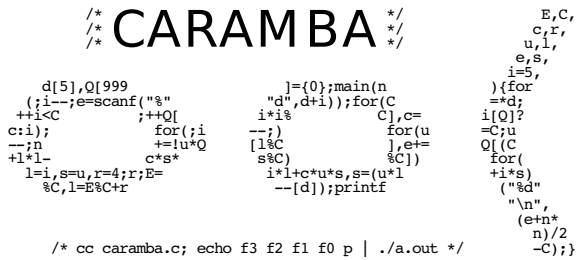
Point counting on hyperelliptic curves: to genus 3 and beyond

Simon Abelard
Université de Lorraine, Nancy

Joint work with P. Gaudry and P.-J. Spaenlehauer

January 25, 2018



It's all about generating series...

A first example

How many solutions of $y^2 = x^7 - 7x^5 + 14x^3 - 7x + 1$ in $\mathbb{F}_{23^k}$?
Goal: generating series associated to these numbers of solutions.
This series is rational so small k's are sufficient (≤ 3 in this case).

It's all about generating series...

A first example

How many solutions of $y^2 = x^7 - 7x^5 + 14x^3 - 7x + 1$ in $\mathbb{F}_{23^k}$?
Goal: generating series associated to these numbers of solutions.
This series is rational so small k's are sufficient (≤ 3 in this case).

Curves and points

Let $f \in \mathbb{F}_q[X]$ be monic, squarefree of degree $2g + 1$.
Equation $Y^2 = f(X) \to$ hyperelliptic curve $\mathcal{C}$ of genus g over $\mathbb{F}_q$.
If $\mathcal{C}$ defined over $\mathbb{F}_q$, $P = (x, y) \in \mathcal{C}$ is rational if $(x, y) \in (\mathbb{F}_q)^2$.

It's all about generating series...

A first example

How many solutions of $y^2 = x^7 - 7x^5 + 14x^3 - 7x + 1$ in $\mathbb{F}_{23^k}$?
Goal: generating series associated to these numbers of solutions.
This series is rational so small k's are sufficient (≤ 3 in this case).

Curves and points

Let $f \in \mathbb{F}_q[X]$ be monic, squarefree of degree $2g + 1$.
Equation $Y^2 = f(X) \rightarrow$ hyperelliptic curve $\mathcal{C}$ of genus g over $\mathbb{F}_q$.
If $\mathcal{C}$ defined over $\mathbb{F}_q$, $P = (x, y) \in \mathcal{C}$ is rational if $(x, y) \in (\mathbb{F}_q)^2$.

Let $\mathcal{C}(\mathbb{F}_{q^i}) = \left\{(x, y) \in (\mathbb{F}_{q^i})^2 \,|\, y^2 = f(x)\right\} \cup \{\infty\}$.
Point counting: computing $\#\mathcal{C}(\mathbb{F}_{q^i})$ for $1 \leq i \leq g$.

. . . Or rather polynomials

Let $\mathcal{C}$ be a hyperelliptic curve of genus g.

Weil conjectures to the rescue

Point counting over $\mathbb{F}_q$ is computing the local ζ function of $\mathcal{C}$:

$$\zeta(s) = \exp\left(\sum_k \#\mathcal{C}(\mathbb{F}_{q^k})\frac{s^k}{k}\right) \overset{thm}{=} \frac{\Lambda(s)}{(1-s)(1-qs)}.$$

With $\Lambda \in \mathbb{Z}[X]$ of degree $2g$ having bounded coefficients.

. . . Or rather polynomials

Let $\mathcal{C}$ be a hyperelliptic curve of genus g.

Weil conjectures to the rescue

Point counting over $\mathbb{F}_q$ is computing the local ζ function of $\mathcal{C}$:

$$\zeta(s) = \exp\left(\sum_k \#\mathcal{C}(\mathbb{F}_{q^k})\frac{s^k}{k}\right) \overset{thm}{=} \frac{\Lambda(s)}{(1-s)(1-qs)}.$$

With $\Lambda \in \mathbb{Z}[X]$ of degree $2g$ having bounded coefficients.

