Counting monic irreducible polynomials in $\mathbb{F}_p[x]$

Let p be prime. For $n \in \mathbb{N}$ denote by a_n the number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$. In this note we shall derive an explicit formula for a_n and in particular prove that $a_n > 0$ for any $n \in \mathbb{N}$. The latter, combined with Theorem 25.2 proved in class, implies that for any prime p and any $n \in \mathbb{N}$ there exists a field of order p^n.

From now on we fix a prime p. Let $f_1, f_2, \dots,$ be all monic irreducible polynomials in $\mathbb{F}_p[x]$ listed in some order (we may assume that we first list all monic irreducibles of degree 1, then degree 2 etc., but this is not essential). The fact that there are infinitely many monic irreducibles can be proved using Euclid's argument for the infiniteness of the set of prime numbers, but once again we do not need to assume this in advance. For any $i \in \mathbb{N}$ let $d_i = deg(f_i)$.

Definition: An infinite sequence of real numbers $\{x_i\}$ will be called *finitary* if there exists $N \in \mathbb{N}$ such that $x_n = 0$ for $n > N$.

Claim 1: *Given $n \in \mathbb{N}$ let S_n be the set of finitary sequences $\{m_i\}$ where each $m_i \in \mathbb{Z}_{\geq 0}$ and $\sum_{i=1}^{\infty} m_i d_i = n$. Then $|S_n| = p^n$.*

Proof: We shall establish a bijection between S_n and the set P_n of all monic polynomials of degree n in $\mathbb{F}_p[x]$. It is clear that $|P_n| = p^n$.

Define $\pi : S_n \to P_n$ by $\pi(\{m_i\}) = \prod_{i=1}^{\infty} f_i^{m_i}$ (the product on the right-hand side is in fact finite since the sequence $\{m_i\}$ is finitary). Note that π indeed maps S_n to P_n since

$$deg(\prod_{i=1}^{\infty} f_i^{m_i}) = \sum_{i=1}^{\infty} m_i\, deg(f_i) = \sum_{i=1}^{\infty} m_i d_i = n.$$

Uniqueness of factorization in $\mathbb{F}_p[x]$ implies that π is bijective. □

Claim 2: *The following equality of power series in $\mathbb{Z}[[t]]$ holds:*

$$\frac{1}{1-pt} = \prod_{i=1}^{\infty} \frac{1}{1-t^{d_i}}.$$

Remark: The product on the right-hand side is defined as $\lim_{N\to\infty} \prod_{i=1}^{N} \frac{1}{1-t^{d_i}}$, and the limit is taken with respect to the following notion of convergence on $\mathbb{Z}[[t]]$:

Given $u = \sum_{i=0}^{\infty} u_i t^i \in \mathbb{Z}[[t]]$ and a sequence $\{u_k\}$ in $\mathbb{Z}[[t]]$ where $u_k = \sum_{i=0}^{\infty} u_{i,k} t^i \in \mathbb{Z}[[t]]$, we say that $u_k \to u$ if for any $i \in \mathbb{N}$ there exists $K(i)$ such that $u_{i,k} = u_i$ for any $k > K(i)$.

Proof: Note that $\prod_{i=1}^{\infty} \frac{1}{1-t^{d_i}} = \prod_{i=1}^{\infty}(\sum_{m_i=0}^{\infty} t^{d_i m_i})$. Multiplying this product out (and using the above notion of the limit) we get $\prod_{i=1}^{\infty} \frac{1}{1-t^{d_i}} = \sum_{(m_1,m_2,\dots)} t^{\sum_{i=1}^{\infty} m_i d_i}$ where the sum is over all finitary sequences $\{m_i\}$. By Claim 1, for each $n \in \mathbb{N}$ there are precisely p^n finitary sequences of non-negative integers with $\sum_{i=1}^{\infty} m_i d_i = n$. Thus, $\prod_{i=1}^{\infty} \frac{1}{1-t^{d_i}} = \sum_{n=0}^{\infty} p^n t^n = \frac{1}{1-pt}$.
□

