Mon Oct 7

The study of mathematics is CUMULATIVE. Now we will see an example of this by building a major theorem from the ground up.

The theorem is the following.

Unique Factorization Theorem 2.54 (A.K.A. The Fundamental Theorem of Arithmetic):

Every $0 \neq n \in \mathbb{Z}$ can be expressed as

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1, p_2, \ldots, p_k$ are primes with exponents $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$.

And this expression is UNIQUE.

First, what is a prime?

Def: Given $p \in \mathbb{N}$ with $p > 1$, we say that p is prime if

$$\forall a \in \mathbb{N},\ a \mid p \Rightarrow a = 1 \text{ or } p.$$

(We say p has no nontrivial divisors)

If $n \in \mathbb{N}$ is not prime we say it is composite. i.e.

$$\exists\, a \in \mathbb{Z},\ a \mid p \text{ and } 1 < a < p.$$

(We say n has a nontrivial divisor) ///

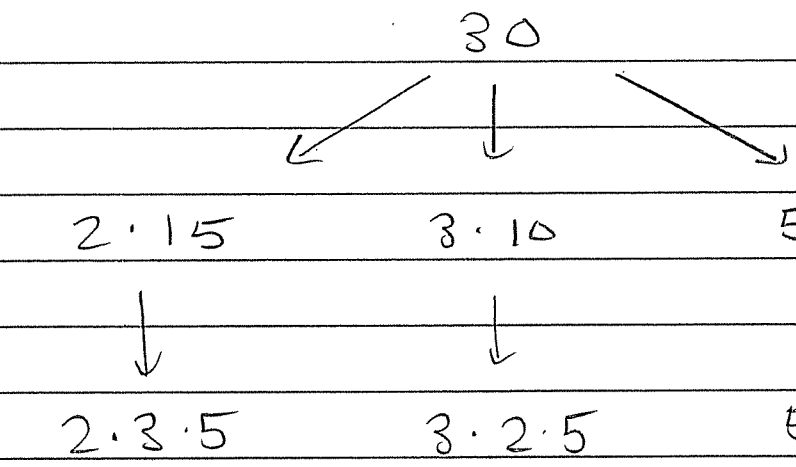
Example: The first primes are

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

The number 30 is composite.

Let's factor it!

↓



We got the same final answer no matter how we factored 30.
That's called

UNIQUE PRIME FACTORIZATION.

$30 = 2 \cdot 3 \cdot 5 = 2 \cdot 5 \cdot 3 = 3 \cdot 2 \cdot 5$
$= 3 \cdot 5 \cdot 2 = 5 \cdot 2 \cdot 3 = 5 \cdot 3 \cdot 2$

order doesn't matter.

Note: It didn't have to be this way.

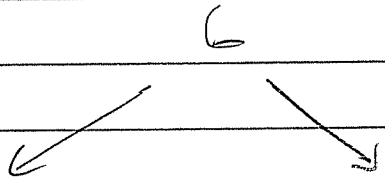
∃ number systems without unique factorization.

↓

Example: Consider the number system

$$\mathbb{Z}[\sqrt{-5}] := \{ a + b\sqrt{-5} : a, b \in \mathbb{Z} \}.$$

Then try to factor $6 \in \mathbb{Z}[\sqrt{-5}]$:



$2 \cdot 3$ $\qquad$ $(1+\sqrt{-5})(1-\sqrt{-5})$

↓ ? $\qquad$ ↓ ?

can't be factored further !

So $6 \in \mathbb{Z}[\sqrt{-5}]$ has two different prime factorizations

Our goal is to prove that $\mathbb{Z}$ has unique factorization

Our tool is the concept of

gcd = greatest common divisor

Def: Given integers $a, b \in \mathbb{Z}$, not both zero, consider the set of common divisors

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

Example:

$$\text{Div}(18,30) = \{-6,-3,-2,-1,1,2,3,6\}$$

We define $\gcd(a,b)$ to be the highest element of $\text{Div}(a,b)$

$$\gcd(a,b) := \max \text{Div}(a,b)$$

Example: $\gcd(18,30) = 6$

Q: Why does $\text{Div}(a,b)$ have a highest element?

