# Poincaré series from Cryptology and Exceptional Towers

Mike Fried, UCI and MSU-B 03/26/07

Part 0: Exceptionality and fiber products

Part I: Exceptional rational functions over number fields

Part II: The exceptional tower $\mathcal{T}_{Z,\mathbb{F}_q}$ of any variety $Z$ over $\mathbb{F}_q$

Part III: Generalizing Exceptionality: Pr-exceptional covers and Davenport pairs

Part IV: (Chow) motives from exceptional covers and Davenport pairs: Diophantine category of Poincare series over $(Z, \mathbb{F}_q)$

Part V: Comparing $\mathcal{T}_{\mathbb{P}^1,\mathbb{F}_q}$ with various subtowers: Generated by Serre's Open Image Theorem, **CM** part; By Serre's Open Image Theorem, **GL** part; By Wildly ramified polynomials.

# Part 0: Exceptionality and fiber products

http://math.uci.edu/~mfried $\longrightarrow$ §1.a. Articles and Talks: $\longrightarrow$ • Finite fields, Exceptional covers and motivic Poincare series

An $\mathbb{F}_q$ cover $\varphi : X \longrightarrow Z$ of *absolutely irreducible normal varieties* is *exceptional* if $\varphi$ one-one on $\mathbb{F}_{q^t}$ points for infinitely many $t$.

For a # field: $\varphi$ has infinitely many exceptional residue class field reductions. We use the Davenport-Lewis name exceptional because, equivalently, a version of their geometric property holds for $\varphi$.

# Using fiber products

Assume $\varphi_i : X_i \to Z$, $i = 1, 2$, are two covers (of normal varieties) over $K$. The set theoretic fiber product has geometric points

$$\{(x_1, x_2) \mid x_i \in X_i(\bar{K}), i = 1, 2, \ \varphi_1(x_1) = \varphi_2(x_2)\} :$$

$x \in X(\bar{\mathbb{F}}_q)$ is a point in $X$ with coordinates in $\bar{\mathbb{F}}_q$.

Won't be normal at $(x_1, x_2)$ if $x_1$ and $x_2$ both ramify over $Z$. The *categorical* fiber product here is *normalization* of the result: components are disjoint, normal varieties, $X_1 \times_Z X_2$.

## Galois closure of a cover

Denote $X \times_Z X$ minus the diagonal by $X^2_Z \setminus \Delta$.

$X^k_Z \setminus \Delta$: $k$th iterate of the fiber product minus the *fat diagonal*; empty if $k > n = \deg(\varphi)$.

Any $K$ component $\hat{X}$ of $X^n_Z \setminus \Delta$ is a $K$ Galois closure of $\varphi$: unique up to $K$ isomorphism of Galois covers of $Z$.

$S_n$ action on $X^n_Z \setminus \Delta$ gives the Galois group $G(\hat{X}/Z) \stackrel{\text{def}}{=} \hat{G}_\varphi$: subgroup fixing $\hat{X}$. Without $\hat{\ }$, $G_\varphi$, denotes absolute Galois closure.

## Part I: Exceptional rational functions over # fields

Cyclic polynomials have the form $x \longrightarrow x^n$. RSA code scheme uses these. Fewer people know about Chebychev polynomials. Yet, these also have their cryptography use, as do compositions of these types.

**Proposition 1.** *If $(n, p-1) = 1$, then we can use $x^n$ to* scramble *data into $\mathbb{Z}/p$. If $n$ is odd, there are infinitely many such primes $p$.*

*Proof.* Euler's Theorem: Powers of a single integer $\alpha$ fill out $\mathbb{Z}/p \setminus \{0\} \stackrel{\text{def}}{=} \mathbb{Z}/p^*$. $\square$

## Residue Primes that work for (odd) $n$

Take $p \in \{k + m \cdot n | m \in \mathbb{Z}\}$ where $k$ satisfies:

- $(k, n) = 1$ (apply Dirichlet's Theorem); and
- $(k - 1, n) = 1$ $((p - 1 = k - 1 + m \cdot n, n) = 1)$.

Example: $k = 2$ works; other integers may too.

## Tchebychev polynomials of odd degree $n$

$$T_n(\tfrac{1}{2}(x+1/x)) = \tfrac{1}{2}(x^n+1/x^n),$$
$$T_n : \{\infty, \pm 1\} \mapsto \{\infty, \pm 1\}.$$

**Proposition 2.** *If* $(n,6)=1$, *then* $T_n : \mathbb{Z}/p \longrightarrow \mathbb{Z}/p$ *maps one-one for infinitely many* $p$. *Exactly those primes* $p$ *with* $(p^2-1,n)=1$.

