Arithmetic geometry as a toolbox for computer algebra

Part II - 06/03/2026

Pierre-Jean Spaenlehauer

Inria Nancy

JNCF 2026

Yesterday

Elliptic curves over finite fields.

Deterministic root-finding.

Slogan: elliptic curves make every prime special.

Today

Complex multiplication.

More arithmetico-geometric approaches to deterministic polynomial root-finding.

Isogenies.

Elliptic curve FFT.

Drinfeld modules and polynomial factorization.

Elliptic curves, group law, division polynomials

Elliptic curves over $\mathbb{F}_q$

Defined by **equations** of the form $Y^2 = X^3 + aX + b$, with $a, b \in \mathbb{F}_q$.

Abelian group structure $E(\mathbb{F}_q)$ on the **rational** solutions of $Y^2 = X^3 + aX + b$ (+ point at infinity).

Arise from a **rank-2 analog** of complex cyclotomy.

There are **many elliptic curves**: for any $U < 2\sqrt{q}$ coprime with q, there exist an elliptic curve with $|E(\mathbb{F}_q)| = q + 1 \pm U$ (Deuring'41).

$E(\mathbb{F}_q) \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ with $m_1 \mid m_2$ (Cassels'66).

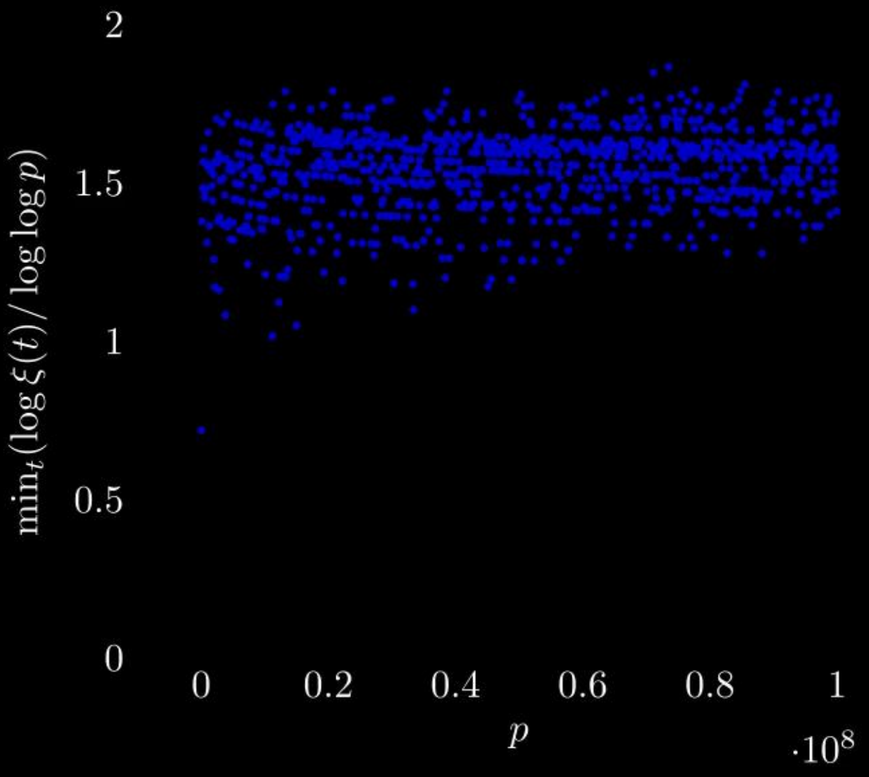
Goal: replace a cyclotomic **smoothness** condition on $q - 1$ by a **smoothness** condition on $|E(\mathbb{F}_q)|$ for a good elliptic curve E.

Finding a suitable elliptic curve

Precomputation depending only on p.

Hope: very good elliptic curves always exist!

Conjecture: for any large prime p, there exists an elliptic curve $E/\mathbb{F}_p$ s.t. $|E(\mathbb{F}_p)|$ and $|\widetilde{E}(\mathbb{F}_p)|$ are $(\leq (\log p)^2)$-smooth.

