IRREDUCIBILITY-PRESERVING SUBSTITUTIONS FOR POLYNOMIALS OVER FINITE FIELDS

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. We examine a version of this conjecture with the ring of integers $\mathbf{Z}$ replaced by the ring of polynomials $\mathbf{F}_q[u]$ over a finite field, restricting our attention to polynomials with constant coefficients (i.e., with coefficients from $\mathbf{F}_q$ instead of $\mathbf{F}_q[u]$). Our principal result is that if $f_1, \dots, f_r \in \mathbf{F}_q[T]$ are irreducible and if q is sufficiently large (depending only on r and the sum of the degrees of the f_i), then there are infinitely many substitutions $T \mapsto g(T)$ which preserve the irreducibility of every f_i. Our work extends the methods used by Hall ([16], pp. 14-15) in his proof of a twin prime conjecture in the polynomial setting.

1. INTRODUCTION

In 1854, Bouniakowsky [6] 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 [21] with Sierpiński) proposed the following generalization, which contains (implicitly or more or less explicitly) many classical conjectures in number theory:

Hypothesis H. *Suppose that $f_1(T), f_2(T), \dots, f_r(T)$ are irreducible polynomials over the integers. Moreover, suppose that there is no prime p for which every integer n satisfies the congruence*

$$f_1(n)f_2(n)\cdots f_r(n) \equiv 0 \pmod{p}.$$

Then for infinitely many positive integers n, the evaluations $f_1(n), \dots, f_r(n)$ are simultaneously prime (positive or negative).

The numerical and heuristic evidence for this conjecture (even in a stronger, quantitative form) is nearly overwhelming. Yet it remains unproved in all but the simplest case, corresponding to prime values of a single linear polynomial (Dirichlet's theorem on primes in arithmetic progressions).

In light of the strong analogy between number fields and function fields, it is natural to wonder whether Hypothesis H has an analogue in the ring of one-variable polynomials over a finite field $\mathbf{F}_q$. (For an exploration of the many analogies between $\mathbf{Z}$ and the one-variable polynomial ring over a finite field, we recommend the opening chapters of Rosen's monograph [20] as well as the expository account of Effinger, Hicks and Mullen [14].) The following conjecture appears to be a plausible partial answer to this query:

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

Hypothesis H over $\mathbf{F}_q[u]$. *Let $f_1(T), \dots, f_r(T)$ be irreducible polynomials belonging to $\mathbf{F}_q[u][T]$. Suppose that there is no prime $\pi \in \mathbf{F}_q[u]$ for which every $g \in \mathbf{F}_q[u]$ satisfies*

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

Moreover, suppose that all the f_i are separable over $\mathbf{F}_q(u)$; i.e., that none of the f_i lie in $\mathbf{F}_q[u][T^p]$. Then the specializations $f_1(g), \cdots, f_r(g)$ are simultaneously irreducible for infinitely many monic $g \in \mathbf{F}_q[u]$.

This is a direct translation of the usual Hypothesis H into the language of polynomials, save for one surprise: we have required here that the f_i be separable over $\mathbf{F}_q(u)$. This condition is *not* necessary for the f_i to possess infinitely many prime specializations (see the example of §2). But separability does play an important role, brought to light by Conrad, Conrad & Gross ([9]; see also the survey [11]). They investigate a quantitative version of the polynomial Hypothesis H; when all the polynomials are involved are separable over $\mathbf{F}_q(u)$, they find that the naive analogue of the Bateman-Horn/Hardy-Littlewood conjectures appears intact, but for general polynomials it is necessary to introduce a correction factor, the conjectural behavior of which they proceed to examine in detail. (The results of [9] and [11] are stated for a single polynomial, i.e., the case $r = 1$; however, as remarked in [10], the methods extend to finite collections as well.)

As an extreme illustration of what can go wrong, one can write down an irreducible, inseparable polynomial which meets the local conditions of Hypothesis H but which has no prime specializations at all: $f(T) = T^{4q} + u^{2q-1}$ provides such an example over any finite field $\mathbf{F}_q$ ([11], Example 4.3). Rather than dive into deep waters not of particular concern to us here, we have taken the cautionary route of incorporating the separability hypothesis into our statement above.

