Asymptotics for prime specialization over finite fields

B. Conrad
(joint with K. Conrad, R. Gross)

A classical (hard) question

Consider a polynomial in $\mathbf{Z}[T]$ of degree $d \geq 1$,

$$f(T) = c_d T^d + \cdots + c_1 T + c_0.$$

Question. Is $f(n)$ prime in $\mathbf{Z}$ (< 0 allowed) for infinitely many $n \in \mathbf{Z}$?

Example. Primes of the form $n^2 + 1$.

Example Prime of the form $n^2 - n + 2$. These are *even*, hence prime only finitely often ($n = 0, 1$).

Example Primes of the form $5n - 7$.

There is not a single f with $\deg(f) > 1$ *for which an affirmative answer is proved!*

The classical conjecture

For $f(T) = c_d T^d + \cdots + c_1 T + c_0$, if $f(n)$ is prime infinitely often then $f(T)$ is irreducible in $\mathbf{Z}[T]$.

But $h(T) = T^2 - T + 2$ is irreducible and $h(n)$ is always even.

Definition. Say $f(T)$ has a *local obstruction* at p if $p | f(n)$ for all n.

Conjecture. (Hardy–Littlewood) *For irreducible $f \in \mathbf{Z}[T]$ with no local obstructions,*

$$\pi_f(x) := \#\{1 \leq n \leq x : f(n) \text{ prime}\} \stackrel{?}{\sim} \frac{C(f)}{\deg f} \cdot \frac{x}{\log x}$$

where $C(f) > 0$ is a certain infinite product over primes.

Not even "$\pi_f(x) \to \infty$" is proved for a single f with $\deg(f) > 1$.

An analogy

For a prime p, let $\mathbf{F}_p$ be the finite field of integers mod p.

Example. $\mathbf{F}_5 = \{0, 1, 2, 3, 4\}$, $2 + 4 = 1$, etc.

There is a dictionary between $\mathbf{Z}$ and $\mathbf{F}_p[u]$. For example:

- The rings $\mathbf{Z}$ and $\mathbf{F}_p[u]$ share algebraic and *finiteness* properties.
- The analogue of "prime number" in $\mathbf{Z}$ is "irreducible polynomial" in $\mathbf{F}_p[u]$.

Example. Determining if an integer is squarefree is analogous to determining if a polynomial in $\mathbf{F}_p[u]$ has repeated irreducible factors or not.

To check if $n \in \mathbf{Z}$ is squarefree, must *factor* n.

For $h(u) \in \mathbf{F}_p[u]$ just compute $\gcd(h(u), h(u)')$: no factoring!

Why consider $\mathbf{F}_p[u]$?

Problems over $\mathbf{Z}$ often have analogues over $\mathbf{F}_p[u]$, and we may get insight or make progress this way.

- Elements of $\mathbf{F}_p[u]$ are functions on a "line"; can access geometric techniques unavailable in $\mathbf{Z}$.

- There are more operations, such as differentiation $h(u) \mapsto h'(u)$ (no analogue in $\mathbf{Z}$).

- Generalized Riemann Hypothesis is *proved* for function fields over finite fields, by work of Weil, Grothendieck, Deligne. It gives the best "proved evidence" for usual Riemann Hypothesis (in $\mathbf{Z}$), and suggests how to think about the Riemann Hypothesis and its conjectural generalizations.

$\mathbf{F}_p[u]$-analogue of the classical question

Fix a prime p. The analogue of $\mathbf{Z}[T]$ is $\mathbf{F}_p[u][T] = \mathbf{F}_p[u,T]$.

$$f(T) \stackrel{\text{def}}{=} f(u,T) = c_d(u)T^d + \cdots + c_1(u)T + c_0(u).$$

Question. When should

$$f(g(u)) \stackrel{\text{def}}{=} f(u,g(u)) = \sum c_j(u)g(u)^j$$

be prime (i.e., irreducible) in $\mathbf{F}_p[u]$ for infinitely many $g \in \mathbf{F}_p[u]$?

Analogue of classical "sampling" of values at $1 \leq n \leq x$ as $x \to \infty$ is "sampling" values of $f(u,T)$ at $g \in \mathbf{F}_p[u]$ with $\deg(g) \leq D$ as $D \to \infty$. This is a *finite* sampling space.