Proof: Use finite fields $\mathbb{F}_{p^2} \supset \mathbb{Z}/p$: $\mathbb{F}^*_{p^2}$ cyclic.

## 2. Schur's Conjecture:

Cryptography we recognize in modern algebra goes back to the middle of the 1800s. They used finite fields as the place to encode a message.

**Conjecture 3 (Schur 1921).** Only compositions of cyclic, Tchebychev and degree 1 ($x \mapsto ax + b$) give polynomials mapping 1-1 on $\mathbb{Z}/p$ for $\infty$-ly many $p$.

**Problem 4.** How to check if an $f(x)$ is a composition of the correct polynomials? If so, how to check if it is 1-1 for $\infty$ of $p$ (notation: $1–1_\infty$)?

## Points toward proving Schur's conjecture:

Step 1: If $f = f_1 \circ f_2$ ($f_i \in \mathbb{F}_q[x]$), then $f$ is $1$–$1_\infty$ if and only $f_1$ *and* $f_2$ are $1$–$1_\infty$.

Subtle reduction: If $f$ decomposes over $\mathbb{C}$ then it decomposes over $\mathbb{Q}$ (not automatic for *rational* functions). So, to prove Schur's conjecture we consider $f$ *indecomposable* over $\bar{K}$.

Step 2: Consider $1$–$1_\infty f$ with $f : \mathbb{Z}/p \to \mathbb{Z}/p$ 1-1. Then, the polynomial expression

$$(*)\ \varphi(x,y) = \frac{f(x)-f(y)}{x-y} = 0$$

has no solutions $(x_0, y_0) \in \mathbb{Z}/p \times \mathbb{Z}/p$, $x_0 \neq y_0$.

## Cover characterization of exceptionality

**Proposition 5 (Weil).** *If* $\varphi(x,y)$ *has* $u$ *absolutely irreducible factors (over* $\mathbb{F}_p$*), then (*) has at least* $u \cdot p + A\sqrt{p}$ *solutions (some* $A$ *constant in* $p$*).*

**Corollary 6.** *If* $f$ *is* $1$–$1_\infty$*, then* $\varphi(x,y) \mod p$ *has no absolutely irreducible factors (for* $p$ *large).*

**Proposition 7.** [DL63] $\rightarrow$ [Mc67] $\rightarrow$ [Fr74] $\rightarrow$ [Fr05] $\rightarrow$ [GLTZ07]: *General* $\mathbb{F}_q$ *cover of normal varieties:* $\varphi: X \rightarrow Z$ *exceptional over* $\mathbb{F}_{q^t}$

$\Leftrightarrow X_Z^2 \setminus \Delta$ *has no* $\mathbb{F}_{q^t}$ *abs. irred. components.*

## For 1–$1_\infty$ $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$, the groups $\hat{G}_f$ and $G_f$

Consider $f(x) - z = 0$ with $z$ a variable. Find $n$ solutions $x_1, \ldots, x_n$ in some algebraic closure $F$ of $\mathbb{Q}(z)$: $f(x_i) = z$; they generate a field $\mathbb{Q}(x_1, \ldots, x_n, z) \stackrel{\text{def}}{=} L_f$. Then, $\hat{G}_f = G(L_f/\mathbb{Q}(z))$.

**Proposition 8.** *Then, $G_f \le S_n$ is primitive, not doubly transitive, and contains an $n$-cycle.*

**Example 9.** Assume $n > 2$ is prime. The group $D_n$ (Dihedral of degree $n$) with generators

$$\begin{aligned} g_1 = &\ (1\,n)(2\,n{-}1)\cdots(\tfrac{n-1}{2}\,\tfrac{n+3}{2}) \\ g_2 = &\ (2\,n)(3\,n{-}1)\cdots(\tfrac{n+1}{2}\,\tfrac{n+3}{2}) \end{aligned}$$

is primitive,not double transitive, has an $n$-cycle.

## Why primitive with an $n$-cycle?

With $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ (exceptionality allows monic). Solve for $x$ from $f(x) = z$. Solution:

$$x_1 = z^{1/n} + b_0 + b_1 z^{-1/n} + b_2 z^{-2/n} + \cdots .$$

Substitute $e^{\frac{2\pi i \cdot k}{n}} z^{\frac{1}{n}} \mapsto z^{1/n}$ for $n$-cycle in $G_f$.

Let $G_f(x_1)$ be the subgroup of $G_f$ fixing $x_1$. Primitive means no proper group $H$ with $G_f(x_1) < H < G_f$. Galois correspondence: Such an $H$ would mean a field $L = \mathbb{Q}(w)$ with $\mathbb{Q}(z) < L < \mathbb{Q}(x_1)$. So, $w = f_2(x_1)$, and $z = f_1(w)$. Contrary to indecomposable $f$: $f_1(f_2(x_1)) = z$.

