

Point counting on Drinfeld modules

Antoine Leudière

University of Calgary

Ouragan seminar, July 8th 2025

From integers to Drinfeld modules

Drinfeld modules

Point counting

From integers to Drinfeld modules

Drinfeld modules

Point counting

Two general problems

Hilbert's tenth problem

Given a Diophantine equations, can one tell if it has integer solutions?

Matiyasevich's theorem (1970): no algorithm can do that.

Integer linear programming

Find a vector $x \in \mathbb{Z}^n$ that maximizes

$$\langle c, x \rangle, \quad c \in \mathbb{Z}^n,$$

under the constraints

$$\begin{cases} Ax \leq b, & A \in \mathbb{Z}^{m \times n}, \quad b \in \mathbb{Z}^m, \\ x \geq 0. \end{cases}$$

Integer linear programming is NP-complete.

Elliptic curves

No hope of solving general problems: consider geometrical problems.

Elliptic curves

Projective curve given by $y^2z = x^3 + axz^2 + bz^3$, with a, b verifying $4a^3 + 27b^2 \neq 0$.

1. Geometrical structure.
2. Arithmetic structure (abelian group, *i.e.* \mathbb{Z} -module).

Applications of elliptic curves

- Fermat-Wiles.
- abc and BSD conjectures.
- In computer algebra: ECPP (primality testing), ECM (integer factorization).
- In cryptography: ECDH (pre-quantum key exchange), SQIsign family (post-quantum key exchange).

General philosophy

1. Elliptic curves/roots of unity: characteristic 0 and number fields.
2. Drinfeld modules: characteristic p and function fields.

Two examples from *class field theory*

- Kronecker-Weber-Hilbert: every abelian number field lies in a cyclotomic field (*i.e.* extension of \mathbb{Q} generated by roots of unity).
- The *Hilbert class field* (maximal unramified abelian extension) of an imaginary quadratic number field $\mathbb{Q}(\sqrt{-d})$ is generated by the j -invariants of elliptic curves with complex multiplication in $\mathbb{Q}(\sqrt{-d})$.

Analogies

Zero characteristic	Positive characteristic
\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}	$\mathbb{C}_\infty = \text{completion of } \overline{\mathbb{R}_\infty}$
Roots of unity	Drinfeld modules
Elliptic curves	Drinfeld modules

Mantra

Our integers are polynomials.

The benefits of positive characteristic

- Unconditional results (*e.g.* GRH).
- Faster algorithms (*e.g.* factorization).
- Geometrical structure properties of function fields.
- \mathbb{F}_q -linearity.
- Non-Archimedean analysis.

Applications of Drinfeld modules

Function field arithmetics

- Explicit class field theory and theory of complex multiplication.
- Geometric Langlands program.
- Exponential and logarithm functions.
- Drinfeld modular forms.

Computer algebra

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

Cryptography

Drinfeld module analogues of standard elliptic curve schemes fail, because of \mathbb{F}_q -linear structures.

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

From integers to Drinfeld modules

Drinfeld modules

Point counting

Ore polynomials

Fix K/\mathbb{F}_q , and

$$\begin{aligned}\tau^n : \overline{K} &\rightarrow \overline{K} \\ x &\mapsto x^{q^n}.\end{aligned}$$

Definition of $K\{\tau\}$

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

Properties

- Representation as polynomials: $K\{\tau\} = \{\sum_{i=0}^n x_i \tau^i, n \in \mathbb{Z}_{\geq 0}, x_i \in K\}$.
- 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

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

Representation

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

Morphisms

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

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

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

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

$\mathbb{F}_q[T]$ -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 ” is

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

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

From integers to Drinfeld modules

Drinfeld modules

Point counting

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.

Abstract definition of π

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

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

Canonical basis

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

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

Recursive process *via* Ore Euclidean division:

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

Morphisms as matrices

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

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

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

$$f, \tau f, \dots, \tau^{r-1} f.$$

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:

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

Verify:

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

Our contribution

Caruso, L., 2023

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

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

Cost of computing χ

Las Vegas algorithm, cost in bit operations:

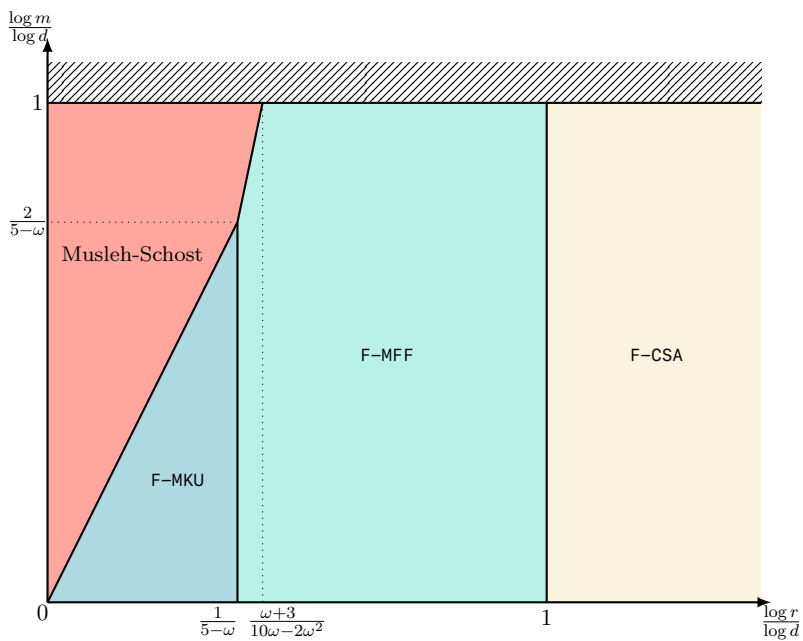
- [F-MFF] $O^{\sim}(d \log^2 q) + (\text{SM}^{\geq 1}(d, d) + d^2 r + d r^{\omega}) \log q)^{1+o(1)},$
- [F-MKU] $O^{\sim}(d \log^2 q) + ((d^2 r^{\omega-1} + d r^{\omega}) \log q)^{1+o(1)},$
- [F-CSA] $O^{\sim}(d \log^2 q) + (r d^{\omega} \log q)^{1+o(1)}.$

d = $[K : \mathbb{F}_q]$

r = rank of ϕ

ω = feasible exponent for matrix multiplication in a field

$\text{SM}^{\geq 1}$ = related to fast multiplication of Ore polynomials [Caruso-Le Borgne, 2017]



For general endomorphisms

Deterministic algorithm:

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

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

- $O^\sim(d \log^2 q) + ((\text{SM}^{\geq 1}(n, d) + ndr + (n + d)r^\omega) \log q)^{1+o(1)}.$

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

$\text{SM}^{\geq 1}$ = related to fast multiplication of Ore polynomials [Caruso-Le Borgne, 2017]

For isogeny norms

Deterministic algorithm:

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

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

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

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

$\text{SM}^{\geq 1}$ = related to fast multiplication of Ore polynomials [Caruso-Le Borgne, 2017]