Discrete logarithms in all finite finite fields

Antoine Joux
DGA and UVSQ

IPAM (October 9th, 2006)

Joint work with
Reynald Lercier, Nigel Smart, Frederik Vercauteren

Index calculus algorithms

- A general algorithmic approach to solve:
  - Factoring problems
  - Discrete logarithms in finite fields
- Two main subcases:
  - Number field sieve (factoring and DL in medium to large char.)
  - Function field sieve (DL in small to medium char.)

Previously known complexity results

- Complexity usually expressed as:

$$L_Q(\alpha, c) = \exp((c + o(1))(\log Q)^\alpha (\log\log Q)^{1-\alpha}).$$

- Two extreme (well known) cases:
  - $\mathbb{F}_p$, with p a large prime. NFS yields a

$$L_p\left(\frac{1}{3}, \left(\frac{64}{9}\right)^{1/3}\right) \text{ complexity.}$$

  - $\mathbb{F}_{p^n}$, with fixed (small) p. FFS yields a

$$L_{p^n}\left(\frac{1}{3}, \left(\frac{32}{9}\right)^{1/3}\right) \text{ complexity.}$$

- In between, the best known result was $L(1/2)$. (Adleman-Demarrais)

New results for DLOG in $\mathbb{F}_Q$

- Assume $Q = p^n$
- Eurocrypt 2006: Revisit the FFS
  - For p up to $L_Q(1/3)$
  - Works without function fields
  - Basic simplest case: $p = L_Q(1/3)$
- Crypto 2006: Revisit the NFS
  - Works for p from $L_Q(1/3)$ up to Q
  - With an individual logarithm phase
  - Basic simplest case: $p = L_Q(2/3)$
- Put together: $L_Q(1/3)$ complexity for all finite fields

Overall strategy

- As in any index calculus approach, setup followed by:
  - Sieving
  - Linear algebra using SGE and Lanczos or Wiedemann
  - Individual logarithms

Basic case (Setup)

- Assume $p = L_Q(1/3, c)$
- Thus:

$$n = \frac{1}{c}\left(\frac{\log Q}{\log\log Q}\right)^{2/3}.$$

- Choose two univariate polynomials f_1 and f_2
  with degrees d_1 and d_2 and $d_1 d_2 \geq n$.
- Such that $\mathrm{Res}(y - f_1(x), x - f_2(y))$ has:
  an irreducible factor of degree n (modulo p).

Basic case (Setup/Sieving)

- Irreducible factor: $I_x(x)$ or $I_y(y)$
- Two definitions of the (same) finite field $\mathbb{F}_{p^n}$
- Both x and y have well defined images α and β in $\mathbb{F}_{p^n}$.

- Take elements of the form:

$$\alpha\beta + a\alpha + b\beta + c \quad \text{or} \quad a\alpha + \beta + b$$

- In this expression, replace β by $f_1(\alpha)$
- Or replace α by $f_2(\beta)$

Basic case (Sieving)

- Yields an equation:

$$h_1(\alpha) = h_2(\beta).$$

- Where h_1 (resp. h_2) has degree $d_1 + 1$ (resp. $d_2 + 1$)
- Good case:
  - h_1 and h_2 split into linear factors
- Multiplicative equality (up to a constant in $\mathbb{F}_p$)
  - Between terms $\alpha + \mathfrak{a}$ and $\beta + \mathfrak{b}$.

Example: $\mathbb{F}_{65537^{25}}$

- Take $f_1(x) = x^5 + x + 3$ and $f_2(y) = -y^5 - y - 1$
- Then:

$$
\begin{aligned}
I_x(x) &= x^{25} + 5x^{21} + 15x^{20} + 10x^{17} + 60x^{16} + 90x^{15} + 10x^{13} + \\
&\quad 90x^{12} + 270x^{11} + 270x^{10} + 5x^{9} + 60x^{8} + 270x^{7} + \\
&\quad 540x^{6} + 407x^{5} + 15x^{4} + 90x^{3} + 270x^{2} + 407x + 247 \\
I_y(y) &= y^{25} + 5y^{21} + 5y^{20} + 10y^{17} + 20y^{16} + 10y^{15} + \\
&\quad 10y^{13} + 30y^{12} + 30y^{11} + 10y^{10} + 5y^{9} + 20y^{8} + \\
&\quad 30y^{7} + 20y^{6} + 7y^{5} + 5y^{4} + 10y^{3} + 10y^{2} + 7y - 1
\end{aligned}
$$