Dirichlet's techniques again suffice to prove the $\mathbf{F}_q[u]$-Hypothesis H in the case of a single polynomial linear in T; this was first worked out by Kornblum [17] (see also [20], Chapter 2). More surprising is that in the polynomial setting we are not limited to these examples, as illustrated by the following 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 $\mathbf{F}_q[T]$.*

The cases of Theorem 1 when $\alpha = 1$ and $q \neq 2, 3$ are treated in Hall's doctorial thesis ([16], pp. 14-15). In §3 we present a self-contained proof of the above theorem as a way of initiating the reader to our techniques. Prior to the work of Hall, sieve methods had been used by Cherly ([7], Theorem 1.2) to show that f and $f + \alpha$ infinitely often each have at most four prime factors (counted with multiplicity).

In this paper we consider more generally the polynomial Hypothesis H when the f_i are *pure polynomials* in T, by which we mean that the coefficients of the f_i are restricted to lie in $\mathbf{F}_q$ (instead of $\mathbf{F}_q[u]$). Note that in this scenario the separability hypothesis is automatic, since now all the $f_i(T)$ are irreducible over $\mathbf{F}_q[T]$ while the finite field $\mathbf{F}_q$ is perfect.

Our main theorem is as follows:

Theorem 2. *Let $f_1(T), \dots, f_r(T)$ be irreducible polynomials over $\mathbf{F}_q[T]$. If q is sufficiently large (depending on 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*

$$T \mapsto T^{l^k} - \beta \quad \textit{with} \quad k = 1, 2, 3, \dots$$

leaves all of $f_1, \dots, f_r$ irreducible. Consequently the polynomial version of Hypothesis H is true for a family of pure polynomials in T provided q is sufficiently large.

Explicitly, if we suppose (as may be done without loss of generality) that the f_i are pairwise nonassociated, then the above conclusion holds provided $q > 3$ and

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

Remark. Since (2) is not entirely transparent, it may be helpful to remark that (2) is satisfied whenever

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

as a short computation shows. Since $q > 3$ in this case as well, this condition suffices to guarantee the conclusion of Theorem 2.

It may be initially troubling that there is no local condition appearing in the statement of our result; however, the assumption that q is large obviates the need for such a hypothesis. The proof of Theorem 2 is based on the ideas of Hall and an estimate for incomplete character sums derived from Weil's Riemann Hypothesis.

Notation. For E/F a finite extension of fields, we use $\mathrm{Nm}_{E/F}$ and $\mathrm{Tr}_{E/F}$ to denote the norm and trace maps respectively from E down to F.

2. Our Fundamental Lemma and Plan of Attack

A key ingredient in our work is the following lemma asserting that under appropriate hypothesis on f and l, the entire family of substitutions $T \mapsto T^{l^k}$ (with $k = 1, 2, \dots$) leaves f irreducible. The lemma dates back (even in a stronger form) to Serret ([22], Théorème I, p. 656) and Dickson ([12], p. 382; see also [13], §34), but excepting the recent work of Hall its applications to Hypothesis H seem to have gone unnoticed.

Recall that if $f(T) \in \mathbf{F}_q[T]$ is an irreducible polynomial not a constant multiple of T, then by the *order of f* we mean the order of any of its roots in the multiplicative group of its splitting field (equivalently, the order of T in the unit group $(\mathbf{F}_q[T]/f)^{\times}$). Thus if f has degree d, the order of f is a divisor of $q^d - 1$.

