
Appendix 4C. Irreducible polynomials modulo p

The Fundamental Theorem of Algebra (section [3.22](#) of appendix 3F) states that every monic polynomial can be factored into monic irreducible polynomials in a unique way, which is completely analogous to how positive integers are factored into primes in the Fundamental Theorem of Arithmetic. In appendix 4B we associated the primes with $\zeta(s)$, the generating function for the integers. In this appendix we associate the irreducible monic polynomials mod p with the generating function for the monic polynomials mod p .

4.12. Irreducible polynomials modulo p

The monic polynomials mod p of degree d take the form

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0 \quad \text{such that each } a_j \in \mathbb{Z}/p\mathbb{Z}.$$

(The notation $\mathbb{Z}/p\mathbb{Z}$ was introduced in appendix 2A, to stand for the residue classes mod p .) There are p possible values for each a_j , and there are d different a_j to be selected, so there are a total of p^d monic polynomials mod p , of degree d .

Exercise 4.12.1. Suppose that $h(x)$ is a given polynomial mod p of degree d . Prove that there are exactly p^{m-d} monic polynomials in $\mathbb{F}_p[x]$ of degree m that are divisible by $h(x)$, provided $m \geq d$.

We will determine N_d , the number of monic *irreducible* polynomials mod p , of degree d . This is surprisingly straightforward using the Möbius inversion formula.⁶ It is most elegant if we define the analogy to the von Mangoldt function by

$$\Lambda(g(x)) = \begin{cases} \deg p(x) & \text{if } g(x) = p(x)^k \text{ with } p(x) \text{ irreducible and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

⁶Though there is no known analogous argument known for counting the primes themselves.

We are going to compute the degree of the product of all of the monic polynomials mod p , of degree m , in two different ways: Firstly, since there are p^m such polynomials and since they each have degree m , the total degree is mp^m . On the other hand, the degree of each such polynomial $h(x)$ equals the sum of the degrees of all of its irreducible monic factors (counting each factor the number of times it occurs in the factorization); that is,

$$\begin{aligned} \deg h(x) &= \sum_{\substack{p(x) \text{ monic irreducible} \\ k \geq 1, p(x)^k \text{ divides } h(x)}} \deg p(x) \\ &= \sum_{\substack{g(x) \text{ monic} \\ g(x) \text{ divides } h(x)}} \Lambda(g(x)). \end{aligned}$$

Therefore, summing this over all polynomials $h(x)$ of degree m we obtain

$$mp^m = \sum_{h(x) \text{ monic of degree } m} \deg h(x) = \sum_{g(x) \text{ monic}} \Lambda(g(x)) \sum_{\substack{h(x) \text{ monic of degree } m \\ g(x) \text{ divides } h(x)}} 1.$$

If $g(x)$ has degree d , then the last term is 0 unless $d \leq m$, in which case exercise [4.12.1](#) yields that

$$mp^m = \sum_{d=1}^m p^{m-d} \sum_{g(x) \text{ monic of degree } d} \Lambda(g(x)).$$

Subtracting p times this identity for $m-1$ from this identity for m , we obtain

$$(4.12.1) \quad \boxed{\sum_{g(x) \text{ monic of degree } m} \Lambda(g(x)) = p^m.}$$

The terms on the left-hand side are given by $g(x) = p(x)^k$ for each factorization $m = dk$ as $p(x)$ runs over the irreducible polynomials of degree d . Therefore

$$(4.12.2) \quad \sum_{d|m} dN_d = p^m,$$

and then, by the Möbius inversion formula (given in section [4.6](#) of appendix 4A, with $f(d) = dN_d$), we deduce that

$$(4.12.3) \quad \boxed{mN_m = \sum_{ab=m} \mu(a)p^b = \sum_{d|m} \mu(d)p^{m/d}.}$$

This is an *exact formula* for the number of irreducible polynomials of degree m . The largest term in the sum on the right side comes from $d = 1$, the term being p^m , so the number of irreducible polynomials of degree m is roughly p^m/m . The second largest term has $d = 2$ (when m is even), so equals $-p^{m/2}$ and otherwise is smaller. Therefore

$$|mN_m - p^m| \leq \sum_{d|m, d \neq 1} p^{m/d} \leq \sum_{k \leq [m/2]} p^k \leq 2p^{[m/2]}.$$

One can then deduce that $N_m > 0$ for all prime powers p^m ; that is, there exists an irreducible polynomial mod p of every degree ≥ 1 . This is useful since, as will

be explained in section [7.25](#) of appendix 7E, an irreducible polynomial mod p of degree n can be used to construct a finite field with p^n elements.

An alternative approach uses generating functions. We define

$$F(t) := \sum_{h(x) \text{ monic}} t^{\deg h(x)} = \sum_{m \geq 1} \sum_{h(x) \text{ monic of degree } m} t^m = \sum_{m \geq 1} p^m t^m = \frac{1}{1 - pt}.$$

On the other hand

$$t^{\deg h(x)} = \prod_{\substack{p(x) \text{ monic irreducible} \\ k \geq 1, p(x)^k \parallel h(x)}} t^{\deg(p(x)^k)} = \prod_{\substack{p(x) \text{ monic irreducible} \\ k \geq 1, p(x)^k \parallel h(x)}} t^{k \deg(p(x))}$$

and so, summing $t^{\deg h(x)}$ over all monic polynomials $h(x)$, we obtain (using the Fundamental Theorem of Arithmetic for polynomials to ensure unique factorization)

$$\begin{aligned} F(t) &= \prod_{p(x) \text{ monic irreducible}} \left(1 + t^{\deg(p(x))} + t^{2 \deg(p(x))} + \dots \right) \\ &= \prod_{d \geq 1} \prod_{p(x) \text{ monic irreducible, degree } d} (1 - t^d)^{-1} = \prod_{d \geq 1} (1 - t^d)^{-N_d}. \end{aligned}$$

We have therefore proved the remarkable identity

$$F(t) = \frac{1}{1 - pt} = \prod_{d \geq 1} (1 - t^d)^{-N_d}$$

which we have obtained much like we obtained Dirichlet series and their Euler products in appendix 4B. Now we take the logarithmic derivative to obtain

$$\frac{-F'(t)}{F(t)} = \frac{p}{1 - pt} = \sum_{d \geq 1} \frac{d N_d t^{d-1}}{1 - t^d}.$$

Multiplying through by t and expanding we have

$$\sum_{n \geq 1} p^n t^n = \frac{pt}{1 - pt} = \sum_{d \geq 1} d N_d \frac{t^d}{1 - t^d} = \sum_{d \geq 1} d N_d \sum_{m \geq 1} t^{dm} = \sum_{n \geq 1} \left(\sum_{d|n} d N_d \right) t^n.$$

Comparing the coefficients of t^n on both sides we again obtain the identity [\(4.12.2\)](#), which then leads to our exact formula for the number of irreducible polynomials of degree d .

Exercise 4.12.2. Prove that $N_m \leq p^m/m$.