Logic in Mathematics

We've discussed how logic is encoded by computers. Now we'll discuss how logic is used by humans.

Humans use logic for arguments/proofs, and the most important symbol in a proof is " $\Longrightarrow$ ".

Here's the truth table

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

When we read it we say

$$\text{"}P \Rightarrow Q\text{"} = \text{"if } P \text{ then } Q\text{"}$$
$$= \text{"}P \text{ implies } Q\text{"}$$

You might worry that $F \Rightarrow F = T$. In other words, "if $1+1=3$ then $1+1=5$" is a true statement.

But don't worry. The truth table of $\Rightarrow$ is NOT THE POINT!

Here's the point:

$$\boxed{T \text{ flows along } \Rightarrow}$$

So, this is OK

$$F \Rightarrow F \Rightarrow T \Rightarrow T \Rightarrow T \quad \checkmark$$

This is OK

$$F \Rightarrow F \Rightarrow F \Rightarrow F \Rightarrow F \quad \checkmark$$

But this is NOT OK

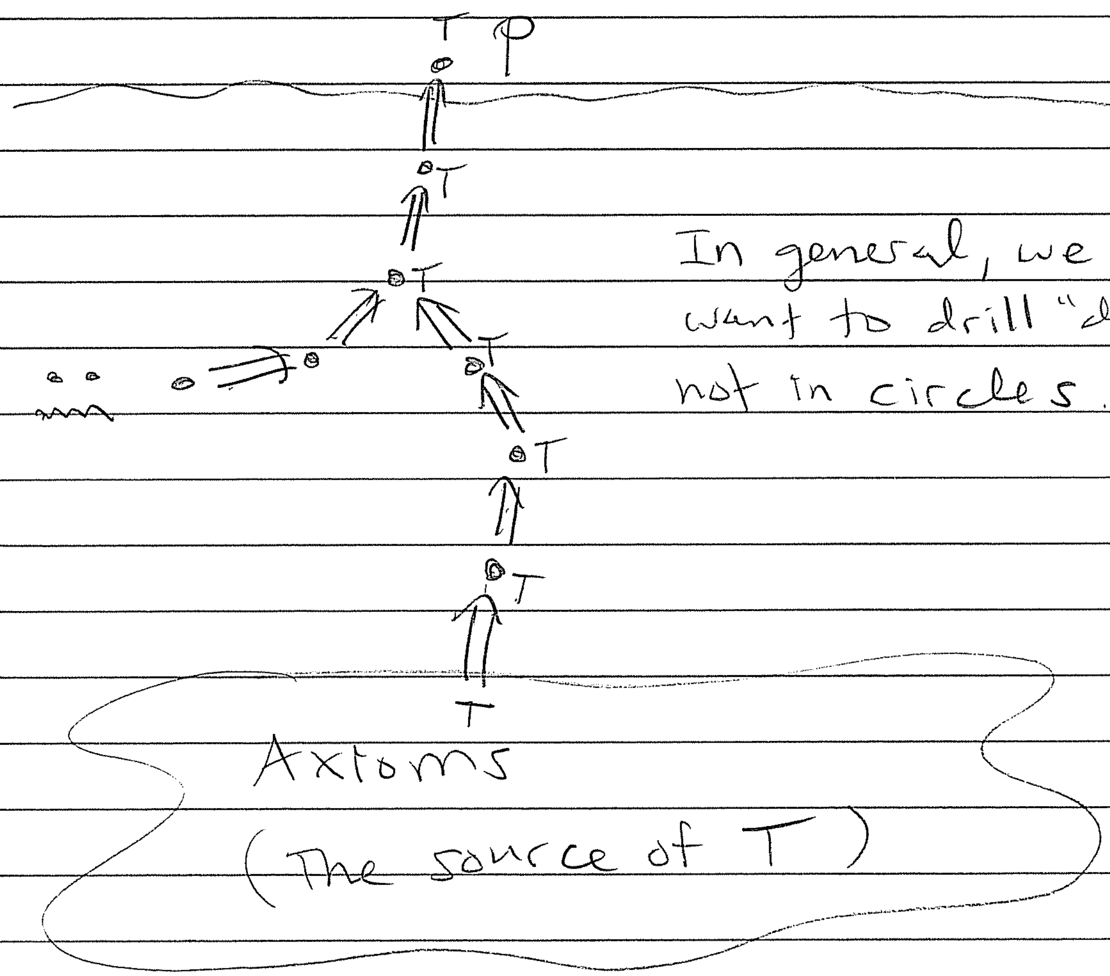
$$T \Rightarrow T \Rightarrow T \Rightarrow F \Rightarrow F$$

This T is not flowing properly.

