

TD 3: Finite fields

Exercice 1. \mathbb{F}_8

a. Give the addition, multiplication and inversion tables of the field with 8 elements.

1. in the polynomial representation;
2. in the Zech log representation.

Exercice 2. Generators of a multiplicative group

We want to check whether 2 is a generator of the multiplicative group $(\mathbb{Z}/101\mathbb{Z})^*$.

- a.** Explain why it suffices to compute $2^{\frac{100}{2}} \pmod{101}$ and $2^{100/5} \pmod{101}$.
- b.** Compute these values and conclude

We wish now to find a generator of $(\mathbb{Z}/31\mathbb{Z})^*$.

- c.** What is the order of 2?
- d.** Find an element of order 2?
- e.** Find an element of order 3?
- f.** Deduce a generator of the group $(\mathbb{Z}/31\mathbb{Z})^*$.