Lemma 3 (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*

$$l \text{ divides } e \quad \text{but} \quad l \text{ does not divide } (q^d - 1)/e. \tag{3}$$

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

Example 1. We give a quick illustration of Lemma 3. Take $q = p = 7$ and $f(T) = T - 3$. Then $d = 1$. In this case e is the order of 3 modulo 7, so that $e = 6$. We now see that the conditions of the lemma hold with $l = 3$, and we conclude that $u^{3^k} - 3$ is irreducible in $\mathbf{F}_7[u]$ for every $k = 1, 2, 3, \dots$. Consequently, for every j the polynomial Hypothesis H holds for $T^{3^j} - 3 \in \mathbf{F}_q[u][T]$. Taking this observation in a different direction, note that when 6 divides k, the prime $p = 7$ divides $3^k - 1$, so that we may write

$$u^{3^k} - 3 = u \cdot u^{3^k - 1} - 3 = u(u^{(3^k-1)/7})^7 - 3.$$

This implies that the conclusion of the polynomial Hypothesis H holds also for $f(T) := uT^7 - 3 \in \mathbf{F}_q[u][T]$. This last example is of theoretical interest because f is inseparable over $\mathbf{F}_7(u)$.

We now describe our overall strategy for proving Theorem 2. Let $f_1, f_2, \dots, f_r$ be given irreducible polynomials over $\mathbf{F}_q[T]$. If we choose a prime l for which the hypotheses of Lemma 3 are satisfied simultaneously with respect to every f_i, then the conclusion of Theorem 2 follows immediately: all the substitutions $T \mapsto T^{l^k}$, where $k = 1, 2, 3, \dots$, preserve the irreducibility of the f_i. Of course there is no *a priori* guarantee that such an l exists.

Theorem 2 is proved by showing that for large enough q there is always such an l, provided 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 $\beta \in \mathbf{F}_q$. Theorem 1 is proved in the same way (with $f_1(T) = T$ and $f_2(T) = T + \alpha$), but the technical details can be handled in a more elementary way. It should be noted that this line of attack only proves Theorem 1 for large q. In the proof of Theorem 1 the small q must be handled individually, and ultimately we appeal to Lemma 3 directly in each case.

3. Proof of Theorem 1

The following is a simple but useful corollary of Lemma 3 on the irreducibility of binomials. It is essentially this result that Hall appealed to in his thesis, deducing it not from Lemma 3 but from Capelli's general theorem on the irreducibility of binomials (see [18], Theorem 9.1).

Corollary 4. *Let l be an odd prime. If $\beta \in \mathbf{F}_q$ is not an lth power, then*

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

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

We also require the following simple combinatorial observation:

Lemma 5. *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 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 $S' := \{s - \alpha : s \in S\}$. □

We now prove Theorem 1, dividing the argument into three cases. In the first two cases we distinguish between whether or not $q - 1$ has an odd prime divisor; in each case the large q of the corresponding type can be handled by a uniform argument, but small q must be treated separately. These small q we treat individually in the third case.

3.1. Case I: $q \equiv 1 \pmod l$ for some odd prime l. Theorem 1 for a given α then follows from Corollary 4 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 $q/2$ in the cases under consideration except when $q = 4$ and $l = 3$ (which will be treated in Case III). We now appeal to Lemma 5, 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 [23], p. 374, Exercise 1). We apply Corollary 4 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 Fermat primes, 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

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

simplifying this expression using the well-known evaluation $\sum \left(\frac{a}{p}\right)\left(\frac{a+\alpha}{p}\right) = -1$ of the Jacobsthal sum (cf. [5], 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 3. 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 3 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 $k = 1, 2, 3, \ldots$. □

It is likely possible to prove the result analogous to Theorem 1 for prime triples $f, f+\alpha, f+\beta$ (when $q > 3$), but working out the details may take some computational chutzpah. (That such a result is valid for all but finitely many q is immediate from Theorem 2; the task here is to check the validity of this result over the remaining "small" finite fields $\mathbf{F}_q$, as in our Table 1.)

4. Proof of Theorem 2

We begin by establishing an estimate for incomplete character sums. The proof uses the following consequence of Weil's Riemann Hypothesis (see [24], Corollary 2.2):

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

Table 1. Explicit twin prime pairs for small q. Each q and α is shown together with a pair of twin prime polynomials $f, f+\alpha$, the respective order of these polynomials, the size of q^d-1 (where d is the degree of f) and a prime l for which Lemma 3 can be applied to the given pair simultaneously.

