Catrel Workshop, École Polytechnique — October 1-2, 2015

New record in $\mathbb{F}_{p^3}$

R. Barbulescu P. Gaudry A. Guillevic F. Morain

cnrs dépasser les frontières

IMJ-PRG
Institut de Mathématiques
de
Jussieu-Paris Rive Gauche

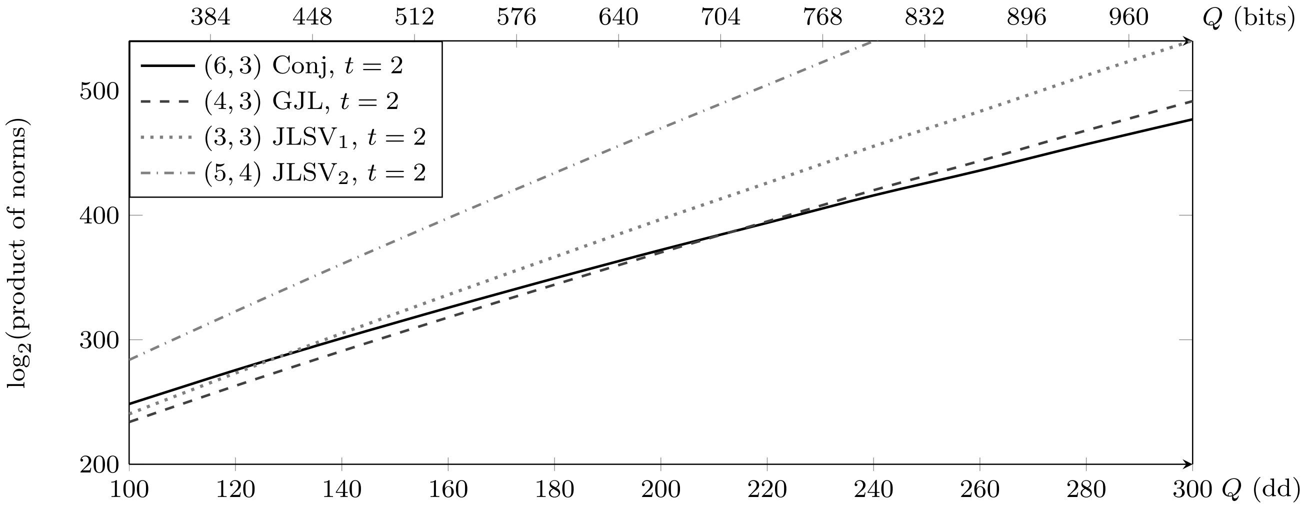
Context

Notation

p17dd42: DLP in $\mathbb{F}_{p^{17}}$ when p has 42 decimal digits.

- In 2000 Joux proposed a one round key exchange protocol based on pairings, which requires that DLP in $\mathbb{F}_{p^n}$ is strong when $n > 1$.
- In 2006 Joux Lercier Smart Vercauteren made a record for p3dd40.
- In August 2014 B. Gaudry Guillevic Morain made a record in p2dd90.
- One week ago, B. Gaudry Guillevic Morain finished computations in p4dd30.
- New: B. Gaudry Guillevic Morain finished computations in p3dd52.

Which method?



Experiments

- Galois is important $\Rightarrow$ Conjugation or JLSV$_1$;
- p3dd10, p3dd20, p3dd30, p3dd40 showed that conjugation has a smaller slope.

Record details (1/3)

CADO

We modified the code of sieve, but rely heavily on CADO.

Goal

Field: GF(p^3) with $p = 2350818717208688087749020262268575297768527372596629$
(512 bits as a whole, $p = \lfloor 2^{169}\pi \rfloor + 94530$.)
Goal: DL in subgroup of order $\ell = \frac{p^2+p+1}{3}$.

Polynomials

$$\begin{aligned} f &= 274508703714183749205794 06x^3 + 949567610881092134556 0989x^2 \\ &\quad -7285693500544420341617 7229x - 274508703714183749205794 06 \\ g &= x^6 - 3x^4 + 4x^3 + 12x^2 + 6x + 1. \end{aligned}$$

- Conjugation method in Magma (negligible time);
- Both have automorphism $x \mapsto -1 - 1/x$ of order three.

Record details (2/3)

Sieving

- special-q on both sides (balanced norms).
- took advantage of Galois action (saved factor of 3).
- factor base bound: 50M.
- large prime bound: 27 bits (allow 2 on each side).
- $I = 15$.
- Total CPU-time: 850 core-days.

Filtering

- 26 M raw rels
- 15.7M single rels (40% duplicates)
- Final matrix: 3.72 M rows/cols, 150 coef/row.

Schirokauer maps

- due to improvement in Emmanuel Thomé's talk, their cost is zero;
- two on each side (in other cases $5 + 2$).

Record details (3/3)

Linear algebra

- Block-Wiedemann algorithm. Used 8 sequences in parallel, 4 of them having SM vector as input. Typical setting: 8 blocks of 4 nodes of 16 cores, each contributing to one sequence.
- time
  - Krylov sequence: 700,000 iterations per sequence, at 0.8 s / it.
  - Berlekamp-Massey step: 7 hours on 64 cores.
  - Mksol: 460,000 iterations per sequence, at 0.8 s / it.
  - Total linalg cpu-time: 5,500 core-days

Individual logarithm

- smoothing (boot) using the improvement of Aurore's talk.
- descent (parameters needed)

$$\log(t+2) = 2209677825943257194568673102207758670512936096971885535410620201382259296269317656690962472796603956 04$$

in an unknown base (second descent needed).