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

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.

A fraction $\frac{a}{b}$ is in lowest form iff a and b are relatively prime, i.e. if $gcd(a, b) = 1$.

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 $g|(a - b * q)$
$\therefore$ 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** $a = b * q + r \therefore h|a$
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.

$$gcd(a, b) = gcd(b, a\, mod\, b)$$

Example: Find $gcd(72, 15)$

From Euclid's Remainder Thm:

$$a = b * (a\, div\, b) + a\, mod\, b \;\wedge\; 0 \leq a\, mod\, b < b$$

$72\, div\, 15 = \lfloor \frac{72}{15} \rfloor = 4$ and $72\, mod\, 15 = 72 - 15 * \lfloor \frac{72}{15} \rfloor = 12$

$72 = 15 * 4 + 12$
$\therefore gcd(72, 15) = gcd(15, 12)$
$15 = 12 * 1 + 3$
$\therefore gcd(15, 12) = gcd(12, 3)$
$12 = 3 * 4 + 0$
$\therefore gcd(12, 3) = 3$ as $3|12$ and $3|3$
$\therefore gcd(72, 15) = 3$ as $gcd(72, 15) = gcd(15, 12) = gcd(12, 3) = 3$

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, there is an 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
$a *_n x = 1$
From Euclid's Remainder Theorem: given a, b there exists q such that $a = b * q + a \, mod \, b$
With substitutions $a := a * x$, $b := n$, $q := y$ then
$a * x = n * y + a *_n x$, some y. i.e.
$a * x - n * y = (a *_n x)$, 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 $\mathbb{Z}_n$.

Inverse for $a \in \mathbb{Z}_n$

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 $3 * k$ 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 $a \, mod \, b < b$ then there exists x' and y' such
$b * x' + (a \, mod \, b) * y' = gcd(b, \; a \, mod \, b)$
but $gcd(b, a \, mod \, b) = gcd(a, b)$
Also, $a \, mod \, b = a - b * (a \, div \, b)$
$\therefore$

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 $h|(a * x + b * y)$
$\therefore h|gcd(a, b)$.
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:

$$1147 = 851 * 1 + 296$$

$\therefore gcd(1147, 851) = gcd(851, 296)$

$$851 = 296 * 2 + 259$$

$\therefore gcd(1147, 851) = gcd(296, 259)$

$$296 = 259 * 1 + 37$$

$\therefore gcd(1147, 851) = gcd(259, 37)$
$\{ 259 = 7 * 37 \}$
$\therefore$

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

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:

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

Other Solutions

There may be many solutions to $a * x + b * y = gcd(a, b)$
Let $g = gcd(a, b)$ then
if x_0 and y_0 is a solution to $a * x + b * y = g$ then
$x_0 + \frac{b}{g} * k$ and $y_0 - \frac{a}{g} * k$ is a solution for $k \in \mathbb{Z}$.
Example:
For equation $37 = 1147 * x + 851 * y$ we have solution $x_0 = 3$ and
$y_0 = -4$.
$gcd(1147, 851) = 37$ and $\frac{a}{g} = \frac{1147}{37} = 31$, $\frac{b}{g} = \frac{851}{37} = 23$
Let $k = -1$ in $3 + 23 * k$ and $-4 - 31 * k$ then check solution
$x = -20$ and $y = 27$:
$1147 * (-20) + 851 * 27$
$= -22940 + 22977$
$= 37$

$a * x + b * y = k$

If $gcd(a, b) | k$ i.e. $k = d * gcd(a, b)$ some, d then $a * x + b * y = k$ has a solution based on the solution for $a * x + b * y = gcd(a, b)$.
If x_0, y_0 is a solution to $a * x + b * y = gcd(a, b)$ then $d * x_0$ and $d * y_0$ is a solution for $a * x + b * y = k$ as $a * x_0 + b * y_0 = gcd(a, b) \therefore$
$a * (d * x_0) + b * (d * y_0) = d * gcd(a, b)$ where $k = d * gcd(a, b)$.