Point counting

Input: $f \in \mathbb{F}_q[X]$ defining a hyperelliptic curve
Output: the polynomial Λ

. . . Or rather polynomials

Let $\mathcal{C}$ be a hyperelliptic curve of genus g.

Weil conjectures to the rescue

Point counting over $\mathbb{F}_q$ is computing the local ζ function of $\mathcal{C}$:

$$\zeta(s) = \exp\left(\sum_k \#\mathcal{C}(\mathbb{F}_{q^k})\frac{s^k}{k}\right) \overset{thm}{=} \frac{\Lambda(s)}{(1-s)(1-qs)}.$$

With $\Lambda \in \mathbb{Z}[X]$ of degree $2g$ having bounded coefficients.

Point counting

Input: $f \in \mathbb{F}_q[X]$ defining a hyperelliptic curve
Output: the polynomial Λ

We study the complexity of such algorithms.

A broad range of related problems

Finding 'nice' curves

Cryptography: $g \leq 2$ and q large, needed to assess security.
Error-correcting codes: need curves with many rational points.

Arithmetic geometry

Conjectures in number theory e.g. Sato-Tate in genus ≥ 2.
L-functions associated: $L(s, \mathcal{C}) = \sum_p A_p / p^s$ with $A_p = \#\mathcal{C}(\mathbb{F}_p)/\sqrt{p}$.
Computing them relies on point-counting primitives.

A broad range of related problems

Finding 'nice' curves

Cryptography: $g \leq 2$ and q large, needed to assess security.
Error-correcting codes: need curves with many rational points.

Arithmetic geometry

Conjectures in number theory e.g. Sato-Tate in genus ≥ 2.
L-functions associated: $L(s, \mathcal{C}) = \sum_p A_p / p^s$ with $A_p = \#\mathcal{C}(\mathbb{F}_p)/\sqrt{p}$.
Computing them relies on point-counting primitives.

Two families of algorithms

- p-adic methods: polynomial in g, exponential in $\log p$
  Satoh'99, Kedlaya'01, Lauder'04
- ℓ-adic methods: exponential in g, polynomial in $\log q$
  Schoof'85, Gaudry-Schost'12

Overview and contributions

Asymptotic complexities (hyperelliptic case)

Pila'90	*Huang-Ierardi'98*	*Adleman-Huang'01*	**Our result**
$(\log q)^{O_g(1)}$	$(\log q)^{g^{O(1)}}$	$(\log q)^{O(g^2 \log g)}$	$O_g\left((\log q)^{cg}\right)$

Overview and contributions

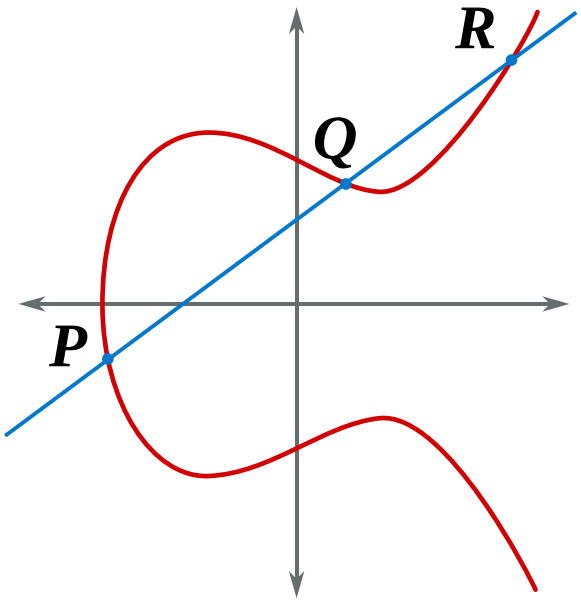
Asymptotic complexities (hyperelliptic case)

Pila'90	*Huang-Ierardi'98*	*Adleman-Huang'01*	**Our result**
$(\log q)^{O_g(1)}$	$(\log q)^{g^{O(1)}}$	$(\log q)^{O(g^2 \log g)}$	$O_g\left((\log q)^{cg}\right)$