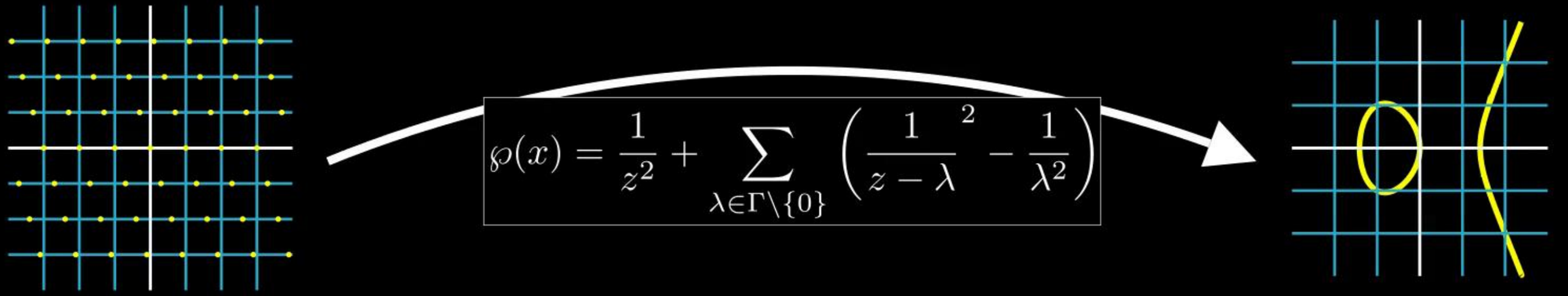


Complex multiplication

Endomorphisms of elliptic curves: algebraic morphisms compatible with the group law.

Over $\mathbb{C}$, endomorphisms are $\mathbb{Z}$-linear endomorphisms of Γ.

Characteristic polynomial: degree 2 polynomial in $\mathbb{Z}[X]$.



Frobenius endomorphism $\pi : (x, y) \mapsto (x^q, y^q)$ of $E/\mathbb{F}_q$.

For any N coprime to $\mathrm{char}(\mathbb{F}_q)$, $E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$.

π acts as a $\mathbb{Z}/N\mathbb{Z}$-linear map on $E[N]$
$\rightsquigarrow$ characteristic polynomial $\chi_{\pi,N}(X)$ in $(\mathbb{Z}/N\mathbb{Z})[X]$.

Theorem: $\exists \chi_\pi(X) \in \mathbb{Z}[X]$ s.t. $\chi_{\pi,N}(X) \equiv \chi_\pi(X) \bmod N$ for all N coprime with q.

Theorem: $\chi_\pi(X) = X^2 - tX + q$, with $t \in [-2\sqrt{q}, 2\sqrt{q}]$.

Zeta function, Weil conjectures, and point-counting

Point-counting problem for elliptic curves

Compute the **order** of $E(\mathbb{F}_q)$, where $E : Y^2 = X^3 + aX + b$.

Related to the **zeta function** of E:

$$\zeta_E(s) = \exp\Big(\sum_{m \geq 1} \frac{|E(\mathbb{F}_{q^m})|}{m} q^{-ms}\Big).$$

Weil conjectures (proved) $\Rightarrow \zeta_E(s) = \dfrac{1 - tq^{-s} + q^{1-2s}}{(1 - q^{-s})(1 - q^{1-s})}$.

Characteristic polynomial of the Frobenius endomorphism: $X^2 - tX + q$.

Inverse problem: constructing EC with given number of points

CM method: efficient when $t^2 - 4q$ is "small" $(< 2^{50})$.

$\rightsquigarrow$ Morain'91, Sutherland'10.

Can be used to construct elliptic curves with **prescribed number of rational points**.

Schoof's algorithm ('85)

Computes $|E(\mathbb{F}_q)| = q + 1 - t$ by computing the **trace** of the Frobenius endomorphism.

Characteristic polynomial of the Frobenius endomorphism: $X^2 - tX + q$.

For ℓ prime, the **ℓ-torsion** $E[\ell]$ (over $\overline{\mathbb{F}_q}$) is encoded by the **division polynomial** $\psi_\ell(X, Y)$.

Find $t \bmod \ell$ via the equation
$(X^{q^2}, Y^{q^2}) + [q] \cdot (X, Y) = [t] \cdot (X^q, Y^q) \bmod \langle \psi_\ell(X, Y), Y^2 - X^3 - aX - b \rangle$.

Repeat for many ℓ, and compute $t \in \mathbb{Z}$ via the CRT.