What does it mean to prove a mathematical statement P?

It's like drilling a well. We construct a chain of arrows backwards from P until we hit the axioms.
Then T flows up!

Picture



In general, we want to drill "down", not in circles.

The first formal use of proof was in ancient Greece (Thales ⇝ Pythagoras ⇝ Euclid). The first theory of human argument was written down by Aristotle:

Example: "Syllogism"

All men are mortal	Premise 1
Socrates is a man	Premise 2
$\therefore$ Socrates is mortal	Conclusion

$\therefore$ "Therefore"

Aristotle considred this argument self-evidently valid. We can "prove" this with a truth table.

Let P = "x is socrates"
Q = "x is a man"
R = "x is mortal".

The argument is

$$\begin{array}{l} Q \Rightarrow R \\ P \Rightarrow Q \\ \hline \therefore\ P \Rightarrow R \end{array}$$

Here is a truth table

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$P \Rightarrow R$	
T	T	T	T	T $\longrightarrow$	T	✓
T	T	F	T	F	F	
T	F	T	F	T	T	
T	F	F	F	T	F	
F	T	T	T	T $\longrightarrow$	T	✓
F	T	F	T	F	T	
F	F	T	T	T $\longrightarrow$	T	✓
F	F	F	T	T $\longrightarrow$	T	✓

If the premises are T then the conclusion is T, so the argument is <u>valid</u>.

We can say this formally as follows.

For all values $P, Q, R \in \{T, F\}$ we have

$$(((Q \Rightarrow R) \wedge (P \Rightarrow Q)) \Rightarrow (P \Rightarrow R)) = T.$$

"if $Q \Rightarrow R$ and $P \Rightarrow Q$ then $P \Rightarrow R$".

In general an (Aristotelian) argument looks like

$$\begin{array}{ll} P_1 & \text{Premise 1} \\ P_2 & \text{Premise 2} \\ \vdots & \vdots \\ \underline{P_k} & \underline{\text{Premise } k} \\ \therefore Q & \therefore \text{Conclusion} \end{array}$$

We say the argument is valid if for all Boolean inputs we have

$$((P_1 \wedge P_2 \wedge \cdots \wedge P_k) \Rightarrow Q) = T$$

Example: "Modus Ponens"

$$\begin{array}{ll} P \Rightarrow Q & \text{If today is Monday I will teach 309.} \\ \underline{P} & \underline{\text{Today is Monday}} \\ \therefore Q & \therefore \text{I will teach 309.} \end{array}$$

VALID?

We analyze the statement $((P \Rightarrow Q) \wedge P) \Rightarrow Q$

P	Q	$P \Rightarrow Q$	$(P \Rightarrow Q) \wedge P$	$((P \Rightarrow Q) \wedge P) \Rightarrow Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

The argument is valid.

Another Example: "Modus Tollens"

$$\begin{array}{l} P \Rightarrow Q \\ \neg Q \\ \hline \neg P \end{array} \qquad \begin{array}{l} \text{Every dog has hair} \\ x \text{ has no hair} \\ \hline x \text{ is not a dog} \end{array}$$

VALID?

We analyze $((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$.

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$(P \Rightarrow Q) \wedge \neg Q$	$((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$
T	T	F	F	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	F	T
F	F	T	T	T	T	T

VALID ✓

"Modus Tollens" is related to an important principle of logic.

☆ The Principle of Contrapositive.

For all statements P, Q we have

$$\boxed{\text{"}P \Rightarrow Q\text{"} \underset{\substack{\uparrow \\ \text{logically equivalent}}}{=} \text{"}\neg Q \Rightarrow \neg P\text{"}}$$

Proof: Look at the truth table

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	$Q \Rightarrow P$	$\neg P \Rightarrow \neg Q$
T	T	F	F	T	T	T	T
T	F	F	T	F	F	T	T
F	T	T	F	T	T	F	F
F	F	T	T	T	T	T	T

same. $\qquad$ same

Note that "$P \Rightarrow Q$" = "$\neg Q \Rightarrow \neg P$"

but "$P \Rightarrow Q$" $\neq$ "$Q \Rightarrow P$"

//

Here's an argument from Lewis Carroll:

Babies are illogical
Nobody is despised who can manage a crocodile.
Illogical persons are despised.
Therefore, babies cannot manage crocodiles.

