Point counting without points

Antoine Leudière

University of Calgary

Number Theory and Combinatorics Seminar
University of Lethbridge, November 26th 2025

Today

What are Drinfeld modules? How do they compare to elliptic curves?

A method for counting points on Drinfeld modules, using Anderson motives.

Joint work with Xavier Caruso.

The rules of point counting

Philosophy of Drinfeld modules

Representation of Drinfeld modules

Point counting without points

Cost of the algorithms

The rules of point counting

Philosophy of Drinfeld modules

Representation of Drinfeld modules

Point counting without points

Cost of the algorithms

What is point counting?

Naive approach

Counting solutions to an equation.

Generally a hard problem:

- Algebraic varieties on a finite field.
- Matiyasevich's theorem (1970): no algorithm can tell if any given Diophantine equation has integer solutions.

Consider object with more structure: *elliptic curves*, *abelian varieties*.

What is point counting?

Naive approach

Counting solutions to an equation.

Generally a hard problem:

- Algebraic varieties on a finite field.
- Matiyasevich's theorem (1970): no algorithm can tell if any given Diophantine equation has integer solutions.

Consider object with more structure: *elliptic curves*, *abelian varieties*.

What is point counting?

Naive approach

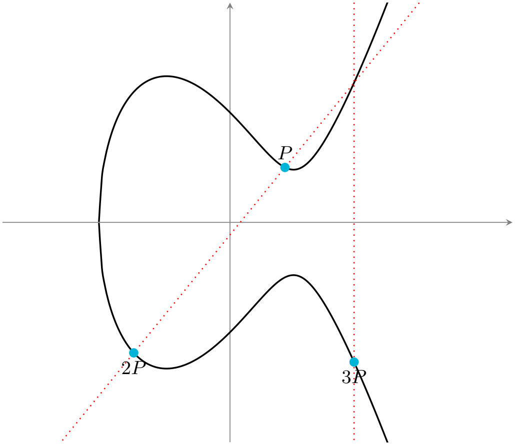
Counting solutions to an equation.

Generally a hard problem:

- Algebraic varieties on a finite field.
- Matiyasevich's theorem (1970): no algorithm can tell if any given Diophantine equation has integer solutions.

Consider object with more structure: *elliptic curves*, *abelian varieties*.

Elliptic curves



Smooth algebraic projective curves with genus 1 and a distinguished point O.

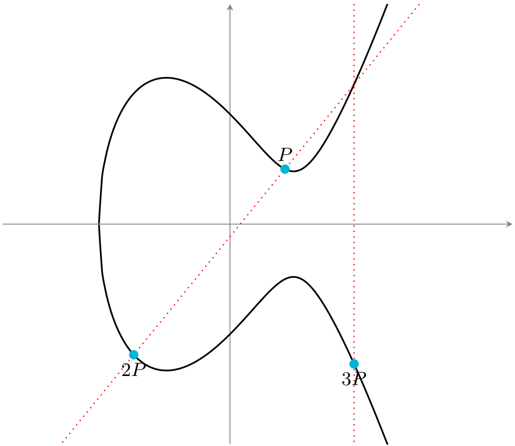
Double nature

Arithmetic-geometric objects.

Applications

- Number theory
- Cryptography (pre & post-quantum)
- Computer algebra (ECPP, ECM)

Elliptic curves



Smooth algebraic projective curves with genus 1 and a distinguished point O.

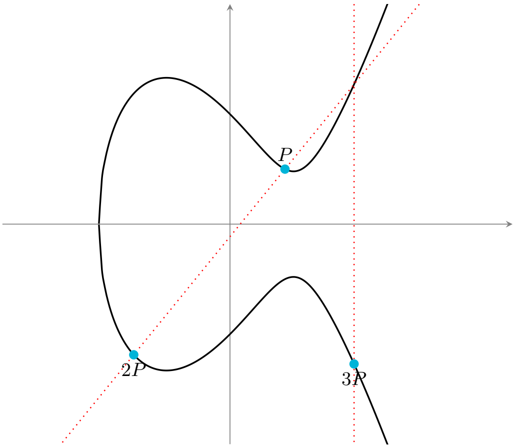
Double nature

Arithmetic-geometric objects.

Applications

- Number theory
- Cryptography (pre & post-quantum)
- Computer algebra (ECPP, ECM)

Elliptic curves



Smooth algebraic projective curves with genus 1 and a distinguished point O.

Double nature

Arithmetic-geometric objects.

