Division With Remainder

We have now fully discussed the definition of $\mathbb{Z}$ and it's time to start developing the theory of $\mathbb{Z}$. This is the subject of

Number Theory.

We will systematically develop some of the main theorems in this subject and then we will discuss some applications [in particular, to cryptography].

Recall that $\mathbb{Z}$ is not a "group" under multiplication because integers do not (usually) have multiplicative inverses. Our first theorem will tell us how to recover some sort of "division" in $\mathbb{Z}$.

☆ The Division Theorem:

Given integers $a, b \in \mathbb{Z}$ with $b \neq 0$,

① $\exists\, q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \& \quad 0 \leq r < |b|.$$

② These q & r are <u>unique</u>. We call them "the" quotient and "the" remainder of a <u>modulo</u> b.

<u>Proof</u>: For part ① consider any integers $a, b \in \mathbb{Z}$ with $b \neq 0$. It is easy to find $q, r \in \mathbb{Z}$ with $a = qb + r$, but can we do it such that $0 \leq r < |b|$?

Define the set

$$\begin{aligned} S &= \{a - nb : n \in \mathbb{Z}\} \\ &= \{\ldots, a-2b, a-b, a, a+b, a+2b, \ldots\}. \end{aligned}$$

Since $b \neq 0$, this set must contain a non-negative number.

Let $r \in S$ be the smallest non-negative number in S (which exists by well-ordering). By definition of S, there exists $q \in \mathbb{Z}$ such that $r = a - qb$, and hence $a = qb + r$. By definition we also have $0 \leq r$.

Now I claim that $r < |b|$. To prove this, assume for contradiction that $|b| \leq r$. Then we have

$$\begin{aligned} |b| &\leq r \\ |b| - |b| &\leq r - |b| \\ 0 &\leq r - |b|. \end{aligned}$$

On the other hand, since $b \neq 0$ we have $r - |b| < r$. Finally, since

$$r - |b| = a - qb - |b| = a - (q \pm 1) b$$

we conclude that $r - |b| \in S$. This contradicts the fact that r is the smallest non-negative element of S.

///

We have shown that q & r exist with the desired properties. For part (2) we will show that they are unique.

To do this, suppose that we have $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$a = q_1 b + r_1 \quad \& \quad a = q_2 b + r_2$$
$$0 \leq r_1 < |b| \qquad\quad 0 \leq r_2 < |b|.$$

In this case we will show that

$$q_1 = q_2 \quad \& \quad r_1 = r_2.$$

Suppose for contradiction that $r_1 \neq r_2$. Without loss of generality, let's say that $r_1 < r_2$. Then we have

(*) $$0 = r_1 - r_1 < r_2 - r_1 \leq r_2 < |b|.$$

Then since $q_1 b + r_1 = a = q_2 b + r_2$, we have

$$q_1 b + r_1 = q_2 b + r_2$$
$$q_1 b - q_2 b = r_2 - r_1$$
$$(q_1 - q_2) b = (r_2 - r_2)$$

Since $r_1 \neq r_2$, we have $r_2 - r_1 \neq 0$ so that HW2 Problem 3(d) implies

$$|b| \leq |r_2 - r_1| = r_2 - r_1,$$

which contradicts (*). We conclude that $r_1 = r_2$ and hence

$$(q_1 - q_2) b = 0.$$

Since $b \neq 0$ this implies [why?] that $q_1 - q_2 = 0$ and hence $q_1 = q_2$.

//

We conclude that the quotient and remainder of a mod b (mod is short for "modulo") are unique.

QED.

[Remark: At the end of the proof we used the fact that $\mathbb{Z}$ satisfies

☆ Multiplicative Cancellation:

Given $a, b, c \in \mathbb{Z}$ with $a \neq 0$ we have

$$ab = ac \implies b = c.$$

You proved this on HW3.]

The Division Theorem finally allows us to prove a fact that we've been taking for granted for a long time.

Definition: Let $n \in \mathbb{Z}$. We say that n is <u>even</u> if $\exists\, k \in \mathbb{Z}$ with $n = 2k$ and we say that n is <u>odd</u> if $\exists\, l \in \mathbb{Z}$ with $n = 2l + 1$.

Theorem: Every integer is either even or odd; not both, not neither.

Proof: Consider any $n \in \mathbb{Z}$. Since $2 \neq 0$, the Division Theorem says that there exist unique $q, r \in \mathbb{Z}$ such that

$$n = q \cdot 2 + r \quad \& \quad 0 \leq r < 2.$$

Since $0 \leq r < 2$ implies $r \in \{0, 1\}$ we see that n is either even or odd, and it can't be both because the remainder is unique. ///

Here's another basic fact we can finally prove.

