Greatest Common Divisor
and
The Euclidean Algorithm

Next Topic : Greatest common divisor.

Let $a, b \in \mathbb{Z}$ with a & b not both zero. Without loss of generality, let's assume that $a \neq 0$. Now consider the set of common divisors

$$Div(a,b) = \{ d \in \mathbb{Z} : d|a \wedge d|b \}.$$

Note that for all $d \in Div(a,b)$ we have $d|a$, and since $a \neq 0$ this implies that $d \leq |d| \leq |a|$. We conclude that the set $Div(a,b)$ is bounded above by $|a|$.

[If $b \neq 0$, then the set is also bounded above by $|b|$. What happens if a & b are both zero?]

Since $\text{Div}(a,b)$ is bounded above, Well-Ordering says that it has a greatest element. We will denote this element by $\gcd(a,b)$ and call it the "greatest common divisor" of a & b.

Note: Since we also have $1 \in \text{Div}(a,b)$ [indeed, 1 divides every integer] and since $\gcd(a,b)$ is the greatest element of $\text{Div}(a,b)$ we conclude that

$$1 \leq \gcd(a,b).$$

///

Recall that every integer divides 0, so if $n \neq 0$ we have

$$\begin{aligned} \text{Div}(n,0) &= \text{Div}(n) \\ &= \{d \in \mathbb{Z} : d \mid n\}. \end{aligned}$$

Since the greatest divisor of n is $|n|$, we conclude that $\gcd(n,0) = |n|$.

Q: If a, b are both nonzero, how can we <u>compute</u> $\gcd(a,b)$?

A: There are two ways.

(1) The bad way

We know that $1 \leq \gcd(a,b) \leq \min\{|a|,|b|\}$. Since this is a finite set we can just test every number in this range to see if it divides a & b and report the largest number that does.

Example: To compute $\gcd(-8,30)$, we test every number from 1 to 8.

$$1, 2, \cancel{3}, \cancel{4}, \cancel{5}, \cancel{6}, \cancel{7}, \cancel{8}$$

We conclude that $\gcd(-8,30) = 2$.

When a, b are large this method is very slow, and it doesn't give us any <u>understanding</u> of the situation.

(2) The good way.

This method was called "antenaresis" by Euclid (Book $\underline{\text{VII}}$ Prop 2) and today we call it the "Euclidean Algorithm". It was also known to the Indian mathematician Brahmagupta (c. 628), who called it "kutaka" (the "pulverizer"). Anyway, it's a famous algorithm.

Here's an example:

To compute gcd(1053, 481) we first divide the bigger by the smaller:

$$\underline{1053} = 2 \cdot \underline{481} + \underline{91}$$

Then we "repeat" the process:

$$\underline{481} = 5 \cdot \underline{91} + \underline{26}$$

$$\underline{91} = 3 \cdot \underline{26} + \underline{13}$$

$$\underline{26} = 2 \cdot \underline{13} + \underline{0}$$

The last nonzero remainder is the gcd.
We conclude that $\gcd(1053, 481) = 13$.

That's a pretty fast algorithm [it used 4 divisions instead of 481]

But why does it work? The proof is based on the following Lemma.

☆ Lemma: Consider $a, b \in \mathbb{Z}$, not both zero, and suppose we have $q, r \in \mathbb{Z}$ such that $a = qb + r$. [These q, r are not necessarily the quotient and remainder, but they might be.] Then we have

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

<u>Proof</u>: We will show that the <u>sets</u> $\mathrm{Div}(a,b)$ & $\mathrm{Div}(b,r)$ are equal and it will follow that their greatest elements are equal. To do this we must prove two separate things,

(i) $\mathrm{Div}(a,b) \subseteq \mathrm{Div}(b,r)$
(ii) $\mathrm{Div}(b,r) \subseteq \mathrm{Div}(a,b)$.

For (i) assume that $d \in Div(a,b)$ so that $d|a$ & $d|b$. Since $r = a - qb$ it follows from HW2 Problem 3(b) that $d|r$, hence $d \in Div(b,r)$ as desired.

