Article 1: Finding Irreducible Polynomials

Debadatta Kar

June 2, 2025

1 Introduction

We want to generate an irreducible polynomial in any given field.
$x^{p^n} - x$ is pricisely the product of all distinct irreducible monic polynomials in $F_p[x]$ whose degree divides n.

Example 1.1. *Over F_2 we have to find all monic irreducible polynomials whose degree divides 2.*
Take $p = 2$ and $q = 2$ which gives the polynomial $x^{2^2} - x$

$$x^{2^2} - x = x^4 - x = x \cdot (x^3 - 1) = x. \cdot (x - 1) \cdot (x^2 + x + 1)$$

Clearly $x, x - 1, x^2 + x + 1 \in F_2[x]$ are all monic irreducible polynomials of degree ≤ 2.

2 Some Results

Suppose that we have a field F_q where q is some prime or power of a prime. Consider the follwing notations:

1. $N_q(d) :=$ number of monic irreducible polynomilas of degree d in F_q.
2. $\mu(n)$ is the Möbious function defined in 3

Result 2.1.

$$q^n = \sum_{d|n} d \times N_q(d) \tag{1}$$

Result 2.2.

$$\mu(n) = \begin{cases} 1; & n = 1 \\ (-1)^k; & n \text{ is product of } k \text{ distinct primes} \\ 0; & \text{if for some prime } p,\ p^2 \mid n \end{cases} \tag{2}$$

Theorem 2.3. *Let $\mu(x)$ be the Möbius function then*

$$\sum_{d|n} \mu(d) = \begin{cases} 0; & n > 1 \\ 1; & n = 1 \end{cases} \tag{3}$$

Proof. For the case $n = 1$ it is trivial.
For $n > 1$ we have

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i_1=1}^{k} \mu(p_i) + \sum_{1 \leq i_1 < i_2 \leq k} \mu(p_{i_1} p_{i_2}) + \cdots + \mu(p_{i_1} p_{i_2} \cdots p_{i_n})$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k$$
$$= \binom{k}{0}(-1)^0 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k$$
$$= (1 + (-1))^k$$
$$= 0$$

□

We keep this as a result, to use in the upcoming part.

Theorem 2.4. *The total number of irreducible polynomilas of degree d is calculated explicitly by using the Möbious function as:*

$$N_q(d) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \times q^d = \sum_{d|n} \mu(d) \times q^{n/d}$$

Proof. To prove the above result we will use the Möbious inversion formula.

Let $h, H : \mathbb{N} \to G$ be a map.
H is defined as $H(n) = \sum_{d|n} h(n)$ for all natural number n. Then one can also recover $h(n)$ from $H(n)$ as

$$h(n) = \sum_{d|n} H\left(\frac{n}{d}\right) \mu(d) = \sum_{d|n} H(d)\mu\left(\frac{n}{d}\right)$$

We know that $q^n = \sum_{d|n} d \times N_1(d)$
Let's define $h(n) = n \times N_q(n)$
Now,

$$H(n) = \sum_{d|n} h(n) = \sum_{d|n} n \times N_q(d)$$

By applying the inversion rule we can deduce,

$$n \times N_q(n) = \sum_{d|n} \mu(d) q^{n/d}$$

and subsequently,

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

□

The theorem above gives an explicit way to count the number of irreducible polynomials of degree d in a field F_q.

Lemma 2.5. *Existence of irreducible polynomials*

We have

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d \geq \frac{1}{n}(q^n - q^{n-1} + \cdots + q^1) = \frac{1}{n}\left(q^n - \frac{q^n - q}{q-1}\right) > 0$$

This fact concludes the existence of irreducible polynomials.

3 Finding Irreducible polynomials

In this part we will show a probabilistic algorithm to find a random monic polynomial defined over a field.
Lets define P_d as the product of all irreducible monic polynomials of degree d over F_q. Now, $deg(P_d) = d \times N_q(d)$ Previously, we have,

$$q^n = \sum_{d|n} d \times N_q(d)$$

We will now try to bound N_q in terms of q and n.

$$q^n = n \times N_q(n) + \text{rest terms}$$

Since, the rest terms are all positive,

$$q^n \geq n \times N_q$$

and finally,

$$N_q \leq \frac{q^n}{n}$$

Now, on manupulating the summation,

$$\sum_{d<n/2} d \times N_q(d) \leq \sum_{d\ len/2} d \times \frac{q^d}{d} = \sum_{d\ len/2} q^d \leq \frac{q^{n/2+1-} - q}{q-1} \leq 2q$$

so from the above expression,

$$q^n = n \times N_q(n) + \text{rest terms} \leq n \times N_q(d) + 2q^{n/2}$$

and this gives,

$$n \times N_q(d) \geq q^n - 2q^{n/2}$$

and finally,

$$N_q(d) \geq \frac{q^n - 2q^{n/2}}{n}$$

Putting all things together we get

$$\frac{q^n - 2q^{n/2}}{n} \leq N_q(d) \leq \frac{q^n}{n} \tag{4}$$

Now the above inequality suggests that a randomized algorithm can give us an irreducible polynomial efficiently.

4 Algorithm

1. Pick a monic polynomial f of degree n over F_q uniformly at random
2. Test if f is irreducible.
3. If not go to step 1.

References

[1] Lidl R, Niederreiter H, *Finite Fields*, 2nd ed. Cambridge University Press; 1996

[2] Markus Blaser, Chandan Saha, *Computational Number Theory and Algebra*, Notes, IISc.