



ALGORITHMIC ASPECTS OF MESTRE'S  
*p*-ADIC POINT COUNTING IDEAS

Reynald Lercier

Reynald.Lercier@m4x.org

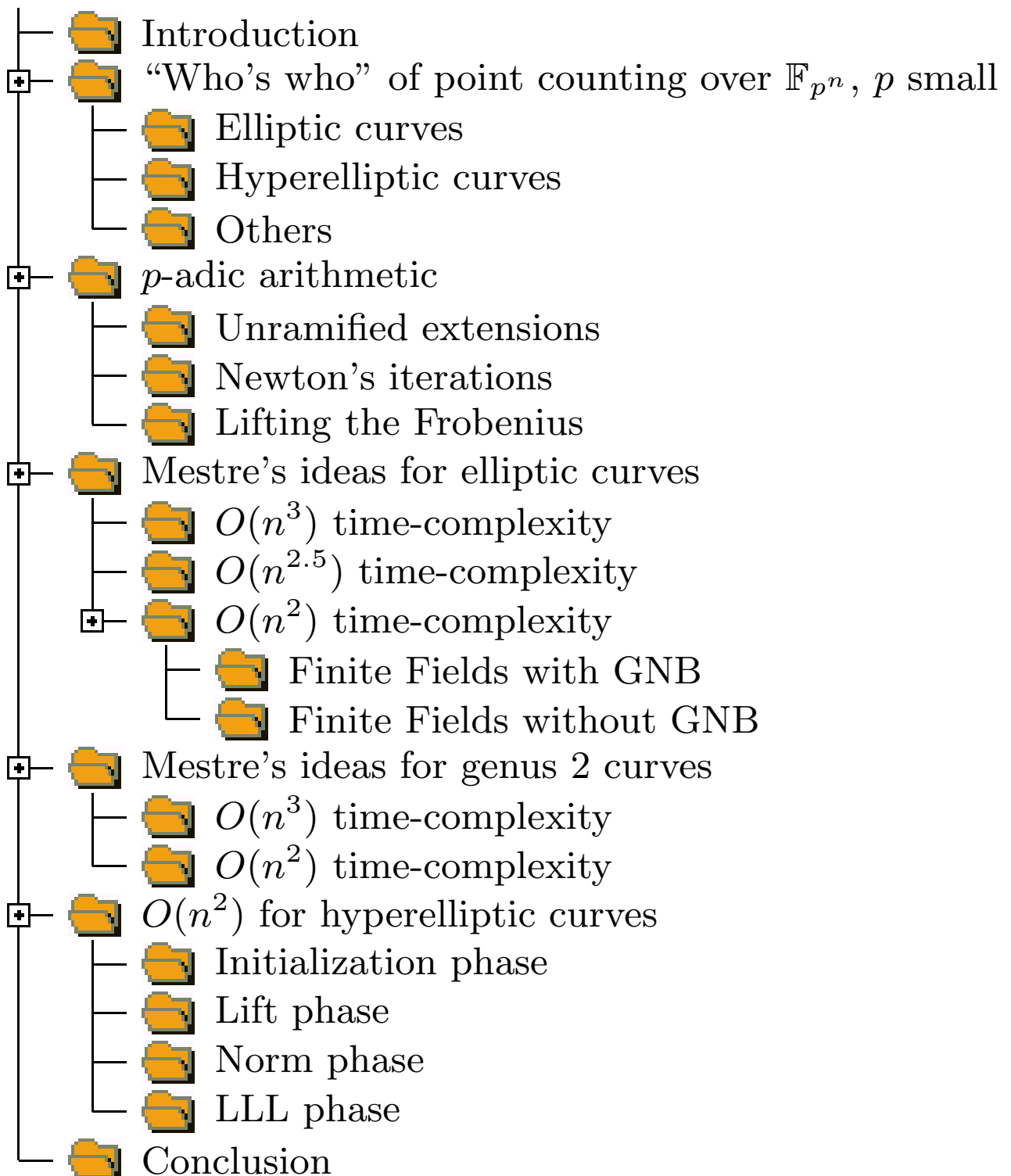
—

David Lubicz

lubicz@celar.fr

August 2003

## Overview



Introduction
“Who’s who” of point counting over $\mathbb{F}_{p^n}$ , $p$ small
$p$ -adic arithmetic
Mestre’s ideas for elliptic curves
Mestre’s ideas for genus 2 curves
$O(n^2)$ for hyperelliptic curves
Conclusion

## Algebraic curves and cryptography

Algebraic curves are an alternative to the use of finite fields in cryptographic schemes (Miller 1986, Koblitz 1987, ...).

For non supersingular curves of small genus, the discrete logarithm problem is hard. The only known attack is a variant of Pollard’s algorithm with exponential running time.

A prerequisite is to count efficiently points on curves. It used to be a difficult task.

It is no more the case for curves defined over  $\mathbb{F}_{p^n}$ ,  $p$  small, especially thanks to a **Satoh**’s breakthrough for elliptic curves and clever simplifications and extensions due to **Mestre** for the “small” genus hyperelliptic case.

**Goal of this talk** : give a complete overview of the algorithmic tools needed to efficiently implement these ideas.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
  - Elliptic curves
  - Hyperelliptic curves
  - Others
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Elliptic curves

$O(np^{n/4})$  in time:

- **D. Shanks**. *Class number, a theory of factorization, and genera*. In Proc. Symp. Pure Math., 20, 1971.
- **J.M. Pollard**. *Monte Carlo methods for index computation (mod  $p$ )*. Math. Comp., 32, 1978.

