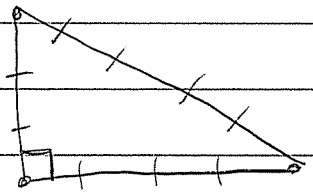
HW 2 Ave 17.5
Med 18 /20.

Mon Sept 24.

Back to the story of math...

We all know that $3^2+4^2=5^2$



(Ancient engineering)

Maybe you also know $5^2+12^2=13^2$.

Q: How could we find more of these "Pythagorean triples"?
(i.e. integers a, b, c such that $a^2+b^2=c^2$)

There is a Babylonian clay tablet from ~1800 BC ("Plimpton 322") that contains a systematic table of 15 Pyth. triples
- suggests they knew a method.

eg. $120^2+119^2=169^2$

$\vdots$

$90^2+56^2=106^2$.

We will solve the problem.

Suppose a, b, c are integers with $a^2 + b^2 = c^2$

Divide by c^2 to get

$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$$

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

$\Rightarrow$ $(x, y) = \left(\frac{a}{c}, \frac{b}{c}\right)$ is a "rational point" on the unit circle, written with a common denominator. We may assume a, b, c have no common factor.

Conversely, let $x^2 + y^2 = 1$ with x, y rational and write $x = \frac{a}{c}$, $y = \frac{b}{c}$ and reduce fractions so a, b, c have no common factors. Then

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$$

$$\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$$

$\Rightarrow$ $a^2 + b^2 = c^2$.

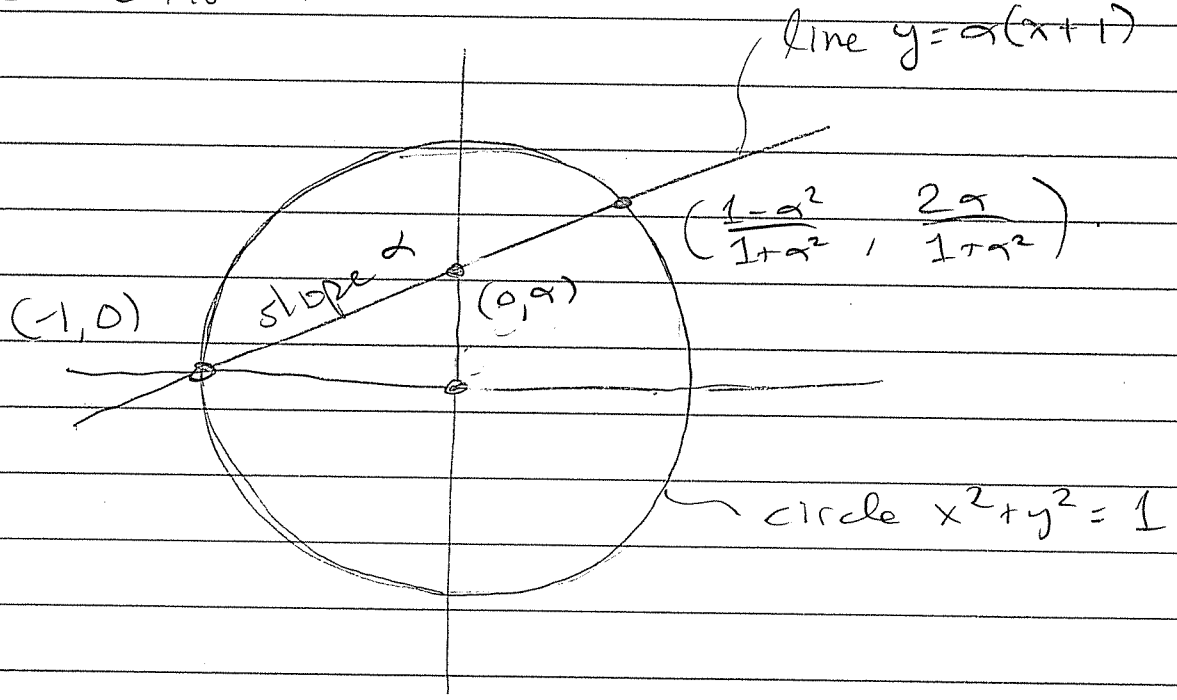
Conclusion: There is a bijection between

rational points on $x^2+y^2=1$ $\longleftrightarrow$ Pythagorean triples $a^2+b^2=c^2$ where a, b, c have no common factor.

