Math 189H Joy of Numbers Activity Log

Thursday, October 20, 2011

Bertrand Russell: "In all affairs it's a healthy thing now and then to hang a question mark on the things you have long taken for granted."

Winston Churchill: "Success is the ability to go from one failure to another with no loss of enthusiasm."

Today we returned to our old conjecture: *If p is prime and relatively prime to 10, then $10^{p-1} \underset{p}{\equiv} 1$. (I.e., $p | 10^{p-1} - 1$.)* [If n is <u>not</u> relatively prime to 10, then <u>usually</u> $n \not| 10^{n-1} - 1$.] With our recent discoveries, this looked more like it was within reach now!

Before starting on the road to showing this, we looked at some tables of powers modulo n for n from 2 to 21, to see if there was even more we could expect to be true. What we noticed first was that for all of the *prime* moduli n in the table, there was nothing really special about 10 at all; for every number a from 1 to $n-1$ we saw that $a^{n-1} \underset{n}{\equiv} 1$ (if n was prime).

If n was not prime, then this turned out not to be true; in fact, rarely (never?) was $a^{n-1} \underset{n}{\equiv} 1$ for any a (except $a = 1$ (!)). But we were able to spot still more patterns: If we looked for 1's in the table (meaning pairs of moduli n and exponents k so that so that $a^k \underset{n}{\equiv} 1$ holds for more a's than usual), we found that, for example,

for $n = 14$, $a^6 \underset{n}{\equiv} 1$ for $a = 1, 3, 5, 9, 11, 13$
for $n = 15$, $a^4 \underset{n}{\equiv} 1$ for $a = 1, 2, 4, 7, 8, 11, 13, 14$
for $n = 16$, $a^4 \underset{n}{\equiv} 1$ for $a = 1, 3, 5, 7, 9, 11, 13, 15$
for $n = 18$, $a^6 \underset{n}{\equiv} 1$ for $a = 1, 5, 7, 11, 13, 17$

In trying to find a pattern to these collections of numbers, we eventually took our lead from the list for $n = 16$: it consists of all of the odd numbers. In other words, it consist of all of the number except the even ones! Looking at the other lists, paying attention to what is <u>missing</u>, we found that

for $n = 14$, the missing numbers are $0, 2, 4, 6, 7, 8, 10, 12$
for $n = 15$, the missing numbers are $0, 3, 5, 6, 9, 10, 12$
for $n = 16$, the missing numbers are $0, 2, 4, 6, 8, 10, 12, 14$
for $n = 18$, the missing numbers are $0, 2, 3, 6, 8, 9, 10, 12, 14, 15, 16$

In these lists we could see that every number shares a factor in common with the modulus n. Looking closer, the previous lists (with powers congruent to 1) each consist of precisely the numbers which are relatively prime to the modulus. But when we are dealing with a prime p, the numbers from 1 to $p-1$ (whose $p-1$st powers are, we think congruent to 1) <u>also</u> consists of precisely the numbers relatively prime to p. So the overall pattern appears to be: *for every modulus n, there is an exponent k so that, for every number a relatively prime to n, we have $a^k \underset{n}{\equiv} 1$. Further, if n is prime, then that exponent can be chosen to be $n-1$.* [We don't yet know what the exponent might be for non-prime n.]

To prove this, we can break it down into, it seems, three pieces. First, if $\gcd(n, a) = 1$, then $a^k \underset{n}{\equiv} 1$ for some exponent $k > 0$. Second, for all of the numbers relatively prime to n, there is a single exponent k that works for all of them. Finally, for n prime, the exponent $n-1$ will, in fact, always work.