# Concluding Schur's Conjecture

Why $G_f$ is not doubly transitive: Equivalent to $\varphi(x,y)$ $(X_Z^2 \setminus \Delta)$ has at least two factors over $\bar{\mathbb{Q}}$ (from no abs. irred. factors over $\mathbb{Q}$).

Get Schur's conjecture if $1\text{–}1_\infty$ and indecomposable $f$ is variable change of cyclic or Chebychev polynomial. Chebychev case: variable change, $(z,x) \longrightarrow (az+b, a'x+b')$ $(a,b,a',b' \in K)$, allows $f(\pm u) = \pm u$ with $u^2 = a \in K$.

Then, with $\ell_u : x \mapsto ux$, $f = \ell_u \circ T_n \circ \ell_{u^{-1}} \stackrel{\text{def}}{=} T_{n,a}$: $u^{n-1}T_{n,a}$ is what a large literature calls a *Dickson polynomial* [LMT93].

## All exceptional prime degree rational $f$

Step 1: Show $G_f$ is a cyclic or dihedral group.

**Proposition 10 (Famous Group Results).** *If $n$ is a prime, then (Burnside):*

$$G_f \le \left\{\left(\begin{smallmatrix} u & v \\ 0 & 1 \end{smallmatrix}\right) \mid u \in (\mathbb{Z}/n)^*, v \in \mathbb{Z}/n\right\} \stackrel{\text{def}}{=} \mathbb{Z}/n \times^s (\mathbb{Z}/n)^*.$$

*For $n$ not prime there is no such $G_f$: Schur.*

Step 2: Show $G_f$ dihedral (resp. cyclic) $\iff$ polynomial $f$ is Chebychev (resp. cyclic) after changing variables.

Best part: *Monodromy method* solves many other problems (Schur's conjecture the easiest).

## Step 2 cont: Apply Riemann's Existence Theorem.

For $g \in S_n$, $\operatorname{ind}(g) \stackrel{\mathrm{def}}{=} n-$ # of disjoint cycles in $g$ (including length 1).

If $f : \mathbb{C}_x \cup \{\infty\} \to \mathbb{C}_z \cup \{\infty\}$, with branch points $z_1, \dots, z_r \implies r$ elements $g_1, \dots, g_r \in G_f$ (*branch cycles*) with these properties:

- $G_f = \langle g_1, \dots, g_{r-1} \rangle$ (generation);
- $\prod_{i=1}^{r} g_i = 1$ (product-one); and
- $2(n-1) = \sum_{i=1}^{r} \operatorname{ind}(g_i)$ (genus 0).

# Finish Polynomial case

- $g_r \stackrel{\text{def}}{=} g_\infty$ is an $n$-cycle; and
- $n - 1 = \sum_{i=1}^{r-1} \text{ind}(g_i)$ (genus 0).

**Proposition 11.** *Combine with*

$$g_1, \dots, g_{r-1}, g_\infty \in \mathbb{Z}/n \times^s (\mathbb{Z}/n)^*.$$

*Polynomial Result:*

- $\{g_1, \dots, g_{r-1}\} = \{g_1, g_2\}$ *as in Ex. 9 modulo conjugation in* $S_n$, $g_\infty = (1\,2\,\dots\,n)^{-1}$; *or*
- $r = 2$ *and* $g_1 = (1\,2\,\dots\,n)$.

*Tchebychev/cyclic polynomial branch cycles.*

## Dominant rational (not polynomial) function case

Branch cycles are $(g_1, g_2, g_3, g_4)$, $g_i$s conjugate to $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}/n \times^s \{\pm 1\}$. Most new functions from Weierstrass $\wp$-functions through this diagram:

$$\begin{array}{ccc} \mathbb{C}_{\{\pm w\}} \cup \{\infty\} & \xrightarrow{f} & \mathbb{C}_{\{\pm z\}} \cup \{\infty\} \\ \text{mod } \{\pm 1\} \uparrow & & \uparrow \text{mod } \{\pm 1\} \\ \mathbb{C}_w/L_w & \xrightarrow{\text{mod } L_z/L_w \equiv \mathbb{Z}/n} & \mathbb{C}_z/L_z. \end{array}$$

Here $L_w \le L_z$ both generated over $\mathbb{Z}$ by two linearly independent (over $\mathbb{R}$) complex numbers.