"primitive Pyth. Triples".

Does this help?

Recall HW 2.5.



You proved: α is rational $\Longleftrightarrow$ the point $\left(\frac{1-\alpha^2}{1+\alpha^2}, \frac{2\alpha}{1+\alpha^2}\right)$ is rational

Idea: As α moves between $-\infty$ and $+\infty$ we get every rational point on $x^2+y^2=1$ (i.e. primitive Pythagorean triple) exactly once.

So let $\alpha = m/n$ in lowest terms. Then

$$\frac{1-a^2}{1+a^2} = \frac{1-m^2/n^2}{1+m^2/n^2} = \frac{n^2-m^2}{n^2+m^2}.$$

$$\frac{2a}{1+a^2} = \frac{2m/n}{1+m^2/n^2} = \frac{2mn}{n^2+m^2}$$

Hence

$$\left(\frac{n^2-m^2}{n^2+m^2}\right)^2 + \left(\frac{2mn}{n^2+m^2}\right)^2 = 1.$$

$$(n^2-m^2)^2 + (2mn)^2 = (n^2+m^2)^2.$$

this gives us all the primitive Pythagorean triples.

eg.

coprime		prim. Pyth. triple.	
(m,n)	$\longrightarrow$	$(n^2-m^2,\ 2mn,\ n^2+m^2)$	
$(1,2)$	$\longrightarrow$	$(3,\ 4,\ 5)$	$3^2+4^2=5^2$
$(2,3)$	$\longrightarrow$	$(5,\ 12,\ 13)$	$5^2+12^2=13^2$
$(3,4)$	$\longrightarrow$	$(7,\ 24,\ 25)$	$7^2+24^2=25^2$

$(55,72) \longrightarrow (2159,\ 7920,\ 8209)$

$$2159^2 + 7920^2 = 8209^2$$

To get <u>all</u> Pythagorean Triples, just scale these

Theorem: Every Pyth. Triple $a^2+b^2=c^2$ has the form

$$(a,b,c) = (k(n^2-m^2),\ k2mn,\ k(n^2+m^2))$$

for some integers k, m, n. (And every triple of this form is Pythagorean.)

Euclid knew this (Prop X.29), but he didn't know about rational points on a circle (Why?).

The "parametrization" of rational $x^2+y^2=1$

by $$x = \frac{1-\alpha^2}{1+\alpha^2}, \quad y = \frac{2\alpha}{1+\alpha^2}$$

was discovered by Diophantus of Alexandria ~ 250 AD in his "Arithmetica" (of 13 books, only 6 have survived).

Thinking Homework:

Find all the rational points on $x^2+y^2=3$

Wed Sept 26.

Exam 1 Average 16.8 /20.
Median 18.5
(Ave. too high to assign grades ☹)
≥10 is a pass.

(Compare Euclid ~300BC)

Recall: Diophantus of Alexandria ~250AD knew the following in some form.

∃ bijection between rational numbers and rational points on the unit circle (minus one special point).

