CoCoALib - Feature #667

factor: multivariate + finite characteristic

02 Mar 2015 11:23 - Anna Maria Bigatti

Status:	New	**Start date:**	02 Mar 2015
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	New Function	**Estimated time:**	0.00 hour
Target version:	CoCoALib-1.0	**Spent time:**	0.50 hour

Description

(if I remember well)
The problem about factorizing a multivariate polynomial in finite characteristic was just the square free decomposition.
Now that that step has been solved+implemented can we close the factor limitation?

Related issues:

Related to CoCoALib - Feature #664: Impl small non-prime finite fields (using...	**Resolved**	**11 Feb 2015**

History

#1 - 04 Mar 2015 13:31 - John Abbott

The squarefree decomposition is the normal first step, but there are other problematic steps (*e.g.* mapping down to univariate by substitution).

Here is an example: ((x^3-x)*y+1)*((y^3-y)*x+1) in FF_3 any substitution will make one of the factors collapse to 1; to avoid this one normally passes to an algebraic extension, factorizes there, and then recombines the factors to obtain the factorization in the smaller field.
[actually, my information may be outdated now]

Kaltofen mapped down to bivariate; I think he showed that this is "safe with high probability". The final step down to univariate remains a problem though, I think. I will have to reread the relevant articles.

#2 - 04 Mar 2015 16:45 - Anna Maria Bigatti

John Abbott wrote:

> The squarefree decomposition is the normal first step, but there are other problematic steps (*e.g.* mapping down to univariate by substitution).
>
> Here is an example: ((x^3-x)*y+1)*((y^3-y)*x+1) in FF_3 any substitution will make one of the factors collapse to 1; to avoid this one normally passes to an algebraic extension, factorizes there, and then recombines the factors to obtain the factorization in the smaller field.

ah, ok. Far more difficult that I thought.

Problem 2: and how difficult is it to factorize on an algebraic extension? (supposing we have algebraic extensions ;-)

#3 - 04 Mar 2015 20:08 - John Abbott

Factorizing in F_q[x] is largely the same as factorizing in F_p[x]; the algorithm is essentially the same (but coeff arithmetic is not, of course).

Werner asked for a decent impl of F_q, at least for small field sizes. I just have to find the time and energy to do it...