



Re: root of polynomial over galois field

Examples 8.4–8.5 may not be sufficient explanation. To help you out,

I will step you through some iterations of the inner while loop of the algorithm,

pointing out some facts that could lead to loop invariants and a correctness

proof, if they were developed fully enough. At the outset,

$$a = \text{product}(f_k^k, k)$$

$$b = a' = \text{sum}(k * f_k' / f_k, k) * a \leq \text{Terms with } p|k$$

vanish here.

$$c = \text{gcd}(a, b) = \text{product}(f_k^{(k-1)}, p \text{ does not divide } k) * \text{product}(f_k^k, p \text{ divides } k)$$

$$w = a/c = \text{product}(f_k, p \text{ does not divide } k)$$

Here we've written "a" in the form of a squarefree factorization, the  $f_k$  being

pairwise relatively prime. The "b" has the interesting property regarding " $p|k$ ".

This results in "c" resembling "a", but the exponents of the  $f_k$  are reduced by 1

iff  $p$  does not divide  $k$ . I refer you to Examples 8.4–8.5 for the concrete examples.

In the first iteration of the while loop,

$$y = \text{gcd}(w, c) = \text{product}(f_k, p \text{ does not divide } k \text{ and } k > 1)$$

$$z = f_1 \leq \text{!!!!}$$

$$w = \text{product}(f_k, p \text{ does not divide } k \text{ and } k > 1)$$

$\leq$  Update to  $w$

$$c = \text{product}(f_k^{(k-2)}, p \text{ does not divide } k \text{ and } k > 1) * \text{product}(f_k^k, p$$

## Re: root of polynomial over galois field

divides  $k$ )  $\Leftarrow$  Update to  $c$

Next iteration of the while loop,  $z=f_2$ , and the " $k>1$ " changes to " $k>2$ ".

Next

iteration of the while loop,  $z=f_3$ , and the " $k>1$ " changes to " $k>3$ ". Etc.

The  $f_k$

factors of  $w$  are all picked off eventually, leaving  $w=1$  and

$c = \text{product}(f_k^k, p \text{ divides } k)$

Here we reach the Line 14, but now we see  $c = \text{product}(f_k^{(k/p)}, p \text{ divides } k)^p$  !

Conclusion: whenever the algorithm reaches Line 15, " $c(x) \leftarrow c(x)^{1/p}$ ",

the

$c(x)$  will indeed always be a perfect  $p$ th power of a polynomial in

$\text{GF}(q)[x]$ .

The book is correct, it just needed a little more elaboration.

Hello again,

Just another question, am I right in thinking that when dividing two polynomials over a Galois field that this is not always possible? Sorry this may seem quite a basic question but its been a while since I did any abstract algebra and I've forgotten nearly all of it.

What I have done is to take a standard Euclidean Division routine and convert it to run in modular arithmetic, and use that as a means of dividing two polynomial over  $\text{GF}(q)$ . But I have discovered instances where the routine fails, and have read in Geddes, Czapor & Labahn that polynomial division over a finite field is not always possible, but it doesnt go in to too much detail and also I cant seem to find anything on google about this.

None of this is surprising considering that a multiplicative inverse does not always exist for any element in a Galois field (that is true isnt it..??)

For instance taking the polynomials  $P1 = x^6$  and  $P2 = 2x^3 + 2$  and dividing  $P1$  by  $P2$  over  $\text{GF}(4 = 2^2)$ , then this clearly cant be done as no multiplicative inverse of the leading coefficient of  $P2$  (that being 2)

Re: root of polynomial over galois field

## Re: root of polynomial over galois field

exists in  $GF(4)$ .

So if this is true then am I correct in also thinking that the modular GCD of these polynomials could not be defined either as using the Euclidean algorithm to find it is dependent on the division of polynomials? Or is it simply set to '1' as a default in this instance?

This all being true then how are the GCD and division calculations in Algorithm 8.3 able to be relied upon for the case where 'q' is not prime? Am I misunderstanding something fundamental here about abstract algebra?