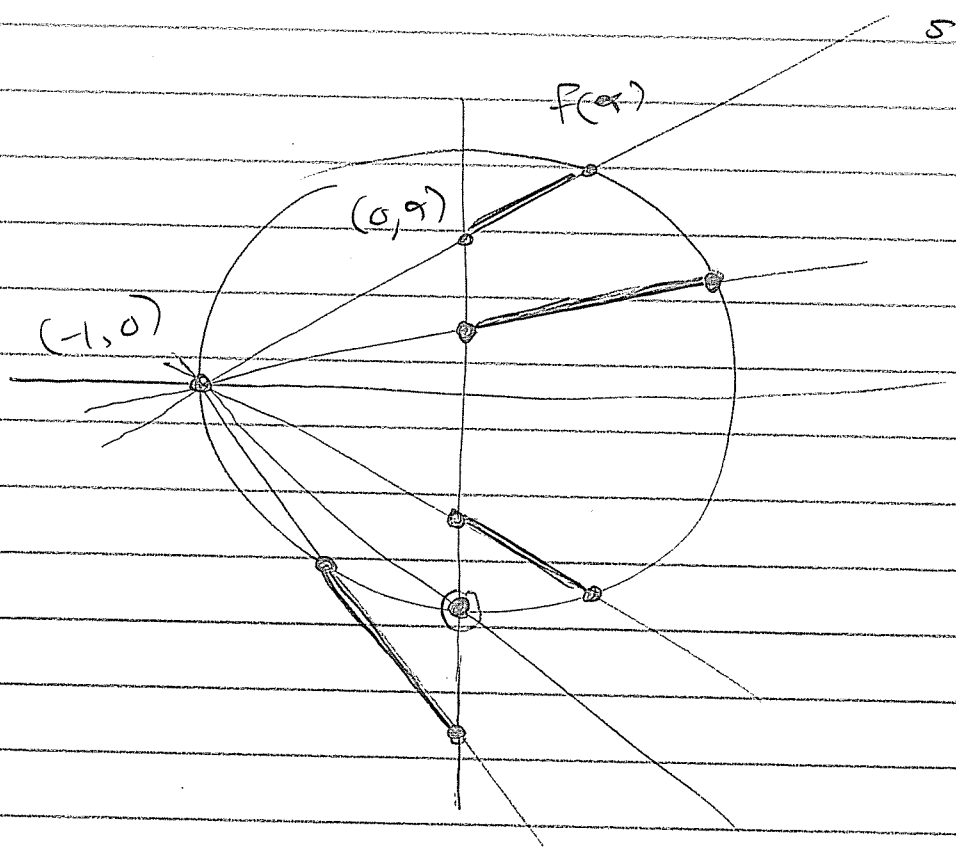
set of rational numbers $\mathbb{Q}$ $\longrightarrow$ $\{(x,y)\in\mathbb{Q}^2 : x^2+y^2=1\} - \{(-1,0)\}$.

Defined by $f(\alpha) := \left(\frac{1-\alpha^2}{1+\alpha^2}, \frac{2\alpha}{1+\alpha^2}\right)$.

We showed this function is invertible with inverse

$$f^{-1}(X,Y) = \frac{Y}{X+1}.$$

Modern (Cartesian) Picture:



Think of y-axis as $\mathbb{Q}$

$(0,\alpha) \longleftrightarrow \alpha$

Diophantus used this to classify "Pythagorean Triples"

$(a,b,c) \in \mathbb{Z}^3$ with $a^2 + b^2 = c^2$

Then Alexandria fell.
- the library was destroyed
- Hypatia was murdered.

⋮

people forgot

⋮

(13 books)

6 books of Diophantus' "Arithmetica" survived. Bachet's edition was published in 1621.

Enter Pierre de Fermat.

Quote: "perhaps posterity will thank me for having shown it that the ancients did not know everything"

Theorem (Fermat): There are NO rational points on the circle $x^2+y^2=3$.

Proof?

Suppose that there is a rational point. Take common denominators to write

$$\left(\frac{A}{C}\right)^2 + \left(\frac{B}{C}\right)^2 = 3$$

$$A^2 + B^2 = 3C^2 \qquad (*)$$

for some integers A, B, C.

$(*)$ implies that A and B are both multiples of 3. (Why? There are four cases.)

So let $A = 3a$ and $B = 3b$. Then

$$(3a)^2 + (3b)^2 = 3C^2$$
$$9a^2 + 9b^2 = 3C^2$$
$$3a^2 + 3b^2 = C^2$$
$$3(a^2 + b^2) = C^2$$

Hence C^2 (and also C) is a multiple of 3. Say $C = 3c$. Then

$$A^2 + B^2 = 3C^2$$
$$(3a)^2 + (3b)^2 = 3(3c)^2$$
$$9a^2 + 9b^2 = 27c^2$$
$$a^2 + b^2 = 3c^2$$

So what?

