ACTA ARITHMETICA
136.1 (2009)

Arithmetic properties of polynomial specializations over finite fields

by

Paul Pollack (Urbana, IL)

1. Introduction. Multiplicative properties of values taken on by integer polynomials have been the subject of intense scrutiny. This is not only because of this subject's intrinsic interest (highlighted in famous problems like the twin prime conjecture), but also because results in this direction have more than demonstrated their usefulness as auxiliary tools in diverse number-theoretic investigations.

The purpose of this paper is to point out how the techniques of [27] can be applied to attack problems of this type in the setting of polynomials over finite fields. We concentrate on four concrete examples; in each case we begin by discussing a problem or result in rational number theory and follow up with a nontrivial result towards the corresponding polynomial analogue.

1.1. *Twin primes and Brun's constant.* We begin by recalling Brun's classical result [3] towards the twin prime problem:

Theorem A (Brun). *The sum of the reciprocals of those primes which are members of a twin prime pair converges* (*or is a finite sum*); *that is*,

$$B := \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots<\infty.$$

While constants like π and e are known to billions of digits, our knowledge of Brun's constant B is surprisingly modest. The sharpest known unconditional bounds are (roughly)

$$1.830 < B < 2.347.$$

2000 *Mathematics Subject Classification*: Primary 11T55; Secondary 11N32.
Key words and phrases: twin primes, Brun's constant, prime gaps, smooth values of polynomials, twin prime polynomials.

This work was done while the author was supported by an NSF Graduate Research Fellowship.

DOI: 10.4064/aa136-1-5

(Thus we do not know B to even one decimal place!) The lower bound here is due to Sebah [29], who computed all the twin prime pairs up to 10^{16} and summed their reciprocals. The upper bound is due to Crandall and Pomerance ([5, pp. 16–17], see also [19, Chapter 3]), who bound the sum of the twin prime pairs past 10^{16} using an explicit upper estimate of Riesel and Vaughan [28] for the number of twin prime pairs. Much sharper estimates for Brun's constant are available if one assumes a suitable quantitative version of the twin prime conjecture; e.g., it is plausible that

$$B = 1.902160583121 \pm 4.08 \times 10^{-8}.$$

This last estimate is taken from the recent thesis of Klyve [19], which the reader should consult for references to earlier work.

Questions analogous to the twin prime conjecture have been considered in the ring of polynomials over a finite field. Whereas a solution to the rational twin prime problem remains a holy grail of modern research, in [14] Hall proves by quite elementary means that there exist infinitely many prime pairs $P, P+1 \in \mathbb{F}_q[T]$ whenever $q > 3$. In [25] Hall's result is extended to the infinitude of prime pairs $P, P+\alpha$, for any $\alpha \in \mathbb{F}_q^\times$ and any $q \neq 2$. Unfortunately the families of twin prime pairs produced in these papers are quite sparse, and the consequent lower bounds on the number of such pairs are quite far from the conjectured asymptotics.

If $\mathbb{F}_q$ is a finite field containing the nonzero element α, we define the *Brun constant associated to q and α* by

$$B_{q,\alpha} := \sum_{P, P+\alpha \text{ monic primes}} \frac{1}{|P|}.$$

(Here and below we write $|M|$ for the size of $\mathbb{F}_q[T]/(M)$, i.e., $|M| = q^{\deg M}$.) The proof of Theorem A can be adapted to show that $B_{q,\alpha}$ is finite for any q and α (cf. [32, Corollary, p. 349] or [18, Theorem 5.5]). Actually we can be far more precise about the values of $B_{q,\alpha}$:

THEOREM 1. *If $\mathbb{F}_q$ is a finite field with characteristic $p > 2$, then*

$$B_{q,\alpha} = \frac{\pi^2}{6} + O\left(\frac{1}{p} + \frac{\log\log q}{\log q}\right), \tag{1}$$

uniformly for $\alpha \in \mathbb{F}_q^\times$. Moreover, for every finite field $\mathbb{F}_q$,

$$\frac{1}{q-1} \sum_{\alpha \in \mathbb{F}_q^\times} B_{q,\alpha} = \frac{\pi^2}{6} + O(q^{-1/2}). \tag{2}$$

Thus $B_{q,\alpha}$ tends to $\pi^2/6$ as the characteristic of $\mathbb{F}_q$ tends to infinity, for example if q tends to infinity through prime values. Moreover, the error term in this approximation is rather small on average over α once q is

large (regardless of the characteristic). We suspect that $B_{q,\alpha}$ tends to $\pi^2/6$, uniformly in α, whenever q tends to infinity, but we have not so far succeeded in showing this.

