

Second lecture

- Factorization in primes

Existence

Uniqueness

- Modular arithmetic, \mathbb{Z}_m

Counting (mod m)

Invertible elements in \mathbb{Z}_m

\mathbb{Z}_p , p prime