A: Note that $\text{Div}(a,b)$ is bounded above by $\min\{|a|,|b|\}$. Indeed, let $d \in \text{Div}(a,b)$.

Then $d|a \Rightarrow d \leq |d| \leq |a|$
and $d|b \Rightarrow d \leq |d| \leq |b|$

hence $d \leq \min\{|a|, |b|\}$. ///

Since $Div(a,b)$ is bounded above, it has a highest element by Well-Ordering.

This is true for subsets of $\mathbb{Z}$, but not subsets of $\mathbb{R}$.

Example: Consider the open interval

$(0,1) := \{x \in \mathbb{R} : 0 < x < 1\}$.

Then $(0,1)$ is bounded above (by 1) but it has no highest element

Proof: Assume $(0,1)$ does have a highest element, say $x \in (0,1)$.

But then $(1+x)/2$ is higher:

$$x < \frac{1+x}{2} < 1.$$

Contradiction. ///

So $\sqrt{2}$ and π have no greatest common divisor.

But for all $a, b \in \mathbb{Z}$, not both zero,

$\gcd(a, b)$ exists.

Q: How to compute it?

$\gcd(1053, 481) = ?$

Wed Oct 9

HW 3 due Wed Oct 23
NO CLASS Fri Oct 18 (Fall Break)
NO CLASS Fri Oct 25 (I'm out of town)

Exam 1 statistics

Total 20	A ≈ 13 – 19.5	(9)
Average 11.8	B ≈ 9.5 – 12	(8)
Median 11	C ≈ 6 – 8.5	(8)
St. Dev 4		

Where were we?

Given $a, b \in \mathbb{Z}$ not both 0, consider the set of common divisors

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

Then define the greatest common divisor

$$gcd(a,b) := \max Div(a,b)$$

Example:

$$Div(12,18) = \{-6,-3,-2,-1,1,2,3,6\}$$

gcd

Problem: Compute $\gcd(1053, 481)$.

Two Methods.

(1) Bad Method. (Slow)

For all d from 1 to 481, test if $d \mid 1053$ and $d \mid 481$.
Report the largest such d.

(2) Good Method (Fast).

This method depends on a trick.

☆ Proposition 2.21.

Given $a, b, q, r \in \mathbb{Z}$ with $a = qb + r$ we have that

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

To prove this we will show an equality of sets

$$Div(a,b) = Div(b,r).$$

It will then follow that

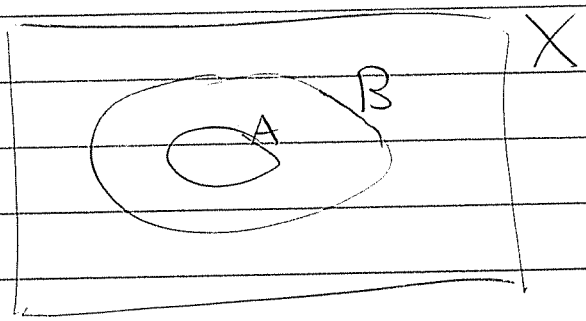
$$\gcd(a,b) = \max Div(a,b) = \max Div(b,r) = \gcd(b,r).$$

How can we show that two sets are equal?

Let X be a set and consider two subsets $A, B \subseteq X$.

What does it mean to say that "$A \subseteq B$"

Picture:



Formally:

"$A \subseteq B$" $\equiv$ "$\forall x \in X,\ x \in A \Rightarrow x \in B$"

To prove that "$A \subseteq B$":

Consider an arbitrary element $x \in A$.
Show that x is also in B.

The statement "$A = B$" means exactly

"$A = B$" $\equiv$ "$(A \subseteq B)$ AND $(B \subseteq A)$"

$\equiv$ "$\forall x \in X,\ x \in A \Leftrightarrow x \in B$".

To prove "$A = B$" there are two steps.

i) Prove $A \subseteq B$.
ii) Prove $B \subseteq B$.

(Just like proving $\Leftrightarrow$).

Proof of Prop 2.21:

Let $a = qb + r$. We will prove that $\mathrm{Div}(a,b) = \mathrm{Div}(b,r)$ and it follows that $\gcd(a,b) = \gcd(b,r)$.

