Iteration Dynamics from Cryptology on Exceptional Covers

Mike Fried, UCI 05/20/08

Part 0: Exceptionality and fiber products

Part I: Generalization of Davenport-Lewis Criterion

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

Part III: Subtowers generated by Serre's O(pen) I(mage) T(heorem): **CM** part or **GL** part.

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

Part V: Generalizing: Pr-exceptionality and Davenport pairs

Part 0: Exceptionality and fiber products

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

With p prime, $q = p^u$, an $\mathbb{F}_q$ cover $\varphi : X \to Z$ of *absolutely irreducible normal varieties* is *exceptional* if φ one-one on $\mathbb{F}_{q^t}$ points for infinitely many t.

For a # field: φ has infinitely many exceptional residue class field reductions. Use $n_\varphi = n$ for $\deg(\varphi)$.

Definition 1. φ is *indecomposable* or *primitive* if φ does not factor through a lower degree (≥ 2) cover of Z over $\mathbb{F}_q$.

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 $\bar{\mathbb{F}}_q$. It 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 the *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 $X^2_Z \setminus \Delta$.

$X^{n_\varphi}_Z \setminus \Delta$: n_φth iterate of the fiber product minus the *fat diagonal*.

Galois closure of φ over K: Any K component, $\hat{X}$, of $X^n_Z \setminus \Delta$. Galois group $G(\hat{X}/Z) \stackrel{\text{def}}{=} \hat{G}_\varphi$: subgroup of S_n fixing $\hat{X}$.

Group Fact: φ primitive $\Leftrightarrow$ $\hat{G}_\varphi$ primitive. Stabilizer:

$$\hat{G}_\varphi(1) = \{g \in \hat{G}_\varphi | g(1) = 1\} : \text{acts on } \{2, \dots, n\}.$$

Without $\hat{}$, G_φ, denotes *absolute* Galois closure.

Part I: Generalization of Davenport-Lewis Exceptionality Criterion

Cyclic polynomials: $x \longrightarrow x^n$ as in RSA coding.

Proposition 2. *If $(n, p-1) = 1$, can use x^n to scramble data into $\mathbb{Z}/p$. For n odd, ∞-ly many such primes p.*

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

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

- $(k, n) = 1$ (Dirichlet's Thm. gives ∞-ly many p);
- $(k-1, n) = 1$ $((p - 1 = k - 1 + m \cdot n, n) = 1)$.

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 3. *If* $(n,6)=1$*, then* $T_n : \mathbb{Z}/p \to \mathbb{Z}/p$ *is exceptional* mod p *for those* 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 in modern algebra is from the middle of the 1800s. Used finite fields as the place to encode a message.

Conjecture 4 (Schur 1921). Only compositions of cyclic, Tchebychev and degree 1 ($x \mapsto ax + b$) give polynomials mapping 1-1 on $\mathbb{Z}/p$ for ∞-ly many p. (Solved [Fr69].)

Problem 5. 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 ∞ of p (notation: $1\text{–}1_\infty$)?

Cover characterization of exceptionality

Proposition 6. [DL63] $\to$ [Mc67] $\to$ [Fr74] $\to$ [Fr05] $\to$ [GLTZ07]: *General* $\mathbb{F}_q$ *cover of normal varieties:* $\varphi : X \to Z$ *exceptional over* $\mathbb{F}_{q^t}$ $\Leftrightarrow X^2_Z \setminus \Delta$ *has no* $\mathbb{F}_{q^t}$ *abs. irred. components.*

Equivalently: Each orbit of $\hat{G}_\varphi(1)$ on $\{2, \dots, n_\varphi\}$ breaks into (strictly) smaller orbits of $G_\varphi(1)$.

Absolutely indecomposable: For $\varphi(x) \in K[x]$, $(\mathrm{char}(K), n_\varphi) = 1$, φ primitive over $K \Leftrightarrow$ over $\bar{K}$. This is *not* true for $\varphi(x) \in K(x)$.

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

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

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

Each $\hat{K}_\varphi(k)/K$ is Galois: *kth 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

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

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

Theorem 7. *For K a finite field, $G(\hat{K}_\varphi(2)/K)$ having no fixed points under $T_{\varphi,2}$ characterizes φ 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 ψ from (X, φ) to (X', φ').

Then ψ 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, ψ) 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_φ; coset of 1 by v_φ 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 abs. irred. $X_1 \times_Z X_2$ comps.

Assume $(t, t_0) = 1$: $\Rightarrow X_1 \times_Z X_2$ has no abs. irr. comps. over $\mathbb{F}_{q^t}$. Normality $\implies X_1 \times_Z X_2(\mathbb{F}_{q^t}) = \emptyset$.

Then, $t \in (\mathbb{Z}/d(\varphi_i))^*$, $i = 1, 2$, $\implies \varphi_i$ is 1-1 and onto over $\mathbb{F}_{q^t}$, $i = 1, 2$. Weil: For t large $\Rightarrow$ $\exists z \in Z(\mathbb{F}_{q^t})$ and $\exists x_i \in X_i(\mathbb{F}_{q^t}) \mapsto z, i = 1, 2$.