If (A, B, C) is an integer solution to $A^2 + B^2 = 3C^2$, then so is

$$(a, b, c) = \left(\frac{A}{3}, \frac{B}{3}, \frac{C}{3}\right).$$

Repeat: Then we get another solution

$$(a', b', c') = \left(\frac{a}{3}, \frac{b}{3}, \frac{c}{3}\right).$$

Repeat ... Wait, this is impossible.
CONTRADICTION

///

This is called Fermat's method of "infinite descent".

He used it to prove that many "Diophantine equations" have NO solution

1670 : Pierre's son published an edition of Arithmetica with comments by Pierre. In it Fermat claimed that

$x^n + y^n = z^n$ has NO integer solution when $n \geq 3$.

"I have discovered a truly marvelous proof of this, which this margin is too narrow to contain"

OOPS !

Andrew Wiles proved it in 1995

Fri Sept 8

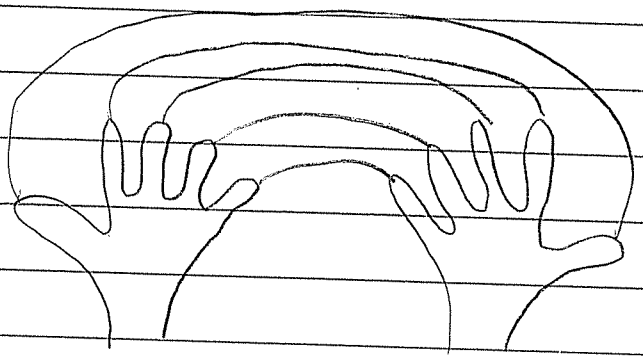
Today: The definition of $\mathbb{Z}$

Q: What is a "number"?
(The Greeks tried and failed to answer this.)

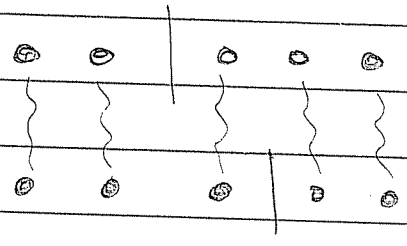
Step 1: A "number" is a quantity of discrete things (e.g. pebbles on a beach).

Two collections of things have the same "number" if $\exists$ a bijection between them.

eg.



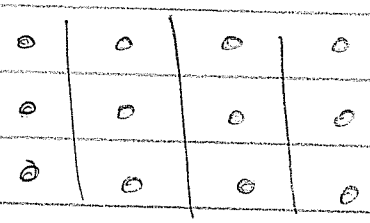
"Numbers" can be added and multiplied



$2+3=5$

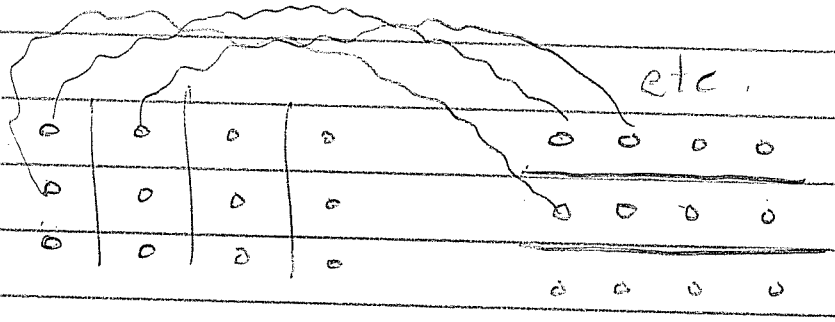
$3+2=5$

Theorem: Addition is commutative!

Next:  $4 \times 3 = 12$

Is $\times$ commutative? Yes!

