Math 189H Joy of Numbers Activity Log

Tuesday, November 8, 2011

Steven Wright: "You can't have everything. Where would you put it?"

Albert Einstein: "Do not worry about your difficulties in Mathematics. I can assure you mine are still greater.'

132=12+13+21+23+31+32. It is the smallest number equal to the sum of all of the rearrangements of pairs of its digits.

Today we returned to further considerations stemming from Euler's Theorem:

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

Two questions which come to mind, prompted partly by observations we made in the process of formulating and proving this result, are:

How can we actually <u>compute</u> $\phi(n)$? Is there a 'formula' for it?

What more can we say about the values of k so that $a^k \underset{n}{\equiv} 1$ for all a relatively prime to n?

The second question was motivated by our observation that, to the extent that our tables of powers ran, for a fixed n the collection of k that worked for all a with $\gcd(a, n) = 1$ were always the multiples of a particular k (that, it turned out, was <u>not</u> always the value $\phi(n)$; sometimes (like $n = 8$ and $n = 16$) still smaller values worked). But we felt confident enough to conjecture:

If k is the smallest positive integer so that $a^k \underset{n}{\equiv} 1$ for all a rel prime to n, then for any other m with $a^m \underset{n}{\equiv} 1$ for all a rel prime to n, we must have $k|m$.

The question was, how to prove this? How do we show that k must divide m? That is, how do we show that $m = k\ell$ for some integer ℓ. Prompted by the (general) question "How do you show something is true when you don't know how to show that it is true?", our immediate response was "by induction!"; but kicking this idea around a little bit, we concluded that knowing about powers mod $n-1$ probably wasn't going to tell us much about powers mod n (by looking at our lists of k's that 'worked'). On the other hand, there did seem to be some kind of correlation between what worked for n and what worked for factors of n, suggesting that some kind of complete induction might work? But then it seemed like primes (having no proper factor) would sort of have to be treated individually, and so this didn't feel like it was going to lead us to a solution.

So we went back to the original statement and, thinking for a bit, concluded that whatever m is, we can at least divide k into it, giving $m = k\ell + r$ for some r with $0 \leq r \leq k - 1$. And what we really want to show is that $r = 0$, so that $k|m$. But given what we know, namely that $a^m \underset{n}{\equiv} 1$ and $a^k \underset{n}{\equiv} 1$ we found that, using what we know about exponentiation (and how sums and products of exponents behave)

$$1 \underset{n}{\equiv} a^m = a^{k\ell+r} = a^{k\ell}a^r = (a^k)^\ell a^r \underset{n}{\equiv} 1^\ell a^r = a^r$$

so $a^r \underset{n}{\equiv} 1$ (where in the middle of that computation we used that $b \underset{n}{\equiv} c$ implies $b^\ell \underset{n}{\equiv} c^\ell$). But r is smaller than k, which was supposed to be the smallest positive exponent that worked! The only conclusion we can draw is that, since r works, it can't be positive! Meaning that $r = 0$, wich is precisely what we needed to show. So the exponents that work ($a^m \underset{n}{\equiv} 1$ for all a rel prime to n) are all multiples of the smallest one that works. In particular, since we know $\phi(n)$ works, the smallest one must be a factor of $\phi(n)$. [It is worth noting that the same reasoning applies if you are looking for the exponents that work for a single base a, or a particular collection of bases (all rel prime to n); the exponents that work will all be multiples of the smallest one that works.]

So in the end, if we wanted to find the smallest exponent that works, we "only" need to look at the factors of $\phi(n)$, because <u>that</u> exponent always works. Which brings us to our second/first question; how can we really compute $\phi(n)$? If n is very large, we probably don't want to use our definition to do it; we would have to test every number from 1 to n for relative primalitousness (primality?), which we can do, one by one, using the Euclidean algorithm!, but which would still take a very long time. Instead, we tried to find patterns in the values of $\phi(n)$ which would enable us to compute it faster. So we had Maple 15 generate a list of paris of values $(n, \phi(n))$ to stare at, and looked for patterns. What we noted (over time) was:

Except for $n = 2$, all of the values of $\phi(n)$ are even.
If n is prime, then $\phi(n) = n - 1$. [We had shown this earlier.]
$\phi(n)$ is never 14 (!). Looking further, we also suspected that $\phi(n)$ is never 26?
Looking at powers of 2, we thought that $\phi(2^n) = 2^{n-1}$.
In the same vein, $\phi(3^n) = 2 \cdot 3^{n-1} = \frac{2}{3}3^n$.

This actually motivated a conjecture: If p is prime, then

$$\phi(p^n) = (1 - \frac{1}{p})p^n = (p-1)p^n,$$

which we effectively proved on the spot, by thinking about the numbers that <u>aren't</u> relatively prime to p^n; they are precisely the multiples of p between 1 and p^n, which is one in every p numbers (for a total of p^{n-1}), so $\phi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$, as desired. Still further observations:

If $n = 2m$ with m odd, then $\phi(n) = \phi(2m) = \phi(m)$.
More generally, if $n = 2^k m$ with m odd, then $\phi(n) = \phi(2^k m) = 2^{k-1}\phi(m) = \phi(2^k)\phi(m)$.

And finally, looking at the values of n that these observations still didn't 'explain' (namely non-prime odd numbers), we found that $\phi(15) = \phi(3\cdot 5) = 8 = \phi(3)\phi(5)$, $\phi(21) = \phi(3\cdot 7) = 12 = \phi(3)\phi(7)$, and $\phi(35) = \phi(5 \cdot 7) = 24 = \phi(5)\phi(7)$, which made us very suspicious that a still more general pattern is lurking out there! But at this point it was time to go do something else for awhile; we'll show that these observations are more generally true next time?