Math 189H Joy of Numbers Activity Log

Thursday, September 29, 2011

Albert Einstein: "Everything should be made as simple as possible, but not simpler."

Alfred North Whitehead: "Civilization advances by extending the number of important operations which we can perform without thinking about them."

$1318820881^2 = 1739288516161616161$

The goal for today was to learn what we could learn from the calculations and procedures we developed in the past week! We had discovered that divisibility by 11 could be tested by cutting your number up into chunks of size 2 (from the right), adding them up, and asking the same question about that sum. And disibility by 13 could be answered by the same procedure, except we would use chunks of size 6. The point to both of these, in the end, was that $10^2 \underset{11}{\equiv} 1$ and $10^6 \underset{13}{\equiv} 1$. For a number of size less than the chunk size, by finding the remainders of all of the powers of 10 on division by our divisor of interest up to the chunk size, we could replace our number by a sum (of small products), and test that number instead.

All of this required us to compute the remainders of products and sums of numbers. Being good lazy matheamticians, we wanted to know, is there a quicker way to do this? Last time we learned that congruence behaves well under products: if $n \underset{d}{\equiv} m$ and $a \underset{d}{\equiv} b$, then $na \underset{d}{\equiv} mb$. [NOTE THAT THIS IS RIGHT, WHAT WAS IN THE PREVIOUS LOG WAS WRONG!] And true to form, we could see that addition and subtraction work well, as well. If $n \underset{d}{\equiv} m$ and $a \underset{d}{\equiv} b$, then $n+a \underset{d}{\equiv} m+b$ and $n-a \underset{d}{\equiv} m-b$. The reasoning is very much the same: since $n = m + dx$ and $a = b + dy$, then $n + a = (m + b) + d(x + y)$, and $n - a = (m - b) + d(x - y)$. What these mean for us is that, if all we care about is what remainder some number has on division by d, where the number is built out of other numbers by various arithmetical operations, then we can replace all of the numbers going into the calculations with their remainders first, without changing the remainder of the outcome.

So, for example, when we were building our table of powers of 10, computing the remainders in order to find the size of the chunk to use, we didn't need to compute 10^5, say, and then find the remainder on division by 13; instead we could have used the fact that we knew that 10^4 had remainder 3, multiplied that by 10 to get 30, found its remainder, 4, and concluded that $10^5 \underset{13}{\equiv} 4$. This observation also prompted us to remember that taking powers is an arithmetic operation, too, sort of, and to note that congruence likes exponentiation, too: If $n \underset{d}{\equiv} m$ then for any positive integer k we have $n^k \underset{d}{\equiv} m^k$. In discussing this, we could see why it ought to be true: taking powers is really repeated multiplication, and congruence likes multiplication, so surely it likes repeated multiplication?! A formal justification of this will need a new tool in our toolkit (the relevant word is 'induction'), which we will take up sometime later. But back to powers of 10...

A part of all of our divisibility tests required us to find a power 10^k of 10 that was congruent to 1 modulo the number n whose divisibility test we were constructing. The question is, how do we find that k? We could do what we had always done, starting with $10^0 = 1$ and continuing up until we found it. Sometimes, we could stumble across it by combining values we had previously determined, by the new rules we have learned about congruence. For example, playing with (I think) $n = 23$, we found that $10^2 \equiv 8$, so $10^3 \equiv 80 \equiv 11$, so $10^6 = (10^3)^2 \equiv 11^2 = 121 \equiv 6$, and $10^5 = 10^2 \cdot 10^3 \equiv 88 \equiv 19 \equiv -4$, so $10^{11} \equiv (6)(-4) = -24 \equiv -1$, so $10^{22} \equiv (-1)^2 = 1$. This, and other calculations, prompted us to ask, for a given modulus n, what is the smallest k so that $10^k \equiv 1 \bmod n$? After playing for awhile, we noted that some numbers aren't allow to play at all: if $2|n$, then $10^k = 1 + nt$ can only happen for $k = 0$, since otherwise we have $2|10^k$ (since $2|10$) but $1 + nt$ would leave remainder 1 on division by 2. So multiples of 2 are out of luck. For the same reason (since $5|10$), multiples of 5 can't play.