Lemma 6 (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 7. *Let $f_1(T), \dots, f_s(T)$ be pairwise-nonassociated 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 each $i = 1, 2, \dots, s$ we have a character χ_i of $\mathbf{F}_q(\alpha_i)$ and that at least one of these χ_i is nontrivial. Then*

$$\left|\sum_{\beta\in\mathbf{F}_q} \chi_1(\alpha_1+\beta)\cdots\chi_s(\alpha_s+\beta)\right| \leq (D-1)\sqrt{q}, \tag{4}$$

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

Proof. We argue as in [24], Corollary 2.4. Define $F := f_1 f_2 \cdots f_s$, so that D is the degree of F. The composite map

$$\begin{aligned} \mathbf{F}_q[T]/(F) \cong &\mathbf{F}_q[T]/(f_1) \times \cdots \times \mathbf{F}_q[T]/(f_s) \cong \mathbf{F}_q(\alpha_1) \times \cdots \times \mathbf{F}_q(\alpha_s) \\ &g \mapsto (g \bmod f_1, \dots, g \bmod f_s) \mapsto (g(\alpha_1), \dots, g(\alpha_s)) \end{aligned}$$

is a ring-isomorphism, and so we obtain a multiplicative character χ on the $\mathbf{F}_q$-algebra $A := \mathbf{F}_q[T]/(F)$ by setting

$$\chi(g \bmod F) := \prod_{i=1}^{s} \chi_i(g(\alpha_i)).$$

Moreover, using the surjectivity of the isomorphism and the hypothesis that χ_i is nontrivial on $\mathbf{F}_q(\alpha_i)$ for at least one i, it follows that χ is a nontrivial character of

A. Now observe that for $\beta \in \mathbf{F}_q$,

$$\begin{aligned}\chi((\beta - T) \bmod F) &= \prod_{i=1}^{s} \chi_i(\beta - \alpha_i) \\ &= \prod_{i=1}^{s} \chi_i(-1) \prod_{i=1}^{s} \chi_i(\alpha_i - \beta).\end{aligned}$$

The first factor on the right hand side is independent of β and lies on the unit circle. To complete the proof we sum over β and invoke Lemma 6 (with $x = T \bmod F$), noting that the algebra $\mathbf{F}_q[T]/(F)$ has degree $D = \deg F$ over $\mathbf{F}_q$. □

We now turn to the proof of Theorem 2. We may assume that no f_i is a unit multiple of f_j for $i \neq j$. We also assume $q > 3$ and that q is large enough that (2) holds. Choose roots $\alpha_1, \ldots, \alpha_r$ of $f_1, \ldots, f_r$ respectively from a fixed algebraic closure of $\mathbf{F}_q$. Fix l so that one of the following two conditions holds:

(i) l is an odd prime dividing $q - 1$,

(ii) $l = 2$ and $q \equiv 1 \pmod 4$.

Since $q > 3$, if there is no l for which (i) holds, then (ii) is necessarily satisfied.

Lemma 8. *Assuming the above notation and hypotheses, there always exists an element $\beta \in \mathbf{F}_q$ with the property that for every $i = 1, 2, \ldots, r$,*

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

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 7, we can bound from below the absolute value of the sum

$$\sum_{\beta \in \mathbf{F}_q} (1 - \chi_1(\alpha_1 + \beta))(1 - \chi_2(\alpha_2 + \beta)) \cdots (1 - \chi_r(\alpha_r + \beta)) \tag{5}$$

by

$$\begin{aligned} q - \sum_{\substack{\mathcal{I} \subset \{1,2,\ldots,r\} \\ \mathcal{I} \neq \emptyset}} \left(-1 + \sum_{i \in \mathcal{I}} \deg f_i\right) \sqrt{q} &= \\ q + (2^r - 1)\sqrt{q} - \sum_{i=1}^{r} \deg f_i \left(\sum_{\substack{\mathcal{I} \subset \{1,2,\ldots,r\} \\ i \in I}} 1 \right) \sqrt{q} &= \\ q + (2^r - 1)\sqrt{q} - 2^{r-1} \left(\sum_{i=1}^{r} \deg f_i \right) \sqrt{q}. \end{aligned} \tag{6}$$

