MAS114 Solutions

Sheet 9 (Week 10)

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 $(10^{10})^{10}$.

   Solution We know from Fermat's Little Theorem that $10^{40} \equiv 1 \pmod{41}$. But 10^{10} is a multiple of 40, so

   $$10^{10^{10}} \equiv 1 \pmod{41}.$$

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?

   Solution Modulo 2: Squares can be odd or even, so $\{0, 1\}$ are the residues of squares mod 2.

   Modulo 3:

   $$0^2 \equiv 0; \qquad 1^2 \equiv 2^2 \equiv 1.$$

   So $\{0, 1\}$ are the residues of squares mod 3.

   Modulo 4:

   $$0^2 \equiv 2^2 \equiv 0; \qquad 1^2 \equiv 3^2 \equiv 1.$$

   So $\{0, 1\}$ are the residues of squares mod 4.

   Modulo 5:

   $$0^0 \equiv 0; \qquad 1^2 \equiv 4^2 \equiv 1; \qquad 2^2 \equiv 3^2 \equiv 4.$$

   So $\{0, 1, 4\}$ are the residues of squares mod 5.

Modulo 6:

$$0^0 \equiv 0; \qquad 1^2 \equiv 5^2 \equiv 1; \qquad 2^2 \equiv 4^2 \equiv 4; \qquad 3^2 \equiv 3.$$

So $\{0, 1, 3, 4\}$ are the residues of squares mod 6.

Modulo 7:

$$0^0 \equiv 0; \qquad 1^2 \equiv 6^2 \equiv 1; \qquad 2^2 \equiv 5^2 \equiv 4; \qquad 3^2 \equiv 4^2 \equiv 2.$$

So $\{0, 1, 2, 4\}$ are the residues of squares mod 7.

Modulo 8:

$$0^0 \equiv 4^2 \equiv 0; \qquad 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1; \qquad 2^2 \equiv 6^2 \equiv 4.$$

So $\{0, 1, 4\}$ are the residues of squares mod 8.

Modulo 9:

$$0^2 \equiv 3^2 \equiv 6^2 \equiv 0; \qquad 1^2 \equiv 8^2 \equiv 1; \qquad 2^2 \equiv 7^2 \equiv 4; \qquad 4^2 \equiv 5^2 \equiv 7.$$

So $\{0, 1, 4, 7\}$ are the residues of squares mod 9.

Modulo 10:

$$0^2 \equiv 0; \qquad 1^2 \equiv 9^1 \equiv 1; \qquad 2^2 \equiv 8^2 \equiv 4; \qquad 3^2 \equiv 7^2 \equiv 9; 4^2 \equiv 6^2 \equiv 6; 5^2 \equiv 5.$$

So $\{0, 1, 4, 5, 6, 9\}$ are the residues of squares mod 10.

The smallest proportion is modulo 8, where only 37.5% of the residues are 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) $a^3 + b^4 = 19^{19}$.

   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?

Solution

(i) Since squares are congruent to 0 or 1 modulo 4, we can't have two squares adding up to something that's 3 (mod 4).

(ii) Since squares are congruent to 0, 1 or 4 modulo 8, we can't have three squares adding up to something that's 7 (mod 8).

(iii) Since a^2 is congruent to 0, 1, 2 or 4 modulo 7, and $7b^2$ is congruent to zero, the left-hand side is congruent to 0, 1, 2, or 4, while the right-hand side is congruent to 3.

(iv) Cubes are congruent to 0, 1 or 6 modulo 7, so two of them can't add up to make something that's 4 mod 7.

(v) There are no solutions modulo 13.

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.

Solution Working modulo 7, we can prove by induction that every term is congruent to 1, 2 or 4.