Irreducible Values of Polynomials: a Non-analogy

Keith Conrad

Department of Mathematics, Univ. of Connecticut, Storrs, CT 06269-3009 U.S.A.
kconrad@math.uconn.edu

1 Introduction

For a polynomial $f(T) \in \mathbb{Z}[T]$, the frequency with which the values $f(n)$ are prime has been considered since at least the 18-th century. Euler observed, in a letter to Goldbach in 1752, that the sequence $n^2 + 1$ has many prime values for $1 \leq n \leq 1500$. Legendre assumed an arithmetic progression $an + b$ with $(a, b) = 1$ contains infinitely many primes in his work on the quadratic reciprocity law. There is also the old question of twin prime pairs n and $n+2$, but we will focus here only on a *single* polynomial (in one variable).

An asymptotic estimate for

$$\pi_f(x) := |\{1 \leq n \leq x : f(n) \text{ is prime}\}| \tag{1}$$

as $x \to \infty$ amounts to a higher-degree generalization of the prime number theorem and Dirichlet's theorem. Conjectural estimates for $\pi_f(x)$ have been around since the work of Hardy and Littlewood in the early 20-th century, and this will be recalled later.

Hardy and Littlewood did not pursue a characteristic p version of this topic, but the framework is simple to set up. Let $\kappa[u]$ be the polynomial ring in one variable over a finite field κ. Given $f(T) = f(u, T)$ in $\kappa[u][T]$, how often is $f(g)$ irreducible in $\kappa[u]$ as g runs over $\kappa[u]$? We will see that it is trivial to translate Hardy and Littlewood's conjectural estimate for (1) into the setting of $\kappa[u]$, but a completely unexpected development will unfold: the Hardy–Littlewood conjecture in characteristic p is not always true! This discovery leads to new nontrivial theorems concerning polynomials over finite fields, and with these results the Hardy–Littlewood conjecture in characteristic p can be corrected. Moreover, the new understanding we gain in characteristic p leads to an interesting family of elliptic curves over $\kappa(u)$.

This paper is a summary of joint work. The results pertaining to the Hardy–Littlewood conjecture in characteristic p are joint work with B. Conrad and R. Gross [1]. The application to elliptic curves is joint work with B. Conrad

and H. Helfgott [2]. Full proofs and other details can be found in the references cited.

I thank the organizers of the conference on the analogy between number fields and function fields for a stimulating week on Texel Island.

2 The Classical Situation

Given a non-constant $f(T) \in \mathbb{Z}[T]$, there are two necessary conditions that f must satisfy in order for $f(n)$ to be prime infinitely often:

(1) $f(T)$ is irreducible in $\mathbb{Q}[T]$,
(2) no prime p divides $f(n)$ for every $n \in \mathbb{Z}$. (That is, for no p is the function $f\colon \mathbb{Z} \to \mathbb{Z}/(p)$ identically 0.)

The need for (1) is obvious. The role of (2) was first noticed by Bouniakowsky in 1854; it excludes examples (such as $T^2 - T + 2$) that are irreducible as polynomials yet have all values on $\mathbb{Z}$ containing a common prime factor (such as 2). We allow negative primes, so we do not require f to have a positive leading coefficient. Whereas (2) implies that $f(T)$ is primitive (i.e., its coefficients have no common factor), (2) is a strictly stronger condition than primitivity. We call (1) and (2) the *Bouniakowsky conditions*, and we consider the failure of (2) to be a local obstruction to the growth of $\pi_f(x)$. Condition (2) is equivalent to there being at least one pair of relatively prime values $f(m)$ and $f(n)$ for $m \neq n$, and this is how (2) is checked in practice.

Conjecture 2.1 (Bouniakowsky). For non-constant $f(T) \in \mathbb{Z}[T]$, $f(n)$ is prime for infinitely many $n \in \mathbb{Z}$ if and only if conditions (1) and (2) hold.

Bouniakowsky's conjecture is known for f of degree 1, but no instance of it has been established when $\deg f > 1$.

The Hardy–Littlewood conjecture (also called the Bateman–Horn conjecture) makes the Bouniakowsky conjecture quantitative.

Conjecture 2.2 (Hardy–Littlewood). If $f(T) \in \mathbb{Z}[T]$ satisfies both (1) and (2), then

$$\pi_f(x) \stackrel{?}{\sim} C(f) \sum_{n \leq x} \frac{1}{\log |f(n)|} \sim \frac{C(f)}{\deg f} \frac{x}{\log x},$$

where $C(f) = \prod_p (1 - \omega_f(p)/p)/(1 - 1/p)$ and $\omega_f(p)$ is the number of solutions to $f(n) = 0$ in $\mathbb{Z}/(p)$.

Remark 2.3. When f is irreducible, $C(f) = 0$ if and only if one of its factors is 0, which is exactly when condition (2) fails. Assuming (1) and (2), the product $C(f)$ converges, although only conditionally when $\deg f > 1$. Rapidly convergent formulas for the Hardy–Littlewood constant $C(f)$ can be obtained from L-functions by writing $\omega_f(p)$ in terms of character values on a Frobenius element at p in the splitting field of f over $\mathbb{Q}$.

3 The Characteristic p (Non)analogue

Let κ be a finite field. We consider polynomials $f(T) = f(u, T)$ in $\kappa[u][T]$ that have positive T-degree. Let

$$\pi_f(n) := |\{g \in \kappa[u] : \deg g = n, f(g) \text{ is irreducible in } \kappa[u]\}| .$$

(One might consider a count over $\deg g \leq n$, rather than over $\deg g = n$, to be more analogous to the classical setting. If so, two points are worth noting: (i) the number of g with degree n grows exponentially with n, so sampling by degree is substantive, and (ii) the new phenomenon we will see later is essentially impossible to describe if we count by $\deg g \leq n$.)

