# Computing the Matrix of Absolute Frobenius via Kedlaya's Algorithm

Jennifer Balakrishnan
jenb@mit.edu
joint work with William Stein

MSRI
July 31, 2006

# Outline

# What Kedlaya's algorithm does

- Given a genus $g$ curve, Kedlaya's algorithm uses Monsky-Washnitzer cohomology of an affine subcurve to compute the zeta function of its reduction over finite fields $\mathbf{F}_{p^r}$.
  - In the situation of $g = 1$ (elliptic curves), this is not the best way to compute zeta functions.
  - For higher genus (and relatively small $p$), this algorithm is great.
- However, as an intermediate step in the algorithm, one computes the matrix of absolute Frobenius, which is useful for computing the cyclotomic $p$-adic height pairing (Mazur, Stein, Tate).
- I'll explain the underlying theory behind Kedlaya's algorithm and compute an example of this matrix.

# What Kedlaya's algorithm does

- Given a genus $g$ curve, Kedlaya's algorithm uses Monsky-Washnitzer cohomology of an affine subcurve to compute the zeta function of its reduction over finite fields $\mathbf{F}_{p^r}$.
    - In the situation of $g = 1$ (elliptic curves), this is not the best way to compute zeta functions.
    - For higher genus (and relatively small $p$), this algorithm is great.
- However, as an intermediate step in the algorithm, one computes the matrix of absolute Frobenius, which is useful for computing the cyclotomic $p$-adic height pairing (Mazur, Stein, Tate).
- I'll explain the underlying theory behind Kedlaya's algorithm and compute an example of this matrix.

# What Kedlaya's algorithm does

- Given a genus $g$ curve, Kedlaya's algorithm uses Monsky-Washnitzer cohomology of an affine subcurve to compute the zeta function of its reduction over finite fields $\mathbf{F}_{p^r}$.
    - In the situation of $g = 1$ (elliptic curves), this is not the best way to compute zeta functions.
    - For higher genus (and relatively small $p$), this algorithm is great.
- However, as an intermediate step in the algorithm, one computes the matrix of absolute Frobenius, which is useful for computing the cyclotomic $p$-adic height pairing (Mazur, Stein, Tate).
- I'll explain the underlying theory behind Kedlaya's algorithm and compute an example of this matrix.

# What Kedlaya's algorithm does

- Given a genus $g$ curve, Kedlaya's algorithm uses Monsky-Washnitzer cohomology of an affine subcurve to compute the zeta function of its reduction over finite fields $\mathbf{F}_{p^r}$.
    - In the situation of $g = 1$ (elliptic curves), this is not the best way to compute zeta functions.
    - For higher genus (and relatively small $p$), this algorithm is great.
- However, as an intermediate step in the algorithm, one computes the matrix of absolute Frobenius, which is useful for computing the cyclotomic $p$-adic height pairing (Mazur, Stein, Tate).
- I'll explain the underlying theory behind Kedlaya's algorithm and compute an example of this matrix.

# What Kedlaya's algorithm does

- Given a genus $g$ curve, Kedlaya's algorithm uses Monsky-Washnitzer cohomology of an affine subcurve to compute the zeta function of its reduction over finite fields $\mathbf{F}_{p^r}$.
  - In the situation of $g = 1$ (elliptic curves), this is not the best way to compute zeta functions.
  - For higher genus (and relatively small $p$), this algorithm is great.
- However, as an intermediate step in the algorithm, one computes the matrix of absolute Frobenius, which is useful for computing the cyclotomic $p$-adic height pairing (Mazur, Stein, Tate).
- I'll explain the underlying theory behind Kedlaya's algorithm and compute an example of this matrix.

# How it works

Three main steps of Kedlaya's algorithm:

- Initialization
- Compute the action of Frobenius on differentials
- Apply a reduction algorithm

# How it works

Three main steps of Kedlaya's algorithm:

- Initialization
- Compute the action of Frobenius on differentials
- Apply a reduction algorithm

# How it works

Three main steps of Kedlaya's algorithm:

- Initialization
- Compute the action of Frobenius on differentials
- Apply a reduction algorithm

# Part I: Initialization

- $E$: elliptic curve $y^2 = Q(x)$ over $\mathbf{Z}_p$ in Weierstrass form
- $p \geqslant 5$: prime of good ordinary reduction
- $\overline{Q}(x)$: the reduction of $Q(x)$ over $\mathbf{F}_p$
- $C_Q$: affine curve over $\mathbf{Z}_p$ defined by $y^2 = Q(x)$
- $C'_Q = C_Q \setminus \{\text{zeros of } y\}$
- $A = \mathbf{Q}_p[x, y, z]/(y^2 - Q(x), yz - 1)$: coordinate ring of $C'_Q$ over $\mathbf{Q}_p$

# Part I: Initialization

- $E$: elliptic curve $y^2 = Q(x)$ over $\mathbf{Z}_p$ in Weierstrass form
- $p \geqslant 5$: prime of good ordinary reduction
- $\overline{Q}(x)$: the reduction of $Q(x)$ over $\mathbf{F}_p$
- $C_Q$: affine curve over $\mathbf{Z}_p$ defined by $y^2 = Q(x)$
- $C'_Q = C_Q \setminus \{\text{zeros of } y\}$
- $A = \mathbf{Q}_p[x, y, z]/(y^2 - Q(x), yz - 1)$: coordinate ring of $C'_Q$ over $\mathbf{Q}_p$

# Part I: Initialization

- $E$: elliptic curve $y^2 = Q(x)$ over $\mathbf{Z}_p$ in Weierstrass form
- $p \geqslant 5$: prime of good ordinary reduction
- $\overline{Q}(x)$: the reduction of $Q(x)$ over $\mathbf{F}_p$
- $C_Q$: affine curve over $\mathbf{Z}_p$ defined by $y^2 = Q(x)$
- $C'_Q = C_Q \setminus \{\text{zeros of } y\}$
- $A = \mathbf{Q}_p[x,y,z]/(y^2 - Q(x), yz - 1)$: coordinate ring of $C'_Q$ over $\mathbf{Q}_p$