## Part II: Exceptional tower $\mathcal{T}_{Z,\mathbb{F}_q}$ of variety $Z$ over $\mathbb{F}_q$

### Extension of constants series

Let $\hat{K}_\varphi(k)$ be the minimal def. field of (geom.) $\bar{K}$ components of $X_Z^k \setminus \Delta$, $1 \le k \le n$:

$$\ker(\hat{G}_\varphi \to G(\hat{K}_\varphi(n)/K)) = G_\varphi.$$

Each $\hat{K}_\varphi(k)/K$ is Galois: *$k$th ext. of constants field*: $G(\hat{K}_\varphi(k)/K)$ permutes geom. components of $X_Y^k \setminus \Delta$. Denote perm. rep. by $T_{\varphi,k}$.

# Characterize exceptional

There is a natural sequence of quotients

$$G(\hat{X}/Y) \to G(\hat{K}_\varphi(n)/K) \to \cdots \to G(\hat{K}_\varphi(k)/K)$$
$$\to \cdots \to G(\hat{K}_\varphi(1)/K).$$

$G(\hat{K}(1)/K)$ is trivial iff all $K$ components of $X$ are absolutely irreducible.

**Theorem 12.** *For $K$ a finite field, $G(\hat{K}_\varphi(2)/K)$ having no fixed points under $T_{\varphi,2}$ characterizes $\varphi$ being exceptional (*[Fr74], [Fr05], [GLTZ07]*).*

## The tower $\mathcal{T}_{Z,\mathbb{F}_q}$ and its cryptology potential

Morphisms $(X,\varphi) \in \mathcal{T}_{Z,\mathbb{F}_q}$ to $(X',\varphi') \in \mathcal{T}_{Z,\mathbb{F}_q}$ are covers $\psi : X \to X'$ with $\varphi = \varphi' \circ \psi$. Partially order $\mathcal{T}_{Z,\mathbb{F}_q}$ by $(X,\varphi) > (X',\varphi')$ if there is an $(\mathbb{F}_q)$ morphism $\psi$ from $(X,\varphi)$ to $(X',\varphi')$.

Then $\psi$ induces:

- a homomorphism $G(\hat{X}_\varphi/X_\varphi)$ to $G(\hat{X}_{\varphi'}/X_{\varphi'})$; and
- canonical map from cosets of $G(\hat{X}_\varphi/X_\varphi)$ in $G(\hat{X}_\varphi/Z)$ to the corresponding cosets for $X'$.

Note: $(X,\psi)$ is automatically in $\mathcal{T}_{X',\mathbb{F}_q}$.

## Forming the exceptional tower

Nub of an exceptional tower of $(Z, \mathbb{F}_q)$: $\exists$ unique minimal exceptional cover $X$ — the *fiber product* — dominating exceptional covers $\varphi_i : X_i \to Z$, $i = 1, 2$. Note: Everything depends on $\mathbb{F}_q$.

For $(X, \varphi) \in \mathcal{T}_{Z,\mathbb{F}_q}$ denote cosets of $G(\hat{X}_\varphi / X_\varphi)$ in $G(\hat{X}_\varphi / Z) = \hat{G}_\varphi$ by $V_\varphi$; coset of 1 by $v_\varphi$ and the rep. of $\hat{G}_\varphi$ on these cosets by $T_\varphi : \hat{G}_\varphi \to S_{V_\varphi}$. Write $G(\hat{K}_{\varphi_i}(2)/\mathbb{F}_q)$ as $\mathbb{Z}/d(\varphi_i)$, $i = 1, 2$.

## Why $X_1 \times_Z X_2$ has exactly one abs. irred. comp.

Do $\frac{1}{2}$, suppose none! Let $\mathbb{F}_{q^{t_0}}$ contain coefficients of all absolutely irred. $X_1 \times_Z X_2$ comps. Then, if $(t, t_0) = 1$, $X_1 \times_Z X_2$ has no abs. irr. com. over $\mathbb{F}_{q^t}$. Normality $\implies X_1 \times_Z X_2(\mathbb{F}_{q^t}) = \emptyset$.

D-L criterion allows assuming $\varphi_i$ s are étale. Then, $t \in (\mathbb{Z}/d(\varphi_i))^*$, $i = 1, 2$, $\implies \varphi_i$ is 1-1 and onto (over $\mathbb{F}_{q^t}$), $i = 1, 2$. For $t$ large, $\exists z \in Z(\mathbb{F}_{q^t})$ $\implies \exists x_i \in X_i(\mathbb{F}_{q^t}) \mapsto z$, $i = 1, 2$.

So $(x_1, x_2) \in X_1 \times_Z X_2(\mathbb{F}_{q^t})$.