Theorem: There does <u>not</u> exist an integer $a \in \mathbb{Z}$ such that $2a = 1$.

Proof: Suppose for contradiction that there <u>does</u> exist $a \in \mathbb{Z}$ such that $2a = 1$. This implies that

$\downarrow$

$$1 = a \cdot 2 + 0,$$

so the remainder of 1 modulo 2 is 0. On the other hand, we have

$$1 = 0 \cdot 2 + 1,$$

so the remainder of 1 mod 2 is 1. Since $0 \neq 1$ this contradicts the uniqueness of the remainder.

Pretty good, huh? I think we've now proved all of the obvious properties of integers that we once assumed.

Greatest Common Divisor

Now we are studying Number Theory.
My goal is to develop a sequence of results building to a major theorem:

☆ Fundamental Theorem of Arithmetic:

Every integer can be factored as a product of primes, and the prime factors are unique up to reordering.

It will take several days of work to get there.

We began last time by proving the result that is the foundation for everything else.

☆ The Division Theorem:

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers $q, r \in \mathbb{Z}$ with the following properties

- $a = qb + r$
- $0 \leq r < |b|$.

We call q the "quotient" and r the "remainder" of a mod b.

Example: Consider $a = -5$ and $b = 2$. There are many ways to write

$$-5 = q \cdot 2 + r,$$

e.g.

$$-5 = 1 \cdot 2 - 7$$
$$-5 = 0 \cdot 2 - 5$$
$$-5 = -1 \cdot 2 - 3$$
$$-5 = -2 \cdot 2 - 1$$
$$-5 = -3 \cdot 2 + 1$$
$$\vdots$$

etc.

But there is a unique way to do it such that $0 \leq r < |2| = 2$. By the above calculations we conclude that the quotient of -5 mod 2 is -3 and the remainder is 1.

Jargon: Let $n \in \mathbb{Z}$ if the remainder of n mod 2 is 1, we say that n is "odd".

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

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

Note that for all $d \in \mathrm{Div}(a,b)$ we have $d|a$, and since $a \neq 0$ this implies that $d \leq |d| \leq |a|$. We conclude that the set $\mathrm{Div}(a,b)$ 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 $\mathrm{Div}(a,b)$ 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 $1 \in \mathrm{Div}(a,b)$ [indeed, 1 divides every integer] and since $\gcd(a,b)$ is the greatest element of $\mathrm{Div}(a,b)$ we conclude that

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

///

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

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

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 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

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

Proof: We will show that the sets $\mathrm{Div}(a,b)$ & $\mathrm{Div}(b,r)$ 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 <u>easier</u> to compute than $\gcd(a,b)$

Stay tuned...

The Euclidean Algorithm

Right now we are building a chain of results that will lead to the Fundamental Theorem of Arithmetic (unique prime factorization of integers).

Each result builds on the previous ones so be careful not to forget what the previous theorems said.

I'll remind you what we did so far.

- D.T. : $\forall a, b \in \mathbb{Z}$ with $b \neq 0$, $\exists$ unique $q, r \in \mathbb{Z}$ such that $(a = qb + r \wedge 0 \leq r < |b|)$.

- Given $a, b \in \mathbb{Z}$, not both zero, the set

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

is bounded above so it has a greatest element called $\gcd(a,b)$.

- If $a \neq 0$ then $1 \leq \gcd(a,b) \leq |a|$.
- If $a \neq 0$ then $\gcd(a,0) = |a|$.
- Given any integers $a, b, q, r \in \mathbb{Z}$ with a & b not both zero, if $a = qb + r$ then we have

$$\mathrm{Div}(a,b) = \mathrm{Div}(b,r)$$

and hence

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

[Note: The q & r here are not necessarily the quotient and remainder, but they might be.

///

This last result leads to a very efficient method for computing greatest common divisors, called the "Euclidean Algorithm".

☆ 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.

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

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

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

$$\underline{35} = 2 \cdot \underline{14} + \underline{7}$$ 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

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

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

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

///

Linear Diophantine Equations

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 <u>coprime</u> (or <u>relatively prime</u>). In this case we have

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

We conclude that 8 & 5 are coprime.

