Complexity news: discrete logarithms in multiplicative groups of small-characteristic finite fields— the algorithm of Barbulescu, Gaudry, Joux, Thomé

D. J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Also somewhat related:

I'm starting to analyze
cost of NFS + CVP
for class groups, unit groups,
short generators of ideals, etc.;
exploiting subfields
(find short *norms* first),
small Galois groups, etc.
Anyone else working on this?

Cryptanalytic applications:
attack NTRU, Ring-LWE, FHE.
I think NTRU should switch to
random prime-degree extensions
with big Galois groups.

Discrete logarithms

Goal: Compute some
group isomorphism
$\mathbf{F}_q^* \to \mathbf{Z}/(q-1)$,
represented in the usual way.

Algorithm input:
$h_1, h_2, \ldots \in \mathbf{F}_q^*$.

Algorithm output:
$\log_g h_1, \log_g h_2, \ldots \in \mathbf{Z}/(q-1)$
for some g.

"$\log_g$" means the isomorphism
$g \mapsto 1$, if it exists.

“Generic” $\log_g$ algorithms:
on average $q^{1/2+o(1)}$ operations
uniform, $q^{1/3+o(1)}$ non-uniform.
Want something faster.

“Generic” $\log_g$ algorithms:
on average $q^{1/2+o(1)}$ operations
uniform, $q^{1/3+o(1)}$ non-uniform.
Want something faster.

“Basic index calculus”: 1968
Western–Miller, 1979 Merkle,
1979 Adleman, 1983 Hellman–
Reyneri, 1984 Blake–Fuji-Hara–
Mullin–Vanstone, 1985 ElGamal,
1986 Coppersmith–Odlyzko–
Schroeppel, 1991 LaMacchia–
Odlyzko, 1993 Adleman–
DeMarrais, 1995 Semaev,
1998 Bender–Pomerance.

“NFS”: 1991 Schirokauer, 1993 Gordon, 1993 Schirokauer, 1994 Odlyzko, 1996 Schirokauer–Weber–Denny, 1996 Weber, 1998 Weber–Denny, 2001 Joux–Lercier, 2006 Joux–Lercier–Smart–Vercauteren.

“FFS”: 1984 Coppersmith, 1985 Coppersmith–Davenport, 1985 Odlyzko, 1990 McCurley, 1992 Gordon–McCurley, 1994 Adleman, 1999 Adleman–Huang, 2001 Joux–Lercier, 2006 Joux–Lercier, 2010/2012 Hayashi–Shinohara–Wang–Matsuo–Shirase–Takagi.

"FFS", continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

“FFS”, continued: 2012 Hayashi–Shimoyama–Shinohara–Takagi, 2012.10 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann, 2013.04 Barbulescu–Bouvier–Detrey–Gaudry–Jeljeli–Thomé–Videau–Zimmermann.

“Not your grandpa’s FFS”: 2012.12 Joux, 2013.02 Joux, 2013.02 Göloğlu–Granger–McGuire–Zumbrägel, 2013.05 Göloğlu–Granger–McGuire–Zumbrägel, 2013.06 Barbulescu–Gaudry–Joux–Thomé.

Reasonable conjectures
for fixed characteristic:

FFS costs $\le T$ where
$\log T \in (\log q)^{1/3+o(1)}$.

Reasonable conjectures for fixed characteristic:

FFS costs $\leq T$ where $\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm: $\log T \in (\log q)^{1/4+o(1)}$.

Reasonable conjectures for fixed characteristic:

FFS costs $\leq T$ where $\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm: $\log T \in (\log q)^{1/4+o(1)}$.

2013.06 Barbulescu–Gaudry–Joux–Thomé algorithm: $\log T \in (\log \log q)^{2+o(1)}$.

Reasonable conjectures
for fixed characteristic:

FFS costs $\leq T$ where
$\log T \in (\log q)^{1/3+o(1)}$.

2013.02 Joux algorithm:
$\log T \in (\log q)^{1/4+o(1)}$.

2013.06 Barbulescu–Gaudry–
Joux–Thomé algorithm:
$\log T \in (\log \log q)^{2+o(1)}$.

1994 Shor algorithm:
$\log T \in (\log \log q)^{1+o(1)}$, proven;
but needs a quantum computer.

Field construction

I'll make simplifying assumption:
$q = p^{2n}$ where
p is an odd prime power,
$n \in \mathbf{Z}$, $\sqrt{p} \le n \le p$.

