# There's Someting About Primitive Polynomials

Paul Stankovski

A polynomial $f(x) \in \mathbb{F}_p[x]$ is a primitive polynomial of a finite field extension $\mathbb{F}_{p^k}$ if it has degree $k$ and has a root $\alpha \in \mathbb{F}_{p^k}$ ($f(\alpha) = 0$) that generates all non-zero elements of $\mathbb{F}_{p^k}$ (by iterating $\{\alpha, \alpha^2, \alpha^3, \ldots\}$).

A primitive polynomial must necessarily be irreducible, but all irreducible polynomials are not primitive.

A somewhat longer explanation follows below.

## 1 Finite Field Basics

A finite field $\mathbb{F}_q$ of order (the number of elements) $q$ exists if and only if $q$ is a prime power $p^k$ ($p$ is prime, $k$ is a positive integer).

All finite field of the same order are isomorphic. That is, even if two finite field of the same order are represented differently, they still *are* the same field. While the elements may have been relabeled from one representation to another, they still behave the same way.

The non-zero elements (all except the zero) of a finite field form a multiplicative group that is cyclic, so this group can be generated by one single element.

## 2 Finite Fields $\mathbb{F}_p$ of Prime Order

Finite fields $\mathbb{F}_p$ of prime order behave exactly like $\mathbb{Z}/p\mathbb{Z}$ (the integers modulo $p$). These are isomorphic.

## 3 Finite Fields $\mathbb{F}_{p^k}$ of Prime Power Order

Finite fields $\mathbb{F}_{p^k}$ of prime power order (with $k \geq 2$) *do not* behave like the integers modulo $p^k$. Instead, we can "expand" $\mathbb{F}_p$ by constructing an extension field $\mathbb{F}_{p^k}$ using polynomials in a special way. We do this because that is how $\mathbb{F}_{p^k}$ *does* behave, like this somewhat special bunch of polynomials.

As an example, consider $\mathbb{F}_{2^4} = \mathbb{F}_{16}$. Using the primitive[1] polynomial $f(x) = x^4 + x + 1$, we can construct $\mathbb{F}_{2^4}$ as $\mathbb{F}_2[x] / \langle f(x) \rangle = \mathbb{F}_2[x] / \langle x^4 + x + 1 \rangle$. That

[1] Keep reading, it will be explained below.

is, our finite field elements can be represented by polynomials over $\mathbb{F}_2$ that are taken modulo the polynomial $f(x)$.

The polynomial $f(x)$ corresponds to the zero element, so we can write

$$x^4 + x + 1 = 0,$$

which we can also express as a rule for reducing exponents in our polynomials according to

$$x^4 = x + 1.$$

Using this rule, we can reduce every polynomial of degree 4 or higher to a degree of 3 or less. The elements of $\mathbb{F}_2\big[x\big]/\left\langle x^4 + x + 1\right\rangle$ are the polynomials

$$a_3x^3 + a_2x^2 + a_1x + a_0,$$

where all $a_i \in \mathbb{F}_2$. With four such $a_i$, and each taking the values 0 or 1, there are $2^4 = 16$ different polynomials/elements.

Addition and multiplication on these polynomials are performed "as usual", with the additional reduction step at the end to reduce the degree if necessary.

# 4 Multiplication Table for $\mathbb{F}_2\big[x\big]/\left\langle x^4 + x + 1\right\rangle$

Now, letting the symbol $\alpha$ denote a zero of $f(x)$, so that $f(\alpha) = 0$, we can write the reduction rule above as

$$\alpha^4 = \alpha + 1.$$

We can also use the symbol $\alpha$ to write a multiplication table for $\mathbb{F}_2\big[x\big]/\left\langle x^4 + x + 1\right\rangle$.

$$
\begin{aligned}
&1,\\
&\alpha,\\
&\alpha^2,\\
&\alpha^3,\\
&\alpha^4 = \alpha + 1,\\
&\alpha^5 = \alpha^2 + \alpha,\\
&\alpha^6 = \alpha^3 + \alpha^2,\\
&\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1,\\
&\alpha^8 = \alpha^4 + \alpha^2 + \alpha = \alpha^2 + 1,\\
&\alpha^9 = \alpha^3 + \alpha,\\
&\alpha^{10} = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1,\\
&\alpha^{11} = \alpha^3 + \alpha^2 + \alpha,\\
&\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1,\\
&\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + 1,\\
&\alpha^{14} = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + 1,\\
&\alpha^{15} = \alpha^4 + \alpha = 1.
\end{aligned}
$$

Note that we cycle through after 15 iteration, returning to 1 with $\alpha^{15}$. If all non-zero elements (15 out of the 16 in $\mathbb{F}_{16}$ in this case) can be generated in this way, then the polynomial $f(x)$ is *primitive*.

Replacing $\alpha$ with $x$, one can see that all non-zero polynomials over $\mathbb{F}_2$ with degree 3 or lower are present. The non-zero elements form a cyclic subgroup (under multiplication), and every such element can be expressed as a power of $x$. One way of multiplying, say, $x^3 + x^2 + 1$ with $x^2 + x + 1$ is to realize that they equal $x^{13}$ and $x^{10}$, respectively, so their product is $x^{13+10} = x^{23}$, and we get

$$x^{23} = x^8 = x^2 + 1$$

simply by reducing the exponent modulo 15 and peeking into our multiplication table.

If we would have chosen a polynomial that is not primitive, then we would have cycled though earlier. In this case, since a subgroup must divide the order of the entire group, we would have found that either $\alpha^3 = 1$ or $\alpha^5 = 1$.

If you are merely interested in finding out if a given polynomial is primitive, then it suffices to cycle through to the largest proper divisor of $q - 1$. In our example above, when we have shown that $\alpha^5 = \alpha^2 + \alpha \neq 1$, then we know that the polynomial is primitive, since the "next" opportunity for a full cycle is at $\alpha^{15}$.