Applications

- Number theory
- Cryptography (pre & post-quantum)
- Computer algebra (ECPP, ECM)

Changing the rules

Let E be an elliptic curve. As an abelian group,

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

So

$$\#E(\mathbb{F}_q) = |d_1 \cdots d_n|.$$

Let R be a PID, M be a finite R-module. There are $m_1, \ldots, m_\ell \in R$ s.t.:

$$M \simeq R/m_1R \times \cdots \times R/m_\ell R.$$

R-cardinality

Define the *R-cardinality of M* as

$$m_1 \cdots m_\ell.$$

Changing the rules

Let E be an elliptic curve. As an abelian group,

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

So

$$\#E(\mathbb{F}_q) = |d_1 \cdots d_n|.$$

Let R be a PID, M be a finite R-module. There are $m_1, \ldots, m_\ell \in R$ s.t.:

$$M \simeq R/m_1R \times \cdots \times R/m_\ell R.$$

R-cardinality

Define the *R-cardinality of M* as

$$m_1 \cdots m_\ell.$$

Changing the rules

Let E be an elliptic curve. As an abelian group,

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

So

$$\#E(\mathbb{F}_q) = |d_1 \cdots d_n|.$$

Let R be a PID, M be a finite R-module. There are $m_1, \ldots, m_\ell \in R$ s.t.:

$$M \simeq R/m_1R \times \cdots \times R/m_\ell R.$$

R-cardinality

Define the *R-cardinality of M* as

$$m_1 \cdots m_\ell.$$

An alternative to $\mathbb{Z}$

Replace $\mathbb{Z}$ by $R = \mathbb{F}_q[T]$!

Both Euclidean rings:

- $\mathbb{Z}$: world of number fields.
- $\mathbb{F}_q[T]$: world of function fields.

Advantages of function fields

- Unconditional results (*e.g.* GRH).
- Faster algorithms (*e.g.* factorization).
- Geometrical properties of function fields.
- And others: $\mathbb{F}_q$-linearity, non-Archimedean analysis, etc.

An alternative to $\mathbb{Z}$

Replace $\mathbb{Z}$ by $R = \mathbb{F}_q[T]$!

Both Euclidean rings:

- $\mathbb{Z}$: world of number fields.
- $\mathbb{F}_q[T]$: world of function fields.

Advantages of function fields

- Unconditional results (*e.g.* GRH).
- Faster algorithms (*e.g.* factorization).
- Geometrical properties of function fields.
- And others: $\mathbb{F}_q$-linearity, non-Archimedean analysis, etc.

An alternative to $\mathbb{Z}$

Replace $\mathbb{Z}$ by $R = \mathbb{F}_q[T]$!

Both Euclidean rings:

- $\mathbb{Z}$: world of number fields.
- $\mathbb{F}_q[T]$: world of function fields.

Advantages of function fields

- Unconditional results (*e.g.* GRH).
- Faster algorithms (*e.g.* factorization).
- Geometrical properties of function fields.
- And others: $\mathbb{F}_q$-linearity, non-Archimedean analysis, etc.

An alternative to $\mathbb{Z}$

Replace $\mathbb{Z}$ by $R = \mathbb{F}_q[T]$!

Both Euclidean rings:

- $\mathbb{Z}$: world of number fields.
- $\mathbb{F}_q[T]$: world of function fields.

Advantages of function fields

- Unconditional results (*e.g.* GRH).
- Faster algorithms (*e.g.* factorization).
- Geometrical properties of function fields.
- And others: $\mathbb{F}_q$-linearity, non-Archimedean analysis, etc.

What are elliptic curves for $R = \mathbb{F}_q[T]$?

Module structure	
$\mathbb{Z}$-module	$\mathbb{F}_q[T]$-module
Torsion	
$(\mathbb{Z}/n\mathbb{Z})^2$, $p \nmid n$	$(\mathbb{F}_q[T]/a\mathbb{F}_q[T])^2$, $\mathfrak{p} \nmid a$
Endomorphism ring	
$\mathbb{Z}$, order in $\mathbb{Q}(\sqrt{-d})$, order in $\mathcal{B}_{p,\infty}$	Same over the function field $\mathbb{F}_q(T)$

Applications to class field theory.

Drinfeld modules!

What are elliptic curves for $R = \mathbb{F}_q[T]$?

Module structure	
$\mathbb{Z}$-module	$\mathbb{F}_q[T]$-module
Torsion	
$(\mathbb{Z}/n\mathbb{Z})^2$, $p \nmid n$	$(\mathbb{F}_q[T]/a\mathbb{F}_q[T])^2$, $\mathfrak{p} \nmid a$
Endomorphism ring	
$\mathbb{Z}$, order in $\mathbb{Q}(\sqrt{-d})$, order in $\mathcal{B}_{p,\infty}$	Same over the function field $\mathbb{F}_q(T)$

Applications to class field theory.

Drinfeld modules!

What are elliptic curves for $R = \mathbb{F}_q[T]$?