For (ii) assume that $d \in Div(b,r)$ so that $d|b$ & $d|r$. Since $a = qb + r$ it follows from the same result that $d|a$, hence $d \in D(a,b)$ as desired. ///

Maybe you can see already why this lemma implies the result we want. The key observation is that if $|a| > |b|$ and $|b| > |r|$ then $\gcd(b,r)$ is easier to compute than $\gcd(a,b)$

Stay tuned ...

☆ Theorem (Euclidean Algorithm):

Consider $a, b \in \mathbb{Z}$ with $b \neq 0$. To compute $\gcd(a,b)$ we first apply the Division Theorem to $a \bmod b$ to obtain

$$a = q_1 b + r_1 \quad \text{with} \quad 0 \leq r_1 < |b|.$$

If $r_1 \neq 0$ then we can apply the Division Theorem to $b \bmod r_1$ to obtain

$$b = q_2 r_1 + r_2 \quad \text{with} \quad 0 \leq r_2 < r_1 .$$

If $r_2 \neq 0$ then we obtain

$$r_1 = q_3 r_2 + r_3 \quad \text{with} \quad 0 \leq r_3 < r_2 .$$

I claim that this process eventually terminates; i.e.; $\exists\, n \in \mathbb{N}$ such that

$$r_{n-1} > 0 \quad \text{and} \quad r_n = 0 .$$

Furthermore, I claim that this r is equal to $\gcd(a,b)$. //

Proof: Suppose for contradiction that the process never terminates. Then we obtain an infinite descending sequence

$$|b| = r_0 > r_1 > r_2 > r_3 > \cdots \geq 0$$

Let $S = \{r_0, r_1, r_2, r_3, \cdots\} \subseteq \mathbb{N}$. Since this set is bounded below (by 0), Well-Ordering says that S contains a smallest element, say $m \in S$. Since $m \in S$ we must have $m = r_i$ for some $i \in \mathbb{N}$. But then $r_{i+1} \in S$ is a smaller element of S. Contradiction.

We conclude that $\exists\, n \in \mathbb{N}$ with $r_{n-1} > 0$ and $r_n = 0$. To prove that r_{n-1} is the gcd of a & b, we use the previous lemma to obtain

$$\begin{aligned}
\gcd(a,b) &= \gcd(b, r_1) \\
&= \gcd(r_1, r_2) \\
&= \gcd(r_2, r_3) \\
&\;\;\vdots \\
&= \gcd(r_{n-1}, r_n) \\
&= \gcd(r_{n-1}, 0) = r_{n-1}.
\end{aligned}$$

//

Example: Let's use this to compute the gcd of 385 and 84.

$$\underline{385} = 9 \cdot \underline{84} + \underline{49}$$

$$\underline{84} = 1 \cdot \underline{49} + \underline{35}$$

$$\underline{49} = 1 \cdot \underline{35} + \underline{14}$$

$$\underline{35} = 2 \cdot \underline{14} + \underline{7} \quad \text{last nonzero remainder}$$

$$\underline{14} = 2 \cdot \underline{7} + 0$$

We conclude that $\gcd(385, 84) = 7$

Q: OK, great. But what can we do with gcd's?

A: We can use them to solve the following problem of number theory.

Linear Diophantine Equations :

Let $a, b, c \in \mathbb{Z}$. Our goal is to find all integer solutions $x, y \in \mathbb{Z}$ to the "linear Diophantine equation"

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

HOW? First note that there are some obvious restrictions.

- If $a = b = 0$ and $c \neq 0$ then there are NO SOLUTIONS. If $a = b = 0$ and $c = 0$ then all $x, y \in \mathbb{Z}$ are solutions.

- So assume that $a, b \in \mathbb{Z}$ are not both zero and let $d = \gcd(a, b)$. Say that $a = da'$ and $b = db'$ for some integers $a', b' \in \mathbb{Z}$.

Now if $x, y \in \mathbb{Z}$ is a solution to $(*)$ then we have

$$\begin{aligned} c &= ax + by \\ &= da'x + db'y \\ &= d(a'x + b'y) \end{aligned}$$

which implies that $d \mid c$.

Conclusion: If $\gcd(a,b) \nmid c$ then equation (*) has NO SOLUTIONS.

