9 Congruences and factorizations of polynomial rings

9.1. Find all polynomials $f \in \mathbb{Z}_2[x]$ satisfying congruences:

(a) $(x^3 + x + 1)f \equiv 1 \pmod{x^4 + x + 1}$ in $\mathbb{Z}_2[x]$

(b) $(2x + 1)f \equiv x^3 \pmod{x^2 + 1}$ in $\mathbb{Z}_3[x]$.

Solutions: (a) $(x^2 + 1) + s(x^4 + x + 1)$ *for* $s \in \mathbb{Z}_2[x]$, *(b)* $x + 2 + s(x^2 + 1)$ *for* $s \in \mathbb{Z}_3[x]$

9.2. For the ring $T = \mathbb{Z}_3[\alpha]/(\alpha^2 + 1)$

(a) prove that the polynomial $x^2 + 1$ over $\mathbb{Z}_3$ is irreducible and find its roots in T,

(b) explain why T is a field, and determine the number of elements of T,

(c) calculate in T:
(i) $(2\alpha + 1) + (2\alpha + 2)$, (ii) α^5, (iii) α^{-1},
(iv) $(\alpha + 1)^{-1}$, (v) $2\alpha \cdot (2\alpha + 1)$, (vi) $\alpha^{-1} \cdot (\alpha + 2)$.

Solutions: (a) $x^2 + 1 = (x + \alpha)(x - \alpha)$ *(b)* $|T| = 9$, *(c)* α, α, 2α, $\alpha + 2$, $2 + 2\alpha$, $\alpha + 1$.

9.3. Construct rupture fields (i.e. a field containing a root) of the polynomials in $\mathbb{Z}_2[x]$:

(a) $x^2 + x + 1$,

(b) $x^3 + x + 1$.

Note that both fields are even splitting fields and decompose the polynomials into linear factors.

Solutions: (a) $x^2 + x + 1 = (x + \alpha)(x + (\alpha + 1))$ *in* $\mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$ *(b)* $x^3 + x + 1 = (x + \alpha)(x + (\alpha^2))(x + (\alpha^2 + \alpha))$ *in* $\mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$

9.4. Find a polynomial f of the smallest possible degree satisfying

(a) $f \in \mathbb{Z}_5[x]$, $f \equiv x + 1 \pmod{x^2 + 1}$, $f \equiv x \pmod{x^3 + 1}$,

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

Solutions: (a) $3x^4 + 3x^3 + 4x + 3$, *(b)* $\frac{1}{2}(3x^2 - 5x + 2)$

9.5.* Let p be a prime number. Applying the Chinese remainder theorem, prove that

$$x^p - x = \prod_{a \in \mathbb{Z}_p} (x - a) \text{ in } \mathbb{Z}_p[x].$$