MAS114 Problems

Sheet 9 (Week 10)

Preamble

Themes from this week (ask your tutorial staff if you're stuck): 1. Wilson's theorem. 2. Public Key Cryptography. 3. Irrational numbers.

Work on these problems one at a time in small groups (of around four). For many problems there is designed to be a lot of work that's best shared; and for others discussion is vital to understanding.

1

Use facts about exponention in modular arithmetic to find the remainder left by dividing $10^{10^{10}}$ by 41.

Remember that $10^{10^{10}}$ is *not* the same thing as $\left(10^{10}\right)^{10}$.

2

Find all possible residue classes of squares modulo m, for each m from 2 to 10. Which modulus has the smallest proportion of squares?

3

Show using modular arithmetic that there are no solutions to the following equations:

(i) $a^2 + b^2 = 100003$;

(ii) $a^2 + b^2 + c^2 = 100007$;

(iii) $a^2 + 7b^2 = 700003$;

(iv) $a^3 + b^3 = 700004$;

(v) $a^3 + b^4 = 19^{19}$.

For discussion: In general, if you see an equation and want to show there are no solutions using modular arithmetic, what are good techniques for choosing a good modulus to work with?

4

I have a sequence of positive integers $a_1, a_2, \ldots$, where $a_1 = 1$ and for each $n \geq 1$ we either have $a_{n+1} = 2a_n$, $a_{n+1} = a_n^2$ or $a_{n+1} = a_n - 7$.
Can this sequence contain the number 3? Explain your answer carefully.