1.2. *The distribution of prime gaps.* The following conjecture is a well-known consequence of Cramér's probabilistic model (see, e.g., [13] for background):

CONJECTURE A. *Fix $\lambda > 0$. Suppose h and N tend to infinity in such a way that $h \sim \lambda \log N$. Then*

$$\lim_{N\to\infty} \frac{1}{N} \#\{n \le N : \pi(n+h) - \pi(n) = k\} = e^{-\lambda} \frac{\lambda^k}{k!}$$

for every fixed integer $k = 0, 1, 2, \ldots$.

Additional support for Conjecture A comes from the work of Gallagher [10], who shows that it follows from a plausible uniform version of Hardy and Littlewood's prime k-tuples conjecture.

Granville (personal communication) suggests the following polynomial analogue of Conjecture A. For a prime p and an integer a, let $\overline{a}$ denote the residue class of a in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. For each prime p and each integer $h \ge 0$, define

$$I(p;h) := \Big\{ \overline{a}_0 + \overline{a}_1 T + \cdots + \overline{a}_j T^j : 0 \le a_0, \ldots, a_j < p \text{ with } \sum a_i p^i < h \Big\}. \tag{3}$$

Let $P_k(p;h,n)$ be the number of polynomials $A(T)$ of degree n over $\mathbb{F}_p$ for which the translated "interval" $A + I(p;h)$ contains exactly k primes.

CONJECTURE 1. *Fix $\lambda > 0$. Suppose h and n tend to infinity in such a way that $h \sim \lambda n$. Then*

$$\frac{1}{p^n} P_k(p;h,n) \to e^{-\lambda} \frac{\lambda^k}{k!} \quad (\text{as } n \to \infty) \tag{4}$$

for each fixed $k = 0, 1, 2, \ldots$, uniformly in the prime p.

In §3.1, we show that, in analogy with Gallagher's result, this conjecture follows from a suitable uniform version of the prime k-tuples conjecture. Our main result towards Conjecture 1 is the following; it shows that (4) holds whenever p tends to infinity faster than any power of n^{n^2}, as long as $k = o(\sqrt{n})$:

THEOREM 2. *For each compact set $I \subset (0,\infty)$, there is a constant C with the following property: For integers n, h and k with $n \ge 2$, $h \ge 1$, $0 \le k \le h$, and $h/n \in I$, upon setting $\lambda := h/n$ we have*

$$\frac{1}{p^n} P_k(p;h,n) = e^{-\lambda} \frac{\lambda^k}{k!} \left(1 + O_I\left(\frac{(k+1)^2}{n}\right)\right) + O(p^{-1/2} \exp(Cn^2 \log n)),$$

where the second O-constant is absolute.

1.3. *Smooth values of polynomials.* Both of the preceding problems concerned the distribution of primes. On the opposite end of the multiplicative spectrum one has the smooth numbers, those composed only of small prime factors. (More precisely, an integer n is called *y-smooth* if its largest prime factor $P(n)$ is $\le y$.) Dickmann [6] has shown that for fixed u, the number of $n \le x$ which are $x^{1/u}$-smooth is asymptotic to $\varrho(u)x$, where ϱ is the (unique) continuous solution of the differential-delay equation

$$u\varrho'(u) = -\varrho(u-1) \quad \text{with the initial condition } \varrho(u) = 1 \text{ for } 0 \le u \le 1.$$

One could ask, more generally, for an asymptotic formula for the number of $x^{1/u}$-smooth values assumed by a polynomial $F(T)$ on integers $1 \le n \le x$. Denote this number by $\Psi(F; x, x^{1/u})$. Then we have the following conjecture of Martin [21], which we state in a slightly strengthened form:

Conjecture B (Martin). *Let F be an arbitrary but fixed nonzero integer-valued polynomial and let $d_1, \dots, d_K$ be the degrees of the nonassociate irreducible factors of F. Then for each $U > 0$, the asymptotic formula*

$$\Psi(F; x, x^{1/u}) \sim x\varrho(d_1 u) \cdots \varrho(d_K u)$$

holds as $x \to \infty$, uniformly for $0 < u \le U$.