Module structure	
$\mathbb{Z}$-module	$\mathbb{F}_q[T]$-module
Torsion	
$(\mathbb{Z}/n\mathbb{Z})^2$, $p \nmid n$	$(\mathbb{F}_q[T]/a\mathbb{F}_q[T])^2$, $\mathfrak{p} \nmid a$
Endomorphism ring	
$\mathbb{Z}$, order in $\mathbb{Q}(\sqrt{-d})$, order in $\mathcal{B}_{p,\infty}$	Same over the function field $\mathbb{F}_q(T)$

Applications to class field theory.

Drinfeld modules!

The rules of point counting

Philosophy of Drinfeld modules

Representation of Drinfeld modules

Point counting without points

Cost of the algorithms

Analogies

$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((\frac{1}{T}))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Elliptic curves	Drinfeld modules

Mantra

Our integers are polynomials.

Analogies

$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((\frac{1}{T}))$
$\mathbb{C}$	$\mathbb{C}_\infty$ = completion of $\overline{\mathbb{R}_\infty}$
Elliptic curves	Drinfeld modules

Mantra

Our integers are polynomials.

Analogies

$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((\frac{1}{T}))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Elliptic curves	Drinfeld modules

Mantra

Our integers are polynomials.

Analogies

$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((\frac{1}{T}))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Elliptic curves	Drinfeld modules

Mantra

Our integers are polynomials.

Analogies

$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((\frac{1}{T}))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Elliptic curves	Drinfeld modules

Mantra

Our integers are polynomials.

Applications of Drinfeld modules

Function field arithmetics

- Explicit class field theory and theory of complex multiplication.
- Geometric Langlands program.
- Others: exponential and logarithm functions, Drinfeld modular forms, etc.

Computer algebra

State-of-the art factorization in $\mathbb{F}_q[T]$ (Doliskani-Narayanan-Schost, 2021).

Cryptography

Drinfeld module analogues of standard elliptic curve schemes: ☠️ ($\mathbb{F}_q$-linearity).

Highlights both similarities and fundamental differences with elliptic curves.

Applications of Drinfeld modules

Function field arithmetics

- Explicit class field theory and theory of complex multiplication.
- Geometric Langlands program.
- Others: exponential and logarithm functions, Drinfeld modular forms, etc.

Computer algebra

State-of-the art factorization in $\mathbb{F}_q[T]$ (Doliskani-Narayanan-Schost, 2021).

Cryptography

Drinfeld module analogues of standard elliptic curve schemes: ☠ ($\mathbb{F}_q$-linearity).

Highlights both similarities and fundamental differences with elliptic curves.

Applications of Drinfeld modules

Function field arithmetics

- Explicit class field theory and theory of complex multiplication.
- Geometric Langlands program.
- Others: exponential and logarithm functions, Drinfeld modular forms, etc.

Computer algebra

State-of-the art factorization in $\mathbb{F}_q[T]$ (Doliskani-Narayanan-Schost, 2021).

Cryptography

Drinfeld module analogues of standard elliptic curve schemes: ☠️ ($\mathbb{F}_q$-linearity).

Highlights both similarities and fundamental differences with elliptic curves.

Broader questions

Elliptic curves	*vs*	Drinfeld modules
Integers	*vs*	Polynomials
Number fields	*vs*	Function fields
Zero characteristic	*vs*	Positive characteristic

Ore polynomials

Fix $K/\mathbb{F}_q$, and

$$\begin{array}{rccc} \tau^n: & \overline{K} & \to & \overline{K} \\ & x & \mapsto & x^{q^n}. \end{array}$$

Definition of $K\{\tau\}$

Finite K-linear combinations of τ^n'; ring for addition and composition.

Properties

- Representation as polynomials: $K\{\tau\} = \{\sum_{i=0}^n x_i \tau^i, n \in \mathbb{Z}_{\geqslant 0}, x_i \in K\}$.
- Notion of τ-degree.
- Noncommutative: for $\lambda \in K$, $\tau^n \lambda = \lambda^{q^n} \tau^n$.
- Left-euclidean: for any $A, B \in K\{\tau\}$, there exist $Q, R \in K\{\tau\}$ such that:

$$A = QB + R, \quad \deg_\tau(R) < \deg_\tau(B).$$

Ore polynomials

Fix $K/\mathbb{F}_q$, and

$$\begin{array}{rccc} \tau^n : & \overline{K} & \to & \overline{K} \\ & x & \mapsto & x^{q^n}. \end{array}$$

Definition of $K\{\tau\}$

Finite K-linear combinations of τ^n'; ring for addition and composition.

