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: $a = 44$, $b = 30$

$$\boxed{44x_i + 30y_i = r_i}$$

Row	x_i	y_i	r_i	q_i
1	1	0	44	–
2	0	1	30	–
3	1	−1	14	1
4	−2	3	$\boxed{2}$	2
			0	

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

$$\gcd\Big(\underbrace{\frac{6}{2}}_{3},\ \underbrace{\frac{10}{2}}_{5}\Big)=1$$

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 $\gcd(a,c) = 1$ (use part 1 of the previous proposition). Let q be an integer, such that $ab = cq$. Write

$$b = \underbrace{1}_{= ax+cy} \cdot b = \underbrace{ab}_{= cq}x + cby = c(qx + by).$$

So $c \mid b$. $\square$

<u>Prop</u>: (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.

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

<u>"if" direction</u>: Assume that d satisfies (i), (ii), (iii). Then $d \neq 0$, by (ii), since $d \mid a$ and $a \neq 0$. So $\boxed{d > 0}$, by part (i). Let c be a common divisor of a and b. Then $c \mid d$, by (iii). So $|c| \leq |d| = d$, by Prop 2.11 (iv). So $c \leq d$. So d is the greatest common divisor.

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

So $d \geq 0$, by def of gcd. So (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 $d = ax + by$. Write $a = cq_1$, $b = cq_2$, then $d = cq_1x + cq_2y = c(q_1x + q_2y)$. So $c | d$. So (iii) holds. ∎

Sec 2.3 Linear Diophantine Equations:

Ex: $a = 44$, $b = 30$. We saw $\gcd(a,b) = 2$ and

(*) $\boxed{44(-2) + 30\cdot(3) = 2} = \gcd(44,30)$

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:

(**) $\boxed{44X + 30y = 104}$

$104 = 52 \cdot 2$, $2 = \gcd(44,30)$

So $(X_0, y_0) = (\overbrace{52\cdot(-2)}^{-104}, \overbrace{52\cdot 3}^{156})$ is a particular solution of (*)

If (x_h, y_h) is an integer solution of

(***) $\boxed{44X + 30y = 0}$, then

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

Eq $(***)$ is equivalent to $\dfrac{(**)}{\gcd(44,30)}$

$(***)'$ $\boxed{22x+15y=0}$

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

(+) $\boxed{\begin{aligned}(x,y) &= (x_0+x_n, y_0+y_n) = \\ &= (-104+15k, 156+(-22)k)\end{aligned}}$

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

<u>Question</u>; Find all solution (x,y) with non-negative integers x, y, of the eq $(**)$ $\boxed{44x+30y=104}$.

<u>Answer</u>; We need to find all values of k, for which the pair (+) is non negative.

$$-104 + 15k \geq 0$$
$$156 - 22k \geq 0$$

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

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

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

Theorem: (i) The Linear Diophantine equation $\boxed{ax+by=c}$ (+)

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

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

Proof: (i) If $\gcd(a,b) = d \mid c$, write $c = dq$, where q is an integer. Let $(\underline{x}, y)$ be a sol'n of $ax+by=d$ (exists, by the E.E.A.) Then (xq, yq) is a solution to (+).

If the exists a sol'n to $ax+by=c$, then $d :\underset{\text{def}}{=} \gcd(a,b)$ divides c, because c is a linear combination of a, b with integer coeff.

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

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

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

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

Then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \underline{1}$, by a previous proposition. So $\left(\frac{a}{d}\right) \Big| \; y_1-y_0$, 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 $a \neq 0$, and $b \neq 0$, then

$k_2 + k_1 = 0$, so $k_2 = -k_1$.

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

Ex: Find all solutions to

$$6x + 15y = \underset{\substack{\shortparallel \\ c}}{2}.$$

$\gcd(6, 15) = 3$

$$3 \nmid 2.$$

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