In order for $f(g)$ to be irreducible infinitely often in $\kappa[u]$, the appropriate Bouniakowsky conditions must hold:

(1) $f(T)$ is irreducible in $\kappa(u)[T]$,
(2) there are no local obstructions: no irreducible π in $\kappa[u]$ divides $f(g)$ for every $g \in \kappa[u]$.

The following conjecture is the obvious analogue of Conjecture 2.2. We call it the Naive Conjecture. In many cases it fits numerical data well, but there are cases where the conjecture is wrong, so the "Naive" label is important.

Conjecture 3.1. Let κ have size q. When $f(T) \in \kappa[u][T]$ satisfies conditions (1) and (2),

$$\pi_f(n) \stackrel{?}{\sim} C(f) \sum_{\deg g = n} \frac{1}{\deg f(g)} \sim \frac{C(f)}{\deg_T f} \frac{(q-1)q^n}{n}$$

as $n \to \infty$, where $C(f) = \prod_{(\pi)} (1 - \omega_f(\pi)/\mathrm{N}\pi)/(1 - 1/\mathrm{N}\pi)$, $\omega_f(\pi)$ is the number of solutions to $f = 0$ in $\kappa[u]/(\pi)$, and $\mathrm{N}\pi = |\kappa[u]/(\pi)| = q^{\deg \pi}$.

Remark 3.2. The convergence of $C(f)$ is proved just as in the classical case, and in particular depends on condition (2). Analogies between number fields and function fields suggest replacing $\deg f(g)$ in the denominator with

$$\log \mathrm{N}(f(g)) = (\log q)(\deg f(g)) .$$

Then $C(f)$ should be replaced with $(\log q)C(f)$ to maintain the same overall values on the right side. From the viewpoint of base-change properties, the product $(\log q)C(f)$ is in fact a better $\kappa[u]$-analogue of the classical Hardy–Littlewood constant than $C(f)$, and it is this product with $\log q$ which goes under the label $C(f)$ in [1].

When $\deg_T f = 1$, the Naive Conjecture is a theorem (an analogue of Dirichlet's theorem) and has been known for a long time. No case has been proved when $\deg_T f > 1$.

Numerical data when $\deg_T f > 1$, at first, present evidence in favor of the Naive Conjecture. But then we meet examples like those in the four tables below, which suggest the Naive Conjecture is *not* true in general. (In each table, the choice of $f(T)$ and κ is indicated along the top. The irreducibility of f over $\kappa(u)$ is left to the reader to check. Since $f(0)$ and $f(1)$ are relatively prime in $\kappa[u]$, the second Bouniakowsky condition is satisfied.)

In the headings of the tables, 'Naive Est.' means the expression on the right side of the $\sim^?$ in Conjecture 3.1, and 'Ratio' means the ratio of the two sides of the $\sim^?$, which should be tending to 1 if the Naive Conjecture is true. The ratios do not seem to be tending to 1 according to the data in the tables. In Table 1, the ratios seem to tend to 2 for odd n and equal 0 for even n. In Table 2, the ratios seem to be tending to the periodic values 1,2,1,0. In Table 3, the ratios appear to be tending to a number ≈ 1.33. In Table 4, it looks like $\pi_f(n) = 0$ for $n > 0$. (Clearly $\pi_f(0) = 5$.)

Table 1. $T^4 + u$ over $\mathbb{F}_2[u]$

n	$\pi_f(n)$	Naive Est.	Ratio
9	24	14.2	1.690
10	0	25.6	0
11	92	46.5	1.978
12	0	85.3	0
13	336	157.5	2.133
14	0	292.6	0
15	1076	546.1	1.970
16	0	1024.0	0

Table 2. $T^3 + u$ over $\mathbb{F}_3[u]$

n	$\pi_f(n)$	Naive Est.	Ratio
9	1404	1458.0	0.963
10	7776	3936.6	1.975
11	10746	10736.2	1.001
12	0	29524.5	0
13	82140	81760.2	1.005
14	455256	227760.4	1.999
15	637440	637729.2	1.000
16	0	1793613.4	0

Unlike the classical case over $\mathbb{Z}$, the Bouniakowsky conditions (1) and (2) over $\kappa[u]$ are apparently *not* sufficient to guarantee that $f(T)$ takes infinitely many irreducible values in $\kappa[u]$. In fact, the Bouniakowsky conditions over $\kappa[u]$

Table 3. $T^{12} + (u+1)T^6 + u^4$ over $\mathbb{F}_3[u]$

n	$\pi_f(n)$	Naive Est.	Ratio
9	1624	1168.3	1.390
10	4228	3154.5	1.340
11	11248	8603.2	1.307
12	31202	23658.7	1.319
13	87114	65516.5	1.330
14	244246	182510.2	1.338
15	683408	511028.6	1.337
16	1914254	1437268.0	1.332

Table 4. $T^{10} + u$ over $\mathbb{F}_5[u]$

n	$\pi_f(n)$	Naive Est.	Ratio
1	0	4.0	0
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
15	0	1627604166.7	0
16	0	7629394531.3	0

are not sufficient to guarantee that $f(T)$ takes any irreducible values. For an example in any $\kappa[u][T]$, let $f(T) = T^{4q} + u^{2q-1}$, where q is the size of κ. This polynomial is irreducible in $\kappa(u)[T]$ and $f(0)$ and $f(1)$ are relatively prime, so the Bouniakowsky conditions are satisfied. However, it can be proved that $f(g)$ is reducible for every $g \in \kappa[u]$. (We will see a proof in Example 4.3.) This example in the case $q = 2$ was found by Swan [7] over 40 years ago, but in a different context. It seems that nobody noticed the connection to a failure of the Hardy–Littlewood conjecture (and even the Bouniakowsky conjecture) in characteristic p.

