Math 189H Joy of Numbers Activity Log

Tuesday, October 25, 2011

Winston Churchill: "Men occasionally stumble over the truth, but most of them pick themselves up and hurry off as if nothing ever happened."

Anonymous: "There are 10 *kinds of people in the world; those who understand binary arithmetic and those who don't."*

Unsolved problem: Can 33 be expressed as the sum of three perfect cubes? Is $33 = a^3 + b^3 + c^3$? [Note: it is known that if it can be, then at least one of a, b, c must be at least 10^{14}...]

Today our goal was to finish our (twice refined) conjecture: *If n is prime and a is relatively prime to n, then $a^{n-1} \underset{n}{\equiv} 1$.* (I.e., $n|a^{n-1} - 1$.) Last time we showed that there was some exponent k that worked, and that we didn't really need n to be prime to do that. Our goal for today is to identify an exponent that will work for any given modulus n, and show why it works! To do this, we started by looking at the moduli n from 2 through 16, listing both the numbers relatively prime to n and the exponents k (less than n: we showed last time that for any one a such a 'smallish' k works, although we don't really know that one will work for all a...) that 'work' for all of them, drawn from our tables of powers mod n, in the hopes of discovering a usable pattern:

$n = 2$: $a = 1$: $k = 1$
$n = 3$: $a = 1, 2$: $k = 2$
$n = 4$: $a = 1, 3$: $k = 2, 4$
$n = 5$: $a = 1, 2, 3, 4$: $k = 4$
$n = 6$: $a = 1, 5$: $k = 2, 4, 6$
$n = 7$: $a = 1, 2, 3, 4, 5, 6$: $k = 6$
$n = 8$: $a = 1, 3, 5, 7$: $k = 2, 4, 6, 8$
$n = 9$: $a = 1, 2, 4, 5, 7, 8$: $k = 6$
$n = 10$: $a = 1, 3, 7, 9$: $k = 4, 8$
$n = 11$: $a = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$: $k = 10$
$n = 12$: $a = 1, 5, 7, 11$: $k = 2, 4, 6, 8, 10, 12$
$n = 13$: $a = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$: $k = 12$
$n = 14$: $a = 1, 3, 5, 9, 11, 13$: $k = 6, 12$
$n = 15$: $a = 1, 2, 4, 7, 8, 11, 13, 14$: $k = 4, 8, 12$
$n = 16$: $a = 1, 3, 5, 7, 9, 11, 13, 15$: $k = 4, 8, 12, 16$

What patterns could we see? We noticed that all of the exponents (well, except for the first one!) were even. We also noticed that the exponents that work in each row are all multiples of the smallest one in each row; this is an important observation that we will return to (and exploit) later! Looking at the lists of a's, we eventually noted that (again, except for the first row) the number of a's in each row is also always even. Looking still deeper, with a little nudge from your instructor (although in your defense, presenting the same evidence later to one of my fellow faculty members, that person really didn't hit upon the pattern, either...), we noted that the number of a's relatively prime to n was in the list of exponents k that work for n. This surely is too weird to be a coincidence (and you can verify that it happens for still more); moreover, it is consistent with our original conjecture, since for a prime p there are $p-1$ numbers between 1 and p (namely, 1 through $p-1$) that are relatively prime to p, and the exponent we expected to work in those cases was $p-1$. So we now made a new (thrice refined) conjecture, adopting the notation

$\phi(n)$ = the number of a's between 1 and n with $\gcd(n,a) = 1$; ϕ is called the *Euler phi-function* (or *Euler totient function* [I looked up the definition of 'totient', but it was completely meaningless to me; it is essentially a made-up word from the 1880's?]);

Conjecture: For any positive integer n and integer a with $\gcd(n,a) = 1$ we have $a^{\phi(n)} \underset{n}{\equiv} 1$.

Which leaves us the task of showing this! To do that, we turned to our lists of multiplication tables modulo n (for underhanded reasons known only to your instructor), and looked at multiplications of a's relatively prime to n with one another. Extracting some lines from each, where for a modulus n and a number a rel prime to n, we listed products of a with the other numbers rel prime to n, we found:

for $n = 14$, $a = 1$, the products were $1, 3, 5, 9, 11, 13$ (i.e., the numbers a in order)
for $n = 14$, $a = 3$, the products were $3, 9, 1, 13, 5, 11$
for $n = 14$, $a = 11$, the products were $11, 5, 13, 1, 9, 3$
for $n = 14$, $a = 13$, the products were $13, 11, 9, 5, 3, 1$

for $n = 15$, $a = 1$, the products were $1, 2, 4, 7, 8, 11, 13, 14$
for $n = 15$, $a = 8$, the products were $8, 1, 2, 11, 4, 13, 14, 7$

for $n = 6$, $a = 1$, the products were $1, 5$
for $n = 6$, $a = 5$, the products were $5, 1$

