Extended Euclidean Algorithm

Yan Huang

Can you sell exactly 4 gallons of gasoline?

$z: 8, 16, 24, \ldots$

$8x, \quad x \in \mathbb{Z}$

$3, 6, 9, \ldots$

$3y, \quad y \in \mathbb{Z}$

$a: 4 \in S$?

8 Gallon

3 Gallon

$2 \times 8 + (3) \times (-4) = 4$

$z \in \{8x + 3y \mid x, y \in \mathbb{Z}\} = S$

Are there integers x and y that satisfy $8x+3y=4$?

Can you sell 1 gallon of gasoline with containers of these two sizes?

1. Pour 8*2 gallons of gasoline the tank.
2. Fill the 3-gallon container with gasoline in the tank, 5 times.
3. Sell the remaining 1 gallon gasoline in the tank.

8 Gallon

3 Gallon

Theorem: $\gcd(a,b) = d$ if and only if d is the least positive integer that can be expressed as $ax + by$ where $x, y \in \mathbb{Z}$.

Proof: "$\Leftarrow$"

(For the purpose of contradiction). we assume $d \nmid a$.

and d is the min of $S = \{ax+by \mid x,y \in \mathbb{Z}\}$.

Then $a = dq + r$. $(0 < r < d)$ division with remainder

so $r = a - dq = a - (ax+by)q = a(1-xq) + b(-yq) \in S$

So $d \mid a$ similarly, we can prove $d \mid b$.

If $d' \mid a$, $d' \mid b$. then $d' \mid ax+by$, $\forall x,y \in \mathbb{Z}$. hence $d' \mid d$.

Theorem: $\gcd(a, b) = d$ if and only if d is the least positive integer that can be expressed as $ax + by$ where $x, y \in \mathbb{Z}$.

"$\Rightarrow$" if $d = \gcd(a, b)$, then $d \in S$

because $d \mid a$, $a = kd$. $(\exists\, k \in \mathbb{Z})$.

set $x = k$, $y = 0$. $d = ax + by \in S$.

$\exists\, x, y \in \mathbb{Z}$ $ax + by = \gcd(a, b)$

Theorem: $\gcd(a, b) = d$ if and only if d is the least positive integer that can be expressed as $ax + by$ where $x, y \in \mathbb{Z}$.

ex(1) $a = 3 \quad b = 8$.

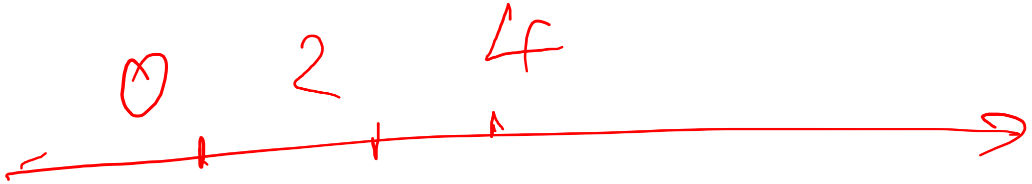
$\gcd\ 8\ 3 = \gcd\ 3\ (8 \bmod 3) = \gcd\ 3\ 2 = \gcd\ 2\ 1$

$= 1$

$\{3x + 8y \mid \forall x, y \in \mathbb{Z}\}$

ex.(2) $a = 2,\ b = 4$.

$\{2x + 4y \mid x, y \in \mathbb{Z}\}$,



2 is the least positive int in $\{2x + 4y \mid x, y \in \mathbb{Z}\}$

2 is gcd(2, 4)

Theorem: $\gcd(a, b) = d$ if and only if d is the least positive integer that can be expressed as $ax + by$ where $x, y \in \mathbb{Z}$.

Proof (by *contradiction*): Consider the set of integers

$$\mathrm{S} = \{ax + by \,|x, y \in \mathbb{Z}\} \text{ and } d = \min S.$$

Assume (for the sake of contradiction) that $d \nmid a$. Then $a = dq + r$ where $0 \leq r < d$. Therefore, $r = d - aq = ax + by - aq = a(x - q) + by \in S$, which contradicts to the fact that $d = \min S$ since $r \in S$ and $r < d$. Thus, the assumption was wrong and $d|a$.

if $\gcd(a, b) = 1$. $\exists x, y$. $ax + by = 1$. $\Rightarrow$ $ax + by \bmod b$
$= ax \bmod b = 1$

Theorem: $\gcd(a, b) = d$ if and only if d is the least positive integer that can be expressed as $ax + by$ where $x, y \in \mathbb{Z}$.

(continued) Similarly, we can show $d|b$. Hence d is a common divisor of a and b.

If d' is a common divisor of a and b, then $d'|d$ (because $d = ax + by$ for some $x, y \in \mathbb{Z}$). QED.

Examples

- $a = 6$ and $b = 8$

$GCD(6, 8) = 2$ -- by the Euclidean Algorithm

Let $x = -1$, $y = 1$. then

$6x + 8y = 2$

Examples

- $a = 3$ and $b = 8$

$GCD(3, 8) = 1$

Let $x = 3$, $y = -1$, then

$3x + 8y = 1$

Find $x, y \in \mathbb{Z}$ such that a$x + by = \mathrm{gcd}(a, b)$?

```
egcd :: Int -> Int -> (Int, Int, Int)
egcd a 1 = (0, 1, 1)
egcd a 0 = (1, 0, a)
egcd a b | a < b = let (x, y, d) = egcd b a in (y, x, d)
         | otherwise = let (x, y, d) = egcd b (a `mod` b)
                           q = a `div` b
                       in (y, x-y*q, d)
```

Examples

```
egcd :: Int -> Int -> (Int, Int, Int)
egcd a 1 = (0, 1, 1)
egcd a 0 = (1, 0, a)
egcd a b | a < b = let (x, y, d) = egcd b a in (y, x, d)
         | otherwise = let (x, y, d) = egcd b (a `mod` b)
                           q = a `div` b
                       in (y, x-y*q, d)
```

- Find x, y such that 12*x + 8*y = gcd(12, 8)

egcd (12, 8)

q = 12 div 8 q = 8 div 4

egcd (12, 8) → egcd (8, 4) → egcd (4, 0)

x = −1, y = 1

(−1, 0 − (−1) · 1, 4) ← (0, 1 − 0 · 2, 4) ← (1, 0, 4)

$\underline{x}$, $\underline{y}$, $\underline{d}$

|| ||

(−1, 1, 4) (0, 1, 4)

$\underline{x}$ $\underline{y}$ $\underline{d}$

Exercise

- Find integer x, y such that 27*x + 42*y = gcd(27, 42)

egcd (27, 42)