The study of this Question reveals features unlike anything known (or expected) in the classical case. It has consequences for abelian varieties over global function fields.

Counting prime values in $\mathbf{F}_p[u]$

Let

$$f(T) = c_d(u)T^d + \cdots + c_1(u)T + c_0(u)$$

be in $\mathbf{F}_p[u][T]$. Count by *separate degrees*; for $m \geq 0$,

$$\pi_f(m) := \#\{g \in \mathbf{F}_p[u] : \deg(g) = m, f(g) \text{ prime}\} < \infty.$$

Example. $f(T) = T^3 + u^2T^2 + u$ over $\mathbf{F}_2[u]$.

g	$f(g)$
1	$u^2 + u + 1$
u	$u(u^3 + u^2 + 1)$
$u + 1$	$u^4 + u^3 + 1$
u^2	u
$u^2 + 1$	$u^4 + u + 1$
$u^2 + u$	$u(u^2 + u + 1)^2$
$u^2 + u + 1$	$u^5 + u^4 + u^3 + u^2 + 1$

$$\pi_f(0) = 1, \pi_f(1) = 1, \pi_f(2) = 3, \cdots, \pi_f(10) = 68.$$

$T^{12} + (u+1)T^6 + u^4$ over $\mathbf{F}_3[u]$

m	Actual	Approx.	Ratio
1	2	1.603	1.248
2	6	2.404	2.496
3	6	4.808	1.248
4	20	10.818	1.849
5	30	25.963	1.155
6	80	64.907	1.233
7	250	166.904	1.498
8	572	438.125	1.306
9	1624	1168.332	1.390
10	4228	3154.498	1.340
11	11248	8603.175	1.307
12	31202	23658.732	1.319
13	87114	65516.488	1.330
14	244246	182510.217	1.338

Ratios seem to tend to ≈ 1.33, not 1!

$T^3 + u$ over $\mathbf{F}_3[u]$

m	Actual	Approx.	Ratio
1	2	2.00	1
2	6	3.00	2
3	6	6.00	1
4	0	13.50	0
5	36	32.40	1.111
6	144	81.00	1.778
7	216	208.29	1.037
8	0	546.75	0
9	1404	1458.00	0.963
10	7776	3936.60	1.975
11	10746	10736.18	1.001
12	0	29524.50	0
13	82140	81760.25	1.005
14	455256	227760.43	1.999

Ratios appear to have *four* interlaced statistics!

Is $\pi_f(m) = 0$ for $m \equiv 0 \bmod 4$, $m > 0$?

$T^5 + u^3$ over $\mathbf{F}_5[u]$

m	Actual	Approx.	Ratio
1	4	4.0	1
2	0	10.0	0
3	0	33.3	0
4	0	125.0	0
5	0	500.0	0
6	0	2083.3	0
7	0	8928.6	0
8	0	12686.5	0
9	0	173611.1	0
10	0	781250.0	0
11	0	3551136.4	0
12	0	16276041.7	0
13	0	75120192.3	0
14	0	348772321.4	0

Polynomial is irred. and has no local obstructions.

Does it have irred. values only *finitely many* times?!?

Observations

Analogue of Hardy–Littlewood:

$$\pi_f(m) \overset{?}{\sim} \frac{C(f)}{\deg_T f} \cdot \frac{(p-1)p^m}{\log(p^m)}.$$

Properties of apparent counterexamples:

- Such $f(T)$ is a polynomial in T^p (but not conversely).
- The ratio appears to fall into 1, 2, or 4 interlaced limiting sequences depending on $\deg g$ mod 4.
- Those 1, 2, or 4 limits appear to lie in $\mathbf{Q} \cap [0, 2]$.

The key discovery is a new *global* obstruction to primality/irreducibility with no classical analogue.

Get computable "correction factor" $\Lambda_f(m) \in \mathbf{Q} \cap [0, 2]$ to predict $\pi_f(m)$, and the main theorem is that it depends on m mod 4 for $m \gg 0$.

The Möbius function

Are factorization properties of $f(n)$ "random"?

Example. How often does n^2+1 have an even or odd number of prime factors (for $1 \le n \le x$, $x \to \infty$)?