# Part I: Initialization

- $E$: elliptic curve $y^2 = Q(x)$ over $\mathbf{Z}_p$ in Weierstrass form
- $p \geqslant 5$: prime of good ordinary reduction
- $\overline{Q}(x)$: the reduction of $Q(x)$ over $\mathbf{F}_p$
- $C_Q$: affine curve over $\mathbf{Z}_p$ defined by $y^2 = Q(x)$
- $C'_Q = C_Q \setminus \{\text{zeros of } y\}$
- $A = \mathbf{Q}_p[x, y, z]/(y^2 - Q(x), yz - 1)$: coordinate ring of $C'_Q$ over $\mathbf{Q}_p$

# Part I: Initialization

- $E$: elliptic curve $y^2 = Q(x)$ over $\mathbf{Z}_p$ in Weierstrass form
- $p \geqslant 5$: prime of good ordinary reduction
- $\overline{Q}(x)$: the reduction of $Q(x)$ over $\mathbf{F}_p$
- $C_Q$: affine curve over $\mathbf{Z}_p$ defined by $y^2 = Q(x)$
- $C'_Q = C_Q \setminus \{\text{zeros of } y\}$
- $A = \mathbf{Q}_p[x, y, z]/(y^2 - Q(x), yz - 1)$: coordinate ring of $C'_Q$ over $\mathbf{Q}_p$

# Part I: Initialization

- $E$: elliptic curve $y^2 = Q(x)$ over $\mathbf{Z}_p$ in Weierstrass form
- $p \geqslant 5$: prime of good ordinary reduction
- $\overline{Q}(x)$: the reduction of $Q(x)$ over $\mathbf{F}_p$
- $C_Q$: affine curve over $\mathbf{Z}_p$ defined by $y^2 = Q(x)$
- $C'_Q = C_Q \setminus \{\text{zeros of } y\}$
- $A = \mathbf{Q}_p[x, y, z]/(y^2 - Q(x), yz - 1)$: coordinate ring of $C'_Q$ over $\mathbf{Q}_p$

# The hyperelliptic involution

Let $\iota : (a, b) \mapsto (a, -b)$ denote the hyperelliptic involution.

- $\iota$ gives an automorphism of the curves $C_{\mathbb{Q}}$ and $C'_{\mathbb{Q}}$.
- This induces automorphisms $\iota^*$ of algebraic de Rham cohomology $H^1(C'_{\mathbb{Q}})$ and $H^1(C_{\mathbb{Q}})$, decomposing them into eigenspaces on which $\iota^*$ acts as 1 and $-1$.
- In particular, $H^1(C'_{\mathbb{Q}}) = H^1(C'_{\mathbb{Q}})^+ \oplus H^1(C'_{\mathbb{Q}})^-$.
- Goal: compute the action of Frobenius on $H^1(C'_{\mathbb{Q}})^-$.

# The hyperelliptic involution

Let $\iota : (a, b) \mapsto (a, -b)$ denote the hyperelliptic involution.

- $\iota$ gives an automorphism of the curves $C_Q$ and $C'_Q$.
- This induces automorphisms $\iota^*$ of algebraic de Rham cohomology $H^1(C'_Q)$ and $H^1(C_Q)$, decomposing them into eigenspaces on which $\iota^*$ acts as 1 and $-1$.
- In particular, $H^1(C'_Q) = H^1(C'_Q)^+ \oplus H^1(C'_Q)^-$.
- Goal: compute the action of Frobenius on $H^1(C'_Q)^-$.

# The hyperelliptic involution

Let $\iota : (a, b) \mapsto (a, -b)$ denote the hyperelliptic involution.

- $\iota$ gives an automorphism of the curves $C_Q$ and $C'_Q$.
- This induces automorphisms $\iota^*$ of algebraic de Rham cohomology $H^1(C'_Q)$ and $H^1(C_Q)$, decomposing them into eigenspaces on which $\iota^*$ acts as 1 and $-1$.
- In particular, $H^1(C'_Q) = H^1(C'_Q)^+ \oplus H^1(C'_Q)^-$.
- Goal: compute the action of Frobenius on $H^1(C'_Q)^-$.

# The hyperelliptic involution

Let $\iota : (a, b) \mapsto (a, -b)$ denote the hyperelliptic involution.

- $\iota$ gives an automorphism of the curves $C_Q$ and $C'_Q$.
- This induces automorphisms $\iota^*$ of algebraic de Rham cohomology $H^1(C'_Q)$ and $H^1(C_Q)$, decomposing them into eigenspaces on which $\iota^*$ acts as 1 and $-1$.
- In particular, $H^1(C'_Q) = H^1(C'_Q)^+ \oplus H^1(C'_Q)^-$.
- Goal: compute the action of Frobenius on $H^1(C'_{\underline{Q}})^-$.

# The $\mathbf{Q}_p$-vector space $H^1(C'_Q)^-$

As a good "first guess," we consider the $\mathbf{Q}_p$-vector space $H^1(C'_Q)^-$:

- It's spanned by the classes of differentials $\{[zdx], [xzdx]\}$.
- However, the underlying coordinate ring $A$ does not admit the proper lift of Frobenius.
- So we restrict to the "dagger ring":

$$A^\dagger = \left\{ \sum_{i,j} a_{i,j} x^i y^j : a_{i,j} \in \mathbf{Q}_p, \liminf_{|j| \to \infty} \frac{v_p(a_{i,j})}{|j|} > 0 \right\}.$$

# The $\mathbf{Q}_p$-vector space $H^1(C'_Q)^-$

As a good "first guess," we consider the $\mathbf{Q}_p$-vector space $H^1(C'_Q)^-$:

- It's spanned by the classes of differentials $\{[zdx], [xzdx]\}$.
- However, the underlying coordinate ring $A$ does not admit the proper lift of Frobenius.
- So we restrict to the "dagger ring":

$$A^\dagger = \left\{ \sum_{i,j} a_{i,j} x^i y^j : a_{i,j} \in \mathbf{Q}_p, \liminf_{|j| \to \infty} \frac{v_p(a_{i,j})}{|j|} > 0 \right\}.$$

# The $\mathbf{Q}_p$-vector space $H^1(C'_Q)^-$

As a good "first guess," we consider the $\mathbf{Q}_p$-vector space $H^1(C'_Q)^-$:

- It's spanned by the classes of differentials $\{[zdx], [xzdx]\}$.
- However, the underlying coordinate ring $A$ does not admit the proper lift of Frobenius.
- So we restrict to the "dagger ring":

$$A^\dagger = \left\{ \sum_{i,j} a_{i,j} x^i y^j : a_{i,j} \in \mathbf{Q}_p, \liminf_{|j| \to \infty} \frac{v_p(a_{i,j})}{|j|} > 0 \right\}.$$