Our explanation for the unexpected examples in the tables (and others that are not given here, including polynomials $f(T)$ which are not monic in T) is a new global obstruction that has no known counterpart in characteristic 0. This is the topic of the next section.

4 Möbius Fluctuations

We have found many examples that appear to deviate from the Naive Conjecture. These examples have two common properties:

(a) $f(T)$ is a polynomial in $\kappa[u][T^p]$, where p is the characteristic of κ,
(b) the sequence of ratios has interlaced limiting trends for $n \gg 0$, which fall into a cycle of 1, 2, or 4 limits. (See, respectively, Tables 3, 1, and 2.)

Not all polynomials in $\kappa[u, T^p]$ disagree (numerically) with the Naive Conjecture. For instance, $T^p + u^2$ over $\mathbb{F}_3[u]$, $\mathbb{F}_5[u]$, $\mathbb{F}_7[u]$, and $\mathbb{F}_9[u]$ appears to fit the Naive Conjecture. We expect that the Naive Conjecture is correct if $f(T) \notin \kappa[u][T^p]$, but we have not proved anything in that direction.

A closer examination of the data behind the four tables in the previous section reveals a more subtle third common property:

(c′) there is a Möbius bias: the non-zero values of $\mu(f(g))$, where μ is the Möbius function on $\kappa[u]$, are not ± 1 equally often.

The Möbius function on $\kappa[u]$ is defined by analogy with its classical counterpart: it vanishes on polynomials with a multiple irreducible factor and is ± 1 on squarefree polynomials in accordance with the parity of the number of (monic) irreducible factors.

Let us explain the meaning of (c′) through our four examples. In Table 1, we found numerically that $\mu(f(g)) = \mu(g^4 + u)$ is -1 when $\deg g$ is odd and is 1 when $\deg g$ is positive and even. In particular, if such a pattern persists, $g^4 + u$ must be reducible when $\deg g$ is positive and even since the Möbius value is not -1. In Table 2, we found numerically that $\mu(g^3 + u)$ is ± 1 equally often in each odd degree, while $\mu(g^3 + u) = -1$ for $\deg g \equiv 2 \bmod 4$ and $\mu(g^3 + u) = 1$ for $\deg g \equiv 0 \bmod 4$. In Table 3, we found numerically that $\mu(f(g))$ is -1 twice as often as it is 1 when sampling over g with a fixed degree ≥ 2. (While $\mu(f(g))$ can also vanish, the point is the apparent bias among non-zero values.) In Table 4, we found numerically that $\mu(f(g)) = 1$ when $\deg g > 0$. We can prove these numerically observed Möbius patterns are true in all degrees, as special cases of Theorem 4.4.

That biases in irreducibility statistics of $f(g)$ are linked to biases in non-zero values of $\mu(f(g))$ was our basic numerical discovery, but this link is a bit more subtle than the data so far suggest. Consider Table 5, where the ratio of irreducibility counts to the estimate coming from the Naive Conjecture seems to be approaching the limiting values $0, 1, 2, 1$. In particular, the Naive Conjecture looks good in even degrees. Consistent with this, computations suggest $\mu(f(g))$ is equally often ± 1 in even degrees. (As before, Möbius value 0 is not taken into account.) However, though the Naive Conjecture looks bad in odd degrees (bad in different ways depending on the degree modulo 4), it appears from computations that $\mu(f(g))$ is still equally often ± 1 in odd degrees. It turns out that property (c′) has to be amended (which is why it is called (c′) and not (c)). This will be treated later.

Table 5. $T^9 + (2u^2 + u)T^6 + (2u + 2)T^3 + u^2 + 2u + 1$ over $\mathbb{F}_3[u]$

n	$\pi_f(n)$	Naive Est.	Ratio
5	0	11.0	0
6	28	27.4	1.022
7	146	70.5	2.071
8	173	185.1	0.935
9	0	493.6	0
10	1345	1332.8	1.009
11	7348	3634.9	2.022
12	10138	9996.1	1.014
13	0	27681.4	0
14	77288	77112.5	1.002
15	432417	215915.0	2.003

In both $\mathbb{Z}$ and $\kappa[u]$, the definition of the Möbius function is useless for effective computations. But unlike the case over $\mathbb{Z}$, there is another formula for the Möbius function in $\kappa[u]$, and this does not require factoring.

Lemma 4.1. *When κ is a finite field with odd characteristic and $h \in \kappa[u]$ is non-zero,*

$$\mu(h) = (-1)^{\deg h}\chi(\operatorname{disc}_\kappa h)\,. \tag{2}$$

Here χ is the quadratic character on $\kappa^\times$, with $\chi(0) = 0$, and $\operatorname{disc}_\kappa h$ is the discriminant of h.

