Wed Oct 3

Last time we talked about subtraction.

Theorem: For all $n \in \mathbb{Z}$ there exists a unique integer $m \in \mathbb{Z}$ such that $n + m = 0$.

Since m is unique we give it a special name: "$-n$". And we call it "THE additive inverse of n".

This allows us to define subtraction.

DEF: For all $a, b \in \mathbb{Z}$ we set

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

We can also define absolute value.

DEF: For all $n \in \mathbb{Z}$ we set

$$|n| := \begin{cases} n & \text{if } n \geq 0 \\ -n & \text{if } n < 0 \end{cases}$$

Thinking Homework: For all $a, b \in \mathbb{Z}$ prove that $|ab| = |a||b|$.

[Hint: See Homework 3.4] ///

Now we will discuss division.
(Chapter 2.1 of the text)

DEF: Given $a, b \in \mathbb{Z}$ with $b \neq 0$, we say that $a | b$ (i.e. "a divides b") if $\exists k \in \mathbb{Z}$ such that $b = ka$.

Prop 2.11 in the book is a useful Lemm. For now we just need

Prop 2.11 (iv): If $a | b$ and $b \neq 0$ then $|a| \leq |b|$.

Proof: If $a | b$, $\exists k \in \mathbb{Z}$ with $b = ka$. If $b \neq 0$ then also $k \neq 0$, hence $|k| \geq 1$, and hence

$$|b| = |k||a| \geq |a|$$

$\blacksquare$

Is this rigorous?
I didn't go all the way to the axioms but that's OK.

(logically, NOT chronologically)

Now we have the First Theorem of Number Theory.

Theorem (The Division Algorithm 2.12):

Given $a, b \in \mathbb{Z}$ with $b \neq 0$, $\exists$ unique $q, r \in \mathbb{Z}$ such that

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

eg. Let $(a, b) = (-14, -6)$

$$-14 = \underbrace{3}_{\text{THE quotient}} \cdot (-6) + \underbrace{4}_{\text{THE remainder}}$$

Note: $0 \leq 4 < |-6|$ ✓

What about $(a, b) = (-14, +6)$.

$$-14 = \underbrace{(-3)}_{\text{THE quotient}} \cdot 6 + \underbrace{4}_{\text{THE remainder}}$$

- Quotient can be negative
- Remainder can NOT

Proof of 2.12 : (Just watch, we'll discuss after)

Let $S := \{a - qb : q \in \mathbb{Z}\}$
$= \{\ldots, a-b, a, a+b, a+2b, \ldots\}$

Since $b \neq 0$, S contains some non-negative element.

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

By Well-Ordering, S^+ has a smallest element. Call it r.

Since $r \in S$, $\exists\, q \in \mathbb{Z}$ with $a - qb = r$, i.e. $a = qb + r$. Since $r \in S^+$ we have $0 \leq r$. We need to show $r < |b|$.

Suppose not, i.e. suppose $r \geq |b|$.
Then $r - |b| \geq |b| - |b| = 0$ and
$r - |b| = a - qb - |b| = a - (q \pm 1) b$,
hence $r - |b| \in S^+$
But $r - |b| < r$ contradicts the fact that $r \in S^+$ is smallest.

We conclude that $a = qb + r$ with $0 \leq r < |b|$.
Hence q and r EXIST ✓

But are they UNIQUE?

Suppose that $a = q_1 b + r_1$ and $a = q_2 b + r_2$ with $0 \le r_1 < |b|$ and $0 \le r_2 < |b|$.
We claim that $q_1 = q_2$ and $r_1 = r_2$.

Suppose NOT, i.e. suppose that $r_1 \ne r_2$, say $r_1 < r_2$. Then we have

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

But $q_1 b + r_1 = a = q_2 b + r_2$

$\Rightarrow q_1 b - q_2 b = r_2 - r_1$.

$\Rightarrow b(q_1 - q_2) = (r_2 - r_1)$

$\Rightarrow b \mid (r_2 - r_1)$. (Recall: $b \ne 0$).

Finally Prop 2.11 (iv) says $|b| \le |r_2 - r_1| = r_2 - r_1$, CONTRADICTING $(*)$

Hence $r_1 = r_2$.
And $b(q_1 - q_2) = r_2 - r_1 = 0$
with $b \ne 0 \Rightarrow (q_1 - q_2) = 0$

$\Rightarrow q_1 = q_2$

$\blacksquare$

That's a <u>real</u> Theorem

Fri Oct 5.