$O(n^{5+\varepsilon})$  in time,  $O(n^2)$  in space:

- **R. Schoof**. *Elliptic curves over finite fields and the computation of square roots mod  $p$* . Math. Comp., 44, 1985.
- **A. O. L. Atkin**. *The number of points on an elliptic curve modulo a prime*, 1988. Number Theory Mailing List.
- **A.J. Menezes, S.A. Vanstone, R. J. Zuccherato**. *Counting points on elliptic curves over  $\mathbb{F}_{2^m}$* . Math. Comp., 60, 1993.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
  - Elliptic curves
  - Hyperelliptic curves
  - Others
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Elliptic curves

$O(n^{4+\varepsilon})$  in time,  $O(n^2)$  in space:

- N. D. Elkies. *Explicit isogenies*. Draft, 1991.
- A. O. L. Atkin. *The number of points on an elliptic curve modulo a prime*, 1991. Number Theory Mailing List.
- R. Schoof. *Counting points on elliptic curves over finite fields*. J. Théor. Nombres Bordeaux, 1995.
- J. M. Couveignes. *Quelques calculs en théorie des nombres*. thèse, Université de Bordeaux I, 1994.
- R. Lercier. *Computing isogenies in  $\mathbb{F}_{2^n}$* . ANTS-II, LNCS, 1996.
- J. M. Couveignes. *Computing  $l$ -isogenies with the  $p$ -torsion*. ANTS-II, LNCS, 1996.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
  - Elliptic curves
  - Hyperelliptic curves
  - Others
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Elliptic curves

$O(n^{3+\varepsilon})$  in time,  $O(n^3)$  in space:

- **T. Satoh**. *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*. J. Ramanujan Math. Soc., 15, 2000.
- **M. Fouquet, P. Gaudry R.J. Harley**. *An extension of Satoh’s algorithm and its implementation*. J. Ramanujan Math. Soc., 2000.
- **B. Skjernaa**, *Satoh’s algorithm in characteristic 2*. To appear in Math. Comp., preprint, 2000.

$O(n^{3+\varepsilon})$  in time,  $O(n^2)$  in space:

- **F. Vercauteren, B. Preneel, J. Vandewalle**. *A Memory Efficient Version of Satoh’s Algorithm*. EUROCRYPT 2001, LNCS.
- **J.F. Mestre**. *AGM pour le genre 1 et 2*. Lettre à Gaudry et Harley, december 2000.

Introduction
“Who’s who” of point counting over $\mathbb{F}_{p^n}$ , $p$ small
Elliptic curves
Hyperelliptic curves
Others
$p$ -adic arithmetic
Mestre’s ideas for elliptic curves
Mestre’s ideas for genus 2 curves
$O(n^2)$ for hyperelliptic curves
Conclusion

## Elliptic curves

$O(n^{2.5+\varepsilon})$  time,  $O(n^2)$  in space:

- T. Satoh, B. Skjernaas, Y. Taguchi. *Fast computation of canonical lifts of elliptic curves and its application to point counting*, August 2001.
- T. Satoh. *On  $p$ -adic point counting algorithms for elliptic curves over finite fields*. ANTS-V, July 2002.
- H.Y. Kim, J.Y. Park, J.H. Cheon, J.H. Park, J.H. Kim, S.G. Hahn. *Fast elliptic curve point counting using gaussian normal basis*. ANTS-V, July 2002.
- P. Gaudry. *A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2*. ASIACRYPT 2002, December 2002.

$O(n^{2+\varepsilon})$  in time,  $O(n^2)$  in space:

- R. Lercier, D. Lubicz. *Counting points on elliptic curves over finite fields in quadratic time*, submitted for publication, September 2002.
- R.J. Harley, *Algorithmes avancés pour l’arithmétique des courbes*, Thesis, draft, 2003.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
  - Elliptic curves
  - Hyperelliptic curves
  - Others
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Hyperelliptic curves of any genus

### Polynomial in time:

- **J. Pila.** *Frobenius maps of abelian varieties and finding roots of unity in finite fields.* Math. Comp., 1990.

### $O(g^{6+\varepsilon}n^{3+\varepsilon})$ in time, $O(g^3n^3)$ in space:

- **A.G.B Lauder, D. Wan.** *Computing zeta functions of Artin-Schreier curves over finite fields.* London Mathematical Society JCM 5, 2002.

### $O(g^{5+\varepsilon}n^{3+\varepsilon})$ in time, $O(g^3n^3)$ in space:

- **K. Kedlaya.** *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology,* J. Ramanujan Mathematical Society 16 (2001).
- **A.G.B Lauder, D. Wan.** *Computing zeta functions of Artin-Schreier curves over finite fields II.* Preprint, 2002.
- **J. Denef, F. Vercauteren.** *An Extension of Kedlaya’s Algorithm to Artin-Schreier Curves in Characteristic 2.* ANTS-V, 2002.
- **F. Vercauteren,** *Computing Zeta Functions of Hyperelliptic Curves over Finite Fields of Characteristic 2.* CRYPTO 2002.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
  - Elliptic curves
  - Hyperelliptic curves
  - Others
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Hyperelliptic curves of small genus

Genus 2,  $O(n^{3+\varepsilon})$  in time,  $O(n^2)$  in space:

- **J.F. Mestre.** *AGM pour le genre 1 et 2.* Lettre à Gaudry et Harley, 2000.
- **P. Gaudry.** *Algorithms for counting points on curves.* ECC, Waterloo, 2001.

$O(p^g n^{3+\varepsilon})$  in time,  $O(p^g n^2)$  in space:

- **J.F. Mestre.** *Algorithmes pour compter des points en petite caractéristique en genre 1 et 2.* Talk at the cryptographic seminar of Rennes, 2002.

$O(p^g n^{2+\varepsilon})$  in time,  $O(p^g n^2)$  in space:

- **R. Lercier, D. Lubicz.** *A quasi-quadratic time algorithm for hyperelliptic curve point counting* preprint, 2003.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
  - Elliptic curves
  - Hyperelliptic curves
  - Others
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Others

Superelliptic curves,  $O(g^{4+\varepsilon}n^{3+\varepsilon})$  in time,  $O(g^3n^3)$  in space:

- **P. Gaudry, N. Gurel.** *An extension of Kedlaya’s point-counting algorithm to superelliptic curves.* ASIACRYPT 2001, LNCS.

