7 - Implementacja arytmetyki Z_p/W

Tuesday, 18 June 2024 19:11

Jeśli wielomian W stopnia d jest nierozkładalny to:

$\mathbb{Z}_p/W$ jest ciałem o p^d elementach.

- dodawanie/odejmowanie: po współrzędnych (mod p)
- mnożenie: splot i „normalizacja" za pomocą W (mod W)
- dzielenie: w słupku (normalizacja)