First we show $\mathrm{Div}(a,b) \subseteq \mathrm{Div}(b,r)$.
So assume $d \in \mathrm{Div}(a,b)$, i.e., $a = da'$ and $b = db'$ for some $a', b' \in \mathbb{Z}$.
Then we have

$$r = a - qb = da' - qdb' = d(a' - qb'),$$

hence $d \mid r$. It follows that $d \in \mathrm{Div}(b,r)$. //

Next we show $\mathrm{Div}(b,r) \subseteq \mathrm{Div}(a,b)$.
So assume $d \in \mathrm{Div}(b,r)$, i.e., $b = db'$ and $r = dr'$ for some $b', r' \in \mathbb{Z}$.
Then we have

$$a = qb + r = qdb' + dr' = d(qb' + r'),$$

hence $d \mid a$. It follows that $d \in \mathrm{Div}(a,b)$.

Let's apply the trick to compute gcd(1053, 481).

First divide 1053 by 481:

$$1053 = 2 \cdot 481 + 91 \qquad \gcd(1053, 481) = \gcd(481, 91)$$

$$481 = 5 \cdot 91 + 26 \qquad = \gcd(91, 26)$$

$$91 = 3 \cdot 26 + 13 \qquad = \gcd(26, 13)$$

$$26 = 2 \cdot 13 + 0 \qquad = \gcd(13, 0)$$

Hence

$$\gcd(1053, 481) = \gcd(13, 0) = 13$$

That was <u>much</u> faster than the Bad Method.

Bad Method	Good method
2×481 divisons	4 divisions

This Good Method is called

"The Euclidean Algorithm"

Theorem 2.22:
To compute $\gcd(a,b)$ for $a,b \in \mathbb{Z}$ with $b \neq 0$, divide a by b. Then repeat:

$$a = q_1 b + r_1, \quad 0 \leq r_1 < |b|$$
$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2$$
$$\vdots$$

we obtain a sequence of remainders

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

By Well-Ordering $\exists\, n$ such that

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

Claim: $\gcd(a,b) = r_{n-1}$

(last nonzero remainder).

Proof: By the trick (Prop 2.21) we have

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

$r_n = 0$

Fri Oct 11

HW 3 due Wed Oct 23
NO CLASS Fri Oct 18 (Fall Break)
NO CLASS Fri Oct 25 (I'm out of town)

Recall Prop 2.21:

Given $a, b, q, r \in \mathbb{Z}$ with $a = qb + r$ we have

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

Recall The Euclidean Algorithm 2.22:

Consider $a, b \in \mathbb{Z}$ with $b \neq 0$. To compute $\gcd(a, b)$, first divide a by b. Then repeat.

$$a = q_1 b + r_1 \quad , \quad 0 \leq r_1 < |b|$$
$$b = q_2 r_1 + r_2 \quad , \quad 0 \leq r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3 \quad , \quad 0 \leq r_3 < r_2$$
$$\vdots$$

etc.

We obtain a sequence of remainders

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

By Well-Ordering, $\exists\, n \in \mathbb{N}$ such that

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

Claim: $\gcd(a,b) = r_{n-1}$
= last nonzero remainder.

Proof: By Prop 2.21 we have

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

Remark: The Euclidean Algorithm is FAST. Given $0 < a < b$, we could compute $\gcd(a,b)$ as follows:

For all d from 1 to a check if:

$$d \mid a \quad \text{and} \quad d \mid b$$

Report the largest such d. This process will require

$2 \times a$ divisions with remainder.

By contrast, computing $\gcd(a, b)$ with the Euclidean Algorithm takes

$< 2 \cdot \log_2(a)$ divisions with remainder.

(Proof omitted).

Brute Force	Euclidean Algorithm
$2a$ ☹	$2 \cdot \log_2(a)$ ☺

Example: Compute $\gcd(21, 13)$.
It will take $< 2 \cdot \log_2(13) \approx 7.4$ steps.