The classical *Möbius function* $\mu_{\mathbf{Z}} : \mathbf{Z} \to \{0, 1, -1\}$ is:

$$\mu_{\mathbf{Z}}(m) \stackrel{\text{def}}{=} \begin{cases} 0, & \text{if } p^2|m, \\ (-1)^r, & \text{if } m = \pm p_1 \cdots p_r. \end{cases}$$

Example. Parity of prime-factor counting for n^2+1 is governed by asymptotics for $(1/x)\sum_{1 \le n \le x} \mu_{\mathbf{Z}}(n^2+1)$ as $x \to \infty$. Mysterious!

For nonzero h in $\mathbf{F}_p[u]$, define the Möbius function

$$\mu(h) \stackrel{\text{def}}{=} \begin{cases} 0, & \text{if } \pi^2|h, \\ (-1)^r, & \text{if } h = \pi_1 \cdots \pi_r. \end{cases}$$

We will see that μ is a lot more tractable than $\mu_{\mathbf{Z}}$!

Global obstruction via Möbius bias

Main point: for $f \in \mathbf{F}_p[u][T^p]$, $\mu(f(u, g(u)))$ will be a *non-random* quantity as g varies.

Example. Recall the polynomial (with "4/3 discrepancy")

$$f(T) = T^{12} + (u+1)T^6 + u^4 \in \mathbf{F}_3[u][T].$$

We prove $\mu(f(g)) = -1$ twice as often as $\mu(f(g)) = 1$ (when $f(g)$ is squarefree), so the "average" nonzero value of $\mu(f(g))$ is $-1/3$, and this deviates from 1 by $1 - (-1/3) = 4/3$. Aha!

Qualitative principle: if $\mu(f(g))$ is "skewed" toward -1 as g varies, then $f(g)$ should be more likely to be irreducible than Hardy–Littlewood predicts.

Quantitative idea: use a suitable "average" of $\mu(f(g))$ to define a correction factor. Does such an average have good mathematical properties?

Proved counterexample

The "4/3" example is merely suggestive that Hardy–Littlewood fails and a Möbius average provides the right correction factor. We can do better:

Example. For $f(T) = T^5 + u^3 \in \mathbf{F}_5[u][T]$ we prove $\mu(f(g)) \neq -1$ if $\deg g > 1$. Thus, $f(g)$ is reducible for all such g, so the Hardy–Littlewood analogue conjecture is provably false.

There is *no formula* for how to factor $g(u)^5 + u^3$. We infer reducibility through understanding $\mu(g(u)^5 + u^3)$.

How can we prove anything about $\mu(f(g))$ as g varies? In contrast, $\mu_{\mathbf{Z}}(n^2 + 1)$ is intractable.

The starting point is *Swan's formula*: computes $\mu(h)$ by a mechanism unrelated to factoring, instead using structures related to to algebraic geometry over $\mathbf{F}_p$.

Swan's formula ($p \neq 2$)

For $h \in \mathbf{F}_p[u]$, let $d = \deg h$ and let $\mathrm{lead}(h)$ denote the leading coefficient of h.

Let $\chi_p : \mathbf{F}_p \to \{0, 1, -1\}$ be the "quadratic character": $\chi_p(0) = 0$, $\chi_p(c) = 1$ if $c \in \mathbf{F}_p$ is a nonzero square, $\chi_p(c) = -1$ if $c \in \mathbf{F}_p$ is not a square.

If $h' \neq 0$ we have *Swan's formula*:

$$\mu(h) = (-1)^d \chi_p \left(\frac{(-1)^{\frac{d(d-1)}{2}}}{\mathrm{lead}(h)^{\deg h + \deg h'}} \cdot \mathrm{Res}(h, h') \right).$$

Example. In the special case $h = f(u, g(u))$ with $f(u, T) \in \mathbf{F}_p[u, T^p]$, the Chain Rule gives

$$h' = (\partial_u f)(u, g) + (\partial_T f)(u, g) g' = (\partial_u f)(u, g)$$

because $\partial_T f = 0$ (characteristic p with $f \in \mathbf{F}_p[u, T^p]$!).