# Monsky-Washnitzer cohomology

The de Rham complex of $A^\dagger$ is given by

$$\begin{aligned} d : A^\dagger &\longrightarrow A^\dagger \frac{zdx}{2} \\ \sum_{i,j} a_{i,j} x^i z^j &\mapsto \sum_{i,j} a_{i,j} d(x^i z^j) \\ &= \sum_{i,j} a_{i,j} (2ix^{i-1} z^{j-1} - jx^i Q' z^{j+1}) \frac{zdx}{2}. \end{aligned}$$

# Monsky-Washnitzer cohomology

- We denote the cohomology groups of this complex by $H^i_{\mathrm{MW}}(C'_{\mathbb{Q}})$.
- As before, they are $\mathbf{Q}_p$-vector spaces split into eigenspaces by the hyperelliptic involution.
- Passing from $A$ to $A^\dagger$ does not change the presentation of cohomology.
- Thus we work with $H^1_{\mathrm{MW}}(C'_{\mathbb{Q}})^-$ and its basis $zdx$ and $xzdx$ to compute the action of Frobenius.

# Monsky-Washnitzer cohomology

- We denote the cohomology groups of this complex by $H^i_{\mathrm{MW}}(C'_Q)$.
- As before, they are $\mathbf{Q}_p$-vector spaces split into eigenspaces by the hyperelliptic involution.
- Passing from $A$ to $A^\dagger$ does not change the presentation of cohomology.
- Thus we work with $H^1_{\mathrm{MW}}(C'_Q)^-$ and its basis $zdx$ and $xzdx$ to compute the action of Frobenius.

# Monsky-Washnitzer cohomology

- We denote the cohomology groups of this complex by $H^i_{\mathrm{MW}}(C'_Q)$.
- As before, they are $\mathbf{Q}_p$-vector spaces split into eigenspaces by the hyperelliptic involution.
- Passing from $A$ to $A^\dagger$ does not change the presentation of cohomology.
- Thus we work with $H^1_{\mathrm{MW}}(C'_Q)^-$ and its basis $zdx$ and $xzdx$ to compute the action of Frobenius.

# Monsky-Washnitzer cohomology

- We denote the cohomology groups of this complex by $H^i_{\mathrm{MW}}(C'_Q)$.
- As before, they are $\mathbf{Q}_p$-vector spaces split into eigenspaces by the hyperelliptic involution.
- Passing from $A$ to $A^\dagger$ does not change the presentation of cohomology.
- Thus we work with $H^1_{\mathrm{MW}}(C'_Q)^-$ and its basis $zdx$ and $xzdx$ to compute the action of Frobenius.

# Part II: Action of Frobenius

We compute the action of Frobenius on $H^1_{\mathrm{MW}}(C'_Q)^-$ by computing its action on the basis elements:

- Begin by letting $G(x) = \frac{\mathrm{Frob}_p(Q(x)) - (Q(x))^p}{p}$.
- Then $F_{p,i} := \mathrm{Frob}_p\left(x^i z dx\right) = \sum_{0 \leqslant k < M} \left(\binom{-1/2}{k} p^{k+1} G^k x^{p(i+1)-1} z^{(2k+1)p-1}\right) z dx$, with a precision of $N$ digits.
- $N$ determines the number of digits of precision of the $p$-adic height to be computed (i.e., modulo $p^N$).
- $M$ is the smallest integer such that $M - \lfloor \log_p(2M+1) \rfloor \geqslant N$.

# Part II: Action of Frobenius

We compute the action of Frobenius on $H^1_{\mathrm{MW}}(C'_Q)^-$ by computing its action on the basis elements:

- Begin by letting $G(x) = \frac{\mathrm{Frob}_p(Q(x)) - (Q(x))^p}{p}$.
- Then $F_{p,i} := \mathrm{Frob}_p\left(x^i z dx\right) = \sum_{0 \leqslant k < M} \left( \binom{-1/2}{k} p^{k+1} G^k x^{p(i+1)-1} z^{(2k+1)p-1} \right) z dx$, with a precision of $N$ digits.
- $N$ determines the number of digits of precision of the $p$-adic height to be computed (i.e., modulo $p^N$).
- $M$ is the smallest integer such that $M - \lfloor \log_p(2M+1) \rfloor \geqslant N$.

# Part II: Action of Frobenius

We compute the action of Frobenius on $H^1_{\mathrm{MW}}(C'_{\mathbb{Q}})^-$ by computing its action on the basis elements:

- Begin by letting $G(x) = \frac{\mathrm{Frob}_p(Q(x)) - (Q(x))^p}{p}$.
- Then $F_{p,i} := \mathrm{Frob}_p\left(x^i z dx\right) =$ $\sum_{0 \leqslant k < M} \left( \binom{-1/2}{k} p^{k+1} G^k x^{p(i+1)-1} z^{(2k+1)p-1} \right) z dx$, with a precision of $N$ digits.
- $N$ determines the number of digits of precision of the $p$-adic height to be computed (i.e., modulo $p^N$).
- $M$ is the smallest integer such that $M - \lfloor \log_p(2M+1) \rfloor \geqslant N$.

# Part II: Action of Frobenius

We compute the action of Frobenius on $H^1_{\mathrm{MW}}(C'_Q)^-$ by computing its action on the basis elements:

- Begin by letting $G(x) = \frac{\mathrm{Frob}_p(Q(x)) - (Q(x))^p}{p}$.
- Then $F_{p,i} := \mathrm{Frob}_p\left(x^i z dx\right) = \sum_{0 \leqslant k < M} \left( \binom{-1/2}{k} p^{k+1} G^k x^{p(i+1)-1} z^{(2k+1)p-1} \right) z dx$, with a precision of $N$ digits.
- $N$ determines the number of digits of precision of the $p$-adic height to be computed (i.e., modulo $p^N$).
- $M$ is the smallest integer such that $M - \lfloor \log_p(2M+1) \rfloor \geqslant N$.

