

Recall: The Extended Euclidean Algorithm enables us to find

i) The $\gcd(a, b)$.

ii) Find a solution (x_0, y_0) consisting of a pair of integers to the equation $ax + by = \gcd(a, b)$.

Ex: $a = 44, b = 30$

$$44x_i + 30y_i = r_i$$

Row	x_i	y_i	r_i	g_i
1	1	0	44	—
2	0	1	30	—
3	1	-1	14	1
4	-2	3	2	2

$\gcd(44, 30)$

$$44(-2) + 30(3) = 2 = \gcd(44, 30)$$

Def: Two integers a, b are said to be
RELATIVELY PRIME if
 $\gcd(a, b) = 1$.

Prop: (i) $\gcd(a, b) = 1$, if and only if there exists a pair of integers (x, y) , such that $ax + by = 1$.

(ii) If $d = \gcd(a, b) \neq 0$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof: (i) was proved last time.

(ii) Suppose $d = \gcd(a, b) \neq 0$.

Then there exists a pair of integers (x, y) , such that $ax + by = d$, by the E.E.A.

Divide both sides by d to get

$$\left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = 1.$$

So $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, by Part (i). $\square$

Ex: $\gcd(6, 10) = 2$

$$\gcd\left(\underbrace{\frac{6}{2}}_3, \underbrace{\frac{10}{2}}_5\right) = 1$$

Prop 2.28: If a, b, c are integers and $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

Proof: There exists a pair of integers (x, y) , such that $ax + cy = 1$, since $\gcd(a, c) = 1$ (we used part 1 of the previous proposition). Let g be an integer, such that $ab = cg$.

$$\text{Write } b = \underbrace{1}_{ax+cy} \cdot b = \underbrace{abx}_{cg} + cby = c(gx + by).$$

so $c \mid b$. □

Prop: (Another characterization of gcd). Let a, b be integers. An integer d is the $\gcd(a, b)$ if and only if it satisfies the following:

- (i) $d \geq 0$.
- (ii) d divides both a and b .
- (iii) Any divisor of both a and b divides also d .

Proof: The case where $a = b = 0$ is clear, Assume one of them is not 0, say $a \neq 0$.

"if" direction: Assume that d satisfies (i), (ii), (iii). Then $d \neq 0$, by (ii), since $d|a$ and $a \neq 0$. So $\boxed{d > 0}$, by part (i).

Let c be a common divisor of a and b . Then $c|d$, by (iii). So

$|c| \leq |d| = d$, by Prop 2.11 (iv).

So $c \leq d$. So d is the greatest common divisor.

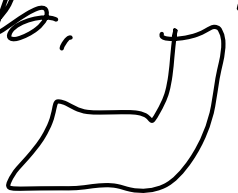
"only if direction": Let $d = \gcd(a, b)$

So $d \geq 0$, by def of gcd, (i) holds,
(ii) also holds, by def of gcd.

Let c be a common divisor of a and b . There exists a pair of integers (x, y) , such that

$$d = ax + by. \quad \text{Write } \begin{matrix} a = c\epsilon_1 \\ b = c\epsilon_2, \end{matrix}$$

$$\text{then } d = c\epsilon_1 x + c\epsilon_2 y = c(\epsilon_1 x + \epsilon_2 y)$$

So $c|d$. So (iii) holds. 

Sec 2.3 Linear Diophantine Equations?

Ex: $a = 44$, $b = 30$. We saw

$\gcd(a, b) = 2$ and

(*) $44(-2) + 30(3) = 2 = \gcd(44, 30)$

The equation

$44x + 30y = 2$ is an example of a linear Diophantine Eq.

Ex: Find all solutions (x, y) , consisting of pairs of integers, of the equation?

(**) $44x + 30y = 104$

So $(x_0, y_0) = (\underbrace{52 \cdot (-2)}_{-104}, \underbrace{52 \cdot 3}_{156})$ is a particular solution of (*)
 $\underbrace{52 \cdot 2}_{= \gcd(44, 30)}$

If (x_n, y_n) is an integer solution of

(***) $44x + 30y = 0$, then

$(x_0 + x_n, y_0 + y_n)$ is a solution to $(**)$.

$\exists$ $(***)$ is equivalent to $\frac{(***)}{\gcd(44, 30)}$

$(***)$

$$22x + 15y = 0$$

Note that $(x_1, y_1) = (15, -22)$ is a soln to $(***)'$ and so are $(x_n, y_n) = (15k, -22k)$, for every integer k . So we see that

$$(H) \quad \begin{aligned} (x, y) &= (x_0 + x_n, y_0 + y_n) = \\ &= (-104 + 15k, 136 + (-22)k) \end{aligned}$$

is a solution of $(**)$, for all integers k .