Properties

- Representation as polynomials: $K\{\tau\} = \{\sum_{i=0}^{n} x_i \tau^i, n \in \mathbb{Z}_{\geqslant 0}, x_i \in K\}$.
- Notion of τ-degree.
- Noncommutative: for $\lambda \in K$, $\tau^n \lambda = \lambda^{q^n} \tau^n$.
- Left-euclidean: for any $A, B \in K\{\tau\}$, there exist $Q, R \in K\{\tau\}$ such that:

$$A = QB + R, \quad \deg_\tau(R) < \deg_\tau(B).$$

Ore polynomials

Fix $K/\mathbb{F}_q$, and

$$\begin{array}{rccc} \tau^n: & \overline{K} & \to & \overline{K} \\ & x & \mapsto & x^{q^n}. \end{array}$$

Definition of $K\{\tau\}$

Finite K-linear combinations of τ^n'; ring for addition and composition.

Properties

- Representation as polynomials: $K\{\tau\} = \{\sum_{i=0}^{n} x_i \tau^i, n \in \mathbb{Z}_{\geqslant 0}, x_i \in K\}$.
- Notion of τ-degree.
- Noncommutative: for $\lambda \in K$, $\tau^n \lambda = \lambda^{q^n} \tau^n$.
- Left-euclidean: for any $A, B \in K\{\tau\}$, there exist $Q, R \in K\{\tau\}$ such that:

$$A = QB + R, \quad \deg_\tau(R) < \deg_\tau(B).$$

Ore polynomials

Fix $K/\mathbb{F}_q$, and

$$\begin{array}{rccc} \tau^n : & \overline{K} & \to & \overline{K} \\ & x & \mapsto & x^{q^n}. \end{array}$$

Definition of $K\{\tau\}$

Finite K-linear combinations of τ^n'; ring for addition and composition.

Properties

- Representation as polynomials: $K\{\tau\} = \{\sum_{i=0}^n x_i \tau^i, n \in \mathbb{Z}_{\geqslant 0}, x_i \in K\}$.
- Notion of τ-degree.
- Noncommutative: for $\lambda \in K$, $\tau^n \lambda = \lambda^{q^n} \tau^n$.
- Left-euclidean: for any $A, B \in K\{\tau\}$, there exist $Q, R \in K\{\tau\}$ such that:

$$A = QB + R, \quad \deg_\tau(R) < \deg_\tau(B).$$

Ore polynomials

Fix $K/\mathbb{F}_q$, and

$$\begin{array}{rccc} \tau^n: & \overline{K} & \to & \overline{K} \\ & x & \mapsto & x^{q^n}. \end{array}$$

Definition of $K\{\tau\}$

Finite K-linear combinations of τ^n'; ring for addition and composition.

Properties

- Representation as polynomials: $K\{\tau\} = \{\sum_{i=0}^n x_i \tau^i, n \in \mathbb{Z}_{\geqslant 0}, x_i \in K\}$.
- Notion of τ-degree.
- Noncommutative: for $\lambda \in K$, $\tau^n \lambda = \lambda^{q^n} \tau^n$.
- Left-euclidean: for any $A, B \in K\{\tau\}$, there exist $Q, R \in K\{\tau\}$ such that:

$$A = QB + R, \quad \deg_\tau(R) < \deg_\tau(B).$$

Representing Drinfeld modules

(Almost) Definition (Drinfeld, 1977)

A *Drinfeld* $\mathbb{F}_q[T]$*-module over* K is a morphism of $\mathbb{F}_q[T]$-algebras

$$\begin{array}{rccc} \phi: & \mathbb{F}_q[T] & \to & K\{\tau\} \\ & a & \mapsto & \phi_a. \end{array}$$

Representation

ϕ is represented by ϕ_T. The *rank* of ϕ is $\deg_\tau(\phi_T)$.

Morphisms

A *morphism* $u : \phi \to \psi$ is an Ore polynomial $u \in K\{\tau\}$ such that

$$\forall a \in \mathbb{F}_q[T], \qquad u\phi_a = \psi_a u.$$

Representing Drinfeld modules

(Almost) Definition (Drinfeld, 1977)

A *Drinfeld* $\mathbb{F}_q[T]$*-module over* K is a morphism of $\mathbb{F}_q[T]$-algebras

$$\begin{array}{rccc} \phi: & \mathbb{F}_q[T] & \to & K\{\tau\} \\ & a & \mapsto & \phi_a. \end{array}$$

Representation

ϕ is represented by ϕ_T. The *rank* of ϕ is $\deg_\tau(\phi_T)$.

Morphisms

A *morphism* $u : \phi \to \psi$ is an Ore polynomial $u \in K\{\tau\}$ such that

$$\forall a \in \mathbb{F}_q[T], \qquad u\phi_a = \psi_a u.$$

Representing Drinfeld modules

(Almost) Definition (Drinfeld, 1977)

A *Drinfeld* $\mathbb{F}_q[T]$*-module over* K is a morphism of $\mathbb{F}_q[T]$-algebras

$$\begin{array}{rccc} \phi : & \mathbb{F}_q[T] & \to & K\{\tau\} \\ & a & \mapsto & \phi_a. \end{array}$$

Representation

ϕ is represented by ϕ_T. The *rank* of ϕ is $\deg_\tau(\phi_T)$.