# Part III: Reduction algorithm

As $zdx$ and $xzdx$ span $H^1_{\mathrm{MW}}(C'_Q)^-$, we must now be able to write an arbitrary element in $(A^-)^\dagger \frac{zdx}{2}$, where

$$A^- = \bigoplus_{0 \leqslant i < 3, j \equiv 1(2)} \mathbf{Q}_p x^i z^j,$$

as a linear combination of $d(x^i z^j)$, $zdx$, and $xzdx$.

# Monomial ordering

## Definition

Given a multivariate polynomial $f(x,y,z)$ in $\mathbf{Z}_p[x,y,z]/(y^2 - Q(x), yz - 1)$, the highest monomial of $f$ is the one with smallest power of $z$ and largest power of $x$.

# Example: monomial ordering

## Example

Given $Q(x) = x^3 - x + \frac{1}{4}$ (our $37a$ example), the highest monomial of

$$d(x^i z^j) = 2ix^{i-1}z^{j-1} - 3jx^{i+2}z^{j+1} - jx^i z^{j+1}$$

is $x^{i-1}z^{j-1}$ if $1 \leqslant i < 3$ and $x^2 z^{j+1}$ if $i = 0$.

# The reduction algorithm

Begin by computing a list of differentials $d(x^i z^j)$, where $0 \leqslant i < 3$ and $j \equiv 1 \pmod 2$.

- Group the terms in $\mathrm{Frob}_p(x^i z dx)$ as $(\sum c_{i,j} z^j) z dx$, where $c_{i,j} \in \mathbf{Z}_p[x]$ have degree less than 3.
- If $F_{p,i}$ has a term $(x^i z^j) z dx$ with $j > 0$:

# The reduction algorithm

Begin by computing a list of differentials $d(x^i z^j)$, where $0 \leqslant i < 3$ and $j \equiv 1 \pmod 2$.

- Group the terms in $\mathrm{Frob}_p(x^i z dx)$ as $(\sum c_{i,j} z^j) z dx$, where $c_{i,j} \in \mathbf{Z}_p[x]$ have degree less than 3.
- If $F_{p,i}$ has a term $(x^i z^j) z dx$ with $j > 0$:
  - Consider the term $(c_{i,j} z^j) z dx$ where $j$ is maximal.
  - Take the unique linear combination of the $d(x^k z^{j-1})$ such that when this linear combination is subtracted off of $F_{p,i}$, the resulting "$F_{p,i}$" no longer has terms of the form $(x^m z^j) z dx$.
  - Repeat this process until $F_{p,i}$ (or, in more precise terms, the resulting "$F_{p,i}$" at each step minus linear combinations of differentials) has no terms $(x^m z^j) z dx$ with $j > 0$.

# The reduction algorithm

Begin by computing a list of differentials $d(x^i z^j)$, where $0 \leqslant i < 3$ and $j \equiv 1 \pmod 2$.

- Group the terms in $\mathrm{Frob}_p(x^i z dx)$ as $(\sum c_{i,j} z^j) z dx$, where $c_{i,j} \in \mathbf{Z}_p[x]$ have degree less than 3.
- If $F_{p,i}$ has a term $(x^i z^j) z dx$ with $j > 0$:
    - Consider the term $(c_{i,j} z^j) z dx$ where $j$ is maximal.
    - Take the unique linear combination of the $d(x^k z^{j-1})$ such that when this linear combination is subtracted off of $F_{p,i}$, the resulting "$F_{p,i}$" no longer has terms of the form $(x^m z^j) z dx$.
    - Repeat this process until $F_{p,i}$ (or, in more precise terms, the resulting "$F_{p,i}$" at each step minus linear combinations of differentials) has no terms $(x^m z^j) z dx$ with $j > 0$.

# The reduction algorithm

Begin by computing a list of differentials $d(x^i z^j)$, where $0 \leqslant i < 3$ and $j \equiv 1 \pmod 2$.

- Group the terms in $\mathrm{Frob}_p(x^i z dx)$ as $(\sum c_{i,j} z^j) z dx$, where $c_{i,j} \in \mathbf{Z}_p[x]$ have degree less than 3.
- If $F_{p,i}$ has a term $(x^i z^j) z dx$ with $j > 0$:
  - Consider the term $(c_{i,j} z^j) z dx$ where $j$ is maximal.
  - Take the unique linear combination of the $d(x^k z^{j-1})$ such that when this linear combination is subtracted off of $F_{p,i}$, the resulting "$F_{p,i}$" no longer has terms of the form $(x^m z^j) z dx$.
  - Repeat this process until $F_{p,i}$ (or, in more precise terms, the resulting "$F_{p,i}$" at each step minus linear combinations of differentials) has no terms $(x^m z^j) z dx$ with $j > 0$.

# The reduction algorithm

Begin by computing a list of differentials $d(x^i z^j)$, where $0 \leqslant i < 3$ and $j \equiv 1 \pmod 2$.

- Group the terms in $\mathrm{Frob}_p(x^i z dx)$ as $(\sum c_{i,j} z^j) z dx$, where $c_{i,j} \in \mathbf{Z}_p[x]$ have degree less than 3.
- If $F_{p,i}$ has a term $(x^i z^j) z dx$ with $j > 0$:
  - Consider the term $(c_{i,j} z^j) z dx$ where $j$ is maximal.
  - Take the unique linear combination of the $d(x^k z^{j-1})$ such that when this linear combination is subtracted off of $F_{p,i}$, the resulting "$F_{p,i}$" no longer has terms of the form $(x^m z^j) z dx$.
  - Repeat this process until $F_{p,i}$ (or, in more precise terms, the resulting "$F_{p,i}$" at each step minus linear combinations of differentials) has no terms $(x^m z^j) z dx$ with $j > 0$.

# The reduction algorithm, continued

- If $F_{p,i}$ has terms with $j \leqslant 0$:
  - Let $(x^m z^j)zdx$ be the term with the highest monomial of $F_{p,i}$.
  - Let $(x^k z^l)zdx$ be the term such that $d(x^k z^l)$ has highest term $(x^m z^j)zdx$ and subtract off the appropriate multiple of $d(x^k z^l)$ such that the resulting $F_{p,i}$ no longer has terms of the form $(x^m z^j)zdx$ with $j \neq 0$.
  - Repeat this process until the resulting $F_{p,i}$ is of the form $(a_{0i} + a_{1i}x)\ zdx$.

