MONT 104Q – Mathematical Journeys: From Known To Unknown
Discussion Day 4, part b
How do we decide what to prove? – October 30, 2015

Background

Recall that for any two positive integers m, n, there exist *unique* integers q and r with

(1) $$n = qm + r \qquad \text{and} \qquad 0 \leq r < m.$$

(Another way to say this would be that $\frac{n}{m} = q + \frac{r}{m}$ with $0 \leq r < m$, but we won't make use of the fraction form.) The q is called the *quotient* and the r is called the *remainder* on division.

To have a reasonable way to describe the output of this integer division process, let's introduce the notation $n\, R\, m$ for the remainder r when we divide m into n. Thus, for example

$$17\, R\, 3 = 2 \quad \text{since} \quad 17 = 5 \cdot 3 + 2$$

is the unique equation of the form (1) for $n = 17$ and $m = 3$. Similarly, with a slightly larger example

$$361\, R\, 15 = 1 \quad \text{since} \quad 361 = 24 \cdot 15 + 1,$$

so the remainder on division is 1. Note that the possible values of $n\, R\, m$ are $0, 1, \ldots, m-1$ no matter what n is. Also note that if $n < m$, then $n\, R\, m = n$ since the division in that case gives the rather uninteresting equation $n = 0 \cdot m + n$.

Last time, we were investigating *the remainders of the powers*

$$r\, R\, m, r^2\, R\, m, \ldots r^k\, R\, m, \ldots$$

for the $r = 1, 2, \ldots, m-1$. We saw that mathematicians often try to investigate a new area by *"experimenting"* or *gathering data*. But we also ran into a small bottleneck here: The computations $r^k\, R\, m$ can get very tedious if k is large, or if we need to do a lot of them because m is large. So to begin today, let's prove a "short cut" to help us compute these powers in a more reasonable way.

Questions

A) Show that if $n_1\, R\, m = r_1$ and $n_2\, R\, m = r_2$, then $n_1 \cdot n_2\, R\, m = r_1 \cdot r_2\, R\, m$. (Note: by the uniqueness of the quotient and the remainder in the range $0 \leq R < m$ in (1), this amounts to showing that $n_1 \cdot n_2 - r_1 \cdot r_2$ is a multiple of m.)

Next, we need to understand why I said knowning the fact in part A would give us a short-cut(!) To see why this is true, consider the problem of computing the power remainders $5^k\, R\, 17$. That would get really tedious really fast "the old way!" Notice that

$$5^2\, R\, 17 = 25\, R\, 17 = 8$$

What part A says is that to compute the higher powers $5^3\,R\,17$, $5^4\,R\,17$, we don't need to multiply out the $5^3, 5^4, \ldots$. We just need to use the previous power R-value and multiply *that* by 5 each time:

$$5^2\,R\,17 = 8 \text{ and } 5\,R\,17 = 5 \Rightarrow 5^3\,R\,17 = 8 \cdot 5\,R\,17 = 40\,R\,17 = 6$$

since $40 = 2 \cdot 17 + 6$. Then

$$5^4\,R\,17 = 6 \cdot 5\,R\,17 = 30\,R\,17 = 13,$$

(since $30 = 1 \cdot 17 + 13$), then

$$5^5\,R\,17 = 13 \cdot 5\,R\,17 = 65\,R\,17 = 14$$

(since $65 = 3 \cdot 17 + 14$), and so on. The real benefit of using A this way is that we're severely cutting down on the sizes of the numbers we need to deal with by not directly computing 5^k each time!

B) Using the shortcut provided by part A repeat the sorts of computations we were doing last time on the power remainders $r^k\,R\,17$ for $r = 1, 2, \ldots, 16$ and enough k's to see some patterns. This is a significantly larger calculation than the ones you were doing last time, so it will pay to divide the labor in a smart way.

C) As a nice by-product of part A, you should now be able to understand something you may have noticed before. What happens when $r^k\,R\,m = 1$ for some k and some r (for a given m)? What is true about the higher power remainders $r^{k+1}\,R\,m$, $r^{k+2}\,R\,m$, etc. when this happens?

(D) By this point, between Wednesday and today, you should have generated enough data to start to see patterns and ask questions about what should happen in general (i.e. for some "special" m, or m in general). Formulate the questions or conjectures about general patterns that have come up in your discussions. We will continue with this next Wednesday after the midterm exam.

Assignment

Each group should keep a record of its work on these questions together with the questions from Wednesday, to turn in at the end of the period today.