Math 189H Joy of Numbers Activity Log

Thursday, September 15, 2011

Thomas Jefferson: "I have only contempt for anyone who can think of only one way to spell a word."

Richard J. Trudeau: "Pure mathematics is the world's best game. It is more absorbing than chess, more of a gamble than poker, and lasts longer than Monopoly. It's free. It can be played anywhere - Archimedes did it in a bathtub."

12758 is the largest number that cannot be expressed as a sum of distinct primes (i.e., as $a_1^3 + a_2^3 + \cdots + a_k^3$ with $a_1, \ldots, a_k$ all distinct).

Class started by describing how to write 67 as four 4's! Your instructor felt like he had cheated, since he resorted to a 'standard' mathematical construction, the 'integer part' of a number (denoted using the 'floor' function, $\lfloor x \rfloor$), which is the largest integer that is less than or equal to x. But since we will be using this notation shortly, it seemed appropriate! Online sources gave much more mundane ways to express 67...

We then went back to our exploration of what we will call *linear combinations* of integers a and b, namely the integers $ax + by$ with $x, y \in \mathbb{Z}$. We started with our pairs from last time. For 1131 and 468, the smallest combination anyone could make was 39 (which quite surprised your instructor). If we ran the Euclidean algorithm, we could accomplish this:
$1131 = 468 \cdot 2 + 195$
$468 = 195 \cdot 2 + 78$
$195 = 78 \cdot 2 + 39$
$78 = 39 \cdot 2 + 0$

We didn't construct the linear combination realizing 39, although we have seen in other examples that we can work from the bottom up to achieve this. For our other examples we found by a similiar string of long divisions that we could write 1 as linear combinations.

We could verify in the above case that 39 is also the largest common divisor of 1131 and 468, by factoring these numbers (basically, finding 'small' factors to chip away at them).
$1131 = 3 \cdot 377 = 3 \cdot 13 \cdot 29$ and $468 = 2 \cdot 234 = 2 \cdot 2 \cdot 117 = 2^2 \cdot 3 \cdot 39 = 2^2 \cdot 3^2 \cdot 13$
so the largest common factor we can build is $3 \cdot 13 = 39$. What we knew from last time was that the largest common factor (what we will from now on call the *greatest common divisor* or *GCD* to remain in line with what everybody else says) could be at most 39, since anything that divides both 1131 and 468 must divide all linear combinations, in particular, 39. But the calculations above also already tell us that 39 divides both 1131 and 468. The last equation shows that 39 divides 78, the previous remainder before 39. Then the next equation up, since 39 divides both 78 and 39, tells us that 39 divides 195 (as a linear combination of 78 and 39). Then the next line up says that 468, a linear combination of 195 and 78, is divisible by 39; and the first equation then says that 1131, a linear combination of 468 and 195, is divisible by 39, as well!

We can see that this holds more generally. If we apply the Euclidean algorithm to numbers a and b, repeatedly using long division of the previous divisor by the previous remainder to create a new remainder, then the last positive remainder r that we create will be a linear combination of a and b, and so $\gcd(a,b) \le r$; but as we saw above r will divide all previous remainders, and so will divide both a and b, so r <u>is</u> a divisor of a and b, and so $r \le \gcd(a,b)$. But since the only way to be both smaller and bigger than another number is to <u>be</u> that number, we can conclude that $r = \gcd(a,b)$.

In particular, the smallest positive linear combination of a and b is the <u>same</u> as the greatest common divisor of a and b. And the last remainder standing when we run the Euclidean algorithm on a and b is this common value.

At this point, we took a little side-trip, since our computation of (what we can now recognize as) $\gcd(1131,468) = 39$ had the rather interesting additional feature that all of the quotients we encountered were 2. It turns out that one can use this list of quotients to build an interesting representation of the quotient $\dfrac{1131}{468}$ [and which will also teach us some useful notation].

$1131 = 468 \cdot 2 + 195$ can be rewritten as $\dfrac{1131}{468} = 2 + \dfrac{195}{468}$.