$21 = 1 \cdot 13 + 8$
$13 = 1 \cdot 8 + 5$
$8 = 1 \cdot 5 + 3$
$5 = 1 \cdot 3 + 2$
$3 = 1 \cdot 2 + (1)$
$2 = 2 \cdot 1 + 0$ ↓

$\gcd(21, 13) = 1$

Definition: When $\gcd(a,b) = 1$ we say that a and b are coprime (or relatively prime).

Example: 21 & 13 are coprime.

Closely related problem:

Given $a, b, c \in \mathbb{Z}$ find all solutions $x, y \in \mathbb{Z}$ to the linear equation

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

Note: If $d = \gcd(a,b)$, then $a = da'$ and $b = db'$ for some a', b', hence

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

$\Longrightarrow d \mid c$.

$\Longrightarrow (*)$ has NO SOLUTION unless

$$\gcd(a,b) \mid c$$

For simplicity, assume $c = d := \gcd(a,b)$.
Find all solutions $x, y \in \mathbb{Z}$ to the equation

$$ax + by = d.$$

Eg. $21x + 13y = 1$.

How?

Idea: Use the Euclidean Algorithm.

Start with two easy equations

$$21 \cdot 1 + 13 \cdot 0 = 21 \quad (1)$$
$$21 \cdot 0 + 13 \cdot 1 = 13 \quad (2)$$

Combine to make more true equations

$$21 \cdot 1 + 13 \cdot (-1) = 8 \quad (3) = (1) - (2)$$
$$21(-1) + 13(2) = 5 \quad (4) = (2) - (3)$$
$$21(2) + 13(-3) = 3 \quad (5) = (3) - (4)$$
$$21(-3) + 13(5) = 2 \quad (6) = (4) - (5)$$
$$21(5) + 13(-8) = 1 \quad (7) = (5) - (6)$$
$$21(-13) + 13(21) = 0 \quad (8) = (6) - 2(7)$$

What did we find?

$$21(5) + 13(-8) = 1$$

is a solution ✓

Are there other solutions? Yes! Note that equation (1) + k(8) is true for all $k \in \mathbb{Z}$.

$$\begin{array}{l} [21(5) + 13(-8) = 1] \\ +k[21(-13) + 13(21) = 0] \end{array}$$

$$21(5 - 13k) + 13(-8 + 21k) = 1 + 0k$$

we get infinitely many solutions

Claim: This is the complete solution.

Proof: Postponed.

Now solve the more general problem

$$21x + 13y = c.$$

Take the solution

$$21(5 - 13k) + 13(-8 + 21k) = 1$$

and multiply both sides by c:

$$21\left[c(5 - 13k)\right] + 13\left[c(-8 + 21k)\right] = c$$

The general solution is

$$x = c(5 - 13k)$$

$$y = c(-8 + 21k)$$

$\forall\, k \in \mathbb{Z}$.

★ Today's office hours 1:30 – 2:30

NO CLASS this Friday Oct 18

HW 3 due Wed Oct 23

NO CLASS next Fri Oct 25

Where were we?

Find all solutions $x, y, z \in \mathbb{Z}$ to the equation

$$3094x + 2513y = z$$

First compute $\gcd(3094, 2513)$ using the Euclidean Algorithm:

$$3094 = 1 \cdot 2513 + 581 \qquad = \gcd(3094, 2513)$$
$$2513 = 4 \cdot 581 + 189 \qquad = \gcd(2513, 581)$$
$$581 = 3 \cdot 189 + 14 \qquad = \gcd(581, 189)$$
$$189 = 13 \cdot 14 + 7 \qquad = \gcd(189, 14)$$
$$14 = 2 \cdot 7 + 0 \qquad = \gcd(14, 7)$$
$$= \gcd(7, 0)$$
$$= 7.$$

$$\gcd(3094, 2513) = 7$$

If $\exists\ x,y,z \in \mathbb{Z}$ with

$$3094x + 2513y = z.$$

Then $7 \mid$ left side $\Rightarrow 7 \mid z$.

By contrapositive, if $7 \nmid z$ then

there is NO SOLUTION $x,y,z \in \mathbb{Z}$.

