Chapter 12

The Arithmetic of $\mathbb{F}_p[X]$

In this chapter we will prove several theorems in $\mathbb{F}_p[X]$ that are close analogs of results we have proved before for the ring of integers $\mathbb{Z}$. In particular, we will derive the quadratic reciprocity law in $\mathbb{F}_p[X]$.

12.1 The Analogy between $\mathbb{Z}$ and $\mathbb{F}_p[X]$

Let P be a prime in $\mathbb{F}_p[X]$. We have already seen that there are exactly $NP = p^{\deg P}$ residue classes modulo P. The ring (actually a field since P is prime) of residue classes modulo P is denoted by $\mathbb{F}_p[X]/(P)$, and we have $N(P) = \#\mathbb{F}_p[X]/(P)$. Since every nonzero residue class modulo P has an inverse (in other words: since every nonzero element in $\mathbb{F}_p[X]/(P)$ is a unit), an application of Lagrange's theorem gives us the analog of Fermat's Little Theorem:

$$F^{NP-1} \equiv 1 \bmod P$$

for all $F \in \mathbb{F}_p[X]/(P)$ not divisible by P. It is also clear how to generalize this to composite polynomials P and derive the analog of Euler-Fermat:

$$F^{\Phi(A)} \equiv 1 \bmod A, \quad \text{where} \quad \Phi(A) = \#(\mathbb{F}_p[X]/(A))^\times.$$

Proving the formula $\Phi(P^m) = (NP-1)N(P)^{m-1}$ for prime powers P^m and the analog of Euler's phi-function is straightforward. Similarly, we can show that $\Phi(FG) = \Phi(F)\Phi(G)$ for coprime polynomials $F, G \in \mathbb{F}_p[X]$. You are also invited to check whether our proof of Fermat's 2-squares theorem can be transferred to $\mathbb{F}_p[X]$.

domain	$\mathbb{Z}$	$\mathbb{Z}[i]$	$\mathbb{F}_p[X]$
norm	$\lvert m\rvert$	$N(a+bi) = a^2+b^2$	$N(f) = p^{\deg f}$
Fermat	$a^{\lvert p\rvert-1} \equiv 1\ (p)$	$(a+bi)^{N\pi-1} \equiv 1\ (\pi)$	$F^{N(P)-1} \equiv 1\ (F)$

12.2 Quadratic Reciprocity in $\mathbb{F}_p[X]$

Again we can define the quadratic Legendre symbol via Euler's criterium: If P is an irreducible polynomial over $\mathbb{F}_p$ with p odd, then $f^{NP-1} \equiv 1 \bmod P$, hence $0 \equiv f^{NP-1} - 1 = (f^{(NP-1)/2} - 1)(f^{(NP-1)/2} + 1)$, and since P is prime we conclude that $f^{(NP-1)/2} \equiv \pm 1 \bmod p$. Now define $(\frac{f}{P})_2 \in \{-1, +1\}$ by

$$\Big(\frac{f}{P}\Big)_2 \equiv f^{\frac{NP-1}{2}} \bmod P.$$

For example, $P = X^2+1$ is prime in $\mathbb{F}_3[X]$ and $(\frac{X+1}{X^2+1})_2 \equiv (X+1)^{(3^2-1)/2} = (X+1)^4 = (X^2+2X+1)^2 \equiv (2X)^2 = 4X^2 = X^2 \equiv -1 \bmod P$ shows that $(\frac{X+1}{X^2+1})_2 = -1$.

Here are a few formal properties whose proofs are left as an exercise:

Proposition 12.1. *For $A, B, P \in \mathbb{F}_p[X]$, where p is an odd prime and P irreducible, we have*

1. $(\frac{A}{P})_2 = (\frac{B}{P})_2$ *if* $A \equiv B \bmod P$;
2. $(\frac{AB}{P})_2 = (\frac{A}{P})_2(\frac{B}{P})_2$;
3. $(\frac{A}{P})_2 = 1$ *if* $A \equiv B^2 \bmod P$.