The '2' we get as quotient is the 'integer part' of the fraction $x = \dfrac{1131}{468}$, the largest integer that isn't bigger than it. It is often denoted $2 = \lfloor \frac{1131}{468} \rfloor$. The remainder, $\dfrac{1131}{468} - 2 = \dfrac{1131}{468} - \lfloor \frac{1131}{468} \rfloor = \dfrac{195}{468}$ is called the 'fractional part' (it is $x - \lfloor x \rfloor$). The next equation,

$468 = 195 \cdot 2 + 78$, can be written $y = \dfrac{468}{195} = 2 + \dfrac{78}{195}$

which expresses y as $\lfloor y \rfloor + (y - \lfloor y \rfloor)$, it's integer and fractional part. But y here is the reciprocal of the fractional part of x! This pattern continues through the Euclidean algorithm for any pair of integers a and b: At the first step the quotient is $q = \lfloor \frac{a}{b} \rfloor$, with remainder $r = a - bq$ (i.e., fractional part $\dfrac{r}{b} = \dfrac{a}{b} - q = \dfrac{a}{b} - \lfloor \frac{a}{b} \rfloor$). Then one continues with the reciprocal of the fractional part, $\dfrac{b}{r}$ (which is now greater than 1) and repeat the process! So one can implement the Euclidean algorithm as repeated use of the 'integer part' function $\lfloor x \rfloor$, subtraction, and taking reciprocals. It ends when there is no fractional part left.

The intriguing part of our calculation of $\gcd(1131,468) = 39$ was that all of the integer parts we saw were 2. This leads to an interesting expression for $\dfrac{1131}{468}$:

We have: $\dfrac{1131}{468} = 2 + \dfrac{195}{468}$ $\quad \dfrac{468}{195} = 2 + \dfrac{78}{195}$ $\quad \dfrac{195}{78} = 2 + \dfrac{39}{78}$ $\quad \dfrac{78}{39} = 2$

Putting these all together, we find that

$$1131/468 = 2 + [195/468] = 2 + 1/(468/195) = 2 + 1/(2 + [78/195])$$
$$= 2 + 1/(2 + 1/(195/78)) = 2 + 1/(2 + 1/(2 + [39/78])) = 2 + 1/(2 + 1/(2 + 1/2)))$$

This looks much more interesting if you don't try to fit it on a single line!

$$\frac{1131}{468} = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2}}}$$

This kind of expression is known as a *continued fraction*: the typical form is $\dfrac{m}{n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \frac{1}{a_k}}}}$. A common shorthand notation for this: $[a_0, a_1, a_2, \ldots, a_k]$.

And the Euclidean algorithm can be used to build it! You can even build continued fractions for numbers that aren't quotients of integers (i.e., *rational* numbers), although then the expression will not 'terminate'. A quick jump onto the web found us an (infinite) continued fraction for the famous number $e = 2.718281828459045\ldots$:

$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, \ldots]$

which displays far more of a pattern than anyone previously would have expected. This brought up the question of what is so important about the number e, which your instructor did a not terribly good job of answering (because a precise answer requires dragging in too much higher mathematics). But you will find the number e (and the exponential function e^x) quite literally all over the place, in the physical sciences, economics, and certainly throughout mathematics, most often where the rates of change of quantities are important.

We then had some fun with a one-line implementation of the Euclidean algorithm (using the floor function) that your instructor typed up in Maple 15, to watch the greatest common divisors of pairs of numbers being computed in 'real time'. These computations appeared blazingly fast, even when we tried to crash the computer by feeding it pairs of numbers with 100 and more digits. This prompted our thought question for next Tuesday: how fast shuld we 'expect' the Euclidean algorithm to be?

Computing gcd's (as, technically, smallest linear combination) is all well and good, but we should try to get back to our main goal: stalking big primes. Can they help us to do that? Can they help us find factors of numbers, or tell us that a number has no <u>proper</u> factors (which we defined to mean factors of n other than the 'obvious' ones, ± 1 and $\pm n$). The answer, we will see, is 'Yes'! We can see some of that by thinking about some of the compuations we watched the computer do; in under a second, it could tell us that the gcd of two 100-digit numbers was (as was often the case) 1. This means that the two numbers share no factors in common, other than ± 1. And the point was, it did this without knowing what the factors of the two numbers were. It in effect compared the two lists of proper factors of the numbers and discovered that there was no number common to both lists, without building either list! This is our first indication that what was asserted at the very beginning of the course was true: it is possible to obtain information about the list of factors of a number (like, there <u>are</u> proper factors) without knowing what the list <u>is</u> (i.e., without knowing any proper factors).

To stimulate discussion for Tuesday, we had the following question:

How fast is the Euclidean algorithm? How many times do we need to carry out long divisions starting from two numbers m and n, in order to compute their GCD?