Complexity: $\widetilde{O}((\log q)^4)$ ops in $\mathbb{F}_q$.

Kayal's approach to polynomial factoring

Root-finding method for $f(T) \in \mathbb{F}_q[T]$

Pick an **elliptic curve** parametrized by $a(T), b(T) \in \mathbb{F}_q[T]/f(T)$:

$\rightsquigarrow E : Y^2 = X^3 + a(T)X + b(T)$.

Pick ℓ prime (coprime with q).

Compute $(X^{q^2}, Y^{q^2}) - [t] \cdot (X^q, Y^q) + [q] \cdot (X, Y)$ mod $\langle \psi_\ell(X, Y), Y^2 - X^3 - a(T)X - b(T), f(T) \rangle$ for each $t \in \{0, \ldots, \ell - 1\}$.

Separates roots t_1, t_2 of $f(T)$ via a **GCD** if the number of solutions in $\mathbb{F}_q$ of $Y^2 = X^3 + a(t_1)X + b(t_1)$ and $Y^2 = X^3 + a(t_2)X + b(t_2)$ are **not congruent** modulo ℓ.

Presented by Kayal in a talk in 2005.

Wolfsdorf's Master thesis'06.

Generalization to **abelian varieties** in Poonen'17.

$\rightsquigarrow$ Deterministic polynomial-time under an **heuristic argument**.

Elliptic Curve Fast Fourier Transform (ECFFT)

Ben-Sasson/Carmon/Kopparty/Levit'21: ECFFT.

Idea: replace the smooth subgroup of $\mathbb{F}_q^\times$ required by the FFT by a **smooth cyclic subgroup** in $E(\mathbb{F}_q)$ for an elliptic curve E.

Problem: If P is a rational point of $E/\mathbb{F}_q$, then there is in general no endomorphism $E \to E$ with kernel $\langle P \rangle$.

Solution: Isogenies!

Isogenies of elliptic curves

$$\begin{array}{ccc} & [n] & \\ E & \longrightarrow & E \\ \iota \downarrow & & \downarrow \iota \\ E' & \longrightarrow & E' \\ & [n] & \end{array}$$

Isogeny: nonzero morphism $\iota : E \to E'$ between elliptic curves.

Compatible with **group structure**, and **algebraic structure**.

Kernel is a **finite subgroup**.

Cyclic subgroups of $E(\overline{\mathbb{F}_q})[\ell]$ give ℓ-isogenies.

An ℓ-isogeny (ℓ odd) $\iota : E \to E'$ has a **kernel polynomial** which divides $\psi_{\deg \iota}(X)$.

Can be used to **speed up** Schoof's algorithm!

Isogeny - example

E: $Y^2 = X^3 + 11251\,X + 43019$ over $\mathbb{F}_{65521}$.

$(32776, 0) \in E(\mathbb{F}_q)$ is a 2-torsion point.

$$\iota(X, Y) = \left(\frac{X^2 + 32776X + 60632}{X - 32776}, \frac{X^2Y + 65490XY + 21029Y}{(X - 32776)^2} \right).$$

$\iota : E \to E'$.

$E' : Y^2 = X^3 + 65428X^2 + 3416X$.

Low-degree isogenies are easy to compute with.

Detour: SEA algorithm

For ℓ odd prime, the ℓ-torsion $E(\overline{\mathbb{F}_q})[\ell]$ is encoded by the **division polynomial** $\psi_\ell(X)$.

Assume that we know a (rational) ℓ-isogeny $\iota : E \to E'$.

$\rightsquigarrow$ replace $\psi_\ell(X)$ by the **kernel polynomial** of ι.

When $X^2 - tX + q$ factors in $\mathbb{Z}/\ell\mathbb{Z}[X]$ (heuristically half of the time), we can find such an isogeny using **modular polynomials**.

Find $t \bmod \ell$ via the equation
$(X^{q^2}, Y^{q^2}) + [q] \cdot (X, Y) = [t] \cdot (X^q, Y^q) \bmod \langle \psi_\iota(X), Y^2 - X^3 - aX - b \rangle$.

Heuristic **complexity improvement**: $\widetilde{O}((\log q)^3)$ ops in $\mathbb{F}_q$.