VALID?

Let $P =$ "x is a baby"
$Q =$ "x is illogical"
$R =$ "x can manage a crocodile"
$S =$ "x is despised".

The argument is

$$\begin{array}{l} P \Rightarrow Q \\ R \Rightarrow \neg S \\ Q \Rightarrow S \\ \hline \therefore\ P \Rightarrow \neg R \end{array}$$

We can replace $R \Rightarrow \neg S$ by its equivalent contrapositive $S \Rightarrow \neg R$.

to get
$$\begin{array}{c} P \Rightarrow Q \\ S \Rightarrow \neg R \\ Q \Rightarrow S \\ \hline \therefore\ P \Rightarrow \neg R \end{array}$$

We can rearrange the order of the premises to get

$$\begin{array}{c} P \Rightarrow Q \\ Q \Rightarrow S \\ S \Rightarrow \neg R \\ \hline \therefore\ P \Rightarrow \neg R \end{array}$$

This is valid. It is just two "syllogisms" put together. The generalized syllogism

$$\begin{array}{c} P_1 \Rightarrow P_2 \\ P_2 \Rightarrow P_3 \\ \vdots \\ P_{k-1} \Rightarrow P_k \\ \hline \therefore\ P_1 \Rightarrow P_k \end{array}$$

is valid. It is sometimes called a "sorites", or a "polysyllogism".

It is proved by induction.

Q: Do you like the word "polysyllogism"?

The Contrapositive

Today: More about "$\Longrightarrow$".

Recall the truth table

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

The disjunctive normal form is

"$P \Rightarrow Q$" = "$(P \wedge Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q)$"

but this is not very nice. Instead look at $\neg$"$P \Rightarrow Q$" = "$P \not\Rightarrow Q$"

P	Q	$P \not\Rightarrow Q$
T	T	F
T	F	T
F	T	F
F	F	F

The disjunctive normal form is

$$\text{"}P \not\Rightarrow Q\text{"} = \text{"}P \wedge \neg Q\text{"}$$

and this is nice. Then using de Morgan we have

$$\begin{aligned}\text{"}P \Rightarrow Q\text{"} &= \neg \text{"}P \not\Rightarrow Q\text{"} \\ &= \neg (P \wedge \neg Q) \\ &= \neg P \vee \neg\neg Q \\ &= \neg P \vee Q.\end{aligned}$$

This can be useful:

$$\boxed{\text{"}P \Rightarrow Q\text{"} = \text{"}\neg P \vee Q\text{"}}$$

For example, we can use it to demonstrate the

☆ Principle of Contrapositive:

$$\boxed{\text{"}P \Rightarrow Q\text{"} = \text{"}\neg Q \Rightarrow \neg P\text{"}}$$

Proof: $\text{"}P \Rightarrow Q\text{"} = \text{"}\neg P \vee Q\text{"}$
$= \text{"}Q \vee \neg P\text{"}$
$= \text{"}\neg(\neg Q) \vee (\neg P)\text{"}$
$= \text{"}\neg Q \Rightarrow \neg P\text{"}$ //

Q: What is the contrapositive in the language of set theory?

Recall the "dictionary"

$$A \cup B = \{x \in U : x \in A \text{ OR } x \in B\}$$
$$A \cap B = \{x \in U : x \in A \text{ AND } x \in B\}$$
$$A^c = \{x \in U : \text{NOT } x \in A\}$$

Now we have one more

$$\text{"}A \subseteq B\text{"} = \text{"}x \in A \Rightarrow x \in B\text{"}$$
(if $x \in A$ then $x \in B$)

The contrapositive says

$$\begin{aligned} \text{"}A \subseteq B\text{"} &= \text{"}x \in A \Rightarrow x \in B\text{"} \\ &= \text{"}x \notin B \Rightarrow x \notin A\text{"} \\ &= \text{"}x \in B^c \Rightarrow x \in A^c\text{"} \\ &= \text{"}B^c \subseteq A^c\text{"} \end{aligned}$$

In summary:

The Contrapositive for sets says

$$\boxed{\text{"} A \subseteq B \text{"} = \text{"} B^c \subseteq A^c \text{"}}$$

Recall how we define equality of sets:

"$A = B$" = "$A \subseteq B$ AND $B \subseteq A$"

= "$x \in A \Rightarrow x \in B$ AND $x \in B \Rightarrow x \in A$"

We have a name for this operation:

Given $P, Q \in \{T, F\}$ we define

"$P \Leftrightarrow Q$" := "$P \Rightarrow Q$ AND $Q \Rightarrow P$"

$(P \Leftrightarrow Q) = (P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Truth table

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

So $\Leftrightarrow$ acts like an equals sign.
We call it logical equivalence.

