
Then $a * 1 + b * 0 = gcd(a, b)$ as $gcd(a, 0) = a$.
Induction step: (Assume true for $k < b$, show true for b)
Since $a \bmod b < b$ then there exists x' and y' such
$b * x' + (a \bmod b) * y' = gcd(b, \ a \bmod b)$
but $gcd(b, a \bmod b) = gcd(a, b)$
Also, $a \bmod b = a - b * (a \operatorname{div} b)$
$\therefore$

Cont'd

$gcd(a, b)$
$= gcd(b,\ a\,mod\,b)$
{ by induction }
$= b * x' + (a\,mod\,b) * y'$
$= b * x' + (a - b * (a\,div\,b)) * y'$
$= b * x' + a * y' - b * (a\,div\,b) * y'$
$= a * y' + b * (x' - (a\,div\,b) * y')$
$= a * x + b * y$ where $x = y'$ and $y = (x' - (a\,div\,b) * y')$

Alternate definition gcd

Since there are integers x, y such that

$$gcd(a, b) = a * x + b * y$$

then if $h|a$ and $h|b$ then $h|(a * x + b * y)$
tf. $h|gcd(a, b)$.
Alternative definition of gcd(a,b)

Definition

$g = gcd(a, b)$ iff
1) $g|a$ and $g|b$ **i.e.** g is a common divisor of a and b
2) If $h|a$ and $h|b$ then $h|g$ **i.e.** any common divisor divides g.

Construct Solution to a*x+b*y=gcd(a,b)

Example

Find integers x, y such that

$$1147 * x + 851 * y = gcd(1147, 851)$$

In principle, for a solution, we could check all multiples $1147, 1147 * 2, 1147 * 3$ up to $1147 * 850$ until we find $1147 * x$ that leaves a remainder, $gcd(1147, 851)$ on division by 851 i.e find x such that $1147 * x \equiv_{851} gcd(1147, 851)$.
An easier solution can be found based on calculating the $gcd(1147, 851)$. To construct a solution of $a * x + b * y = gcd(a, b)$, find $gcd(a, b)$ via Euclid's Algorithm; then 'reverse' the calculation to find x and y.

Solution $1147 * x + 851 * y = gcd(1147, 851)$

Using Euclid's Remainder Theorem:

$$1147 = 851 * 1 + 296$$

tf. $gcd(1147, 851) = gcd(851, 296)$

$$851 = 296 * 2 + 259$$

tf. $gcd(1147, 851) = gcd(296, 259)$

$$296 = 259 * 1 + 37$$

tf. $gcd(1147, 851) = gcd(259, 37)$
$\{ \; 259 = 7 * 37 \; \}$
tf.

$$gcd(1147, 851) = 37$$

Find x,y

Then 'reversing' the calculation (Euclid's Algorithm):

$$\begin{aligned}
37 &= 296 * 1 - 259 * 1 \\
&= 296 * 1 - (851 - 296 * 2) \\
&= 851 * (-1) + 296 * 3 \\
&= 851 * (-1) + (1147 - 851 * 1) * 3 \\
&= 1147 * 3 + 851 * (-1) + 851 * (-3) \\
&= 1147 * 3 + 851 * (-4)
\end{aligned}$$

$\therefore$

$37 = 1147 * 3 + 851 * (-4)$

Solution:

$$37 = 1147 * x + 851 * y$$

$$\text{where } x = 3 \text{ and } y = -4$$

Check by calculation:

$$1147 * 3 - 851 * 4 = 3441 - 3404 = 37$$

Exercise

Exercise:
Find x, y such that

$$1785 * x + 374 * y = gcd(1785, 374)$$

General Solution to $a * x + b * y = gcd(a, b)$

If x_0 and y_0 is a solution to $a * x + b * y = gcd(a, b)$ so also is:
$x_0 + m$ and $y_0 + n$ where $a * m + b * n = 0$.
$a * (x_0 + m) + b * (y_0 + n) = gcd(a, b)$
$a * x_0 + a * m + b * y_0 + b * n = gcd(a, b)$
$(a * m + b * n) + a * x_0 + b * y_0 = gcd(a, b)$
$a * x_0 + b * y_0 = gcd(a, b)$.