Error in HW 3.2.
I'll email a fix today.

Last time we proved the 1st Theorem of number theory

Theorem (The Division Algorithm 2.12):

Given $a, b \in \mathbb{Z}$ with $b \neq 0$, $\exists$ unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|.$$

[You can practice this on HW 3.3]

Proof Reminder: (Sketch)

Let $S = \{a - qb : q \in \mathbb{Z}\}$ and $S^+ = \{n \in S : n \geq 0\}$.
By Well-Ordering, S^+ has a smallest element. Call it $r \in S^+$.

By definition of S, $\exists$ $q \in \mathbb{Z}$ such that $r = a - qb$, i.e. $a = qb + r$.

Check that $0 \leq r < |b|$: If NOT, then $r - |b|$ is a smaller element of S^+, contradiction ✓

So q, r EXIST with the desired properties. Are they UNIQUE?

Suppose $a = q_1 b + r_1$ and $a = q_2 b + r_2$ with $0 \leq r_1 < |b|$ and $0 \leq r_2 < |b|$.

Then $q_1 b + r_1 = q_2 b + r_2$

$\Longrightarrow q_1 b - q_2 b = r_2 - r_1$

$\Longrightarrow b(q_1 - q_2) = (r_2 - r_1)$

$\Longrightarrow b \mid (r_2 - r_1)$

If $r_1 \neq r_2$ this leads to a contradiction.

Hence $r_1 = r_2$ and then $q_1 = q_2$ $\blacksquare$

That's a real theorem and a real proof

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

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

If $d \in \mathrm{Div}(a,b)$ then by Prop 2.11 (iv) we have $d \le |d| \le |a|$ and $d \le |d| \le |b|$.

Hence $\mathrm{Div}(a,b)$ is bounded above by $\min\{|a|, |b|\}$

i.e.

$$\forall d \in \mathrm{Div}(a,b), \quad d \le \min\{|a|, |b|\}.$$

DEFINE

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

the "greatest common divisor"

(Why does gcd exist? Well-Ordering.)

Note: $1 \in \mathrm{Div}(a,b)$.

$$\Longrightarrow 1 \le \gcd(a,b) \le \min\{|a|, |b|\}.$$

eg. $\mathrm{Div}(8,12) = \{-4, -2, -1, 1, 2, 4\}$

Hence $\gcd(8,12) = 4$.

$\gcd(-8, 12) = ?\ \ 4$

$\gcd(-8, -12) = ?\ \ 4$

$\gcd(1, 100) = ?\ \ 1$

$\gcd(0, 100) = ?\ \ 100.$

$\gcd(1053, 481) = ?$

How can we compute gcd?

Prop 2.21: If $a = qb + r$ then

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

Proof: Postponed.

Let's APPLY it. Divide 1053 by 481.

$$\begin{aligned}
& & &\gcd(1053, 481)\\
1053 &= 2 \cdot 481 + 91 & &= \gcd(481, 91)\\
481 &= 5 \cdot 91 + 26 & &= \gcd(91, 26)\\
91 &= 3 \cdot 26 + 13 & &= \gcd(26, 13)\\
26 &= 2 \cdot 13 + 0 & &= \gcd(13, 0)\\
&\text{DONE} & &= 13
\end{aligned}$$

This is an "algorithm".

- called the "pulverizer" (kuttak) by Brahmagupta. (598 - 668 CE).
  - inventor of zero
- common name:
  The Euclidean Algorithm

Mon Oct 8

See updated HW 3

New Problem 2: Given $d \geq 0$. Prove that if $\sqrt{d} \notin \mathbb{Z}$ then $\sqrt{d} \notin \mathbb{Q}$.
(You already know this for $d = 2, 3, 5$.)

You might try to prove a Lemma:
$\forall n \in \mathbb{Z}$, if $d \mid n^2$ and d is not square then $d \mid n$.

But it's not true!
$$12 \mid 6^2 \quad \text{BUT} \quad 12 \nmid 6$$

So I suggested a different method, using Fermat's "infinite descent".

Where are we? Recall:

Given $a, b \in \mathbb{Z}$ not both zero, let

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

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

Note : $1 \in \mathrm{Div}(a,b)$ always

$\Rightarrow 1 \le \gcd(a,b)$

and $d \in \mathrm{Div}(a,b) \Rightarrow d \mid a \Rightarrow d \le |a|$

and $\Rightarrow d \mid b \Rightarrow d \le |b|$.

$\Rightarrow \gcd(a,b) \le \min\{|a|, |b|\}$.

