

Re: Computing in finite fields: what programming language to choose?

Source: <http://coding.derkeiler.com/Archive/General/comp.programming/2006-09/msg00148.html>

- *From:* "Rob Thorpe" <robert.thorpe@xxxxxxxxxxxxx>
 - *Date:* 6 Sep 2006 11:03:02 -0700
-

xarnaudx@xxxxxxxx wrote:

hi,

i've some work to do concerning computing in finite fields and i would like to know what programming language would fit the best.

I must be able to create fields and manipulate their elements:

$ans = \alpha^4 + \alpha^7$

$ans = 01011 * 12012$ (characteristic not always 2)

Also i must be able to play with polynomials:

$F(X) = 01011 * X^2 + \alpha^5 * X + 12121$

...and also on a higher levels:

$F(Z) = \text{Sum}(a:A) \text{Product}(b:B, b!=a) (G(a) * Z + H(b))$

So now the question is: what programming language fits the best for these type of calculus?

There are several possibilities, you could use a programming languages specifically for mathematics. AXIOM could probably do it.

You could also do it using normal programming languages. Languages that support lambda calculus would be useful as another suggested. In Lisp you could create a mini-language within lisp that described finite fields and use that. This path is not simple for a beginner though.

So, I'd recommend using a mathematical language like Axiom or something specific to the problem. Someone else mentioned Gap which looks very close to what you want.

.