Genus 3,  $O(n^{3+\varepsilon})$  in time,  $O(n^2)$  in space:

- **C. Ritzenhaller.** *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis.* Thesis, Université Paris 7, 2003.

⇒ yields a  $O(n^{2+\varepsilon})$  algorithm with these ideas.

Algebraic varieties, polynomial in time:

- **A.G.B Lauder, D. Wan.** *Counting rational points on varieties over finite fields of small characteristic.* MSRI, Algorithmic Number Theory, 2002.
- **A.G.B Lauder.** *Counting solutions to equations in many variables over finite fields.* Preprint, 2003.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic**
  - Unramified extensions
  - Newton’s iterations
  - Lifting the Frobenius
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## p-adic numbers

**p-adic norm**  $|\cdot|_p$  of  $r \in \mathbb{Q}^*$  is  $|r|_p = p^{-\rho}$ ,  $r = p^\rho u/v$ ,  
 $\rho, u, v \in \mathbb{Z}$ ,  $p \nmid u$ ,  $p \nmid v$ .

Field of **p-adic numbers**  $\mathbb{Q}_p$  is the completion of  $\mathbb{Q}$   
w.r.t.  $|\cdot|_p$ ,

$$\sum_{i=\rho}^{\infty} a_i p^i, \quad a_i \in \{0, 1, \dots, p-1\}, \quad \rho \in \mathbb{Z}.$$

**p-adic integers**  $\mathbb{Z}_p$  is the ring with  $|\cdot|_p \leq 1$  or  
 $\rho \geq 0$ .

Unique maximal ideal

$$M = \{x \in \mathbb{Q}_p \mid |x|_p < 1\} = p\mathbb{Z}_p$$

and  $\mathbb{Z}_p/M \cong \mathbb{F}_p$ .

### Alternative construction.

**Def.** Let  $\pi_m$  be the projection from  $\mathbb{Z}/p^{m+1}\mathbb{Z}$  onto  
 $\mathbb{Z}/p^m\mathbb{Z}$ , then a **p-adic integer** is a sequence  
 $x = (x_1, x_2, \dots, x_m, \dots)$  with  $x_m \in \mathbb{Z}/p^m\mathbb{Z}$  and  
such that  $\pi_m(x_{m+1}) = x_m$ .

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic**
  - Unramified extensions
  - Newton’s iterations
  - Lifting the Frobenius
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Unramified extensions of $p$ -adics

$K$  extension of  $\mathbb{Q}_p$  of degree  $n$  with **valuation ring**  $\mathbb{Z}_q$  and **maximal ideal**  $M_{\mathbb{Z}_q} = \{x \in K \mid |x|_K < 1\}$  where  $|\cdot|_K$  is the unique extension of  $|\cdot|_p$  to  $K$ .

$K$  is said **unramified** iff  $\mathbb{Z}_q/M_{\mathbb{Z}_q} \cong \mathbb{F}_q$  (**residue field**).

**Def.** The **Teichmuller Lift** is the map

$\omega : \mathbb{F}_q \rightarrow \mathbb{Z}_q$  defined by  $\omega(0) = 0$  and for  $x \neq 0$ ,  $\omega(x)$  is the unique  $q - 1$ -th root of unity in  $\mathbb{Z}_q$  such that  $\pi(\omega(x)) = x$  with  $\pi$  the canonical projection of  $\mathbb{Z}_q$  to  $\mathbb{F}_q$ .

**Def.** The **semi-Witt** decomposition of  $x \in \mathbb{Z}_q$  is the unique sequence  $(x_i)_{i \geq 0}$  of  $\mathbb{F}_q$  such that

$$x = \sum_{i \geq 0} \omega(x_i) p^i.$$

**Galois group** of  $K$  over  $\mathbb{Q}_p$  is cyclic with generator **Frobenius substitution**  $\sigma$  and  $\sigma$  modulo  $M_{\mathbb{Z}_q}$  equals to the small Frobenius on  $\mathbb{F}_q$ .

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic**
- Unramified extensions
- Newton’s iterations
- Lifting the Frobenius
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Unramified extensions of $p$ -adics

**Polynomial Basis:** Let  $\mathbb{F}_q \cong \mathbb{F}_p[t]/(\overline{F}(t))$  then,  $K$  can be constructed as

$$K \cong \mathbb{Q}_p[t]/(F(t)),$$

with  $F(t)$  any lift of  $\overline{F}(t)$  to  $\mathbb{Z}_p[t]$ . Such a choice yields a basis  $\{1, t, \dots, t^{n-1}\}$ .

Multiplication at precision  $m$  of two  $p$ -adics costs

$$T_{m,n} = O((nm)^\mu).$$

**Gaussian Normal Basis:** For Galois extension  $K/\mathbb{Q}_p$ , there exists elements  $\alpha$  which yields basis of the form  $\{\alpha, \alpha^\sigma, \dots, \alpha^{\sigma^{n-1}}\}$ .

**Def.** For some  $T$  such that  $\exists$  a primitive  $T$ -th root of unity  $\tau$  in  $\mathbb{Z}/(nT + 1)\mathbb{Z}$  and such that  $\alpha = \sum_{i=0}^{T-1} \gamma^{\tau^i}$  (where  $\gamma$  is a primitive  $(nT + 1)$ -th root of unity) generates a normal basis over  $\mathbb{Q}_p$  called a **Gaussian Normal Basis** (GNB) of type  $T$ .

In this case,  $T_{m,n} = O((Tnm)^\mu)$ .

