

3a: Suppose that $a(x) \equiv b(x) \pmod{n(x)}$. Then by the polynomial division algorithm, there exists $q_1(x), q_2(x)$ such that $a(x) = q_1(x)n(x) + r_1(x)$ and $b(x) = q_2(x)n(x) + r_2(x)$. Computing their difference, we see

$$a(x) - b(x) = q_1(x)n(x) - q_2(x)n(x) = [q_1(x) - q_2(x)]n(x)$$

We see that $n(x)$ divides $a(x) - b(x)$. Now suppose that $n(x) \nmid a(x) - b(x)$. There exists some polynomials $q_1(x), q_2(x), r_1(x), r_2(x)$ such that $a(x) = q_1(x)n(x) + r_1(x)$ and $b(x) = q_2(x)n(x) + r_2(x)$ with $\deg(r_1(x)) < \deg(q_1(x))$ and $\deg(r_2(x)) < \deg(q_2(x))$. Since $n(x) \nmid a(x) - b(x)$ there exists some $q(x)$ where $n(x)q(x) = a(x) - b(x)$. Now we compute that

$$a(x) - b(x) - (q_1(x)n(x) - q_2(x)n(x)) = r_1(x) - r_2(x) = (q(x) - q_1(x) + q_2(x))n(x)$$

Assume that $(q(x) - q_1(x) + q_2(x)) \neq 0$. This implies that $\deg(r_1(x) - r_2(x)) \geq \deg(n(x))\deg(q(x) - q_1(x) + q_2(x)) \geq \deg(n(x))$. This is a contradiction. Thus $a(x) \equiv b(x) \pmod{n(x)}$

3b: Since $a(x) \equiv b(x) \pmod{n(x)}$ when they have the same remainder after division by $n(x)$, to count $\mathbb{F}_p[X]/n(x) \mathbb{F}_p[x]$ it suffices to count how many polynomials with coefficients in \mathbb{F}_p exist with degree less than $\deg(n(x))$. There are $\deg(n(x))$ possible terms in each polynomial, and each term has a choice of p coefficients. Thus by basic counting $|\mathbb{F}_p[X]/n(x) \mathbb{F}_p[x]| = p^{\deg(n(x))}$

3c: Suppose that $a(x) \equiv a'(x) \pmod{n(x)}$ and $b(x) \equiv b'(x) \pmod{n(x)}$. By 3a we know that there exists $q_1(x)$ and $q_2(x)$ such that $a(x) - a'(x) = q_1(x)n(x)$ and $b(x) - b'(x) = q_2(x)n(x)$. We compute

$$[a(x) + b(x)] - [a'(x) + b'(x)] = [q_1(x) + q_2(x)]n(x)$$

Which implies that $a(x) + b(x) \equiv a'(x) + b'(x) \pmod{n(x)}$. Hence addition is well defined. We now check multiplication. We compute

$$\begin{aligned} a(x)b(x) - a'(x)b'(x) &= (a'(x) + q_1(x)n(x))(b'(x) + q_2(x)n(x)) - a'(x)b'(x) \\ &= a'(x)b'(x) + a'(x)q_2(x)n(x) + b'(x)q_1(x)n(x) + q_1(x)q_2(x)n^2(x) - a'(x)b'(x) \\ &= n(x)[a'(x)q_2(x) + b'(x)q_1(x) + q_1(x)q_2(x)n(x)] \end{aligned}$$

Therefore, $a(x)b(x) \equiv a'(x)b'(x) \pmod{n(x)}$ hence multiplication is well defined.

3d: Suppose that $\gcd(a(x), b(x)) = d(x) \nmid a(x)$. By the division algorithm there exists polynomials $q(x), r(x)$ such that $a(x) = q(x)d(x) + r(x)$. Since $d(x) = u(x)a(x) + v(x)b(x)$ for some $u(x), v(x) \in \mathbb{F}_p[x]$, we can rewrite

$$r(x) = a(x) - q(x)d(x) = a(x) - q(x)[u(x)a(x) + v(x)b(x)] = (1 - q(x)u(x))a(x) + (-q(x)v(x))b(x)$$

Let $r \in \mathbb{F}_p$ be the leading coefficient of $r(x)$. We have that $\gcd(p, r) = 1$ and so by corollary 3.8, $rx \equiv 1 \pmod{p}$ will have a solution y . If we multiply $r(x)$ by y then we have that

$$y \cdot r(x) = y \cdot (1 - q(x)u(x))a(x) + y \cdot (-q(x)v(x))b(x)$$

Since we multiplied by the inverse of r , $\cdot r(x)$ is not monic. By the division algorithm, $\deg(r(x)) < \deg(d(x))$, and so $\deg(y \cdot r(x)) < \deg(d(x))$ which is a contradiction. Therefore, $d(x) \mid a(x)$ and similarly $d(x) \mid b(x)$.