Example: $\mathbb{F}_{65537^{25}}$

- Take the element $\beta + 2\alpha - 20496$
- It can be written as:

$$\alpha^5 + 3\alpha - 20493 =$$
$$(\alpha + 2445) \cdot (\alpha + 9593) \cdot (\alpha + 31166) \cdot (\alpha + 39260) \cdot (\alpha + 48610)$$

- Or as:

$$-2\beta^5 - \beta - 20498 =$$
$$-2(\beta + 1946) \cdot (\beta + 17129) \cdot (\beta + 18727) \cdot (\beta + 43449) \cdot (\beta + 49823)$$

- Linear equation between terms $\log(\alpha + \mathfrak{a})$ and $\log(\beta + \mathfrak{b})$ modulo $(p^n - 1)/(p - 1)$

Example: $\mathbb{F}_{65537^{25}}$ (Linear algebra)

- Cardinality of $\mathbb{F}^*_{65537^{25}}$:

  $65536 \cdot 3571 \cdot 37693451 \cdot 137055701 \cdot 108537058945639689370 51 \cdot P_{247}$

- We compute the linear algebra modulo $q_0 = (p^n - 1)/(65536 \cdot 3571)$, finding:

  95805410880093234842298898214533393829434304594545362348
  24840375483524017353229706334323184929723853320944439485
  and
  46495712756925209185601240503381083970050573012881700517
  18556686238431642289730613529631676496393555258546887691

  the logarithms of $\alpha + 1$ and β in base α.

Complexity analysis

- Linear system in $2p$ unknowns
- For each candidate, the (heuristic) probability of success is:

$$\frac{1}{(d_1+1)!} \cdot \frac{1}{(d_2+1)!}$$

- Expected number of candidates (sieving time):

$$2p(d_1+1)! \cdot (d_2+1)!$$

- Time for solving the sparse linear system:

$$O((d_1+d_2)p^2)$$

Complexity analysis

- With $d_1 \approx d_2 \approx \sqrt{n}$
- The complexities written as $L_Q(1/3)$ become:
  - Linear algebra:

$$O((d_1 + d_2)p^2) = L_Q(1/3, 2c)$$

  - Sieving:

$$2p(d_1 + 1)! \cdot (d_2 + 1)! = L_Q\left(\frac{1}{3}, c + \frac{2}{3\sqrt{c}}\right)$$

- Important constraint, size of sieving space:

$$p^3 = L_Q(1/3, 3c)$$

Complexity analysis

- The algorithm is valid when:

$$3c \geq c + \frac{2}{3\sqrt{c}} \quad \text{or} \quad c \geq (1/3)^{2/3}$$

- Complexity: $L_Q(1/3, c + \max(c, \frac{2}{3\sqrt{c}}))$
- Minimum at $c = (1/3)^{2/3}$, complexity $L_Q(1/3, 3^{1/3})$

Individual logarithm: example in $\mathbb{F}_{65537^{25}}$

- Logarithm to find:

$$\lambda = \sum_{i=0}^{24} (\lfloor \pi \cdot 65537^{i+1} \rfloor \bmod 65537)\alpha^i = 41667\alpha^{24} + \cdots + 9279.$$

