AN EXPLICIT APPROACH TO HYPOTHESIS H FOR POLYNOMIALS OVER A FINITE FIELD

PAUL POLLACK

Abstract. Schinzel's Hypothesis H predicts that a family of irreducible polynomials over the integers satisfying certain necessary local conditions simultaneously assumes prime values infinitely often. Here we consider an analogue of Hypothesis H for one-variable polynomials over the q-element finite field $\mathbf{F}_q$ and show that it holds whenever q is large compared to the degree of the product of the polynomials involved. We also show that for fixed q, the conclusion of our Hypothesis H holds for "almost all" single-polynomial families. Along the way we propose a new polynomial analogue of the Hardy-Littlewood/Bateman-Horn conjectures.

1. Introduction

1.1. **Hypothesis H: From $\mathbf{Z}[T]$ to $\mathbf{F}_q[T]$.** In 1854, Bouniakowsky [4] put forward a conjectural characterization of those polynomials over $\mathbf{Z}$ which assume infinitely many prime values. A century later, Schinzel (in a joint paper [22] with Sierpiński) proposed the analogous conjecture for finite families of integer polynomials; this conjecture, bearing the sadly nondescript title "Hypothesis H," contains (implicitly or more or less explicitly) many of the classical conjectures of number theory. In this article we investigate the following analogue of Hypothesis H for polynomials over a finite field:

Conjecture 1 (A function field analogue of Hypothesis H)**.** *Let $f_1(T)$, $\dots$, $f_r(T)$ be irreducible polynomials belonging to $\mathbf{F}_q[T]$. Suppose that there is no prime $P \in \mathbf{F}_q[T]$ for which every $g(T) \in \mathbf{F}_q[T]$ satisfies*

$$f_1(g(T)) \cdots f_r(g(T)) \equiv 0 \pmod{P}. \tag{1}$$

Then the specializations $f_1(g(T)), \dots, f_r(g(T))$ are simultaneously irreducible for infinitely many monic polynomials $g(T) \in \mathbf{F}_q[T]$.

Schinzel's Hypothesis H has only been proved in the case of a single linear polynomial, where it amounts to Dirichlet's theorem on primes in an arithmetic progression. Dirichlet's 1837 proof of this result marks the birth of modern analytic number theory, and Kornblum's 1914

1991 *Mathematics Subject Classification.* Primary: 11T55, Secondary: 11N32.
The author is supported by an NSF Graduate Research Fellowship.

translation of this proof into the setting of polynomials over a finite field [17] marks the first serious investigation into the analytic arithmetic of global function fields. The known results in the remaining (open) cases of Hypothesis H depend for the most part on sieve methods, the study of which was pioneered by Brun at the beginning of the 20th century. Significant work has been done translating these techniques to the polynomial setting (see, e.g., Car [6] [7], Cherly [8], Hsu [16]), and the consequent results constitute partial progress towards a function field analogue of Hypothesis H that is more general than our Conjecture 1 (see the discussion at the end of this section). However, as in the classical case, it seems unlikely that sieve methods can provide a complete solution to any of the remaining cases of Hypothesis H. Our purpose in this paper is to report on a simple but powerful approach to Conjecture 1 that seems intrinsic to the polynomial setting.

This method is of quite recent origin; it was only in 2003 that Hall, in his Ph.D thesis (cf. [14, p. 140]) observed that the existence of infinitely many "twin prime polynomial pairs" $f, f+1$ could be easily obtained from classical results in the theory of finite fields. (Actually, he proved this only in the case $q > 3$, leaving the case $q = 3$ open.) Our first theorem is an extension of this result:

Theorem 1 (Twin prime polynomial theorem)**.** *For every $q \neq 2$ and every $\alpha \in \mathbf{F}_q^\times$, there are infinitely many monic twin prime polynomials $f, f+\alpha$ in $\mathbf{F}_q[T]$.*

Theorem 1 shows that Conjecture 1 holds for $f_1(T) = T$ and $f_2(T) = T + \alpha$. Our main result shows that Conjecture 1 holds for an arbitrary family of polynomials, provided q is large in a suitable sense:

Theorem 2 (Conjecture 1 for "large q")**.** *Let $f_1(T), \dots, f_r(T)$ be irreducible polynomials over $\mathbf{F}_q$. If q is large compared to both r and the sum of the degrees of the f_i, then there is a prime l dividing $q-1$ and an element $\beta \in \mathbf{F}_q$ for which every subsitution*

$$T \mapsto T^{l^k} - \beta \quad \textit{with} \quad k = 0, 1, 2, \dots$$

leaves all of $f_1, \dots, f_r$ irreducible. Explicitly, the above conclusion holds provided

$$q \geq 2^{2r} \left(1 + \frac{1}{2} \sum_{i=1}^{r} \deg f_i\right)^2. \tag{2}$$

In fact we obtain the theorem for q satisfying a slightly weaker (but more complicated) inequality than (2). It may be initially surprising that we have not included a local condition in our statement of Theorem

2. But such a condition is actually implicit in our requirements on q: the number of incongruent solutions to (1) is bounded by the sum of the degrees of the f_i, so that the local condition of Conjecture 1 is automatically satisfied for $q > \sum_{i=1}^{r} \deg f_i$, an inequality less stringent than (2).

Thus Conjecture 1 holds provided q is 'large.' The remaining cases appear more difficult. Here we restrict ourselves to some remarks concerning the cases when $r = 1$ and q is fixed. In this direction we prove the following conditional result. Below $l_a(m)$ denotes the multiplicative order of a modulo m.

Theorem 3. *Fix a finite field $\mathbf{F}_q$. For each $d \geq 2$, define*

$$\mathcal{A}_d := \{f \in \mathbf{F}_q[T] : \deg f = d;\ \textit{for some prime } l \mid q^d - 1,\ f(T^{l^k}) \textit{ is irreducible for } k = 0, 1, 2, \dots\},$$

and let $\mathcal{E}_d$ denote the set of monic irreducibles of degree d not in $\mathcal{A}_d$. Then for any $\epsilon > 0$,

$$\#\mathcal{E}_d \ll q^d/d^2 \qquad (\textit{unconditionally}), \tag{3}$$

$$\ll_\epsilon q^{1+\epsilon d} \qquad (\textit{assuming the abc-conjecture}). \tag{4}$$

Moreover, if we assume that

$$\sum_{\substack{r \ prime \\ r \nmid q}} \frac{1}{l_q(r^2)} < \infty, \tag{5}$$

then $\mathcal{E}_d$ is empty for almost all d (in the sense of asymptotic density).