- So let $d = \gcd(a,b)$ and assume that $d \mid c$, say $c = dc'$ for some $c' \in \mathbb{Z}$.

Then equation (*) becomes

$$\begin{aligned} ax + by &= c \\ da'x + db'y &= dc' \\ \cancel{d}(a'x + b'y) &= \cancel{d}c' \\ a'x + b'y &= c' \end{aligned}$$

by canceling d from both sides.
[This is allowed because $d \neq 0$.]

The new equation

(**) $$\boxed{a'x + b'y = c'}$$

is called the "reduced form" of (*), and it has exactly the same set of solutions.

Proof: If $x, y \in \mathbb{Z}$ solves (*), then

$$ax + by = c$$
$$\cancel{d}a'x + \cancel{d}b'y = \cancel{d}c'$$
$$a'x + b'y = c'.$$

Conversely, if $x, y \in \mathbb{Z}$ solves (**), then

$$a'x + b'y = c'$$
$$d(a'x + b'y) = dc'$$
$$da'x + db'y = dc'$$
$$ax + by = c.$$

///

We'll return to this on Monday.

Linear Equations of Integers

Last time we discussed the Euclidean Algorithm and proved that it works.

Example: Compute gcd(8, 5).

$$\underline{8} = 1 \cdot \underline{5} + \underline{3}$$

$$\underline{5} = 1 \cdot \underline{3} + \underline{2}$$

$$\underline{3} = 1 \cdot \underline{2} + \underline{1}$$

$$\underline{2} = 2 \cdot \underline{1} + 0 \quad \text{STOP.}$$

We conclude that $\gcd(8,5) = 1$.

[Jargon: If $\gcd(a,b) = 1$ then we say the integers a & b are coprime (or relatively prime). In this case we have

$$\mathrm{Div}(a,b) = \{\pm 1\}.$$
]

We conclude that 8 & 5 are coprime.

Q: So what?

A: we will use this to solve the linear Diophantine equation

$$(*) \qquad \boxed{24x + 15y = 3}$$

The word "Diophantine" [after Diophantus of Alexandria (c. AD 200-300)] means that we are only interested in <u>integer</u> solutions $x, y \in \mathbb{Z}$.

The first step is to compute $\gcd(24, 15)$:

$$\begin{aligned} 24 &= 1 \cdot 15 + 9 \\ 15 &= 1 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \implies \gcd(24, 15) = 3. \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

Now we divide both sides of $(*)$ by 3 to get the "reduced equation":

$$(**) \qquad \boxed{8x + 5y = 1}.$$

Note that $x, y \in \mathbb{Z}$ is a solution of (*) if and only if it is a solution of (**), so we only have to solve (**).

There are two steps:

(1) Find any one particular solution $x', y' \in \mathbb{Z}$ to (**),

$$8x' + 5y' = 1.$$

(2) Find the general solution of the associated "homogeneous equation"

$$\boxed{8x + 5y = 0} \qquad (***)$$

It turns out that step (2) is the easy part. Suppose we have a solution $x, y \in \mathbb{Z}$ to (***). Then we get

$$8x + 5y = 0$$
$$8x = -5y,$$

hence $8 \mid 5y$ & $5 \mid 8x$.

Since 8 & 5 are <u>coprime</u>, you will prove on HW 4 Problem 2(a) that this implies

$$8 \mid y \quad \& \quad 5 \mid x,$$

say $y = 8k$ & $x = 5\ell$ for some $k, \ell \in \mathbb{Z}$. Substituting these into (***) gives

$$8(5\ell) + 5(8k) = 0.$$
$$40\ell + 40k = 0$$
$$40(\ell + k) = 0.$$

Since $40 \neq 0$ this implies that $\ell + k = 0$, hence $\ell = -k$. We conclude that the general solution of (***) is

$$(x, y) = (-5k, 8k) \quad \forall\, k \in \mathbb{Z}.$$

[Note: There are infinitely many solutions and they are "parametrized" by $\mathbb{Z}$.]

Step (2) is done so we return to step (1).