Also note : If $b \mid a$ then $\gcd(a,b) = |b|$

How to compute gcd ?

eg. Compute $\gcd(3094, 2513)$.

Bad method : For every $d = 1, \ldots, 2513$, test if $d \mid 3094$ and $d \mid 2513$.

Good Method : Divide 3094 by 2513

$3094 = 1 \cdot 2513 + 581$.

If $d \mid 3094$, say $3094 = kd$ and
$d \mid 2513$, say $2513 = ld$

Then $581 = 3094 - 2513 = kd - ld$
$= (k-l)d$

$\Rightarrow d \mid 581$ Also.

In other words:

$$\mathrm{Div}(3094, 2513) \subseteq \mathrm{Div}(2513, 581)$$
$$\gcd(3094, 2513) \leq \gcd(2513, 581).$$

In fact they are equal.

Lemma (Prop 2.21): Given $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$.
If $\alpha = \beta\gamma + \delta$ then $\gcd(\alpha, \beta) = \gcd(\beta, \delta)$.

Proof: We will prove that $\mathrm{Div}(\alpha, \beta) = \mathrm{Div}(\beta, \delta)$ and hence

$$\max \mathrm{Div}(\alpha, \beta) = \max \mathrm{Div}(\beta, \delta)$$
$$\gcd(\alpha, \beta) = \gcd(\beta, \delta).$$

We must show two things:

1. $\mathrm{Div}(\alpha, \beta) \subseteq \mathrm{Div}(\beta, \delta)$.

So suppose $d \in \mathrm{Div}(\alpha, \beta)$, say $\alpha = dk$ and $\beta = dl$ for some $k, l \in \mathbb{Z}$. Then

$$\delta = \alpha - \beta\gamma = dk - dl\gamma = d(k - l\gamma),$$

i.e. $d \mid \delta$. Hence $d \in \mathrm{Div}(\beta, \delta)$.

(2) $Div(\beta,\delta) \subseteq Div(\alpha,\beta)$.

So suppose $d \in Div(\beta,\delta)$, i.e. $\beta = dk$ and $\delta = dl$ for some $k, l \in \mathbb{Z}$. Then we have

$$\alpha = \beta\gamma + \delta = dk\gamma + dl = d(k\gamma + l),$$

i.e. $d \mid \alpha$. Hence $d \in Div(\alpha,\beta)$. $\blacksquare$

Hence $\gcd(3094, 2513) = \gcd(2513, 581)$ and we can Repeat.

$$
\begin{aligned}
& & & \gcd(3094, 2513) \\
3094 &= 1 \cdot 2513 + 581 & &= \gcd(2513, 581) \\
2513 &= 4 \cdot 581 + 189 & &= \gcd(581, 189) \\
581 &= 3 \cdot 189 + 14 & &= \gcd(189, 14) \\
189 &= 13 \cdot 14 + 7 & &= \gcd(14, 7) \\
14 &= 2 \cdot 7 + 0 & &= \gcd(7, 0) \\
& & &= 7
\end{aligned}
$$

We did 5 divisons with remainder instead of 2513 !

:)

Official Statement.

Theorem (Euclidean Algorithm 2.22):
To compute $\gcd(a,b)$ for $a, b \in \mathbb{Z}$ with $b \neq 0$. Apply the Division Algorithm 2.11 to divide a by b. Then repeat

$$a = q_1 b + r_1, \quad 0 \le r_1 < |b|$$
$$b = q_2 r_1 + r_2, \quad 0 \le r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3, \quad 0 \le r_3 < r_2$$
etc.

Get a sequence

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

By Well-Ordering $\exists\, n$ with $r_n = 0$ and $r_{n-1} > 0$.

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

Proof: By Lemma (Prop 2.21) we have

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

$\blacksquare$

Example: compute $\gcd(31, 12)$.

$$\begin{aligned} 31 &= 2 \cdot 12 + 7 \\ 12 &= 1 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \longrightarrow \gcd = 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

We say 12 & 31 are coprime.

Wed Oct 10.

HW 3 due Friday.

Today: The Coin Problem

You live in a country where the coins come in two denominations a and b.

Q: Which amounts of money can you obtain in this country?

A: You want to solve the equation

$$ax + by = d.$$

For $x, y, d \in \mathbb{Z}$ (probably positive).

We will use the Euclidean Algorithm.