This can be viewed as a smooth number analogue of Schinzel's Hypothesis H. Martin links the two conjectures by showing that a sufficiently uniform quantitative version of Hypothesis H implies the truth of Conjecture B for every $U < (d - 1/K)^{-1}$, where d is the maximal degree of an irreducible factor of F and K is the number of nonassociate irreducible factors of F of degree d. (Note that Conjecture B is trivial in the narrower range $U < d^{-1}$.)

The distribution of smooth polynomials mimics the distribution of smooth integers: for instance, the number of polynomials of degree n over $\mathbb{F}_q$ all of whose prime factors have degree $\le n/u$ is asymptotically $\varrho(u)q^n$ (in large ranges of u and uniformly in q; see, e.g., [4], [24]). This motivates the following analogue of Conjecture B: For a polynomial $F(T)$ over $\mathbb{F}_q$, define $\Psi(F; n, m)$ as the number of monic, degree n polynomials $g(T)$ over $\mathbb{F}_q$ for which every prime factor of $F(g(T))$ has degree bounded by m.

Conjecture 2. *Fix $B, U \ge 1$. Let $F(T)$ be a nonconstant polynomial over $\mathbb{F}_q$ of degree at most B. Let K be the number of distinct monic irreducible factors of F, and let $d_1, \dots, d_K$ be the degrees of those factors. Then as $n \to \infty$,*

$$\Psi(F; n, n/u) \sim q^n \varrho(d_1 u) \cdots \varrho(d_K u)$$

uniformly for $0 < u \le U$ and uniformly for all q, F, and K.

Once again, the methods of [27] allow us to confirm this conjecture when q grows much faster than n (say when q grows faster than any power of n^n) and satisfies $\gcd(q, 2n) = 1$:

THEOREM 3. *Fix $B, U \geq 1$. Let $F(T)$ be a nonconstant polynomial over $\mathbb{F}_q$ of degree at most B. Let K be the number of distinct monic irreducible factors of F, and let $d_1, \dots, d_K$ be the degrees of these factors. If $n \geq BU$ and $(q, 2n) = 1$, then*

$$\Psi(F; n, n/u) = q^n \varrho(d_1 u) \cdots \varrho(d_K u) + O_B(uq^n/n) + O_B(q^{n-1/2} n!^{2B})$$

for $0 < u \leq U$.

Without giving details, we remark that minor modifications of our arguments give analogous results for the number of smooth values of $F(h(T))$ when $h(T)$ is restricted to monic prime values (cf. Martin's prediction [21, equation (1.8)]).

1.4. *Smooth values of consecutive integers.* The final conjecture we consider can be viewed as a smooth number analogue of the prime k-tuples conjecture:

CONJECTURE C. *Let $0 \leq \alpha < \beta \leq 1$, and let A be the set of integers $n \geq 2$ whose largest prime factor $P(n)$ satisfies $n^\alpha \leq P(n) \leq n^\beta$. Then for every k, one can find k consecutive integers $n+1, \dots, n+k$ all of which belong to A.*

The origin of this problem lies with Erdős (see, e.g., [7]), who asked for a proof in the case when $k = 2$ and $[\alpha, \beta] = [1 - \varepsilon, 1]$. The case $k = 2$ was settled in its entirety by Hildebrand [15] (via the solution of a more general conjecture of Balog). Moreover, when $\alpha = 0$, Conjecture C follows (for any $\beta > 0$ and every k) from the results of Balog and Wooley [2]. (All of these theorems can in fact be proved in stronger, quantitative forms.) Nevertheless, Conjecture C remains open in general. A partial result when $k > 2$ is contained in [16]. See also the survey [17].

A similar problem appears in the work of Erdős and Pomerance [8]; they ask whether the largest prime factors of n and $n+1$ are independent events, in the sense that the proportion of $n \leq x$ with $P(n) > x^{\alpha_1}$ and $P(n+1) > x^{\alpha_2}$ tends to $a(\alpha_1)a(\alpha_2)$, where $a(t) := 1 - \varrho(1/t)$. This is still unsolved. Even the weaker assertion that asymptotically half of all positive integers n have $P(n) > P(n+1)$ remains open. This last problem goes all the way back to correspondence in the 1930s between Erdős and Turán (see [30, pp. 100–101]).

The results of Balog and Wooley mentioned above have been translated into the polynomial setting by Masuda and Panario [22]. However, it seems that there are no results for polynomials in the direction of Conjecture C when $\alpha > 0$. Our next theorem deals with this case, and at the same time proves an independence statement for the largest prime factors of neighboring polynomials.