## $\mathcal{T}_{Z,\mathbb{F}_q}$ is a very rigid category

**Proposition 13.** *In* $\mathcal{T}_{Z,\mathbb{F}_q}$ *there is at most one* $(\mathbb{F}_q)$ *morphism between any two objects. So,* $\varphi : X \to Z$ *has no* $\mathbb{F}_q$ *automorphisms:* $\mathrm{Cen}_{S_{V_\varphi}}(\hat{G}_\varphi) = \{1\}$.

*Then,* $\{(\hat{G}_\varphi, T_\varphi, v_\varphi)\}_{(X,\varphi)\in\mathcal{T}_{Z,\mathbb{F}_q}}$ *canonically defines a compatible system of permutation representations; it has a projective limit* $(\hat{G}_Z, T_Z)$.

Value of the Tower: It now makes sense to form the subtower generated by special exceptional covers: The minimal tower including all covers in the set. Examples: Tamely ramified subtower; Schur-Dickson subtower of $\mathcal{T}_{\mathbb{P}^1_z,\mathbb{F}_q}$; Subtower generated by **CM** (or $\mathbf{GL}_2$) covers from Serre's OIT (Part V).

## Exceptional scrambling

For any $t$ let $\mathcal{T}_{Z,\mathbb{F}_q}(t)$ be those covers with $t$ in their *exceptionality set*.

Cryptology starts by encoding a message into a set. For $t$ large our message encodes in $\mathbb{F}_{q^t}$. Then, select $(X,\varphi) \in \mathcal{T}_{Z,\mathbb{F}_q}(t)$. Embed our message as $x_0 \in X(\mathbb{F}_{q^t})$. Use $\varphi$ as a one-one function to pass $x_0$ to $\varphi(x_0) = z_0 \in Z(\mathbb{F}_{q^t})$ for "publication." You and everyone else who can understand "message" $x_0$ can see $z_0$ below it. To find out what is $x_0$ from $z_0$, need an *inverting function* $\varphi_t^{-1} : Z(\mathbb{F}_{q^t}) \to X(\mathbb{F}_{q^t})$.

## Inverting the scrambling map

**Question 14 (Periods).** With $X = \mathbb{P}^1_x$ and $Z = \mathbb{P}^1_z$, identify them to regard $\varphi$ on $\mathbb{F}_{q^t}$ as $\varphi_t$, permuting $\mathbb{F}_{q^t} \cup \{\infty\}$. Label the order of $\varphi_t$ as $m_{\varphi,t} = m_t$. Then, $\varphi_t^{m_t-1}$ inverts $\varphi_t$. How does $m_{\varphi,t}$ vary, for genus 0 exceptional $\varphi$, as $t$ varies?

Standard RSA inverts $x \mapsto x^n$ by inverting the $n$th power map on $\mathbb{F}^*_{q^t}$ (mult. by $n$ on $\mathbb{Z}/(q^t - 1)$ — Euler's Theorem). Works for all covers in the *Schur Sub-Tower* of $(\mathbb{P}^1_y, \mathbb{F}_q)$ *generated* by $x^n$s and $T_n$s. (For $T_n$s, "invert mult. by $n$" on $\mathbb{Z}/(q^{2t} - 1)$.)

# Part III: pr-exceptional covers and Davenport pairs

**Definition 15.** $\varphi : X \to Z$ is *p(ossibly)r(educible)-exceptional*: $\varphi : X(\mathbb{F}_{q^t}) \to Z(\mathbb{F}_{q^t})$ surjective for $\infty$-ly many $t$.

Then, $\varphi$ is exceptional iff $X$ is abs. irreducible. We even allow $X$ to have no abs. irred. comps.

Form $\hat{X} \to Z$ (with its canonical rep. $T_\varphi$), the Galois closure with group $\hat{G}_\varphi$, and get an extension of constants field with $G(\hat{\mathbb{F}}_\varphi/\mathbb{F}_q) = \mathbb{Z}/\hat{d}(\varphi)$.

## D-L generalization; pr-exceptional characterization

For $t \in \mathbb{Z}/\hat{d}(\varphi)$:

$$\hat{G}_{\varphi,t} \stackrel{\text{def}}{=} \{g \in \hat{G}_\varphi \mid \text{ restricts to } t \in \mathbb{Z}/\hat{d}(\varphi)\}.$$

*Exceptionality set* $E_\varphi$ of a pr-exceptional cover: $\{t \in \mathbb{Z}/\hat{d}(\varphi) \mid \forall g \in \hat{G}_{\varphi,t}$ fixes $\geq 1$ letter of $T_\varphi\}$.

pr-exceptional correspondences: $W \subset X_1 \times X_2$ with projections $W \to X_i$ s pr-exceptional.