On the other hand, if for every $\beta \in \mathbf{F}_q$, there is some i for which $\alpha_i + \beta$ is an lth power (in $\mathbf{F}_q(\alpha_i)$), then the sum (5) has absolute value at most $2^{r-1}r$. Indeed, if $\alpha_i + \beta$ is a nonzero lth power in $\mathbf{F}_q(\alpha_i)$, then the term of the sum corresponding to β vanishes. If $\alpha_i + \beta$ is zero, then β belongs to the r-element set $\{-\alpha_1, \ldots, -\alpha_r\}$, and each of the corresponding summands has absolute value at most 2^{r-1}. Comparing this bound with (6) we find

$$q + (2^r - 1)\sqrt{q} - 2^{r-1} \left(\sum_{i=1}^{r} \deg f_i \right) \sqrt{q} - 2^{r-1} r \leq 0,$$

which contradicts the condition (2). □

Proof of Theorem 2. With β as in Lemma 8, apply the substitution $T \mapsto T-\beta$ to the sequence of polynomials $f_1, \dots, f_r$. This yields a new sequence $g_1, \dots, g_r$ (say) of irreducible polynomials over $\mathbf{F}_q$ with corresponding roots $\alpha_1+\beta, \dots, \alpha_r+\beta$. By Lemma 3 all the polynomials

$$g_1(T^{l^k}) = f_1(T^{l^k}-\beta), \quad \dots, \quad g_r(T^{l^k}) = f_r(T^{l^k}-\beta) \quad \text{for } k = 1, 2, 3, \dots$$

are irreducible, which proves the theorem. □

5. Further Examples

Example 2. A well-known open question in analytic number theory, popularized as one of Landau's "four unattackable problems," asks whether there are infinitely many primes one more than a perfect square. Analogously, one can ask whether there are infinitely many prime polynomials over $\mathbf{F}_q$ of the form f^2+1. If q is even or if $q \equiv 1 \pmod 4$, then -1 is a square in $\mathbf{F}_q$ and so there can be no irreducibles of this form. In the remaining case, when $q \equiv 3 \pmod 4$, Cherly ([7], Theorem 1.3) proved that there are infinitely many monic f for which f^2+1 has at most six prime divisors. Using Theorem 2 we can now settle the polynomial question completely.

Assume that $q \equiv 3 \pmod 4$, so that T^2+1 is irreducible over $\mathbf{F}_q$. Taking $r=1$ and $f_1 = T^2+1$ in Theorem 2, we obtain infinitely many monic primes of the form f^2+1 provided that both $q > 3$ and the condition (2) is satisfied. Condition (2) is easily seen to hold already for all $q \geq 3$, and so we obtain an affirmative answer to our question for $q > 3$. The proof of Theorem 2 can be modified so as not to exclude the case of $\mathbf{F}_3$, but it is also easy to treat this case directly. Indeed, the irreducible polynomial $(T+1)^2+1$ has order $8 = 3^2-1$, and so Lemma 3 shows that $(T^{2^k}+1)^2+1$ is irreducible over $\mathbf{F}_3$ for every $k = 1, 2, 3, \dots$.

Example 3. We proved Theorem 2 by arguing that if q is sufficiently large, then there is some translate of our given family of polynomials to which we can apply Lemma 3 (with the same prime l simultaneously). But if we are given a specific family $\{f_i(T)\}$ of polynomials over a specific finite field, it may be the case that no translate of this type exists; situations of this kind arose in Case III of our proof of Theorem 1.

