

Irreducible cubic polynomial in char 2

Source: <http://sci.tech-archive.net/Archive/sci.math/2008-04/msg00291.html>

- *From:* ema <emanuele.cesena@xxxxxxxxxx>
 - *Date:* Wed, 2 Apr 2008 07:20:02 -0700 (PDT)
-

Hi,

I have a polynomial $F = x^3 + x + k$, with k in \mathbb{F}_q , $q=2^m$ (m prime).
I know that F is irreducible, and I would like to find a root in a degree 3 extension of \mathbb{F}_q .

Well, if I take $L = \mathbb{F}_q[x]/(F)$, then x is a solution.
However, I prefer to consider $L = \mathbb{F}_q[a]/(a^3+a+1)$.

So, I'd like to find x_i , s.t. $x = x_2 a^2 + x_1 a + x_0$ and $F(x)=0$.
It is easy to prove that $x_0 = 0$.
Any idea on how to explicitly find x_1/x_2 ?
It would be nice to find them as function of k ... please note that I need only a single solution.

I'm looking at Bill Allombert "Explicit Computation of Isomorphisms Between Finite Fields", *Finite Fields*, 8, 2002, 332-342.
<http://www.math.u-bordeaux.fr/~allomber/fpisom.ps>
but at the moment I have no useful result.

Thank you in advance,

—
ema

.