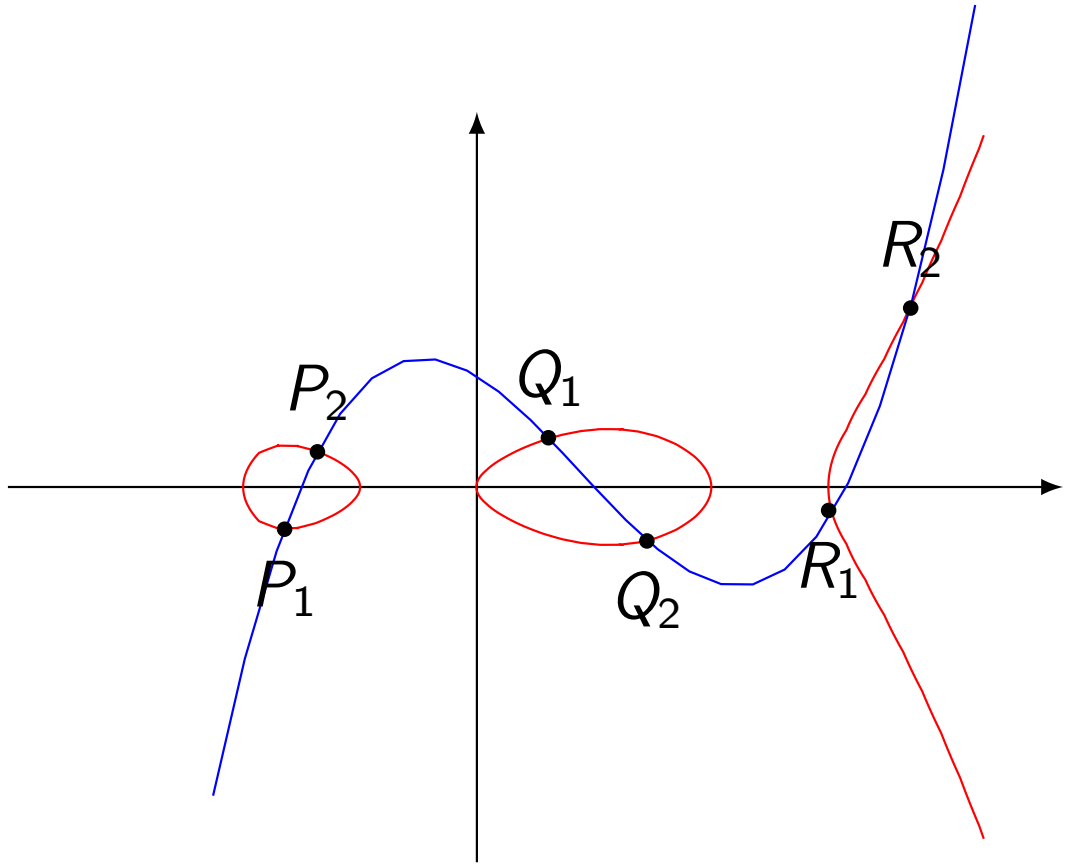
Practical algorithms

Genus	Complexity	Authors
$g = 1$	$\widetilde{O}(\log^4 q)$	Schoof-Elkies-Atkin
$g = 2$	$\widetilde{O}(\log^8 q)$	Gaudry-Schost
$g = 3$	$\widetilde{O}(\log^{14} q)$?	
$g = 2$ with RM	$\widetilde{O}(\log^5 q)$	Gaudry-Kohel-Smith
$g = 3$ with RM	$\widetilde{O}(\log^6 q)$	**Our result**

From curves to groups



$$P + Q + R = 0$$



$$P_1 + P_2 + Q_1 + Q_2 + R_1 + R_2 = 0$$

Counting points on hyperelliptic curves

Let $\mathcal{C} : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{F}_q$.
Let J be its Jacobian and g its genus.