Morphisms

A *morphism* $u : \phi \to \psi$ is an Ore polynomial $u \in K\{\tau\}$ such that

$$\forall a \in \mathbb{F}_q[T], \qquad u\phi_a = \psi_a u.$$

The points of a Drinfeld module

For an elliptic curve, the *points* form a $\mathbb{Z}$-module.

Geometric points

ϕ acts on $\overline{K}$ *via*

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (a, z) & \mapsto & \phi_a(z). \end{array}$$

$\mathbb{F}_q[T]$-module denoted by $\phi(\overline{K})$.

K-rational points

Write

$$\phi(K) := \phi(\overline{K}) \cap K.$$

The underlying set of $\phi(K)$ is always K.

The points of a Drinfeld module

For an elliptic curve, the *points* form a $\mathbb{Z}$-module.

Geometric points

ϕ acts on $\overline{K}$ *via*

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (a, z) & \mapsto & \phi_a(z). \end{array}$$

$\mathbb{F}_q[T]$-module denoted by $\phi(\overline{K})$.

K-rational points

Write

$$\phi(K) := \phi(\overline{K}) \cap K.$$

The underlying set of $\phi(K)$ is always K.

The points of a Drinfeld module

For an elliptic curve, the *points* form a $\mathbb{Z}$-module.

Geometric points

ϕ acts on $\overline{K}$ *via*

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (a, z) & \mapsto & \phi_a(z). \end{array}$$

$\mathbb{F}_q[T]$-module denoted by $\phi(\overline{K})$.

K-rational points

Write

$$\phi(K) := \phi(\overline{K}) \cap K.$$

The underlying set of $\phi(K)$ is always K.

The points of a Drinfeld module

For an elliptic curve, the *points* form a $\mathbb{Z}$-module.

Geometric points

ϕ acts on $\overline{K}$ *via*

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (a, z) & \mapsto & \phi_a(z). \end{array}$$

$\mathbb{F}_q[T]$-module denoted by $\phi(\overline{K})$.

K-rational points

Write

$$\phi(K) := \phi(\overline{K}) \cap K.$$

The underlying set of $\phi(K)$ is always K.

The number of points

For an elliptic curve,

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_n),$$

and

$$(\#E(\mathbb{F}_q)) \simeq (d_1 \cdots d_n)$$

Assume K is finite. Decompose

$$\phi(K) \simeq \mathbb{F}_q[T]/(d_1) \times \cdots \times \mathbb{F}_q[T]/(d_n).$$

The "number of K-rational points of ϕ" ($\mathbb{F}_q[T]$-cardinality) is

$$(|\phi(K)|) = (d_1 \cdots d_n).$$

Often referred to as the *Euler-Poincaré characteristic* or *Fitting ideal* of $\phi(K)$.

The number of points

For an elliptic curve,

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_n),$$

and

$$(\#E(\mathbb{F}_q)) \simeq (d_1 \cdots d_n)$$

Assume K is finite. Decompose

$$\phi(K) \simeq \mathbb{F}_q[T]/(d_1) \times \cdots \times \mathbb{F}_q[T]/(d_n).$$

The "number of K-rational points of ϕ" ($\mathbb{F}_q[T]$-cardinality) is

$$(|\phi(K)|) = (d_1 \cdots d_n).$$

Often referred to as the *Euler-Poincaré characteristic* or *Fitting ideal* of $\phi(K)$.

The elliptic curve case

First deterministic polynomial time: Schoof, 1985.

Number of points *via* the Frobenius endomorphism

1. An elliptic curve $E/\mathbb{F}_q$ has a *Frobenius endomorphism* $\pi : (x, y) \mapsto (x^q, y^q)$.
2. π has a *characteristic polynomial*

$$\chi = X^2 - tX + q \in \mathbb{Z}[X]$$

   such that

$$\chi(\pi) = \pi^2 - t\pi + q = 0.$$

3. We have

$$|E(\mathbb{F}_q)| = \chi(1).$$

Important invariant.

The elliptic curve case

First deterministic polynomial time: Schoof, 1985.

Number of points *via* the Frobenius endomorphism

1. An elliptic curve $E/\mathbb{F}_q$ has a *Frobenius endomorphism* $\pi : (x, y) \mapsto (x^q, y^q)$.
2. π has a *characteristic polynomial*
$$\chi = X^2 - tX + q \in \mathbb{Z}[X]$$
such that
$$\chi(\pi) = \pi^2 - t\pi + q = 0.$$
3. We have
$$|E(\mathbb{F}_q)| = \chi(1).$$

Important invariant.

The elliptic curve case

First deterministic polynomial time: Schoof, 1985.

