Theorem.

Math 115 Lecture Notes (Prof. Paul Vojta)

□

Vignesh Nydhruva

September 17, 2024

For this lecture, the following topics were covered: multiplicative inverses mod m, theorems of Euler and Wilson, and solutions of the congruence $x^2 \equiv -1 \pmod{m}$ for prime p. The reading for the following lecture is §2.3 and 2.4 from Niven. In addition, for today, $m \in \mathbb{Z}_{>0}$.

Theorem. *Let $a \in \mathbb{Z}$. Then there exists an $x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{m}$ iff $\gcd(a, m) = 1$.*

Proof.