Here we say a few more words about what can be done when this transpires. Observe that to obtain the conclusion of Hypothesis H, it suffices that there be a single monic polynomial $s(T)$ for which the Serret-Dickson lemma can be applied (with the same prime l simultaneously) to the family $\{f_i(s(T))\}$. In our proof of Theorem 1, appropriate preliminary substitutions were found by hand. But there are also theoretical results which can be useful in this direction. In many cases, a suitable substitution can be squeezed out of the following criterion due to Agou ([1]; see also [8], pp. 409-410):

Lemma 9. *Let f be an irreducible polynomial of degree m over $\mathbf{F}_q$ with a root $\beta \in \mathbf{F}_{q^m}$. For a nonzero $\alpha \in \mathbf{F}_q$, the polynomial $f(T^p - \alpha T)$ is irreducible over $\mathbf{F}_q$ if and only if*

$$\alpha = A^{p-1} \text{ for some } A \in \mathbf{F}_{q^m} \quad \text{and} \quad \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_p}(\beta/A^p) = 0.$$

Here p denotes the characteristic of $\mathbf{F}_q$.

Polynomial	**Order**	**Order after substitution $T \mapsto T^5 + T$**
$T^2 + 2$	2^3	$2^3 \cdot 11 \cdot 71$
$(T+1)^2 + 2$	$2^3 \cdot 3$	$2^3 \cdot 3 \cdot 11 \cdot 71 \cdot 521$
$(T+2)^2 + 2$	$2 \cdot 3$	$2 \cdot 3 \cdot 11 \cdot 71 \cdot 521$
$(T+3)^2 + 2$	3	$3 \cdot 11 \cdot 71 \cdot 521$
$(T+4)^2 + 2$	$2^3 \cdot 3$	$2^3 \cdot 3 \cdot 11 \cdot 71 \cdot 521$

Table 2. Table corresponding to the example of §5. Note that $5^{10} - 1 = 2^3 \cdot 3 \cdot 11 \cdot 71 \cdot 521$.

For example, consider the family of polynomials $\{f_\alpha(T)\}_{\alpha \in \mathbf{F}_5}$ over $\mathbf{F}_5$ defined by $f_\alpha(T) := (T + \alpha)^2 + 2$. Since -2 is not a square modulo 5, the f_α are irreducible. Moreover, the admissibility of this family for Hypothesis H is obvious, since $\prod_{\alpha \in \mathbf{F}_5} f_\alpha(0) \neq 0$. From Table 2 we see that Lemma 3 is not applicable to the family $\{f_\alpha\}$ since, e.g., no prime l divides the order of both f_0 and f_3. Moreover, any translation substitution $T \mapsto T - \beta$ merely permutes the f_α, so will not facilitate the application of Lemma 3.

However, a suitable preliminary substitution can be found from Lemma 9:

Corollary 10. *Let $f(T)$ be an irreducible quadratic polynomial over $\mathbf{F}_p$, where p is prime. Then the substitution $T \mapsto T^p + T$ leaves f irreducible.*

Proof. We apply Lemma 9 to the polynomial $f(T)$, taking $q = p$ and $m = 2$. The substitution $T \mapsto T^p + T$ corresponds to the choice $\alpha = -1$. Observe that if we fix a generator g of $\mathbf{F}_p^\times$, we have $\alpha = -1 = A^{p-1}$ when $A := \sqrt{g} \in \mathbf{F}_{p^2}$. So to complete the proof it suffices to verify the nonvanishing condition on the trace. But

$$\mathrm{Tr}_{\mathbf{F}_p^2/\mathbf{F}_p}(\beta/A^p) = \beta/A^p + \beta^p/A^{p^2} = -\beta/A + \beta^p/A = A^{-1}(\beta^p - \beta),$$

which is nonzero since otherwise $\beta \in \mathbf{F}_p$ and f is not irreducible. □

Returning to our given family $\{f_\alpha(T)\}$, Corollary 10 guarantees that the substitution $T \mapsto T^5 + T$ is irreducibility-preserving. As seen in Table 2, for the resulting family of polynomials the hypotheses of Lemma 3 are satisfied with $l = 11$ (or $l = 71$). Thus the conclusion of Hypothesis H holds for the family $\{f_\alpha(T^5 + T)\}$ and so also for the family $\{f_\alpha(T)\}$.