Q: So what?
A: We will use this to solve the linear Diophantine equation

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

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":

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

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"

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

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 coprime, you will prove on HW4 Problem 2(a) that this implies

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

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

$$8(5l) + 5(8k) = 0.$$
$$40l + 40k = 0$$
$$40(l+k) = 0.$$

Since $40 \neq 0$ this implies that $l + k = 0$, hence $l = -k$. 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

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

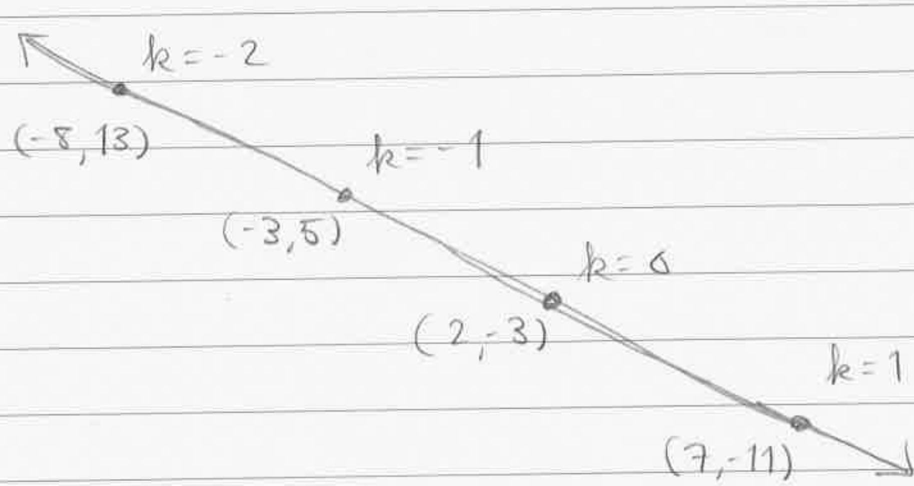
Then the general solution of the linear Diophantine equation (*),

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

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 $y = (1 - 8x)/5$:



Extended Euclidean Algorithm

Recall : Last time we solved the linear Diophantine equation

$$24x + 15y = 3. \qquad *$$

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

$$8x + 5y = 1. \qquad **$$

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

$$8x + 5y = 0 \qquad ***$$

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

Step 3 : Finally, we use the Extended Euclidean Algorithm

$\downarrow$

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

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

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

$$\begin{aligned} a(x - qx') + b(y - qy') &= (ax + by) - q(ax' + by') \\ &= z - qz', \end{aligned}$$

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 $(1, 0, a)$ & $(0, 1, b)$:

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

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 <u>is</u> 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 $k \in \mathbb{Z}$.

The fact that this is the <u>complete</u> solution again follows from your work on HW4.

We have seen that the E.E.A. is useful for solving integer (i.e. "Diophantine") equations. Next time we will use it for more <u>theoretical</u> purposes.

Bézout's Identity

Last time we used the Extended Euclidean Algorithm to find the complete solution of a Linear Diophantine equation. Today we will use the E.E.A. for more theoretical purposes. This will lead to the proof of the Fundamental Theorem of Arithmetic.

First I'll introduce a bit of notation. Consider two sets of integers $S_1, S_2 \subseteq \mathbb{Z}$. Normally it is not possible to "add" sets but in this case we can because both sets consist of numbers. Let

$$\text{"}S_1 + S_2\text{"} := \{ n_1 + n_2 : n_1 \in S_1, n_2 \in S_2 \}.$$

For any integer $a \in \mathbb{Z}$ and set of integers $S \subseteq \mathbb{Z}$ we also define the set

$$\text{"}aS\text{"} := \{an : n \in S\} \subseteq \mathbb{Z}.$$

We will apply these notions in one special situation: Given any integers $a, b \in \mathbb{Z}$, consider the set

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by : x, y \in \mathbb{Z}\}.$$

What can we say about this set? Is it easy to determine which integers are in here?

☆ Theorem (Bézout's Identity):

Consider $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a, b)$. Then we have an equality of sets

$$\boxed{a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}}.$$

Proof: By the E.E.A., we know that there exist integers $x', y' \in \mathbb{Z}$ such that

$$\{$$

* $$ax' + by' = d$$

[In fact there are infinitely many solutions, but right now we only care about the existence of a solution.]

Since $d = \gcd(a,b)$ we also know that $a = da'$ & $b = db'$ for some $a', b' \in \mathbb{Z}$.

Now we will prove that

① $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$
② $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$.