To show the first part, we can think of taking a single number a, and look at the string of powers $1 = a^0, a = a^1, a^2, a^3, \ldots$, looking at their remainders modulo n, giving us a string of numbers $1 = a_0, a = a_1, a_2, a_3, \ldots$ all lying between 0 and $n-1$. The thing is, that since the list runs on forever, we realized that it must eventually start to repeat itself. A formal statement of this goes by the name of the *Pigeonhole Principle*: If you are given n buckets, and told to put n things into them, without ever putting two things into the same bucket, then you will have to put exactly one thing into each bucket. In particular, every bucket will have something in it. The same idea says that if somebody gives you more than n things and n buckets to put them in, you will have to put more than one thing into at least one of the buckets. [This can be proved (by induction!) from the original statement of the principle.] If we think of 'have the same remainder on division by n' (i.e., are congruent to one another modulo n) as our buckets, then since there are only n possible values for the remainder, we have n buckets. Since we can keep taking higher powers all we want, we could conclude that among the powers $1 = a^0, a = a^1, a^2, \ldots a^n$, two of them must land in the same bucket, i.e., $a^k \underset{n}{\equiv} a^{k+i}$ for some k and $k+i$ between 0 and n (with $i > 0$).

An important observation made at this point was that for the numbers we are looking at, with a relatively prime to n, one of the buckets that cannot have an a^k in it is the one labeled 0; if $n|a^k = a(a^{k-1})$, then since $\gcd(n, a) = 1$, we must have $n|a^{k-1}$. But so long as we have a positive number of a's we can keep peeling another one off, yielding, in the end $n|a$, which is absurd (since then $\gcd(n, a) = n$). So in our argument above we actually can pretend that we have $n-1$ buckets, not n. This will be a very useful observation later on!

But at this point what we know is that a^k and a^{k+i} have the same remainder on division by n, meaning that $n|a^{k+i} - a^k$. But how does this help us find a power of a congruent to 1 modulo n? We can take a clue from that previous observation! $a^{k+i} - a^k$ has factors of a in it: $a^{k+i} - a^k = a^k(a^i - 1)$. By the same reasoning as our previous observation, since $n|a^k(a^i - 1)$ and $\gcd(n, a) = 1$, we can peel off each of the factors of a one by one, using our result that dividing a product but being relatively prime to one factor implies that you must divide the other factor. This leaves us, in the end, with $n|a^i - 1$, which is precisely what our first part asserts! [Note that this also implies that the first time that our list of powers repeats itself, it is when a 1 appears for the second time (after a^0).]

With the first part in hand, we turned to the second part. If we list every number between 1 and $n-1$ that is relatively prime to n, as $a_1, \ldots, a_r$, then we now know that each one of them has an exponent k_i so that $a_i^{k_i} \underset{n}{\equiv} 1$. How then do we show that there is a single exponent that works for all of them? Our clue came from wondering what <u>other</u> powers of a_1, say, we could guarantee are congruent to 1. Since we had previously shown that if $a \underset{n}{\equiv} b$ then $a^k \underset{n}{\equiv} b^k$, and $1^k = 1$ for any k, we quickly realized that if $a_1^{k_1} \underset{n}{\equiv} 1$, then

$(a_1^{k_1})^2 = a_1^{2k_1} \underset{n}{\equiv} 1^2 = 1$, and, even more, that $a_1^{k_1 s} \underset{n}{\equiv} 1$ for any positive integer s. So, for example, $a_1^{k_1 k_2} \underset{n}{\equiv} 1$ and $a_2^{k_2 k_1} = a_2^{k_1 k_2} \underset{n}{\equiv} 1$, as well. From there it was a short walk to the realization that if we set $k = k_1 \cdots k_r$, then $a_i^k \underset{n}{\equiv} 1$ for every single integer a_i, i.e., for every integer between 0 and n that is relatively prime to n. This gives us our second part; there is positive integer k so that, whenver $\gcd(n, a) = 1$, then $a^k \underset{n}{\equiv} 1$.

But our arguments above give us no clue how to determine what this integer k <u>is</u> (other than by following the prescription above, finding each k_i in turn) In particular, we will (eventually) be interested in knowing what the <u>smallest</u> k is that works for every a relatively prime to n (or, at least, how to identify a small(ish) k...). This we will take up next time!