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic**
  - Unramified extensions
  - Newton’s iterations
  - Lifting the Frobenius
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Newton iteration

To compute the root of a polynomial  $f(x)$  from

$$f(x + p^w \delta) = f(x) + p^w \delta \frac{\partial f}{\partial x}(x) + O(p^{2w}).$$

---

### Algorithm Newton

---

Algorithm to compute a root of  $f(x) \bmod p^m$ , knowing a solution  $x_0$  modulo  $p^{2k+1}$  where  $k = v(\partial f / \partial x(x_0))$ .

---

INPUT:  $x_0 \in \mathbb{Z}_q / p^{2k+1} \mathbb{Z}_q$ ,  $m \in \mathbb{N}$ .

OUTPUT:  $x$  a solution of  $f(x) \bmod p^m$ .

---

1. **if**  $m \leq 2k + 1$  **then return**  $x_0$ ;
2.  $w := \lceil \frac{m}{2} \rceil + k$ ;
3.  $x := \text{Newton}(x_0, w)$ ;
4. Lift  $x$  to precision  $m$ ;
5.  $V := f(x) \bmod p^m$ ;  $\Delta_x := \partial f / \partial x(x) \bmod p^{w-k}$ ;
6. **return**  $x - V / \Delta_x$ ;

**Remark.** Very fast in practice (precision is nearly doubled at each step). For polynomials with  $O(1)$  terms of degree  $O(1)$ , time complexity is  $O(T_{m,n})$ .

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic**
  - Unramified extensions
  - Newton’s iterations
  - Lifting the Frobenius**
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Lifting the Frobenius at precision $m$

**Prop.** Let  $(x_i)_{i \geq 0}$  be the semi-Witt decomposition of a  $p$ -adic  $x$ , then

$$x^\sigma = \sum_{i \geq 0} \omega(x_i)^p p^i.$$

### Polynomial Basis by [Sato-Harley]:

At first, one lifts  $\overline{F}(t)$  at precision  $m$  to the minimal polynomial  $F(t)$  of  $\omega(t)$  using the fact that

$$F(t^p) = \prod_{i=0}^{p-1} F(t\zeta^i) \text{ with } \zeta^p = 1.$$

This can be done by a newton iteration in  $O(T_{m,n} \log n)$  ?

It follows that  $t^\sigma = t^2$  and  $x^\sigma = \sum_{i=0}^{n-1} x_i t^{2i}$  can be easily computed in  $O(T_{m,n})$ .

### GNB by [Kim et al.]:

Computing  $\sigma^k$  can be done by a permutation of the  $nT$  components of  $x$ . This can be easily done in  $S_{m,n} = O(nmT)$ .

A more elaborated implementation strategy (with indexes) yields a  $O(n)$  time complexity.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
  - $O(n^3)$  time-complexity
  - $O(n^{2.5})$  time-complexity
  - $O(n^2)$  time-complexity
    - Finite Fields with GNB
    - Finite Fields without GNB
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

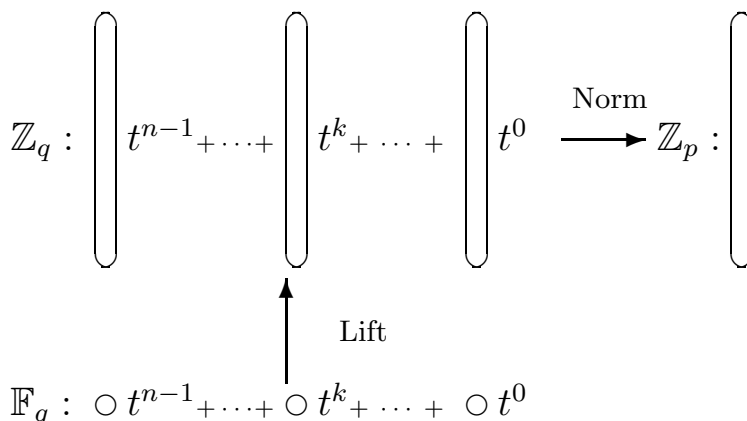
## The “lift” and “norm” paradigm

Let  $E$  be an elliptic curve defined over the field  $\mathbb{F}_{2^n}$  by an equation  $y^2 + xy = x^3 + \alpha$ .

$$\#E(\mathbb{F}_{2^n}) = 2^n + 1 - c \text{ with } |c| \leq 2\sqrt{2^n}.$$

A first  $O(n^3)$  algorithm given by **Satoh** to compute  $c$ , improved by Vercauteren et al. to get a  $O(n^2)$  in space.

At the same time, a completely different method given by **Mestre** for the characteristic 2 case, same complexity, based on AGM.



- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
  - $O(n^3)$  time-complexity
  - $O(n^{2.5})$  time-complexity
  - $O(n^2)$  time-complexity
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## $O(n^3)$ time complexity

Given an explanation of the mathematics which are “behind” the scene is out of the scope of this talk.

A first explanation by Mestre based on isogenies of degree 2 between elliptic curves, more recently an explanation based on the Riemann  $\theta$  functions (cf. [Carls2003], [Ritzenthaler2003]).

---

### Algorithm AGM

---

Algorithm to compute the trace of an ordinary elliptic curve  $E/\mathbb{F}_{2^n} : y^2 + xy = x^3 + \alpha$ .

---

INPUT:  $\alpha \in \mathbb{F}_{2^n}$ .

OUTPUT: The trace  $c$  of  $E$ .

---

*\\Lift phase*

1.  $a := 1 + 8\alpha \in \mathbb{Z}_q; b := 1 \in \mathbb{Z}_q;$
2. **for** ( $i := 1; i < n/2 + O(1); i := i + 1$ ) {
3.      $a, b := \frac{a+b}{2}, \sqrt{ab};$
4. }

*\\Norm phase*

5.  $A := a; B := b;$
6. **for** ( $i := 1; i < n; i := i + 1$ ) {
7.      $a, b := \frac{a+b}{2}, \sqrt{ab};$
8. }
9. **return**  $\frac{A}{a} \bmod 2^n$  as a signed integer in  $[-2\sqrt{2^n}, 2\sqrt{2^n}]$ .