Exceptional correspondence between $X_1$ and $X_2$ $\implies |X_1(\mathbb{F}_{q^t})| = |X_2(\mathbb{F}_{q^t})|$ for $\infty$-ly many $t$.

If $X_2 = \mathbb{P}^1_z$, then $\sum_{t=1}^{\infty}(a_n \stackrel{\text{def}}{=} |X_1(\mathbb{F}_{q^t})|)u^t$ has $a_n = q^t + 1$ for $\infty$-ly many $t$.

## A zoo of high genus except. correspondences between $\mathbb{P}^1_{x_1}$ and $\mathbb{P}^1_{x_2}$

If $\varphi_i : \mathbb{P}^1_{x_i} \longrightarrow \mathbb{P}^1_z$, $i = 1, 2$ is exceptional, then $\mathbb{P}^1_{x_1} \times_{\mathbb{P}^1_z} \mathbb{P}^1_{x_2}$ has a unique absolutely irreducible component, an exceptional cover of $\mathbb{P}^1_{x_i}$, $i = 1, 2$.

Suppose $\varphi_i : X_i \longrightarrow Z$, $i = 1, 2$, are abs. irreducible covers. The minimal ($\mathbb{F}_q$) Galois closure $\hat{X}$ of both is any $\mathbb{F}_q$ component of $\hat{X}_1 \times_Z \hat{X}_2$. Attached group, $\hat{G} = \hat{G}_{(\varphi_1,\varphi_2)} = G(\hat{X}/Z)$: Fiber product of $G(\hat{X}_1/Z)$ and $G(\hat{X}_2/Z)$ over maximal $H$ through which they both factor.

## D(avenport)Pairs: new pr-except. correspondences

**Definition 16.** $(\varphi_1, \varphi_2)$ is a DP (resp. i(sovalent)DP) if $\varphi_1(X_1(\mathbb{F}_{q^t})) = \varphi_2(X_2(\mathbb{F}_{q^t}))$ for $\infty$-ly many $t$ (resp. ranges assumed with same multiplicity; T. Bluer's name).

### Equivalent to being a DP:

$X_1 \times_Z X_2 \xrightarrow{\text{pr}_{X_i}} X_i$, is pr-exceptional, and the exceptionality sets $E_{\text{pr}_i}(\mathbb{F}_q)$, $i = 1, 2$, have nonempty (so infinite) intersection

$$E_{\text{pr}_1}(\mathbb{F}_q) \cap E_{\text{pr}_2}(\mathbb{F}_q) \stackrel{\text{def}}{=} E_{\varphi_1,\varphi_2}(\mathbb{F}_q).$$

## Part IV: (Chow) motives: Diophantine category of Poincare series over $(Z, \mathbb{F}_q)$

Let $W_{D,\mathbb{F}_q}(u) = \sum_{t=1}^{\infty} N_D(t) u^t$ be a Poincaré series for a diophantine problem $D$ over a finite field $\mathbb{F}_q$. We call these *Weil vectors*. Example: $F(\boldsymbol{x}, \boldsymbol{z}) \in \mathbb{F}_q[\boldsymbol{x}, \boldsymbol{z}]$,

$$N_D(t) = |\{\boldsymbol{z} \in \mathbb{F}_{q^t}^{m_{\boldsymbol{z}}} \mid \exists \boldsymbol{x} \in \mathbb{F}_{q^t}^{m_{\boldsymbol{x}}}, F(\boldsymbol{x}, \boldsymbol{z}) = 0\}|.$$

*Weil Relation* between $W_{D_1,\mathbb{F}_q}(u)$ and $W_{D_2,\mathbb{F}_q}(u)$: $\infty$-ly many coefficients of $W_{D_1,\mathbb{F}_q}(u) - W_{D_2,\mathbb{F}_q}(u)$ equal 0. Effectiveness result: For any Weil vector, the support set of $t \in \mathbb{Z}$ of 0 coefficients differs by a finite set from a union of full Frobenius progressions.

## Motivic formulation

**Question 17.** If Poincare series of $X$ over $\mathbb{F}_q$ has $t$-th coefficient equal $q^t + 1$ for $\infty$-ly many $t$, is there a chain of except. correspondences from $X$ to $\mathbb{P}^1$?

Equivalent to characterizing $X$ for which $\sum_{t=1}^{\infty} \mathrm{tr}_{\mathrm{Fr}_{q^t}}[\sum_0^2 (-1)^i H_\ell^i(X)]u^t$ has a relation with the series with $X = \mathbb{P}^1$: *Chow motive* coefficients.

There are $p$-adic versions: Replace $\mathbb{F}_{q^t}$ by higher residue fields with the Witt vectors $R_t$ with residue class $\mathbb{F}_{q^t}$; and use integration instead of counting.