1. (Hasse-Weil) coefficients of Λ are bounded integers.
2. ℓ-torsion $J[\ell] = \{D \in J | \ell D = 0\} \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$
3. Frobenius $\pi : (x, y) \mapsto (x^q, y^q)$ acts linearly on $J[\ell]$
4. For χ the char. polynomial of π, $\chi^{\text{rev}} = \Lambda \bmod \ell$

Algorithm *a la* Schoof

For each prime $\ell \leq (9g + 3) \log q$
  Describe I_ℓ the ideal of ℓ-torsion
  Compute $\chi \bmod \ell$ by testing char. eq. of π in I_ℓ
  Deduce $\Lambda \bmod \ell$
Recover Λ by CRT

Counting points on hyperelliptic curves

Let $\mathcal{C} : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{F}_q$.
Let J be its Jacobian and g its genus.

1. (Hasse-Weil) coefficients of Λ are bounded integers.
2. ℓ-torsion $J[\ell] = \{D \in J | \ell D = 0\} \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$
3. Frobenius $\pi : (x, y) \mapsto (x^q, y^q)$ acts linearly on $J[\ell]$
4. For χ the char. polynomial of π, $\chi^{\text{rev}} = \Lambda \bmod \ell$

Algorithm *a la* Schoof

For each prime $\ell \leq (9g + 3) \log q$
  Describe I_ℓ the ideal of ℓ-torsion
  Compute $\chi \bmod \ell$ by testing char. eq. of π in I_ℓ
  Deduce $\Lambda \bmod \ell$
Recover Λ by CRT

Counting points on hyperelliptic curves

Let $\mathcal{C} : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{F}_q$.
Let J be its Jacobian and g its genus.

1. (Hasse-Weil) coefficients of Λ are bounded integers.
2. ℓ-torsion $J[\ell] = \{D \in J | \ell D = 0\} \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$
3. Frobenius $\pi : (x, y) \mapsto (x^q, y^q)$ acts linearly on $J[\ell]$
4. For χ the char. polynomial of π, $\chi^{\text{rev}} = \Lambda \bmod \ell$

Algorithm *a la* Schoof

For each prime $\ell \leq (9g + 3) \log q$
  Describe I_ℓ the ideal of ℓ-torsion
  Compute $\chi \bmod \ell$ by testing char. eq. of π in I_ℓ
  Deduce $\Lambda \bmod \ell$
Recover Λ by CRT

Counting points on hyperelliptic curves

Let $\mathcal{C} : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{F}_q$.
Let J be its Jacobian and g its genus.

1. (Hasse-Weil) coefficients of Λ are bounded integers.
2. ℓ-torsion $J[\ell] = \{D \in J | \ell D = 0\} \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$
3. Frobenius $\pi : (x, y) \mapsto (x^q, y^q)$ acts linearly on $J[\ell]$
4. For χ the char. polynomial of π, $\chi^{\text{rev}} = \Lambda \bmod \ell$

Algorithm *a la* Schoof

For each prime $\ell \leq (9g + 3) \log q$
  Describe I_ℓ the ideal of ℓ-torsion
  Compute $\chi \bmod \ell$ by testing char. eq. of π in I_ℓ
  Deduce $\Lambda \bmod \ell$
Recover Λ by CRT

Handling the torsion

Goal: represent $J[\ell]$, ideal of ℓ-torsion.
Method: write $\ell D = 0$ formally, then 'solve' that system.

Here comes trouble...

How to model and solve it efficiently?

Handling the torsion

Goal: represent $J[\ell]$, ideal of ℓ-torsion.
Method: write $\ell D = 0$ formally, then 'solve' that system.

Here comes trouble...

How to model and solve it efficiently?

$\longrightarrow$ multihomogeneous structure

Modelling the ℓ-torsion

Writing $\ell D = 0$

Formally, $D = P_1 + \cdots + P_g$, coordinates of P_i (x_i, y_i) are variables.
Compute ℓP_i, then apply zero-test to $\ell D = \sum_i \ell P_i$.

Modelling the ℓ-torsion

Writing $\ell D = 0$

Formally, $D = P_1 + \cdots + P_g$, coordinates of P_i (x_i, y_i) are variables.
Compute ℓP_i, then apply zero-test to $\ell D = \sum_i \ell P_i$.

