Modular Arithmetic: week 5 (pretty much the same as weeks 1-4 because ....)

Right. Finally we got back to some modular arithmetic, after I sadly was forced to shatter all of your illusions about Logic and Set Theory proofs actually giving any meaningful *intuitions or insights into infinity* ..... so I'm going to leave all notions of cardinality, space-filling, real numbers, etc and let you investigate those in your spare time over the coming weeks/months/years.

Speaking of which, we touched on the subject of how the number systems we deal with in modular mathematics are actually *nothing like* the real numbers, nor even the complex numbers. To illustrate this one only needs to multiply the number 3 by 4 (or by 8, for that matter ...) modulo 12 ... we get *zero*!! For this reason number systems like the integers modulo 12 are said to have *zero divisors*.

- Q1: Which moduli $\mathbf{m}$ give number systems which have zero divisors? Which moduli give *no* zero divisors?

Just as problematic is that we lose the notion of *order*, or even of *positivity*. For example working modulo $\mathbf{m} = 25$, we might decide to say that 24 is greater than 2, but then $24 \equiv -1 \mod 25$ .... errrrm .... so to regain some notions of 'common sense' in the realm of modular arithmetic we have to go back to first principles and recall what the notation $\mathbb{Z}/\mathbf{m}\mathbb{Z}$ means ..... namely the collection of the $\mathbf{m}$ sets of the form

$$\{0 + n\mathbf{m} : n \in \mathbb{Z}\} \ , \ \{1 + n\mathbf{m} : n \in \mathbb{Z}\} \ , \ \{2 + n\mathbf{m} : n \in \mathbb{Z}\} \ , \ \{3 + n\mathbf{m} : n \in \mathbb{Z}\},$$
$$\ldots \ , \ \{(\mathbf{m}-2) + n\mathbf{m} : n \in \mathbb{Z}\} \ , \ \{(\mathbf{m}-1) + n\mathbf{m} : n \in \mathbb{Z}\}.$$

So for example if you want to know what happens when $\mathbf{m} = 17$ and you multiply 13 by 5, we actually think of it as *the set of all of the products of all pairs made up of exactly one number from each set*:

$$\{13 + 17n : n \in \mathbb{Z}\} * \{5 + 17r : r \in \mathbb{Z}\} =$$
$$\{(65 + 5 * 17n + 13 * 17r + 17^2 * nr) : n, r \in \mathbb{Z}\} \subseteq$$
$$\{14 + 17 * (3 + 5n + 13r + 17nr) : n, r \in \mathbb{Z}\};$$
$$\text{that is to say, } 13 * 5 \equiv 14 \mod 17$$

MAKE SURE YOU UNDERSTAND THIS THOROUGHLY!!!!! It is the same process you use implicitly when you deal with fractions (ie $\mathbb{Q}$), though I admit this modular stuff may seem much more complicated at first sight.

- Q2: Write out the same type of calculation: (i) multiplying 36 and 14 when the modulus is 56; and (ii) multiplying -7 and 3 when the modulus is 15.

But we did regain some sense of *orderliness*, if not exactly *order* in the usual sense, by looking at solutions of equations like $x^2 \equiv 1 \mod \mathbf{m}$. We observed that modulo 3, 7, 9 or 27 we seemed to have exactly one primitive square root of 1 .... that is, -1 ... but then if we work with modulus $\mathbf{m} = 8$ then what happens when we square 3? And 5? And 7 ... oh yeah, that's -1 again ..... Any ideas? :)

Anyway I had already put the rat amongst the sparrows by showing you that 2×2-matrices can have infinitely many 'primitive square roots of 1' ... so arithmetic systems that are not the real or complex numbers (or subsets of those, like $\mathbb{Z}$ or $\mathbb{Q}$) may not behave as nicely as we might naively hope ... but then they 'make up for it' in other surprising and elegant ways, which is what we shall see as the course wears on ....

- Q3: We call $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ the $(2 \times 2$-$)$ *identity matrix*. Find two 2×2-matrices with **integer** entries which are *primitive* square roots of the identity matrix and whose sum is the *zero matrix* $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

And also remember how in sheet 1 when working modulo 12 we showed that 9 divided by 3 was 3 ... or was it 7 ... or was it just 11 .... I forget :) Any ideas now?

- Q4*: Explain what is going on here with 'division modulo 12' in the same framework as you did Q2.

Finally we looked in some detail at multiplication modulo 3, 9 and 27. That will be our beginning point next Monday. Here is a question to refresh your memories.

- Q5*: For $\mathbf{m} = 3, 9, 27, 81$, show how the 'central additive triangle' exists in all 4 modular systems. Also show that the multiples of 3 always produce zero when raised to a high enough power (what power is that?). How many zero divisors do each of these systems have, if any? Numbers which are not multiples of 3 seem to have powers which give 1 eventually. Is that true of ALL such numbers for all of these values of $\mathbf{m}$? If so, why? If not, why not? :)

- Q6*: Now consider *any odd prime modulus* $\mathbf{m} = p$. Take *any* number a between 1 and $p - 1$. Is there a non-zero power $r \in \mathbb{N}$ which *guarantees* us that $a^r \equiv 1 \mod p$? Why (not)? :) :) :)

- Q7**: Do the Fundamental Theorems of Arithmetic or Algebra hold in modular systems for *any* values of $\mathbf{m}$? (Would get 100 :)'s if I could put them all in)

Have fun.