The complicated-looking assumption (5) asserts, in crude terms, that there are not too many q-Wieferich primes (i.e., primes r for which $q^{r-1} \equiv 1 \pmod{r^2}$). For example, in order for (5) to hold, it suffices that there be $\ll (\log x)^{1-\delta}$ such primes up to x; the natural conjecture is that there are only $\ll \log\log x$. We note that in the case $q = 2$ an assumption equivalent to (5) already appears in the work of Granville & Soundararajan (cf. [13, Theorem 4]).

Before proceeding we emphasize that Conjecture 1 is only one possible function field analogue of Hypothesis H. A more general conjecture would allow for families of polynomials with coefficients from $\mathbf{F}_q[u]$ and not merely from the constant field $\mathbf{F}_q$. However, even formulating the correct conjecture in this generality requires some care, as the following example illustrates: For each finite field $\mathbf{F}_q$, the polynomial $T^{4q} + u^{2q-1}$ is irreducible over $\mathbf{F}_q[u]$ and without a fixed prime divisor from $\mathbf{F}_q[u]$. Yet it can be proved that there is not a single $A \in \mathbf{F}_q[u]$ for which

$A^{4q} + u^{2q-1}$ is irreducible! For a discussion of the underlying cause for this anomaly and quantitative versions of Hypothesis H in the polynomial case taking these considerations into account, see the paper of Conrad, Conrad, and Gross [10].

1.2. **Recent progress.** Theorems 1–3 depend on a simple technique which we call the "substitution method," which was the subject of the author's address at the Anatomy of Integers conference. Since that time there has been further progress towards Conjecture 1, and we recount some of it here. (Details will appear in [19] and the author's doctoral thesis, currently in progress.)

We begin by proposing a quantitative hypothesis which implies our Conjecture 1. It may be considered a polynomial analogue of the classical Bateman-Horn conjecture [1]:

Conjecture 2 (A quantitative constant-coefficient Hypothesis H)**.** *Let $f_1, \dots, f_r$ be nonassociate irreducible one-variable polynomials over $\mathbf{F}_q$ with the degree of $f_1 \cdots f_r$ bounded by B. Suppose that there is no prime P of $\mathbf{F}_q[T]$ for which the map*

$$g(T) \mapsto f_1(g(T)) \cdots f_r(g(T)) \bmod P$$

is identically zero. Then

$$\begin{aligned} &\#\{g(T) : g \text{ monic}, \deg g = n, \text{ and } f_1(g(T)), \dots, f_r(g(T)) \text{ all prime}\} \\ &\qquad = (1 + o_B(1)) \frac{\mathfrak{S}(f_1, \dots, f_r)}{\prod_{i=1}^r \deg f_i} \frac{q^n}{n^r} \quad \text{as } q^n \to \infty. \end{aligned} \tag{6}$$

Here the local factor $\mathfrak{S}(f_1, \dots, f_r)$ is defined by

$$\mathfrak{S}(f_1, \dots, f_r) := \prod_{m=1}^{\infty} \prod_{\substack{P \\ \deg P = m \\ P \text{ monic, prime}}} \frac{1 - \omega(P)/q^m}{(1 - 1/q^m)^r},$$

where

$$\omega(P) := \#\{A \bmod P : f_1(A) \cdots f_r(A) \equiv 0 \pmod P\}.$$

Remark. It should be noticed that the asymptotic relation (6) is conjectured to hold as $q^n \to \infty$, so when *either* q or n tends to infinity. In the appendix to this article we provide a heuristic argument for Conjecture 2. Two properties of the singular series $\mathfrak{S}(f_1, \dots, f_r)$ are worth extracting from that discussion:

(i) Under the hypotheses of Conjecture 2, the product defining $\mathfrak{S}(f_1, \dots, f_r)$ converges to a positive constant. In particular, fixing $f_1, \dots, f_r$ (and so also q) and letting n tend to infinity, we see that Conjecture 2 implies Conjecture 1.

(ii) Putting equation (14) together with Lemma 7 yields the estimate

$$\frac{\mathfrak{S}(f_1,\dots,f_r)}{\prod_{i=1}^r \deg f_i} = 1 + O_B(1/q).$$

This is useful in explaining the form of Theorem A below.

Our main result in [19] is the following asymptotic formula, which (in view of the second remark above) confirms Conjecture 2 when q is large compared to n and B, subject to a mild restriction on the characteristic:

Theorem A. *Let n be a positive integer. Let $f_1(T),\dots,f_r(T)$ be nonassociate irreducible polynomials over $\mathbf{F}_q$ with the degree of the product $f_1\cdots f_r$ bounded by B. The number of univariate monic polynomials g of degree n for which all of $f_1(g(T)),\dots,f_r(g(T))$ are irreducible over $\mathbf{F}_q$ is*

$$q^n/n^r + O_{n,B}(q^{n-1/2})$$

provided $\gcd(q,2n)=1$.

The proof of Theorem A makes use of an explicit version of the Chebotarev density theorem for function fields (resting on Weil's Riemann Hypothesis), and is similar in structure to the arguments employed by Cohen [9] and Ree [20] to establish Chowla's conjecture that irreducible polynomials of the form T^n+T+a exist over $\mathbf{F}_p$ provided $p > p_0(n)$. (Cf. also the related recent work of Bender & Wittenberg [2].) The implied constant in Theorem A is effective but somewhat unpleasant, depending on estimates for the genus of function fields that arise in the proof.