6. Concluding Remarks

There are various ways one might seek to improve Theorem 2. Establishing the conjectured count for the number of irreducibility-preserving substitutions seems out of reach, even in the constant-coefficient situation we have been considering. Short of this, one could hope to establish certain weak consequences of such a result. For example, on the basis of the Hardy-Littlewood heuristics, one is led to conjecture that for a fixed family of (constant-coefficient) polynomials satisfying the necessary local conditions, there is an irreducibility-preserving substitution of degree n whenever n is sufficiently large. (Note that the degrees of the substitutions produced by the methods of this paper form a lacunary set.) This conjecture again appears rather difficult.

We draw solace from the history of the polynomial analogue of Dirichlet's theorem. Five years before Artin ([2], pp. 242-246) proved the asymptotic formula in this case (i.e., the polynomial prime number theorem for arithmetic progressions), Landau proved ([17], §2) that in every coprime arithmetic progression of polynomials, there are infinitely many monic prime polynomials whose degrees lie in a specified arithmetic progression of integers. In this spirit, we will prove in forthcoming work [19] the following version of Theorem 2 for prime fields:

Theorem. *Let $f_1, f_2, \dots, f_r$ be irreducible polynomials over $\mathbf{F}_p[T]$, and fix an arbitrary (integer) arithmetic progression $a \pmod{m}$. Assume that p is sufficiently large, depending on r, the degrees of the f_i, and the modulus m. Then there are infinitely many substitutions $T \mapsto g(T)$ which preserve the irreducibility of all the f_i, with $g(T)$ monic and with $\deg g(T) \equiv a \pmod{m}$.*

We apply the same methods to settle in the affirmative Hall's question as to whether there are infinitely many twin prime pairs $f, f+1$ of odd degree over every finite field $\mathbf{F}_q$ with $q > 2$. The proof of the above theorem rests on an asymptotic formula of independent interest applicable in the general situation of Theorem 2. However, in our asymptotic formula, it is the field $\mathbf{F}_q$ which varies instead of the degree of the substitution. For example, we will prove that for fixed n, the number of twin prime pairs $f, f+1$ of degree n over $\mathbf{F}_q$ is asymptotic to q^n/n^2 provided q tends to infinity subject to the restriction $(q, 2n) = 1$.

Given the utility of Hypothesis H in providing conditional solutions to interesting problems about rational integers, one might wonder if the polynomial Hypothesis H has a similarly wide range of applicability. In forthcoming work with Gallardo and Rahavandrainy [15], we use the results of the present paper to investigate perfect polynomials over finite fields, which are the positive characteristic analogue of perfect numbers. (See [3] for the relevant definitions.)

Lastly, we point out that Bender & Wittenberg [4] have recently proposed another polynomial analogue of Hypothesis H. They prove:

Theorem (Bender & Wittenberg). *Let $f_1, f_2, \dots, f_r \in \mathbf{F}_q[u, T]$ be irreducible polynomials whose total degrees $\deg(f_i)$ satisfy $p \nmid \deg(f_i)(\deg(f_i)-1)$ for all i. Assume that the curves $C_i \in \mathbf{P}^2_{\mathbf{F}_q}$ defined as the Zariski closures of the affine curves*

$$f_i(u, T) = 0$$

are smooth. Then, for any sufficiently large positive integer s, there exist $a, b \in \mathbf{F}_{q^s}$ such that the polynomials $f_1(u, au+b), \dots, f_r(u, au+b) \in \mathbf{F}_{q^s}[u]$ are all irreducible.

This result has a very different flavor than anything we have been discussing here. In particular, since their theorem produces only finitely many prime specializations and since these are produced not over $\mathbf{F}_q$ but over a finite extension, the result of Bender & Wittenberg does not appear to imply any example of what we have been referring to as the polynomial Hypothesis H.