Most interesting: $n \approx p$.
Example: $p = 1009$, $n = 997$.
(Can you find all primes dividing
$p^{2n} - 1 = (p^n - 1)(p^n + 1)$?)

Find "random" poly in $\mathbf{F}_{p^2}[x]$
with an irreducible divisor
φ of degree n.

Construct $\mathbf{F}_q$ as $\mathbf{F}_{p^2}[x]/\varphi$.

How many polys to try?
What's chance that $r \in \mathbf{F}_{p^2}[x]$
has an irreducible divisor
φ of degree n?

For $n \le \deg r < 2n$:
express each successful r
uniquely as $\varphi \cdot$ cofactor.
$\approx (p^2)^{\deg r+1}$ polys r,
$\approx (p^2)^n/n$ monic irreds φ,
$\approx (p^2)^{\deg r-n+1}$ cofactors $\Rightarrow$
chance $\approx 1/n$ that r works.

Similar story for $\deg r \ge 2n$.

Factoring r is fast.
$\Rightarrow$ Quickly find r, φ.

Don't use random polys!
(Starting now: abandon proofs.)

Find φ dividing
$x^p - x^2 - \beta$ for some $\beta \in \mathbf{F}_{p^2}$.
Then $x^p = x^2 + \beta$ in $\mathbf{F}_q$.

p^2 choices of $\beta \in \mathbf{F}_{p^2}$,
so overwhelmingly likely
that at least one works.
e.g. $p = 1009$, $n = 997$:
can have $\beta^2 + 92\beta + 447 = 0$.

Easily generalize: e.g., take
$x^p = x^2 + \beta x + \gamma$ or
$x^p = (x + \beta)/(x + \gamma)$.
But larger degrees are slower.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \le D$. Choose
$D \ge 1$; $D \in O(\log n / \log\log n)$.

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \le D$. Choose
$D \ge 1$; $D \in O(\log n / \log\log n)$.

Non-uniform approach:
algorithm A_q knows table!

Low-degree discrete logs

First step of algorithm:
build table of $h \mapsto \log_g h$ for
each small $h \in \mathbf{F}_{p^2}[x] - \varphi\mathbf{F}_{p^2}[x]$.
Easily choose g at same time.

"Small h": $\deg h \le D$. Choose
$D \ge 1$; $D \in O(\log n / \log\log n)$.

Non-uniform approach:
algorithm A_q knows table!

Two reasons to be more explicit:
1. Want A with q as an input.
2. Method to build table
will be reused for larger h.

The first relation for $D = 1$

$\prod_{\alpha \in \mathbf{F}_p} (x - \alpha) \equiv x^2 - x + \beta$.

"$\equiv$" for $\mathbf{F}_{p^2}[x]$: equal mod $x^p - x^2 - \beta$; forces $=$ in $\mathbf{F}_q$.

Hope that $x^2 - x + \beta$ splits in $\mathbf{F}_{p^2}[x]$, say as $f_1 \cdot f_2$. Not an unreasonable hope: $\approx$50% of quadratics split.

Then $\log_g f_1 + \log_g f_2 = \sum_{\alpha \in \mathbf{F}_p} \log_g (x - \alpha)$.

This is a "relation" among discrete logs of monic linear polys.

More relations for $D = 1$

For $a, b, c, d \in \mathbf{F}_{p^2}$:

$$(cx + d) \prod_{\alpha \in \mathbf{F}_p} (ax + b - \alpha(cx + d))$$

$$= (cx + d)(ax + b)^p$$
$$- (ax + b)(cx + d)^p$$

$$= (cx + d)(a^p x^p + b^p)$$
$$- (ax + b)(c^p x^p + d^p)$$

$$\equiv (cx + d)(a^p(x^2 + \beta) + b^p)$$
$$- (ax + b)(c^p(x^2 + \beta) + d^p).$$

Left side is product of linear polys in $\mathbf{F}_{p^2}[x]$.
Often right side is too.

$\lambda \in \mathbf{F}_{p^2}^*$, $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow$ $M, \lambda M$ are redundant.

$m \in \mathrm{GL}_2(\mathbf{F}_p)$, $M \in \mathrm{GL}_2(\mathbf{F}_{p^2})$
$\Rightarrow$ M, mM are redundant.