Recall: To compute $\gcd(31, 12)$,

$$31 = 2 \cdot 12 + 7$$
$$12 = 1 \cdot 7 + 5$$
$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1 \longrightarrow \gcd(31, 12) = 1.$$
$$2 = 2 \cdot 1 + 0$$

"coprime".

But we can get more information from this.

Let $V = \{ (x, y, d) \in \mathbb{Z}^3 : 12x + 31y = d \}$

= the set of integer solutions to

$12x + 31y = d$.

Claim: V is "closed" under vector addition and "scalar" multiplication by $\mathbb{Z}$.

eg. if $(x_1, y_1, d_1), (x_2, y_2, d_2) \in V$

i.e. $12x_1 + 31y_1 = d_1$ and $12x_2 + 31y_2 = d_2$.

Then for any $\alpha \in \mathbb{Z}$ we have

$(x_1, y_1, d_1) + \alpha(x_2, y_2, d_2)$

$= (x_1 + \alpha x_2, y_1 + \alpha y_2, d_1 + \alpha d_2) \in V$

i.e. $12(x_1 + \alpha x_2) + 31(y_1 + \alpha y_2) = d_1 + \alpha d_2$.

Proof: First note that

$12x_2 + 31y_2 = d_2 \implies 12(\alpha x_2) + 31(\alpha y_2) = \alpha d_2$.

Then $12x_1 + 31y_1 = d_1$

$+\ 12(\alpha x_2) + 31(\alpha y_2) = \alpha d_2$

$12(x_1 + \alpha x_2) + 31(y_1 + \alpha y_2) = d_1 + \alpha d_2$ $\blacksquare$

This is very useful. Let's use it.

First note that $(0,1,31), (1,0,12) \in V$.
since $0 \cdot 12 + 1 \cdot 31 = 31$ and $1 \cdot 12 + 0 \cdot 31 = 12$.

x	y	d	
0	1	31	①
1	0	12	②
−2	1	7	③ = ① − 2②
3	−1	5	④ = ② − 1③
−5	2	2	⑤ = ③ − 1④
13	−5	1	⑥ = ④ − 2⑤
−31	12	0	⑦ = ⑤ − 2⑥

This is the Extended Euclidean Algorithm 2.25.

So what? Every row is $\in V$, so

⑥ $\Longrightarrow 12(13) + 31(-5) = 1 = \gcd(12,31)$.
⑦ $\Longrightarrow 12(-31) + 31(12) = 0$

Moreover, ⑥ $+ k$ ⑦ $\in V \quad \forall k \in \mathbb{Z}$

i.e. $12(13-31k) + 31(-5+12k) = 1$

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

More generally,

$$d \, (6) + k \, (7) \in V \quad \forall \, d, k \in \mathbb{Z}.$$

$$12 \underbrace{(13d - 31k)}_{x} + 31 \underbrace{(-5d + 12k)}_{y} = d \cdot 1 - k \cdot 0$$
$$= d.$$

OK, so in the country of ¢12 and ¢31 coins, can you obtain ¢d ?

Yes if $\exists \, k \in \mathbb{Z}$ such that

$$13d - 31k \geq 0 \quad \& \quad -5d + 12k \geq 0.$$
$$13d \geq 31k \qquad\qquad 12k \geq 5d.$$
$$\frac{13d}{31} \geq k \qquad\qquad k \geq \frac{5d}{12}.$$

$$\frac{5d}{12} \leq \underset{\in \mathbb{Z}}{\underset{\uparrow}{k}} \leq \frac{13d}{31}.$$

For which $d \in \mathbb{Z}$ can this be solved?

It has a solution if

$$\frac{5d}{12} \quad \overset{?}{k} \quad , \quad \frac{13d}{31}$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{\geq 1.}$$

$$\frac{13d}{31} - \frac{5d}{12} \geq 1.$$

$$\left(\frac{13}{31} - \frac{5}{12}\right) d \geq 1.$$

$$\left(\frac{156 - 155}{372}\right) d \geq 1.$$

$$\left(\frac{1}{372}\right) d \geq 1.$$

$$d \geq 372$$

You can make change for <u>ANY</u> value $\geq$ ¢ 372.

(Below that the problem is trickier.)