So let's try to solve

$$3094x + 2513y = 7c$$

We use the

"Extended Euclidean Algorithm" 2.25

Start with two easy equations

$$3094 \cdot 1 + 2513 \cdot 0 = 3094 \quad (1)$$
$$3094 \cdot 0 + 2513 \cdot 1 = 2513 \quad (2)$$

To save ink, just write the coefficients:

1	0	3094	①
0	1	2513	②.

Now combine these to get new equations

1	0	3094	①
0	1	2513	②
1	-1	581	③ = ① - 1②
-4	5	189	④ = ② - 4③
13	-16	14	⑤ = ③ - 3④
-173	213	7	⑥ = ④ - 13⑤
359	-442	0	⑦ = ⑤ - 2⑥

The last two equations are the key.

$3094(-173) + 2513(213) = 7$ ⑥

$3094(359) + 2513(-442) = 0$ ⑦

Combine them: ⑥ + k⑦.

$$3094(-173 + 359k) + 2513(213 - 442k) = 7 + 0 \cdot k$$

infinitely many solutions

Finally, multiply both sides by c:

$$3094\underbrace{\left[c(-173+359k)\right]}_{x} + 2513\underbrace{\left[c(213-442k)\right]}_{y} = \underbrace{7c}_{z}.$$

This is the complete solution to

$$3094x + 2513y = z.$$

$$\left.\begin{aligned} x &= c(-173+359k) \\ y &= c(213-442k) \\ z &= 7c \end{aligned}\right\} \forall\, k, c \in \mathbb{Z}$$

Why did we do this?

We have a theoretical reason.

Theorem (Bézout's Identity):

Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. Then $\exists\, x, y \in \mathbb{Z}$ such that

$$ax + by = d.$$

Proof: We can use the Extended Euclidean Algorithm to find such $x, y \in \mathbb{Z}$. (They are not unique.)

Now let $a, b \in \mathbb{Z}$ (not both zero) and consider the set of $\mathbb{Z}$-linear combinations

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

Let $d = \gcd(a, b)$ and consider the set

$$d\mathbb{Z} := \{dz : z \in \mathbb{Z}\} \leq \mathbb{Z}.$$

Corollary (Characterization of GCD):

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

Proof: First show $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$.
Consider any $ax + by \in a\mathbb{Z} + b\mathbb{Z}$.
Since $d \mid a$ and $d \mid b$ we have
$a = da'$ and $b = db'$ for some $a', b' \in \mathbb{Z}$.
Then

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

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

Next show $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$.

Consider any $dz \in d\mathbb{Z}$. By Bézout's Identity $\exists\ x, y \in \mathbb{Z}$ such that

$$d = ax + by.$$

$$\Rightarrow dz = (ax + by)z$$
$$= a(xz) + b(yz) \in a\mathbb{Z} + b\mathbb{Z}.$$

$$\Rightarrow d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}.$$ ▨

In words:

$\gcd(a, b)$ is the smallest positive $\mathbb{Z}$-linear combination of a & b.

wed Oct 16

NO CLASS Friday
HW 3 due next Wed Oct 23
NO CLASS next Fri Oct 25

Recall the Characterization of GCD:

Given $a, b \in \mathbb{Z}$ not both zero, consider the set of linear combinations

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

Theorem: This set has a simpler description

$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\,\mathbb{Z}$$

$$= \{\gcd(a,b) \cdot k : k \in \mathbb{Z}\}$$

Example

$$14\mathbb{Z} + 26\mathbb{Z} = 2\mathbb{Z}$$

$$= \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}.$$

Today we will consider prime factorization.

Theorem: Every $n \in \mathbb{Z}$, $n \geq 2$, has a prime factor.

Proof by Contradiction:

Suppose the statement is false and let

$$S := \{ n \geq 2 : n \text{ has no prime factor} \}$$

By assumption $S \neq \emptyset$ hence by Well-Ordering $\exists$ smallest element, say $m \in S$.

