10 Polynomial CRT and finite fields

10.1. Construct finite fields consisting of (a) 25, (b) 8, (c) 125 elements.

Solutions: e.g. factors (a) $\mathbb{Z}_5[\alpha]/(\alpha^2+2)$, *(b)* $\mathbb{Z}_2[\alpha]/(\alpha^3+\alpha+1)$, *(c)* $\mathbb{Z}_5[\alpha]/(\alpha^3+\alpha+1)$.

10.2. Construct a splitting field of the polynomials

(a) x^3+1 over the field $\mathbb{Z}_2$,

(b) x^2+1 over the field $\mathbb{Z}_7$,

(c) x^9-x over the field $\mathbb{Z}_3$,

and decompose all the polynomials into linear factors.

Solutions: (a) $x^3+1=(x+1)(x+\alpha)(x+\alpha+1)$ *over* $\mathbb{F}_4=\mathbb{Z}_2[\alpha]/(\alpha^2+\alpha+1)$
(b) e.g. $x^2+1=(x+\alpha)(x-\alpha)$ *over* $\mathbb{F}_{49}=\mathbb{Z}_7[\alpha]/(\alpha^2+1)$,
(c) $x^9-x=\prod_{a\in\mathbb{F}_9}(x-a)$ *over* $\mathbb{F}_9$, *e.g.* $\mathbb{F}_9=\mathbb{Z}_3[\alpha]/(\alpha^2+1)$

10.3. Find all polynomials f of degree < 3 satisfying

(a) $f(0)=1,\ f(1)=2,\ f(2)=3,\ f\in\mathbb{Z}_7[x]$,

(b) $f(0)=3,\ f\equiv x+1 \pmod{x^2+1},\ f\in\mathbb{Q}[x]$.

Solutions: (a) $f=x+1$, *(b)* $f=3+x+2x^2$.

10.4. Design a secret sharing protocol for 5 participants such that at least 3 of them are needed to reveal the secret where the secret is an element of the field $\mathbb{F}_7$.

10.5.* Prove that $\mathbb{Z}_3[\alpha]/(\alpha^4+\alpha^3+\alpha+2)$ is not a field.

Hint: Decompose $\alpha^4+\alpha^3+\alpha+2=(2+\alpha+\alpha^2)(1+\alpha^2)$.

10.6.* Prove that the map $\rho:\mathbb{Z}_5[\alpha]/(\alpha^4-1)\to\mathbb{Z}_5^4$ given by $\rho(f)=(f(1),f(2),f(3),f(4))$ is a bijection.

Hint: Show that $x^4-1=(x-1)(x-2)(x-3)(x-4)$ *and apply CRT.*