Write $L(A)$ for the degree of the largest irreducible factor of a polynomial A. Suppose that $I = [\alpha, \beta]$ is a compact subinterval of $[0,1]$. (Here and in what follows, intervals are always understood to be of nonzero length, so that $\alpha < \beta$.) If $\alpha \neq 0$, we define $\kappa(I) = 1/\alpha$, otherwise we set $\kappa(I) = 1/\beta$.

THEOREM 4. *Let k be a positive integer, and let S be a k-element subset of $\mathbb{F}_q$. Suppose that for each $s \in S$ we are given a compact subinterval $I_s = [\alpha_s, \beta_s] \subset [0,1]$ and let $C := \max_{s \in S} \kappa(I_s)$.*

(a) *The number of monic, degree n polynomials $A(T) \in \mathbb{F}_q[T]$ with*

$$\alpha_s \deg A(T) \le L(A(T)+s) \le \beta_s \deg A(T) \quad \text{for every } s \in S \tag{5}$$

is given by

$$q^n \prod_{s \in S} (\varrho(\beta_s^{-1}) - \varrho(\alpha_s^{-1})) + O_{k,C}(q^n/n) + O(n!^{2k} q^{n-1/2}),$$

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

(b) *Suppose that the length of each interval I_s is bounded below by $\varepsilon > 0$. If q is odd and sufficiently large (depending only on k and ε), then there are infinitely many monic polynomials $A(T) \in \mathbb{F}_q[T]$ for which* (5) *holds.*

We emphasize that the estimate in (a) is only nontrivial when q is large compared to n, since otherwise our bound on the error term exceeds the total number of monic, degree n polynomials. The proof of (a) depends on an extension of the main result of [27]; this extension implies (in particular) the stronger result that in a similar range of q, the *factorization types* (defined below) of neighboring polynomials are close to independent.

To illustrate Theorem 4, fix $\alpha_1, \alpha_2 \ge 0$. Then applying Theorem 4 with $I_0 = [\alpha_1, 1]$, $I_1 = [\alpha_2, 1]$, and $S = \{0,1\} \subset \mathbb{F}_q$, we see that the proportion of degree n polynomials $A(T)$ over $\mathbb{F}_q$ with $L(A(T)) \ge \alpha_1 n$ and $L(A(T)+1) \ge \alpha_2 n$ is asymptotic to $a(\alpha_1)a(\alpha_2)$, provided n and q tend to infinity with $q \ge n^{4n}$ (say) and $\gcd(q, 2n) = 1$. This confirms, in a certain range, the polynomial analogue of the independence result conjectured by Erdős and Pomerance.

1.5. *The key estimate.* We now turn to a description of the main technical tool required to obtain these results. First some notational preliminaries: We use λ to denote a partition of the positive integer n, i.e., λ is a sequence of positive integers $(t_1, t_2, \dots)$ with $t_1 \ge t_2 \ge \cdots$ and $\sum t_i = n$. Alternatively, we may write $\lambda = \langle 1^{\alpha_1}, 2^{\alpha_2}, \dots \rangle$, where α_j is the number of times j occurs in the sequence of summands t_i. If d is a positive integer and $\lambda = (t_1, t_2, \dots)$ is a partition of n, we write $d \times \lambda$ for the partition of dn given by $(dt_1, dt_2, \dots)$.

If $f(T)$ is a degree n polynomial over a field, the partition corresponding to the list of degrees of its irreducible factors is referred to as the *cycle type*

or *factorization type* of $f(T)$. Similarly, the *cycle type* of a permutation on n letters refers to the partition $\langle 1^{\alpha_1}, \dots, n^{\alpha_n}\rangle$, where α_j is the number of j-cycles in its decomposition into disjoint cycles. We use the notation $T(\lambda)$ for the proportion of permutations on n letters with cycle type λ. Thus, if $\lambda = \langle 1^{\alpha_1}, 2^{\alpha_2}, \dots\rangle$ is a partition of n, then (as proved by Cauchy)

$$T(\lambda) = \frac{1}{1^{\alpha_1}\cdots n^{\alpha_n}\alpha_1!\cdots\alpha_n!}.$$

We can now state our main theorem, which extends the main result of [27]:

THEOREM 5. *Let n be a positive integer and let $\lambda_1, \dots, \lambda_r$ be partitions of the integer n. Let $f_1(T), \dots, f_r(T)$ be nonassociate irreducible polynomials over $\mathbb{F}_q$ of respective degrees $d_1, \dots, d_r$, with $\sum_{i=1}^r d_i \le B$. The number of univariate monic polynomials h of degree n for which $f_i(h(T))$ has factorization type $d_i \times \lambda_i$ for every $1 \le i \le r$ is*

$$q^n \prod_{i=1}^{r} T(\lambda_i) + O((nB)n!^B q^{n-1/2}),$$

provided $\gcd(q, 2n) = 1$. *Here the implied constant is absolute.*

REMARK. As will be clear from the proof, the same estimate holds if we also insist that all the polynomials $f_i(h(T))$ are squarefree.