No other obvious redundancies.

Is there a nice way to represent the set of cosets of $\mathrm{PGL}_2(\mathbf{F}_p)$ in $\mathrm{PGL}_2(\mathbf{F}_{p^2})$? Best hints so far: Cremona points me to $\mathbf{F}_{p^4}^*/\mathbf{F}_{p^2}^*$; Bartel gives solution for GL_2.

Mindless enumeration of cosets is not a real bottleneck here but want fast multipoint eval.

$p^3 + p$ potential relations,
conjecturally $\approx$independent.
Each succeeds with chance $\approx$1/6.

Only p^2 monic linear polys.
Expect enough relations
to determine their logs
(or *most* logs: ok to miss a few),
unless p is very small.

BGJT say sparse linear algebra;
but fast matrix multiplication
gives better const in exponent.

(How to avoid annihilating $\mathbf{F}_{p^2}^*$?
Maybe cleanest: $x^p = \beta x^2 + 1$,
where β generates $\mathbf{F}_{p^2}^*$.)

More relations for arbitrary D

For each small $h \in \mathbf{F}_{p^2}[x]$:

$$(ch+d)\prod_{\alpha\in\mathbf{F}_p}(ah+b-\alpha(ch+d))$$

$$= (ch+d)(ah+b)^p$$
$$- (ah+b)(ch+d)^p$$

$$= (ch+d)(a^p h^p + b^p)$$
$$- (ah+b)(c^p h^p + d^p)$$

$$\equiv (ch+d)(a^p h(x^2+\beta) + b^p)$$
$$- (ah+b)(c^p h(x^2+\beta) + d^p).$$

Left side is product of small polys; sometimes right side is too.
$\approx$5% as $D \to \infty$. BGJT say 1/6.

Larger discrete logs

What if $D < \deg h \le 2D$?

Use same equation:

$$(ch+d)\prod_{\alpha\in\mathbf{F}_p}(ah+b-\alpha(ch+d))$$
$$\equiv (ch+d)(a^p h(x^2+\beta)+b^p)$$
$$-\,(ah+b)(c^p h(x^2+\beta)+d^p).$$

Occasionally right side is product of small polys.
We now know those discrete logs.

Left side is product on new factor base: $\{h+\gamma : \gamma\in\mathbf{F}_{p^2}\}$.
Solve for each $\log_g(h+\gamma)$.

For $\deg h \le (u/3)D$:
D-smoothness chance $\approx u^{-u}$
so $\approx u^{-u} p^3$ relations.

Need $\approx p^2$ relations.
Note free relations: smooth $h + \gamma$.

Works for $u \approx \log p / \log \log p$.

Reminiscent of linear sieve
(1977 Schroeppel):
$(\lceil \sqrt{q} \rceil + a)(\lceil \sqrt{q} \rceil + b)$
$\equiv (a+b) \lceil \sqrt{q} \rceil + ab + \lceil \sqrt{q} \rceil^2 - q$
mod large prime q.
Factor base in linear sieve:
$\{\lceil \sqrt{q} \rceil + a\} \cup \{\text{small primes}\}$.

Arbitrary discrete logs

For $(u/3)D < \deg h \le (u/3)^2 D$:

Use same equation

$$(ch+d) \prod_{\alpha \in \mathbf{F}_p} (ah+b-\alpha(ch+d))$$
$$\equiv (ch+d)(a^p h(x^2+\beta)+b^p)$$
$$-(ah+b)(c^p h(x^2+\beta)+d^p).$$

Occasionally $(u/3)D$-smooth right side; again $\{h+\gamma\}$ for left side. Have seen subroutine to compute $(u/3)D$-smooth discrete logs.

$p^{O(1)}$ subroutine calls, of which $\Theta(p^2)$ are important.

For larger h: recurse.

Reach degree $n-1$ using
$$\frac{\log n}{\log(u/3)} \in \Theta\Bigl(\frac{\log n}{\log\log n}\Bigr)$$
levels of recursion.

Total cost $p^{\Theta(\log n/\log\log n)}$
$$= \exp\Theta\Bigl(\frac{(\log n)^2}{\log\log n}\Bigr)$$
$$= \exp\Theta\Bigl(\frac{(\log\log q)^2}{\log\log\log q}\Bigr).$$

What about p^{2n} with $p < n$?
Embed into an extension field.
Can also use x^{char} etc.