Exercise 2 Cheat Sheet
Finite Fields $\mathbb{F}_p[X]/(P(X))$: Generators, Powers & Inverses

Recognition

Work in:

$$\mathbb{F}_p[X]/(P(X)), \quad \alpha = [X]$$

Typical tasks:

- test if α is a generator
- compute powers
- compute inverses

If called a field, assume $P(X)$ is irreducible.

Core Rule (No Mixing)

$$\boxed{\text{Compute in } X \ \rightarrow \ \text{final answer in } \alpha}$$

Never mix representations during computation.

Step 0: Reduction Rule (GENERAL)

From:

$$P(X) = X^k + a_{k-1}X^{k-1} + \cdots + a_0$$

derive:

$$X^k \equiv -(a_{k-1}X^{k-1} + \cdots + a_0) \pmod{p}$$

Important:

- all coefficients are reduced mod p

Example (only in $\mathbb{F}_2$):

$$X^4 + X + 1 = 0 \Rightarrow X^4 \equiv X + 1$$

Structure Facts

Let $\deg(P) = k$.

$$|K| = p^k, \quad |K^\times| = N = p^k - 1$$

$$a^N = 1 \quad (a \neq 0)$$

$$(a^m)^{-1} = a^{N-m}$$

Generator Test

Factor:

$$N = \prod q_i$$

Check only:

$$\alpha^{N/q_i}$$

Decision:

$$\alpha \text{ generator} \iff \forall q_i : \alpha^{N/q_i} \neq 1$$

Inverse Methods

Method 1: Exponent Method (fast)

If element is α^m:

$$(\alpha^m)^{-1} = \alpha^{N-m}$$

Use repeated squaring + reduction via $P(X)$.
Best when element is already a power of α.

Method 2: Extended Euclidean Algorithm (EEA)

Use when element is a polynomial in α.
Goal:

$$A(X)^{-1} \bmod P(X)$$

Step 1 (Euclidean algorithm):

$$P(X) = Q_1 A(X) + R_1, \quad A(X) = Q_2 R_1 + R_2, \ldots$$

until:

$$R_k = 1$$

Step 2 (Bezout identity):

$$1 = U(X)A(X) + V(X)P(X)$$

Step 3 (mod reduction):

$$V(X)P(X) \equiv 0 \Rightarrow 1 \equiv U(X)A(X)$$

Thus:

$$\boxed{A(X)^{-1} = U(X) \ (\mathrm{mod} P(X))}$$

Worked Pattern (EEA Example)

Given:

$$P(X) = X^4 + X + 1, \quad A(X) = X^2 + 1$$

Forward:

$$X^4 + X + 1 = (X^2 + 1)^2 + X$$
$$X^2 + 1 = X \cdot X + 1$$

Backward (compressed form):

$$1 = (X^2 + 1)(X^3 + X + 1) + X(X^4 + X + 1)$$

Modulo $P(X)$:

$$X(X^4 + X + 1) \equiv 0$$

So:

$$(X^2 + 1)^{-1} \equiv X^3 + X + 1$$

Back to α:

$$\boxed{\alpha^{-8} = \alpha^3 + \alpha + 1}$$

Exam Template

$$\mathbb{F}_2[X]/(X^4 + X + 1), \quad N = 15$$

Generator test:

$$\alpha^3,\ \alpha^5$$

Inverse:

$$(\alpha^8)^{-1} = \alpha^7$$

or use EEA if expression is not a pure power.

Shortcuts

- Only test exponents N/q
- Reduce after every multiplication
- EEA avoids discrete log
- Exponent method avoids polynomial algebra

Common Mistakes

- Mixing X and α
- Forgetting coefficient reduction mod p
- Using exponent method on non-powers

$$\boxed{|K^\times| = p^k - 1, \quad (a^m)^{-1} = a^{N-m}, \quad a \text{ primitive} \iff a^{N/q} \neq 1}$$