[Remark: m is a "minimal criminal"]

Since $m \in S$, m is not prime (since otherwise m is a prime factor of itself).
By definition this means $\exists$ $a, b \in \mathbb{Z}$ such that

$$m = ab \quad \text{and} \quad 1 < a, b < m.$$

Since $a < m \Rightarrow a \notin S$, we know that a does have a prime factor,

Say $a = pk$ where p is prime. But then

$$m = ab = pkb = p(kb)$$

$\Rightarrow$ m has a prime factor, contradicting the fact that $m \in S$ ▨

Theorem: Every $n \in \mathbb{Z}$, $n \geq 2$, can be written as a product of primes

Proof by contradiction:

Assume the statement is false. Then by Well-Ordering there exists a smallest $m \geq 2$ with no prime factorization.

This m is not prime, but it has a prime factor by the previous Theorem, say $m = pk$ where $1 < k < m$.

Since m was minimal we know that k has a prime factorization, say

$$k = p_1 p_2 \cdots p_r$$

But then m has a prime factorization

$$m = p\, p_1 p_2 \cdots p_r.$$

Contradiction. 

Corollary: Every $n \in \mathbb{Z}$, $n \neq 0$, can be written as a product of primes (times ± 1).

Example:

- 1 is not prime, but it is 1 times a product of primes (i.e. no primes)
- if $n < 0$ then $-n > 0$ is 1 times a product of primes.

$$n = (-1) \cdot \text{product of primes}$$

- $364 = 2 \cdot 2 \cdot 7 \cdot 13$
  $= 2 \cdot (-2) \cdot (-7) \cdot 13$
  $= (-2) \cdot (-2) \cdot (-7) \cdot (-13)$

  etc.

- $-8 = (-1)\cdot 2\cdot 2\cdot 2$
  $= (-2)(-2)(-2)$
  $= 2(-2)\,2$
  etc.

Don't worry about ± 1 !

We know prime factorizations EXIST.
Are they UNIQUE ?

We need one final tool.

Theorem 2.53 ("Euclid's Lemma"):

Let p be prime. Then $\forall\, a, b \in \mathbb{Z}$,

$$p \mid ab \implies p \mid a \text{ OR } p \mid b$$

Proof: We will prove the equivalent statement:

$$p \mid ab \text{ AND } p \nmid a \implies p \mid b.$$

So assume $p \mid ab$, say $ab = pk$, and assume that $p \nmid a$. Then we have $\gcd(a, p) = 1$ (Why?)

By Bézout's Identity $\exists\, x, y \in \mathbb{Z}$ such that $1 = ax + py$. Multiplying both sides by b gives

$$b = abx + pby.$$

$$= pkx + pby$$

$$= p(kx + by).$$

Hence $p \mid b$, as desired ▨

Multiplying both sides of $1 = ax + py$ by b was a "trick" (an "uphill step" in the proof), and it worked!

Mon Oct 21

HW 3 due Wed

NO CLASS Friday

Recap:

- $\gcd(a,b) := \max \mathrm{Div}(a,b)$, where

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

- If $a = qb + r$ with $b \neq 0$ then

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

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

- This + Division Algorithm = The Euclidean Algorithm. It allows us to compute $\gcd(a,b)$ quickly.

- Moreover, the Extended Euclidean Algorithm allows us to solve the equation

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

for $x, y \in \mathbb{Z}$.

- Then we can characterize the GCD in a nice way:

$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$$

- We say $p \in \mathbb{Z}$ is prime if $\forall a, b \in \mathbb{Z}$

$$p = ab \implies a = \pm 1 \text{ OR } b = \pm 1$$

- We say $n \in \mathbb{Z}$ is composite if it is not prime, i.e. $\exists\ a, b \in \mathbb{Z}$ with

$$a, b \neq \pm 1 \quad \text{AND} \quad n = ab.$$

[we say these a, b are proper factors of n]
(or nontrivial factors)

- We used well-ordering to show that $\forall n \in \mathbb{Z}$, $n \neq 0$, we have an expression

$$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1, p_2, \ldots, p_k$ are prime.

Q: Is this expression unique?

A: How could it not be?

Here is the key point:

☆ Theorem 2.53 ("Euclid's Lemma")
(Book VII Prop 30 in Euclid):

Let $p \in \mathbb{Z}$ be prime. Then $\forall\, a, b \in \mathbb{Z}$ we have

$$\boxed{p \mid ab \implies p \mid a \text{ OR } p \mid b.}$$

[Note: This fails for non-prime p.
Eg. $p = 4$. We have

$4 \mid 12 = 2 \cdot 6$ BUT $4 \nmid 2$ AND $4 \nmid 6$.]