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
  - $O(n^3)$  time-complexity
  - $O(n^{2.5})$  time-complexity
  - $O(n^2)$  time-complexity
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## $O(n^{2.5})$ time complexity

First, the AGM iterations

$$\begin{cases} a_{i+1} &= \frac{a_i + b_i}{2}, \\ b_{i+1} &= \sqrt{a_i b_i}, \end{cases}$$

can be replaced via  $c_i = a_i/b_i$  by

$$c_{i+1} = \frac{2 + c_i}{2\sqrt{c_i}}.$$

Second,

$$c_{i+1} = c_i^\sigma.$$

Consequently, one must solve at precision  $n/2 + O(1)$ ,

$$4x(x^\sigma)^2 = (1+x)^2$$

This equation is an equation of the form  $\phi(x, x^\sigma)$  where  $\phi(x, y)$  is a bivariate polynomial.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
  - $O(n^3)$  time-complexity
  - $O(n^{2.5})$  time-complexity
  - $O(n^2)$  time-complexity
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## SST

---

### Algorithm SSTLift

---

Algorithm to compute a root of  $\phi(x, x^\sigma) \bmod p^m$ , knowing a solution  $x_0$  modulo  $p^{k+1}$  where  $k = v(\partial\phi/\partial x(x_0, x_0^\sigma))$ .

---

INPUT:  $x_0 \in \mathbb{Z}_q/p^{k+1}\mathbb{Z}_q$ ,  $m \in \mathbb{N}$ .

OUTPUT:  $x$  a solution of  $\phi(x, x^\sigma) \bmod p^m$ .

---

1.  $w := \lceil m^{\mu/(\mu+1)} \rceil$ ;  $d$  any lift of  $(\partial_x \phi(x_0, x_0^\sigma))$  to  $\mathbb{Z}_q/p^{w+k}\mathbb{Z}_q$ ;
2.  $x$  any lift of  $x_0$  to  $\mathbb{Z}_q/p^{w+k}\mathbb{Z}_q$
3. **for** ( $i := k + 1$ ;  $i < w + k$ ;  $i := i + 1$ ) {
4.        $y := x^\sigma$ ;
5.        $x := x - \phi(x, y)/d$ ;
6. }
7.  $y := x^\sigma \bmod p^{w+k}$ ;
8.  $D_x := \partial_x \phi(x, y) \bmod p^{w+k}$ ;  $D_y := \partial_y \phi(x, y) \bmod p^{w+k}$ ;
9. **for** ( $j := 1$ ;  $jw + k < m$ ;  $j := j + 1$ ) {
10.       Lift  $x$  to  $\mathbb{Z}_q/p^{(j+1)w+k}\mathbb{Z}_q$ ;
11.        $y := x^\sigma \bmod p^{(j+1)w+k}$ ;
12.        $V := \phi(x, y) \bmod p^{(j+1)w+k}$ ;
13.       **for** ( $i := 0$ ;  $i < w$ ;  $i := i + 1$ ) {
14.                $\Delta_x = -p^{-(jw+i)}V/d$ ;
15.                $\Delta_y = \Delta_x^\sigma \bmod p^{w-i+k}$ ;
16.                $x := x + p^{jw+i}\Delta_x \bmod p^{(j+1)w+k}$ ;
17.                $V+ := p^{jw+i}(D_x\Delta_x + D_y\Delta_y) \bmod p^{(j+1)w+k}$ ;
18.       }
19. }
20. **return**  $x$ ;

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
  - $O(n^3)$  time-complexity
  - $O(n^{2.5})$  time-complexity
  - $O(n^2)$  time-complexity
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## The Norm phase

Once a root  $c_{\lceil n/2 \rceil + 3}$  of

$$4x(x^\sigma)^2 = (1 + x)^2$$

is computed, it remains to get  $c$ .

In fact, it turns out that

$$c = N_{\mathbb{Z}_{2^n}/\mathbb{Z}_2} \left( \frac{2c_{\lceil n/2 \rceil + 3}}{1 + c_{\lceil n/2 \rceil + 3}} \right).$$

Satoh outlines that when  $\text{ord}_p(a - 1) > \frac{1}{p-1}$ , the following formula can be used

$$N_{\mathbb{Z}_q/\mathbb{Z}_p}(a) = \exp(\text{Tr}_{\mathbb{Z}_q/\mathbb{Z}_p}(\log a)).$$

This yields a  $O(n^\mu m^{\mu + \frac{1}{2}})$  time complexity with space equal to  $O(nm)$ .

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
  - $O(n^3)$  time-complexity
  - $O(n^{2.5})$  time-complexity
  - $O(n^2)$  time-complexity
    - Finite Fields with GNB
    - Finite Fields without GNB
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Generalized Newton iterations

Recent results enable to generalize Newton iterations to equations of the form  $\phi(x, x^\sigma) = 0$ . Based on

$$\phi(x + p^w \delta, (x + p^w \delta)^\sigma) = \phi(x, x^\sigma) + p^w \delta \frac{\partial \phi}{\partial x}(x, x^\sigma) + p^w \delta^\sigma \frac{\partial \phi}{\partial y}(x, x^\sigma) + O(p^{2w}).$$

---

### Algorithm NewtonLift

---

Algorithm to compute a root of  $\phi(x, x^\sigma) \bmod p^m$ , knowing a solution  $x_0$  modulo  $p^{2k+1}$  where  $k = v(\partial \phi / \partial y(x_0, x_0^\sigma))$ .

---

INPUT:  $x_0 \in \mathbb{Z}_q / p^{2k+1} \mathbb{Z}_q$ ,  $m \in \mathbb{N}$ .

