c is a *common divisor* of a and b means c|a and c|b.

gcd(a,b) ::= the **greatest common divisor** of a and b.

gcd

Euclid: gcd(a,b) = gcd(b,r)!

$a=qb+r$

spc(a,b) = **smallest positive** integer linear **combination** of a and b

Theorem. gcd(a,b) = spc(a,b)

$sa+tb$, $s,t\in\mathbb{Z}$

Let d denote the greatest common divisor of 1102 and 399.

(a) Find d using the Euclidean algorithm.

(b) Find the integers m and n, solution of $1102m + 399n = d$.

(c) Determine whether the equation $1102x + 399y = 57$ has a solution, such that $(x, y) \in \mathbb{Z}^2$. If such a solution exists, find that for which x is positive and as small as possible; otherwise explain why not.

(a) $\gcd(1102, 399)$

$= \gcd(399, 304)$

$= \gcd(304, 95)$

$= \gcd(95, 19)$

$= 19$

$a = qb + r$

$1102 = 2 \times 399 + 304$

$399 = 1 \times 304 + 95$

$304 = 3 \times 95 + 19$

$95 = 5 \times 19$

(b) $a = 1102$ $b = 399$ $1102m + 399n = 19$

$\underbrace{1102}_{a} = 2 \times \underbrace{399}_{b} + 304$

$399 = 1 \times 304 + 95$

$304 = 3 \times 95 + 19$

$95 = 5 \times 19$

$304 = a - 2b$

$95 = b - (a - 2b) = 3b - a$

$19 = (a - 2b) - 3(3b - a)$

$= 4a - 11b$

$$\underbrace{4}_{m} \times 1102 \underbrace{-11}_{n} \times 399 = 19$$

$m = 4$ $n = -11$

(c)

$12 \times 1102 - 33 \times 399 = 57$

$\begin{cases} x = 12 \ (>0) \\ y = -33 \end{cases}$

(19)

$\boxed{1102x + 399y = 57}$

$1102(x + \Delta x) + 399(y - \Delta y) = 57$

$1102x + 399y + \underbrace{(1102\Delta x - 399\Delta y)}_{/} = 57$

$\downarrow 0$

$1102\Delta x = 399\Delta y \quad (\div 19)$

$58\Delta x = 21\Delta y$

$\Delta x = 21k$

$\Delta y = 58k$

$1102(12+21k) + 399(-33-58k) = 57$

$\begin{cases} x = 12 + 21k \\ y = -33 - 58k \end{cases} \quad k \in \mathbb{Z}$

$x = 12$ smallest

$\left(1102x + 399y = 57 \right.$

$\left. 1102\left(x + \frac{399k}{19}\right) + 399\left(y - \frac{1102k}{19}\right) = 57 \right)$

② FQ6

Prove that if $\gcd(x, y)=1$, then $\gcd(x+y, x-y)=1$ or 2 $(x \geq y)$

SPC

$\gcd(7,3)=1$ $\gcd(10,4)=2$

$\gcd(4,3)=1$ $\gcd(7,1)=1$ → can be 1 or 2

Assume $\exists x, y$, $\gcd(x+y, x-y) = d > 2$

by def:

$$\begin{cases} x+y = k_1 d \\ x-y = k_2 \cdot d \end{cases} \Rightarrow \begin{cases} x = \boxed{\dfrac{k_1+k_2}{2}} \cdot d \\ y = \dfrac{k_1-k_2}{2} \cdot d \end{cases}$$

d is odd: $d \mid x \quad d \mid y \quad \gcd(x,y) \geq d > 1$

d is even: $d = 2k \ (k > 1) \Rightarrow \begin{cases} x = (k_1 + k_2) \cdot k \\ y = (k_1 - k_2) \cdot k \end{cases}$

$k \mid x \quad k \mid y \quad \gcd(x,y) \geq k > 1$

contradiction!

SPC

$\gcd(x,y) = 1 = \mathrm{spc}(x,y)$

$\exists s, t \in \mathbb{Z} \quad sx + ty = 1$

$\gcd(x+y, x-y) = \mathrm{spc}(x+y, x-y) = m(x+y) + n(x-y)$

$= (m+n)x + (m-n)y \quad \exists m, n \in \mathbb{Z}$

min

$\begin{cases} m+n = s \\ m-n = t \end{cases} \Rightarrow \begin{cases} m = \frac{s+t}{2} \\ n = \frac{s-t}{2} \end{cases}$

① s, t have same parity

$\gcd(x+y, x-y) = sx + ty = 1$

② s, t have different parity

$\begin{cases} m = s+t \\ n = s-t \end{cases}$

$\gcd(x+y, x-y) = 2sx + 2ty = 2$

Suppose n is even and $\gcd(m, n) = 5$, show that m is odd

spc

$$\gcd(m,n) = \mathrm{spc}(m,n) = \underline{sm} + tn = 5 \qquad s,t \in \mathbb{Z}$$

sm → odd

tn → even

5 → odd

$\Rightarrow$ m is odd

General Solution for Die Hard

Theorem. Given water jugs of capacity a and b with $a \leq b$, it is possible to have exactly k ($\leq b$) gallons in one jug if and only if k is a multiple of gcd(a,b).

Given jug of 21 and jug of 26, is it possible to have exactly 3 gallons in one jug?

$$\gcd(21,26) = 1$$
$$\Rightarrow 5\times21 - 4\times26 = 1$$
$$\Rightarrow 15\times21 - 12\times26 = 3$$

Repeat 15 times:

1. Fill the 21-gallon jug.
2. Pour all the water in the 21-gallon jug into the 26-gallon jug.
   Whenever the 26-gallon jug becomes full, empty it out.