Fast Fourier Transform

Goal: Multiply polynomials $f(X)$ and $g(X)$ in $\mathbb{F}_q[X]$.

Assume 2^n divides $q-1$, where $2^n \geq \deg(f) + \deg(g)$.

Let $\zeta \in \mathbb{F}_q^\times$ be a **2^n-th root of unity**.

Multi-point evaluation of $f(X)$ and $g(X)$ at ζ^i for $i \in \{0, \ldots, 2^n - 1\}$.

$$f(X) = X^5 + 2X^4 + 5X^3 + X^2 + 7X + 2$$

$$f(X) = 2X^4 + X^2 + 2 + X^5 + 5X^3 + 7X$$

$$f(\zeta^i) = f_0(\zeta^{2i}) + \zeta^i f_1(\zeta^{2i})$$

One evaluation of degree $\deg(f)$ at 2^n points $\rightarrow$ two evaluations of degree $\deg(f)/2$ at 2^{n-1} points.

Complexity: $O(n \log n)$.

Restriction: Requires a primitive 2^n-th root of unity in $\mathbb{F}_q^\times$.

Classical FFT with "synthetic roots"

Schönage-Strassen'71, Cantor/Kaltofen'91
$\rightsquigarrow$ adding **artificial roots** by computing in $\mathbb{F}_q[X][Y]/(Y^\delta + 1)$.

$\rightsquigarrow \widetilde{O}(n \log n \log\log n)$ with no restriction on $q - 1$.

Harvey/van der Hoeven/Lecerf'2014, Harvey/van der Hoeven'2019

$\rightsquigarrow O(n \log q \log(n \log q))$ bit complexity in the Turing machine model (under a conjecture).

Ben-Sasson/Carmon/Kopparty/Levit'21: ECFFT

Idea: Replace **2^n-th root of unity** in $\mathbb{F}_q^\times$ by a **2^n-th torsion point** in $E(\mathbb{F}_q)$.

Step 1 (precomp): find an elliptic curve $E/\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ has a rational point Q of **order 2^n**.

Multipoint evaluation of $f \in \mathbb{F}_q(E)$ at $\infty, Q, 2Q, \ldots, (2^n-1)Q$ (assuming no pole).

Step 2 (precomp): Compute a **2-isogeny** $\iota : E \to E'$ with kernel $\{\infty, 2^{n-1} \cdot Q\}$ and set $Q' = \iota(Q)$. Also compute $g \in \mathbb{F}_q(E)$ with no zero at $\langle Q \rangle$ s.t. $g(\infty) = 1$, $g(P + 2^{n-1}Q) = -g(P)$, $\deg(g) = O(1)$.

Step 3: Compute $f_0, f_1 \in \mathbb{F}_q(E')$ such that $f(P) = f_0(\iota P) + g(P) f_1(\iota P) \rightsquigarrow$ $\deg(f_0), \deg(f_1) \approx \deg(f)/2$.

$f_0(\iota P) = (f(P) + f(P + 2^{n-1}Q))/2$, $f_1(\iota P) = (f(P) - f(P + 2^{n-1}Q))/(2g(P))$.

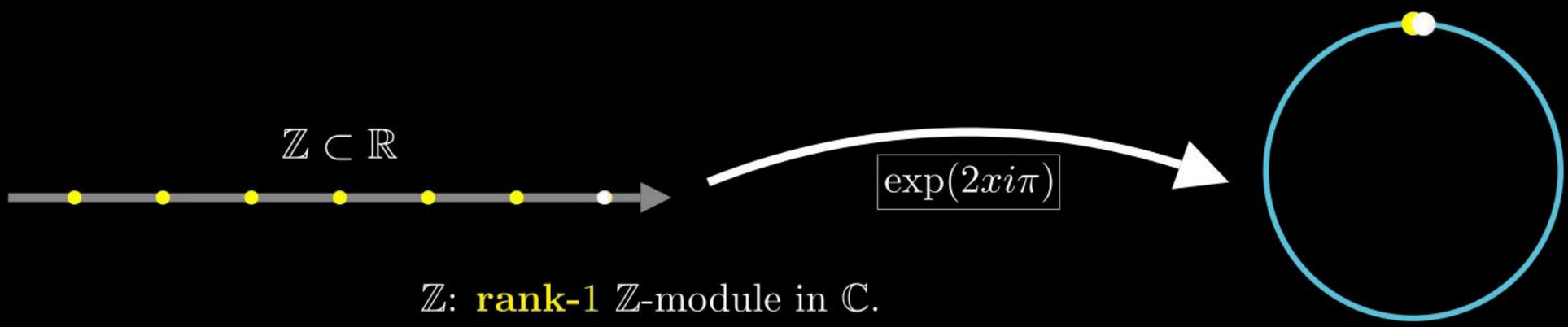
Step 4: Recurse!

