From elliptic curves to Drinfeld modules

Antoine Leudière

University of Calgary

INRIA Grace seminar

December 2nd 2025

Today

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

How **effective** are Drinfeld modules? **Counting points** using Anderson motives.

Potential **applications**.

Joint work with Xavier Caruso.
Algorithms for computing norms and characteristic polynomials on general Drinfeld modules. Mathematics of Computation. 2026.

The rules of point counting

A new area

Representing Drinfeld modules

Point counting without points

The rules of point counting

A new area

Representing Drinfeld modules

Point counting without points

What is point counting?

Naively

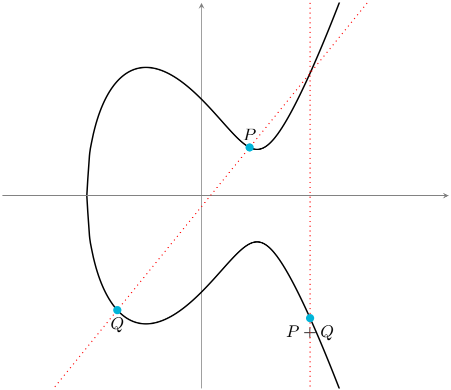
Counting solutions to an equation.

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 geometric objects with more structure: *elliptic curves*.

Elliptic curves



Smooth algebraic projective curves of genus 1 with a distinguished point.

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 over $\mathbb{F}_q$. 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

$$m_1 \cdots m_\ell.$$

Drinfeld modules!

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

Both Euclidean domains.

Analogies

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

Mantra

Our integers are polynomials.

The rules of point counting

A new area

Representing Drinfeld modules

Point counting without points

From elliptic curves to Drinfeld modules

	Elliptic curves	Drinfeld modules
Introduction	1850-1900	1977
Practical applications	1980s	2021

Drinfeld modules were introduced (and were successful) for:

- Class field theory (Kronecker-Weber, complex multiplication).
- Langlands conjectures for function fields (GL_2 then GL_r).

Research on algorithmics of Drinfeld modules is a very new area!

Our goal

- Modern techniques for manipulating Drinfeld modules.
- Efficiency and generality (rank and function fields).
- Applications (coding theory, computer algebra).

Timeline

- Early works on computational aspects: 1980s (Gekeler, Bae & Koo, etc).
- First thesis on the computational aspects: 2018 (Caranay).
- First computer algebra application: 2021 (Doliskani, Narayanan, Schost).
- First high generality algorithms: 2023 (Musleh & Schost, Caruso & Leudière).

My research

- Computer algebra of Drinfeld modules (Caruso-L. 2023, L. 2026).
- SageMath implementation (Ayotte-Caruso-L.-Musleh 2023).
- Algorithmics of function fields (L.-Spaenlehauer, 2023).
- (Small cyclotomic integers (Bajpai, Das, Kedlaya, Le, L. Lee, Mello, 2025).)

The rules of point counting

A new area

Representing Drinfeld modules

Point counting without points

Ore polynomials

Fix $K/\mathbb{F}_q$, and for all $n \in \mathbb{Z}_{\geqslant 0}$:

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

Definition (Ore polynomials)

$K\{\tau\}$ = 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 homomorphism of $\mathbb{F}_q$-algebras

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

Morphisms

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

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

An *isogeny* is a nonzero morphism.

The rank of a Drinfeld module

Definition (rank)

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

Elliptic curves correspond to rank 2 only! (Lattices in $\mathbb{C}$ vs $\mathbb{C}_\infty$.)

Point counting state of the art

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
2023	**Caruso, L.**	Any endomorphism, any r, field, function field + isogeny norms

The points of a Drinfeld module

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

Geometric points

The $\mathbb{F}_q[T]$-*module of points*, denoted by $\phi(\overline{K})$, is given by:

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

K-rational points

The $\mathbb{F}_q[T]$-*module of K-rational points* is

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

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 rules of point counting

A new area

Representing Drinfeld modules

Point counting without points

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* $F : (x, y) \mapsto (x^q, y^q)$.
2. F has a *characteristic polynomial*

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

   such that

$$\chi(F) = F^2 - tF + q = 0.$$

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* $F = \tau^{[K:\mathbb{F}_q]} \in K\{\tau\}$.
2. F 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

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

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 F 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 F on these modules lifts to a single polynomial $\chi \in \mathbb{F}_q[T][X]$.

Problem

- Manipulate torsion elements in possibly large extensions.
- Or derive an efficient theory of *division polynomials*.

Anderson motives

Definition (Anderson motive of ϕ)

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

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

Canonical basis

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

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

Explicit decomposition in the canonical basis

Ore Euclidean division and recursion:

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

Morphisms as matrices

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

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

Effective computation

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

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

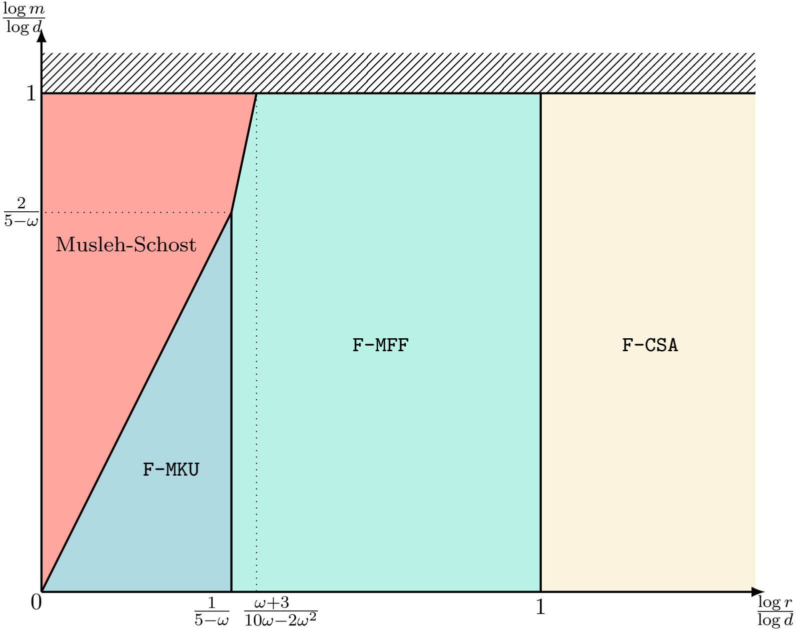
Norms and characteristic polynomials

Let $u : \phi \to \psi$ be an isogeny of Drinfeld modules.
Consider $\mathbb{M}(u) : \mathbb{M}(\psi) \to \mathbb{M}(\phi)$ as a matrix in the canonical bases.

- If u is an endomorphism, its characteristic polynomial is that of $\mathbb{M}(u)$.
- The *norm* of u is $\det(\mathbb{M}(u))$.

Our work

- Prove it (for any function ring, field, rank, isogeny).
- Multiple variants, optimization, analysis.
- Implementation.
- (An extra algorithm, only for the Frobenius, based on reduced norms.)



$\frac{\log m}{\log d}$
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
$\frac{\log r}{\log d}$

Conclusion

Problems inspired from elliptic curves.
New solutions (efficiency, generality).

Potential of Drinfeld modules

- Reveal differences between number fields and function fields.
- Computer algebra of polynomials.
- Coding theory:
  - Drinfeld modular curve (asymptotically good towers of curves).
  - Function Field Decoding Problem (Bombar, Couvreur & Debris-Alazard).
  - Rank-metric, locally recoverable codes (Bastioni, Darwish & Micheli).