MONT 104Q – Mathematical Journeys: From Known To Unknown
Discussion Day 5
Proving the "power theorem" – November 4 and 6, 2015

Background

Last week, by gathering "a bunch of" data, we were able to *conjecture* (i.e. make an educated guess) that: *If m is a prime number and $r = 1, 2, \ldots, m-1$, then (using our invented notation for remainders)*:

$$r^{m-1}\, R\, m = 1. \tag{1}$$

(That is, we seem to be seeing that all the sequences of powers r^k for fixed r cycle back to 1 for $k = m-1$, even when there are smaller values of k for which $r^k\, R\, m = 1$ as well.)

This leads to some questions on the table for us: *Is this always true? Does it work for all prime numbers m? Can we prove that? And maybe also, if we're feeling ambitious, what exactly is the pattern when m is not a prime number?* There seem to be similar things going on, at least for some r's even when m is not prime, but cycling back to 1 doesn't happen for $m-1$ – it happens for already for smaller exponents. *What are those exponents?*

The following ideas will be useful to develop a proof of the statement (1) above, and your goal is to put these ingredients together into a reasonably complete explanation for why (1) holds for *all primes m*.

Questions

A) First, explain why (1) is equivalent to saying that $r^{m-1} - 1$ is a *multiple of m* (i.e. equals m times some integer).

B) Suppose we take any fixed r in the collection $1, 2, \ldots, m-1$ and multiply it by each of $1, 2, 3, \ldots m-1$, then take remainders on division by m. Do we ever get the same remainder twice? Why or why not? In other words, are the remainders

$$r\, R\, m, (2r)\, R\, m, (3r)\, R\, m, \ldots, ((m-1)r) R m$$

all different, or could we ever get the same remainder twice? Why? (Hint: Generalizing from what you were doing in question A, saying $a\, R\, m = b\, R\, m$ is the same thing as saying that $b - a$ is a multiple of m, or equivalently that m divides $b - a$ evenly.)

C) What happens if we compute this remainder of a product

$$(r)(2r)(3r)\cdots((m-1)r)\, R\, m?$$

On the one hand, we could say it's equal to $(r^{m-1}(m-1)!)\, R\, m$ by rearranging the factors. (That exclamation point is the *factorial* of $m-1$ – it's a shorthand way of writing the product:

$$(m-1)! = (m-1)\cdot(m-2)\cdots 3\cdot 2\cdot 1.)$$

But what does your result from question B) say about this? If the remainders $r\,R\,m, \ldots, (m-1)r\,R\,m$ are all different, what do they have to be? (You might want to try a couple of examples to understand the question and see the pattern!)

D) Now can you finish off a proof of (1)? There is one other point you might want to address: You might want or need to use a fact like this: If m is prime and m divides a product of two integers $a \cdot b$, but m does not divide a, then m must divide b. (This is a result in number theory often called *Euclid's Lemma* – it appears in Book VII of Euclid's *Elements*. Look this up in Wikipedia, learn the proof given in the online article on that subject, and write it up in your own words as part of your solution.)

E) If you have finished questions A - D, you may want to think about the case where m is not prime too, but that is extra credit!

Assignment

Each group should keep a record of its work on these questions and aim to turn in a full proof of (1) by the end of class on Friday, November 6. (If absolutely necessary, I will grant extensions until Monday, November 9.)