Fri Oct 12

Recall: Extended Euclidean Algorithm 2.25

To compute gcd(3094, 2513).
First we had

$$3094 = 1 \cdot 2513 + 581$$
$$2513 = 4 \cdot 581 + 189$$
$$581 = 3 \cdot 189 + 14$$
$$189 = 13 \cdot 14 + 7 \leftarrow \text{gcd.}$$
$$14 = 2 \cdot 7 + 0$$

Now we have $3094x + 2513y = r$.

x	y	r	
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

Bonus:

$$3094(-173) + 2513(213) = 7$$
$$= \gcd(3094, 2513).$$

and even more: ⑥ + k⑦ says

$$3094\underbrace{(-173+359k)}_{x}+2513\underbrace{(213-442k)}_{y}=7$$

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

Corollary to EEA 2.25

Theorem (Bézout's Identity):
Given $a, b \in \mathbb{Z}$ not both zero $\exists\, x, y \in \mathbb{Z}$ (not unique) such that

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

VERY USEFUL

eg. If $d \mid a$ & $d \mid b$ then $d \mid \gcd(a,b)$.

Proof: Suppose $d \mid a$ and $d \mid b$, say $a = dk$ and $b = dl$. Then by Bézout's Identity, $\exists\, x, y \in \mathbb{Z}$ such that

$$\begin{aligned}\gcd(a,b) &= ax + by \\ &= dkx + dly \\ &= d(kx + ly) \implies d \mid \gcd(a,b)\end{aligned}$$

Topic: Prime Numbers

DEF: We say that $d|a$ is a "proper divisor if $d \notin \{\pm 1, \pm a\}$.

We say $p \in \mathbb{Z}$ is prime if it has NO proper divisors.

eg. The divisors of 7 are

$$Div(7) = \{-7, -1, 1, 7\}$$

so 7 is prime. Q: Is -7 prime?

If $n \in \mathbb{Z}$ is not prime we say it is "composite"

Proposition 2.51: Every integer $n \neq 0$ can be written as a product of primes, times ± 1.

eg. $60 = 2 \cdot 30$

$= 2 \cdot 2 \cdot 15$

$= 2 \cdot 2 \cdot 3 \cdot 5$ DONE

$= (-2)(-2)(-3)(-5)$

$= (-2) \cdot 2 (-3) \cdot 5$

(we dont care about minus signs)

Proof Idea: To factor $n \neq 0$.
If n is prime we're <u>done</u>. Otherwise
we can write

$$n = ab$$

with $1 < |a|, |b| < |n|$.

If a and b are prime we're done.
Otherwise, factor a and b.
Repeat until you can't continue...

~~Is this a proof~~?

We can do better.

Formal Proof of Prop 2.51:

Let $S = \{ |n| : n \neq 0$ has no prime factorization $\}$

Suppose for contradiction that $S \neq \emptyset$. Then by Well-Ordering it has a smallest element, say $m \in S$.

By assumption m is not prime (because it has no prime factorization). Hence we can write

$$m = ab$$

with $1 < a, b < m$.

But then $a, b \notin S$ (since $m \in S$ is smallest), hence they can both be factored into primes.

$\Longrightarrow$ Hence so can m!

Contradiction.

We conclude that $S = \emptyset$ as desired

$\blacksquare$

Mon Oct 15

HW 4 due Mon Oct 22
Exam 2 Wed Oct 24

Today: Fundamental Theorem of Arithmetic.

Recall that every $n \in \mathbb{Z}$, $n \neq 0$ can be factored as a product of primes, times ± 1
(we don't care about negative signs).

Proof by contradiction: Suppose not. By Well-Ordering, let m be the smallest integer > 1 that CANNOT be factored into primes. Since m is not prime $\exists\, a, b \in \mathbb{Z}$ with $1 < a \leq b < m$ such that $m = ab$. Since $a, b < m$, BOTH can be factored into primes. But then so can m.
Contradiction. $\blacksquare$

m is a "minimal criminal"

eg. $364 = 2 \cdot 2 \cdot 7 \cdot 13$
$= 7 \cdot 2 \cdot 13 \cdot 2$
$= 7(-2)(-13)2.$ } all essentially the same.

Q: Are the prime factors UNIQUE?
A: How could they not be.

eg. Consider a different number system

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

Then we have

I won't prove this or even define what it means.

$$6 = \underbrace{\overset{\text{prime}}{2 \cdot 3} = \overset{\text{Claim: prime}}{(1+\sqrt{-5})(1-\sqrt{-5})}}_{\text{Two different prime factorizations!}}$$

Goal: Show that this can't happen in $\mathbb{Z}$.

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

Given $a, b, p \in \mathbb{Z}$ with p prime, if $p \mid ab$ then $p \mid a$ OR $p \mid b$.