Proof. If h has a multiple irreducible factor, then the result is obvious since both sides vanish. Assume h is separable. Both sides are multiplicative functions of h, so it suffices to check the case when $h = \pi$ is irreducible. Now (2) is equivalent to $\chi(\operatorname{disc}_\kappa \pi) = (-1)^{\deg \pi - 1}$, which is easily checked using Galois theory of finite fields: the Frobenius over κ acts as a cycle of length $\deg \pi$ on the roots of π. □

When κ has characteristic 2, there is a Möbius formula due to Swan [7], in terms of a characteristic 0 lifting of $\kappa[u]$ to $W(\kappa)[u]$, where $W(\kappa)$ is the Witt vectors of κ. We omit this formula. The special case when $\kappa = \mathbb{F}_2$ was described by Stickelberger at the first International Congress of Mathematicians in 1897 using a lift to $\mathbb{Z}[u]$ rather than a lift to $\mathbb{Z}_2[u]$.

Remark 4.2. When $\kappa = \mathbb{F}_p$ for $p \neq 2$ and h is squarefree in $\mathbb{F}_p[u]$, (2) can be rewritten as $(\frac{\operatorname{disc} h}{p}) = (-1)^{n-r}$, where $n = \deg h$ and h has r distinct irreducible factors in $\mathbb{F}_p[u]$. This goes back to Pellet (1878) and is related to Stickelberger's formula $(\frac{\Delta}{p}) = (-1)^{n-r}$, where Δ is the discriminant of a number field of degree n in which p is unramified with r prime ideal factors.

Example 4.3. Let q be the size of κ and $f(T) = T^{4q} + u^{2q-1}$. For $g \in \kappa[u]$, clearly $f(g)$ is reducible when $g(0) = 0$; in fact, $\mu(f(g)) = 0$. When q is odd

and $g(0) \neq 0$, a calculation using (2) shows $\mu(f(g)) = 1$. When q is even and $g(0) \neq 0$, it can also be shown that $\mu(f(g)) = 1$. Since $\mu(f(g))$ is never -1, we see that $f(g)$ is reducible for every $g \in \kappa[u]$. This is an example where the Bouniakowsky conditions hold but no irreducible values occur.

By a substantial extension of Swan's ideas in [7], and motivated by our numerical data, we proved the surprising fact that $\mu(f(g))$ is essentially a periodic function of g if $f(T) \in \kappa[u][T]$ is a polynomial in T^p when $p \neq 2$ or is a polynomial in T^4 when $p = 2$. (When $p = 2$, the case of polynomials in T^2 which are not polynomials in T^4 still has not been completely understood.)

Theorem 4.4 ([1]). *Let κ be a finite field with characteristic p. Let $f(T)$ be squarefree in $\kappa[u][T]$ with positive T-degree. Assume, moreover, that $f(T)$ is a polynomial in T^p when $p \neq 2$ and is a polynomial in T^4 when $p = 2$. When $p \neq 2$, let χ be the quadratic character on $\kappa^\times$.*

There is a non-zero $M = M_{f,\kappa}$ in $\kappa[u]$ such that for $g_1 = c_1u^{n_1} + \cdots$ and $g_2 = c_2u^{n_2} + \cdots$ in $\kappa[u]$ with sufficiently large degrees n_1 and n_2,

$$g_1 \equiv g_2 \bmod M, \quad n_1 \equiv n_2 \bmod 4, \quad \chi(c_1) = \chi(c_2) \Longrightarrow \mu(f(g_1)) = \mu(f(g_2))$$

when $p \neq 2$ and

$$g_1 \equiv g_2 \bmod M, \quad n_1 \equiv n_2 \bmod 4 \Longrightarrow \mu(f(g_1)) = \mu(f(g_2))$$

when $p = 2$.

Proof. (Sketch) Very briefly, the proof of Theorem 4.4 requires a careful study of resultants.

According to (2), $\mu(f(g))$ depends on the discriminant of $f(g)$ when $p \neq 2$. The discriminant of $f(g)$ can be expressed in terms of the resultant of $f(g)$ and $(\mathrm{d}/\mathrm{d}u)(f(g)) = (\partial f/\partial u)(g)$. (This derivative calculation indicates why $f(T) = f(u, T)$ being a polynomial in $\kappa[u, T^p]$ is useful in the proof.) In order to exploit inductive arguments, we replace the study of the resultant $R(f(g), (\partial f/\partial u)(g))$ with $R(f_1(g), f_2(g))$, where f_1 and f_2 are fairly general polynomials in $\kappa[u, T]$. There are properties of resultants which resemble the properties of greatest common divisors, and this suggests a method for computing $R(f_1(g), f_2(g))$ by a procedure analogous to the Euclidean algorithm. However, a moment's thought about the difference between, say, $R(u^2 + 1, u^3 + u + 1)$ and $R(ug^2 + (u + 1)g + 1, g^4 + u^2g + u)$ for varying g in $\kappa[u]$ indicates why a proof that $R_{\kappa[u]}(f_1(g), f_2(g))$ has a periodic structure in g does not follow right away from any kind of basic elementary property of resultants for one-variable polynomials.

To correctly handle the varying polynomial g, we view the resultant of $f_1(g)$ and $f_2(g)$ as an algebraic function of g. This requires a combination of polynomial algebra and algebraic geometry, and is the main content of [1]. We study the geometry of the zero-scheme of $R(f_1(g), f_2(g))$ on the space of polynomials g with a fixed degree in order to get a formula for this resultant

function in terms of the geometry of the intersections of the plane curves $f_1 = 0$ and $f_2 = 0$. (Recall f_1 and f_2 are in $\kappa[u][T] = \kappa[u, T]$.) This geometric formula for the resultant has the asserted periodicity by inspection. (The case of characteristic 2 has its own set of complications.)