Theorem A, though of independent interest, also serves a useful adjunct to the substitution method. To illustrate, we consider the question posed in [14] of whether there are infinitely many twin prime pairs $f, f+1$ of *odd degree* over $\mathbf{F}_q$. For any particular $q>2$, the substitution method gives one a chance to answer this question in the affirmative: one finds a "suitable" twin prime pair of odd degree and bootstraps it to an infinite family. The difficulty comes in knowing that for large q, this process can get off the ground; Theorem A guarantees that such 'starter polynomials' are plentiful. In this way we show in [19] that there are infinitely many twin prime polynomials $f, f+1$ with degree of either prescribed parity over $\mathbf{F}_q$, for every $q>2$. By the same method we prove in [19] the following general statement:

Theorem B. *Let $f_1(T),\dots,f_r(T)$ be nonassociate irreducibles over $\mathbf{F}_q$ with the degree of $f_1\cdots f_r$ bounded by B. Let $a \bmod m$ be an arbitrary*

infinite arithmetic progression of integers. If the finite field $\mathbf{F}_q$ *is sufficiently large, depending just on* m, r, *and* B, *and if* q *is prime to* $2\gcd(a,m)$, *then there are infinitely many univariate monic polynomials* g *over* $\mathbf{F}_q$ *with*

$$\deg g \equiv a \bmod m \quad \textit{and} \quad f_1(g(T)), \dots, f_r(g(T)) \textit{ all prime in } \mathbf{F}_q[T].$$

It seems that the combination of this "Chebotarev method" and the substitution method should have many other applications. Here is an example of a slightly different flavor; details will appear in the author's dissertation:

Theorem C. *If* $\mathbf{F}_q$ *is a finite field with characteristic* > 3, *then infinitely many monic primes* P *over* $\mathbf{F}_q$ *have a representation in the form*

$$P = A^3 + B^3 + C^3, \quad \textit{where } A, B, C \textit{ are monic primes, and } \deg A > \max\{\deg B, \deg C\}.$$

By contrast, it was only recently, following ideas of Friedlander and Iwaniec, that Heath-Brown [15] established the existence of infinitely many rational primes that are sums of three (not necessarily prime) cubes, by a sophisticated application of the sieve.

Notation and conventions. The letter P always denotes an irreducible polynomial over $\mathbf{F}_q$. We write φ_q for the $\mathbf{F}_q[T]$-analogue of the Euler totient function, so that $\varphi_q(A)$ is the size of the unit group $\mathbf{F}_q[T]/(A)^\times$. We call two polynomials over $\mathbf{F}_q$ *associates* (or *associated*) if one is an $\mathbf{F}_q^\times$-multiple of the other.

We use $\mathrm{rad}(n) := \prod_{p|n} p$ to denote the *radical* of the positive integer n and $\mathrm{rad}'(n)$ to denote the odd part of $\mathrm{rad}(n)$, i.e., $\mathrm{rad}'(n) := \prod_{p|n, p>2} p$. Finally we remind the reader that $l_a(m)$ denotes the multiplicative order of a modulo m.

2. The substitution method

Suppose $f(T)$ is an irreducible polynomial over a finite field. Under what conditions is the composite $f(g(T))$ also irreducible? At the heart of the substitution method is the observation that this question has a simple answer when $g(T)$ is a binomial polynomial $T^m - \beta$.

Since the linear substitution $T \mapsto T - \beta$ always preserves irreducibility, to understand the effect of binomial substitutions it suffices to study the case when $g(T) = T^m$. This question was considered by Serret in the case of prime fields [23] and Dickson in the general case ([11], p. 382; see also [12], §34). Since it is somewhat simpler and suffices for us,

we restrict ourselves to the case when m is a prime power. Recall that the *order* of an irreducible polynomial $f(T) \in \mathbf{F}_q[T]$, not associated to T, is the multiplicative order of any of its roots.

Lemma 1 (Serret, Dickson)**.** *Let f be an irreducible polynomial over $\mathbf{F}_q$ of degree d and order e. Let l be an odd prime. Suppose that f has a root $\alpha \in \mathbf{F}_{q^d}$ which is not an lth power, or equivalently that*

$$l \text{ divides } e \quad \text{but} \quad l \text{ does not divide } (q^d - 1)/e. \tag{7}$$

Then the substitution $T \mapsto T^{l^k}$ leaves f irreducible for every $k = 1, 2, 3, \ldots$. The same holds for the prime $l = 2$ under the additional hypothesis $q^d \equiv 1 \pmod 4$.

As an immediate corollary, one obtains the following result (which can also be deduced from Capelli's classification of irreducible binomials; see, e.g., [18, Chapter VI, Theorem 9.1]):

Corollary 1. *Let l be an odd prime. If $\alpha \in \mathbf{F}_q$ is not an lth power, then*

$$T^{l^k} - \alpha \quad \text{is irreducible over } \mathbf{F}_q \text{ for every } k = 0, 1, 2, \ldots.$$

The same result holds for $l = 2$ if also $q \equiv 1 \pmod 4$.

How are these results useful? Consider, e.g., the problem of producing twin prime pairs $f, f + 1$ over a finite field. With l a prime to be chosen conveniently, we consider the binomials $T^{l^k} + \alpha$ and $T^{l^k} + \alpha + 1$. Corollary 1 tells us that whether or not both of these polynomials are irreducible depends (at least if $l > 2$) only on the lth power character of α and $\alpha + 1$. (In particular, there is no dependence on k!) Thus, if we can choose l and α appropriately, then varying k gives us an infinite family of twin prime pairs. This was Hall's strategy, and it is also our strategy in proving Theorem 1.

Consider now the situation of Theorem 2. Thus we are given irreducibles $f_1, \ldots, f_r$ over $\mathbf{F}_q$ and we seek a prime l and a $\beta \in \mathbf{F}_q$ for which each $f_i(T^{l^k} - \beta)$ is irreducible (for all $k \geq 0$). If l is a prime for which the hypotheses of Lemma 1 are satisfied simultaneously with respect to every $f_i(T)$, then our job is easy: use this l and take $\beta = 0$. Of course there is no guarantee that such an l exists. We prove Theorem 2 by showing that we can always satisfy the hypotheses of Lemma 1 for some l if we allow ourselves to replace the given family $\{f_i(T)\}_{i=1}^r$ by the translated family $\{f_i(T - \beta)\}_{i=1}^r$ for an appropriate $\beta \in \mathbf{F}_q$.

To summarize, in both cases our success hinges on the existence of an appropriate configuration of lth power nonresidues. In the proof of Theorem 1, the arguments guaranteeing that these configurations exist

are usually combinatorial. To prove Theorem 2, we take a different tack, detecting configurations of nonresidues via estimates for character sums.

3. Proof of Theorem 1

The following near-trivial combinatorial lemma is at the heart of Theorem 1:

Lemma 2. *Let α be a nonzero element of $\mathbf{F}_q$. Suppose that for every pair a, b of elements of $\mathbf{F}_q$ which differ by α, either a or b belongs to some given set S. Then $\#S \geq q/2$; i.e., S contains at least half the elements of $\mathbf{F}_q$.*

Proof. Indeed, in this case $\mathbf{F}_q \subset S \cup S'$, where $S' := \{s - \alpha : s \in S\}$. $\square$

The remainder of the proof is divided into three cases:

3.1. Case I: $q \equiv 1 \pmod{l}$ for some odd prime l. Theorem 1 for a given α then follows from Corollary 1 if we can produce a pair of lth power nonresidues of $\mathbf{F}_q$ differing by α. The set of lth powers in $\mathbf{F}_q$ has cardinality $1 + (q-1)/l$, and this is strictly smaller than $q/2$ except when $q = 4$ and $l = 3$ (which will be treated in Case III). We now appeal to Lemma 2, taking for S the set of lth powers in $\mathbf{F}_q$; this finishes the proof whenever $q - 1$ has an odd prime divisor and $q \neq 4$.