[Note: This fails if p is not prime. eg. $4 \mid 12$, but $4 \nmid 2$ and $4 \nmid 6$]

Proof: We will show the logically equivalent statement: $(p \mid ab \text{ and } p \nmid a) \Rightarrow p \mid b$.

So suppose $p \mid ab$, say $ab = pk$, and suppose $p \nmid a$. Then $\gcd(a, p) = 1$ (Why?) By Bézout's Identity, $\exists\, x, y \in \mathbb{Z}$ such that

$$ax + py = 1$$

Multiply by b (TRICK) to get

$$(ax + py)\, b = b$$
$$abx + pby = b$$
$$pkx + pby = b$$
$$p(kx + by) = b \Rightarrow p \mid b.$$

$\blacksquare$

Thinking Homework: 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?

Finally,

Unique factorization Theorem 2.54
"Fundamental Theorem of Arithmetic"

Every integer $n \neq 0$ has a unique factorization into primes (apart from reordering and negative signs).

Proof Idea: Suppose n can be written

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$

where $p_1, \dots, p_k, q_1, \dots, q_\ell$ are prime.

Since $p_1 \mid n$ we have

$$p_1 \mid q_1 q_2 \cdots q_\ell$$

By Euclid's Lemma we have $p_1 \mid q_i$ for some i. But since p_1, q_i are prime this implies $p_1 = \pm q_i$.
Cancel from both sides to get

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

$$\underbrace{\text{Repeat until you're done} \ldots}_{\text{Is this a proof ?}}$$

Formal Proof of Unique Factorization :
Suppose $\exists$ an integer with <u>two</u> <u>different</u> prime factorizations. By Well-Ordering let m be the <u>smallest</u> such and write

$$m = \underbrace{p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell}_{\text{different in some } \underline{\text{nontrivial}} \text{ way.}} \qquad (*)$$

Since $p_1 \mid m$ we have $p_1 \mid q_1 q_2 \cdots q_\ell$ and Euclid's Lemma $\Longrightarrow$ $p_1 \mid q_i$ for some i. Since p_1, q_i are prime this implies $p_1 = \pm q_i$

Divide p_1 from (*) to get

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

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

$\blacksquare$

Wed Oct 17

HW 4 due Mon Oct. 22
Exam 2 Wed Oct 24.

What have we done?

- What is a "number"?
- Definition of $\mathbb{Z}$
  - Well-Ordering Axiom
- Division Algorithm:
  - $\forall a, b \in \mathbb{Z}$, $b \neq 0$, $\exists$ unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$.
- Euclidean Algorithm
  - to compute $\gcd(a,b)$
- Extended Euclidean Algorithm
  - to solve the equation $ax + by = r$.
- Bézout's Identity
  - $\exists x, y \in \mathbb{Z}$, $ax + by = \gcd(a,b)$.
- Euclid's Lemma
  - if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.
  - Proof uses Bézout (see HW 4.4)
- Fundamental Theorem of Arithmetic
  - every $n \neq 0$ can be written <u>uniquely</u> as a product of primes, times ± 1.

i.e. we can write

$$n = \pm p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$$

where $1 < p_1 < p_2 < \cdots < p_k$.

Thus we can reduce the study of $\mathbb{Z}$ to the study of <u>prime</u> <u>numbers</u>.

<u>eg.</u> Suppose $a, b \in \mathbb{Z}$ satisfy.

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

for some primes $1 < p_1 < p_2 < \cdots < p_n$.

Then $\gcd(a,b) = p_1^{d_1} p_2^{d_2} \cdots p_n^{d_n}$.

where $d_i = \min\{a_i, b_i\} \ \forall i$.

<u>eg.</u> let $a = 336$, $b = 2156$

$$336 = 2^4 \cdot 3 \cdot 7 \quad = 2^4 \cdot 3^1 \cdot 7^1 \cdot 11^0$$
$$2156 = 2^2 \cdot 7^2 \cdot 11 \quad = 2^2 \cdot 3^0 \cdot 7^2 \cdot 11^1$$

$$\gcd(336, 2156) = 2^2 \cdot 3^0 \cdot 7^1 \cdot 11^0$$
$$= 28.$$

[Warning: This is not computationally useful. Factoring is "hard"!]