We will prove the equivalent statement

$p \mid ab$ AND $p \nmid a \implies p \mid b$.

[Recall:

"$P \Rightarrow (Q \text{ OR } R)$" $\equiv$ "$(P \text{ AND NOT } Q) \Rightarrow R$"]

Proof: Let $p \in \mathbb{Z}$ be prime. Suppose that $p \mid ab$, say $ab = pk$, and suppose that $p \nmid a$.

Let $d = \gcd(a, p)$. Since $d \mid p$ we have $d = 1$ or $d = p$. But since $d \mid a$ and $p \nmid a$ we conclude $d = 1$.

By Bézout's identity $\exists\, x, y \in \mathbb{Z}$ such that

$$1 = ax + py.$$

Now multiply both sides by b to get

$$\begin{aligned} b &= b(ax + py) \\ &= bax + bpy \\ &= abx + pby \\ &= pkx + pby \\ &= p(kx + by). \end{aligned}$$

Hence $p \mid b$, as desired. ∎

More Generally: Let p be prime.

If $p \mid a_1 a_2 \cdots a_k$ then $p \mid a_i$ for some i.

[How would you prove this?]

Now we have everything we need to prove unique prime factorization.

☆ Unique Factorization Theorem 2.54 ("Fundamental Theorem of Arithmetic"):

Every integer $n \neq 0$ has a unique expression as a product of primes (apart from reordering and negative signs)

Proof Idea: Suppose n can be expressed

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

where $p_1, \ldots, p_k, q_1, \ldots, q_l$ are prime.

Since $p_1 \mid n$ we have

$$p_1 \mid q_1 q_2 \cdots q_l$$

Since p_1 is prime, Euclid's Lemma says that we have $p_1 \mid q_i$ for some i. Since p_1 and q_i are both prime, this implies $p_1 = \pm q_i$

Cancel the common factor from both sides to get

$$p_2 p_3 \cdots p_k = \pm (q_1 \cdots q_{i-1} q_{i+1} \cdots q_\ell)$$

Now repeat until you're done...

Is that a proof? NOT REALLY

Formal Proof:

Suppose $\exists$ integer $\neq 0$ with two different prime factorizations. By Well-Ordering, let m be the smallest such integer and write

$$m = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell \quad (*)$$

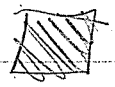
Different in some nontrivial way.

Since $p_1 | m$ we have $p_1 | q_1 q_2 \cdots q_l$ and Euclid's Lemma $\Rightarrow p_1 | q_i$ for some i. Since p_1, q_i are prime this implies that $p_1 = \pm q_i$

Cancel p_1 from (*) to get

$$m' = \underbrace{p_2 p_3 \cdots p_k}_{\text{still different}} = \pm q_1 \cdots q_{i-1} q_{i+1} \cdots q_l$$

with $|m'| < |m|$. But this contradicts the fact that m was minimal



Remarks:

- We skipped some details, didn't we?
- Did we skip anything important?
- Would adding details make the proof better, or worse?

Wed Oct 23

HW 3 is due NOW.
NO CLASS Friday

Let's look at HW 3 Problem 3:

What is a fraction?

Given $a, b \in \mathbb{Z}$ with $b \neq 0$ we define an abstract symbol:

$$\text{“}\frac{a}{b}\text{”}$$

We declare rules for "multiplying" and "adding" abstract symbols:

$$\text{“}\frac{a}{b}\text{”} \cdot \text{“}\frac{c}{d}\text{”} := \text{“}\frac{ac}{bd}\text{”}$$

$$\text{“}\frac{a}{b}\text{”} + \text{“}\frac{c}{d}\text{”} := \text{“}\frac{ad+bc}{bd}\text{”}$$

We declare when two abstract symbols are "equal":

"$\frac{a}{b}$" = "$\frac{c}{d}$" $\iff$ $ad = bc$.

Definition: The set

$$\mathbb{Q} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

is called the system of rational numbers.