## Result of Denef-Loeser [Fr77], [DL01], [Ni04]

Consider a number field version, by $R_{\boldsymbol{p}}$ the completion the integers of $K$ with respect to prime $\boldsymbol{p}$. Then, $W_{D,R_{\boldsymbol{p}}}(u) \stackrel{\text{def}}{=} \sum_{v=1}^{\infty} N_{D,R_{\boldsymbol{p}}}(v)u^v$ with $N_{D,R_{\boldsymbol{p}}}(v)$ using values in $R_{\boldsymbol{p}}/\boldsymbol{p}^v$ that lift to values in $R_{\boldsymbol{p}}$. To make this useful motivically requires doing this for those $D$ with a map to a fixed space $Z/K$.

Given $D$, There is a string of — relative to $Z$ — Chow motives (over $K$) $\{[M_v]\}_{v=0}^{\infty}$, so for almost all $\boldsymbol{p}$, $W_{D,R_{\boldsymbol{p}}}(u) = \sum_{t=1}^{\infty} \mathrm{tr}_{\mathrm{Fr}_{\boldsymbol{p}}}[M_t]u^t$.

## Role of iDPs

Given Weil Vector $W(D, \mathbb{F}_q)$ over $(Z, \mathbb{F}_q)$ and $\varphi : X \longrightarrow Z$ can define *pullback* $W^{\varphi}(D, \mathbb{F}_q)$ over $(X, \mathbb{F}_q)$.

Assume $\varphi_i : X_i \longrightarrow Z$, $i = 1, 2$, is an iDP over $\mathbb{F}_q$, $X_1 = X_2$ and $D$ has a map to $Z$. Then, $(\varphi_1, \varphi_2)$ produces new Weil vectors $W^{\varphi_i}_{D,\mathbb{F}_q}$, $i = 1, 2$, and a *relation* between $W^{\varphi_1}_{D,\mathbb{F}_q}(u)$ and $W^{\varphi_2}_{D,\mathbb{F}_q}(u)$: $\infty$-ly many coefficients of $W^{\varphi_1}_{D,\mathbb{F}_q}(u) - W^{\varphi_2}_{D,\mathbb{F}_q}(u)$ equal 0.

## Part V: CM and $\mathrm{GL}_2$ exceptional genus 0 covers

Test for a cover $\varphi : X \to Z$ decomposing. Check $X \times_Z X \setminus \Delta$ for irreducible components $Z$ of form $X' \times_Z X'$. If none, then $\varphi$ is indecomposable. Otherwise, $\varphi$ factors through $X' \to Z$ (Gutierrez, et.al. from [FrM69]).

Denote the minimal Galois extension of $K$ over which $\varphi$ decomposes into absolutely indecomposable covers by $K_\varphi(\text{ind})$: The indecomposability field of $\varphi$.

**Proposition 18.** *For any cover $\varphi : X \to Z$ over a field $K$, $K_\varphi(\mathrm{ind}) \subset \hat{K}_\varphi(2)$.*

# Most of rest of genus 0 except. covers/$\mathbb{Q}$

[Fr78], [GSM04]: From Weierstrass $\wp$-functions.

$$\begin{array}{ccc} \mathbb{P}^1_{\pm w} & \xrightarrow{f} & \mathbb{P}^1_{\{\pm z\}} \\ \text{mod } \{\pm 1\} \uparrow & & \uparrow \text{mod } \{\pm 1\} \\ \mathbb{C}_w/L_w & \xrightarrow{\text{mod } L_z/L_w} & \mathbb{C}_z/L_z. \end{array}$$

- Case CM: $\deg(f) = r$, a prime
- Case $\mathrm{GL}_2$: $\deg(f) = r^2$, a prime squared

[O67], [Se68], [Se81], [R90], [Se03] $\Leftrightarrow$ case of Serre's O(pen)I(mage)T(heorem). CM case can describe inversion period from "Euler's Theorem," essentially equivalent to the theory of complex multiplication.

## $\mathbf{GL}_2$ gist [Fr05, §6.1-.2], Serre's $\mathbf{GL}_2$ OIT [Se68, etc]

- $[f] \mapsto \mathbb{P}^1_j$ by the $j$-invariant of the 4 branch points;
- $G_f = (\mathbb{Z}/r)^2 \times^s \{\pm 1\}$; yet
- for a non-CM $j$-invariant (say in $\mathbb{Q}$), then for a.a. $r$, then for $f \stackrel{\text{def}}{=} f_{j,r}$, $\hat{G}_f = (\mathbb{Z}/r)^2 \times^s \mathrm{GL}_2(\mathbb{Z}/r)$.