Significance. For $h = f(g)$,

$$\mathrm{Res}(h, h') = \mathrm{Res}(f(g), (\partial_u f)(g))$$

is an *algebraic* function of g (for $\deg g \gg 0$).

To understand this function of g, we study the geometry of its zero locus on the space of g's of fixed degree.

Main periodicity theorem ($p \neq 2$)

Pick a squarefree $f(T) \in \mathbf{F}_p[u][T]$ with $f \in \mathbf{F}_p[u][T^p]$, $p \neq 2$. Swan's formula for $\mu(f(g))$ can be replaced with a much better formula, using the geometry of the plane curve $\{f = 0\}$. Let B be its set of branch points over T-axis.

Let $M_f \in \mathbf{F}_p[u]$ be the monic polynomial whose (geometric) roots are the u-coordinates of points of B.

Periodicity Theorem. *For f as above, there is a formula for $\mu(f(g))$ that only depends on $g \bmod M_f$, $\deg g \bmod 4$, and $\mathrm{lead}(g) \bmod \square$ for $\deg g \gg 0$.*

Example. Let $f(T) = T^9 + (2u^4 + u^3 + u + 2)T^6 + 2$ in $\mathbf{F}_3[u][T]$, and χ_3 be the quad. character on $\mathbf{F}_3$. Then $M_f(u) = u - 1$, and for $g(u) = cu^n + \cdots$ in $\mathbf{F}_3[u]$ ($n > 0$),

$$\mu(f(g)) = (-1)^n(\chi_3(-1))^{n(n-1)/2}\chi_3(c)\chi_3(g(1) + 2).$$

This only depends on $g \bmod (u - 1)$, $n \bmod 4$, and $c \bmod \square$.

Application to corrected conjecture ($p \neq 2$)

Modified H-L Conjecture for $\mathbf{F}_p[u]$. For $f \in \mathbf{F}_p[u][T^p]$ irreducible in $\mathbf{F}_p(u)[T]$ and without local obstructions,

$$\pi_f(n) \overset{?}{\sim} \Lambda_f(n) \cdot \frac{C(f)}{\deg_T f} \cdot \frac{(p-1)p^n}{\log(p^n)},$$

where

$$\Lambda_f(n) := 1 - \frac{\sum_{\deg g = n, \gcd(f(g), M_f)=1} \mu(f(g))}{\sum_{\deg g = n, \gcd(f(g), M_f)=1} |\mu(f(g))|}.$$

Though $\Lambda_f(n)$ *looks* horrible, averaging over g's of large degree n kills the dependence of $\mu(f(g))$ on

- $\mathrm{lead}(g) \bmod \square$ (since g exhausts both options equally often),
- $g \bmod M_f$ (g exhausts all congruence classes equally often for $n > \deg M_f$).

Upshot. Only the dependence of $\mu(f(g))$ on $\deg g \bmod 4$ survives! So despite appearances, $\Lambda_f(n)$ has period 1, 2, or 4 when $n \gg 0$.

Examples of Λ-periodicity ($p \neq 2$)

Here are examples of the tail of values $\Lambda_f(n)$ (first three over $\mathbf{F}_3[u]$, last over $\mathbf{F}_5[u]$), beginning with $n \equiv 1 \mod 4$:

Polynomial $f(T)$	$\Lambda_f(n)$ $(n \gg 0)$
$T^{12} + (u+1)T^6 + u^4$	4/3
$T^3 + u$	1, 2, 1, 0
$T^{12} + (u^4 + u^2 + 2u + 2)T^6 + 2$	18/25
$(2u^2 + u + 3)T^{15} + (4u^2 + u + 3)T^5$ $+(4u^2 + u + 3)$	13/10, 1

The right column fits numerical deviations from Hardy–Littlewood!

But we can ask more about $\Lambda_f(n) \ldots$

Asymptotic question

Katz philosophy. For $\mathbf{F}_p[u]$-analogues of classical problems over $\mathbf{Z}$, the "large finite field limit" should reflect the classical behavior.

Interpretation. Fix $f \in \mathbf{F}_p[u, T^p]$ as above, consider $f(u, g(u))$ for $g \in \mathbf{F}_{p^r}[u]$ with $r \to \infty$. Can define $\Lambda_{f,r}(n)$ for conjecture on $f(g)$'s with $g \in \mathbf{F}_{p^r}[u]$.