# The reduction algorithm, continued

- If $F_{p,i}$ has terms with $j \leqslant 0$:
  - Let $(x^m z^j)zdx$ be the term with the highest monomial of $F_{p,i}$.
  - Let $(x^k z^l)zdx$ be the term such that $d(x^k z^l)$ has highest term $(x^m z^j)zdx$ and subtract off the appropriate multiple of $d(x^k z^l)$ such that the resulting $F_{p,i}$ no longer has terms of the form $(x^m z^j)zdx$ with $j \neq 0$.
  - Repeat this process until the resulting $F_{p,i}$ is of the form $(a_{0i} + a_{1i}x)\, zdx$.

# The reduction algorithm, continued

- If $F_{p,i}$ has terms with $j \leqslant 0$:
  - Let $(x^m z^j)zdx$ be the term with the highest monomial of $F_{p,i}$.
  - Let $(x^k z^l)zdx$ be the term such that $d(x^k z^l)$ has highest term $(x^m z^j)zdx$ and subtract off the appropriate multiple of $d(x^k z^l)$ such that the resulting $F_{p,i}$ no longer has terms of the form $(x^m z^j)zdx$ with $j \neq 0$.
  - Repeat this process until the resulting $F_{p,i}$ is of the form $(a_{0i} + a_{1i}x)\, zdx$.

# The reduction algorithm, continued

- If $F_{p,i}$ has terms with $j \leqslant 0$:
  - Let $(x^m z^j) z dx$ be the term with the highest monomial of $F_{p,i}$.
  - Let $(x^k z^l) z dx$ be the term such that $d(x^k z^l)$ has highest term $(x^m z^j) z dx$ and subtract off the appropriate multiple of $d(x^k z^l)$ such that the resulting $F_{p,i}$ no longer has terms of the form $(x^m z^j) z dx$ with $j \neq 0$.
  - Repeat this process until the resulting $F_{p,i}$ is of the form $(a_{0i} + a_{1i} x) \, z dx$.

# Result: The matrix of absolute Frobenius

Now we take the two reduced $F_{p,0} = (a_{00} + a_{10}x)\, zdx$ and $F_{p,1} = (a_{01} + a_{11}x)\, zdx$ and form the matrix of absolute Frobenius:

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}.$$

# Example: $37a$ at $p = 5$

We compute the matrix of absolute Frobenius for the elliptic curve $37a$ (with minimal model $y^2 + y = x^3 - x$) at $p = 5$:

**Step 1** Put the curve into Weierstrass form $y^2 = x^3 + a_4x + a_6$, via the transformation

$$a_4 = -\frac{c_4}{2^4 \cdot 3},$$
$$a_6 = -\frac{c_6}{2^5 \cdot 3^3}.$$

In our case, we obtain the curve

$$y^2 = x^3 - x + \frac{1}{4}.$$

Let

$$Q(x) = x^3 - x + \frac{1}{4}.$$

# Example: $37a$ at $p = 5$

Step 2 Fix the precision $N$ and compute $M$. In our case, $N = 2$ and $M = 3$.

Step 3 Compute the action of Frobenius on $zdx$ and $xzdx$ as an element of $\mathbf{Z}_p[x, y, z]/(y^2 - Q(x), yz - 1)$ with a precision of $N$ digits and group the terms of $\mathrm{Frob}_p(x^i zdx)$ as $\sum(c_{i,j}z^j)zdx$.

In our case, we compute

$$\mathrm{Frob}_5(zdx) \equiv (5xz^2 + (5x + 5x^2)z^4)zdx \pmod{25},$$

$$\mathrm{Frob}_5(xzdx) \equiv (10 + 10x + 5x^3 + (20 + 5x + 15x^2)z^2 + (10 + 20x + 15x^2)z^4)zdx \pmod{25}.$$

# Example: $37a$ at $p = 5$

**Step 2** Fix the precision $N$ and compute $M$. In our case, $N = 2$ and $M = 3$.

**Step 3** Compute the action of Frobenius on $zdx$ and $xzdx$ as an element of $\mathbf{Z}_p[x, y, z]/(y^2 - Q(x), yz - 1)$ with a precision of $N$ digits and group the terms of $\mathrm{Frob}_p(x^i zdx)$ as $\sum(c_{i,j} z^j)zdx$.

In our case, we compute

$$\mathrm{Frob}_5(zdx) \equiv (5xz^2 + (5x + 5x^2)z^4)zdx \pmod{25},$$

$$\mathrm{Frob}_5(xzdx) \equiv (10 + 10x + 5x^3 + (20 + 5x + 15x^2)z^2 + (10 + 20x + 15x^2)z^4)zdx \pmod{25}.$$

# Example: $37a$ at $p = 5$

**Step 2** Fix the precision $N$ and compute $M$. In our case, $N = 2$ and $M = 3$.

**Step 3** Compute the action of Frobenius on $zdx$ and $xzdx$ as an element of $\mathbf{Z}_p[x, y, z]/(y^2 - Q(x), yz - 1)$ with a precision of $N$ digits and group the terms of $\mathrm{Frob}_p(x^i zdx)$ as $\sum(c_{i,j}z^j)zdx$.

In our case, we compute

$$\begin{aligned}\mathrm{Frob}_5(zdx) &\equiv (5xz^2 + (5x + 5x^2)z^4)zdx \pmod{25},\\ \mathrm{Frob}_5(xzdx) &\equiv (10 + 10x + 5x^3 + (20 + 5x + 15x^2)z^2 +\\ &\quad (10 + 20x + 15x^2)z^4)zdx \pmod{25}.\end{aligned}$$

# Example: $37a$ at $p = 5$

**Step 4** Now we must reduce the $\mathrm{Frob}_5(x^i z dx)$.

Using the relation

$$d(x^i z^j) = 2ix^{i-1}z^{j-1} - 3jx^{i+2}z^{j+1} - jx^i z^{j+1},$$

compute the following list of differentials:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2 + 11z^2x^2)zdx$ |
| 1 | 1 | $(12 + 16z^2 + 24z^2x)zdx$ |
| 2 | 1 | $(13x + 16z^2x + 24z^2x^2)zdx$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

