FLINT 2.3

William Hart   Fredrik Johansson   Sebastian Pancratz,
Andy Novocin   (David Harvey)

December 16, 2011

iFLINT 2.3

William Hart   Fredrik Johansson   Sebastian Pancratz,
Andy Novocin   (David Harvey)

December 16, 2011

Introduction to FLINT

Fast Library for Number Theory

History of FLINT

- Began in late 2006

History of FLINT

- Began in late 2006
- Version 0.1 in Sage by August 2007

History of FLINT

- Began in late 2006
- Version 0.1 in Sage by August 2007
- Version 1.0 released December 2007

History of FLINT

- Began in late 2006
- Version 0.1 in Sage by August 2007
- Version 1.0 released December 2007
- I started a complete rewrite of FLINT from scratch in secret September 2009 – flint 2 was born

History of FLINT

- Began in late 2006
- Version 0.1 in Sage by August 2007
- Version 1.0 released December 2007
- I started a complete rewrite of FLINT from scratch in secret September 2009 – flint 2 was born
- Version 1.6 December 2010 release – ends flint 1 series

History of FLINT

- Began in late 2006
- Version 0.1 in Sage by August 2007
- Version 1.0 released December 2007
- I started a complete rewrite of FLINT from scratch in secret September 2009 – flint 2 was born
- Version 1.6 December 2010 release – ends flint 1 series
- Version 2.0 released January 2011

History of FLINT

- Began in late 2006
- Version 0.1 in Sage by August 2007
- Version 1.0 released December 2007
- I started a complete rewrite of FLINT from scratch in secret September 2009 – flint 2 was born
- Version 1.6 December 2010 release – ends flint 1 series
- Version 2.0 released January 2011
- Version 2.3 released December 2011

What does FLINT do?

- Over 100,000 lines of C code

What does FLINT do?

- Over 100,000 lines of C code
- Word sized integer and modular arithmetic

What does FLINT do?

- Over 100,000 lines of C code
- Word sized integer and modular arithmetic
- Multiprecision integer and rational arithmetic

What does FLINT do?

- Over 100,000 lines of C code
- Word sized integer and modular arithmetic
- Multiprecision integer and rational arithmetic
- Multiprecision integer factoring (MPQS)

What does FLINT do?

- Over 100,000 lines of C code
- Word sized integer and modular arithmetic
- Multiprecision integer and rational arithmetic
- Multiprecision integer factoring (MPQS)
- *p*-adic arithmetic

What does FLINT do?

- Over 100,000 lines of C code
- Word sized integer and modular arithmetic
- Multiprecision integer and rational arithmetic
- Multiprecision integer factoring (MPQS)
- *p*-adic arithmetic
- Dense univariate polynomial arithmetic over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, *p*-adics

What does FLINT do?

- Over 100,000 lines of C code
- Word sized integer and modular arithmetic
- Multiprecision integer and rational arithmetic
- Multiprecision integer factoring (MPQS)
- *p*-adic arithmetic
- Dense univariate polynomial arithmetic over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, *p*-adics
- Power series over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$

What does FLINT do?

- Over 100,000 lines of C code
- Word sized integer and modular arithmetic
- Multiprecision integer and rational arithmetic
- Multiprecision integer factoring (MPQS)
- *p*-adic arithmetic
- Dense univariate polynomial arithmetic over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, *p*-adics
- Power series over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$
- Univariate polynomial factoring over $\mathbb{Z}$

What does FLINT do?