3.2. Case II: $q = 1 + 2^k$ for some k. One can show elementarily that the only prime powers q meeting this requirement are $q = 9$ and the Fermat primes (see [24], p. 374, Exercise 1). We apply Corollary 1 with $l = 2$, noting that all the q under consideration satisfy $q \equiv 1 \pmod{4}$ with the single exception of $q = 3$ (which will be treated below). It is straightforward to check directly that every nonzero element of $\mathbf{F}_9$ is a difference of nonsquares. To treat the case when q is a Fermat prime, we note that if p is any odd prime and α any nonzero element of $\mathbf{F}_p$, then the number of pairs of nonsquares in $\mathbf{F}_p$ differing by α is

$$\frac{1}{4} \sum_{\substack{a \pmod p \\ a \not\equiv 0, a+\alpha \not\equiv 0 \pmod p}} \left(1 - \left(\frac{a}{p}\right)\right)\left(1 - \left(\frac{a+\alpha}{p}\right)\right) =$$

$$\frac{1}{4}\left(p + \sum_{a \pmod p} \left(\frac{a}{p}\right)\left(\frac{a+\alpha}{p}\right) - \left(1 - \left(\frac{\alpha}{p}\right)\right) - \left(1 - \left(\frac{-\alpha}{p}\right)\right)\right).$$

q	α	**Twin Prime Pair** $f, f+\alpha$	**Orders**	q^d-1	l
3	1	$T^3-T+1,\ T^3-T+2$	$2\cdot 13,\ 13$	$2\cdot 13$	13
4	1	$T-\beta,\ T-\beta+1$	$3,\ 3$	3	3
	β	$T^2+(\beta+1)T+1, T^2+(\beta+1)T+\beta+1$	$5,\ 3\cdot 5$	$3\cdot 5$	5
	$\beta+1$	$T^2+\beta T+1, T^2+\beta T+\beta$	$5,\ 3\cdot 5$	$3\cdot 5$	5
5	1	$T+2,\ T+3$	$2^2,\ 2^2$	2^2	2
	2	$T^3+T+4,\ T^3+T+1$	$31,\ 2\cdot 31$	$2^2\cdot 31$	31

TABLE 1. Explicit twin prime pairs for small q; in odd characteristic we include only one of $\{\alpha, -\alpha\}$.

Simplifying this expression using the evaluation $\sum \left(\frac{a}{p}\right)\left(\frac{a+\alpha}{p}\right) = -1$ of the Jacobsthal sum (cf. [3], Theorem 2.1.2) gives a count of

$$\frac{1}{4}\left(p-3+\left(\frac{\alpha}{p}\right)+\left(\frac{-\alpha}{p}\right)\right),$$

which is always positive if $p>5$. This settles all cases when $q-1$ has no odd prime divisor, except those corresponding to $q=3$ and $q=5$.

3.3. CASE III: $q = 3$, 4 OR 5. The cases not covered by the above analysis are handled by a direct appeal to Lemma 1. For each q and α, we find a pair of twin prime polynomials $f, f+\alpha$ and a prime l for which the conditions of Lemma 1 hold simultaneously for both f and $f+\alpha$. The pairs $f, f+\alpha$ and the information needed to verify the hypotheses of the lemma are presented in Table 1. For example, the first line of Table 1 describes the proof that the polynomials

$$T^{3\cdot 13^k}-T^{13^k}+1, \quad T^{3\cdot 13^k}-T^{13^k}+2$$

form a twin prime pair over $\mathbf{F}_3$ for each $k=1,2,3,\ldots$. □

Without giving the details, we mention the analogous theorem for prime triplets:

Theorem 4 (Prime triplet theorem)**.** *Let $\mathbf{F}_q$ be a finite field with $q>3$. If α and β are distinct elements of $\mathbf{F}_q^\times$, then there are infinitely many monic prime triplets $f, f+\alpha, f+\beta$ in $\mathbf{F}_q[T]$.*

That such a result is valid for all but finitely many q is immediate from Theorem 2; all that remains is to check the validity of this result over the remaining "small" finite fields $\mathbf{F}_q$, as in our Table 1. This is a straightforward (if somewhat tedious) computation.

4. PROOF OF THEOREM 2

4.1. **A character sum estimate.** The following consequence of Weil's Riemann Hypothesis appears as [26, Corollary 2.2]:

Lemma 3 (Lenstra)**.** *Suppose we are given an n-dimensional commutative $\mathbf{F}_q$-algebra A, an element $x \in A$ and a character χ of the multiplicative group $A^\times$ (extended by zero to all of A) which is nontrivial on $\mathbf{F}_q[x]$. Then*

$$\left| \sum_{\beta \in \mathbf{F}_q} \chi(\beta + x) \right| \leq (n-1)\sqrt{q}.$$

Lemma 4. *Let $f_1(T), \dots, f_s(T)$ be nonassociate irreducible polynomials over $\mathbf{F}_q$. Fix roots $\alpha_1, \dots, \alpha_s$ of $f_1, \dots, f_s$, respectively, lying in an algebraic closure of $\mathbf{F}_q$. Suppose that for every $1 \leq i \leq s$ we are given a multiplicative character χ_i of $\mathbf{F}_q(\alpha_i)$ and that at least one of these χ_i is nontrivial. Then*

$$\left| \sum_{\beta \in \mathbf{F}_q} \chi_1(\alpha_1 + \beta) \cdots \chi_s(\alpha_s + \beta) \right| \leq (D-1)\sqrt{q}, \tag{8}$$

where D is the sum of the degrees of the f_i.