The case when each λ_i equals (n) (where $T(\lambda_i) = 1/n$) corresponds to the simultaneous primality of all the $f_i(h(T))$, which was the case treated in [27]. The proof of Theorem 5 follows [27] closely and is given in §6.

The reader may be puzzled as to why Theorem 5 is stated in terms of partitions of the form $d_i \times \lambda_i$ and not in terms of arbitrary partitions of $d_i n$. Actually the mystery surrounding this restriction is easily dispelled. Suppose that $f(T)$ is irreducible of degree d. Then if $h(T)$ is any polynomial over $\mathbb{F}_q$, every irreducible factor of $f(h(T))$ has degree divisible by d (and thus its cycle type must have the form $d \times \lambda$). Indeed, if $\pi(T)$ divides $f(h(T))$, then f has a root in the field $\mathbb{F}_q[T]/(\pi)$. Thus the extension of $\mathbb{F}_q$ of degree $\deg \pi$ must contain a copy of the extension of $\mathbb{F}_q$ of degree d, which gives the claim.

Several authors have commented on the structural similarities between permutations and polynomials over finite fields; see, e.g., [1], where both objects are considered in the general context of "logarithmic combinatorial structures". Theorem 5 provides a bridge between the statistics of random permutations and those of random polynomial specializations, enabling theorems for permutations to be easily transported to the setting of polynomial specializations. It seems reasonable to expect that this theorem should admit many additional number-theoretic applications. For inspiration in this regard we refer the reader to Granville's survey [12], which in the course

of comparing the anatomy of integers and permutations, chronicles many permutation statistics that are of arithmetic significance.

Notation. In addition to the notation already introduced, we use the symbols μ, ω, and φ for the polynomial analogues of the corresponding arithmetic functions. Thus $\omega(A)$ is the number of distinct monic prime divisors of A, while $\mu(A) := (-1)^{\omega(A)}$ if A is squarefree and zero otherwise, and $\varphi(A)$ is the number of units in the ring $\mathbb{F}_q[T]/(A)$. We reserve the letter P for monic irreducibles.

2. Brun's constant: Proof of Theorem 1. For $\alpha \in \mathbb{F}_q^\times$, let $\pi_2(q; n, \alpha)$ denote the number of monic primes P of degree n over $\mathbb{F}_q$ for which $P + \alpha$ is also prime.

LEMMA 1. *Let n be a positive integer. If $\alpha \in \mathbb{F}_q^\times$ and $(q, 2n) = 1$, then*

$$\pi_2(q; n, \alpha) = \frac{q^n}{n^2} + O(q^{n-1/2} n n!^2). \tag{6}$$

Moreover,

$$\sum_{\alpha \in \mathbb{F}_q^\times} \pi_2(q; n, \alpha) = \frac{q^{n+1}}{n^2}\,(1 + O(n^2/q)). \tag{7}$$

Proof. Estimate (6) follows immediately from Theorem 5 upon choosing $f_1(T) = T$, $f_2(T) = T + \alpha$ and $\lambda_1 = \lambda_2 = (n)$. To prove (7), note that the left-hand side of (7) can be viewed as counting the number of not necessarily monic prime pairs $f, f+1$ of degree n over $\mathbb{F}_q$. (In fact, the term corresponding to α here counts the number of such pairs with leading coefficient α^{-1}.) In this guise, estimate (7) is contained in [26, Theorem 1]. ∎

Proof of Theorem 1. We have

$$B_{q,\alpha} = \sum_{n=1}^{\infty} \frac{1}{q^n}\, \pi_2(q; n, \alpha). \tag{8}$$

We split the sum (8) at a number A with $0 < A < p/2$. Then $(q, 2n) = 1$ for every $n \le A$, so that (6) yields

$$B_{q,\alpha} = \sum_{n \le A} \frac{1}{n^2} + O\Big(q^{-1/2} \sum_{n \le A} n n!^2\Big) + O\Big(\sum_{n > A} q^{-n} \pi_2(q; n, \alpha)\Big).$$