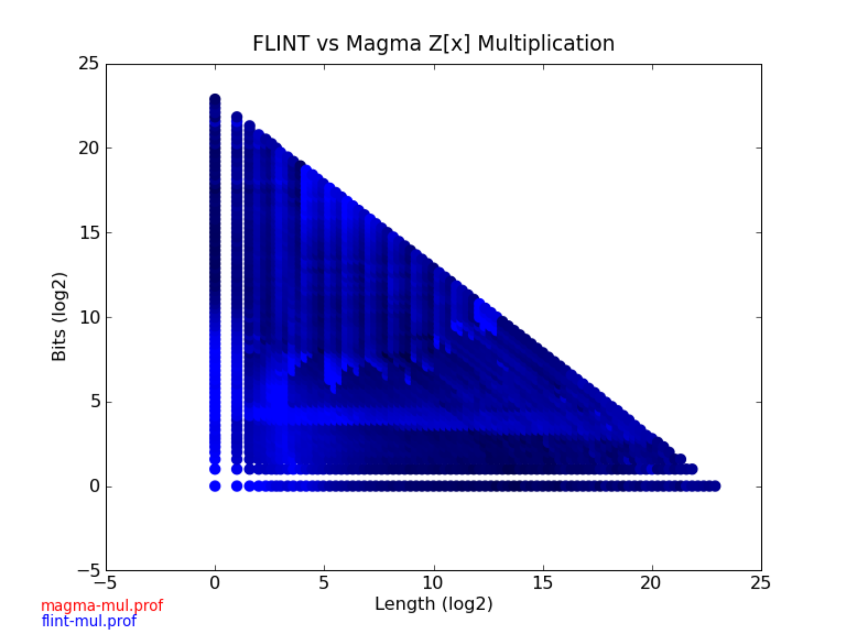
- Over 100,000 lines of C code
- Word sized integer and modular arithmetic
- Multiprecision integer and rational arithmetic
- Multiprecision integer factoring (MPQS)
- *p*-adic arithmetic
- Dense univariate polynomial arithmetic over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, *p*-adics
- Power series over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$
- Univariate polynomial factoring over $\mathbb{Z}$
- Matrices over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}[x]$, *p*-adics

What does FLINT do?

- Over 100,000 lines of C code
- Word sized integer and modular arithmetic
- Multiprecision integer and rational arithmetic
- Multiprecision integer factoring (MPQS)
- *p*-adic arithmetic
- Dense univariate polynomial arithmetic over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, *p*-adics
- Power series over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$
- Univariate polynomial factoring over $\mathbb{Z}$
- Matrices over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}[x]$, *p*-adics
- Subquadratic LLL, Hensel lifting, CRT

What does FLINT do?

- Over 100,000 lines of C code
- Word sized integer and modular arithmetic
- Multiprecision integer and rational arithmetic
- Multiprecision integer factoring (MPQS)
- *p*-adic arithmetic
- Dense univariate polynomial arithmetic over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, *p*-adics
- Power series over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$
- Univariate polynomial factoring over $\mathbb{Z}$
- Matrices over $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}[x]$, *p*-adics
- Subquadratic LLL, Hensel lifting, CRT
- Arithmetic functions


FLINT vs Magma Z[x] Multiplication
Bits (log2)
Length (log2)
25
20
15
10
5
0
−5
−5
0
5
10
15
20
25
magma-mul.prof
flint-mul.prof

Advantages of flint 2

- Cleanly coded (coding conventions)

Advantages of flint 2

- Cleanly coded (coding conventions)
- ANSI C, relies on GMP/MPIR and MPFR only

Advantages of flint 2

- Cleanly coded (coding conventions)
- ANSI C, relies on GMP/MPIR and MPFR only
- Magic build system

Advantages of flint 2

- Cleanly coded (coding conventions)
- ANSI C, relies on GMP/MPIR and MPFR only
- Magic build system
- Automatic manage memory for polynomial coefficients

Advantages of flint 2

- Cleanly coded (coding conventions)
- ANSI C, relies on GMP/MPIR and MPFR only
- Magic build system
- Automatic manage memory for polynomial coefficients
- Many things much, much faster

Advantages of flint 2

- Cleanly coded (coding conventions)
- ANSI C, relies on GMP/MPIR and MPFR only
- Magic build system
- Automatic manage memory for polynomial coefficients
- Many things much, much faster
- Integers mod *n* up to full 32/64 bits

Advantages of flint 2

- Cleanly coded (coding conventions)
- ANSI C, relies on GMP/MPIR and MPFR only
- Magic build system
- Automatic manage memory for polynomial coefficients
- Many things much, much faster
- Integers mod *n* up to full 32/64 bits
- More features

New in flint 2.3

- Many speedups (poly interpolation, composition, series reversion, matrix determinant, matrix solving, matrix inverse, rref, matrix multiplication over $\mathbb{Z}/n\mathbb{Z}$

New in flint 2.3

- Many speedups (poly interpolation, composition, series reversion, matrix determinant, matrix solving, matrix inverse, rref, matrix multiplication over $\mathbb{Z}/n\mathbb{Z}$
- Insanely fast partitions code, Dedekind sums, cyclotomic polynomials