Example:
A solution for $a * m + b * n = 0$ is $m = b$ and $n = -a$.
$\therefore x_0 + b$ and $y_0 - a$ is another solution to
$a * x + b * y = gcd(a, b)$ when x_0 and y_0 is a solution.
e.g. $a * (x_0 + b) + b * (y_0 - a) = gcd(a, b)$
$\equiv a * x_0 + a * b + b * y_0 - b * a = gcd(a, b)$
$\equiv a * x_0 + b * y_0 = gcd(a, b)$

General Solution (Cont'd)

If $a * m + b * n = 0$ then $\frac{a}{d} * m + \frac{b}{d} * n = 0$ where $d = gcd(a, b)$.
In particular, if $m = \frac{b}{d}$ and $n = -\frac{a}{d}$ then $\frac{a}{d} * m + \frac{b}{d} * n = 0$.
$\therefore$ the general solution $x_0 + m$ and $y_0 + n$ can be expressed as
$x_0 + \frac{b}{d} * k$ and $y_0 - \frac{a}{d} * k$ where $d = gcd(a, b)$.
For the equation $37 = 1147 * x + 851 * y$ with $x_0 = 3$ and $y_0 = -4$
we have the general solutions: $3 + 23 * k$ and $-4 - 31 * k$ as
$\frac{851}{37} = 23$ and $\frac{1147}{37} = 31$.

Example:
For equation $37 = 1147 * x + 851 * y$ we have solution $x_0 = 3$ and
$y_0 = -4$.
Let $k = -1$ in $3 + 23 * k$ and $-4 - 31 * k$ then check solution
$x = -20$ and $y = 27$:
$1147 * (-20) + 851 * 27$
$= -22940 + 22977$
$= 37$

Relatively Prime

If $d = gcd(a, b)$ then $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.
$a * x_0 + b * y_0 = gcd(a, b)$ then
$\frac{a}{d} * x_0 + \frac{b}{d} * y_0 = 1$ where $d = gcd(a, b)$.
Example:
Since $37 = 1147 * x + 851 * y$
then $\frac{1147}{37}$ and $\frac{851}{37}$ i.e. 31 and 23 are relatively prime.
Since
$gcd(a, b) = a * x + b * y$ for some x and y then
$gcd(a, b)$ can be expressed as a linear combination of a and b.

Euclid's Lemma

Theorem

Euclid's Lemma

If $gcd(a, b) = 1$ *(i.e. a and b are relatively prime) and also* $a|(b * c)$ *then* $a|c$

Proof.

Since $gcd(a, b) = 1$ there exists x and y such that $a * x + b * y = 1$

$\therefore c * a * x + c * b * y = c.$

From assumption that $a|(b * c)$ we have $a|(c * b * y)$.

Also $a|(c * a * x)$,

$\therefore a|c.$

$\square$

Corollories to Euclid's Lemma

Corollary 1
If p is a prime and $p|a^n$ then $p|a$.
Corollary 2
If $a * b \equiv_n a * c$ and a and n are relatively prime, then $b \equiv_n c$.
Corollary 3
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, $p|c$.

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. $\square$

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 3. 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.

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 $p_1 \leq p_2 \leq \cdots \leq p_j$ and $q_1 \leq q_2 \leq \cdots \leq q_k$. We show $j = k$ and $p_i = q_i$ for $1 \leq i \leq j$.

By Induction on n.

$n = 2$. True, as 2 is a unique product of one prime. □

Fundamental Thm of Arithmetic(Factorisation Thm)

Proof.

Induction step: $n > 2$.
If n is prime, then True as a prime on its own is regarded as a unique product of primes.
If n is composite then $1 < j$ and $1 < k$. By Corollary 4. 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).

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

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

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

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