We often say

"$P \Leftrightarrow Q$" = "P if and only if Q"

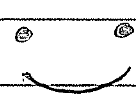
based on the old-fashioned uses

"$Q \Rightarrow P$" = "P if Q"
"$P \Rightarrow Q$" = "P only if Q"

Finally, we can say this:

"$A = B$" = "$x \in A \Leftrightarrow x \in B$"
= "$x \in A$ if and only if $x \in B$"

We have now seen all the logic
we will ever need.



Q: How is logic used in mathematics?

First we need a bit of math to work with.
Recall the set of integers

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

($\mathbb{Z}$ is for "Zahlen")

"Was sind und was sollen die Zahen?"
Richard Dedekind, 1888.

Given $n \in \mathbb{Z}$ we say that n is even
if there exists $k \in \mathbb{Z}$ such that $n = 2k$.

"n is even" := "$\exists k, n = 2k$"

Otherwise we say that n is odd.

$$\begin{aligned} \text{"}n \text{ is odd"} &:= \neg \text{"}n \text{ is even"} \\ &= \neg \text{"}\exists k \in \mathbb{Z}, n = 2k\text{"} \\ &= \text{"}\forall k \in \mathbb{Z}, n \neq 2k\text{"}. \end{aligned}$$

Maybe there is a nicer way to say that n is odd? Yes, in fact we have

"n is odd" = "$\exists k \in \mathbb{Z}, n = 2k+1$"

but we won't prove this today. (Thinking Problem: How could we possibly prove this? We would need a formal definition of the integers, which we don't have yet.)

Let's just assume it for now.

Problem: Given $m, n \in \mathbb{Z}$, prove that

"if mn is even then m is even or n is even."

First attempt at proof:

If mn is even then $\exists k \in \mathbb{Z}$ such that $mn = 2k$. We want to show that $\exists a \in \mathbb{Z}$ such that $m = 2a$, or $\exists b \in \mathbb{Z}$ such that $n = 2b$, or both.

Where would this a or b come from?

First attempt fails.

Second attempt at proof:

Let $P =$ "mn is even"
$Q =$ "m is even"
$R =$ "n is even"

We want to prove that

$$P \Rightarrow (Q \vee R).$$

Does this help? Maybe we can use Boolean algebra to put this in a more convenient form...

Let's try the contrapositive:

"$P \Rightarrow (Q \vee R)$" = "$\neg(Q \vee R) \Rightarrow \neg P$"
= "$(\neg Q \wedge \neg R) \Rightarrow \neg P$"

= "if m and n are both odd, then the product mn is odd"

Let's try to prove that.

If m and n are both odd, then there exist $k, l \in \mathbb{Z}$ such that

$$m = 2k + 1 \quad \text{and} \quad n = 2l + 1.$$

Then the product is

$$\begin{aligned} mn &= (2k+1)(2l+1) \\ &= 4kl + 2k + 2l + 1 \\ &= 2(2kl + k + l) + 1. \end{aligned}$$

Hence $\exists z \in \mathbb{Z}$ (in particular, $z = 2kl + k + l$) such that $mn = 2z + 1$.

We conclude that mn is odd, as desired.

Done.

Second attempt succeeded. :)

Now let's write it up nicely.

<u>Theorem</u>: Given $m, n \in \mathbb{Z}$ we have that

if mn is even then m or n is even.

<u>Proof</u>: We will show the contrapositive statement. That is, we will show that if m and n are both <u>odd</u>, then mn is odd.

So assume that $m = 2k+1$ and $n = 2l+1$. Then the product is

$$\begin{aligned} mn &= (2k+1)(2l+1) \\ &= 4kl + 2k + 2l + 1 \\ &= 2(2kl + k + l) + 1, \end{aligned}$$

wich is odd.