Proof: $\exists$ bijection



$4 \times 3 = 3 \times 4$

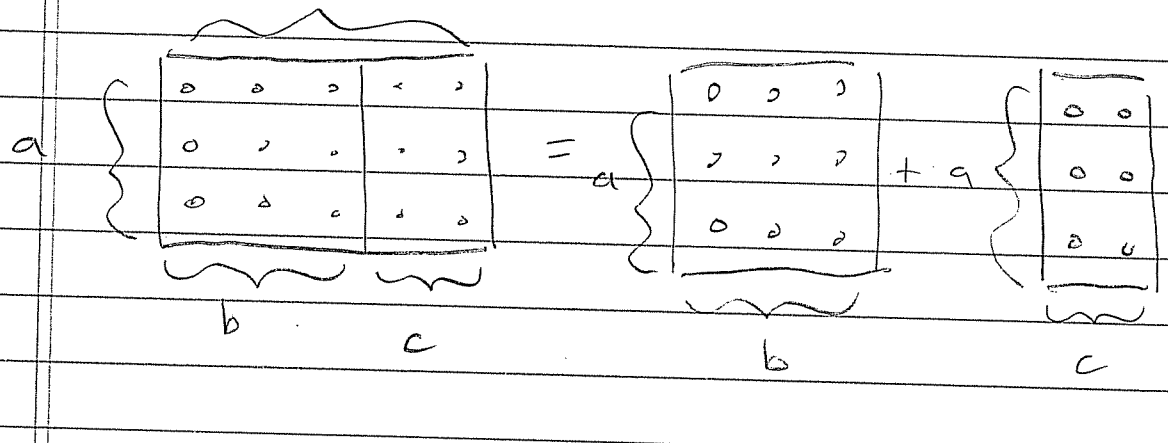
(Did you realize this needs a proof?)

Next: How do $+$ and $\times$ interact?

Answer: They "distribute"

$$a \times (b + c) = a \times b + a \times c$$

Proof:



Thus we can "define" the "natural numbers"
(the "counting numbers")

$$\mathbb{N} := \{1, 2, 3, \ldots\}$$

with commutative & distributive $+, \times$.

Q: Would a Martian Know this too?

Leopold Kronecker (1823 – 1891) thought so.

Quote: "God made $\mathbb{N}$; all else
is the work of man."

(Do you agree?
Compare Euclid.)

Issues:
- What about zero?
- What about subtraction?
- What about order/comparison? (e.g. $5 < 23$)

These are much harder. Over time, our idea of "number" evolved into

The Integers $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

SEE THE HANDOUT.
- There are 12 Axioms!
- The first 11 are "obvious", but they can't distinguish between $\mathbb{Z}$ and $\mathbb{R}$.

Q: So what is the difference between $\mathbb{Z}$ and $\mathbb{R}$?
- This is a subtle question, and it leads to the final Axiom

✡ The Well-Ordering Axiom ✡

Every non-empty subset of $\mathbb{N}$ has a smallest element.

Formally:

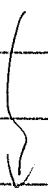
$$\forall X \subseteq \mathbb{N}, X \neq \emptyset, \exists a \in X, \forall b \in X, a \leq b.$$

"For all subsets X of $\mathbb{N}$ such that X is not empty, there exists a number a in X such that for all numbers b in X we have $a \leq b$."

(Exercise: Show that $\mathbb{R}$ is not well-ordered.)

First Application.

Theorem: There are no uninteresting natural numbers.



Proof: Suppose for contradiction that there is an uninteresting natural number and let $X \subseteq \mathbb{N}$ be the set of such. Since by assumption $X \neq \emptyset$, the Well-Ordering Axiom says that X has a smallest element, say $a \in X$. But then a is the "smallest uninteresting number", which is interesting, contradicting the fact that $a \in X$.

(I learned this proof from the audio commentary on a "Futurama" DVD.)

Mon Oct 1

HW 3 due Fri Oct 12.

Today: Subtraction and Division.

I gave you a definition of $\mathbb{Z}$ but it only defines $+$ and $\times$. What about $-$ and $\div$?