# Example: $37a$ at $p = 5$

**Step 4** Now we must reduce the $\mathrm{Frob}_5(x^i z dx)$.

Using the relation

$$d(x^i z^j) = 2ix^{i-1}z^{j-1} - 3jx^{i+2}z^{j+1} - jx^i z^{j+1},$$

compute the following list of differentials:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2 + 11z^2x^2)zdx$ |
| 1 | 1 | $(12 + 16z^2 + 24z^2x)zdx$ |
| 2 | 1 | $(13x + 16z^2x + 24z^2x^2)zdx$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

# Example: $37a$ at $p = 5$

We begin by reducing $F_{5,0} \equiv (5xz^2 + (5x + 5x^2)z^4)zdx \pmod{25}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

- Write $(5x + 5x^2)z^4$ as a linear combination of

$$14z^4 + 8z^4x^2,$$
$$23z^4 + 22z^4x,$$
$$23z^4x + 22z^4x^2.$$

- Note: we ignore the lower powers of $z$ in the differentials

# Example: $37a$ at $p = 5$

We begin by reducing $F_{5,0} \equiv (5xz^2 + (5x + 5x^2)z^4)zdx \pmod{25}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

- Write $(5x + 5x^2)z^4$ as a linear combination of

$$14z^4 + 8z^4x^2,$$
$$23z^4 + 22z^4x,$$
$$23z^4x + 22z^4x^2.$$

# Example: $37a$ at $p = 5$

We begin by reducing $F_{5,0} \equiv (5xz^2 + (5x + 5x^2)z^4)zdx \pmod{25}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

- Write $(5x + 5x^2)z^4$ as a linear combination of

$$14z^4 + 8z^4x^2,$$
$$23z^4 + 22z^4x,$$
$$23z^4x + 22z^4x^2.$$

- Note: we ignore the lower powers of $z$ in the differentials.

# Example: $37a$ at $p = 5$

We begin by reducing $F_{5,0} \equiv (5xz^2 + (5x + 5x^2)z^4)zdx \pmod{25}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

- Write $(5x + 5x^2)z^4$ as a linear combination of

$$14z^4 + 8z^4x^2,$$
$$23z^4 + 22z^4x,$$
$$23z^4x + 22z^4x^2.$$

- Note: we ignore the lower powers of $z$ in the differentials.

# Example: $37a$ at $p = 5$

We begin by reducing $F_{5,0} \equiv (5xz^2 + (5x + 5x^2)z^4)zdx \pmod{25}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

- Write $(5x + 5x^2)z^4$ as a linear combination of

$$14z^4 + 8z^4x^2,$$
$$23z^4 + 22z^4x,$$
$$23z^4x + 22z^4x^2.$$

- Note: we ignore the lower powers of $z$ in the differentials.

# Example: $37a$ at $p = 5$

Taking

$$F_{5,0} - 5d(z^3) - 10d(xz^3) - 20d(x^2z^3) \pmod{25}$$

leaves us with $(10 + 5x)z^2\, zdx$.

# Example: $37a$ at $p = 5$

Now we reduce $(10 + 5x)z^2 \, zdx \pmod{25}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2 + 11z^2x^2)zdx$ |
| 1 | 1 | $(12 + 16z^2 + 24z^2x)zdx$ |
| 2 | 1 | $(13x + 16z^2x + 24z^2x^2)zdx$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

- Write $(10 + 5x)z^2$ as a linear combination of

$$13z^2 + 11z^2x^2$$
$$16z^2 + 24z^2x$$
$$16z^2x + 24z^2x^2$$

# Example: $37a$ at $p = 5$

Now we reduce $(10 + 5x)z^2\, zdx \pmod{25}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2 + 11z^2x^2)zdx$ |
| 1 | 1 | $(12 + 16z^2 + 24z^2x)zdx$ |
| 2 | 1 | $(13x + 16z^2x + 24z^2x^2)zdx$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

- Write $(10 + 5x)z^2$ as a linear combination of

$$13z^2 + 11z^2x^2,$$
$$16z^2 + 24z^2x,$$
$$16z^2x + 24z^2x^2.$$

# Example: $37a$ at $p = 5$

Now we reduce $(10+5x)z^2\ zdx \pmod{25}$:

| $i$ | $j$ | $d(x^iz^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2+11z^2x^2)zdx$ |
| 1 | 1 | $(12+16z^2+24z^2x)zdx$ |
| 2 | 1 | $(13x+16z^2x+24z^2x^2)zdx$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

- Write $(10+5x)z^2$ as a linear combination of

$$13z^2+11z^2x^2,$$
$$16z^2+24z^2x,$$
$$16z^2x+24z^2x^2.$$

# Example: $37a$ at $p = 5$

Now we reduce $(10 + 5x)z^2\ zdx \pmod{25}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2 + 11z^2x^2)zdx$ |
| 1 | 1 | $(12 + 16z^2 + 24z^2x)zdx$ |
| 2 | 1 | $(13x + 16z^2x + 24z^2x^2)zdx$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

- Write $(10 + 5x)z^2$ as a linear combination of

$$13z^2 + 11z^2x^2,$$
$$16z^2 + 24z^2x,$$
$$16z^2x + 24z^2x^2.$$

# Example: $37a$ at $p = 5$

Taking

$$(10 + 5x)z^2\, zdx - 10d(z) - 5d(xz) - 10d(x^2 z)$$

leaves us with

$$(15 + 20x)zdx.$$

We have finished reducing $\mathrm{Frob}_5(zdx)$!

# Example: $37a$ at $p = 5$

Taking

$$(10 + 5x)z^2\, zdx - 10d(z) - 5d(xz) - 10d(x^2 z)$$

leaves us with

$$(15 + 20x)zdx.$$

We have finished reducing $\mathrm{Frob}_5(zdx)$!

