CoCoALib - Feature #797

SmallFpImpl: make it faster

07 Nov 2015 21:57 - John Abbott

Status:	In Progress	**Start date:**	07 Nov 2015
Priority:	Normal	**Due date:**	
Assignee:	John Abbott	**% Done:**	10%
Category:	Improving	**Estimated time:**	0.00 hour
Target version:	CoCoALib-1.0	**Spent time:**	1.25 hour

Description

After comparing gcd for DUPFp and DUPFF, I saw that the latter was significantly faster (*e.g.* factor 2 or more in some cases)

Investigating I saw that the old finite field impl did create log/exp tables (for primes up to a certain limit), and these tables were used to compute implement "shift-add" inside the euclidean algorithm.

Consider whether to have a smallfp impl which combines both SmallFpImpl and SmallFpLogImpl.

Related issues:

Related to CoCoALib - Feature #1154: SmallFpImpl: new ctor arg to say do-not-...	**Closed**	**11 Feb 2018**

History

#1 - 07 Nov 2015 22:35 - John Abbott

- Status changed from New to In Progress

- Assignee set to John Abbott

- % Done changed from 0 to 10

The speed gains varies form platform to platform -- surprise, surprise!

The old DUPFF code was (significantly) faster for GCD of high degree polys with coeffs in medium sized finite fields. The new code was faster (on my old MacBook Pro) when the prime was large (*e.g.* 32003). I should conduct some more speed tests.

Should SmallFpImpl automatically include a SmallFpLogImpl? Or should there be a new SmallFpXYZ class which includes both?

#2 - 02 Dec 2015 15:01 - John Abbott

Some (more or less) obvious comments:

- the advantage of having log/exp tables is that some computations can be noticeably faster (*e.g.* gcd as mentioned in the intro)
- the disadvantage is that it takes longer to construct a (small prime) finite field, and the field itself occupies more space (for the tables)

Overall, I think it is probably worth offering a combined implementation sooner or later; there will also be the question of which impl to use by default when the user asks for a small, prime finite field.

#3 - 11 Feb 2018 20:52 - John Abbott

- Related to Feature #1154: SmallFpImpl: new ctor arg to say do-not-check-that-arg-is-prime added