Find any <u>one particular solution</u> to

$$8x' + 5y' = 1$$

If we can do this, then you will prove on HW 4 Problem 4 that the complete solution to ** (and hence to *) is

$$(x,y) = (x' - 5k,\ y' + 8k) \quad \forall k \in \mathbb{Z}.$$

[The general solution of ** equals the general solution of the associated homogeneous equation ***, shifted by any one particular solution of **.].

Great. So <u>can</u> we find a particular solution $x', y' \in \mathbb{Z}$?

There are two ways to proceed:

(i) Trial-and-Error.

In a small case like this you can probably just guess a solution. But in larger cases guessing is not practical.

(ii) Augment the Euclidean Algorithm so when we compute $\gcd(a,b)$ it also spits out a solution $x, y \in \mathbb{Z}$ to

$$ax + by = \gcd(a,b).$$

This is called the "Extended Euclidean Algorithm". I'll teach it to you by example. The general idea is that we are looking at triples $x, y, z \in \mathbb{Z}$ such that $8x + 5y = z$. There are two obvious such triples

$$8(1) + 5(0) = 8$$
$$8(0) + 5(1) = 5.$$

Now we apply the Euclidean Algorithm to the triples:

x	y	z
1	0	8
0	1	5
1	-1	3
-1	2	2
2	-3	1 $= \gcd(8,5)$.

The last row tells us that

$$8(2) + 5(-3) = 1.$$

We found one particular solution. So let

$$(x', y') = (2, -3).$$

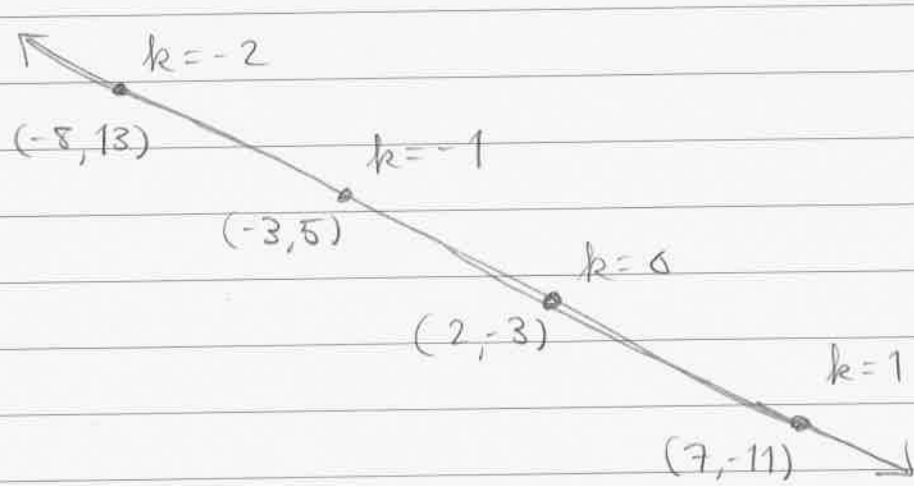
Then the general solution of the linear Diophantine equation (*),

$$24x + 15y = 3,$$

is given by

$$(x, y) = (2 - 5k, -3 + 8k) \quad \forall k \in \mathbb{Z}.$$

In the x, y - plane these are the integer points on the line $y = (1 - 8x)/5$:



Remark: This is actually pretty useful. In the land of Oz their coins only come in two denominations: \$ a & \$ b. If you need to pay for something that costs \$ c, how do you know if this is possible, and if so, how many of each coin to use?

If you don't think that's useful, note that the algorithm can be easily generalized to the case of many coins and many denominations.

Extended Euclidean Algorithm

Recall : Last time we solved the linear Diophantine equation

$$24x + 15y = 3. \quad (*)$$

Step 1 : Reduce the equation by $\gcd(24, 15) = 3$ to get.

$$8x + 5y = 1. \quad (**)$$

Step 2 : Since 8 & 5 are coprime (i.e., $\gcd(8,5) = 1$), the general solution of the homogeneous equation

$$8x + 5y = 0 \quad (***)$$

is $(x, y) = (-5k, 8k) \ \forall k \in \mathbb{Z}$.