Proof. We argue as in [26, Corollary 2.4]. Define $F := \prod_{i=1}^s f_i$ and set $A := \mathbf{F}_q[T]/(F)$. Thus A is generated over $\mathbf{F}_q$ by the residue class $T \bmod F$. By the Chinese remainder theorem, we obtain a multiplicative character χ on A by setting $\chi(g \bmod F) := \prod_{i=1}^s \chi_i(g(\alpha_i))$. Since some χ_i is nontrivial on $\mathbf{F}_q(\alpha_i)$, we see that χ is nontrivial on A. Moreover, for $\beta \in \mathbf{F}_q$, we have $\chi((\beta + T) \bmod F) = \prod_{i=1}^s \chi(\alpha_i + \beta)$. The result now follows from Lemma 3, since A is an $\mathbf{F}_q$-algebra of dimension $\deg F = \sum_{i=1}^s \deg f_i = D$. □

4.2. **Proof of the main theorem.** We now turn to the proof of Theorem 2. We may assume that the f_i are nonassociate. We will prove that the conclusion of Theorem 2 holds provided $q > 3$ and

$$q + (2^r - 1 - 2^{r-1} \sum_{i=1}^r \deg f_i)\sqrt{q} - 2^{r-1} r > 0. \tag{9}$$

A short computation shows that (2) implies both $q > 3$ and (9), so that Theorem 2 will follow.

Choose roots $\alpha_1, \dots, \alpha_r$ of $f_1, \dots, f_r$, respectively, from a fixed algebraic closure of $\mathbf{F}_q$. We can fix l so that one of the following two conditions holds:

(i) l is an odd prime dividing $q-1$,
(ii) $l = 2$ and $q \equiv 1 \pmod 4$.

Indeed, since $q > 3$, if there is no l for which (i) holds, then the choice $l = 2$ always satisfies (ii).

Lemma 5. *Assuming the above notation and hypotheses, there always exists an element $\beta \in \mathbf{F}_q$ with the property that for every $1 \leq i \leq r$,*

$$\alpha_i + \beta \text{ is not an } l\text{th power (vanishing or otherwise) in } \mathbf{F}_q(\alpha_i).$$

Proof. For each $i = 1, 2, \ldots, r$, fix a multiplicative character χ_i of order l on $\mathbf{F}_q(\alpha_i)$. By Lemma 4, we can bound from below the absolute value of the sum

$$\sum_{\beta \in \mathbf{F}_q} (1 - \chi_1(\alpha_1 + \beta))(1 - \chi_2(\alpha_2 + \beta)) \cdots (1 - \chi_r(\alpha_r + \beta)) \tag{10}$$

by

$$\begin{aligned} q - \sum_{\substack{\mathcal{I} \subset \{1,2,\ldots,r\} \\ \mathcal{I} \neq \emptyset}} \left(-1 + \sum_{i \in \mathcal{I}} \deg f_i \right) \sqrt{q} \qquad (11) \\ = q + (2^r - 1)\sqrt{q} - \sum_{i=1}^{r} \deg f_i \left(\sum_{\substack{\mathcal{I} \subset \{1,2,\ldots,r\} \\ i \in I}} 1 \right) \sqrt{q} \\ = q + (2^r - 1)\sqrt{q} - 2^{r-1} \left(\sum_{i=1}^{r} \deg f_i \right) \sqrt{q} > 2^{r-1} r, \end{aligned}$$

using (9) for the last inequality. Suppose that for each $\beta \in \mathbf{F}_q$, there is an $i = i(\beta)$ for which $\alpha_i + \beta$ is an lth power in $\mathbf{F}_q(\alpha_i)$. If $\alpha_i + \beta$ is nonzero for this i, then the summand corresponding to β in (10) vanishes, while if $\alpha_i + \beta = 0$, then the corresponding summand has absolute value at most 2^{r-1}. Since the latter is possible for at most r values of β, the sum (10) is bounded above by $2^{r-1}r$, contradicting (11). □

Proof of Theorem 2. With β as in Lemma 5, apply the substitution $T \mapsto T - \beta$ to the sequence of polynomials $f_1, \ldots, f_r$. This yields a new sequence $h_1, \ldots, h_r$ (say) of irreducible polynomials over $\mathbf{F}_q$ with corresponding nonzero roots $\alpha_1 + \beta, \ldots, \alpha_r + \beta$. By Lemma 1 all the polynomials

$$h_1(T^{l^k}) = f_1(T^{l^k} - \beta), \ldots, h_r(T^{l^k}) = f_r(T^{l^k} - \beta) \quad \text{for } k = 0, 1, 2, \ldots$$

are irreducible, which proves the theorem. □

Example. Let α be any nonsquare in $\mathbf{F}_q^\times$; we show that there are infinitely many monic primes in $\mathbf{F}_q[T]$ of the form $f^2 - \alpha$. By Theorem 2 (with $r = 1$ and $f_1(T) = T^2 - \alpha$), we know this is true for all large q; referring to (9) shows that $q > 3$ is large enough. When $q = 3$,

we must have $\alpha = -1$, and we can treat this case directly. Indeed, the irreducible polynomial $(T+1)^2+1$ has order $8 = 3^2-1$, and so Lemma 1 shows that $(T^{2^k}+1)^2+1$ is irreducible over $\mathbf{F}_3$ for every $k = 0, 1, 2, \dots$.

Example. Let $f(x,y)$ be an irreducible binary form over $\mathbf{F}_q$ of degree $n \geq 2$. We claim that if $q > q_0(n)$, then $f(A, A+1)$ is irreducible for infinitely many monic A. Since $n \geq 2$, we may express f as the homogenization of an irreducible degree n polynomial g:

$$f(x,y) = y^n g(x/y), \quad \text{where} \quad g(T) = a_n T^n + a_{n-1}T^{n-1} + \cdots + a_0.$$

The polynomial $f(T, T+1)$ has leading coefficient $g(1) \neq 0$ and degree n. Let α be a root of $f(T, T+1)$; since $f(-1,0) = a_n(-1)^n \neq 0$, we have $\alpha \neq -1$. Now $\alpha/(\alpha+1)$ is a root of g and so has degree n over $\mathbf{F}_q$. But then α must also have degree n, which yields the irreducibility of $f(T, T+1)$. The original assertion is now obtained by applying Theorem 2 to $f(T, T+1)$. Actually for $q > q_1(n)$, the same statement holds even if we require also that A and $A+1$ are prime, as we see by applying Theorem 2 to the three polynomials T, $T+1$, and $f(T, T+1)$.