Similarly we could define the least common multiple

$$\operatorname{lcm}(a,b) := \min\{ m : a \mid m,\ b \mid m,\ m > 0 \}.$$

and then we have

$$\operatorname{lcm}(a,b) = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

where $e_i = \max\{a_i, b_i\}$ $\forall i$.

eg.

$$336 = 2^4 \cdot 3^1 \cdot 7^1 \cdot 11^0$$
$$2156 = 2^2 \cdot 3^0 \cdot 7^2 \cdot 11^1$$
$$\operatorname{lcm} = 2^4 \cdot 3^1 \cdot 7^2 \cdot 11^1 = 25875$$

Here's a fun observation:

<u>Theorem</u> 2.59: Given positive $a, b \in \mathbb{Z}$,

$$a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b).$$

Proof: Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, $b = p_1^{b_1} \cdots p_n^{b_n}$ for some primes $1 < p_1 < \cdots < p_n$. Note that $\forall i$ we have

$$a_i + b_i = \min\{a_i, b_i\} + \max\{a_i, b_i\}.$$

Now let $d_i := \min\{a_i, b_i\}$, $e_i := \max\{a_i, b_i\}$. Then

$$\begin{aligned} ab &= p_1^{a_1} \cdots p_n^{a_n} p_1^{b_1} \cdots p_n^{b_n} \\ &= p_1^{(a_1+b_1)} p_2^{(a_2+b_2)} \cdots p_n^{(a_n+b_n)} \\ &= p_1^{(d_1+e_1)} p_2^{(d_2+e_2)} \cdots p_n^{(d_n+e_n)} \\ &= \underbrace{p_1^{d_1} \cdots p_n^{d_n}} \underbrace{p_1^{e_1} \cdots p_n^{e_n}} \\ &= \gcd(a,b) \cdot \operatorname{lcm}(a,b). \end{aligned}$$

$\blacksquare$

Q: How would you prove that without prime decomposition?

Thus

"number theory" = study of $\mathbb{Z}$ = study of primes

What are the primes ?

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, etc.

Euclid's Theorem 2.52 :
The list of primes goes on forever.

Proof : Suppose not, and suppose that $p_1, p_2, \ldots, p_n$ are all the primes.

Now define $N = p_1 p_2 \cdots p_n + 1$.
We know N has a prime factor $p | N$.
(every number does). So this p must be in the list of primes.

But $p_i \nmid N$ because if it did then $p_i | (N - p_1 p_2 \cdots p_n) \Rightarrow p_i | 1$.

Thus $p \neq p_i \ \forall i$. Contradiction $\blacksquare$

Observation: Every prime except 2 is odd.
So if p is prime then $p = 4k+1$ or $4k+3$.
$(p \equiv 1 \bmod 4)$ $(p \equiv 3 \bmod 4)$

Notation:

$$a \equiv b \bmod n \iff n \mid a-b.$$
$$(\text{i.e. } a = nk + b)$$

"a and b have the same remainder when divided by n"

Primes:

p	2,	3,	5,	7,	11,	13,	17,	19,	23,	29,	etc.
mod 4	2,	3,	1,	3,	3,	1,	1,	3,	3,	1,	...

Q: Does 1 occur ∞ often?
How about 3?

See HW 4.5.

[Dirichlet's Theorem (1837): If $\gcd(a,n) = 1$, then $\exists$ ∞ many primes of the form $a + kn$ for some $k \in \mathbb{Z}$.]

Fri Oct 19

HW 4 due Mon Oct 22
Exam 2 Wed Oct 24
Fall Break Fri Oct 26 :)

Material for Exam 2:
Chapter 2, except Section 2.4.

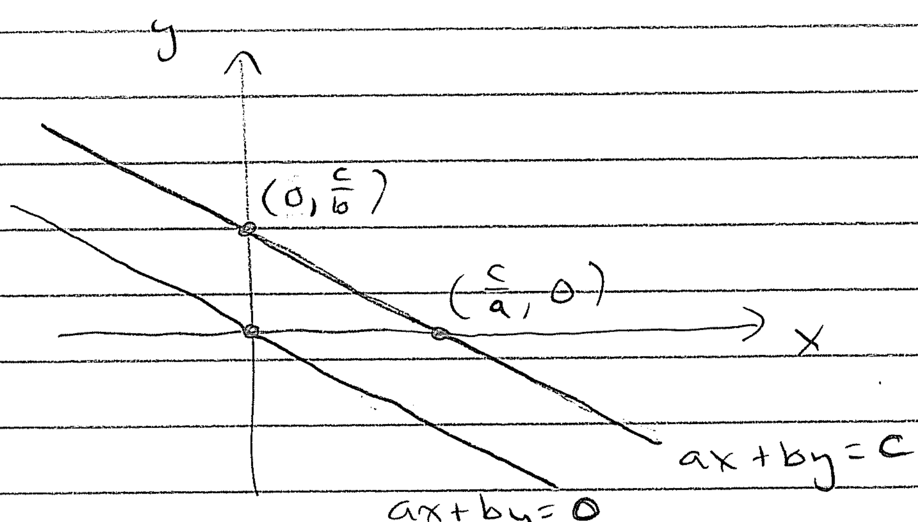
Look at Practice Exam.