Now recall that a_n denotes the number of monic irreducible polynomials of degree n, and thus $a_n = |\{i \in \mathbb{N} : d_i = n\}|$. Thus, the equality in Claim 2 can be rewritten as

$$\frac{1}{1-pt} = \prod_{m=1}^{\infty} \Big(\frac{1}{1-t^m}\Big)^{a_m}.$$

Taking log of both sides, we get

$$\log\Big(\frac{1}{1-pt}\Big) = \sum_{m=1}^{\infty} a_m \log\Big(\frac{1}{1-t^m}\Big).$$

Since $\log(\frac{1}{1-x}) = \sum_{j=1}^{\infty} \frac{x^j}{j}$, we get

$$\sum_{n=1}^{\infty} \frac{p^n}{n} t^n = \sum_{m=1}^{\infty} a_m \Big(\sum_{j=1}^{\infty} \frac{t^{jm}}{j}\Big)$$

The coefficient of t^n on the left-hand side is equal to $\frac{p^n}{n}$, and the coefficient of t^n on the right-hand side is equal to $\sum_{n=mj} \frac{a_m}{j} = \sum_{n=mj} \frac{m a_m}{mj} = \sum_{m|n} \frac{m a_m}{n}$. Thus, we must have

$$\sum_{m|n} m a_m = p^n \text{ for any } n \in \mathbb{N}. \qquad (***)$$

Formula (***) already implies that $a_n > 0$ for any n. Indeed, suppose not and there exists $n \in \mathbb{N}$ such that $a_n = 0$. Since $a_m \le p^m$ for any m and all proper divisors of n do not exceed $n/2$, we get $p^n \le \sum_{m=1}^{[n/2]} m p^m < [n/2] \frac{p^{[n/2]+1}}{p-1} \le n p^{[n/2]}$. Therefore, $p^{n-[n/2]} < n$, which is easily seen to be impossible. However, one can go further and deduce a simple formula for $\{a_n\}$ from (***) using Möbius inversion.

Möbius inversion: Let V be the set of all functions from $\mathbb{N}$ to $\mathbb{Z}$ (in fact $\mathbb{Z}$ can be replaced by any commutative ring with 1), and define a binary operation $*$ on V by setting

$$(f * g)(n) = \sum_{d|n} f(d) g(n/d).$$

It is clear that $*$ is commutative, and it is not hard to check that $*$ is also associative. The set V does not become a group with this operation (even if we remove the zero function); however, there is an identity element $\epsilon : \mathbb{N} \to R$ defined by $\epsilon(1) = 1$ and $\epsilon(n) = 0$ for $n > 1$. It turns out that the constant function $\mathbf{1}$ (defined by $\mathbf{1}(n) = 1$ for any n) has inverse with respect to this operation, called the Möbius function. It is denoted by μ and defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n = p_1 \dots p_r \text{ where } p_1, \dots, p_r \text{ are distinct primes} \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p. \end{cases}$$

Now let us go back to our computation. Consider the functions f and g defined by $f(n) = p^n$ and $g(n) = na_n$ for $n \in \mathbb{N}$. Formula (***) can now be rewritten as equality $f = g * \mathbf{1}$ in V. Multiplying both sides by the Möbius function μ and using the fact that $\mathbf{1} * \mu = \epsilon$ and ϵ is the identity element with respect to $*$, we get $f * \mu = (g * \mathbf{1}) * \mu = g * (\mathbf{1} * \mu) = g * \epsilon = g$. Thus, for any $n \in \mathbb{N}$ we get $g(n) = (f * \mu)(n) = \sum_{d|n} f(d)\mu(n/d)$, whence

$$a_n = \frac{1}{n} \sum_{d|n} p^d \mu(n/d).$$

For instance, if n is prime, $a_n = \frac{1}{n}(p^n - p)$. If n is not prime, the expression is more complicated, but for any small n computation of a_n is very quick.