Orders & Problem Session

Alston Yam

1 Introduction

We're going to be talking about the idea of an *order* today. In addition to that, this lesson will also include a few practice problems for us to use the techniques covered in the previous lessons.

Definition 1.1 – Orders Let p by a prime and $a \not\equiv 0 \pmod{p}$. Then the order of a modulo p is defined to be the smallest positive integer n such that $a^n \equiv 1 \pmod{p}$. We can denote it by $n = ord_p(a)$,

Also, as a recap of some of the modular arithmetic:

Theorem 1.1 – Modular Arithmetic We can do normal addition, subtraction, and multiplication under $\pmod{n}$, but not always division.

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then we have:

$$a + c \equiv b + d \pmod{n}$$
$$a - c \equiv b - d \pmod{n}$$
$$ac \equiv bd \pmod{n}$$

Definition 1.2 – Modular Inverses Let a be an integer and n a positive integer. We say that x is the **inverse** of a modulo n if

$$a \cdot x \equiv 1 \pmod{n}$$

Here, we may write $x \equiv a^{-1} \pmod{n}$

2 Problems

Problem 2.1 – Fundamental Theorem of Orders For a prime p and any integer $a \not\equiv 0 \pmod{p}$, we have

$$a^n \equiv 1 \pmod{n} \iff ord_p(a) \mid n$$

Problem 2.2 Find all n such that $n \mid 2^n - 1$

Problem 2.3 Prove that if p is a prime, then every prime divisor of $2^p - 1$ is greater than p.

Problem 2.4 Find all integers $n \geq 1$ such that n divides $2^{n-1} + 1$