7. Acknowledgements

I would like to thank Keith Conrad for commenting on an early draft of this manuscript and my advisor, Carl Pomerance, for his encouragement and advice at every stage of this work. I am also grateful to the organizers of the Anatomy of Integers conference in Montréal for giving me the opportunity to present on this topic there.

References

[1] *S. Agou*, Irréductibilité des polynômes $f(X^{p^r} - aX)$ sur un corps fini $\mathbf{F}_{p^s}$. J. Reine Angew. Math. **292** (1977), 191–195. MR MR0439825 (55 #12707)

[2] *E. Artin*, Quadratische Körper im Gebiete der höheren Kongruenzen. II. Math. Z. **19** (1924), 207–246.

[3] *J. T. B. Beard, Jr., J. R. O'Connell, Jr., and K. I. West*, Perfect polynomials over GF(q). Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **62** (1977), 283–291. MR MR497649 (81i:12022)

[4] *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. (2005), no. 36, 2237–2248. MR MR2181456

[5] *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. MR MR1625181 (99d:11092)

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

[7] *J. Cherly*, A lower bound theorem in $F_q[x]$. J. Reine Angew. Math. **303/304** (1978), 253–264. MR 80e:12022

[8] *S. D. Cohen*, The reducibility theorem for linearised polynomials over finite fields. Bull. Austral. Math. Soc. **40** (1989), no. 3, 407–412. MR MR1037635 (91b:11140)

[9] *B. Conrad, K. Conrad, and R. Gross*, Prime specialization in genus 0. Transactions of the AMS (to appear), 2006.

[10] ———, Prime specialization in higher genus II. In preparation, 2006.

[11] *K. Conrad*, Irreducible values of polynomials: a non-analogy. Number fields and function fields—two parallel worlds. Progr. Math., vol. 239, Birkhäuser Boston, Boston, MA, 2005, pp. 71–85. MR MR2176587

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

[13] ———, Linear groups: with an exposition of the Galois field theory, with an introduction by W. Magnus. Dover Publications Inc., New York, 1958. MR 21 #3488

[14] *G. Effinger, K. Hicks, and G. L. Mullen*, Integers and polynomials: comparing the close cousins $\mathbf{Z}$ and $\mathbf{F}_q[x]$. Math. Intelligencer **27** (2005), no. 2, 26–34. MR MR2156532

[15] *L. Gallardo, P. Pollack, and O. Rahavandrainy*, On a conjecture of Beard, O'Connell and West concerning perfect polynomials. In preparation, 2006.

[16] *C. J. Hall*, L-functions of twisted Legendre curves. Ph.D. thesis, Princeton University, 2003.

[17] *H. Kornblum*, Über die Primfunktionen in einer arithmetischen Progression. Math. Z. **5** (1919), 100–111. Posthumously edited by E. Landau.

[18] *S. Lang*, Algebra, third ed. Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR MR1878556 (2003e:00003)

[19] *P. Pollack*, Counting irreducibility-preserving substitutions for polynomials over finite fields. In preparation, 2006.

[20] *M. Rosen*, Number theory in function fields. Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR MR1876657 (2003d:11171)

[21] *A. Schinzel and W. Sierpiński*, Sur certaines hypothèses concernant les nombres premiers. Acta Arith. 4 (1958), 185–208; erratum **5** (1958), 259 (French). MR 21 #4936

[22] *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** (1866), 617–688.

[23] *W. Sierpiński*, Elementary theory of numbers, second ed. North-Holland Mathematical Library, vol. 31, North-Holland Publishing Co., Amsterdam, 1988. Edited and with a preface by Andrzej Schinzel. MR 89f:11003

[24] *D. Wan*, Generators and irreducible polynomials over finite fields. Math. Comp. **66** (1997), no. 219, 1195–1212. MR MR1401947 (97j:11060)

Department of Mathematics, Dartmouth College, Hanover, NH 03755
E-mail address: paul.pollack@dartmouth.edu