Exceptionality versus indecomposability: Given $f_{j,r}$ and the set $\mathcal{A}$ of $A \in \mathrm{GL}_2(\mathbb{Z}/r)/\{\pm 1\}$ for which $A$ acts irreducibly on $(\mathbb{Z}/r)^2$. Consider $P_{f_{j,r},\mathcal{A}}$ those primes $p$ with the Frobenius of $f_{j,r} : \mathbb{P}^1_w \to \mathbb{P}^1_z \mod p$ in $\mathcal{A}$. For such $p$

- $f_{j,r} \mod p$ is exceptional; and (equivalently)
- $f_{j,r} \mod p$ is indecomposable, but decomposes over $\bar{\mathbb{F}}_p$.

## Two automorphic function questions

[Fr05,§6] poses an analog of [Se03] to find an automorphic funct. (should exist according to Langlands) for primes of except. for $j \leftrightarrow$ Ogg's curve $3^+$ [Se81, extensive discuss]. Would give an explicit structure to the primes of exceptionality.

For any exceptional $f_{j,r} \mod p$, form a Poincaré series with the period of exceptionality its coefficients. Conjecture, this series is rational. This result would then remove from consideration the arbitrary identification of $\mathbb{P}^1_w$ with $\mathbb{P}^1_z$.

# Bibliography; Parts 0 and I:


- [DL63] H. Davenport and D.J. Lewis, *Notes on Congruences (I)*, Quart. J. Math. Oxford **(2) 14** (1963), 51–60.
- [Fr70] M.D. Fried, *On a conjecture of Schur*, Mich. Math. J. **17** (1970), 41–45.
- [Fr74] M. Fried, *On a Theorem of MacCluer*, Acta. Arith. **XXV** (1974), 122–127.
- [Fr78] M. Fried, *Galois groups and Complex Multiplication*, T.A.M.S. **235** (1978) 141–162.
- [Fr05] M. Fried, *The place of exceptional covers among all diophantine relations*, J. Finite Fields **11** (2005) 367–433.
- [GMS03] R. Guralnick, P. Müller and J. Saxl, *The rational function analoque of a question of Schur and exceptionality of permutations representations*, Memoirs of AMS **162** 773 (2003),ISBN 0065-9266.
- [LMT93] R. Lidl, G.L. Mullen and G. Turnwald, *Dickson Polynomials*, Pitman monographs, Surveys in pure and applied math,**65**, Longman Scientific, 1993.
- [GLTZ07] R. Guralnick, T. Tucker and M. Zieve (behind the scenes Lenstra), *Exceptional covers and bijections on Rational Points*, to appear IRMN, 2007.
- [Mc67] C. MacCluer, *On a conjecture of Davenport and Lewis concerning exceptional polynomials*, Acta. Arith. **12** (1967), 289–299.
- [Sch23] I. Schur, Über den Zusammenhang zwischen einem Problem der Zahlentheorie and einem Satz über algebraische Functionen, S.-B. Preuss. Akad. Wiss., Phys.-Math. Klasse (1923), 123–134.

# Bibliography; Parts II and V:


- [DL01] J. Denef and F. Loeser, *Definable sets, motives and $p$-adic integrals*, JAMS **14** (2001), 429–469.
- [Fr76] M. Fried, *Solving diophantine problems over all residue class fields of a number field . . .*, Annals Math. **104** (1976), 203–233.
- [FGS93] M.D. Fried, R. Guralnick and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. **82** (1993), 157–225.
- [GTZ07] R. Guralnick, T. Tucker and M. Zieve, *Exceptional covers and bijections on rational points*, to appear in IRMN.
- [Le95] H.W. Lenstra Jr., *Talk at Glasgow conference, Finite Fields III*, (1995).
- [Ni04] J. Nicaise, *Relative motives and the theory of pseudo-finite fields*, to appear in IMRN.
- [O67] A.P. Ogg, *Abelian curves of small conductor*, Crelle's J **226** (1967), 204–215.
- [R90] K. Ribet, *Review of new edition of [Se68]*, BAMS **22** (1990), 214–218.
- [Se68] J.-P. Serre, *Abelian $\ell$-adic representations and elliptic curves*, 1st ed., McGill University Lecture Notes, Benjamin, New York • Amsterdam, 1968, in collaboration with Willem Kuyk and John Labute.
- [Se81] J.-P. Serre, *Quelques Applications du Théorème de Densité de Chebotarev*, Publ. Math. IHES **54** (1981), 323–401.
- [Se03] J.-P. Serre, *On a Theorem of Jordan*, BAMS **40** #4 (2003), 429–440.