5. Proof of Theorem 3

Lemma 6. *Fix a finite field $\mathbf{F}_q$. For each $d \geq 2$,*

$$\#\mathcal{E}_d \leq \frac{1}{\mathrm{rad}'(q^d-1)} \frac{q^d-1}{d}. \tag{12}$$

Proof. Let E be the set of elements of $\mathbf{F}_{q^d}$ whose minimal polynomials belong to $\mathcal{E}_d$. By Lemma 1, each α in E is an lth power for every odd prime $l \mid q^d-1$, so is an Lth power for

$$L := \prod_{\substack{l \text{ odd prime} \\ l \mid q^d-1}} l = \mathrm{rad}'(q^d-1).$$

Thus $\#E \leq \#(\mathbf{F}_{q^d}^\times)^L = (q^d-1)/L$. But the action of $\mathrm{Gal}(\mathbf{F}_{q^d}/\mathbf{F}_q)$ partitions E into orbits of length d, each of which corresponds to a single element of $\mathcal{E}_d$. This proves (12). □

Proof of the upper bounds (3) *and* (4) *on* $\#\mathcal{E}_d$. To prove (3), note that if $d > 6$ (as we can assume) then by Bang's theorem (see, e.g., [21]) there is a primitive prime divisor l of q^d-1. Then $l \equiv 1 \pmod{d}$, and so in particular $L \geq l > d$. Lemma 6 now gives (3). The *abc*-conjecture implies that for each $\epsilon > 0$,

$$L \geq \frac{1}{2}\mathrm{rad}(q^d-1) \gg_\epsilon q^{d(1-\epsilon)-1},$$

and this proves (4). □

Remark. Actually one can do a bit better unconditionally than stated in Theorem 3; for example, the results of Stewart & Yu toward the *abc*-conjecture [25] imply that $\mathrm{rad}'(q^d-1) \geq d^{3+o_q(1)}$ as $d \to \infty$, leading to a corresponding (unconditional but no longer elementary) upper bound of $q^d/d^{4+o_q(1)}$.

Proof that $\mathcal{E}_d$ is empty for almost all d, assuming (5). It is enough to prove that for almost all d, no element of $\mathbf{F}_{q^d}$ of degree d over $\mathbf{F}_q$ is an Lth power for $L := \mathrm{rad}'(q^d-1)$. Suppose, contrariwise, that α is such an element. Let

$$Q := \frac{q^d-1}{L} \quad \text{and let} \quad m := l_q(Q).$$

Then trivially $m \leq d$. Now $\alpha^Q = 1$ (as α is a nonzero Lth power), so that

$$\alpha^{q^m} = \alpha \left(\alpha^Q\right)^{\frac{q^m-1}{Q}} = \alpha.$$

Thus α has degree $\leq m$ over $\mathbf{F}_q$ and so $d \leq m \leq d$. So $m = d$.

Now fix a large positive number B. We may restrict attention to those d with a prime factor $> B$, since the exceptional d have density 0. Given d of this type, let $l > B$ be its largest prime factor. As $m = d$, it follows that l divides $m = l_q(Q)$, and so l divides $l_q(R)$ for some prime power $R \parallel Q$. If R is a power of the prime r, then necessarily $r \geq l > B$, and from $r \mid Q$ we deduce that

$$r^2 \mid rQ = \frac{q^d-1}{L/r} \mid q^d - 1,$$

so that $l_q(r^2) \mid d$.

Thus d is divisible by $l_q(r^2)$ for some prime $r > B$. But the number of such $d \leq x$ is

$$\leq \epsilon_B x, \quad \text{where} \quad \epsilon_B := \sum_{\substack{r>B \\ r \text{ prime} \\ r \nmid q}} \frac{1}{l_q(r^2)}.$$

So the upper density of such d is bounded by ϵ_B; but (5) implies that $\epsilon_B \to 0$ as $B \to \infty$. □

Example. In practice it is rare that $d = m$, which as we have just seen is forced upon us if $\mathcal{E}_d \neq \emptyset$. Consider, e.g., the case $q = 2$. At the time of writing, the first d for which the complete factorization of $2^d - 1$ is not known is $d = 787$ (see [5]). Using the known factorizations for

smaller d, one can calculate that $m < d$ for all $d < 787$, except for $d = 364$. In that case

$$\frac{2^{364}-1}{\mathrm{rad}'(2^{364}-1)} = 1093 \quad \text{and} \quad l_2(1093) = 364.$$

Thus the only polynomials $f(T)$ of degree 364 over $\mathbf{F}_2$ for which Buniakowsky's conjecture can fail are those with a root $\alpha \in \mathbf{F}_{2^{364}}$ with $\alpha^{1093} = 1$. Now if $f(T)$ has this property, replace $f(T)$ with $f(T-1)$. This has the root $\alpha + 1$, and we cannot have both

$$\alpha^{1093} = 1 \quad \text{and} \quad (\alpha+1)^{1093} = 1 \quad \text{in } \mathbf{F}_{2^{364}},$$

since one can compute that the resultant

$$\mathrm{Res}(T^{1093}-1, (T+1)^{1093}-1) \not\equiv 0 \pmod 2.$$

So Bouniakowsky's conjecture must hold for $f(T-1)$, and so also for our original f. We conclude that Bouniakowsky's conjecture holds for every irreducible of degree $d < 787$.

Appendix: A heuristic argument for Conjecture 2

When q is fixed and n tends to infinity, Conjecture 2 is totally analogous to the Bateman-Horn conjecture [1] and is suggested by a completely parallel argument. In order to explain why we should expect the asymptotic relation (6) to hold in the wider range $q^n \to \infty$, we need to revisit the heuristic. The following approach leads to a uniform prediction that looks superficially different from that of Conjecture 2, but which will be shown identical in Lemma 7.

Write d_i for the degree of f_i. Fix roots $\alpha_1, \dots, \alpha_r$ of $f_1, \dots, f_r$ from an algebraic closure of $\mathbf{F}_q$. We begin by observing that $f_i(g(T))$ is irreducible over $\mathbf{F}_q$ precisely when $g(T) - \alpha_i$ is irreducible over $\mathbf{F}_{q^{d_i}}$. Thus the left hand side of (6) counts the number of monic, degree n polynomials $g(T)$ in $\mathbf{F}_q[T]$ for which the r-tuple $(g(T)-\alpha_1, \dots, g(T)-\alpha_r)$ has its ith coordinate irreducible over $\mathbf{F}_{q^{d_i}}$ for each $1 \le i \le r$. A random monic polynomial of degree n over $\mathbf{F}_{q^{d_i}}$ is prime with probability about $1/n$ (more precisely, with probability $(1 + o_B(1))/n$). So if our r-tuple behaves randomly in the appropriate sense, we expect the left hand side of (6) to be roughly q^n/n^r.

