Math 189H Joy of Numbers Activity Log

Tuesday, September 13, 2011

Bertrand Russell: "Math may be defined as the subject in which we never know what we are talking about, nor whether what we are saying is true."

Celia Green: "The way to do research is to attack the facts at the point of greatest astonishment."

Fact: Every integer from 1 to 100 can be expressed using four 4's together with mathematical operations ($+, -, *, /, \sqrt{}, !$, etc.)

We started by trying to express the number 67 as four 4's, without success. Then we returned to our plan for finding the smallest combination $na+mb$ of the integers n and m, and its relationship to the common divisors of n and m. We became still more convinced, based on still more examples, that the smallest positive number we could express this way and the largest common factor (what we will come to call the 'greatest common divisor', or 'gcd') are one and the same. For smallish (under 200?) numbers, we tended to find it to be quicker to determine this number by listing factors, and finding the common ones, but for larger numbers (137777771 ? 33339659 ?), finding the factors to compare in two lists appears to quickly get out of control! The key point we are headed for is that finding the smallest combination $na+mb$ can in practice be done much more quickly, and yet will allow us to compute the gcd (i.e., in some sense, find factors!).

Our idea was to take multiples of a number we could express as a combination (this takes too long to write!, let's just call such a number 'a combination'), until we got close to another combination, and then subtract the two; this will yield another, smaller, combination that we can use the same way. We were able to see that such a process could not go on forever; we could not keep finding ever smaller numbers, because we are only looking for <u>positive</u> numbers, so it is like walking down the number line, always stepping (at least one unit) to the left, but with a "wall" called "0" in front of us. Eventually we have to stop! Although what does stopping <u>mean</u>? We will come back to that!

In the end though, we want a more straighforward process for carrying out this "find multiples and subtract" process. What we want is an <u>algorithm</u>, a step-by-step process with explicit procedures which, when given n and m, will unerringly produce the smallest combination of them. To do this, we want to specify, at each step, which numbers to be using as the one to take multiples of and the one to subtract from. sice we start with two ready-made combinations of n and m, namely n and m (!), it seems reasonable use them to begin with. Since it certainly doesn't pay to take the larger one and take mulltiples (the mutiples keep getting farther away from the other), we will start with the smaller, which, WOLOG [which stands for 'without loss of generality', i.e., it doesn't really matter, any other possibility amounts to changing the names of things] is m, we then take multiple of m until we are close to n. [Note that some people use 'WLOG' in place 'WOLOG'!] Basically, we are starting at 0 and taking m-sized steps to the right, until we are close to n. There will be an integer a so that

$$ma \leq n < m(a+1)$$

and any other multiples will be farther away. Being lazy mathematicians and wanting to get as small as we can as fast as we can, we will pick one of these two. Which one? This is a design decision, which we could settle in several ways. In some sense, ma is preferable, since it is essentially what long division would give us: For any integers n and m, we can, by division, find integers q (= 'quotient') and r (= 'remainder') so that

$$n = mq + r \text{ m with } 0 \leq r < m$$

mq is the largest multiple of m which stays below (or equal to) n. Then taking $r = n - mq$ gives a number that we can guarantee is a combination of n and m <u>and</u> is smaller than m.

The other option is to focus on the <u>smaller</u> of $n-mq$ and $m(q+1)-n$, i.e., use the multiple of m that is <u>closest</u> to n. This fits with our stated goal of getting smaller faster, and is a perfectly reasonable option in going forward. In order to express our steps most explicitly, we will adopt the first strategy ($n - mq = r$) in going forward.

We now know that $r =$ the remainder of n on division by m, is a combination. Now, repeat the process, using the <u>next</u> smallest combination that we know of, namely m. [Although it you think about it, $m - r = m(q+1) - n$ is probably even smaller? If we just want to know the smallest combination, this is probably faster, although we will shortly see that there is often more information that we want, which makes a more conservative course of action possibly preferable.]

That is, we now look at the remainder of m on division by r. since both m and r are combinations of n and m, this new remainder will be, too, and it will also be smaller than r. Since we are getting into the situation of wanting to talk about multiple remainders, it is time to start numbering them: we will write, symbolically,

$n = mq_1 + r_1$
$m = r_1 q_2 + r_2$
$r_1 = r_2 q_3 + r_3$

and so on. The idea is that repeating this process, since the numbers r_1 and r_2 are combinations, r_3 will be, too, and it will also be smaller than the previous remainder computed. We looked at this process with a specfic example:

For $n = 1331$ and $m = 177$, these steps went
$1331 = 177 \cdot 7 + 92$
$177 = 92 \cdot 1 + 85$
$92 = 85 \cdot 1 + 7$
$85 = 7 \cdot 12 + 1$
$7 = 1 \cdot 7 + 0$

We noted while doing this that in the first step it paid off to overshoot 1331:
$177 \cdot 8 - 1331 = 7$ gave a much smaller number to work with right away. [And as we noted, it doesn't hurt the search for a smallest combination to do this.] These computations tell us that 1 is the smallest positive number we can express as a combination of 1331 and 177, since there is no smaller positive number! We can also use these computations to tell us <u>how</u> to write 1 as a combination:

$92 = 1331 - 7 \cdot 177$ and so $85 = 177 - 1 \cdot 92 = 177 - 1 \cdot (1331 - 7 \cdot 177) = 8 \cdot 177 - 1 \cdot 1331$, and we can continue:

$7 = 92 - 1 \cdot 85 = (1331 - 7 \cdot 177) - 1 \cdot (8 \cdot 177 - 1 \cdot 1331) = 2 \cdot 1331 - 15 \cdot 177$,
and then
$1 = 85 - 12 \cdot 7 = (8 \cdot 177 - 1 \cdot 1331) - 12(2 \cdot 1331 - 15 \cdot 177) = 188 \cdot 177 - 25 \cdot 1331$.

We also could see a definite pattern in how our succession of long division calculations were carried out; the numbers were were dividing into (the dividend?) and the numbers we are dividing by (the divsor?) keep shifting left in our equations, with the new remainder becoming the new divisor, and then in the next step the dividend! This procedure is known as Euclid's Algorithm, and the last non-zero remainder is, we shall see, both the smallest positive combination of n and m and the greatest common divisor of n and m! We have already observed part of the reason for this; any number d that divides both n and m must divide r_1 (since it is a combination of n and m). But now d divides both m and r_1, so by the same reasoning it divides r_2. Now dividing r_1 and r_2 means it divides r_3, and so on... So anything that divides n and m divides all of the remainders. This means that r_k, our last positive remainder, is divisible by the gcd of m and n, and so is at least as big as it. I.e., $r_k \geq \gcd(n, m)$. The rest of the story will come next time!

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

Use our smallest-combination process to find the answers for the pairs of numbers (1131,468) , (1337,2011) , (49,94) .