$\Rightarrow$ there is a $\varphi(X, Y) = P(X) + YQ(X)$ such that $\ell D = (\varphi)$.

Modelling the ℓ-torsion

Writing $\ell D = 0$

Formally, $D = P_1 + \cdots + P_g$, coordinates of P_i (x_i, y_i) are variables.
Compute ℓP_i, then apply zero-test to $\ell D = \sum_i \ell P_i$.

$\Rightarrow$ there is a $\varphi(X, Y) = P(X) + YQ(X)$ such that $\ell D = (\varphi)$.

All computations done...

For each i we get the following congruence:

$$P(X) + Q(X)v_i(X) \equiv 0 \mod u_i(X)$$

About g^2 equations in g^2 variables $\Rightarrow$ Bézout bound in ℓ^{g^2}.
$\Rightarrow$ seems hard to improve previous bound in $(\log q)^{O(g^2)}$...
But not all these variables appear with high degrees.

Multihomogeneity and complexity

$2g$ variables (x_i, y_i)
$\prod_i d_g(x_i) \neq 0,\ y_i^2 - f(x_i) = 0$
$d_{ij} = d_j(x_i),\ e_{ij} = e_j(x_i)$

- degree $O_g(\ell^3)$ in x_i
- $O(g^2)$ equations

Searching $\varphi = P(X) + Q(X)Y$
$g^2 - g$ variables p_i and q_i
$P + Qv_i \equiv 0 \bmod u_i$
$\forall i \neq j,\ \mathrm{Res}(u_i, u_j) \neq 0$

- deg $\leq g^2$ in d_{ij}
- deg ≤ 1 in p_i, q_i, e_{ij}
- $O(g^2)$ variables
- $O(g^2)$ equations

Multihomogeneity and complexity

$2g$ variables (x_i, y_i)
$\prod_i d_g(x_i) \neq 0,\ y_i^2 - f(x_i) = 0$
$d_{ij} = d_j(x_i),\ e_{ij} = e_j(x_i)$

- degree $O_g(\ell^3)$ in x_i
- $O(g^2)$ equations

Searching $\varphi = P(X) + Q(X)Y$
$g^2 - g$ variables p_i and q_i
$P + Qv_i \equiv 0 \bmod u_i$
$\forall i \neq j,\ \mathrm{Res}(u_i, u_j) \neq 0$

- deg $\leq g^2$ in d_{ij}
- deg ≤ 1 in p_i, q_i, e_{ij}
- $O(g^2)$ variables
- $O(g^2)$ equations

Theorem (*Giusti-Lecerf-Salvy'01, Cafure-Matera'06*)

Assume $f_1, \cdots, f_n$ have degrees $\leq d$ and form a reduced regular sequence, and let $\delta = \max_i \deg\langle f_1, \ldots, f_i\rangle$. There is an algorithm computing a geometric resolution in time polynomial in δ, d, n.

With $\delta = O_g\left(\ell^{3g}\right)$ bounded by multihomogeneous Bézout bound.

Handling the torsion

Goal: represent $J[\ell]$, ideal of ℓ-torsion.
Method: write $\ell D = 0$ formally, then 'solve' that system.

Here comes trouble...

How to model and solve it efficiently?
$\longrightarrow$ multihomogeneous structure

Overall result

Model the ℓ-torsion with complexity $O_g(\ell^{cg})$.
Recall the largest ℓ is in $O_g(\log q)$.

$\Rightarrow$ **we compute Λ in $O_g(\log^{cg} q)$.**

Overview and contributions

Asymptotic complexities (hyperelliptic case)

Pila'90	*Huang-Ierardi'98*	*Adleman-Huang'01*	**Our result**
$(\log q)^{O_g(1)}$	$(\log q)^{g^{O(1)}}$	$(\log q)^{O(g^2 \log g)}$	$O_g\left((\log q)^{cg}\right)$

Practical algorithms

Genus	Complexity	Authors
$g = 1$	$\widetilde{O}(\log^4 q)$	Schoof-Elkies-Atkin
$g = 2$	$\widetilde{O}(\log^8 q)$	Gaudry-Schost
$g = 3$	$\widetilde{O}(\log^{14} q)$?	
$g = 2$ with RM	$\widetilde{O}(\log^5 q)$	Gaudry-Kohel-Smith
$g = 3$ with RM	$\widetilde{O}(\log^6 q)$	**Our result**

Experiments in genus 3?