OUTPUT:  $x$  a solution of  $\phi(x, x^\sigma) \bmod p^m$ .

---

1. **if**  $m \leq 2k + 1$  **then return**  $x_0$ ;
2.  $w := \lceil \frac{m}{2} \rceil + k$ ;
3.  $x := \text{NewtonLift}(x_0, w)$ ;
4. Lift  $x$  to  $\mathbb{Z}_q / p^m \mathbb{Z}_q$ ;  $y := x^\sigma \bmod p^m$ ;
5.  $\Delta_x := \partial_x \phi(x, y) \bmod p^{w-k}$ ;  $\Delta_y := \partial_y \phi(x, y) \bmod p^{w-k}$ ;
6.  $V := \phi(x, y) \bmod p^m$ ;
7.  $a, b := \text{ArtinSchreierRoot}(-V / (p^{w-k} \Delta_y), -\Delta_x / \Delta_y, w-k, n)$ ;
8. **return**  $x + p^{w-k} (1 - a)^{-1} b$ ;

**Remark.** ArtinSchreierRoot is a “black box” which solves equations of the form

$$x^\sigma = ax + b, \quad a \text{ and } b \text{ in } \mathbb{Z}_q.$$

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
  - $O(n^3)$  time-complexity
  - $O(n^{2.5})$  time-complexity
  - $O(n^2)$  time-complexity
    - Finite Fields with GNB
    - Finite Fields without GNB
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Artin-Schreier equations with GNB [Lercier-Lubicz]

- For all  $k \in \mathbb{N}$ ,  $x^{\sigma^k} \equiv a_k x + b_k \pmod{p^w}$ .
- $x^{\sigma^n} = x$ , which means that  $(1 - a_n)x = b_n$ .
- A classical “square and multiply” composition formula,  $\forall k, k' \in \mathbb{Z}^2$ ,

$$x^{\sigma^{k+k'}} = a_k^{\sigma^{k'}} a_{k'} x + a_k^{\sigma^{k'}} b_{k'} + b_k^{\sigma^{k'}}.$$

---

### Algorithm ArtinSchreierRoot

---

Algorithm to compute a root of  $x^\sigma = ax + b$  (when called with  $\nu = n$ ).

---

INPUT:  $a$  and  $b$  in  $\mathbb{Z}_q/p^m\mathbb{Z}_q$ ,  $m$  and  $\nu$  in  $\mathbb{N}$ .

OUTPUT:  $A$  and  $B$  s.t.  $x = Ax^{\sigma^{n-\nu}} + B \pmod{p^m}$ .

---

1. if  $\nu = 1$  then return  $a^{\sigma^{n-1}}, b^{\sigma^{n-1}} \pmod{p^m}$ ;
2.  $A, B := \text{ArtinSchreierRoot}(a, b, m, \lfloor \frac{\nu}{2} \rfloor)$ ;
3.  $A, B := AA^{\sigma^{n-\lfloor \frac{\nu}{2} \rfloor}}, AB^{\sigma^{n-\lfloor \frac{\nu}{2} \rfloor}} + B \pmod{p^m}$ ;
4. if  $\nu \bmod 2$  then  $A, B := Aa^{\sigma^{n-\nu}}, Ab^{\sigma^{n-\nu}} + B \pmod{p^m}$ ;
5. return  $A, B$ ;

Then, the classical “divide and conquer” algorithm to compute the norm works very well for GNB.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
  - $O(n^3)$  time-complexity
  - $O(n^{2.5})$  time-complexity
  - $O(n^2)$  time-complexity
    - Finite Fields with GNB
    - Finite Fields without GNB
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Timings for counting points on elliptic curves defined over $\mathbb{F}_{2^n}$ (GNB)

On a 731 MHz Alpha EV6 CPU.

$n$	GNB type 1		
	Lift	Norm	Total
1018	2.5s	1.5s	4s
2052	10s	7s	17s
4098	1mn	45s	1mn 45
8218	6mn 30	4mn 30	11mn
16420	34mn	23mn	57mn
32770	3h 17	2h 18	5h 35
65538	15h 45	13h 20	1d 5
100002	1d 18	1d 16	3d 10

Current record : 130020 bits by Harley.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
  - $O(n^3)$  time-complexity
  - $O(n^{2.5})$  time-complexity
  - $O(n^2)$  time-complexity
    - Finite Fields with GNB
    - Finite Fields without GNB
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Artin-Schreier equations **without** GNB [Harley-Gaudry]

A cross between Newton iterations and the SST algorithm.

---

### Algorithm ArtinSchreierRoot

---

Algorithm to compute a root of  $x^\sigma = ax + b$ .

---

INPUT:  $x, y, V, i, j, a, b$  such that  $a$  and  $b$  in  $\mathbb{Z}_q/p^m\mathbb{Z}_q$ ,  $v(a) = 1$ ,  $v(b) = 0$ ,  $i$  is the current precision,  $j > i$  is the wanted precision,  $x$  a root at precision  $i$ ,  $y = x^\sigma \pmod{2^j}$  and  $V = y + ax + b$ .

OUTPUT: A root  $x'$  at precision  $j$  and  $x'^\sigma \pmod{2^j}$ .

---

1. **if**  $j = i + 1$  **then return**  $x + 2^i \sqrt{V/2^i}, y + V$ ;
2.  $k := \lfloor \frac{i+j}{2} \rfloor$ ;
3.  $x', y' := \text{ArtinSchreierRoot}(x, y, V, i, k, a, b)$ ;
4.  $y' := y + (x' - x)^\sigma$ ;
5.  $V+ := (x' - x)a + (y' - y)$ ;
6. **return**  $\text{ArtinSchreierRoot}(x', y', V, k, j, a, b)$ ;

Norm computation through the use of Collins’ sub-resultant algorithm ?

