MONT 104Q – Mathematical Journeys: From Known To Unknown
Discussion Day 4, part a
How do we decide what to prove? – October 28, 2015

Background

In our discussion of the proofs from G.H. Hardy's *A Mathematician's Apology*, for the proof that there are infinitely many prime numbers (taken from Proposition 20 in Book IX) we had to make use of the *integer division process*. What this says is that for any two positive integers m, n, there exist *unique* integers q and r with

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

(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 $n = 0 \cdot m + n$.

Questions

A) What happens if you compute the following *remainders of powers of integers*? In each row, keep going until you notice a pattern in what is happening in all the rows. (Note there's nothing to do on the first row – the powers of 1 – since *all* of the R-values on that row will be 1.)

$$1\,R\,5, 1^2\,R\,5, 1^3\,R\,5, \cdots$$

$$2\,R\,5, 2^2\,R\,5, 2^3\,R\,5, \cdots$$

$$3\,R\,5, 3^2\,R\,5, 3^3\,R\,5, \cdots$$

$$4\,R\,5, 4^2\,R\,5, 4^3\,R\,5, \cdots$$

Try to describe the pattern you are seeing in words.

B) Is there a similar (but possibly not identical) pattern when you go to remainders on division by 7? Compute:

$$1\,R\,7, 1^2\,R\,7, 1^3\,R\,7, \cdots$$

$$2\,R\,7, 2^2\,R\,7, 2^3\,R\,7, \cdots$$

$$\vdots$$

$$6\,R\,7, 6^2\,R\,7, 6^3\,R\,7, \cdots$$

C) What if you try the same computations with remainders on division by 6 (take powers of $1, 2, 3, 4, 5$), then remainders on division by 8 (powers of $1, 2, 3, 4, 5, 6, 7$), then remainders on division by 9 (powers of $1, 2, 3, 4, 5, 6, 7, 8$)? Are there common features the remainders on division by $5, 7$? Are there different features? Do $5, 7$ have a property that $6, 8, 9$ do not?

Assignment

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