Math 189H Joy of Numbers Activity Log

Tuesday, August 30, 2011

Gottfried Leibnitz: "Music is the pleasure the human mind experiences from counting without being aware that it is counting."

Walt West: "The trouble with doing something right the first time is that nobody appreciates how difficult it was."

We started (I think!) by considering some of our questions from last time. If $a|b$ and $a|c$, what can we say about $b+c$? One answer was that $b+c$ was bigger than $a+c$, which will play into a later observation; after playing around with some specific examples (2 of them, which ordinarily is probably too small to find a pattern...) we concluded that $a|(b+c)$ and $a|bc$ as well. These we could prove! First we helped ourselves out with

Proposition: If $a|b$ and $b|c$, then $a|c$.

Proof: We know that $b = ax$ and $c = by$ for some $x, y \in \mathbb{Z}$, so $c = by = (ax)x = a(xy)$ with $xy \in \mathbb{Z}$, so $a|c$.

With this, half of our goal became a bit cleaner.

Proposition: If $a|b$ and $a|c$, then $a|b+c$ and $a|bc$.

Proof: From our hypotheses, we know that $b = ai$ and $c = aT$ for some integers $i, T \in \mathbb{Z}$. Then $b + c = ai + aT = a(i + t)$, so $a|b + c$, since $i + T \in \mathbb{Z}$. Further, since $a|b$ and it is certainly true that $b|bc$, since $bc = b(c)$ (!), our first proposition implies that $a|bc$.

This last statement bothered your instructor, since it didn't actually <u>use</u> one of our hypotheses (that $b|c$). We could create a 'stronger' result by assuming fewer hypotheses:

Proposition: If $a|b$ then $a|bc$ for any integer $c \in \mathbb{Z}$.

This is in fact what we showed, since we knew that $b|bc$.

We then used our newfound divisibility notation '$a|b$' to figure out how to describe a prime number: $p \in \mathbb{Z}$ is prime if the only numbers which divide it are ± 1 and $\pm p$. More symbolically:

$$p \text{ is prime if whenever } a|p\text{, we must have either } a = \pm 1 \text{ or } a = \pm p$$

Even more compactly:

$$p \text{ is prime if } [a|p \Rightarrow (a = \pm 1 \text{ or } a = \pm p)]$$

We then starting looking for primes! After initially naming some of our favorite primes (and favorite non-primes! $51 = 3 \cdot 17$, $91 = 7 \cdot 13$), we backed up and started making a more systematic list. The primes, in increasing order, begin with

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 \ldots$$

But wait, how were we generating this list? What were we <u>doing</u>? [Figuring this out will help us in our search for large primes.] Some numbers we could look at and know they weren't prime, because we remembered some 'tricks' for divisibility:

3 divides n precisely when 3 divides the sum of the digits of n.

5 divides n precisely when n ends in either 0 or 5.
9 divides n precisely when 9 divides the sum of the digits of n.
2 divides n precisely when n ends in 0,2,4,6, or 8.
4 divides n precisely when 4 divides the number made from the last two digits of n.

But is, for example, $n = 223$ prime? How would we figure that out? On the face of it we would want to test every number a to see if $a|n$ (in order to rule it out!). But we agreed that there was no point in trying $a = 323$, for example, because it was too big. We could formulate this more precisely as

Prop: If $a|b$ then (remembering that integers can be negative!) $|b| \geq |a|$.

Unfortunately, this isn't quite true! Because we forgot about 0; $5|0$ since $0 = 5(0)$, for example. But excluding 0, things work fine:

Proposition: If $b \neq 0$ and $a|b$, then $|a| \leq |b|$.

Proof: Since $a|b$, we know $b = ah$ for some $h \in \mathbb{Z}$. But $b \neq 0$ means that $h \neq 0$ (since if $h = 0$ then $b = ah = a \cdot 0 = 0$), so $|h| \geq 1$. So

$$|b| = |ah| = |a| \cdot |h| \geq |a| \cdot 1 = |a|.$$

Also, in looking for factors, we could limit ourselves to positive integers: if $a|b$ then $-a|b$ as well (since $b = ag = (-a)(-g)$). So to test for primality of $n = 223$, for example, we need only try the numbers from 1 to 223.

But as one of you observed, factors for numbers come in pairs! If $a|n$ then $n = ab$ for some $b \in \mathbb{Z}$, and so the factor a of n 'gives' us the other factor b, as well. This ought to allow us to cut our work in half? In fact, it will allow us to do a lot more than that!

To stimulate discussion for Thursday, we finished with the following questions:

Is $n = 229$ prime?

What is the smallest positive number that you can express as $5a + 7b$ with $a, b \in \mathbb{Z}$?

What numbers can you express as $5a + 7b$ with $a, b \in \mathbb{Z}$ and $a, b \geq 0$?

Consider the same questions for $21a + 27b$.