Moreover, the congruence $f(X) \equiv f(a) \bmod (X-a)$ implies that $(\frac{f(X)}{X-a})_2 = (\frac{f(a)}{X-a})_2$. The last symbol can be evaluated: $(\frac{f(a)}{X-a})_2 \equiv f(a)^{(p-1)/2} \equiv (\frac{f(a)}{p}) \bmod P$, hence $(\frac{f(X)}{X-a})_2 = (\frac{f(a)}{p})$, where the symbol on the right hand side is the usual Legendre symbol in $\mathbb{Z}$.

In particular, over $\mathbb{F}_3$ we have $(\frac{X^2+1}{X+1})_2 = (\frac{2}{3}) = -1$.

Lemma 12.2. *For $a \in \mathbb{F}_p^\times$ and a prime $P \in \mathbb{F}_p[X]$ we have $(\frac{a}{P})_2 = (\frac{a}{p})^{\deg P}$.*

Proof. Put $m = \deg P$. Since $N(P) = p^m$ and $p^m - 1 = (p-1)(1 + p + p^2 + \ldots + p^{m-1})$, the claim follows from $(\frac{a}{P})_2 \equiv a^{(p^m-1)/2} = (a^{(p-1)/2})^{1+p+\ldots+p^{m-1}} \equiv (\frac{a}{p})^{1+p+\ldots+p^{m-1}} = (\frac{a}{p})^m \bmod P$. □

The reciprocity law for primes of degree 1 is now easily proved. In fact, the lemma above implies $(\frac{X-a}{X-b})_2 = (\frac{b-a}{X-b})_2 = (\frac{b-a}{p})$ and $(\frac{X-b}{X-a})_2 = (\frac{a-b}{X-a})_2 = (\frac{a-b}{p})$. Thus $(\frac{X-a}{X-b})_2(\frac{X-b}{X-a})_2 = (\frac{b-a}{p})(\frac{a-b}{p}) = (\frac{-1}{p})$. This is a special case of the quadratic reciprocity law in $\mathbb{F}_p[X]$:

Theorem 12.3. *Let p be an odd prime, and let $P, Q \in \mathbb{F}_p[X]$ be primes (irreducible monic polynomials with coefficients in $\mathbb{F}_p$). Then*

$$\Big(\frac{P}{Q}\Big)_2\Big(\frac{Q}{P}\Big)_2 = (-1)^{\frac{p-1}{2}\deg P \deg Q}.$$

Just as the reciprocity law in $\mathbb{Z}$ (or the one in $\mathbb{Z}[i]$ for that matter), this also holds for composite polynomials, with the Legendre symbols replaced by Jacobi symbols.

We can also extend the reciprocity law from monic polynomials to arbitrary polynomials. To this end we introduce the function sgn by letting $\operatorname{sgn}(F)$ denote the leading coefficient of F. For example, $\operatorname{sgn}(2X^2+3)=2$. Note that $\operatorname{sgn}:\mathbb{F}_p[X]\longrightarrow\mathbb{F}_p$ is a ring homomorphism; this means $\operatorname{sgn}(F+G)=\operatorname{sgn}(F)+\operatorname{sgn}(G)$ and $\operatorname{sgn}(FG)=\operatorname{sgn}(F)\operatorname{sgn}(G)$. Also observe that if $F\in\mathbb{F}_p[X]$ is an arbitrary polynomial, then $F=\operatorname{sgn}(F)f$, where f is monic.

Now let $F,G\in\mathbb{F}_p[X]$ be prime polynomials, and write $F=\operatorname{sgn}(F)f$ and $G=\operatorname{sgn}(G)g$ for monic $f,g\in\mathbb{F}_p[x]$. Now observe that $A\equiv B \bmod G$ is equivalent to $A\equiv B \bmod g$ since G/g is a unit; thus $(\frac{F}{G})=(\frac{F}{g})$. Next we compute away:

$$\Big(\frac{F}{G}\Big)=\Big(\frac{F}{g}\Big)=\Big(\frac{\operatorname{sgn}(F)}{g}\Big)\Big(\frac{f}{g}\Big)=\Big(\frac{\operatorname{sgn}(F)}{p}\Big)^{\deg g}\Big(\frac{f}{g}\Big),$$

and similarly

$$\Big(\frac{G}{F}\Big)=\Big(\frac{\operatorname{sgn}(G)}{p}\Big)^{\deg f}\Big(\frac{g}{f}\Big),$$