The mod 4 congruence in the conclusion of the theorem has a simple explanation. It is essentially due to the fact that the discriminant of a polynomial of degree n picks up a sign of $(-1)^{n(n-1)/2}$ when written in terms of a resultant, and this sign depends on n mod 4. □

Remark 4.5. The Bouniakowsky conditions (1) and (2) are irrelevant for $f(T)$ in Theorem 4.4. In particular, the hypotheses on $f(T)$ in Theorem 4.4 are preserved when κ is replaced by a finite extension, but the first Bouniakowsky condition does not have to remain true under a finite extension of κ (for the same f).

The following two examples illustrate Theorem 4.4.

Example 4.6. For $f(T)$ as in Table 1 and $g \in \mathbb{F}_2[u]$ with $\deg g \geq 1$, $\mu(f(g)) = (-1)^{\deg g}$. Here $M = 1$ and the mod 4 condition in the characteristic 2 case of Theorem 4.4 can be relaxed to a mod 2 condition.

Example 4.7. For $f(T)$ as in Table 5, and $g(u) = cu^n + \cdots$ in $\mathbb{F}_3[u]$ with $n \geq 2$, the proof of Theorem 4.4 leads to the formula

$$\mu(f(g)) = (-1)^{n(n+1)/2} \left(\frac{c}{3}\right)^{n+1} \left(\frac{g(1)^2 + g(1) + 2}{3}\right) \left(\frac{g(2)}{3}\right), \qquad (3)$$

where $(\frac{\cdot}{3})$ is a Legendre symbol. All of the conditions from Theorem 4.4 are seen in (3): $M = (u-1)(u-2)$, there is a mod 4 dependence on $n = \deg g$, and there is a quadratic dependence on the leading coefficient c of g.

Furthermore, (3) lets us prove $\mu(f(g))$ takes values 1 and -1 equally often in every degree. This means that the deviations from the Naive Conjecture in Table 5, in odd degrees, are apparently not "explained" by the distribution of non-zero values of $\mu(f(g))$ in odd degrees. But a closer look at (3) reveals something peculiar in odd degrees: when $\deg g \equiv 1 \bmod 4$, $\mu(f(g))$ is -1 only when $f(g)$ is divisible by $u-1$ or $u-2$. Therefore $f(g)$ will not be irreducible even in the case that $\mu(f(g)) = -1$. Similarly, when $\deg g \equiv 3 \bmod 4$, $\mu(f(g))$ is 1 only when $f(g)$ is divisible by $u-1$ or $u-2$. In short, if $\mu(f(g))$ is non-zero and $\deg g$ is odd, the sign of $\mu(f(g))$ is fixed when $(f(g), M) = 1$, where $M = (u-1)(u-2)$ is the "modulus" from (3). Classically, one would not expect a non-constant $f(T) \in \mathbb{Z}[T]$ to have the long-range statistics on $\mu(f(n))$ be affected by a local constraint of the form $(f(n), m) = 1$ for some $m \in \mathbb{Z}$. But this can happen in characteristic p.

We now revise the incorrect property (c′) from the start of this section, by using $M_{f,\kappa}$ from Theorem 4.4:

(c) there is a Möbius bias: the non-zero values of $\mu(f(g))$ are not ± 1 equally often when $(f(g), M_{f,\kappa}) = 1$.

The idea in (c) will be used later to correct the Naive Conjecture.

Although Theorem 4.4 does not pin down a unique choice of $M_{f,\kappa}$, it turns out that all possible choices of $M_{f,\kappa}$ are multiples of a choice with least degree. Therefore the choice of $M_{f,\kappa}$ with least degree and leading coefficient 1 could be considered a 'canonical' selection. However, it is important for the proof of the full version of Theorem 4.4, as stated in [1], that we can always choose $M_{f,\kappa}$ in a geometric manner, which is not always a choice with least degree. We describe this geometric construction in characteristic $\neq 2$ for simplicity, first in a special case and then in general:

- When $f(T)$ is monic as a polynomial in T, $M_{f,\kappa}$ is the radical of the resultant of f and $\partial f/\partial u$ as polynomials in T.
- In the general case, when $f(T)$ is not necessarily monic in T, view f as a polynomial in the two variables u and T, and let Z_f be the zero locus of f in $\mathbb{A}^2_\kappa$. The projecton $Z_f \to \mathbb{A}^1_\kappa$ onto the T-axis has a finite non-étale locus on Z_f, and its projection onto the u-axis is a finite set. Let $M_{f,\kappa}$ be the separable (monic) polynomial in $\kappa[u]$ having this subset of the u-axis as its zero locus.

Example 4.8. For $f(T)$ as in Example 4.7, the resultant of f and $\partial f/\partial u$ as polynomials in T is $-(u-1)^6(u-2)^9$, whose radical is $(u-1)(u-2)$. This agrees with the "modulus" for $\mu(f(g))$ according to (3).

Definition 4.9. *For f as in Theorem 4.4 and satisfying the second Bouniakowsky condition, define*

$$\Lambda_\kappa(f;n) := 1 - \frac{\sum_{\deg g = n, (f(g), M_{f,\kappa})=1} \mu(f(g))}{\sum_{\deg g = n, (f(g), M_{f,\kappa})=1} |\mu(f(g))|}. \tag{4}$$

The denominator sum in (4) is the number of g with degree n such that $f(g)$ is squarefree and relatively prime to $M_{f,\kappa}$. By work of Poonen [5] on squarefree values and relatively prime values of polynomials, this denominator is positive for $n \gg 0$. Clearly $0 \leq \Lambda_\kappa(f;n) \leq 2$. While there is not a unique choice for $M_{f,\kappa}$ in Theorem 4.4, the choice used in (4) has no impact on the long-range behavior of $\Lambda_\kappa(f;n)$: two different choices of $M_{f,\kappa}$ from Theorem 4.4 provably give sequences in (4) that agree for $n \gg 0$ (depending on f and κ and the choice of the M's).