Axioms of Addition:

(A1) $\forall a, b \in \mathbb{Z}$, $a+b = b+a$.
(A2) $\forall a, b, c \in \mathbb{Z}$, $a+(b+c) = (a+b)+c$.
(A3) $\exists$ "0" $\in \mathbb{Z}$, $\forall a \in \mathbb{Z}$, $0+a = a$.
(A4) $\forall a \in \mathbb{Z}$, $\exists b \in \mathbb{Z}$, $a+b = 0$.

A4 Says: For all $a \in \mathbb{Z}$ there is some $b \in \mathbb{Z}$ such that $a+b = 0$

Theorem: This b is unique. It is called THE additive inverse of a.

Proof: Suppose that there are two, say

$$a+b_1 = 0 = a+b_2.$$

Then we have

$$\begin{aligned} b_1 &= 0 + b_1 && \text{(A3)} \\ &= b_1 + 0 && \text{(A1)} \\ &= b_1 + (a + b_2) && \text{assumption} \\ &= (b_1 + a) + b_2 && \text{(A2)} \\ &= (a + b_1) + b_2 && \text{(A1)} \\ &= 0 + b_2 && \text{assumption} \\ &= b_2 \end{aligned}$$

Definition: Given $a \in \mathbb{Z}$ let "$-a$" denote THE additive inverse of a.

Then we can define **subtraction**. For all $a, b \in \mathbb{Z}$, let

$$\text{"}a - b\text{"} := a + (-b)$$

Q: How does subtraction interact with multiplication?

See HW 3.4

What about division?

Unfortunately, multiplication of integers is not invertible.

$\nexists\ n \in \mathbb{Z}$ such that $2n = 1$ ☹

But we can still say something useful.

Theorem (The Division Algorithm 2.12):

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

$$a = q \cdot b + r \quad \text{and} \quad 0 \leq r < b$$

↑ "quotient" ↑ "remainder"

e.g.

$15 = 2 \cdot 6 + 3$ ✓

$15 = 3 \cdot 6 - 3$ ✗

We need $0 \leq r < b$ for uniqueness.

↓

eg. $30 = 5 \cdot 6 + 0$.

If the remainder is 0 we say "b divides a" and we write $b \mid a$.

DEF: Given $a, b \in \mathbb{Z}$, the symbol $b \mid a$ means $\exists k \in \mathbb{Z}$ with $a = bk$. (it's an existence statement).

eg. $-10 = (-2) \cdot 6 + 2$. ✓

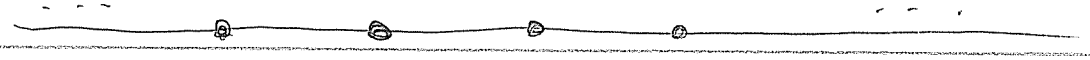
Quotient can be negative
Remainders can't.

Try to prove the Theorem.

It's easy to find $q, r \in \mathbb{Z}$ with $a = qb + r$, but mayke harder to find $0 \leq r < b$.

Idea: Given $a, b \in \mathbb{Z}$ with $b > 0$, consider the infinite set

$S = \{ \ldots, a-b, a, a+b, a+2b, \ldots \}$



What do we want?

If $r = a - qb$ then $a = qb + r$ ✓
So we want to find q such that
$r = a - qb$ is small and nonnegative.

Let $S^+ = \{ n \in S : n \geq 0 \}$.

By Well-Ordering, S^+ has a smallest element call it $r = a - qb$.

Clearly $0 \in r$.
We need to show that $r < b$

Suppose for contradiction that $b \leq r$,
and subtract b to get $0 \leq r - b < r$

But this is a contradiction because.
$r - b = a - qb - b = a - (q+1)b \in S^+$
and r was assumed to be smallest
in S^+.

Hence $0 \leq r < b$.

Summary: Given $a, b \in \mathbb{Z}$, $b > 0$,

Well-ordering $\Rightarrow \exists\, q, r \in \mathbb{Z}$ with

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

Are these q, r unique?