Q.E.D.

$\square$

///

or whatever victory symbol you like.

We use logic in mathematics to be clear about <u>what</u> exa<u>ct</u>ly we are proving, and to express it in the most convenient way.

Epilogue: Given $n \in \mathbb{Z}$, <u>why</u> is it true that

$$\text{“}\forall k \in \mathbb{Z},\ n \underset{\text{not}}{=} 2k\text{''} = \text{“}\exists \ell \in \mathbb{Z},\ n = 2\ell + 1\text{''}$$

??

This has nothing to do with logic. It is a special fact about the integers called the Division Theorem.

☆ The Division Theorem:

Given $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist integers $q, r \in \mathbb{Z}$ such that

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

This q, r are called the “quotient” and “remainder” when a is divided by b.

They are <u>unique</u> in the sense that if

$$a = q_1 b + r_1 \qquad \text{and} \qquad a = q_2 b + r_2$$
$$0 \le r_1 < |b| \qquad\qquad 0 \le r_2 < |b|,$$

it follows that $q_1 = q_2$ and $r_1 = r_2$. //

Proof postponed ☹

As a consequence of the Division Theorem, we see that every integer $n \in \mathbb{Z}$ has the form $n = 2k$ or $n = 2k+1$ for some $k \in \mathbb{Z}$.

<u>Proof</u>: Given $n \in \mathbb{Z}$, we can divide it by 2 to get

$$n = 2q + r$$
$$0 \le r < 2 \qquad (r = 0 \text{ or } r = 1)$$

If $r = 0$ we say n is even. If $r = 1$ we say n is odd. Note that this expression is <u>unique</u> (i.e. it is not possible for n to be <u>both</u> even and odd.) //

This theorem is the FOUNDATION of number theory. I will show you the traditional proof, and maybe this will suggest what the formal definition of $\mathbb{Z}$ should be....

☆ Traditional Proof of the Div. Theorem:

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We want to somehow find $q, r \in \mathbb{Z}$ with the desired properties.

Here's the trick. Consider the set

$$S = \{a - kb : k \in \mathbb{Z}\}$$
$$= \{\ldots, a-2b, a-b, a, a+b, a+2b, \ldots\}$$

Since $b \neq 0$ this set contains both negative and positive numbers. Let

$$S^+ = \{x \in S : x \geq 0\} \subseteq S$$

Since $S^+ \neq \emptyset$, it contains a smallest element. Call this smallest element

$$r \in S^+.$$

Since $r \in S$ we know that there exists $k \in \mathbb{Z}$ such that

$$r = a - kb$$

Why don't we just call this $k = q$?
Then we have

$$a - qb = r$$
$$a = qb + r.$$

Good. But we still need to show that $0 \leq r < |b|$. Since $r \in S^+$ by definition we know that $0 \leq r$. If $r = 0$ we're done, so suppose that we have $0 < r$.

Now we want to show that

$$r < |b|$$

In other words, we want to show that $r \geq |b|$ is <u>impossible</u>.

$\downarrow$

To demonstrate that $r \geq |b|$ is impossible we will show that it leads to a CONTRADICTION. If $r \geq |b|$ then subtracting $|b|$ from both sides gives

$$r \geq |b|$$
$$r - |b| \geq |b| - |b|$$
$$r - |b| \geq 0$$

But note that

depending if b is positive or negative

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

Since $r - |b| = a - (q \pm 1)b$
$= a - (\text{something})b$

and $r - |b| \geq 0$

we conclude that $r - |b|$ is an element of the set S^+. But note that

$$-|b| < 0$$
$$r - |b| < r.$$

(We added r to both sides of $-|b| < 0$.)

Didn't we define <u>define</u> r as the <u>smallest</u> element of S^+?

Yes we did. So we have reached the desired CONTRADICTION.

We conclude that $r \geq |b|$ is impossible and hence we have

$$0 \leq r < |b|$$

as desired.

[Remark: This is already enough to prove that if $n \in \mathbb{Z}$ is <u>not even</u> then $n = 2k+1$ for some $k \in \mathbb{Z}$.

Indeed, suppose $n \in \mathbb{Z}$ is not even. By the above proof $\exists\, q, r \in \mathbb{Z}$ such that

$$n = 2q + r$$
and $$0 \leq r < 2 \quad (\text{i.e. } r = 0 \text{ or } 1).$$

Since n is not even we know that $r \neq 0$. Hence $r = 1$ and we have $n = 2q + 1$.]