Step 3 : Finally, we use the Extended Euclidean Algorithm

to find one particular solution to $**$.
In our case we found

$$8(2) + 5(-3) = 1.$$

We conclude that the full solution of $**$ (and hence $*$) is

$$(x, y) = (2-5k, -3+8k) \quad \forall k \in \mathbb{Z}$$

$$= (2, -3) + k(-5, 8) \quad \forall k \in \mathbb{Z},$$

using vector notation.

You will prove on HW4 that this same process works in general.

Now let's discuss the Extended Euclidean Algorithm a bit more.

Consider $a, b \in \mathbb{Z}$, not both zero (so that $\gcd(a, b)$ exists). We are interested in the set of integer triples (x, y, z) such that

$$ax + by = z.$$

Denote the set by

$$V := \{ (x,y,z) : ax + by = z \}.$$

The Extended Euclidean Algorithm is based on the following lemma.

☆ Lemma: Given two elements (x,y,z) and (x',y',z') of V and an integer $q \in \mathbb{Z}$, we have

$$(x,y,z) - q(x',y',z')$$
$$= (x-qx', y-qy', z-qz') \in V$$

[Jargon: In linear algebra, this is called an "elementary row operation". It is the foundation of "Gaussian elimination".]

Proof: Since $(x,y,z), (x',y',z') \in V$ we know that

$\downarrow$

$$ax + by = z, \quad \text{and}$$
$$ax' + by' = z.$$

Then for all $q \in \mathbb{Z}$ we have

$$a(x - qx') + b(y - qy')$$
$$= (ax + by) - q(ax' + by')$$
$$= z - qz',$$

and hence $(x - qx', y - qy', z - qz') \in V$. ///

So what? We can combine this Lemma with the Euclidean Algorithm as follows.

☆ Extended Euclidean Algorithm

Consider $a, b \in \mathbb{Z}$, not both zero, and define the set

$$V = \{(x, y, z) : ax + by = z\}.$$

There are two obvious elements of this set : $(1, 0, a)$ & $(0, 1, b)$.

Now recall the sequence of divisions we use in the Euclidean Algorithm :

$$
\begin{aligned}
a &= q_1 b + r_1 , & 0 &\le r_1 < |b| \\
b &= q_2 r_1 + r_2 & 0 &\le r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 & 0 &\le r_3 < r_2
\end{aligned}
$$

etc.

We can apply the "same" sequence of steps to the triples $(1, 0, a)$ & $(0, 1, b)$:

$$
\begin{aligned}
&(1 , 0 , a) && ① \\
&(0 , 1 , b) && ② \\
&(1 , -q_1 , r_1) && ③ = ① - q_1 ② \\
&(-q_2 , 1 + q_1 q_2 , r_2) && ④ = ② - q_2 ③
\end{aligned}
$$

etc.

In the end we will find a triple

$$(x, y, \gcd(a,b)),$$

where x & y are some integers. Since $(x, y, \gcd(a,b)) \in V$ by the lemma, we conclude that

$$ax + by = \gcd(a,b).$$

Example: Find one particular solution $x, y \in \mathbb{Z}$ to the equation

$$385x + 84y = 7.$$

It might be hard to guess a solution to this one so we use the E.E.A.:

Consider the set

$$V = \{(x, y, z) : 385x + 84y = z\}.$$

Then we have

x	y	z	
1	0	385	(1)
0	1	84	(2)
1	-4	49	(3) = (1) − 4(2)
-1	5	35	(4) = (2) − 1(3)
2	-9	14	(5) = (3) − 1(4)
-5	23	7	(6) = (4) − 2(5)
12	-55	0	(7) = (5) − 2(6)

From row (6) we conclude that

$$385(-5) + 84(23) = 7.$$

And as a bonus, rows (6) & (7) tell us that the <u>complete</u> solution to the equation $385x + 84y = 7$ is

$$(x,y) = (-5 + 12k, 23 - 55k) \quad \forall k \in \mathbb{Z}.$$

Reason: Well, the lemma implies that this is a solution because

$$(-5, 23, 7) \,\&\, (12, -55, 0) \in V$$

$$\implies (-5, 23, 7) + k(12, -55, 0)$$

$$= (-5 + 12k, 23 - 55k, 7) \in V$$

for all $k \in \mathbb{Z}$.