Corollary 4.10 ([1]). *Let $f(T)$ satisfy the hypotheses of Theorem 4.4 and the second Bouniakowsky condition. For $n \gg 0$, $\Lambda_\kappa(f;n)$ is periodic in n with period 1, 2, or 4.*

Proof. (Sketch) This follows from a careful evaluation of the formula for $\mu(f(g))$ which is established in the proof of Theorem 4.4 (taking separately $p \neq 2$ and $p = 2$). It turns out that $\Lambda_\kappa(f;n)$ depends on n mod 4, so its minimal period as a function of n is 1, 2, or 4. □

The periodicity in Corollary 4.10 shows $\Lambda_\kappa(f;n)$ is a much simpler function of n than its definition suggests! In any particular example, we can use the proof of Theorem 4.4 to compute the periodic part of the sequence $\Lambda_\kappa(f;n)$. As Table 6 shows, when $f(T)$ is one of the polynomials from the previous tables, the periodic part of the sequence $\Lambda_\kappa(f;n)$ appears to fit the deviations from the Naive Conjecture for $\pi_f(n)$.

Table 6. Examples of $\Lambda_\kappa(f;n)$

Table for $f(T)$	$M_{f,\kappa}$	Periodic Part of $\Lambda_\kappa(f;n)$
Table 1	1	2,0 for $n \geq 1$
Table 2	1	1,2,1,0 for $n \geq 1$
Table 3	$u(u-1)$	4/3 for $n \geq 2$
Table 4	1	0 for $n \geq 1$
Table 5	$(u-1)(u-2)$	0,1,2,1 for $n \geq 1$

We believe the following are correct $\kappa[u]$-analogues of the conjectures of Bouniakowsky and Hardy–Littlewood over $\mathbb{Z}$.

Conjecture 4.11 ([1]). Let κ have characteristic $p \neq 2$, and let $f \in \kappa[u][T]$ have positive degree in T. Then $f(g)$ is irreducible for infinitely many g in $\kappa[u]$ if and only if the following conditions hold:

(1) $f(T)$ is irreducible in $\kappa(u)[T]$,
(2) no irreducible π in $\kappa[u]$ divides $f(g)$ for every $g \in \kappa[u]$,
(3) $f(T) \notin \kappa[u][T^p]$ or, if $f(T) \in \kappa[u][T^p]$ then the periodic part of the sequence $\Lambda_\kappa(f;n)$ is not identically 0.

As in the classical case, the second condition in this conjecture is checked in practice by finding a pair of relatively prime values $f(g_1)$ and $f(g_2)$. The third condition can also be checked in practice. When κ has characteristic 2, we believe Conjecture 4.11 is correct if $f(T) \notin \kappa[u][T^2]$ or if $f(T) \in \kappa[u][T^4]$. The case of polynomials in T^2 that are not polynomials in T^4 still needs further study.

Here is a quantitative refinement of Conjecture 4.11, incorporating part of the characteristic 2 case.

Conjecture 4.12 ([1]). Let $f \in \kappa[u][T]$ satisfy the two Bouniakowsky conditions. Let $p = \mathrm{char}(\kappa)$. If $f(T) \notin \kappa[u][T^p]$, then the asymptotic relation in the Naive Conjecture is true. If $f(T)$ is a polynomial in T^p when $p \neq 2$ or $f(T)$ is a polynomial in T^4 when $p = 2$, then

$$\pi_f(n) \sim \Lambda_\kappa(f;n)\frac{C(f)}{\deg_T f}\frac{(q-1)q^n}{n} \tag{5}$$

as $n \to \infty$.

As in Theorem 4.4, we do not yet have a complete formulation of Conjecture 4.12 in characteristic 2, since the behavior of polynomials in T^2 that are not in T^4 is still not adequately understood.

The periodicity of $\Lambda_\kappa(f;n)$ is essential for a proper understanding of (5). When 0 is in the period of $\Lambda_\kappa(f;n)$, the meaning of (5) is that $\pi_f(n)$ equals 0 for those (large) periodic n where $\Lambda_\kappa(f;n) = 0$. In fact, it is easy to prove this: if $\Lambda_\kappa(f;n) = 0$, then for all g of degree n we have either $(f(g), M_{f,\kappa}) \neq 1$ or $\mu(f(g)) \in \{0,1\}$. Thus, for $n \gg 0$ (depending on $M_{f,\kappa}$), the vanishing of $\Lambda_\kappa(f;n)$ implies $\pi_f(n) = 0$. In this way, by making the condition "$n \gg 0$" effective in specific examples, we can prove the 0 patterns in Tables 1, 2, 4, and 5 continue for all larger n. We have not proved a relation between Möbius statistics and irreducibility statistics for those periodic (large) n where $\Lambda_\kappa(f;n) \neq 0$, but the data in these cases agree very well with (5).

We said at the start of this section that some polynomials in T^p appear to fit the Naive Conjecture numerically, such as $T^p + u^2$ over $\mathbb{F}_3[u]$, $\mathbb{F}_5[u]$, $\mathbb{F}_7[u]$, and $\mathbb{F}_9[u]$. If the Naive Conjecture and (5) are going to be compatible, then any polynomial in T^p (for $p \neq 2$) that satisfies the Bouniakowsky conditions and agrees with the Naive Conjecture must have $\Lambda_\kappa(f;n) = 1$ for all large n. This conclusion has been confirmed in several examples of polynomials in T^p (for $p \neq 2$) where the Naive Conjecture appears to look good, e.g., we can prove $\Lambda_\kappa(T^p + u^2; n) = 1$ for $n \geq 1$ and κ any finite field of characteristic $p \neq 2$.