To show ①, consider an arbitrary element $ax+by$ of the set $a\mathbb{Z}+b\mathbb{Z}$. We want to show that $ax+by$ is also in $d\mathbb{Z}$. Indeed, we have

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

To show ②, consider an arbitrary element dn of the set $d\mathbb{Z}$. We want to show that dn is also in $a\mathbb{Z}+b\mathbb{Z}$.

Indeed, using equation $*$ gives

$$d = ax' + by' \in a\mathbb{Z} + b\mathbb{Z}.$$

Remarks:

- This theorem suggests how we might define $\gcd(0,0)$. Since

$$0\mathbb{Z} + 0\mathbb{Z} = 0\mathbb{Z},$$

maybe it makes sense to take

$$\gcd(0,0) := 0 \ ?$$

[It's a completely aesthetic question because it will never matter in applications.]

- The converse of Bézout's Identity is also true. That is: Let $a, b, d \in \mathbb{Z}$ be any integers. IF we have an equality of sets,

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z},$$

then it follows that $\gcd(a,b) = |d|$. ///

We don't need this result right now so I won't prove it. However, I will prove a special case.

☆ Characterization of Coprime Integers:

Let $a, b \in \mathbb{Z}$. Then we have $\gcd(a,b) = 1$ if and only if $\exists\, x, y \in \mathbb{Z}$ such that

$$ax + by = 1.$$

Proof: If $\gcd(a,b) = 1$ then Bézout's Identity says that such x & y exist.

Conversely suppose that $ax + by = 1$ for some $x, y \in \mathbb{Z}$. Now let $d \in \mathbb{Z}$ be any common divisor of a & b, say $a = da'$ and $b = db'$. Then we have

$$\begin{aligned} 1 = ax + by &= da'x + db'y \\ &= d(a'x + b'y), \end{aligned}$$

and hence $d \mid 1$. Since $1 \neq 0$ this implies [by our favorite Problem 3(d) from HW2] that

$$|d| \leq |1| = 1.$$

We also know that 1 is a common divisor of a & b. Hence it must be the greatest common divisor.

- In more abstract kinds of number theory (i.e., number theory in rings other than $\mathbb{Z}$), Bézout's Identity is actually used as the <u>definition</u> of the gcd.

Ok, that's enough about "coprimality". It's time to discuss "primality".

☆ Definition: Let $d, n \in \mathbb{Z}$. If

$$d \mid n \quad \wedge \quad d \notin \{\pm 1, \pm n\}$$

Then we say that d is a proper divisor of n. [The numbers $\pm 1, \pm n$ are called trivial divisors of n.]

We say that $n \in \mathbb{Z}$ is prime if

- n has no proper divisor
- $n \neq \pm 1$.

Discussion:

- 0 is not prime because it has infinitely many proper divisors.
- We do consider $-2, -3, -5, -7, \ldots$ to be prime but you won't lose anything if you just look at positive primes
- We could take ± 1 to be prime but it would make the statement of certain theorems more awkward It's mostly a matter of aesthetics.

Unique Prime Factorization
(Fundamental Theorem of Arithmetic)

Last time we proved the following.

☆ Theorem (Bézout's Identity):

Consider $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a, b)$. Then we have an equality of <u>sets</u>

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

//

The converse statement is also true. That is, given integers $a, b, d \in \mathbb{Z}$, <u>if</u> we have an equality of sets

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z},$$

<u>then</u> it follows that $\gcd(a, b) = |d|$. //

[We only proved this in the case $d = 1$.]

After that we defined prime numbers.

☆ Definition: Let $n \in \mathbb{Z}$ with $n \notin \{0, \pm 1\}$. We say that $d \in \mathbb{Z}$ is a <u>proper divisor</u> of n if

$$d \mid n \quad \& \quad d \notin \{\pm 1, \pm n\}.$$

We say that n is prime if it has <u>no</u> proper divisor. //

═

Since Exam 1 we have been working towards the following result.

☆ Fundamental Theorem of Arithmetic.

Let $n \in \mathbb{Z}$ with $n \notin \{0, \pm 1\}$. Then n can be expressed as a product of finitely many prime numbers. Moreover, if we have two such factorizations

$$n = \pm p_1 p_2 \cdots p_r = \pm q_1 q_2 \cdots q_s,$$

then we have $r = s$ and it is possible to rename the factors so that $p_1 = q_1, p_2 = q_2, \cdots, p_r = q_r$. ///

In other words, every integer $n \notin \{0, \pm 1\}$ has a unique prime factorization.