The former O-term is $\ll q^{-1/2} A^{2A}$. To estimate the latter O-term, we use the bound (valid uniformly over all q, n, and α)

$$\pi_2(q; n, \alpha) \ll \frac{q^n}{n^2}, \tag{9}$$

which follows in a standard way by an application of Selberg's upper bound method (as developed for polynomials in, e.g., [32]). This shows that the

second O-term is $\ll \sum_{n>A} n^{-2} \ll 1/A$. Hence

$$B_{q,\alpha} = \frac{\pi^2}{6} + O(1/A + q^{-1/2}A^{2A}),$$

say. Now take $A = \min\left\{\frac{1}{3}p, \frac{1}{6}\log q/\log\log q\right\}$ to obtain (1).

Turning to (2), we observe that for any $A > 0$,

$$\frac{1}{q-1}\sum_{\alpha\in\mathbb{F}_q^\times} B_{q,\alpha} = \frac{1}{q-1}\sum_{n\le A}\frac{1}{q^n}\sum_{\alpha\in\mathbb{F}_q^\times}\pi_2(q;n,\alpha) + O\biggl(\frac{1}{q-1}\sum_{n>A}\sum_{\alpha\in\mathbb{F}_q^\times}\frac{1}{n^2}\biggr).$$

(Note that we have once again applied (9).) The error term here is $O(1/A)$. Using (7) to estimate the inner sum, we obtain a main term of

$$\frac{q}{q-1}\sum_{n\le A}\frac{1}{n^2}\biggl(1+O\biggl(\frac{n^2}{q}\biggr)\biggr) = \frac{q}{q-1}\sum_{n\le A}\frac{1}{n^2} + O\biggl(\frac{A}{q}\biggr) = \frac{\pi^2}{6} + O\biggl(\frac{1}{A}+\frac{A}{q}\biggr).$$

Taking $A = q^{1/2}$ yields (2). ∎

3. The distribution of prime gaps

3.1. *Gallagher's theorem for polynomials over finite prime fields.* For $\mathbf{D} = (D_1,\dots,D_r)$ an r-tuple of distinct polynomials over $\mathbb{F}_q$, define

$$\mathfrak{S}_{\mathbf{D}} = \prod_P \frac{|P|^{r-1}(|P| - \omega_{\mathbf{D}}(P))}{(|P|-1)^r},$$

where $\omega_{\mathbf{D}}(P)$ is the number of residue classes mod P occupied by $D_1,\dots,D_r$. Let $\pi_{\mathbf{D}}(n;q)$ be the number of monic polynomials A of degree n for which all of $A+D_1,\dots,A+D_r$ are irreducible. Then the usual heuristics offered in favor of the Hardy–Littlewood conjectures suggest that

$$\pi_{\mathbf{D}}(n;q) = (\mathfrak{S}_{\mathbf{D}} + o(1))\,\frac{q^n}{n^r} \quad (n\to\infty). \tag{10}$$

In fact these heuristics suggest that this relation should hold not merely when $\mathbf{D}$ is fixed and $n\to\infty$, but also whenever $q^n\to\infty$, uniformly in $\mathbf{D}$, provided only that every D_i has degree less than n. This suggests the plausibility of the hypothesis in the following theorem, which is an analogue of Gallagher's principal result in [10]:

THEOREM 6. *Fix $\lambda > 0$, and suppose that h and n tend to infinity with $h \sim \lambda n$. Then* (4) *holds uniformly in p, under the following hypothesis*:

(A) *For each fixed r,* (10) *holds as n tends to infinity, uniformly in p, and uniformly for $D_1,\dots,D_r \in I(p;h)$ with the D_i distinct and $\mathfrak{S}_{(D_1,\dots,D_r)} \neq 0$.*

As in Gallagher's paper, the theorem follows from a suitable estimate for the average value of $\mathfrak{S}_{\mathbf{D}}$.

LEMMA 2. *Fix $r \geq 1$. Under hypothesis* (A) *of Theorem* 6, *we have*

$$\sum_{\text{distinct } D_1,\dots,D_r \in I(p;h)} \mathfrak{S}_{\mathbf{D}} \sim h^r \quad (h \to \infty),$$

uniformly in p.