The ring $\kappa[u]$ corresponds to the affine line over κ. Theorem 4.4 can be extended to the coordinate ring of any smooth affine curve over κ whose smooth compactification has only one geometric point '∞' at infinity. The substitute for the sampling condition '$\deg g = n$' is '$\mathrm{ord}_\infty(g) = -n$.' From this point of view, Theorem 4.4 corresponds to genus zero. The proof of the higher-genus generalization uses the work in genus zero as input, and requires additional arguments of a much more elaborate geometric character. Numerical aspects of this work are still in progress.

5 An Application to Elliptic Curves

Having found a Möbius periodicity that is a global obstruction to the Naive Conjecture in characteristic p, we ask: why does no analogous obstruction arise over $\mathbb{Z}$? The belief in the classical Hardy–Littlewood conjecture suggests that the $\mathbb{Z}$-analogue of the new characteristic p correction factor in (4) is 1. This suggests the following: if $f(T) \in \mathbb{Z}[T]$ is a non-constant (irreducible) polynomial taking at least one squarefree value, then

$$\frac{\sum_{n \leq x} \mu(f(n))}{\sum_{n \leq x} |\mu(f(n))|} \to 0 \tag{6}$$

as $n \to \infty$. The denominator of (6) is the number of squarefree values $f(n)$ for $n \leq x$. Granting the *abc*-conjecture, work of Granville [3] shows the de-

nominator of (6) is proportional to x, so (6) should be equivalent to

$$\frac{\sum_{n\le x}\mu(f(n))}{x}\to 0\,. \tag{7}$$

(The equivalence of (6) and (7) is unconditional when $\deg f\le 3$; the *abc*-conjecture is used for $\deg f>3$.) When $f(T)=T$, (7) is equivalent to the prime number theorem. For other f of degree 1, (7) is equivalent to Dirichlet's theorem [6]. No other case of (7) has been proved. Numerical evidence for (7) when $\deg f>1$ looks reasonable. An example in degree 3 is provided in Table 7.

Table 7. (7) for $f(T)=T^3+2T+1$

x	$\frac{1}{x}\sum_{n\le x}\mu(f(n))$
10^2	$-.15$
10^3	$-.015$
10^4	$-.0009$
10^5	$.00432$
10^6	$.00028$

The Ph.D. thesis of H. Helfgott [4] gives a link between a variant on (7) and elliptic curves. Helfgott studies the *average root number* of an elliptic curve over $\mathbb{Q}(T)$, which is essentially the average value of the root number of the smooth specializations at $T=t\in\mathbb{P}^1(\mathbb{Q})$, with t ordered by height. This average lies in $[-1,1]$ if it exists. Assuming two conjectures from analytic number theory about values of polynomials over $\mathbb{Z}$, Helfgott shows that the average root number of any non-isotrivial elliptic curve over $\mathbb{Q}(T)$ exists and lies strictly between -1 and 1. (When the elliptic curve has at least one place of multiplicative reduction, Helfgott can in fact prove the average is 0.) One of the two conjectures Helfgott assumes is

$$\frac{1}{x^2}\sum_{m,n\le x}\lambda(f(m,n))\to 0\,, \tag{8}$$

where $f(X,Y)\in\mathbb{Z}[X,Y]$ is a non-constant non-square homogeneous polynomial and λ is the classical Liouville function. (Recall that $\lambda(\pm p)=-1$ for prime p and λ is totally multiplicative, e.g., $\lambda(12)=-1$.) Considering the similarity of the Möbius and Liouville functions, (8) bears a close resemblance to (7).

The natural analogue of the conjectural (8) for polynomials with coefficients in $\kappa[u]$ rather than $\mathbb{Z}$ is false: explicit counterexamples can be constructed from certain instances of unusual Möbius statistics in characteristic p. Might this imply that some of Helfgott's results over $\mathbb{Q}(T)$ are not true

over $\kappa(u)(T)$? Yes. The following theorem says non-isotrivial elliptic curves over $\kappa(u)(T)$ with average root number 1 *do* exist in odd characteristic, with an additional interesting feature.

Theorem 5.1 ([2], Theorem 1.1). *Let κ be any finite field with characteristic $p \neq 2$. For any $c, d \in \kappa^\times$, the Weierstrass model*

$$E_{c,d,T} : y^2 = x^3 + (c(T^2+u)^{2p} + du)x^2 - (c(T^2+u)^{2p} + du)^3 x \qquad (9)$$

defines a non-isotrivial elliptic curve over $\kappa(u)(T)$ such that

(a) *for every $t \in \mathbb{P}^1(\kappa(u))$, the specialization $E_{c,d,t}$ is an elliptic curve over $\kappa(u)$ having global root number 1, and for $t \neq \infty$ there is a $\kappa(u)$-rational point of infinite order,*
(b) *the Mordell–Weil group $E_{c,d,T}(\kappa(u)(T))$ has rank 1.*

The key word in Theorem 5.1 is "non-isotrivial." Helfgott's work strongly suggests that a non-isotrivial elliptic curve over $\mathbb{Q}(T)$ should not have elevated rank. (We say an elliptic curve over $\mathbb{Q}(T)$ has *elevated rank* when the rank of all but finitely many of its specializations to elliptic curves over $\mathbb{Q}$ exceeds the rank over $\mathbb{Q}(T)$.) Granting the parity conjecture for elliptic curves over $\kappa(u)$, Theorem 5.1(a) implies the rank of $E_{c,d,t}(\kappa(u))$ is positive and even for all $t \in \mathbb{P}^1(\kappa(u)) - \{\infty\}$, so each $E_{c,d,T}$ is non-isotrivial and should have elevated rank over $\kappa(u)(T)$.