- First step, write $\lambda = 9828 \cdot N/D$ with:

$$\begin{aligned} N &= (\alpha + 20471) \cdot (\alpha + 25396) \cdot (\alpha + 34766) \cdot \\ &\quad (\alpha + 54898) \cdot (\alpha^2 + 29819\alpha + 6546) \cdot (\alpha^2 + 44017\alpha + 38392) \cdot \\ &\quad (\alpha^2 + 54060\alpha + 4880) \cdot (\alpha^3 + 23811\alpha^2 + 6384\alpha + 3243) \\ D &= (\alpha + 18919) \cdot (\alpha + 31146) \cdot (\alpha + 38885) \cdot \\ &\quad (\alpha + 53302) \cdot (\alpha^2 + 52365\alpha + 2605) \cdot \\ &\quad (\alpha^3 + 29795\alpha^2 + 54653\alpha + 7616) \cdot \\ &\quad (\alpha^3 + 57354\alpha^2 + 37421\alpha + 53988) \end{aligned}$$

- Second step, compute each log. by descent

Starting the descent

- Take element:

$$(1493\,\alpha + 1)\beta - (40653\,\alpha^2 + 26561\,\alpha + 44820)$$

- Equal to:

$$1493\,\alpha^6 + \alpha^5 - 39160\,\alpha^2 - 22081\,\alpha - 44817 =$$
$$1493 \cdot (\alpha + 1964) \cdot (\alpha^2 + 2977\alpha + 33882) \cdot (\alpha^3 + 23811\alpha^2 + 6384\alpha + 3243)$$

- And also to:

$$24884\,\beta^{10} + 48275\,\beta^6 + 10792\,\beta^5 + 23391\,\beta^2 + 9300\,\beta + 6625 =$$
$$24884 \cdot (\beta + 14197) \cdot (\beta + 14995) \cdot (\beta + 25133) \cdot (\beta + 56789) \cdot$$
$$(\beta^2 + 14732\beta + 57516) \cdot (\beta^2 + 20454\beta + 37544) \cdot (\beta^2 + 50311\beta + 36703)$$

The descent . . . continued

- Take element:

$$21022\,\alpha\beta + \alpha + 17943\,\beta + 65126$$

- Equal to:

$$\begin{aligned}&21022\,\alpha^6 + 17943\,\alpha^5 + 21022\,\alpha^2 + 15473\,\alpha + 53418 = \\ &21022 \cdot (\alpha + 19091) \cdot (\alpha + 36728) \cdot (\alpha + 38567) \cdot (\alpha + 38593) \\ &\qquad \cdot (\alpha + 56621) \cdot (\alpha + 64596)\end{aligned}$$

- And also to:

$$\begin{aligned}&44515\,\beta^6 - \beta^5 + 44515\,\beta^2 + 62457\,\beta + 65125 = \\ &44515 \cdot (\beta + 148) \cdot (\beta + 1344) \cdot (\beta + 15752) \cdot (\beta + 47579) \\ &\qquad \cdot (\beta^2 + 50311\beta + 36703)\end{aligned}$$

Individual logarithm: example in $\mathbb{F}_{65537^{25}}$

- Finally:

  4053736945052440744587988507271545773377910517074639935754736
  3481852609028577772820085371649268383536448936947412841469 99

  is the logarithm of λ in basis 3α.

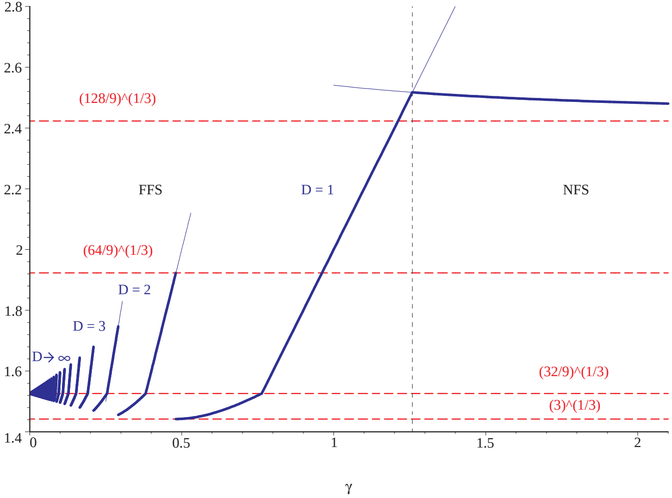
General case (smaller values of p)

- Family of algorithms, parametrized by D
- Sieve over elements of the form:

$$f(\alpha)\beta + g(\alpha),$$

where f and g are polynomials of degree D (f unitary).
- Similar analysis, optimal choice $d_1 \approx Dd_2$