The F.T.A. appears for the first time in Euclid and its proof is based on the following lemma.

☆ Euclid's Lemma (Book VII Prop 30):

Let $p \in \mathbb{Z}$ be prime and consider any integers $a, b \in \mathbb{Z}$. Then

$$p \mid (ab) \Longrightarrow p \mid a \text{ or } p \mid b.$$

Proof: We will prove the logically equivalent statement

$$p \mid (ab) \text{ and } p \nmid a \Longrightarrow p \mid b.$$

So assume that $p \mid ab$, say $ab = pk$, and assume $p \nmid a$. In this case I claim that $\gcd(p, a) = 1$. Indeed, the only divisors of p are $\pm 1, \pm p$.

↓

And we have assumed that $p \nmid a$, so the only <u>common</u> divisors of p & a are ± 1.

Now since $\gcd(p,a) = 1$, Bézout's Identity says $\exists\, x, y \in \mathbb{Z}$ such that

$$px + ay = 1.$$

Finally, we multiply both sides by b to get

$$\begin{aligned}(px+ay)b &= b\\ pbx + aby &= b\\ pbx + pky &= b\\ p(bx+ky) &= b,\end{aligned}$$

hence $p \mid b$ as desired. ///

Remarks:

- It's possible that $p \mid a$ <u>and</u> $p \mid b$, for example if $p = 2$, $a = 6$, $b = 10$,

$$2 \mid 60 \implies 2 \mid 6 \text{ or } 2 \mid 10$$

✓

- The result is <u>false</u> when p is not prime, for example if $p=4$, $a=6$, $b=10$,

$$4 \mid 60 \text{ but } 4 \nmid 6 \text{ and } 4 \nmid 10.$$

- One can use induction to prove the following generalization of Euclid's Lemma:

Let $p \in \mathbb{Z}$ be prime and consider any n integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If

$$p \mid (a_1 a_2 \cdots a_n)$$

then there exists (at least one) index $i \in \{1, 2, \ldots, n\}$ such that

$$p \mid a_i.$$

///

We are now ready to prove the uniqueness of prime factorization in $\mathbb{Z}$. The <u>existence</u> of prime factorization follows from well-ordering [we'll prove it later].

Proof of F.T.A. (uniqueness):

Suppose we have

$$n = \pm p_1 p_2 \cdots p_r = \pm q_1 q_2 \cdots q_s .$$

where $p_1, p_2, \cdots, p_r, q_1, q_2, \cdots, q_s$ are prime.

Since $p_1 \mid (q_1 q_2 \cdots q_s)$, Euclid's Lemma says $\exists$ i such that $p_1 \mid q_i$. By renaming the q's if necessary we can assume that $p_1 \mid q_1$. Since p_1 & q_1 are prime, this implies that

$$p_1 = \pm q_1 .$$

Cancelling this from the factorization gives

$$\pm p_2 p_3 \cdots p_r = \pm q_2 q_3 \cdots q_s .$$

Now since $p_2 \mid (q_2 \cdots q_s)$, $\exists$ i such that $p_2 \mid q_i$. WLOG, say $p_2 \mid q_2$.
Then we have

$$p_2 = \pm q_2$$

and cancelling from both sides gives

$$\pm p_3 p_4 \cdots p_r = \pm q_3 q_4 \cdots q_s .$$

Continuing in this way gives

$$p_1 = \pm q_1 , \; p_2 = \pm q_2 , \; p_3 = \pm q_3 , \; \ldots$$

and we must have $r = s$ since otherwise we will find a prime number equal to ± 1, which we explicitly said is not a prime number.

QED.

Remarks:

- "Continuing in this way" really means that we use induction or well-ordering. Maybe we'll fill this in later; maybe not. We use induction so often that it's not always worthwhile to spell out the details.

- I used "$\pm$" a lot in the proof. This is because prime factorization doesn't really care about negative signs.

For example, "the" prime factorization of 6 is

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= 3 \cdot 2 \\ &= (-2)(-3) \\ &= (-3)(-2) \end{aligned}$$

and we regard all of these as "the same".

- The reason that we don't call ± 1 prime is because it would break the uniquness in a silly way

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= 2 \cdot 3 \cdot 1 \\ &= 2 \cdot 3 \cdot 1 \cdot 1 \\ &= 2 \cdot 3 \cdot 1 \cdot 1 \cdot 1 \\ &\vdots \end{aligned}$$

etc.

To make the statement cleaner we just declare that ± 1 is not prime. It's a purely aesthetic choice