> One evaluation of degree $\deg(f)$ at 2^n points in $E(\mathbb{F}_q) \to$ two evaluations of degree $\approx \deg(f)/2$ at 2^{n-1} points in $E'(\mathbb{F}_q)$.

Complexity: $O(n \log n)$.

Restriction: Requires a 2^n-torsion point in $E(\mathbb{F}_q)$!

Complex cyclotomy



$\mathbb{Z}$: **rank-1** $\mathbb{Z}$-module in $\mathbb{C}$.

all rank-1 $\mathbb{Z}$-modules in $\mathbb{C}$ are **homothetic**.

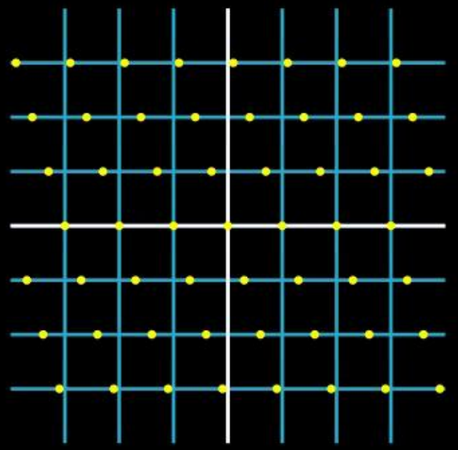
$\mathbb{Z}/n\mathbb{Z}$: n-torsion in $\mathbb{R}/\mathbb{Z}$ $\rightsquigarrow$ sent to solutions of $X^n - 1$.

exp is **transcendental** but solutions of $X^n - 1$ are **algebraic**.

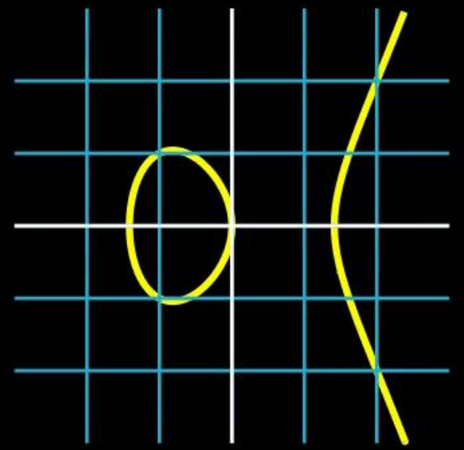
Complex elliptic curves

Complex cyclotomy: rank-1 $\mathbb{Z}$-modules in $\mathbb{C}$ (up to homothety).

Complex elliptic curves: rank-2 $\mathbb{Z}$-modules in $\mathbb{C}$ (up to homothety).



$$\wp(x) = \frac{1}{z^2} + \sum_{\lambda \in \Gamma \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$



$\sin(x)$, $2i\pi\mathbb{Z}$-periodic: compositional inverse to $\int_0^x \frac{dy}{\sqrt{1-y^2}}$.

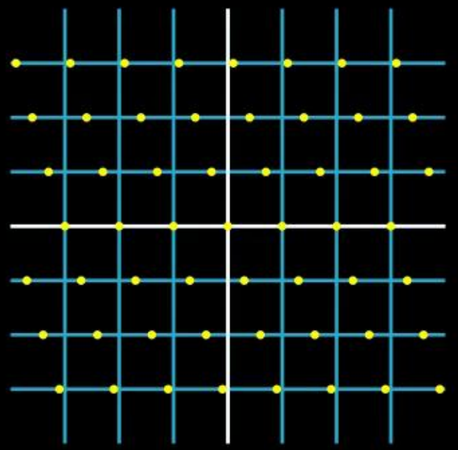
$\wp(x)$, Γ periodic: compositional inverse to $\int_s^\infty \frac{ds}{\sqrt{4s^3 - g_2 s - g_3}}$.