Complexity of the general case when $p = L_Q(1/3)$



Complexity for $p = o(L_Q(1/3))$

- Here D is no longer a constant
- Instead take:

$$D = (2/3)^{2/3} \frac{\log(Q)^{1/3} \log\log^{2/3}(Q)}{\log(p)}$$

- With this choice:
  - Sieve space: $p^{(2D)} = L_Q(1/3, (32/9)^{1/3})$
  - Smoothness base size: $p^D = L_Q(1/3, (4/9)^{1/3})$
  - Smoothness probability:
    $exp(-2\sqrt{(}n/D)\log(2\sqrt{(}n/D)))) = L_Q(1/3, -(4/9)^{1/3})$
- Everything lines up correctly on total complexity:

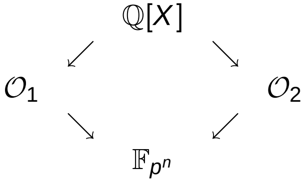
$$L_Q(1/3, (32/9)^{1/3})$$

Possible Extensions of FFS

- Use of Galois group to speed-up computations
- Very useful for $\mathbb{F}_{2^{nm}}$
- Also practical in other cases such as $\mathbb{F}_{370801^{30}}$
- Often need the description with function fields

Basic variation $p = L_{p^n}(2/3, c)$: setup

- Finite field $\mathbb{F}_{p^n}$ with $p = L_{p^n}(2/3, c)$ and c near $2 \cdot (1/3)^{1/3}$
- Choose polynomial f_1 of degree n
  - irreducible over $\mathbb{F}_p$
  - very small coefficients
- Choose second polynomial $\boxed{f_2 = f_1 + p}$
- $K_1 \simeq \mathbb{Q}[X]/(f_1(X)) \cong \mathbb{Q}[\theta_1]$ and $K_2 \cong \mathbb{Q}[X]/(f_2(X)) \cong \mathbb{Q}[\theta_2]$
- Note: $f_1 \equiv f_2 \bmod p$, so we have commutative diagram:



Basic variation $p = L_{p^n}(2/3, c)$: sieving/linear algebra

- Factor bases $\mathcal{F}_1$ and $\mathcal{F}_2$ of degree 1 ideals of small norm
- Choose smoothness bound B and a sieve limit S
- Pairs (a, b) of coprime integers, $|a| \leq S$ and $|b| \leq S$

$$\mathrm{No}(a - b\theta_1) \text{ and } \mathrm{No}(a - b\theta_2) \quad B\text{-smooth}$$

- Add logarithmic maps to take into account $h(K_i) \neq 1$ and unit groups
- Obtain linear equation between “logarithms of ideals” in the smoothness bases
- Solve linear system

Practical optimisation: Galois extensions

- p is inert in K_1, so isomorphism $\mathrm{Gal}(K_1/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{F}_Q/\mathbb{F}_p)$
- Thus: K_1 has to be a cyclic number field of degree n
- Partition factor base $\mathcal{F}_1$ in n parts $\mathcal{F}_{1,k}$ with $k = 1, \ldots, n$

$$(a - b\theta_1) = \prod_{k=1}^{n} \prod_{\mathfrak{p}_i \in \mathcal{F}_{1,1}} \psi^k(\mathfrak{p}_i)^{e_{i,k}}$$

  with $\mathrm{Gal}(K_1/\mathbb{Q}) = \langle \psi \rangle$
- Choose ψ such $\log_g \phi_1(\psi(\delta_i))) = p \log_g \phi_1(\delta_i)$ with $\mathfrak{p}_i = \langle \delta_i \rangle$
- Effectively divides factor base size by n

