Foundations of Mathematics, Lecture 12 (week 13)

András Kornai

BMETE91AM35 Fall 2020-21

Number Theory

1. The greatest idea: mod n counting
2. For any n we have a ring $R_n = \mathbb{Z}/n$
3. If $n = ab$ is composite, the ring has *zero divisors* mod n: neither a nor b is 0, but $ab = 0$
4. If n is prime this doesn't happen, why?
5. mod p everything has a multiplicative inverse (except 0) so R_p is a field, denoted GF(p)
6. Can also be built for prime powers (not discussed here) GF(p^k)
7. All finite fields are uniquely determined by their size

Key observations, theorems

- If $n|a_1, ..., a_{k-1}$ and $n|\sum_{i=1}^{k} a_i$ then $n|a_k$
- Division with remainder: $\forall a, b \in \mathbb{N}\, \exists q, r\ : a = bq + r$
- Divisors of 1 are called *units*
- "Little Fermat" $a^p \equiv a \mod p$
- Euler-Fermat If $(a, n) = 1$ we have $a^{\phi(n)} \equiv 1 \mod n$ Here $\phi(n)$ countes the integers between 1 and n that are relative prime to n
- Wilson's Theorem: $(n-1)! \equiv -1 \mod n \Leftrightarrow n$ is prime