Just writing the systems is hard, solving out of reach for $\ell \geq 5$.

Bad news

Remember $J[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$, must deal with ideals of degree ℓ^6.
Can reach $\widetilde{O}(\ell^{12})$ using naive elimination, hard to go below.
$\Rightarrow$ Intrinsic difficulty due to size of $J[\ell]$.

Experiments in genus 3?

Just writing the systems is hard, solving out of reach for $\ell \geq 5$.

Bad news

Remember $J[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$, must deal with ideals of degree ℓ^6.
Can reach $\widetilde{O}(\ell^{12})$ using naive elimination, hard to go below.
$\Rightarrow$ Intrinsic difficulty due to size of $J[\ell]$.

First step: easier instances

$J[\ell]$ is a vector space of fixed size, what about subspaces?
Context $\Rightarrow$ need π-stable subspaces (i.e. factors of Λ mod ℓ)
Question: find curves with ℓ-torsion that is sum of such subspaces.

A practical case in genus 3

A RM family [Kohel-Smith'06]

Family $\mathcal{C}_t : y^2 = x^7 - 7x^5 + 14x^3 - 7x + t$ with $t \in \mathbb{F}_q$.
$\longrightarrow$ hyperelliptic curves of genus 3, but a bit special.
Denote J_t their Jacobians, recall they are groups.

Where there are groups, there are group (endo)morphisms.
Famous endomorphisms: Frobenius π, multiplication $[\ell]$.

A practical case in genus 3

A RM family [Kohel-Smith'06]

Family $\mathcal{C}_t : y^2 = x^7 - 7x^5 + 14x^3 - 7x + t$ with $t \in \mathbb{F}_q$.
$\longrightarrow$ hyperelliptic curves of genus 3, but a bit special.
Denote J_t their Jacobians, recall they are groups.

Where there are groups, there are group (endo)morphisms.
Famous endomorphisms: Frobenius π, multiplication $[\ell]$.

A remarkable structure

Here, additional endomorphism η, explicit and easy to compute:
For $P = (x, y)$ a generic point on $\mathcal{C}$, $\eta(P) = P_+ + P_-$ with

$$P_\pm = \left(-\frac{11}{4}x \pm \sqrt{\frac{105}{16}x^2 + \frac{16}{9}}, y \right).$$

Exploiting this structure

For some ℓ, decompose multiplication as $[\ell] = \epsilon_1\epsilon_2\epsilon_3$ in $\mathbb{Z}[\eta]$,
Minimal polynomial of η is $X^3 + X^2 - 2X - 1$,
Write $\epsilon_i = a_i + b_i\eta + c_i\eta^2$, and $|a_i|$, $|b_i|$, $|c_i|$ in $O(\ell^{2/3})$.
Split $J_t[\ell] \cong \bigoplus_{i=1}^{3} \operatorname{Ker} \epsilon_i \Rightarrow$ model $\operatorname{Ker} \epsilon_i$ instead of $J_t[\ell]$.

Exploiting this structure

For some ℓ, decompose multiplication as $[\ell] = \epsilon_1\epsilon_2\epsilon_3$ in $\mathbb{Z}[\eta]$,
Minimal polynomial of η is $X^3 + X^2 - 2X - 1$,
Write $\epsilon_i = a_i + b_i\eta + c_i\eta^2$, and $|a_i|$, $|b_i|$, $|c_i|$ in $O(\ell^{2/3})$.
Split $J_t[\ell] \cong \bigoplus_{i=1}^{3} \operatorname{Ker} \epsilon_i \Rightarrow$ model $\operatorname{Ker} \epsilon_i$ instead of $J_t[\ell]$.

