Article 2: Finding Irreducible Polynomials

Debadatta Kar

June 9, 2025

1 Introduction

We want to prove Theorem 1.4 in this article, which we used as a result in the previous article (article 1).

Theorem 1.1. *If F is a finite field with q elements, then every element of F satisfies $a^q = a$.*

Proof. It is trivial to see that $0 \in F$ satisfies the relation.
For the rest of the elements we have F^*, which is a cyclic group of order $q-1$
Thus, $a^{q-1} = 1$
Now multiplying a on both sides, we obtain

$$a^q = a$$

□

Theorem 1.2. *Let $f \in F[x]$ be irreducible and $deg(f) = m$ then $f|x^{q^n} - x$ iff $m|n$.*

Proof. Let, $m|n$ then we have F_{q^m} is a subfield of F_{q^n}.
If α is a root of f in splitting field of f over F_q then $[F_q(\alpha) : F_q] = m$ and so $F_q(\alpha) = F_{q^m}$.
and since, $\alpha \in F_{q^m}$.

$$\alpha^{q^m} = \alpha$$

and thus, α is a root of $x^{q^n} - x \in F_q[x]$

Conversely, if $f|x^{q^n} - x$
Let α be a root of f in its splitting field over F_q.
Then, we have $\alpha^{q^n} = \alpha$ so that $\alpha \in F_{q^n}$.
Now, $F(\alpha)$ is a subfield of F_{q^n}. And if we consider $[F(\alpha) : F_{q^n}] = m$ and $[F_{q^n} : F_q] = n$.
we have,

$$m|n$$

□

Result 1.3. *$b \in F$ is a multiple root of $f \in F[x]$ iff it is a root of both f and f'*

Theorem 1.4. *$x^{p^n} - x$ is precisely the product of all distinct irreducible monic polynomials in $F_p[x]$ whose degree divides n*

Proof. From Theorem 1.2, we can see that all the factors of $x^{q^n} - x$ are of degree d such that $d|n$. Now we claim that all the factors are non-repetitive. We will use result 1.3 here. $g(x) = x^{q^n} - x$, Then on differentiating w.r.t x we obtain,

$$g'(x) = q^n x^{q^n - 1} - 1 = 0 - 1 = -1$$

Now, for any α we have $g'(\alpha) \neq 0$ as $g'(x) = -1$.
Clearly, this shows that we don't have multiple roots. Thus, the distinct factors of $x^{q^n} - x$ can be expressed as the product of irreducible polynomials, s.t. none of them is repeated. $\square$

2 Algorithm for Checking Irreducibility

Suppose that we have a field F_q where q is some prime or power of a prime.
We know that $x^{q^n} - x$ factors out as the product of all monic irreducible polynomials of degree $d|n$.
Using this fact we obtain the following algorithm:

Algorithm 1 Polynomial Irreducibility Check

```
Initialize P(x) ← x
for i = 1 to n do
    P(x) ← (P(x))^q mod T(x)
end for
if P(x) = x then
    return true
else
    return false
end if
```

Here we are given a polynomial $T(x)$, which is of degree n and whose irreducibility is verified. Similarly, we can also check irreducibility by computing the gcd.

References

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

[2] Richard P. Brent, Paul Zimmermann, *Three Ways to Test Irreducibility*