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
  - $O(n^3)$  time-complexity
  - $O(n^2)$  time-complexity
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## $O(n^{3+\varepsilon})$ time complexity

It works for curves with ordinary jacobian i.e. which have maximal  $p$ -rank.

Riemann formulas become for the genus 2,  $p = 2$  :

$$\left\{ \begin{array}{l} a_{i+1} = \frac{a_i + b_i + c_i + d_i}{4}, \\ b_{i+1} = \frac{\sqrt{a_i b_i} + \sqrt{c_i d_i}}{2}, \\ c_{i+1} = \frac{\sqrt{a_i c_i} + \sqrt{b_i d_i}}{2}, \\ d_{i+1} = \frac{\sqrt{a_i d_i} + \sqrt{b_i c_i}}{2}, \end{array} \right.$$

(the so called “Borchardt” mean).

Using an algorithm very similar to AGM algorithm, we are able to get A, B, C, D at the needed precision ( $O(3/2n)$ ).

After  $n$  supplementary iterations, one gets

$$\frac{A}{a} = \frac{B}{b} = \frac{C}{c} = \frac{D}{d}$$

which, thanks to the Thomae-Fay formulas, equals to the product of the eigenvalues of the Frobenius morphism which are invertible modulo 2.

$\Rightarrow O(n^{3+\varepsilon})$  time complexity

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
  - $O(n^3)$  time-complexity
  - $O(n^2)$  time-complexity
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## $O(n^{2+\varepsilon})$ time complexity

Let

$$\Phi(b, c, d) = \frac{(\sqrt{b} + \sqrt{c}\sqrt{d})/2}{(1 + b + c + d)/4},$$

then Borchartd iterations can be replaced by

$$\begin{pmatrix} b_{i+1} \\ c_{i+1} \\ d_{i+1} \end{pmatrix} = \begin{pmatrix} \Phi(b_i, c_i, d_i) \\ \Phi(c_i, b_i, d_i) \\ \Phi(d_i, b_i, c_i) \end{pmatrix} \quad \& \quad \begin{pmatrix} b_{i+1} \\ c_{i+1} \\ d_{i+1} \end{pmatrix} = \begin{pmatrix} b_i^\sigma \\ c_i^\sigma \\ d_i^\sigma \end{pmatrix}$$

**Lift phase.** solved through a generalization of **NewtonLift**.

**Norm phase.** Similar to the elliptic curve case.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
  - $O(n^3)$  time-complexity
  - $O(n^2)$  time-complexity
- $O(n^2)$  for hyperelliptic curves
- Conclusion

## Timings for counting points on genus 2 curves defined over $\mathbb{F}_{2^n}$ (GNB)

On a 731 MHz Alpha EV6 CPU.

$n$	GNB type 1		
	Lift	Norm	Total
1018	2mn	5s	2mn 5
2052	8mn 30	25s	8mn 55
4098	50mn 5s	2mn 15	52mn 20
8218	4h 52mn	13mn	5h 5
16420	1d 5	1h	1d 6
32770	7d 22	6h	8d 4

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Initialization phase
- Lift phase
- Norm phase
- LLL phase
- Conclusion

## $O(n^{2+\epsilon})$ for ordinary hyperelliptic curves

Four main phases:

**Initialization phase.** Given an hyperelliptic curve  $H/\mathbb{F}_{p^n}$  one computes at small precision the values at  $z = 0$  taken by  $p^g$  theta functions with  $p^g$  characteristics.

**Lift phase.** Using Riemann duplication formulas, one has to solve a multivariate system  $F(X) = X^\sigma$  in  $\mathbb{Z}_q$  at a precision  $m$  large enough. Solution from the theta constants computed in the initialization phase thanks to a lifting algorithm

**Norm phase.** Computing the norm  $N_{\mathbb{Z}_q/\mathbb{Z}_p}$  of an element of  $\mathbb{Z}_q$  derived from  $X$  yields at precision  $m$  the product  $\pi_1 \cdots \pi_g$  of the  $g$  eigenvalues (invertible modulo  $p$ ) of the Frobenius defined by  $H$ .

**LLL phase.** With LLL algorithm, one obtains a symmetric polynomial  $P_{sym}(X)$  whose roots are of the form  $X + q/X$  ( $X$  is the product of  $g$  terms which belong to  $\{\pi_1, q/\pi_1\}, \dots, \{\pi_g, q/\pi_g\}$ ). It remains to compute its roots over  $\mathbb{C}$  in order to find the characteristic polynomial  $\chi(\pm X)$  of the Frobenius.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Initialization phase
- Lift phase
- Norm phase
- LLL phase
- Conclusion

## Initialization phase

We first lift in  $\mathbb{Z}_{2^n}$  an affine model of  $H$ ,

$$y^2 + h(x)y = h(x)q(x),$$

as follows,

$$Y^2 = (2y + h(x))^2 = h(x)(h(x) + 2^2q(x)).$$

When  $h(x)$  and  $h(x) + 4q(x)$  completely split over  $\mathbb{Z}_{2^n}$ ,

$$Y^2 = \prod_{i=0}^{2g+1} (X - x_i) \text{ such that } x_i \in \mathbb{Z}_{2^n}^2$$

$$\text{and } x_{2i} \equiv x_{2i+1} \pmod{2^2}.$$

Then, Thomae-Fay formulas enable to compute  $2^g$  theta constants  $\theta_0, \dots, \theta_{2^g-1}$  at small precision through

$$\theta_e = \sqrt{\prod_{0 \leq i < j \leq g} (x_{2i+\epsilon_i} - x_{2j+\epsilon_j})(x_{2i+1-\epsilon_i} - x_{2j+1-\epsilon_j})},$$

where  $\epsilon_0 = 0$  and where  $e$  is written in basis 2 as  $\epsilon_g 2^{g-1} + \dots + \epsilon_1$  (the square root is chosen such that  $\theta_e \equiv 1 \pmod{2^2}$ ).