Complex Drinfeld modules

Complex cyclotomy: rank-1 $\mathbb{Z}$-modules in $\mathbb{C}$ (up to homothety).

Complex elliptic curves: rank-2 $\mathbb{Z}$-modules in $\mathbb{C}$ (up to homothety).

Complex Drinfeld modules: rank-r $\mathbb{F}_q[T]$-modules in $\mathbb{C}_\infty = \widehat{\overline{\mathrm{Frac}(\mathbb{F}_q[[1/T]])}}$ (up to homothety).



$$e_\Gamma(x) = x \prod_{\lambda \in \Gamma \setminus \{0\}} \left(1 - \frac{x}{\lambda}\right).$$

$$\phi_X : x \mapsto \Delta x^{q^2} + g x^q + \gamma x$$

$\mathbb{C}_\infty$

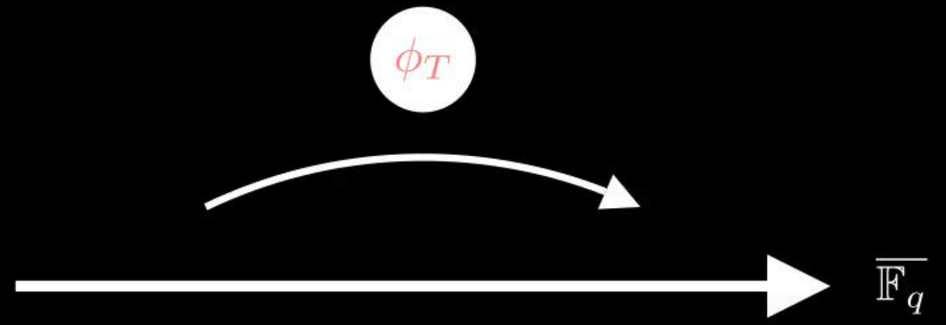
$e_\Gamma(x)$: **Carlitz-Drinfeld exponential**.

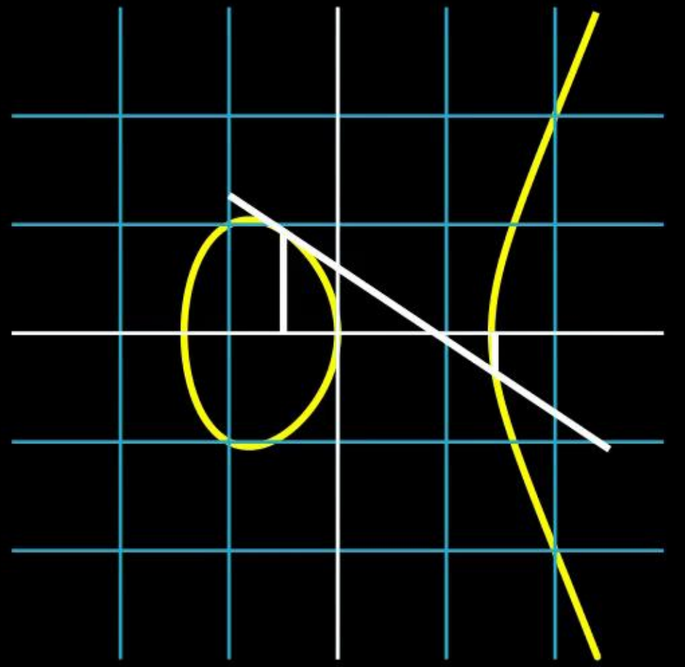
Rank not bounded by 2!

Finite Drinfeld Modules

Finite Drinfeld module:

a (non-homothetic) $\mathbb{F}_q$-linear endomorphism of $\overline{\mathbb{F}_q}$





Analog of the elliptic curve endomorphism $x(P) \mapsto x([n]P)$.

$$\phi_T(x) = \Delta x^{q^2} + \tau x^q + \gamma x$$

$$\forall g \in \mathbb{F}_q[T], \phi_{g(T)}(x) = g(\phi_T)(x)$$

$$\psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$\forall n \in \mathbb{Z}_{>0}, \psi_{2n+1}(x) = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$$

Ore polynomials and rationality

Finite Drinfeld module: an endomorphism $\phi_T \in \mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$.