We can think of $\mathbb{Z}$ as a subset of $\mathbb{Q}$ by identifying

$$n \in \mathbb{Z} \iff \frac{n}{1} \in \mathbb{Q}.$$

The benefit of $\mathbb{Q}$ is that we can divide by nonzero elements.

If $x = \frac{a}{b} \neq 0$, then $a \neq 0$, hence the symbol $\frac{b}{a}$ exists and we have

$$\frac{a}{b} \cdot \frac{b}{a} = 1.$$

Every nonzero rational number has a multiplicative inverse.

Note that fractions do not have a unique representation:

$$\frac{-3}{4} = \frac{3}{-4} = \frac{6}{-8} = \frac{-6}{8} = \text{etc....}$$

Q: Does each $x \in \mathbb{Q}$ have a best representation?

We will say that $x = a/b$ is in lowest terms if

- $b > 0$
- $\gcd(a, b) = 1$

Theorem: Every $x \in \mathbb{Q}$ can be represented uniquely in lowest terms.

[Remark: We have already used this when we proved that $\sqrt{2} \notin \mathbb{Q}$. But we never proved it.]

Proof of Existence (HW 3.3):

Let $x = a/b \in \mathbb{Q}$. We can assume that $b > 0$, otherwise we just write $a/b = (-a)/(-b)$

[Note: $\frac{a}{b} = \frac{-a}{-b}$ because $a(-b) = (-a)b$.]

Now suppose that $d = \gcd(a, b)$, with $a = da'$ and $b = db'$. Then we have

$$x = \frac{a}{b} = \frac{da'}{db'} = \frac{a'}{b'}$$

because $da'b' = db'a'$. Since $b > 0$ and $d > 0$ we have $b' > 0$.

We claim that $\gcd(a', b') = 1$.
Indeed, by Bézout's Identity
$\exists\, x, y \in \mathbb{Z}$ such that

$$d = ax + by.$$
$$d = da'x + db'y$$
$$d = d(a'x + b'y)$$
$$1 = a'x + b'y.$$

Now any common divisor of a' and b' must divide 1. [Suppose $a' = ka''$ and $b' = kb''$. Then

$$1 = a'x + b'y$$
$$= ka''x + kb''y$$
$$= k(a''x + b''y). \ ]$$

Hence $\gcd(a', b') = 1$ and $x = a'/b'$ is in lowest terms. ///

Proof of Uniqueness :

Suppose that $x = \frac{a_1}{b_1} = \frac{a_2}{b_2}$ with

- $b_1 > 0$, $b_2 > 0$
- $\gcd(a_1, b_1) = \gcd(a_2, b_2) = 1$.

We want to show that $a_1 = a_2$ and $b_1 = b_2$.

Since $a_1/b_1 = a_2/b_2$ we have

$$a_1 b_2 = a_2 b_1.$$

We claim that $b_1 \mid b_2$.

Indeed, since $\gcd(a_2, b_2) = 1$ $\exists\, x, y \in \mathbb{Z}$ such that

$$1 = a_2 x + b_2 y$$

Multiply both sides by b_1 to get

$$\begin{aligned} b_1 &= a_2 b_1 x + b_2 b_1 y \\ &= a_1 b_2 x + b_2 b_1 y \\ &= b_2 (a_1 x + b_1 y). \end{aligned}$$

Hence $b_1 \mid b_2$. And similarly $b_2 \mid b_1$.

So we have $b_1 = s b_2$ and $b_2 = t b_1$ for some $s, t \in \mathbb{Z}$. Hence

$$b_1 = s b_2 = st b_1$$

$$\Rightarrow \quad b_1 - st b_1 = 0$$

$$\Rightarrow \quad (1 - st) b_1 = 0$$

Since $b_1 \neq 0$ we get $1 - st = 0$, or $st = 1$, we conclude that $s, t = \pm 1$, hence $b_1 = \pm b_2$

$\square$

Since $b_1 > 0$ and $b_2 > 0$ by assumption, we get $b_1 = b_2$, and

$$a_1 \cancel{b_1} = a_2 b_2 = a_2 \cancel{b_1} \implies a_1 = a_2$$