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Initialization phase
- Lift phase
- Norm phase
- LLL phase
- Conclusion

## Lift phase

Let  $R(t_1) = \frac{2\sqrt{t_1}}{1+t_1}$  for curves of genus  $g = 1$  and

$$R(t_1, \dots, t_{2g-1}) = \frac{2\sqrt{t_1} + 2\sqrt{t_2}\sqrt{t_3} + \dots + 2\sqrt{t_{2g-2}}\sqrt{t_{2g-1}}}{1 + t_1 + \dots + t_{2g-1}} \text{ for } g > 1.$$

Riemann duplication formulas yield

$$\forall e \in \{1, \dots, 2^g - 1\}, \tau_e^\sigma = R(\tau_e, \tau_{i_2}, \tau_{i_3}, \dots, \tau_{i_{2g-2}}, \tau_{i_{2g-1}})$$

where, for each  $e$ , the indexes  $i_2, \dots, i_{2g-1}$  are s.t.

$$\{\{0, e\}, \{i_2, i_3\}, \dots, \{i_{2g-2}, i_{2g-1}\}\} = \{\{j, j \oplus e\} \mid j \in \{1, \dots, 2^g - 1\}\}$$

( $\oplus$  denotes the exclusive or of two integers) and

$$\tau_e = \theta_e / \theta_0 \pmod{2^4}.$$

$\Rightarrow$  solved through a generalization of NewtonLift.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Initialization phase
- Lift phase
- Norm phase
- LLL phase
- Conclusion

## Norm phase

The product  $\pi$  of the  $g$  eigenvalues (invertible modulo 2) of the Frobenius defined by  $H$  satisfies

$$\pi \equiv N_{\mathbb{Z}_{2^n}/\mathbb{Z}_2} \left( \frac{2^g}{1 + \tau_1 + \cdots + \tau_{2^g-1}} \right) \pmod{2^m}.$$

$\Rightarrow$  solved in a way similar to the elliptic curve case.

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Initialization phase
- Lift phase
- Norm phase
- LLL phase
- Conclusion

## LLL phase

At first, we build a symmetric polynomial of degree  $2^{g-1}$  with root  $\eta = \pi + 2^{g^n}/\pi$  thanks to a LLL reduction of the lattice  $\mathcal{L}$  given by

$$\begin{bmatrix} K \times M_1 & K \times M_2 & \cdots & K \times M_{2^{g-1}+1} & K \times 2^m \\ 0 & 0 & \cdots & 2^{\lfloor n \times S_{2^{g-1}+1} \rfloor} & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \\ 0 & 2^{\lfloor n \times S_2 \rfloor} & \cdots & 0 & 0 \\ 2^{\lfloor n \times S_1 \rfloor} & 0 & \cdots & 0 & 0 \end{bmatrix},$$

where

$$M = \left[ 2^{(2^{g-1}-1-i)n} \eta^i \bmod 2^m \mid i \in \{0, \dots, 2^{g-1} - 1\} \right] \cup [\eta^{2^{g-1}} \bmod 2^m, 2^m],$$

and

$$S = \left[ \frac{(i-1)(g-2)}{2} \mid i \in \{1, \dots, 2^{g-1}\} \right] \cup \left[ \frac{2^{g-1}(g-2)}{2} + 1 \right]$$

( $K$  is some arbitrarily large constant).

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_p^n$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Initialization phase
- Lift phase
- Norm phase
- LLL phase
- Conclusion

## Precision needed

The coefficients of  $P_{sym}$  are components of a vector  $\Pi$  of small norm in  $\mathcal{L}$ .

Asymptotic estimates state that the LLL algorithm can compute the lattice reduction of  $\mathcal{L}$  if its euclidian norm  $\| \cdot \|_2$  (or sup-norm  $\| \cdot \|_1$ ) satisfy

$$\| \Pi \|_1 \leq \| \Pi \|_2 \leq \det(\mathcal{L})^{1/\dim \mathcal{L}}.$$

$\Rightarrow$  the precision  $m$  needed for the lift must satisfy

$$m > \frac{2^{2g}(g-2) + 2^{g+1}(g+2)}{16} n.$$

Some numeric values:

$g$	1	2	3	4	5	6
$m$	$n/2$	$2n$	$9n$	$44n$	$220n$	$1088n$

$g$	7	8	9	10
$m$	$5264n$	$24896n$	$115392n$	$525824n$

- Introduction
- “Who’s who” of point counting over  $\mathbb{F}_{p^n}$ ,  $p$  small
- $p$ -adic arithmetic
- Mestre’s ideas for elliptic curves
- Mestre’s ideas for genus 2 curves
- $O(n^2)$  for hyperelliptic curves
- Initialization phase
- Lift phase
- Norm phase
- LLL phase
- Conclusion

## Timings for counting points on genus 3 curves defined over $\mathbb{F}_{2^n}$ (GNB)

On a 731 MHz Alpha EV6 CPU.

$n$	GNB type 1		
	Lift	Norm	Total
1018	8h 30	1mn	8h 31
2052	1d 3	5mn	1d 3
4098	6d 8h	25mn	6d 8h

Introduction	■
“Who’s who” of point counting over $\mathbb{F}_p$ , $p$ small	■
$p$ -adic arithmetic	■
Mestre’s ideas for elliptic curves	■
Mestre’s ideas for genus 2 curves	■
$O(n^2)$ for hyperelliptic curves	■
Conclusion	■

## Conclusions & Open Problems

- We have now algorithms to count points for many curves in time very close to the time needed to multiply a divisor by an integer in the Jacobian.
- Reasonable wishes...
  - Non ordinary hyperelliptic curves ?
  - Non hyperelliptic curves in small genus ?
  - $O(g^? n^{2+\varepsilon})$  time complexities algorithms for hyperelliptic curves of any genus ?
  - etc.
- **Golden Grail**: practical algorithms for large  $p$  ?