Plonk Arithmetization

January 09, 2025

Distributed Lab

zkdl-camp.github.io

github.com/ZKDL-Camp

Plan

Multiplicative Subgroup. Primitive Roots

Motivation

In the Groth16, recall that we needed to interpolate expressions in the following form

$$P(i) = a_i, \quad a_i \in \mathbb{F}, \quad i = 1, \dots, N$$

Recall

The interpolation formula in given by:

$$P(x) = \sum_{i=1}^{N} a_i \cdot \ell_i(x), \quad \ell_i(x) = \prod_{j=1, j \neq i}^{N} \frac{x - j}{i - j}$$

The complexity of this formula is $\mathcal{O}(N^2)$. But can we do better?

Multiplicative Subgroup.

We know that $\mathbb{F}_p$ is a **field**: we have a usual arithmetic $+, \times$.

Question

Does $(\mathbb{F}_p, \times)$ form a group?

No, since 0 does not have an inverse. But, if we consider $(\mathbb{F}_p \setminus \{0\}, \times)$, we do have a group structure!

Definition

A **multiplicative group** of a finite field $\mathbb{F}$, denoted as $\mathbb{F}^\times$, is a multiplicative group $(\mathbb{F} \setminus \{0\}, \times)$.

Number of Elements

The number of elements in $\mathbb{F}_p^\times$ is $p - 1$.

Primitive Root

Theorem

Multiplicative group of a finite field $\mathbb{F}^{\times}$ is cyclic. The generators ω of this group are called ***primitive roots****.*

Example

$\omega = 3$ is the primitive root of $\mathbb{F}_7$. Indeed,

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1.$$

Clearly, $\langle \omega \rangle = \mathbb{F}_7^{\times}$.