Another modelization

Write $\epsilon_i(D) = 0$ instead of $\ell D = 0$, say $D = P_1 + P_2 + P_3 - 3(\infty)$,
Rewrite it $\epsilon_i(P_1) + \epsilon_i(P_2) = -\epsilon_i(P_3)$:

$$\begin{aligned}
\tilde{d}_1(x_1, x_2, y)d_3(x_3) - \tilde{d}_3(x_1, x_2)d_1(x_3) &= 0,\\
\tilde{d}_2(x_1, x_2, y)d_3(x_3) - \tilde{d}_3(x_1, x_2)d_2(x_3) &= 0,\\
\tilde{d}_3(x_1, x_2, y)d_3(x_3) - \tilde{d}_3(x_1, x_2)d_3(x_3) &= 0.
\end{aligned}$$

Exploiting this structure

For some ℓ, decompose multiplication as $[\ell] = \epsilon_1\epsilon_2\epsilon_3$ in $\mathbb{Z}[\eta]$,
Minimal polynomial of η is $X^3 + X^2 - 2X - 1$,
Write $\epsilon_i = a_i + b_i\eta + c_i\eta^2$, and $|a_i|$, $|b_i|$, $|c_i|$ in $O(\ell^{2/3})$.
Split $J_t[\ell] \cong \bigoplus_{i=1}^{3} \operatorname{Ker} \epsilon_i \Rightarrow$ model $\operatorname{Ker} \epsilon_i$ instead of $J_t[\ell]$.

Another modelization

Write $\epsilon_i(D) = 0$ instead of $\ell D = 0$, say $D = P_1 + P_2 + P_3 - 3(\infty)$,
Rewrite it $\epsilon_i(P_1) + \epsilon_i(P_2) = -\epsilon_i(P_3)$:

$$\begin{aligned}
\tilde{d}_1(x_1, x_2, y)d_3(x_3) - \tilde{d}_3(x_1, x_2)d_1(x_3) &= 0,\\
\tilde{d}_2(x_1, x_2, y)d_3(x_3) - \tilde{d}_3(x_1, x_2)d_2(x_3) &= 0,\\
\tilde{d}_3(x_1, x_2, y)d_3(x_3) - \tilde{d}_3(x_1, x_2)d_3(x_3) &= 0.
\end{aligned}$$

Degrees of these polynomials are in $O(\ell^{2/3})$.
Reminder: without splitting $J_t[\ell]$, degrees would be in $O(\ell^2)$.

Solving the system

In theory: no fancy trick

Successive elimination with resultants $\rightarrow \widetilde{O}(\ell^4)$.
About a third of ℓ splits, largest one still in $O(\log q)$.
$\Rightarrow$ Overall complexity in $\widetilde{O}(\log^6 q)$, vs $\widetilde{O}(\log^{14} q)$ in general.

Solving the system

In theory: no fancy trick

Successive elimination with resultants $\rightarrow \widetilde{O}(\ell^4)$.
About a third of ℓ splits, largest one still in $O(\log q)$.
$\Rightarrow$ Overall complexity in $\widetilde{O}(\log^6 q)$, vs $\widetilde{O}(\log^{14} q)$ in general.

In practice (q is a 64-bit prime)

Compute a Gröbner basis using Magma's routines.
Split ℓ we aim for: 13, 29 (also 41 and 43, but speculative)
Other methods yield 2,3 (inert) and 7 (ramified).
Deduce Λ using BSGS, with speed-up $\prod_\ell \ell^{3/2}$.
Ongoing computation, expect Λ in roughly one CPU year.

Conclusion

Describing $J[\ell]$: modelling by polynomial system, then solving.
For curves with RM: split the torsion and describe the smaller bits.

	Theoretic result	Fixed genus case
Curves	hyperelliptic	hyperelliptic with RM
Genus	any g	$g = 3$
Object to model	ℓ-torsion $J[\ell]$	$\mathrm{Ker}\, \epsilon_i$ where $\ell = \prod \epsilon_i$
Equation	$\ell D = 0$	$\epsilon_i(D) = 0$
Complexity	$O_g\left((\log q)^{cg}\right)$	$\widetilde{O}((\log q)^6)$

Thanks for your attention