hence

$$\begin{aligned}\Big(\frac{F}{G}\Big)\Big(\frac{G}{F}\Big)&=\Big(\frac{\operatorname{sgn}(F)}{p}\Big)^{\deg G}\Big(\frac{\operatorname{sgn}(G)}{p}\Big)^{\deg F}\Big(\frac{f}{g}\Big)\Big(\frac{g}{f}\Big)\\&=\Big(\frac{\operatorname{sgn}(F)}{p}\Big)^{\deg G}\Big(\frac{\operatorname{sgn}(G)}{p}\Big)^{\deg F}\Big(\frac{-1}{p}\Big)^{\deg F\deg G}.\end{aligned}$$

Thus the general reciprocity law (assuming we have proved it for monic prime polynomials) reads:

$$\Big(\frac{P}{Q}\Big)\Big(\frac{Q}{P}\Big)=\Big(\frac{\operatorname{sgn}(P)}{p}\Big)^{\deg Q}\Big(\frac{\operatorname{sgn}(Q)}{p}\Big)^{\deg P}\Big(\frac{-1}{p}\Big)^{\deg P\deg Q}.$$

Ok,now all we have to do is prove the reciprocity law. As a first step we derive Gauss's Lemma.

Gauss's Lemma

A halfsystem A modulo Q is a collection of $\frac{1}{2}(NQ-1)$ residue classes modulo Q with the property that every residue class mod Q can be written in the form $a \bmod Q$ or $-a \bmod Q$ for $a\in A$.

Now multiply each element a_i in the half system by P; we find $a_iP\equiv(-1)^{s(i)}a_j \bmod Q$ for some $s(i)\in\{0,1\}$ and some index j. Multiplying all these congruences and observing that the product over all the a_j on the right is equal to the product of the a_i on the left shows that $(\frac{P}{Q})_2=\prod(-1)^{s(i)}=(-1)^{\mu}$ with $\mu=\sum s(i)$.

Here's an example: consider $Q = X^2 + 1$ over $\mathbb{F}_3$. Then $NQ = 9$, hence $\{0, 1, 2, X, X + 1, X + 2, 2X, 2X + 1, 2X + 2\}$ is a complete system of residue classes modulo $X^2 + 1$, and $\{1, X, X + 1, X + 2\}$ is a half system modulo $X^2 + 1$ (this is most easily seen by picking any residue class like 1 and then omitting $-1 = 2$; next pick X and omit $-X = 2X$ etc. until you are done). Actually it is easy to give a halfsystem in general: if Q is a prime of degree n in $\mathbb{F}_p[X]$, let $B = \{1, 2, \ldots, \frac{p-1}{2}\}$ denote a halfsystem modulo p in integers, and put $A = \{f =\in \mathbb{F}_p[X] : \deg f < n, \operatorname{sgn}(f) \in B\}$, where $\operatorname{sgn}(f)$ denotes the leading coefficient of f.

In order to compute $(\frac{X+1}{X^2+1})_2$ using Gauss's Lemma we proceed as follows:

$$\begin{aligned}(X + 1) \cdot 1 &\equiv X + 1 \bmod X^2 + 1,\\ (X + 1) \cdot X &\equiv X^2 + X \equiv X + 2 \bmod X^2 + 1,\\ (X + 1) \cdot (X + 1) &\equiv 2X \equiv -X \bmod X^2 + 1,\\ (X + 1) \cdot (X + 2) &\equiv X^2 + X \equiv 1 \bmod X^2 + 1.\end{aligned}$$

Thus the number of minus signs is 1, hence $\mu = 1$, and thus $(\frac{X+1}{X^2+1})_2 = -1$.

With the preliminaries all in place, let us now move on to the actual proof of the quadratic reciprocity law.

Exercises

12.1 Compute $(\frac{X+1}{X^2+2})_2$ in $\mathbb{F}_5[X]$ using the definition (Euler's criterium) and using Gauss's Lemma.

12.2 Show that $A = \{f =\in \mathbb{F}_p[X] : \deg f < \deg Q, \operatorname{sgn}(f) \in B\}$ is a halfsystem modulo some prime Q in $\mathbb{F}_p[X]$ if B is a half system modulo p in $\mathbb{Z}$.