Suppose now that this lemma is proved. Fix $k \geq 0$, and let $M_k(\lambda)$ be the kth moment of the Poisson distribution with parameter λ. Then as $n \to \infty$, the argument of [10, pp. 5–6] shows that

$$\frac{1}{p^n} \sum_{\substack{A(T) \in \mathbb{F}_p[T] \\ A(T) \text{ monic, of degree } n}} |\{P \in A + I(p;h) : P \text{ prime}\}|^k \to M_k(\lambda),$$

where the convergence is uniform in p. Theorem 6 then follows by an application of the method of moments.

Thus to prove Theorem 6 it only remains to prove Lemma 2.

LEMMA 3. *Let M be a nonzero polynomial over $\mathbb{F}_p$. If $|M| \leq h$, then the number of elements of $I(p;h)$ which lie in a given residue class modulo M is $h/|M| + O(1)$, where the implied constant here is absolute.*

Proof. Write h in base p, so that $h = h_0 + h_1 p + \cdots + h_k p^k$ with $0 \leq h_i < p$ for each i and $h_k \geq 1$. Represent the given residue class as A mod M, where $\deg A < \deg M$. Then $|M| \leq h$ implies that $j := \deg M \leq k$. Assume (with no loss in generality) that M is monic, and write

$$M = T^j + m_{j-1}T^{j-1} + \cdots + m_1 T + m_0.$$

We wish to count the number of $B \in \mathbb{F}_p[T]$ for which $A + MB$ belongs to $I(p;h)$. Any such B can be written in the form

$$B = b_{k-j}T^{k-j} + b_{k-j-1}T^{k-j-1} + \cdots + b_0,$$

and then (if we write $A = \sum a_i T^i$),

$$A + MB = b_{k-j}T^k + (b_{k-j}m_{j-1} + b_{k-j-1} + a_{k-1})T^{k-1} + \cdots + a_0 + b_0 m_0.$$

Looking at the leading coefficient of $A + MB$, we see that $A + MB$ belongs to $I(p;h)$ whenever b_{k-j} is any of $\overline{0}, \overline{1}, \dots, \overline{h_k - 1}$ (regardless of the values of the other b_i). There are $h_k p^{k-j}$ such choices of B. All other choices of B with $A + MB \in I(p;h)$ have $b_{k-j} = \overline{h}_k$. For these B, the condition $A + MB \in I(p;h)$ restricts the next-to-leading coefficient of B: if

$$b_{k-j}m_{j-1} + b_{k-j-1} + a_{k-1} = \overline{0}, \overline{1}, \overline{2}, \dots, \text{ or } \overline{h_{k-1} - 1}, \tag{11}$$

then automatically $A + MB$ belongs to $I(p;h)$. This gives rise to an additional $h_{k-1}p^{k-j-1}$ permissible values of B. Any B not counted so far for which $A + MB$ belongs to $I(p;h)$ has both $b_{k-j} = \overline{h}_k$ and the left-hand side of (11) equal to $\overline{h}_{k-1}$. Continuing this process, we find

$$N := h_k p^{k-j} + h_{k-1}p^{k-j-1} + \cdots + h_j = \lfloor h/|M| \rfloor$$

values of B which guarantee that $A+MB$ belongs to $I(p;h)$. Moreover, there is at most one other value of B for which $A+MB$ belongs to $I(p;h)$, namely that B for which

$$|A+MB-(\overline{h}_kT^k+\overline{h}_{k-1}T^{k-1}+\cdots+\overline{h}_jT^j)|<p^j.$$

If $A+MB$ lies outside $I(p;h)$ for this final value of B, then the quantity to be enumerated is N, otherwise it is $N+1$. In either case the stated estimate holds. ∎

Proof of Lemma 2 (sketch). Define $\Delta:=\prod_{1\le i<j\le r}(D_i-D_j)$. Write the Pth factor of $\mathfrak{S}_{\mathbf{D}}$ in the form

$$1+\frac{|P|^r-\omega_{\mathbf{D}}(P)|P|^{r-1}-(|P|-1)^r}{(|P|-1)^r}=1+a(P,\omega_{\mathbf{D}}(P)).$$