We have shown that $\exists\, q, r \in \mathbb{Z}$ with the desired properties, but we still need to show that they are UNIQUE.

So suppose that we have

$$a = q_1 b + r_1 \qquad \text{and} \qquad a = q_2 b + r_2$$
$$0 \leq r_1 < |b| \qquad\qquad 0 \leq r_2 < |b|.$$

In this case we want to prove that

$$q_1 = q_2 \quad \text{and} \quad r_1 = r_2.$$

First we will show that $r_1 \neq r_2$ is impossible. Indeed, if $r_1 \neq r_2$ (let's say $r_1 < r_2$) then we have

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

[Here we used the facts

$$r_1 < r_2 \implies r_1 - r_1 < r_2 - r_1$$

and $$-r_1 \leq 0 \implies r_2 - r_1 \leq r_2. \quad]$$

But since $a = q_1 b + r_1$ and $a = q_2 b + r_2$ we have

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

Since $r_2 - r_1 \neq 0$ and $b \neq 0$ we know that $q_1 - q_2 \neq 0$. Since $q_1 - q_2$ is an integer (i.e. a "whole number"), this implies that

$$1 \leq |q_1 - q_2|$$
$$|b| \leq |q_1 - q_2| \cdot |b|$$
$$|b| \leq |(q_1 - q_2) b|$$
$$|b| \leq |r_2 - r_1|$$
$$|b| \leq r_2 - r_1.$$

But this CONTRADICTS the fact that $r_2 - r_1 < |b|$, which we know from $(*)$.

This contradiction shows that $r_1 \neq r_2$ is impossible, and hence $r_1 = r_2$, as desired.

Finally, we have

$$(q_1 - q_2)\,b = (r_2 - r_1) = 0.$$

Since $b \neq 0$, this implies that

$$q_1 - q_2 = 0$$
$$q_1 = q_2.$$

We are done. //

Wow. That was a <u>real</u> theorem!

To know what the integers <u>are</u>, we should take careful account of all of the properties that we used in the proof.

Here are the properties I think we used . . . . .

Properties of Addition:

$$a+b=b+a$$
$$a+(b+c)=(a+b)+c$$
$$a+0=a$$
$$\forall a\in\mathbb{Z},\ \exists b\in\mathbb{Z},\ a+b=0 \quad (\text{"subtraction"})$$

Properties of Multiplication:

$$ab=ba$$
$$a(bc)=(ab)c$$
$$a1=a$$

(there is no property of "division", but we did use the property of "cancellation". That is, if $ab=ac$ and $a\neq 0$, then $b=c$)

Property of Distribution:

$$a(b+c)=ab+ac.$$

Properties of Order:

$0 < 1$ (meaning $0 \leq 1$ and $0 \neq 1$)

$a \leq b \implies a + c \leq b + c$

$a \leq b$ <u>and</u> $0 \leq c \implies ac \leq bc$.

.... Did we think of everything?

NO. Because the rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$ also satisfy all of these properties.

What is it about $\mathbb{Z}$ that distinguishes it from, say, $\mathbb{Q}$ and $\mathbb{R}$?

This one puzzled people for a long time.

Stay tuned!

The Definition of "Numbers"

Here we are following in the footsteps of Richard Dedekind (1831–1916). I'll encapsulate his ideas in a

Friendly Definition of $\mathbb{Z}$

$\mathbb{Z}$ is a set equipped with

- an equivalence relation "$=$"
  - $\forall a \in \mathbb{Z}$, $a = a$,
  - $\forall a, b \in \mathbb{Z}$, $a = b \Rightarrow b = a$,
  - $\forall a, b, c \in \mathbb{Z}$, $a = b$ and $b = c \Rightarrow a = c$.
- a total ordering "$\leq$"
  - $\forall a, b \in \mathbb{Z}$, $a \leq b$ and $b \leq a \Rightarrow a = b$,
  - $\forall a, b, c \in \mathbb{Z}$, $a \leq b$ and $b \leq c \Rightarrow a \leq c$,
  - $\forall a, b \in \mathbb{Z}$, $a \leq b$ or $b \leq a$.
- two binary operations
  - $+ : \mathbb{Z}^2 \to \mathbb{Z}$
  - $\times : \mathbb{Z}^2 \to \mathbb{Z}$
- two special elements $0, \underline{1} \in \mathbb{Z}$

satisfying appoximately twelve axioms.