At this point we decided we needed some <u>real</u> data, so we fired up Maple and had it spit out, for whatever modulus n we fancied, what the smallest values of k were so that $10^k \equiv 1 \bmod n$. Assuming your instructor remembered the numbers we fed in correctly, here is (some of) the data we generated:

$n = 73$, then $k = 8, 16, 24, 32, 40, 48, 56, 64, 72, 80$
$n = 41$, then $k = 5, 10, 15, 20, 25, 30, 35, 40, 45, 50$
$n = 17$, then $k = 16, 32, 48, 64, 80$
$n = 1001$, then $k = 6, 12, 18, 24, 30$
$n = 1003$, then $k = 464, 928$
$n = 997$, then $k = 166, 332, 498, 664, 830, 996$
$n = 91$, then $k = 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90$
$n = 23$, then $k = 22, 44, 66, 88$
$n = 27$, then $k = 3, 6, 9, 12, 15, 18, 21$
$n = 29$, then $k = 28, 56, 84$
$n = 31$, then $k = 15, 30, 45, 60$
$n = 129$, then $k = 21, 42, 63, 85, 105, 126$
$n = 139$, then $k = 46, 92, 138$
$n = 141$, then $k = 46, 92, 138$ (interesting coincidence, that!)
$n = 541$, then $k = 540, 1080$
$n = 1137$, then $k = 378, 756, 1134$
$n = 49$, then $k = 42, 84, 126$
$n = 77$, then $k = 6, 12, 18, 24, 30, 36, 42, 48, 60, 66, 72, 78$
$n = 99$, then $k = 2, 4, 6, 8, 10, 12, 14, 16, 18, 20$

and lots of other examples were considered, as well (we were having fun...) OK, so what do these numbers tell us? Well, first, so long as we searched far enough, we never failed to find such values of k ! (And so long as we avoided multiples of 2 or 5.) We didn't really pick up on this point at the time, but it is an important thing to think about; we always <u>found</u> what we went out looking for. Why was it always out there to be found? We should come back to this point sometime!

But at the moment we are after finding the smallest k, for a given n, so that $10^k \equiv 1 \mod n$. What we found was that these numbers bounce all over the place. We'd like the smallest number, since from our original motivation it represents that smallest chunk size we would need to use to test for divisibility by n. But it is hard to see how to predict that smallest number. Then we noticed that sometimes the smallest exponent that works for n is $n-1$; this is true for $n = 17, 23, 29, 97$, and 541, for example. Staring at the data some more, with $n-1$ on our minds, we noted that many times $n-1$, while not being the <u>smallest</u> exponent that works, at least <u>is</u> an exponent that works. This is true, in our data set, for

$n = 17, 23, 29, 31, 41, 73, 91, 99, 139, 541, 997$

but it was not true (if we extended our list high enough to see!) for

$n = 49, 77, 129, 141, 1001, 1003, 1137$

We also found that we could use the values of k we have to decide whether or not $10^{n-1} \equiv 1 \mod n$, in the cases where our list didn't extend far enough. For example, since $10^2 \equiv 1 \mod 99$, we know that $10^{98} = 10^{2\cdot 49} = (10^2)^{49} \equiv 1^{49} = 1$, as well, and since $10^6 \equiv 1 \mod 1001$, we know that $10^{1000} = 10^{6\cdot 166+4} = (10^6)^{166} \cdot 10^4 \equiv 1^{166} \cdot 10^4 = 10^4$, which is <u>not</u> congruent to 1 modulo 1001 (since it didn't appear on our list ahead of 6).

The 64 dollar question is, what distinguishes the numbers on one list from the ones on the other? Initially we got quite excited, since the numbers on the first list appear to be prime? (well, we would have been, maybe, if $91 = 7 \cdot 13$ hadn't been one of the first numbers we discovered that belonged on this list...). But upon further reflection, and some juducious application of calculator time, we found that <u>every</u> number on our second list <u>isn't</u> prime! For example, $1001 = 7 \cdot 11 \cdot 13$, $1003 = 17 \cdot 59$, and $1137 = 3 \cdot 379$. This seems very suggestive... We were left with the impression that if $10^{n-1} \equiv 1 \mod n$ then n is "usually" prime, and if $10^{n-1} \not\equiv 1 \mod n$ then n is <u>not</u> prime. [Here $\not\equiv$ means "not congruent to", using the standard mathematical laziness that a slash through a symbol means "not". Which makes $\not<$ a fun way to write $\geq$!]

The fact that $n = 91 = 7 \cdot 13$ appeared on the "wrong" list prompted your instructor to try to 'explain' this: The point is that $10^6 \equiv 1 \mod 7$, as we discovered when we built our divisiblity by 7 test, and in fact $10^6 \equiv 1 \mod 13$, too, as we discovered last time. (Our grand picture would have predicted 10^{12}; apparently $n = 13$ does better than that.), This means that $10^{60} = (10^6)^{10} \equiv 1^{10} = 1$ modulo both 7 and 13, and it is only a little bit of a stretch (?) to believe that this means that $10^{60} \equiv 1$ modulo their product, as well... These and other explorations will need to wait for next time!