ORMC: MODULAR ARITHMETIC – PART I

OLYMPIAD GROUP 1, WEEK 4

[*Recap: Congruences, Residue classes*]

Problem 1. (Textbook example) Let p be a prime number, and let $a \not\equiv 0 \pmod{p}$ be an integer.

(a) Let b, c be integers. Show that if $ab \equiv ac \pmod{p}$, then $b \equiv c \pmod{p}$.

(b) Show that there exists an integer b such that $ab \equiv 1 \pmod{p}$. Moreover, show that the residue class of b is unique. *Hint: Assume towards a contradiction that b does not exist, and use part (a) together with the Pigeonhole Principle.*

Problem 2. (Textbook example – Fermat's Little Theorem) Let p be a prime number, and let $a \not\equiv 0 \pmod{p}$ be an integer. Show that $a^{p-1} \equiv 1 \pmod{p}$. *Hint: Apply part (a) of the previous exercise to show that the numbers $a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$ are all distinct.*

Problem 3. (Textbook example)

(a) Show that if $7 \mid a^2 + b^2$ for two integers a, b, then in fact $7 \mid a$ and $7 \mid b$.

(b) Solve the equation $a^2 + b^2 = 7c^2$ for all integers a, b, c.

[*More general case: $p \equiv 3 \pmod{4}$*]

Problem 4. Let p be a prime other than 2 and 3. Show that $2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod{p}$.

Problem 5. Let p be an *odd* prime number.

(a) Show that there is at least one residue class $\hat{a}$ mod p that is not a perfect square (that is, there are no integers b such that $b^2 \equiv a \pmod{p}$).

(b) Show that there are exactly $\frac{p-1}{2}$ such residue classes $\hat{a}$. *Note: perfect squares mod p are called the quadratic residues.*

Problem 6.

(a) Find the last digit of 3^{2021}.

(b) Find the residue modulo 70 of 3^{2021}.

Problem 7.

(a) Let p be a prime number, $a \not\equiv 0 \pmod{p}$, and let n be the smallest positive integer such that $p \mid a^n - 1$. If m is another positive integer, show that $p \mid a^m - 1$ if and only if $n \mid m$.

(b) Show that in (a), we have $n \mid p - 1$. *Note: n is called the (multiplicative) order of a mod p.*

(c) Let k be a positive integer. Find all prime divisors p of $2^{2^k} - 1$ of the form $p \equiv 3 \pmod{4}$. *Challenge: Can you find two (significantly different) solutions?*

Problem 8. Show that the equation

$$2^{2021} + (p-2)^{2021} = 3^n$$

has no solutions where n is a positive integer and p is a prime.

Homework

Problem 1. Solve the equation $a^2 + 2b^2 = 5c^2$ for all integers a, b, c.

Problem 2. Find the last digit of $2^{2^{2021}}$.