New in flint 2.3

- Many speedups (poly interpolation, composition, series reversion, matrix determinant, matrix solving, matrix inverse, rref, matrix multiplication over $\mathbb{Z}/n\mathbb{Z}$
- Insanely fast partitions code, Dedekind sums, cyclotomic polynomials
- Euler's constant, zeta constants

New in flint 2.3

- Many speedups (poly interpolation, composition, series reversion, matrix determinant, matrix solving, matrix inverse, rref, matrix multiplication over $\mathbb{Z}/n\mathbb{Z}$
- Insanely fast partitions code, Dedekind sums, cyclotomic polynomials
- Euler's constant, zeta constants
- Rewritten quadratic sieve for integers up to 128 bits

New in flint 2.3

- Many speedups (poly interpolation, composition, series reversion, matrix determinant, matrix solving, matrix inverse, rref, matrix multiplication over $\mathbb{Z}/n\mathbb{Z}$
- Insanely fast partitions code, Dedekind sums, cyclotomic polynomials
- Euler's constant, zeta constants
- Rewritten quadratic sieve for integers up to 128 bits
- (Hopefully) half gcd, Schoenhage-Strassen poly multiplication

New in flint 2.3

- Many speedups (poly interpolation, composition, series reversion, matrix determinant, matrix solving, matrix inverse, rref, matrix multiplication over $\mathbb{Z}/n\mathbb{Z}$
- Insanely fast partitions code, Dedekind sums, cyclotomic polynomials
- Euler's constant, zeta constants
- Rewritten quadratic sieve for integers up to 128 bits
- (Hopefully) half gcd, Schoenhage-Strassen poly multiplication
- Polynomials over $\mathbb{Z}/n\mathbb{Z}$ for multiprecision n

This week

- Upgrade Sage to latest flint

This week

- Upgrade Sage to latest flint
- Switch Sage to use fmpz_poly, nmod_poly and fmpq_poly modules in flint 2.3

This week

- Upgrade Sage to latest flint
- Switch Sage to use fmpz_poly, nmod_poly and fmpq_poly modules in flint 2.3
- final testing, valgrinding, documentation of flint 2.3

This week

- Upgrade Sage to latest flint
- Switch Sage to use fmpz_poly, nmod_poly and fmpq_poly modules in flint 2.3
- final testing, valgrinding, documentation of flint 2.3
- make flint 2.3 support GMP 5 as well as MPIR 2.5

FLINT 2 future

- Implement Hensel lifting, subquadratic LLL and van Hoeij/Novocin factoring of polynomials over $\mathbb{Z}$

FLINT 2 future

- Implement Hensel lifting, subquadratic LLL and van Hoeij/Novocin factoring of polynomials over $\mathbb{Z}$
- Port quadratic sieve for large integers

FLINT 2 future

- Implement Hensel lifting, subquadratic LLL and van Hoeij/Novocin factoring of polynomials over $\mathbb{Z}$
- Port quadratic sieve for large integers
- Finish the new FFT for MPIR and use it in flint

FLINT 2 future

- Implement Hensel lifting, subquadratic LLL and van Hoeij/Novocin factoring of polynomials over $\mathbb{Z}$
- Port quadratic sieve for large integers
- Finish the new FFT for MPIR and use it in flint
- Multivariate polynomials

FLINT 2 future

- Implement Hensel lifting, subquadratic LLL and van Hoeij/Novocin factoring of polynomials over $\mathbb{Z}$
- Port quadratic sieve for large integers
- Finish the new FFT for MPIR and use it in flint
- Multivariate polynomials
- Optional BLAS for matrices over $\mathbb{Z}/p\mathbb{Z}$

Website

- Website: http://www.flintlib.org/

Website

- Website: http://www.flintlib.org/
- Contributors: Fredrik Johansson, Sebastian Pancratz, David Harvey, Andy Novocin, Jan Tuitman, Daniel Woodhouse, Peter Shrimpton, Richard Howell-Peak, Jason Papadopoulos, Burcin Erocal, Gonzalo Tornaria, Tom Boothby, David Howden, Daniel Scott, Tomasz Lechowski, Daniel Ellam, Didier Deshommes, Michael Abshoff, William Stein, Robert Bradshaw, Carl Witty, Craig Citro, Martin Lee, Timothy Abbot, Jaap Spies, Kiran Kedlaya, Kate Minola, Serge Torres, Ralf Hemmecke, (Martin Albrecht, Hanhong Xue, Paul Zimmermann, Damien Stehlé)