MAT-255– Number Theory | Spring 2024 | In Class Work April 19

Your Name: ____________________ Group Members: ____________________ ____________________

In-class Problem 1 (Chapter 6, Exercise 20) Let $x, y, z \in \mathbb{Z}$ and let p be a prime number.

(a) Prove that if $x^{p-1} + y^{p-1} = z^{p-1}$, then $p \mid xyz$.

(b) Prove that if $x^p + y^p = z^p$, then $p \mid (x + y - z)$.

Hint: *Recall Fermat's Little Theorem and its corrollaries.*

Solution: Let p be a prime number.

(a) Let $x, y, z \in \mathbb{Z}$ such that $x^{p-1} + y^{p-1} = z^{p-1}$.

By Fermat's Little Theorem, if $p \nmid x$, then $x^{p-1} \equiv 1 \pmod{p}$. If $p \mid x$, then $x^{p-1} \equiv 0 \pmod{p}$. Similarly for y and z. Thus,

$$x^{p-1} + y^{p-1} \equiv \begin{cases} 0+0 \pmod{p} \\ 0+1 \pmod{p} \\ 1+1 \pmod{p} \end{cases}$$

has a solution if andd only if p divides at least one of x, y. Thus, $p \mid xyz$.

(b) Let $x, y, z \in \mathbb{Z}$ such that $x^p + y^p = z^p$.

By Corollary 5.8, $x^p \equiv x \pmod{p}, y^p \equiv y \pmod{p}$, and $z^p \equiv z \pmod{p}$. Thus,

$$\begin{aligned} x^p + y^p &\equiv z^p \pmod{p} \\ x + y &\equiv z \pmod{p}. \end{aligned}$$

In otherwords, $p \mid (x + y - z)$.

Learning outcomes:
Author(s): Claire Merriman