Let $\lambda_{f,r} : \mathbf{Z}/4\mathbf{Z} \to \mathbf{Q} \cap [0, 2]$ be the periodic tail of $\Lambda_{f,r}(n)$.

Example. Let $f(T) \in \mathbf{F}_3[u][T]$ be

$$f(T) = T^9 + (2u^2 + u)T^6 - (u + 1)T^3 + (u + 1)^2.$$

We have $\lambda_{f,r}(c) = 1$ for $c = 0, 2$, but for $c = 1, 3$:

$$\lambda_{f,r}(c) = \begin{cases} 1 + \frac{2 \cdot (-1)^{(c+1)/2}}{(3^r-1)(3^r-2)}, & r \text{ odd}, \\ 1 + \frac{2}{(3^r-1)(3^r-2)}, & r \text{ even}. \end{cases}$$

This depends on r, but $\lambda_{f,r}(c) \neq 1$ for odd c and $\lambda_{f,r}(c) \to 1$ as $r \to \infty$ for *all* $c \in \{0, 1, 2, 3\}$.

Asymptotic theorems I ($p \neq 2$)

What can be said about $\lim_{r\to\infty} \lambda_{f,r}(c)$ for fixed $c = 0, 1, 2, 3$?

Katz' philosophy suggests it should be 1, since we believe the classical Hardy–Littlewood conjecture!

Geometric information in the proof of Main Periodicity Theorem, coupled with point-counting on varieties over finite fields, gives:

Limit Theorem. *Fix $f \in \mathbf{F}_p[u][T^p]$ with no local obstructions. If $\{f = 0\}$ has non-empty branch locus B_f over the T-axis and some $x \in B_f$ has odd branch multiplicity, then $\lambda_{f,r}(c) \to 1$ as $r \to \infty$ for each c.*

Question 1. Are the branch locus hypotheses on f in the Limit Theorem generic, say if f varies in an algebraic family of polynomials?

Answer. Yes. By using Bertini theorems, if f varies in the algebraic family $\sum c_j(u)T^{pe_j}$ with each $\delta_j = \deg(c_j)$ fixed and some $\delta_{j_0} > 1$ then generic such f has $B_f \neq \emptyset$ and some $x \in B_f$ has multiplicity in $p^{\mathbf{Z}}$ (odd!).

Asymptotic theorems II ($p \neq 2$)

For "most" f, in the large finite-field limit the correction factors are very close to 1. Might they be identically 1?

Question 2. Is the phenomenon of non-trivial correction factors an artifact of working over small finite fields? Is the "correction-factor" function $\lambda_{f,r} : \mathbf{Z}/4\mathbf{Z} \to \mathbf{Q} \cap [0, 2]$ *not* identically 1 for infinitely many r?

To prove non-triviality properties of the function $\lambda_{f,r}$ on $\mathbf{Z}/4\mathbf{Z}$ for $r \to \infty$ and f generic in an algebraic family, we need a better understanding of this function.

Key point. The function $\lambda_{f,r}$ can be related to point-counting on a hyperelliptic curve over a finite field. The Riemann Hypothesis for such curves, together with some geometric arguments, provides estimates to ensure non-triviality:

Non-triviality Theorem. *Let $f(u, T)$ vary in an algebraic family whose generic member has $\deg_T f$ and $\deg_T \partial_u f$ both odd. For generic such f and sufficiently divisible r, the function $\lambda_{f,r}$ on $\mathbf{Z}/4\mathbf{Z}$ is not identically 1.*

Möbius periodicity proof I ($p \neq 2$)

The key to exploiting the Swan formula for $\mu(f(g))$ is to understand the quadratic nature of the *nonzero* values of the resultant function

$$R_n : g \mapsto \mathrm{Res}(f(g), (\partial_u f)(g)) \in \mathbf{F}_p,$$

an algebraic function on the space of g's of degree $n \gg 0$.