Number of points *via* the Frobenius endomorphism

1. An elliptic curve $E/\mathbb{F}_q$ has a *Frobenius endomorphism* $\pi : (x, y) \mapsto (x^q, y^q)$.
2. π has a *characteristic polynomial*

$$\chi = X^2 - tX + q \in \mathbb{Z}[X]$$

   such that

$$\chi(\pi) = \pi^2 - t\pi + q = 0.$$

3. We have

$$|E(\mathbb{F}_q)| = \chi(1).$$

Important invariant.

The elliptic curve case

First deterministic polynomial time: Schoof, 1985.

Number of points *via* the Frobenius endomorphism

1. An elliptic curve $E/\mathbb{F}_q$ has a *Frobenius endomorphism* $\pi : (x, y) \mapsto (x^q, y^q)$.
2. π has a *characteristic polynomial*

$$\chi = X^2 - tX + q \in \mathbb{Z}[X]$$

   such that

$$\chi(\pi) = \pi^2 - t\pi + q = 0.$$

3. We have

$$|E(\mathbb{F}_q)| = \chi(1).$$

Important invariant.

The elliptic curve case

First deterministic polynomial time: Schoof, 1985.

Number of points *via* the Frobenius endomorphism

1. An elliptic curve $E/\mathbb{F}_q$ has a *Frobenius endomorphism* $\pi : (x, y) \mapsto (x^q, y^q)$.
2. π has a *characteristic polynomial*

$$\chi = X^2 - tX + q \in \mathbb{Z}[X]$$

   such that

$$\chi(\pi) = \pi^2 - t\pi + q = 0.$$

3. We have

$$|E(\mathbb{F}_q)| = \chi(1).$$

Important invariant.

The Drinfeld module case

1. Assume K is finite. A Drinfeld module ϕ over K has a *Frobenius endomorphism* $\pi = \tau^{[K:\mathbb{F}_q]} \in K\{\tau\}$.
2. π has a *characteristic polynomial*

$$\chi = X^r + a_{r-1}(T)X^{r-1} + \cdots + a_1(T)X + a_0(T) \in \mathbb{F}_q[T][X]$$

   such that

$$\chi(\pi) = \pi^r + \phi_{a_{r-1}}\pi^{r-1} + \cdots + \phi_{a_1}\pi + \phi_{a_0} = 0.$$

3. We have (Gekeler, 1991)

$$(|\phi(K)|) = (\chi(1))$$

Important invariant.

The Drinfeld module case

1. Assume K is finite. A Drinfeld module ϕ over K has a *Frobenius endomorphism* $\pi = \tau^{[K:\mathbb{F}_q]} \in K\{\tau\}$.
2. π has a *characteristic polynomial*

$$\chi = X^r + a_{r-1}(T)X^{r-1} + \cdots + a_1(T)X + a_0(T) \in \mathbb{F}_q[T][X]$$

   such that

$$\chi(\pi) = \pi^r + \phi_{a_{r-1}}\pi^{r-1} + \cdots + \phi_{a_1}\pi + \phi_{a_0} = 0.$$

3. We have (Gekeler, 1991)

$$(|\phi(K)|) = (\chi(1))$$

Important invariant.

The Drinfeld module case

1. Assume K is finite. A Drinfeld module ϕ over K has a *Frobenius endomorphism* $\pi = \tau^{[K:\mathbb{F}_q]} \in K\{\tau\}$.
2. π has a *characteristic polynomial*

$$\chi = X^r + a_{r-1}(T)X^{r-1} + \cdots + a_1(T)X + a_0(T) \in \mathbb{F}_q[T][X]$$

   such that

$$\chi(\pi) = \pi^r + \phi_{a_{r-1}}\pi^{r-1} + \cdots + \phi_{a_1}\pi + \phi_{a_0} = 0.$$

3. We have (Gekeler, 1991)

$$(|\phi(K)|) = (\chi(1))$$

Important invariant.

The Drinfeld module case

1. Assume K is finite. A Drinfeld module ϕ over K has a *Frobenius endomorphism* $\pi = \tau^{[K:\mathbb{F}_q]} \in K\{\tau\}$.
2. π has a *characteristic polynomial*

$$\chi = X^r + a_{r-1}(T)X^{r-1} + \cdots + a_1(T)X + a_0(T) \in \mathbb{F}_q[T][X]$$

   such that

$$\chi(\pi) = \pi^r + \phi_{a_{r-1}}\pi^{r-1} + \cdots + \phi_{a_1}\pi + \phi_{a_0} = 0.$$

3. We have (Gekeler, 1991)

$$(|\phi(K)|) = (\chi(1))$$

Important invariant.

Abstract definition of χ

Via *Tate modules*

1. Make $\mathbb{F}_q[T]$ act on $\overline{K}$ *via* ϕ.
2. Consider the action of π on (almost all) the ℓ-torsion submodules, $\ell \in \mathbb{F}_q[T]$.
3. Show that these are free with rank r on $\mathbb{F}_q[T]/(\ell)$.
4. Show that the characteristic polynomial of the action of π on these modules lifts to a single polynomial $\chi \in \mathbb{F}_q[T][X]$.