Theorem (Ore)

$\mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$ is generated by:

- homotheties $x \mapsto \alpha x$, $\alpha \in \overline{\mathbb{F}_q}$;
- the q-Frobenius $x \mapsto x^q$.

$\mathrm{End}_{\mathbb{F}_q}(\overline{\mathbb{F}_q})$ = Ring of linearized polynomials $\sum a_i T^{q^i}$ with composition.

Ore polynomials $\overline{\mathbb{F}_q}\{\tau\}$: $\tau\alpha = (x \mapsto (\alpha x)^q) = (x \mapsto \alpha^q x^q) = \alpha^q \tau$.

$\phi_T \in \overline{\mathbb{F}_q}\{\tau\}$ is defined over L (finite extension of $\mathbb{F}_q$) if ϕ_T **commutes with** $\mathrm{Gal}(\mathbb{F}_q \hookrightarrow L) = \langle \tau^{[L:\mathbb{F}_q]} \rangle$, i.e. $\phi_T \in L\{\tau\}$.

Example

$q = 2,\ L = \mathbb{F}_2[Z]/(Z^2 + Z + 1),\ \gamma = \overline{Z}$

$\phi_T = \gamma\tau^2 + \tau + \gamma = (x \mapsto \gamma x^{q^2} + x^q + \gamma x)$

$\phi_{T^2+1} = \gamma^2\tau^4 + \tau^3 + \tau^2 + \tau + \gamma$

$\ker \phi_{T^2+1} \simeq (\mathbb{F}_q[T]/(T^2 + 1))^2$

Example

$q = 2,\ L = \mathbb{F}_2[Z]/(Z^2 + Z + 1),\ \gamma = \overline{Z}$

$\phi_T = \gamma\tau^2 + \tau + \gamma = (x \mapsto \gamma x^{q^2} + x^q + \gamma x)$

$\phi_{T^2+T+1} = \gamma^2\tau^4 + \tau^3 + \gamma^2\tau^2$

$\ker \phi_{T^2+T+1} \simeq \mathbb{F}_q[T]/(T^2 + T + 1)$

Example

$q = 2$, $L = \mathbb{F}_2[Z]/(Z^2 + Z + 1)$, $\gamma = \overline{Z}$

$\phi_T = \tau^2 + \gamma^2\tau + \gamma = (x \mapsto x^{q^2} + \gamma^2 x^q + \gamma x)$

$\phi_{T^2+T+1} = \tau^4$

$\ker \phi_{T^2+T+1} = \{0\}$

Characteristic: $\mathfrak{p} = (p(T)) = (T^2 + T + 1)$.

Supersingularity!

Complex multiplication

ϕ rank-2 Drinfeld module $/L$: $\phi_T = \Delta\tau^2 + g\tau + \gamma \in L\{\tau\}$.

Frobenius endomorphism of ϕ: $\tau^{[L:\mathbb{F}_q]}$.

Theorem: $\exists Q(X,Y) \in \mathbb{F}_q[X][Y]$ of degree 2 such that $Q(\phi_T, \tau^{[L:\mathbb{F}_q]}) = 0$.

$\rightsquigarrow$ **Characteristic polynomial** of the Frobenius:
$Q(X,Y) = Y^2 + t(X)Y + n(X)$.

Hasse-Weil bounds: $\deg(t(X)) \leq [L:\mathbb{F}_q]/2$.

Factoring with Drinfeld Modules (I)

Panchishkin/Potemine'89, van der Heiden'04:
$\rightsquigarrow$ **Drinfeld module analogs** of ECM (Lenstra'87)

Start with a **random rank-$(d+1)$ Drinfeld module** $\phi_T \in B\{\tau\}$ with coefficients in $B = \mathbb{F}_q[X]/f(X)$.

ϕ_T is a **$\mathbb{F}_q$-linear** endomorphism of B.

Compute its **characteristic polynomial** $\chi(T) \in \mathbb{F}_q[T]$.

Compute $g_d(T) = \mathrm{GCD}(\chi(T), T^{q^d} - T) \in \mathbb{F}_q[T]$.

Compute $\mathrm{GCD}(\phi_{g_d(T)}(b(X)), f(X))$, for a random $b \in B$.