The geometric meaning of *vanishing* of resultants gives

$$R_n(g) = c_n(\mathrm{lead}(g))^{b_n} \prod_{x \in B} P_x(g \bmod M_f)^{e_{x,n}};$$

- B is branch locus of $\{f = 0\}$ over T-axis,
- $b_n, e_{x,n} \in \mathbf{Z}_{>0}$ and $c_n \in \mathbf{F}_p - \{0\}$ are abstract,
- P_x is an irreducible algebraic function on space of remainders $\mathbf{F}_p[u]/(M_f)$.

Key Problem. Understand c_n mod $\square$, b_n mod 2, and $e_{x,n}$ mod 2 as n varies.

Interlude: an explicit resultant formula

Let us give an example of the preceding resultant analysis.

Example. For $f(T) \in \mathbf{F}_3[u][T^3]$ given by

$$T^{12} + (u+1)T^6 + u^4,$$

the projection of $\{f = 0\}$ to the T-axis has as branch points

$$B = \{(0,0), (1, \pm\sqrt{-1})\}.$$

The respective intersection numbers $e_x = i_x(f, \partial_u f)$ at these branch points are

$$e_{(0,0)} = 18, \;\; e_{(1,\pm\sqrt{-1})} = 9.$$

For $g \in \mathbf{F}_3[u]$ with degree $n \gg 0$, the resultant

$$R_n(g) = \mathrm{Res}(f(g), (\partial_u f)(g))$$

is given by the formula

$$R_n(g) = (\mathrm{lead}(g))^{72n-36} g(0)^{18} (g(1)^2 + 1)^9.$$

Note the exponents 18 and 9: so $e_{x,n} = e_x$ when $n \gg 0$ for each $x \in B$. Moreover, the mystery coefficient c_n is 1, and the mystery exponent b_n is $72n - 36$ for large n.

Möbius periodicity proof II ($p \neq 2$)

We have a formula for $\mathrm{Res}(f(g), (\partial_u f)(g))$, $\deg g = n \gg 0$:

$$R_n(g) = c_n(\mathrm{lead}(g))^{b_n} \prod_{x \in B} P_x(g \bmod M_f)^{e_{x,n}} \in \mathbf{F}_p.$$

For $x \in B$, let e_x be intersection number for $\{f = 0\}$ and $\{\partial_u f = 0\}$ at x.

Local deformation theory along zero locus of resultant function R_n on space of g's implies $e_{x,n} \leq e_x$ for $n \gg 0$.

Global argument gives $\sum_x e_{x,n} = \sum_x e_x$ for $n \gg 0$, so $e_{x,n} = e_x$ for $n \gg 0$.

So by Swan, $\mu(f(g))$ rests on quadratic nature of $R_n(g)$: involves $g \bmod M_f$, $\mathrm{lead}(g) \bmod \square$, $c_n \bmod \square$, and $b_n \bmod 2$ ($n = \deg g$).

Do $c_n \bmod \square$ *and* $b_n \bmod 2$ *depend on* $n \bmod 4$ ($n \gg 0$)*?*

This analysis works for $\mathrm{Res}(f_1(g), f_2(g))$ with *any* plane curves $\{f_1 = 0\}$ and $\{f_2 = 0\}$ without common components. This yields b_n linear in n and $c_n = \beta_0 \beta_1^n$ for $\beta_0, \beta_1 \in \mathbf{F}_p^\times$ and $n \gg 0$. Gives desired dependence on $n \bmod 4$.

Higher genus and $p = 2$

Generalization I. We can replace $\mathbf{F}_p[u]$ with the coordinate ring of a higher-genus smooth affine curve C over $\mathbf{F}_p$ with one (geometric) point ξ at infinity, say with $p \neq 2$.

- Use genus-0 theory for squarefree norms $\mathrm{N}_\phi f \in \mathbf{F}_p[u][T^p]$ with many branched covers $\phi : C \to \{u\text{-line}\}$ tot. ramified over ∞.

- Weierstrass gaps at ξ obstruct algebraic methods. Use more geometry.

Generalization II. What about $p = 2$?

New structure intervenes in Periodicity Theorem: residues of differential forms! Get good result for polynomials in T^4; case of T^2 is mysterious.

Have to use formal and rigid geometry, non-algebraic 2-adic deformations into characteristic 0.

Asymptotic and non-triviality results for the correction factor carry over via more sophisticated methods, and numerics look good.