

# Re: Primitive polynomials over $GF(2^m)$

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg00340.html>

---

- *From:* Derek Holt <mareg@xxxxxxxxxxxxxx>
  - *Date:* Fri, 02 Nov 2007 02:42:11 -0700
- 

Timothy Murphy wrote:

Derek Holt wrote:

A primitive polynomial is an irreducible polynomial of degree  $m$  with the added constraint that the smallest integer  $n$  for which  $P(x)$  divides  $X^n + 1$  is  $n = 2^m - 1$ .  
..(1)

...

I don't agree! The usual definition is that a primitive polynomial is one whose roots are generators of the multiplicative group of the extension field, and the definition given above is equivalent to that.

Except it should be  $x^n - 1$ , I guess ...

Same thing in characteristic 2, but I agree it would be preferable to write  $x^n - 1$ .

Re: Primitive polynomials over  $GF(2^m)$

Sorry, didn't read carefully enough.

Of course the result holds in any characteristic (with  $p^m - 1$ ).

Incidentally, I never realized that primitive polynomial had another meaning: a polynomial in  $Z[x]$  with coprime coefficients. I hope that meaning is obsolete.

I don't think it is obsolete, but fortunately there is very little danger of any confusion. One meaning only applies to finite fields, and a set of elements of a field is coprime, so "coprime coefficients" is not a sensible concept for polynomials over fields.

Incidentally, both MathWorld and Wikipedia have incorrect/inconsistent definitions of primitive polynomials over finite fields.

MathWorld:

A primitive polynomial is a polynomial that generates all elements of an extension field from a base field.

But then in the following discussion, they are clearly thinking of it as meaning a polynomial whose roots generate the multiplicative group of the field.

Wikipedia:

In field theory, a branch of mathematics, a primitive polynomial is the minimal polynomial of a primitive element of the extension field  $GF(p^m)$ . In other words, a polynomial  $F(X)$  with coefficients in  $GF(p) = Z/pZ$  is a primitive polynomial if it has a root in  $GF(p^m)$  such that the linear span of  $\{1, \alpha, \alpha^2, \alpha^3, \dots\}$  over  $GF(p)$  is the entire field  $GF(p^m)$ , and moreover,  $F(X)$  is the smallest degree polynomial having as root.

The "in other words" part of the definition is wrong, but the following discussion is correct.

Derek Holt.

.