Question; Find all solution (x, y) with non-negative integers x, y , of the eq $(**)$ $44x + 30y = 104$.

Answer | We need to find all values of k , for which the pair (H) is non negative.

$$\begin{aligned} -104 + 15k &\geq 0 \\ 156 - 22k &\geq 0 \end{aligned}$$

$$k \geq \frac{104}{15}$$

(note that $7 \cdot 15 = 105$)
so $k \geq 7$)

$$22k \leq 156 \quad k \leq \frac{156}{22} = 7 + \frac{1}{11}$$

$\boxed{k=7}$ is the only sol'n.

So the unique solution of $(**)$ with non-negative integer solution is

$$\begin{aligned} (x, y) &= (-104 + \underbrace{15 \cdot 7}_{105}, 156 - \underbrace{22 \cdot 7}_{154}) = \\ &= (1, 2). \end{aligned}$$

$$44 \cdot 1 + 30 \cdot 2 = 104 \quad \checkmark$$

Theorem: (i) The Linear Diophantine equation

$$\boxed{ax + by = c} \quad (+)$$

has an integer solution (x, y) , if and only if $\gcd(a, b) \mid c$.

(ii) If $\gcd(a, b) = d \neq 0$ and the pair (x_0, y_0) is a particular solution to $ax + by = c$, then the general solution of (+) is

$$(iii) (x, y) = \left(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k\right), \text{ where } k \text{ is an integer.}$$

Proof: (i) If $\gcd(a, b) = d \mid c$, write $c = dg$, where g is an integer.

Let (x, y) be a soln of $ax + by = d$ (exists, by the E.E.A) Then

(xg, yg) is a solution to (+)

If there exists a soln to $ax + by = c$, then $d := \gcd(a, b)$ divides c ,

because c is a linear combination of a, b with integer coeff.

(ii) We verify that the pairs in (H) are solutions of $\boxed{ax+by=c}$, by plugging in. We show that there are all the solutions.

Let (x_1, y_1) be a solution of (H).

Then $(x_1 - x_0, y_1 - y_0)$ is a sol'n to
 $ax + by = 0$

$$a(x_1 - x_0) + b(y_1 - y_0) =$$

$$\underbrace{(ax_1 + by_1)}_c - \underbrace{(ax_0 + by_0)}_c = c - c = 0.$$

So

$$a(x_1 - x_0) = -b(y_1 - y_0)$$

So

$$\left(\frac{a}{d}\right)(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0).$$

So

$$\left(\frac{a}{d}\right) \mid \left(\frac{b}{d}\right) \cdot (y_1 - y_0).$$

Assume that $a \neq 0$
or $b \neq 0$.
Then $d \geq 0$

Then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, by a previous proposition. So $\left(\frac{a}{d}\right) \mid y_1 - y_0$, by

Prop 2.28. Write $y_1 - y_0 = k_1 \left(\frac{a}{d}\right)$,

Similarly $\left(\frac{b}{d}\right) \mid \left(\frac{a}{d}\right) \cdot (x_1 - x_0)$

and $\gcd\left(\frac{b}{d}, \frac{a}{d}\right) = 1$, so

$\left(\frac{b}{d}\right) \mid (x_1 - x_0)$. Write $x_1 - x_0 = k_2 \left(\frac{b}{d}\right)$.

We get that $x_1 = x_0 + k_2 \left(\frac{b}{d}\right)$

$$y_1 = y_0 + k_1 \left(\frac{a}{d}\right).$$

It remains to show that

$$k_2 = -k_1.$$

$$\frac{a}{d} \underbrace{(x_1 - x_0)}_{k_2 \left(\frac{b}{d}\right)} + \frac{b}{d} \underbrace{(y_1 - y_0)}_{k_1 \left(\frac{a}{d}\right)} = 0$$

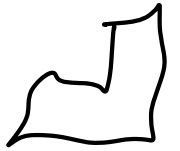
$$\left(\frac{a}{d}\right) \left(\frac{b}{d}\right) k_2 + \left(\frac{a}{d}\right) \left(\frac{b}{d}\right) k_1 = 0.$$

If both $a \neq 0$, $b \neq 0$, ^{and} then

$$K_2 + K_1 = 0, \text{ so } K_2 = -K_1$$

We need to treat the case
 $a = 0$ or $b = 0$ separately.

Exercise.



Ex: Find all solutions
to

$$6x + 15y = 2.$$

$$\gcd(6, 15) = 3$$

$$3 \nmid 2.$$

There aren't any solutions, by
Part (i) of the proposition.