Chapter 1.4. Prime Numbers and Finite Fields

Def. An integer p is called a prime if $p \geq 2$ and the only positive integers dividing p are 1 and p.

Thm. Let p be a prime.

Then, every nonzero element $a \in \mathbb{Z}_p$ has a multiplicative inverse.

i.e, $\exists\, b \in \mathbb{Z}_p$ s.t. $ab \equiv 1 \mod p$

Def. A field is a ring in which every nonzero element has a multiplicative inverse.

Ex. $\mathbb{Z}_6$ is not a field. ($\nexists\, b$ s.t. $2 \cdot b \equiv 1 \mod 6$)

$\mathbb{Z}_7$ is a field.

Note. Let $\mathbb{F}$ be a finite field.

Then, $|\mathbb{F}|$ is a prime or $|\mathbb{F}|$ is a power of prime.

Think thing