# Example: $37a$ at $p = 5$

Now we reduce $\mathrm{Frob}_5(xzdx)$:

$$(10+10x+5x^3+(20+5x+15x^2)z^2+(10+20x+15x^2)z^4)zdx \pmod{25}.$$

- We eliminate the $x^3 zdx$ term first:

$$F_{5,1}-\frac{1}{3}d(x^4z) = (13+2x+(13+10x+7x^2)z^2+(10+20x+15x^2)z^4)\ zdx.$$

# Example: $37a$ at $p = 5$

Now proceed as in the case of $F_{5,0}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

# Example: $37a$ at $p = 5$

Now proceed as in the case of $F_{5,0}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

- Write $(10 + 20x + 15x^2)z^4$ as a linear combination of

$$14z^4 + 8z^4x^2,$$
$$23z^4 + 22z^4x,$$
$$23z^4x + 22z^4x^2.$$

# Example: $37a$ at $p = 5$

Now proceed as in the case of $F_{5,0}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

- Write $(10 + 20x + 15x^2)z^4$ as a linear combination of

$$14z^4 + 8z^4x^2,$$
$$23z^4 + 22z^4x,$$
$$23z^4x + 22z^4x^2.$$

# Example: $37a$ at $p = 5$

Now proceed as in the case of $F_{5,0}$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| $\vdots$ | $\vdots$ | $\vdots$ |
| 0 | 3 | $(14z^4 + 8z^4x^2)zdx$ |
| 1 | 3 | $(9z^2 + 23z^4 + 22z^4x)zdx$ |
| 2 | 3 | $(10z^2x + 23z^4x + 22z^4x^2)zdx$ |

- Write $(10 + 20x + 15x^2)z^4$ as a linear combination of

$$14z^4 + 8z^4x^2,$$
$$23z^4 + 22z^4x,$$
$$23z^4x + 22z^4x^2.$$

# Example: $37a$ at $p = 5$

Taking

$$(13 + 2x + (13 + 10x + 7x^2)z^2 + (10 + 20x + 15x^2)z^4)\, zdx$$
$$- (10d(z^3) + 15d(xz^3) + 5d(x^2z^3))$$

leaves us with

$$(13 + 2x + (3 + 10x + 7x^2)z^2)\, zdx.$$

# Example: $37a$ at $p = 5$

Now we reduce $(13 + 2x + (3 + 10x + 7x^2)z^2)\ zdx$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2 + 11z^2x^2)zdx$ |
| 1 | 1 | $(12 + 16z^2 + 24z^2x)zdx$ |
| 2 | 1 | $(13x + 16z^2x + 24z^2x^2)zdx$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

- Write $(3 + 10x + 7x^2)z^2$ as a linear combination of

$$13z^2 + 11z^2x^2,$$
$$16z^2 + 24z^2x,$$
$$16z^2x + 24z^2x^2$$

# Example: $37a$ at $p = 5$

Now we reduce $(13 + 2x + (3 + 10x + 7x^2)z^2)\ zdx$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2 + 11z^2x^2)zdx$ |
| 1 | 1 | $(12 + 16z^2 + 24z^2x)zdx$ |
| 2 | 1 | $(13x + 16z^2x + 24z^2x^2)zdx$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

- Write $(3 + 10x + 7x^2)z^2$ as a linear combination of

$$13z^2 + 11z^2x^2,$$
$$16z^2 + 24z^2x,$$
$$16z^2x + 24z^2x^2.$$

# Example: $37a$ at $p = 5$

Now we reduce $(13 + 2x + (3 + 10x + 7x^2)z^2)\ zdx$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2 + 11z^2x^2)zdx$ |
| 1 | 1 | $(12 + 16z^2 + 24z^2x)zdx$ |
| 2 | 1 | $(13x + 16z^2x + 24z^2x^2)zdx$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

- Write $(3 + 10x + 7x^2)z^2$ as a linear combination of

$$13z^2 + 11z^2x^2,$$
$$16z^2 + 24z^2x,$$
$$16z^2x + 24z^2x^2.$$

# Example: $37a$ at $p = 5$

Now we reduce $(13 + 2x + (3 + 10x + 7x^2)z^2)\ zdx$:

| $i$ | $j$ | $d(x^i z^j) \pmod{25}$ |
|---|---|---|
| 0 | 1 | $(13z^2 + 11z^2x^2)zdx$ |
| 1 | 1 | $(12 + 16z^2 + 24z^2x)zdx$ |
| 2 | 1 | $(13x + 16z^2x + 24z^2x^2)zdx$ |
| $\vdots$ | $\vdots$ | $\vdots$ |

- Write $(3 + 10x + 7x^2)z^2$ as a linear combination of

$$13z^2 + 11z^2x^2,$$
$$16z^2 + 24z^2x,$$
$$16z^2x + 24z^2x^2.$$

# Example: $37a$ at $p = 5$

Taking

$$(13 + 2x + (3 + 10x + 7x^2)z^2\ zdx - 20d(z) - 23d(xz) - 13d(x^2z)$$

leaves us with

$$(12 + 8x)zdx.$$

# Example: $37a$ at $p = 5$

- Thus we have that $\text{Frob}_5(xzdx) = (12 + 8x)zdx$.

## Step 5

Form the matrix $F$ of the reduced differentials, where each reduced differential gives us a column in the matrix of absolute Frobenius.

In our case, as

$$\text{Frob}_5(zdx) = (15 + 20x)zdx$$
$$\text{Frob}_5(xzdx) = (12 + 8x)zdx,$$

we have

$$F = \begin{pmatrix} 15 & 12 \\ 20 & 8 \end{pmatrix}.$$

# Example: $37a$ at $p = 5$

- Thus we have that $\mathrm{Frob}_5(xzdx) = (12 + 8x)zdx$.

**Step 5** Form the matrix $F$ of the reduced differentials, where each reduced differential gives us a column in the matrix of absolute Frobenius.

In our case, as

$$\mathrm{Frob}_5(zdx) = (15 + 20x)zdx$$
$$\mathrm{Frob}_5(xzdx) = (12 + 8x)zdx,$$

we have

$$F = \begin{pmatrix} 15 & 12 \\ 20 & 8 \end{pmatrix}.$$

# Example: $37a$ at $p = 5$

- Thus we have that $\mathrm{Frob}_5(xzdx) = (12 + 8x)zdx$.

**Step 5** Form the matrix $F$ of the reduced differentials, where each reduced differential gives us a column in the matrix of absolute Frobenius.

In our case, as

$$\mathrm{Frob}_5(zdx) = (15 + 20x)zdx$$
$$\mathrm{Frob}_5(xzdx) = (12 + 8x)zdx,$$

we have

$$F = \begin{pmatrix} 15 & 12 \\ 20 & 8 \end{pmatrix}.$$

# Example: $37a$ at $p = 5$

- Thus we have that $\mathrm{Frob}_5(xzdx) = (12 + 8x)zdx$.

Step 5 Form the matrix $F$ of the reduced differentials, where each reduced differential gives us a column in the matrix of absolute Frobenius.