Problem

Manipulate torsion elements in possibly large extensions.

Anderson motives

Definition

$\mathbb{M}(\phi)$ is the $K[T]$-module

$$\begin{array}{rcl} K[T] \times K\{\tau\} & \to & K\{\tau\} \\ \left(\sum_i \lambda_i T^i, f(\tau)\right) & \mapsto & \sum_i \lambda_i f(\tau) \phi_T^i \end{array}$$

Canonical basis

$\mathbb{M}(\phi)$ is free with rank r (the rank of ϕ) with basis

$$(1, \tau, \ldots, \tau^{r-1}).$$

Recursive process *via* Ore Euclidean division:

$$f(\tau) = Q(\tau)\phi_T + R(\tau), \quad \deg_\tau(R) < r.$$

Anderson motives

Definition

$\mathbb{M}(\phi)$ is the $K[T]$-module

$$\begin{array}{rcl} K[T] \times K\{\tau\} & \to & K\{\tau\} \\ \left(\sum_i \lambda_i T^i, f(\tau)\right) & \mapsto & \sum_i \lambda_i f(\tau) \phi_T^i \end{array}$$

Canonical basis

$\mathbb{M}(\phi)$ is free with rank r (the rank of ϕ) with basis

$$(1, \tau, \ldots, \tau^{r-1}).$$

Recursive process *via* Ore Euclidean division:

$$f(\tau) = Q(\tau)\phi_T + R(\tau), \quad \deg_\tau(R) < r.$$

Anderson motives

Definition

$\mathbb{M}(\phi)$ is the $K[T]$-module

$$\begin{array}{rcl} K[T] \times K\{\tau\} & \to & K\{\tau\} \\ \left(\sum_i \lambda_i T^i, f(\tau)\right) & \mapsto & \sum_i \lambda_i f(\tau) \phi_T^i \end{array}$$

Canonical basis

$\mathbb{M}(\phi)$ is free with rank r (the rank of ϕ) with basis

$$(1, \tau, \ldots, \tau^{r-1}).$$

Recursive process *via* Ore Euclidean division:

$$f(\tau) = Q(\tau)\phi_T + R(\tau), \quad \deg_\tau(R) < r.$$

Morphisms as matrices

Any morphisms $u : \phi \to \psi$ gives a morphism on the Anderson motives

$$\begin{array}{rccc} \mathbb{M}(u): & \mathbb{M}(\psi) & \to & \mathbb{M}(\phi) \\ & f & \mapsto & fu. \end{array}$$

Effective computation

To compute the matrix of $\mathbb{M}(u)$, compute the coordinates of

$$u, \tau u, \cdots, \tau^{r-1} u.$$

Morphisms as matrices

Any morphisms $u : \phi \to \psi$ gives a morphism on the Anderson motives

$$\begin{array}{rccc} \mathbb{M}(u): & \mathbb{M}(\psi) & \to & \mathbb{M}(\phi) \\ & f & \mapsto & fu. \end{array}$$

Effective computation

To compute the matrix of $\mathbb{M}(u)$, compute the coordinates of

$$u, \tau u, \cdots, \tau^{r-1} u.$$

Example

Pick

$$\begin{cases} \mathbb{F}_q = \mathbb{F}_7 \\ K = \mathbb{F}_q[x]/(x^2 + 6x + 3) \simeq \mathbb{F}_{7^2} \\ \phi_T = z + \tau + z\tau^2 \end{cases}$$

The action of τ^2 on $\mathbb{M}(\phi)$ is given by:

$$\begin{pmatrix} (5 + 2z)T - 1 & 2 + 5z \\ 2T + 5z & 5zT + 4 \end{pmatrix}.$$

The characteristic polynomial is:

$$X^2 + (2T + 4)X + 5T^2 + 2T + 1.$$

Verify:

$$(\tau^2)^2 + (2\phi_T + 4)\tau^2 + 5\phi_T^2 + 2\phi_T + 1 = 0.$$

The rules of point counting

Philosophy of Drinfeld modules

Representation of Drinfeld modules

Point counting without points

Cost of the algorithms

Our contribution

Everything is joint work with Xavier Caruso.

Caruso, L., 2023

- Any endomorphism.
- Any r.
- Any K.
- Extends to isogeny norms.
- Any function ring.
- SageMath implementation in the standard library.