Basic variation $p = L_{p^n}(2/3, c)$: individual DLOG

- Adapted variation of special $\mathfrak{q}$-descent procedure
- Represent $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[t]/(f_1(t))$
- Assume we want to compute $\log_t y$ with $y \in \mathbb{F}_{p^n}$
- Search for element $z = y^i t^j$ for some $i, j \in \mathbb{N}$ with
  1. lifting $z \in K_1$, norm factors into primes smaller than some bound $B_1 \in L_{p^n}(2/3, 1/3^{1/3})$,
  2. only degree one prime ideals in the factorisation of (z)
  3. E.g.: the norm of the lift of z should be squarefree
- Remark: probability of *squarefree smoothness* is about $6/\pi^2$ probability of smoothness

Basic variation $p = L_{p^n}(2/3, c)$: individual DLOG

- Factor principal ideal generated by z as

$$(z) = \prod_{p_i \in \mathcal{F}_1} \mathfrak{p}_i^{e_i} \prod_j \mathfrak{q}_j^{e_j}$$

- Ideals $\mathfrak{q}_j$ not contained in $\mathcal{F}_1$, so need to compute DLOGs
- For each $\mathfrak{q}_j$, perform special-$\mathfrak{q}_j$ descent:
  1. Sieve over pairs (a, b) such that $\mathfrak{q}_j | (a - b\theta_1)$ and

     $$\mathrm{No}(a - b\theta_1)/\mathrm{No}(\mathfrak{q}_j) \text{ and } \mathrm{No}(a - b\theta_2) \quad B_2\text{-smooth } B_2 < B_1$$

  2. Factor $(a - b\theta_1)$ and $(a - b\theta_2)$ to obtain new special q_j's
  3. Repeat until bound $B_k < B \Rightarrow$ DLOGs of all $\mathfrak{q}_j$ known
- Remark: special $\mathfrak{q}_j$ in both number fields K_1 and K_2

Practical Optimisation for individual logarithms

- Instead of factoring $\langle z \rangle$, first write z as

$$\frac{\sum a_i t^i}{\sum b_i t^i}$$

with a_i and b_i are of the order of $\sqrt{p}$.

- Use LLL to find short vector in lattice L

$$L = \begin{pmatrix} \mathbf{z} & \mathbf{tz} & \mathbf{t^2 z} & \cdots & \mathbf{t^{n-1} z} & \mathbf{p} & \mathbf{pt} & \mathbf{pt^2} & \cdots & \mathbf{pt^{n-1}} \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

- Expect LLL finds short vector of norm $\sqrt{p}$

Example on 120 digits

- Adaptation of J. & Lercier's implementation for $\mathbb{F}_p$
- Finite field $\mathbb{F}_{p^3}$ with $p = \lfloor 10^{39}\pi \rfloor + 2622$

$$p = 3141592653589793238462643383279502886819$$

- Group order $p^3 - 1$ has 110-bit factor l
- Definition of number fields K_1 and K_2 by

$$f_1(X) = X^3 + X^2 - 2X - 1 \quad \text{and} \quad f_2(X) = f_1(X) + p\,,$$

Specifics of number fields K_1 and K_2

- $\mathbb{Q}[\theta_1]$ is a cubic cyclic number field with Galois group

$$\mathrm{Aut}(\mathbb{Q}[\theta_1]) = \{\theta_1 \mapsto \theta_1, \theta_1 \mapsto \theta_1^2 - 2, \theta_1 \mapsto -\theta_1^2 - \theta_1 + 1\}$$

- K_1 has class number 1 and System of fundamental units

$$u_1 = \theta_1 + 1 \text{ and } u_2 = \theta_1^2 + \theta_1 - 1$$

- $\mathbb{Q}[\theta_2]$ has signature $(1, 1)$, so only need single Schirokauer logarithmic map λ

Factor bases and sieving

- Smoothness bases with 1 000 000 prime ideals
  - in the $\mathbb{Q}[\theta_1]$ side, we include 899 999 prime ideals, but only 300 000 are meaningful due to the Galois action,
  - in the $\mathbb{Q}[\theta_2]$ side, we include 700 000 prime ideals.
- Lattice sieving: only algebraic integers $a + b\theta_2$ divisible by prime ideal in $\mathbb{Q}[\theta_2]$
- Norms to be smoothed in $\mathbb{Q}[\theta_2]$ are 150 bit integers
- Norms in $\mathbb{Q}[\theta_1]$ are 110 bit integers
- Sieving took 12 days on a 1.15 GHz 16-processors HP AlphaServer GS1280