From this data we rather quickly noted a definite pattern: each set of products is just the list of a's rel prime to n, written in a different order. Analyzing this further, and in particular trying to formulate statements which would imply this, we could break this statement down into two pieces. First, every number that appears on the list is rel prime to n; second, every number appears exactly once. With the pigeonhole principle in mind, though, we realized that the second statement is really the same as saying that no a appears on the list <u>twice</u>; since we are fitting $\phi(n)$ things (the multiples of a) into $\phi(n)$ buckets (which value we get), knowing we don't get the same value twice implies that every bucket has something in it, that is, every number rel prime to n appears (exactly once)!

But these are things we can handle! The first essentially says that if $\gcd(n,a) = 1 = \gcd(n,b)$, then $\gcd(n,ab) = 1$ as well. But if $\gcd(n,ab) = d > 1$ (usng the tried and true method of giving ourselves enough room to get ourselves into trouble), then $d|n$ and $d|ab$. We would <u>like</u> to then say (since it sounded so familiar) that then $d|a$ or $d|b$, but that only worked for d a prime. But d does have a prime factor $p > 1$. And then since $p|d$ we know that $p|n$ and $p|ab$, so we do have $p|a$ or $p|b$. But then either $\gcd(n,a) \geq p$ or $\gcd(n,b) \geq p$, both of which get us into trouble! So we must have $\gcd(n,ab) = 1$. That gives us our first assertion.

For the second, if we suppose that for a with $\gcd(n,a) = 1$ and, for two other numbers $1 \leq a_i, a_j \leq n-1$ relatively prime to n, we have $aa_i \underset{n}{\equiv} aa_j$, then this means that $n|aa_i - aa_j =$

$a(a_i - a_j)$. But then since $\gcd(n, a) = 1$ we must have $n|a_i - a_j$. But since both a_i and a_j are small, $a_i - a_j$ lies between $1 - n$ and $n - 1$. And there is only one multiple of n in that range, namely 0. So $a_i - a_j = 0$, i.e., $a_i = a_j$, as we wanted.

So now we know that for any n and a relatively prime to n, if $a_1, \ldots, a_\ell$ are the numbers between 1 and n that are relatively prime to n, then, modulo n, the numbers $aa_1, \ldots, aa_\ell$ are really the numbers $a_1, \ldots, a_\ell$ (possibly) written in a different order. But so what? How does that help us show that $a^\ell \underset{n}{\equiv} 1$? The point is that we now have two different ways to write the same collection of numbers, and one of those ways (as the multiples of a) has ℓ a's in it! With this observation, motivated by the fact that we are looking for a way to build a^ℓ (so that we can say something about it), to build a^ℓ from ℓ numbers that have a's in them, we just multiply them together. What we get (because we know that congruence modulo n 'likes' multiplication) is that

$$(aa_1)\cdots(aa_\ell) = a^\ell(a_1 \cdots a_\ell) \underset{n}{\equiv} a_1 \cdots a_\ell$$

since what order you multiply things together does not affect the resulting product. This then says that $n|a^\ell(a_1 \cdots a_\ell) - (a_1 \cdots a_\ell) = (a^\ell - 1)(a_1 \cdots a_\ell)$. But this is familiar territory for us now! Each of the a_i are relatively prime to n, so we could peel off each one in turn from the product, knowing that n will divide what we left behind. [A more orderly way to express this is that an induction argument (on ℓ) will show that since each a_i is rel prime to n, then $a_1 \cdots a_\ell$ is rel prime to n; the inductive step is really the argument given three paragraphs up!] The result is that since each of the a_i are rel prime to n, we are left with $n|a^\ell - 1$, i.e., $a^\ell \underset{n}{\equiv} 1$, which is precisely what our conjecture stated! So our conjecture is proved! The result we have now established is known as *Euler's Theorem*:

For an integer n, if $\phi(n) =$ the number of integers between 1 and n that are relatively prime to n, then for any a with $\gcd(n, a) = 1$ we have $a^{\phi(n)} \underset{n}{\equiv} 1$.

All that is left now is to lean back and reap the many rewards of this result. Which we will begin to do next time.