In our case, as

$$\begin{aligned} \mathrm{Frob}_5(zdx) &= (15 + 20x)zdx \\ \mathrm{Frob}_5(xzdx) &= (12 + 8x)zdx, \end{aligned}$$

we have

$$F = \begin{pmatrix} 15 & 12 \\ 20 & 8 \end{pmatrix}.$$

# Example: $37a$ at $p = 5$

So the matrix of absolute Frobenius is

$$F = \begin{pmatrix} 15 & 12 \\ 20 & 8 \end{pmatrix}.$$

- As a consistency check, we see that $F$ has trace 23, which is $a_5$ modulo 25 and determinant $-120$, which is $p = 5$ modulo 25.

# Summary

- We used Kedlaya's algorithm to compute the matrix of absolute Frobenius.
  - Compute action of Frob on appropriate cohomology group.
  - Reduce differentials.
- More details in the papers of Kedlaya (also, see exposition by Edixhoven)
- Applications:
  - For genus $g > 1$: compute zeta functions of hyperelliptic curves
  - For genus $g = 1$: compute $p$-adic heights (Mazur, Stein, Tate)

# Summary

- We used Kedlaya's algorithm to compute the matrix of absolute Frobenius.
  - Compute action of Frob on appropriate cohomology group.
  - Reduce differentials.
- More details in the papers of Kedlaya (also, see exposition by Edixhoven)
- Applications:
  - For genus $g > 1$: compute zeta functions of hyperelliptic curves
  - For genus $g = 1$: compute $p$-adic heights (Mazur, Stein, Tate)

# Summary

- We used Kedlaya's algorithm to compute the matrix of absolute Frobenius.
  - Compute action of Frob on appropriate cohomology group.
  - Reduce differentials.
- More details in the papers of Kedlaya (also, see exposition by Edixhoven)
- Applications:
  - For genus $g > 1$: compute zeta functions of hyperelliptic curves
  - For genus $g = 1$: compute $p$-adic heights (Mazur, Stein, Tate)

# Summary

- We used Kedlaya's algorithm to compute the matrix of absolute Frobenius.
  - Compute action of Frob on appropriate cohomology group.
  - Reduce differentials.
- More details in the papers of Kedlaya (also, see exposition by Edixhoven)
- Applications:
  - For genus $g > 1$: compute zeta functions of hyperelliptic curves
  - For genus $g = 1$: compute $p$-adic heights (Mazur, Stein, Tate)

# Summary

- We used Kedlaya's algorithm to compute the matrix of absolute Frobenius.
    - Compute action of Frob on appropriate cohomology group.
    - Reduce differentials.
- More details in the papers of Kedlaya (also, see exposition by Edixhoven)
- Applications:
    - For genus $g > 1$: compute zeta functions of hyperelliptic curves
    - For genus $g = 1$: compute $p$-adic heights (Mazur, Stein, Tate)

# Summary

- We used Kedlaya's algorithm to compute the matrix of absolute Frobenius.
    - Compute action of Frob on appropriate cohomology group.
    - Reduce differentials.
- More details in the papers of Kedlaya (also, see exposition by Edixhoven)
- Applications:
    - For genus $g > 1$: compute zeta functions of hyperelliptic curves
    - For genus $g = 1$: compute $p$-adic heights (Mazur, Stein, Tate)

# Summary

- We used Kedlaya's algorithm to compute the matrix of absolute Frobenius.
    - Compute action of Frob on appropriate cohomology group.
    - Reduce differentials.
- More details in the papers of Kedlaya (also, see exposition by Edixhoven)
- Applications:
    - For genus $g > 1$: compute zeta functions of hyperelliptic curves
    - For genus $g = 1$: compute $p$-adic heights (Mazur, Stein, Tate)

# Workshop problems

Some open problems we'd like to work on these next two weeks:

- Are there simplifications one could make to the above algorithm taking into account the fact that we're working with elliptic curves (e.g., using group structure, etc.)? Should we expect that the matrix of Frobenius be easier to compute in the case of genus 1 curves?
- A question of John Tate: how does the cyclotomic $p$-adic height pairing change for families of elliptic curves, e.g., $y^2 = x^3 + tx + 1$? What about considering families with constant $j$-invariant? Non-constant $j$-invariant? Curves with complex multiplication? Curves without complex multiplication?

# Workshop problems

Some open problems we'd like to work on these next two weeks:

- Are there simplifications one could make to the above algorithm taking into account the fact that we're working with elliptic curves (e.g., using group structure, etc.)? Should we expect that the matrix of Frobenius be easier to compute in the case of genus 1 curves?
- A question of John Tate: how does the cyclotomic $p$-adic height pairing change for families of elliptic curves, e.g., $y^2 = x^3 + tx + 1$? What about considering families with constant $j$-invariant? Non-constant $j$-invariant? Curves with complex multiplication? Curves without complex multiplication?

# Workshop problems, continued

Even more problems:

- Extend the above algorithm to implement the computation of anticyclotomic $p$-adic heights, using new ideas of Mazur.
- (From Christian Wuthrich.) For computational reasons it would be interesting to also include the primes 2 and 3. It should be possible to write a more complicated Kedlaya algorithm at least for 3.
- (From Christian Wuthrich.) There is a well-defined supersingular theory explained by Perrin-Riou. The Kedlaya algorithm can be used to compute the $p$-adic heights also in this case.

# Workshop problems, continued

Even more problems:

- Extend the above algorithm to implement the computation of anticyclotomic $p$-adic heights, using new ideas of Mazur.
- (From Christian Wuthrich.) For computational reasons it would be interesting to also include the primes 2 and 3. It should be possible to write a more complicated Kedlaya algorithm at least for 3.
- (From Christian Wuthrich.) There is a well-defined supersingular theory explained by Perrin-Riou. The Kedlaya algorithm can be used to compute the $p$-adic heights also in this case.

# Workshop problems, continued

Even more problems:

- Extend the above algorithm to implement the computation of anticyclotomic $p$-adic heights, using new ideas of Mazur.
- (From Christian Wuthrich.) For computational reasons it would be interesting to also include the primes 2 and 3. It should be possible to write a more complicated Kedlaya algorithm at least for 3.
- (From Christian Wuthrich.) There is a well-defined supersingular theory explained by Perrin-Riou. The Kedlaya algorithm can be used to compute the $p$-adic heights also in this case.