"Applications" of Number Theory 9/6/18

Given 3¢ and 5¢ coins (unlimited)
Q: What amounts can you make?
A: 0, 3, 5, 6, 8, 9, 10, 11, 12, 13, ...

let $\mathbb{N} := \{0, 1, 2, 3, \ldots\}$
then $3\mathbb{N} + 5\mathbb{N} = \{0, 3, 5, 6, 8, 9, 10, 11, \ldots\}$

How do we know we have it all?
Max: check some early ones, then subtract off 3's from higher ones.

Claim: For every $n \geq 8$, n is in $3\mathbb{N}+5\mathbb{N}$
Proof (Max):
Check that 8, 9, 10, 11, and 12 are in.
Jason: given any $n \geq 13$, subtract one of 8–12 to get a multiple of 5
Then add the needed 5¢ coins to get n.

Will: could also check 8, 9, and 10, and use 3¢ coins instead of 5¢

Now imagine we have an economy with only 3¢ and 5¢ coins.
Can now make 2¢: give 5¢ get back 3¢.
Can make 1¢ by $2 \cdot 3¢ - 5¢$.
Once we have 1¢, we get everything.

Let $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\} = \{\ldots, -1, 0, 1, \ldots\}$
↳ German: "zahlen"

Now we are looking at $3\mathbb{Z}+5\mathbb{Z}$

Claim: $3\mathbb{Z}+5\mathbb{Z}=\mathbb{Z}$

Pf: (Konnor):

Notice $1=6-5=3(2)-5(1)$.

Then for n in $\mathbb{Z}$, $n=1\cdot n=3(2n)-5n$. QED. (end of proof!)

Notation Notes: "x is an element of S" is $x \in S$.

"for every" is $\forall$

$3\mathbb{Z}+5\mathbb{Z}=\mathbb{Z}$

$2\mathbb{Z}+3\mathbb{Z}=\mathbb{Z}$ $(3-2=1)$

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

$7\mathbb{Z}+14\mathbb{Z}=7\mathbb{Z}$

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

Claim: Given $a,b \in \mathbb{Z}$, $\exists d \in \mathbb{Z}$ ("there exists") such that $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$

Ideas:

Max, Jacob, Nkem, Amelia + Sammy: d is the greatest common divisor of a and b?

Ben: Pick $x \in a\mathbb{Z}$ $y \in b\mathbb{Z}$ let $d=\gcd(a,b)$.

$x=aw$, $y=bq$

$\frac{x}{d}=\frac{a}{d}w$ $\frac{y}{d}=\frac{b}{d}q$

then $x+y \in a\mathbb{Z}+b\mathbb{Z}$ and $\frac{x+y}{d} \in \mathbb{Z}$...

Proposition (Ben): $a\mathbb{Z}+b\mathbb{Z} \subseteq d\mathbb{Z}$ ("is a subset of") where $d=\gcd(a,b)$

Pf (Jason):

Let $ax \in a\mathbb{Z}$ $by \in b\mathbb{Z}$ and $d=\gcd(a,b)$.

$\frac{ax+by}{d} = \frac{a}{d}x + \frac{b}{d}y \in \mathbb{Z}$

so $d\left(\frac{ax+by}{d}\right) = ax+by \in d\mathbb{Z}$ □

Now we need $d\mathbb{Z} \subseteq a\mathbb{Z}+b\mathbb{Z}$

Miranda: $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Jason: divide both by d?

Ben: Assume $d \neq 0$ [$d=0$ only when $a=b=0$]

Aside: don't start with what you want to prove

Justin: Enough to show that $\mathbb{Z} \subseteq a\mathbb{Z}+b\mathbb{Z}$ when $\gcd(a,b)=1$

Definition: The $\gcd(a,b)$ is the largest integer that divides both a and b

How do we prove Justin's claim?

Jason: ETS $1 \in a\mathbb{Z}+b\mathbb{Z}$ when $\gcd(a,b)=1$

Def: Whenever $\gcd(a,b)=1$ we say "a is relatively prime to b" or "a and b are coprime"

Ben: If a and b are coprime then $a-b$ and a as well as $a-b$ and b are coprime

Max: If Ben's idea is true, then can repeatedly subtract to get to 1

Prop: If a,b coprime then $1 \in a\mathbb{Z}+b\mathbb{Z}$

Pf:

Suppose $a<b$. then let $c=b-a$.
By Ben's conjecture $b-a$ and a coprime
If $a<c$, keep subtracting a, get $d=c-a$.
keep creating smaller numbers until
we get to 1. (Iteration)

Ex: $a=5$ $b=7$
Then $c=b-a=7-5=2$
now $c<a$.
Take $a-c=5-2=3$.
repeat $3-2=1$. ✓

Lemma: Given $a,b \in \mathbb{Z}$ $b>0$, then $\exists q,r \in \mathbb{Z}$
such that $a=qb+r$ where $0 \leq r < b$.

Pf:

Let $q := \lfloor \frac{a}{b} \rfloor$ ← largest integer less than or equal to a/b ("floor of")
Then $q \leq a/b < q+1$
so $bq \leq a < bq+b$
$0 \leq a-bq < b$ so $r := a-bq$ □