

# Re: Primitive polynomials in extended Galois fields

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-03/msg00803.html>

---

- *From:* Phil Carmody <[thefatphil\\_demunged@xxxxxxxxxxxx](mailto:thefatphil_demunged@xxxxxxxxxxxx)>
  - *Date:* 28 Mar 2007 12:50:10 +0300
- 

"Anup" <[anupkc@xxxxxxxx](mailto:anupkc@xxxxxxxx)> writes:

Hello All

I am trying to generate multi-level sequences in extended Galois fields, GF(4) to be precise, which satisfy the de Bruijn or window property.

The approach I followed was to use a Linear Shift Register with a primitive polynomial in GF(4) as the generator polynomial. But this requires the primitive polynomials to be generated in the extended finite field. For this I could hardly find any fast algorithm. So I resorted to generating irreducible polynomials ( using the inbuilt function from the NTL library at <http://shoup.net/ntl/>) and checking them for primitivity – by ensuring that they are of maximal order.

But this seems to be a costly exercise, since finding out the order requires  $4^{\text{degree}-1}$  division checks. ( where degree is the degree of primitive polynomial to be generated).

Surely the number of checks is the number of factors in the factorisation of the order of the multiplicative group?

Phil

—

"Home taping is killing big business profits. We left this side blank so you can help." — Dead Kennedys, written upon the B-side of tapes of /In God We Trust, Inc./.

.