Dav-Lew Crit. $\implies$ May assume φ_i s are étale. Contradiction: $(x_1, x_2) \in X_1 \times_Z X_2(\mathbb{F}_{q^t})$.

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

Proposition 8. *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 φ 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 9 (Periods). With $X = \mathbb{P}^1_x$ and $Z = \mathbb{P}^1_z$, identify them to regard φ on $\mathbb{F}_{q^t}$ as φ_t, permuting $\mathbb{F}_{q^t} \cup \{\infty\}$. Label the order of φ_t as $m_{\varphi,t} = m_t$. Then, $\varphi_t^{m_t-1}$ inverts φ_t. How does $m_{\varphi,t}$ vary, for genus 0 exceptional φ, as t varies?

Standard RSA inverts $x \mapsto x^n$ by inverting the nth 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^ns and T_ns. (For T_ns, "invert mult. by n" on $\mathbb{Z}/(q^{2t}-1)$.)

Part III: Subtowers generated by Serre's O(pen) I(mage) T(heorem): **CM** part or **GL** part.

Test for $\varphi : X \to Z$ decomposing. Check $X \times_Z X \setminus \Delta$ for irr. comps. of form $Z = X' \times_Z X'$. None $\Rightarrow \varphi$ is indecomposable. Otherwise, φ factors through $X' \to Z$ (Gutierrez, et.al. from [FrM69]).

Indecomposability field, $K_\varphi(\text{ind})$, of φ: Minimal Galois L/K over which φ decomposes no further.

Proposition 10. *For any cover $\varphi : X \to Z$ over a field K, $K_\varphi(\text{ind}) \subset \hat{K}_\varphi(2)$.*

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

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

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

- Case CM: $\deg(f) = r$, a prime
- Case 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 almost all r, and $f \stackrel{\text{def}}{=} f_{j,r}$, $\hat{G}_f = (\mathbb{Z}/r)^2 \times^s \mathrm{GL}_2(\mathbb{Z}/r)$.

Let Fr_p be the Frobenius of a prime p in $f_{j,r} : \mathbb{P}^1_w \to \mathbb{P}^1_z \mod p$. Exceptionality versus indecomposability:

$\mathcal{A}_r \stackrel{\text{def}}{=} \{A \in \mathrm{GL}_2(\mathbb{Z}/r)/\{\pm 1\} | A$ fixs no dim. 1 space in $(\mathbb{Z}/r)^2\}$.

$P_{f_{j,r},\mathcal{A}_r} \stackrel{\text{def}}{=} \{p | \mathrm{Fr}_p \in \mathcal{A}_r\}$. For $p \in P_{f_{j,r},\mathcal{A}_r}$:

- $f_{j,r} \mod p$ 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 $\mathbb{P}^1_z$.

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: $F(\boldsymbol{x}, \boldsymbol{z}) \in \mathbb{F}_q[\boldsymbol{x}, \boldsymbol{z}]$,

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

Weil Relation between $W_{D_1,\mathbb{F}_q}(u)$ and $W_{D_2,\mathbb{F}_q}(u)$: ∞-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 11. If Poincare series of X over $\mathbb{F}_q$ has t-th coefficient equal $q^t + 1$ for ∞-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, $W_{D,R_{\boldsymbol{p}}}(u) \stackrel{\mathrm{def}}{=} \sum_{v=1}^{\infty} N_{D,R_{\boldsymbol{p}}}(v)u^v$ 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 $\boldsymbol{p}$, $W_{D,R_{\boldsymbol{p}}}(u) = \sum_{t=1}^{\infty} \mathrm{tr}_{\mathrm{Fr}_{\boldsymbol{p}}}[M_t]u^t$.

Part V: Generalizing: Pr-exceptionality and Davenport pairs

Definition 12. $\varphi : X \to Z$ is *p(ossibly)r(educible)-exceptional*: $\varphi : X(\mathbb{F}_{q^t}) \to Z(\mathbb{F}_{q^t})$ surjective for ∞-ly many t.

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

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 ∞-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 ∞-ly many t.

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

Definition 13. (φ_1, φ_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 ∞-ly many t (resp. ranges assumed with same multiplicity; T. Bluer's name).

Equivalent to being a DP:

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

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

Role of iDPs

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

Assume $\varphi_i : X_i \to Z$, $i = 1, 2$, is an iDP over $\mathbb{F}_q$, $X_1 = X_2$ and D has a map to Z. Then, (φ_1, φ_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 $W^{\varphi_2}_{D,\mathbb{F}_q}(u)$: ∞-ly many coefficients of $W^{\varphi_1}_{D,\mathbb{F}_q}(u) - W^{\varphi_2}_{D,\mathbb{F}_q}(u)$ equal 0.

Bibliography; Parts 0, I, II:

- [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.
- [Fr05] M. Fried, *The place of exceptional covers among all diophantine relations*, J. Finite Fields **11** (2005) 367–433.
- [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.
- [Fr78] M. Fried, *Galois groups and Complex Multiplication*, T.A.M.S. **235** (1978) 141–162.
- [FGS93] M.D. Fried, R. Guralnick and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. **82** (1993), 157–225.
- [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.
- [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 ℓ-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.