Exercise

Exercise:
Find x, y such that

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

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

Theorem

Cancellation Law
If $a * b \equiv_n a * c$ *and* a *and* n *are relatively prime, (i.e.* $gcd(a, n) = 1$*) then* $b \equiv_n c$

Proof.

Let
$a * b \equiv_n a * c \therefore$
$n|(a * b - a * c) \therefore$
$n|(a * (b - c))$
$\{$ $gcd(a, n) = 1$ and Euclid's Lemma $\}$
$n|(b - c) \therefore$
$b \equiv_n c$

□

Corollories to Euclid's Lemma (Cont'd)

Corollary 1
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 2
If p is a prime and $p|a^n$ then $p|a$.

Pigeon-Hole Principle

Pigeon-Hole Principle

If m items are put into n boxes and $m > n$, then some boxes have more than one item. Since $m > n$, after filling up the n boxes we have still items left over which means some box has more than 1 item.

e.g. In a crowd of 367 people, at least two people have the same birthday.

Handshaking

From Wikipedia

Handshaking

If there are n people who can shake hands with one another (where $n > 1$), the pigeonhole principle shows that there is always a pair of people who will shake hands with the same number of people. As the 'boxes' correspond to number of hands shaken and each person can shake hands with anybody from 0 to $n - 1$ other people, this creates $n - 1$ possible boxes. This is because either the '0' or the '$n - 1$' box must be empty (if one person shakes hands with everybody (else), it's not possible to have another person who shakes hands with nobody; likewise, if one person shakes hands with nobody there cannot be a person who shakes hands with everybody else). This leaves n people to be placed in at most $n - 1$ non-empty boxes, guaranteeing duplication.

$a^k \equiv_n 1$, when gcd(a,n)=1

Theorem

If a is relatively prime to n then there exists $k > 0$ such that $k \leq n$ and $a^k \equiv_n 1$.

Proof

Assume a is relatively prime to n. Consider the remainders of

$$a, a^2, \ldots, a^{n+1}$$

when divided by n. There are $n + 1$ elements in $\{a, a^2, \ldots, a^{n+1}\}$ and there can be only n remainders (from 0 to $n - 1$). By the Pigeon-Hole Principle, there exists $i, j \in \{1..n + 1)$ and $i \neq j$ (assume $i < j$) such that a^i and a^j have the same remainder, i.e. $a^i \equiv_n a^j$.

Inverse via Powers

Since $i < j$, $j - i > 0$ and $j - i \leq n$ (since j is at most $n+1$ and i is at least 1). Since a is relatively prime to n , $a^{i-1} \equiv_n a^{j-1}$ (by cancellation). Continuing to cancel $a's$ on both sides we get (since $i < j$), $1 \equiv_n a^{j-i}$ i.e. $a^k \equiv_n 1$ where $k = j - i$.

Example

Let $a = 3$ and $n = 10$ then 3 and 10 are relatively prime. Find a k such that $3^k \equiv_{10} 1$.

k	1	2	3	4	5	6	7	8	9	10
$3^k mod\, 10$	3	9	7	1	3	9	7	1	3	9

We have $3^4 \equiv_{10} 1$.

Also $3^8 \equiv_{10} 1$.

Finding inverse using $a^k \equiv_n 1$

Finding inverse

Let $a \in \mathbb{Z}_n$. If a and n are relatively prime, there exists a k such that $0 < k \leq n$ and $a^k \equiv_n 1$.
Since $a^k = a * a^{k-1}$ and $a *_n a^{k-1} \equiv_n 1$ and so a^{k-1} is the inverse of a.

Since $gcd(3, 10) = 1$, we can find the inverse of 3.
From above, $3^4 \equiv_{10} 1$, $\therefore 3 * 3^3 \equiv_{10} 1$
From table above $3^3 \equiv_{10} 7$ $\therefore$ 7 is the inverse of 3.
Check: $3 * 7 = 21 \equiv_{10} 1$.