Proof. (Sketch) An explicit calculation of the j-invariant of $E_{c,d,T}$ shows it is non-isotrivial. (Moreover, $j(E_{c,d,T}) = j(E_{c',d',T})$ if and only if $c = c'$ and $d = d'$.)

To verify part (a), the elliptic curve over $\kappa(u)$ obtained by specialization $T \mapsto t$ for any $t \in \mathbb{P}^1(\kappa(u))$ has global root number 1 based on an analysis of local reduction types and a calculation of all the local root numbers. (It is within these local root number calculations, which are carried out in detail in [2], that one sees how we found (9) in the first place. This Weierstrass model was not discovered by random guessing.) We use a function field variant of the Nagell-Lutz criterion to check an explicit rational point in $E_{c,d,T}(\kappa(u)(T))$ has infinite order and retains infinite order after specialization of T to any $t \in \mathbb{P}^1(\kappa(u)) - \{\infty\}$.

The proof of part (b) amounts to showing $E_{c,d,T}(\kappa(u)(T))$ has rank at most 1. (Part (a) already tells us the rank is at least 1.) The 2-torsion is $\langle (0,0) \rangle \cong \mathbb{Z}/2\mathbb{Z}$, so

$$\dim_{\mathbb{F}_2}(E_{c,d,T}(\kappa(u,T))/2 \cdot E_{c,d,T}(\kappa(u,T))) = 1 + r\,,$$

with r being the rank. We show this dimension is at most 2 by a specialization in the u-direction rather than the T-direction.

Abbreviate $E_{c,d,T}$ to $\mathscr{E}$. For any closed point $u_0 \in \mathbb{P}^1_\kappa$, with residue field κ_0 (varying with u_0), consider the natural commutative diagram

$$\begin{array}{ccc} \mathscr{E}(\kappa(u,T))/2\cdot\mathscr{E}(\kappa(u,T)) & \longrightarrow & \mathscr{E}(\overline{\kappa}(u,T))/2\cdot\mathscr{E}(\overline{\kappa}(u,T)) \\ \downarrow & & \downarrow \\ \mathscr{E}_{u_0}(\kappa_0(T))/2\cdot\mathscr{E}_{u_0}(\kappa_0(T)) & \longrightarrow & \mathscr{E}_{\overline{u}_0}(\overline{\kappa}(T))/2\cdot\mathscr{E}_{\overline{u}_0}(\overline{\kappa}(T)) \end{array}$$

where the elliptic curve $\mathscr{E}_{u_0/\kappa_0(T)}$ is the u-specialization at u_0, and $\overline{u}_0 \in \overline{\kappa}$ lies over u_0.

The Lang–Néron theorem tells us $\mathscr{E}(\overline{\kappa}(u,T)) = \mathscr{E}(\kappa(u,T))$ when κ is replaced by a suitable finite extension. We make this enlargement of κ at the beginning of the proof of part (b), so we may take the top map to be an isomorphism. The enlargement of κ might depend on the choice of parameters c and d. Since part (a) has already been checked in full generality (i.e., for all finite constant fields), we may apply it to the new elliptic curve under consideration.

The proof now falls into two parts. Geometric and ramification-theoretic arguments (applicable not just to $\mathscr{E}_{/\kappa(u,T)}$, but to abelian varieties over function fields of varieties fibered over $\mathbb{P}^1$) show that the map along the right column is one-to-one for all but finitely many $\overline{u}_0$. An application of the Chebotarev density theorem and a calculation in étale cohomology show that the map along the bottom side has image with dimension at most 2 for infinitely many u_0. Therefore, by a suitable choice of u_0, we get $1 + r \leq 2$. □

Although Theorem 5.1 does not include characteristic 2, further work should remove this exception.

It required several months of effort to find the curve in Theorem 5.1 and confirm all of its properties, but we never would have had the intuition that such an elliptic curve could exist in characteristic p if the investigation of a function field analogue of the classical Hardy–Littlewood conjecture had not revealed the peculiarities of the Möbius function in characteristic p. Thus, while the topic of this paper is a non-analogy between $\mathbb{Q}$ and $\kappa(u)$, the analogies between these fields provided useful insights during our work.

References

1. Conrad, B., Conrad K., Gross, R.: Irreducible Specialization in Genus 0. Submitted to J. Reine Angew. Math.
2. Conrad, B., Conrad, K., Helfgott, H. A.: Root numbers and ranks in positive characteristic. Submitted to Adv. in Math.
3. Granville, A.: *ABC* allows us to count squarefrees. Internat. Math. Res. Notices, **19**, 991–1009 (1998).
4. Helfgott, H. A.: Root numbers and the parity problem. Ph.D. thesis, Princeton University (2003).
5. Poonen, B.: Squarefree values of multivariable polynomials. Duke Math. J., **118**, 353–373 (2003).
6. Shapiro, H. N.: Some assertions equivalent to the prime number theorem for arithmetic progressions. Comm. Pure Appl. Math., **2**, 293–308 (1949).

7. Swan, R. G.: Factorization of polynomials over finite fields. Pacific J. Math., **12**, 1099–1106 (1962).