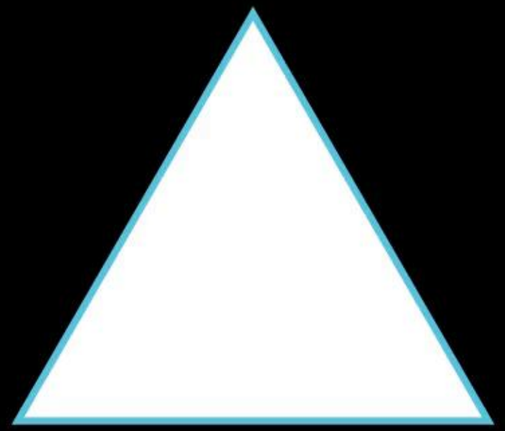
Repeat!

Complexity: $O(dn^3 + n^2 \log q)$ to find an **irreducible factor** of degree d.

Three faces of arithmetico-geometric objects

ECM (Lenstra'87)

Factoring integers using elliptic curves over $\mathbb{Q}$



Kayal'05

Factoring polynomials using elliptic curves over $\mathbb{F}_q(X)$

Panchishkin/Potemine'89, van der Heiden'04

Factoring polynomials using Drinfeld modules over $\mathbb{F}_q$

Factoring with Drinfeld Modules (II)

Doliskani/Narayanan/Schost'18: uses supersingular reductions

Start with a Drinfeld module over $\mathbb{F}_q[X]/f(X)$.

$\phi_T = \Delta(X)\tau^2 + g(X)\tau + X \in \mathbb{F}_q(X)\{\tau\}$.

Compute the **Hasse invariant** $h(X)$ of ϕ modulo $f(X)$.

Deligne recurrence: $r_0(X) = 1$, $r_1(X) = g(X)$,
$r_{k+2}(X) = g(X)^{q^{k+1}} r_{k+1}(X) - (X^{q^{k+1}} - X)\Delta(X)^{q^k} r_k(X) \bmod f(X)$.

Compute $\mathrm{GCD}(r_{\deg(f)}(X), r_{\deg(f)+1}(X))$.

If the initial Drinfeld module has **complex multiplication**, this provides a factor of $f(X)$ with good probability.

Randomize and repeat!

Complexity: $n^{3/2+\varepsilon}(\log q)^{1+o(1)} + n^{1+\varepsilon}(\log q)^{2+o(1)}$.

Same complexity as Kedlaya/Umans+Kaltofen/Shoup.

Isogenies and motives of Drinfeld modules

$$\begin{array}{ccc} & \phi_X & \\ \overline{\mathbb{F}_q} & \to & \overline{\mathbb{F}_q} \\ \iota \downarrow & & \downarrow \iota \\ \overline{\mathbb{F}_q} & \to & \overline{\mathbb{F}_q} \\ & \psi_X & \end{array}$$

Morphism $\phi \to \psi$: $\iota \in \overline{\mathbb{F}_q}\{\tau\}$ s.t. $\iota\phi_T = \psi_T\iota$.

Motive of a Drinfeld module: $\mathbb{M}(\phi) = L\{\tau\}$ with $L[T]$-module structure,

$$(\alpha g(T)) \cdot (a_0 + \ldots + a_\ell\tau^\ell) = \alpha(a_0 + \ldots + a_\ell\tau^\ell)\phi_{g(T)}.$$

Slogan: Action of scalar endomorphisms on the function field.

Addition in the endomorphism field is **compatible** with the addition in the function field.

Now isogenies are 2×2 matrices in $L[T]$!

Fast algorithms for computing isogenies and endomorphism rings.

$\rightsquigarrow$ Musleh'24, Caruso/Leudière'25.

Conclusion

Goal of this talk: applications of **arithmetic geometry** in **computer algebra**.

Huge toolbox for elliptic curves; toolbox for **Drinfeld modules** is growing fast.

$\rightsquigarrow$ Armana/Berardini/Caruso/Leudière/Nardi/Pazuki'26.

$\rightsquigarrow$ Ayotte/Caruso/Leudière/Musleh'23: SageMath implementation.

Development of **computational aspects of elliptic curves**: driven by computational number theory and cryptography.

Using other $\mathbb{F}_q$**-algebraic groups**: torus groups, Jacobians of hyperelliptic curves, etc.

Implementations?

Thank you!