Linear algebra

- Compute the kernel of a $1\,163\,482 \times 793\,188$ matrix
- Coefficients mostly equal modulo ℓ to ± 1, $\pm p$ or $\pm p^2$
- SGE: $450\,246 \times 445\,097$ matrix with $44\,544\,016$ non null entries
- Lanczos's algorithm: about one week
- $h(K_1) = 1$, check DLOGs of generators of ideals in $\mathcal{F}_1$

$$\begin{aligned}
(t^2 + t + 1)^{(p^3-1)/l} &= G^{29406688645015596112746712243217 1}, \\
(t - 3)^{(p^3-1)/l} &= G^{36422456363509538073334012349071 9}, \\
(3\,t - 1)^{(p^3-1)/l} &= G^{46887658774739638067572350292825 7},
\end{aligned}$$

where $G = g^{(p^3-1)/11592682025741777397154621558414 84\,l}$ and $g = -2t + 1$.

Individual DLOGs

- Challenge $\gamma = \sum_{i=0}^{2}(\lfloor \pi \times p^{i+1} \rfloor \bmod p)t^i$
- Using Pollard-Rho, computed DLOG modulo $(p^3 - 1)/l$,

  3889538915890151897584592293694118467753499109961221460457697271386147286910282477328.

- To obtain a complete result, we expressed

$$\gamma = \frac{-909879803559595529347t^2 - 1144430082485221569 10t + 1544936643733412719 98}{949127644415707714 06t^2 - 1200555698097118619 65t - 8195961996444635 2567},$$

- Numerator and denominator are both smooth in $\mathbb{Q}[\theta_1]$
- Three level tree with 80 special-$\mathfrak{q}$ ideals
- Recovered DLOG modulo l, namely 110781190155780903592153105706975
- Each special-$\mathfrak{q}$ sieving took 10 minutes for a total of 14 hours

Complexity analysis of the basic algorithm

- Input:

$$n = \frac{1}{c} \cdot \left(\frac{\log Q}{\log \log Q} \right)^{1/3}, \quad p = \exp \left(c \cdot \log^{2/3} Q \cdot \log^{1/3} \log Q \right).$$

- Parameters:

$$S = B = \exp \left(c' \cdot \log^{1/3} Q \cdot \log^{2/3} \log Q \right),$$

  for some constant c'.
- Number to smooth: $p \cdot B^{2n+o(1)} = L_Q(2/3, c + 2c'/c)$
- Prob. of smoothness: $L_Q(1/3, -(1/3) \cdot (c/c' + 2/c))$
- Complexity minimized at:

$$c' = (1/3) \cdot (c/c' + 2/c)$$

Complexity analysis continued

- Thus:

$$c' = \frac{1}{3}\left(\frac{1}{c} + \sqrt{3c + c^{-2}}\right).$$

  and heuristic complexity $L_q(1/3, 2c')$ depends on c
- Minimum when $c = c_0 = 2 \cdot (1/3)^{1/3}$, where $c' = 2 \cdot (1/3)^{2/3}$.
- At minimum, complexity:

$$L_Q(1/3, (64/9)^{1/3})$$

Variation for smaller p

- Polynomial setup same as in basic case
- Main problem: sieving space is not large enough, due to larger n
- $\Rightarrow$ cannot collect enough relations
- Solution: sieve over elements of larger degree than 1

$$\sum_{i=0}^{t} a_i \theta_1^i \quad \text{and} \quad \sum_{i=0}^{t} a_i \theta_2^i$$

- Bound on norm: $(n+t)^{n+t} {B_a}^n {B_f}^t$ with
  - B_a is an upper bound on the absolute values of the a_i
  - B_f a similar bound on the coefficients of f_1 (resp. f_2)

