Video Extra Notes: Modular Inverses

For any RULE with integer inputs, our slope is rational, and thus we might expect to repeat after a while because of what we saw in the *Donuts* sequence. In fact, as we just saw, applying the rule n times on Plot n we have to end up back at the beginning. Thus, at most we'll have n points on any one line.

In any event, lines defined according to the point/slope recipe of the first Handout in the Straight Lines sequence, would necessarily be rational slope if we're using whole numbers in our ratio; which is certainly the case if we're defining lines by going through trees.

Suppose we go right one unit and up some arbitrary units, m, ie. we have integer slope. Well, on Plot n after going across n to the right, we will have gone up $m \times n$, BUT $n \times m$ will just be the bottom row again, which means, we'll end up in the top right corner. And the top right is the same as the bottom left, so like the rational case we looked at in the Donuts sequence, we have to repeat from here on out.

Here's the interesting thing though: If we hit a tree on the top edge earlier—well top edges are the same as (that is, identified with) bottom edge trees—then we must repeat the sequence we've made to this point. But if that's the case, then the first time we hit the top, we're back to the bottom again, and so if we continue, we'll repeat what we've just done. BUT we know we'll end up in the top right corner in the end (because we just figured that out a moment ago), so the width of this first sequence must divide the width of the whole Plot!

So for instance if we were looking at Plot 4, then the only possibilities for when we first hit the top row are 1, 2 or 4 as the length of the repeating sections; on the other hand with Plot 5, we either repeat immediately, ie. slope 5 (or some multiple thereof), or we don't repeat until we get to the far side, since 5 cannot be evenly divided up any other way (that, of course being what it means to be prime)!

Now here's the magic catch! We can't actually hit the same height twice before then (because otherwise we could just step backwards—sort of "unapply" our RULE—from the second instance, and we'd have to have a match for the bottom row earlier). So, that means we must hit trees on different rows for each column along the way. **THUS**, if we're thinking about Plot5, then m, $2m$, $3m$, and $4m$ must leave remainders 1, 2, 3, $4 \mod 5$, though not necessarily in that order. Crazy beautiful, right! Not only do we hit each column once, we must hit each row once too!

Note: if this sort of feels like it's on that cusp of making sense, and you're kind of getting it bit by bit, but the whole thing together still feels hazy . . . well that's how mathematics often feels when you're at the frontiers. The good news is that we're in a very safe exploring environment right now, we have a support crew right behind us in the form of the *Rule the Trees* Handout (that might be worth revisiting to cement your understanding). But it is kind of fun to think what it must have been like to be one of the first people to see this land,

kind of like a real life explorer heading out across the great plains in search of new country. Exciting to kind of feel that for a moment, and sort of like being on a little track in the bush and wondering if you haven't gotten lost.

Now mathematicians who have gone before us have developed some useful notation that encapsulates what we're seeing here. They say "a is congruent to b modulo n", written:

$$a \equiv b \mod n$$

whenever a and b leave the same remainder after dividing by n. So, for example:

3 and 8 are congruent modulo 5, written:

$$3 \equiv 8 \mod 5$$

because both leave remainder 3 after dividing by 5.

Warning: sometimes when we're being lazy and it's obvious, we negligently omit the modulus (see below for instance).

Finally, notice that the same sort of argument works if we don't have integral slope: we simply need to note that if we're looking at Plot n, then after repeating our RULE n times, we'll have to end up back at the beginning again, which is fun. (Again, that was what we saw in the *Rule the Trees* Handout). Moreover, we can't repeat the same height twice if n is prime (for exactly the same reason as when we were looking at Rule$(1, m)$ a moment ago).

So this means that for any prime number, take 13 for example (think Plot 13), and any other number less than that prime, take 4 for example, there must be some multiple of 4 that leaves remainder 1.

Well, let's check:

$$4, 8, 12, 16 \equiv 3, 20 \equiv 7, 24 \equiv 11, 28 \equiv 2, 32 \equiv 6, 36 \equiv 10, 40 \equiv 1$$

So, $10 \times 4 \equiv 1 \mod 13$.

And in some very real sense: $10 \equiv 1/4 \mod 13$!!

Indeed, all whole numbers, are either congruent to 0 or have inverses when we are working modulo a prime!

Now that's kind of crazy, and it gives rise to some really interesting ideas . . . but sadly for another day.

Of course, this only works for a prime modulus. For instance working $\mod 6$ has issues: In that case we get 2, 4, 0, 2, 4, 0, 2, . . . which is sort of like looking at RULE $(1, 2)$ on Plot 6, and noticing we never end up on the first row!!

Finally, back in the real world, this all means that given only \$$5$ notes and \$$2$ notes, I can still trade exactly \$$1$! In this case $1 = 1 \times 5 - 2 \times 2$, ie the inverse of $2 \mod 5$ is -2, or equivalently 3, but that would give me $2 \times 3 = 6$ and I'd have to take 5 away, ie. $1 = 3 \times 2 - 1 \times 5$.

Even more amazingly: if I only had $\$19$ notes and $\$17$ notes I could still trade exactly $\$1 \ldots$ can you figure out how? I'll leave that for you.