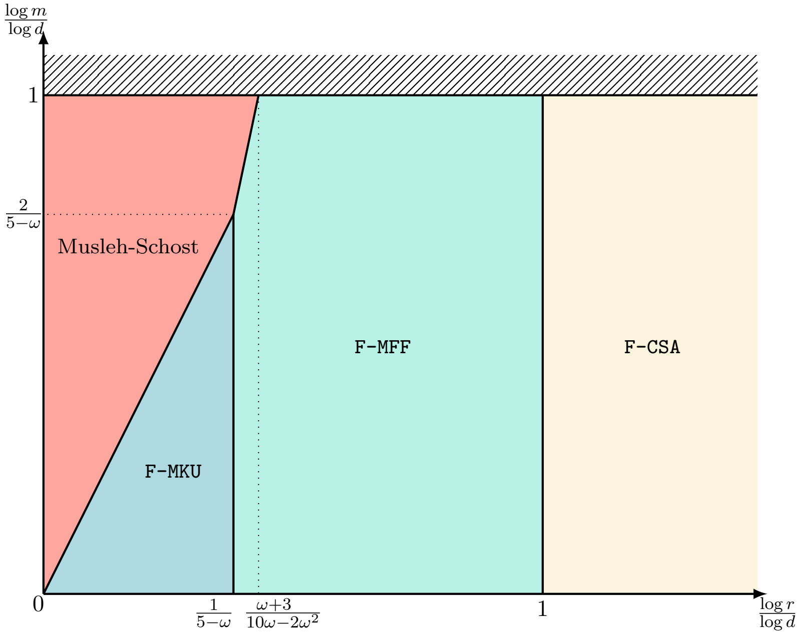
2008	Gekeler	Frobenius, $r = 2$ generalized to $r \in \mathbb{Z}_{\geqslant 0}$ by Musleh
2019	Musleh, Schost	Frobenius, $r = 2$
2020	Garai, Papikian	Frobenius, $r = 2$
2023	Musleh, Schost	Any endomorphism, any r
2024	Musleh	Any endomorphism, any r

For the Frobenius characteristic polynomial

Las Vegas algorithm, cost in bit operations:

- [`F-MFF`] $O\tilde{}(d \log^2 q) + (\mathrm{SM}^{\geqslant 1}(d, d) + d^2 r + d r^\omega) \log q)^{1+o(1)}$,
- [`F-MKU`] $O\tilde{}(d \log^2 q) + ((d^2 r^{\omega-1} + d r^\omega) \log q)^{1+o(1)}$,
- [`F-CSA`] $O\tilde{}(d \log^2 q) + (r d^\omega \log q)^{1+o(1)}$.

d	$=$	$[K : \mathbb{F}_q]$
r	$=$	rank of ϕ
ω	$=$	feasible exponent for matrix multiplication in a field
$\mathrm{SM}^{\geqslant 1}$	$=$	related to fast multiplication of Ore polynomials [Caruso-Le Borgne, 2017]


$\frac{\log m}{\log d}$
1
$\frac{2}{5-\omega}$
Musleh-Schost
F-MKU
F-MFF
F-CSA
0
$\frac{1}{5-\omega}$
$\frac{\omega+3}{10\omega-2\omega^2}$
1
$\frac{\log r}{\log d}$

For general endomorphisms

Deterministic algorithm:

- ◦ $O\tilde{}(n^2 + (n+r)r^{\Omega-1})$ operations in K
  - ◦ $O(n^2 + r^2)$ q-exponentiations in K

If K is finite, Las Vegas algorithm (cost in binary operations):

- $O\tilde{}(d \log^2 q) + ((\mathrm{SM}^{\geqslant 1}(n,d) + ndr + (n+d)r^{\omega}) \log q)^{1+o(1)}$.

n	$=$	τ-degree of the endomorphism
d	$=$	$[K : \mathbb{F}_q]$
r	$=$	rank of ϕ
ω	$=$	feasible exponent for matrix multiplication in a field
Ω	$=$	feasible exponent for characteristic polynomial computation in a field
$\mathrm{SM}^{\geqslant 1}$	$=$	related to fast multiplication of Ore polynomials [Caruso-Le Borgne, 2017]

For isogeny norms

Deterministic algorithm:

- ◦ $O\tilde{}(n^2 + nr^{\omega-1} + r^\omega)$ operations in K
  - ◦ $O(n^2 + r^2)$ q-exponentiations in K

If K is finite, Las Vegas algorithm (cost in bit operations):

- $O\tilde{}(d \log^2 q) + ((\mathrm{SM}^{\geqslant 1}(n, d) + ndr + n \min(d, r) r^{\omega-1} + dr^\omega) \log q)^{1+o(1)}$.

n	$=$	τ-degree of the isogeny
d	$=$	$[K : \mathbb{F}_q]$
r	$=$	rank of ϕ
ω	$=$	feasible exponent for matrix multiplication in a field
Ω	$=$	feasible exponent for characteristic polynomial computation in a field
$\mathrm{SM}^{\geqslant 1}$	$=$	related to fast multiplication of Ore polynomials [Caruso-Le Borgne, 2017]