A more precise answer requires us to quantify the deviations from randomness. To each monic prime P of $\mathbf{F}_q[T]$, we assign a correction factor C_P, viz. the ratio of the probability that P is coprime to all the polynomials $g(T) - \alpha_i$ compared to the probability that P is coprime to all the members of a randomly chosen r-tuple of polynomials with

the ith one in $\mathbf{F}_{q^{d_i}}[T]$. Since P has coefficients from $\mathbf{F}_q$, we know that P has a factor in common with $g(T) - \alpha_i$ precisely when P divides

$$\prod_{\sigma \in \mathrm{Gal}(\mathbf{F}_{q^{d_i}}/\mathbf{F}_q)} (g(T) - \sigma(\alpha_i)) = f_i(g(T)).$$

It follows that P has a factor in common with some $g(T) - \alpha_i$ precisely when $g(T)$ belongs to one of $\omega(P)$ residue classes mod P.

On the other hand, a random r-tuple of monic polynomials whose ith component has coefficients from $\mathbf{F}_{q^{d_i}}$ has all its components coprime to P with probability

$$\prod_{i=1}^{r} \frac{\varphi_{q^{d_i}}(P)}{q^{d_i \deg P}}.$$

Suppose $\deg P = m$. Over $\mathbf{F}_{q^{d_i}}$, the prime P splits into (m, d_i) distinct monic irreducibles of degree $m/(m, d_i)$, and hence

$$\frac{\varphi_{q^{d_i}}(P)}{q^{d_i \deg P}} = \left(1 - \frac{1}{q^{d_i m/(m,d_i)}}\right)^{(m,d_i)}.$$

We therefore set

$$C_P := \frac{1 - \omega(P)/q^m}{\prod_{i=1}^{r} \left(1 - q^{-d_i m/(m,d_i)}\right)^{(m,d_i)}}.$$

Notice that since the f_i are coprime univarate polynomials over $\mathbf{F}_q$, we can write $\omega(P) = \sum \omega_i(P)$, where $\omega_i(P)$ is the number of incongruent roots of f_i modulo P. Moreover, $\omega_i(P)$ is zero unless d_i divides m, in which case $\omega_i(P) = d_i$. Thus

$$C_P = \left(\frac{1 - \sum_{\substack{1 \le i \le r \\ d_i \mid m}} d_i/q^m}{\prod_{\substack{1 \le i \le r \\ d_i \mid m}} (1 - q^{-m})^{d_i}}\right) \prod_{\substack{1 \le i \le r \\ d_i \nmid m}} \frac{1}{\left(1 - q^{-d_i m/(m,d_i)}\right)^{(m,d_i)}} = 1 + O_B(q^{-2m}). \tag{13}$$

We now set

$$\mathfrak{S}'(f_1, \dots, f_r) := \prod_{m=1}^{\infty} \prod_{\deg P = m} C_P.$$

Notice that C_P depends on P only through its degree m; thus (13), along with the estimate $q^m/m + O(q^{m/2}/m)$ for the number of monic primes of degree m, together imply that the contribution to the product from degree m primes is $1 + O_B(m^{-1}q^{-m})$. It follows that the product is absolutely convergent and that

$$\mathfrak{S}'(f_1, \dots, f_r) = 1 + O_B(1/q). \tag{14}$$

Since our local condition guarantees every term in the product is positive, we also have $\mathfrak{S}'(f_1, \dots, f_r) > 0$.

So our revised guess for the number of monic degree n polynomials g for which all of $f_1(g(T)), \dots, f_r(g(T))$ are irreducible is

$$\mathfrak{S}'(f_1, \dots, f_r)\frac{q^n}{n^r}.$$

There is perhaps some reason for suspicion here: e.g., we might think that the product defining $\mathfrak{S}'(f_1, \dots, f_r)$ should be restricted to primes of degree bounded in terms of n. However, since the degree m primes contribute $1 + O_B(m^{-1}q^{-m})$, as long as the bound for the degree of P tends to infinity with n, the resulting partial product is still $(1 + o_B(1))\mathfrak{S}'(f_1, \dots, f_r)$ as $q^n \to \infty$. This suggests the truth of a modified Conjecture 2, where the factor $\mathfrak{S}(f_1, \dots, f_r)/\prod_{1\le i\le r} d_i$ is replaced by $\mathfrak{S}'(f_1, \dots, f_r)$.

Hence the derivation will be complete if we can establish the following identity:

Lemma 7. *With notation as above,*

$$\mathfrak{S}'(f_1, \dots, f_r) = \frac{\mathfrak{S}(f_1, \dots, f_r)}{\prod_{1\le i\le r} d_i}.$$

Below we write $\zeta_q(s)$ for the zeta function of the ring $\mathbf{F}_q[T]$, defined for $\Re(s) > 1$ by

$$\zeta_q(s) = \sum_{A \text{ monic}} \frac{1}{q^{s \deg A}}.$$

In the same region $\zeta_q(s)$ admits the Euler product expansion $\zeta_q(s) = \prod_P (1 - q^{-s \deg P})^{-1}$. Moreover,

$$\zeta_q(s) = \sum_{m=0}^{\infty} \frac{q^m}{q^{ms}} = \frac{1}{1 - q^{1-s}},$$

which provides the meromorphic continuation to the entire complex plane. Note that $\zeta_q(s)$ coincides with the usual zeta function of the rational function field $\mathbf{F}_q(T)$ up to a missing factor from the $(1/T)$-adic valuation.

Proof of Lemma 7. Comparing the products defining $\mathfrak{S}(f_1, \dots, f_r)$ and $\mathfrak{S}'(f_1, \dots, f_r)$, we see that

(15)
$$\mathfrak{S}'(f_1, \dots, f_r) = \mathfrak{S}(f_1, \dots, f_r) \prod_{m=1}^{\infty} \prod_{\deg P = m} \frac{(1 - 1/q^m)^r}{\prod_{i=1}^r (1 - q^{-d_i m/(m,d_i)})^{(m,d_i)}}.$$