(See the handout.)

Eleven of the axioms are fairly obvious, but there is one axiom that is fairly subtle. It took a long time for people to realize that this is an <u>axiom</u> and not a <u>theorem</u>.

☆ Axiom of Well-Ordering:

Every non-empty set of positive (or non-negative; it's not important) integers has a <u>smallest</u> <u>element</u>.

Formally: $\forall X \subseteq \mathbb{N}$ such that $X \neq \emptyset$, $\exists x \in X$ such that $\forall y \in X$, $x \leq y$.

[Remark: While the first 11 axioms are "algebraic", the well-ordering property is "logical" in nature.]

Yes, indeed, we needed well-ordering in our proof of the Division Theorem (look back and see).

Now our definition of $\mathbb{Z}$ is complete. //

Dedekind did this in 1888.
Giuseppe Peano (1858–1932) came along in 1889 and compactified Dedekind's definition.

Peano's Definition of $\mathbb{N}$

$\mathbb{N}$ is a set equipped with

- an equivalence relation "$=$"
- a function $S : \mathbb{N} \to \mathbb{N}$
- a special element $0 \in \mathbb{N}$

satisfying just <u>three</u> <u>axioms</u>:

1. $\forall n \in \mathbb{N}$, $S(n) \neq 0$.
2. $\forall m, n \in \mathbb{N}$ we have

$$S(m) = S(n) \implies m = n.$$

3. If a set $X \subseteq \mathbb{N}$ satisfies
   - $0 \in X$
   - $\forall n \in \mathbb{N}$, $n \in X \Rightarrow S(n) \in X$.

   then it follows that $X = \mathbb{N}$.

//

Remarks on Peano:

- We are supposed to think

$$S(n) = \text{"}n+1\text{"}$$

(S is for "successor").

- The third axiom is called the principle (or axiom) of induction. It is logically equivalent to well-ordering but we probably won't prove this.

- Induction is subtle in the friendly definition (we almost missed it!) but it becomes the very heart of Peano's definition

Moral of the story:

It is not obvious, but

principle of induction $\equiv$ concept of number

Thanks for your attention.

//

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 compute $\gcd(a,b)$?

A: There are two ways.

1) The bad way

We know that $1 \le \gcd(a,b) \le \min\{|a|, |b|\}$. 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 understanding 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

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

Proof: 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

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

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

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

If $r_2 \neq 0$ then we obtain

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

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

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

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 some set of solutions.

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

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

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

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

///

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

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

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"

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

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 one particular solution 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 can 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

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

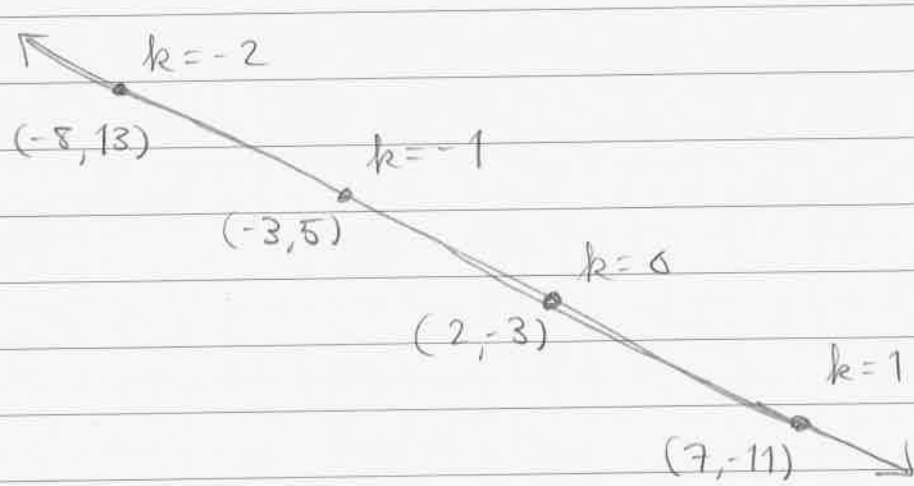
Then the general solution of the linear Diophantine equation (*),

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The fact that this is the complete solution again follows from your work on HW 4.

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 theoretical purposes.