One last idea to discuss:

Given integers $a, b, c \in \mathbb{Z}$ what is the complete solution to the "Linear Diophantine Equation"

$$ax + by = c \, ?$$

Over the Real numbers it's a line



But "Diophantine" means we want the integer points $(x,y) \in \mathbb{Z}^2$ on the line.

So let $d := \gcd(a,b)$.

By HW 4.2 we know that $ax+by=c$ has a solution $\iff d \mid c$.

So suppose $d \mid c$.
Then by HW 4.3 we know the general solution to $ax+by=c$ is

$$(x,y) = (x_0,y_0) + (x',y')$$

where $ax_0+by_0=c$ is any one particular solution and (x',y') is the general solution to the homogeneous equation

$$\underbrace{ax' + by' = 0}.$$

We must solve this.

First note: By Bézout $\exists\, \alpha, \beta \in \mathbb{Z}$ with

$$a\alpha + b\beta = d.$$

Divide by d to get

$$\underbrace{\left(\frac{a}{d}\right)}_{\text{integers.}}\alpha + \underbrace{\left(\frac{b}{d}\right)}_{}\beta = 1.$$

By Problem 1(b) on Practice Exam, this implies $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

General solution to $ax' + by' = 0$:
Divide by d to get

$$ax' + by' = 0$$

$$\Updownarrow$$

$$\left(\frac{a}{d}\right)x' + \left(\frac{b}{d}\right)y' = 0$$

$$\Updownarrow$$

$$\left(\frac{b}{d}\right)y' = -\left(\frac{a}{d}\right)x' \qquad (*)$$

We have $\frac{b}{d} \mid \left(\frac{a}{d}\right) x'$ and $\gcd\left(\frac{b}{d}, \frac{a}{d}\right) = 1$.

HW 4.4 implies that $\frac{b}{d} \mid x'$

i.e. $\exists\, k \in \mathbb{Z}$ with $x' = \frac{b}{d} k$.

Similarly $\exists\, l \in \mathbb{Z}$ with $y' = \frac{a}{d} l$.

Substitute into $(*)$ to get

$$\cancel{\left(\frac{b}{d}\right)\left(\frac{a}{d}\right)} l = -\cancel{\left(\frac{a}{d}\right)\left(\frac{b}{d}\right)} k$$

$$\Longrightarrow \quad l = -k.$$

Conclusion: The general solution of the homogeneous equation

$$ax' + by' = 0$$

is $(x', y') = \left(\frac{b}{d} k, -\frac{a}{d} k\right) \quad \forall\, k \in \mathbb{Z}$.

//

Putting it together, we get

Theorem 2.31 (Lin. Dioph. Eq. Thm.):

Given $a, b, c \in \mathbb{Z}$ and $d := \gcd(a,b)$.

① The equation $ax + by = c$ has a solution $\iff d \mid c$.

② If $ax_0 + by_0 = c$ is one particular solution, then the general solution is

$$(x,y) = \left(x_0 + \frac{b}{d}k,\ y_0 - \frac{a}{d}k\right) \ \forall\, k \in \mathbb{Z}.$$

Example: Find the general solution of $34x + 6y = 8$ (if it has any)

Apply Extended Euclidean Algorithm to 34 and 6:

$(34x + 6y = r)$

x	y	r	
1	0	34	①
0	1	6	②
1	-5	4	③ = ① − 5 · ②
-1	6	2	④ = ② − 1 · ③
3	-17	0	⑤ = ③ − 2 · ④

Conclusion: $\gcd(34, 6) = 2$ with

$$34(-1) + 6(6) = 2 \mid 8 \checkmark$$

Multiply by 4,

$$\underbrace{34(\underset{x_0}{-4}) + 6(\underset{y_0}{24})}_{\text{one particular solution.}} = 8$$

General solution to $34x + 6y = 8$ is

$$(x, y) = \left(x_0 + \frac{b}{d}k,\ y_0 - \frac{a}{d}k\right)$$

$$= (-4 + 3k, 24 - 17k) \ \forall k \in \mathbb{Z}$$

Picture (not to scale)