Using R to denote a generic monic prime polynomial over $\mathbf{F}_{q^{d_i}}$, we have

$$\begin{aligned}\zeta_{q^{d_i}}(s) &= \prod_R \left(1 - 1/q^{sd_i \deg R}\right)^{-1} \\ &= \prod_P \prod_{R|P} (1 - 1/q^{sd_i \deg R})^{-1} = \prod_P (1 - 1/q^{sd_i m/(m,d_i)})^{-(m,d_i)},\end{aligned}$$

where as usual we write m for the degree of P. Thus for $s > 1$,

$$\begin{aligned}(16)\quad \prod_{m=1}^{\infty} \prod_{\deg P = m} \frac{(1-1/q^{ms})^r}{\prod_{i=1}^r (1 - q^{-sd_i m/(m,d_i)})^{(m,d_i)}} &= \frac{1}{\zeta_q(s)^r} \prod_{i=1}^r \zeta_{q^{d_i}}(s) \\ &= \prod_{i=1}^r \frac{1 - q^{1-s}}{1 - q^{d_i(1-s)}} = \prod_{i=1}^r \frac{1}{1 + q^{1-s} + \cdots + q^{(d_i-1)(1-s)}}.\end{aligned}$$

So if we know that the double product (16) is continuous for $s \geq 1$, then taking the limit in (16) as $s \downarrow 1$ shows that the right hand side of (15) is precisely $\mathfrak{S}(f_1, \ldots, f_r)/\prod_{1 \leq i \leq r} d_i$, as desired.

To prove continuity, it is enough to show that for fixed $f_1, \ldots, f_r$, the series

$$(17)\qquad \sum_{m=1}^{\infty} \log \prod_{\deg P = m} \frac{(1-1/q^{ms})^r}{\prod_{i=1}^r (1 - q^{-sd_i m/(m,d_i)})^{(m,d_i)}}$$

converges uniformly for $s \geq 1$. Let $a_m = r - \sum_{\substack{d_i | m \\ 1 \leq i \leq r}} d_i$, so that the term in (17) corresponding to m is

$$\begin{aligned}&\left(\frac{q^m}{m} + O\left(\frac{q^{m/2}}{m}\right)\right)\left(-\frac{a_m}{q^{ms}} + O_B(q^{-2ms})\right) \\ &\qquad = -\frac{a_m}{m q^{m(s-1)}} + O_B(m^{-1} q^{-m(s-1/2)}).\end{aligned}$$

Note that the partial sums $\sum_{m \leq x} a_m$ are bounded; indeed,

$$\sum_{m \leq x} \sum_{\substack{i=1 \\ d_i | m}}^r d_i = \sum_{i=1}^r d_i \left\lfloor \frac{x}{d_i} \right\rfloor = rx + O_B(1).$$

The uniform convergence of (17) for $s \geq 1$ now follows by Abel summation. □

Acknowledgements

The encouragement and advice of Carl Pomerance, my advisor, has been invaluable. I would also like to thank Andrew Granville, Keith

Conrad and an anonymous referee for their comments on earlier versions of this manuscript. In particular, the current (uniform) formulation of Conjecture 2 is due to the nudging of Professors Granville and Pomerance. Finally, I would like to express my gratitude to the organizers of the Anatomy of Integers conference in Montréal for the opportunity to present on this topic and to the editors of these Proceedings for inviting this article.

References

[1] P. T. Bateman and R. A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[2] A. O. Bender and O. Wittenberg. A potential analogue of Schinzel's hypothesis for polynomials with coefficients in $\mathbf{F}_q[t]$. *Int. Math. Res. Not.*, 36:2237–2248, 2005.

[3] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons Inc., New York, 1998. A Wiley-Interscience Publication.

[4] V. Bouniakowsky. Sur les diviseurs numériques invariables des fonctions rationnelles entières. *Mémoires sc. math. et phys.*, 6:306–329, 1854.

[5] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of $b^n \pm 1$*, volume 22 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, third edition, 2002. Updates available at `http://homes.cerias.purdue.edu/~ssw/cun/`.

[6] M. Car. Polynômes irréductibles de $F_q[X]$ de la forme $M + N$ où N est norme d'un polynôme de $F_{q^2}[X]$. *Dissertationes Math. (Rozprawy Mat.)*, 238:50, 1984.

[7] ———. Le théorème de Chen pour $\mathbf{F}_q[X]$. *Dissertationes Math. (Rozprawy Mat.)*, 223:54, 1984.

[8] J. Cherly. A lower bound theorem in $F_q[x]$. *J. Reine Angew. Math.*, 303/304:253–264, 1978.

[9] S. D. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255–271, 1970.

[10] B. Conrad, K. Conrad, and R. Gross. Prime specialization in genus 0. Transactions of the AMS (to appear); available electronically at `http://www.math.lsa.umich.edu/~bdconrad/papers/hlsingle.pdf`, 2006.

[11] L. E. Dickson. Higher irreducible congruences. *Bull. Amer. Math. Soc.*, 3:381–389, 1897.

[12] ———. *Linear groups: with an exposition of the Galois field theory*. With an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[13] A. Granville and K. Soundararajan. A binary additive problem of Erdős and the order of 2 mod p^2. *Ramanujan J.*, 2(1-2):283–298, 1998. Paul Erdős (1913–1996).

[14] C. Hall. L-functions of twisted Legendre curves. *J. Number Theory*, 119(1):128–147, 2006.

[15] D. R. Heath-Brown. Primes represented by $x^3 + 2y^3$. *Acta Math.*, 186(1):1–84, 2001.

[16] C.-N. Hsu. A large sieve inequality for rational function fields. *J. Number Theory*, 58(2):267–287, 1996.
[17] H. Kornblum. Über die Primfunktionen in einer arithmetischen Progression. *Math. Zeitschrift*, 5:100–111, 1919.
[18] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
[19] P. Pollack. Counting irreducibility-preserving substitutions for polynomials over finite fields. Submitted.
[20] R. Ree. Proof of a conjecture of S. Chowla. *J. Number Theory 3 (1971), 210–212; erratum, 4:223*, 1972.
[21] M. Roitman. On Zsigmondy primes. *Proc. Amer. Math. Soc.*, 125(7):1913–1919, 1997.
[22] A. Schinzel and W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith. 4 (1958), 185–208; erratum, 5:259*, 1958.
[23] J.-A. Serret. Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modulaire irréductible. *Mémoires de l'Académie des sciences de l'Institut Impérial de France*, 35:617–688, 1866.
[24] W. Sierpiński. *Elementary theory of numbers*, volume 31 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, second edition, 1988. Edited and with a preface by Andrzej Schinzel.
[25] C. L. Stewart and K. Yu. On the *abc* conjecture. II. *Duke Math. J.*, 108(1):169–181, 2001.
[26] D. Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.

Department of Mathematics, Dartmouth College, Hanover, NH
E-mail address: paul.pollack@dartmouth.edu