Variation for larger p

- Main problem: coefficients in f_2 too large
- Our requirement, f_1 and f_2 with smaller coefficients and GCD of deg. n over $\mathbb{F}_p$
- Idea: construct $f_1(x)$ of degree n and $f_2(x)$ of degree $> n$ with small coefficients such that:

$$f_1(x) \nmid f_2(x) \quad \text{over } \mathbb{Q}$$

- Choose constant W and construct $f_1(x) = f_0(x + W)$, largest coefficient at least W^n
- Use LLL to reduce the lattice

$$L = \begin{pmatrix} \mathbf{f_1(x)} & \mathbf{xf_1(x)} & \mathbf{x^2f_1(x)} & \cdots & \mathbf{x^{D-n}f_1(x)} & \mathbf{p} & \mathbf{px} & \mathbf{px^2} & \cdots & \mathbf{px^D} \end{pmatrix}$$

- Need vector with coefficients smaller than W^n so

$$2^{(D+1)/4} p^{n/(D+1)} \leq W^n$$

Complexity of variations for $p = L_Q(2/3, c)$

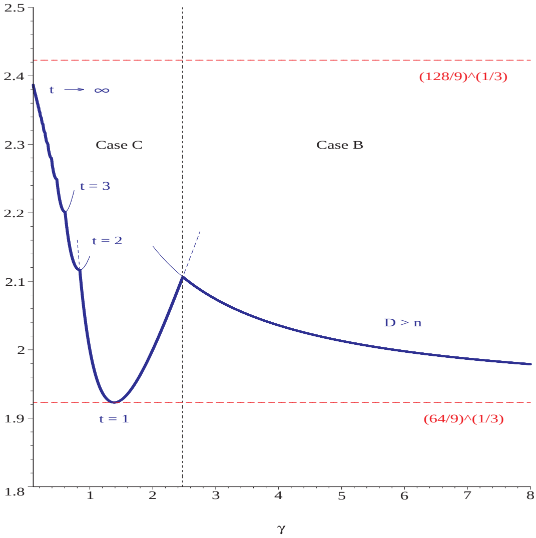
- p can be written as $L_q(2/3, c)$ for a constant $c < c_0$

$$L_q(1/3, 2c') \quad \text{with} \quad c' = \frac{4}{3}\left(\frac{3t}{4(t+1)}\right)^{1/3}$$

  sieve over elements of degree t with $3c^3 t(t+1)^2 - 32 = 0$
- p can be written as $L_q(2/3, c)$ for a constant $c > c_0$

$$L_q(1/3, 2c') \quad \text{with} \quad 9c'^3 - \frac{6}{c}c'^2 + \frac{1}{c^2}c' - 8 = 0$$

Complexity of variations for $p = L_Q(2/3, c)$



Complexity summary for all finite fields

- Three main zones:
  - For p up to $L_Q(1/3)$:

$$L_q(1/3, (32/9)^{1/3}) \simeq L_q(1/3, 1.526\ldots)$$

  - For p from $L_Q(1/3)$ to $L_Q(2/3)$:

$$L_q(1/3, (128/9)^{1/3}) \simeq L_q(1/3, 2.423\ldots)$$

  - For p above $L_Q(2/3)$:

$$L_q(1/3, (64/9)^{1/3}) \simeq L_q(1/3, 1.923\ldots)$$

- Two transitions:
  - For FFS/NFS when $p = L_Q(1/3)$
  - For NFS when $p = L_Q(2/3)$

Conclusion

- New, simple and **practical** variations of FFS and NFS
- FFS sieving short and easy to write
- Can simply adapt existing implementations of NFS for $\mathbb{F}_p$

Field	#digits	When	Who	GIPS years	Method
$\mathbb{F}_p$	130	Jun. 2005	J-L	1.2	NFS
$\mathbb{F}_{2^{613}}$	184	Sep. 2005	J-L	1.6	FFS
$\mathbb{F}_{370801^{18}}$	101	Jun. 2005	L-V	0.4	Tori
$\mathbb{F}_{65537^{25}}$	121	Oct. 2005	J-L	$\simeq 0$	FFS
$\mathbb{F}_{370801^{30}}$	168	Nov. 2005	J-L	0.1	FFS
$\mathbb{F}_{p^3}$	120	Feb. 2006	J-L-S-V	1.2	NFS