For monic, squarefree Q define $a_{\mathbf{D}}(Q):=\prod_{P|Q}a(P,\omega_{\mathbf{D}}(P))$. Then (in analogy with [10, eq. (7)]) we find that

$$a_{\mathbf{D}}(P)\ll\begin{cases}(|P|-1)^{-2} & \text{when } \omega_{\mathbf{D}}(P)=r,\\ (|P|-1)^{-1} & \text{when } \omega_{\mathbf{D}}(P)<r,\end{cases}$$

these two cases occurring respectively when P does not or does divide Δ. Here the implied constant, say C, depends only on r. It follows from these estimates that we have an absolutely convergent series expansion

$$\mathfrak{S}_{\mathbf{D}}=\sum_{Q}a_{\mathbf{D}}(Q).$$

For the tail of this expansion, we have

$$\begin{aligned}\sum_{|Q|>x}|a_{\mathbf{D}}(Q)|&\le\sum_{|Q|>x}\frac{\mu^2(Q)C^{\omega(Q)}}{\varphi(Q)^2}\,\varphi((Q,\Delta))\\&=\sum_{A|\Delta}\frac{\mu^2(A)C^{\omega(A)}}{\varphi(A)}\sum_{\substack{|B|>x/|A|\\(B,\Delta)=1}}\frac{\mu^2(B)C^{\omega(B)}}{\varphi(B)^2},\end{aligned}\tag{12}$$

where in the last line we have written $Q=AB$ with $A\,|\,\Delta$ and $(B,\Delta)=1$. In [10], the analogous double sum is

$$\ll_{r,\varepsilon}x^{-1}(xh)^{\varepsilon};\tag{13}$$

we proceed to establish that this estimate is also valid for (12).

Observe that

$$\begin{aligned}\sum_{|B|\le x}\frac{\mu^2(B)C^{\omega(B)}}{\varphi(B)^2}\,|B|&\le\prod_{|P|\le x}\left(1+\frac{C|P|}{(|P|-1)^2}\right)\le\prod_{|P|\le x}\left(1+\frac{4C}{|P|}\right)\\&\le\exp\left(4C\sum_{|P|\le x}\frac{1}{|P|}\right).\end{aligned}$$

The number of prime polynomials P of degree n over $\mathbb{F}_p$ is bounded above by p^n/n, and this implies that

$$\exp\bigg(4C\sum_{|P|\le x}\frac{1}{|P|}\bigg) \le \exp\bigg(4C\sum_{1\le n\le \log x/\log p}\frac{1}{n}\bigg) \ll (\log x)^{4C}.$$

Partial summation now shows that the inner sum in (12) is $\ll |A|x^{-1}\log^{4C} x$, so that (12) is

$$\begin{aligned}(14)\qquad &\ll (x^{-1}\log^{4C} x)\sum_{A|\Delta}\mu^2(A)C^{\omega(A)}\frac{|A|}{\varphi(A)} \le (x^{-1}\log^{4C} x)\prod_{P|\Delta}(1+2C)\\ &\le (x^{-1}\log^{4C} x)|\Delta|^{\varepsilon}\prod_{\substack{P\in\mathbb{F}_p[T]\\ |P|<(1+2C)^{1/\varepsilon}}}(1+2C)|P|^{-\varepsilon} \ll_\varepsilon (x^{-1}\log^{4C} x)h^{\varepsilon\binom{r}{2}}\end{aligned}$$

for any $\varepsilon>0$. (Note that the last product over P is finite for each fixed p and empty for $p>(1+2C)^{1/\varepsilon}$, and so it is $\ll_\varepsilon 1$.) To obtain (13), we replace ε in (14) with εr^{-2} (say). From this point the proof proceeds exactly as in [10], save that the "lattice point argument" of [10, p. 7] now requires an appeal to Lemma 3. ∎

Remark. The restriction to prime fields $\mathbb{F}_p$ was introduced to ensure a canonical embedding from $[0,p-1]$ into $\mathbb{F}_p$. This restriction is in some sense merely cosmetic. More precisely, suppose that for each q we have fixed a bijection $a\mapsto\overline{a}$ between $[0,q-1]$ and $\mathbb{F}_q$. Define $I(q;h)$ as in (3) with p replaced by q. Then the proofs of this section show that Theorem 6 remains valid with p replaced by q throughout.

3.2. *Proof of Theorem 2.* We may assume that $p>\max\{h,n\}$, for otherwise the theorem is trivial. Thus Theorem 5 can be employed to count the occurrences of prime r-tuples $A+D_1,\dots,A+D_r$ with $D_i\in I(p;h)$.

Fix one of the $\binom{h}{k}$ subsets $S\subset I(p;h)$ with k elements. We first count the number of monic, degree n polynomials A for which $A+s$ is prime for all $s\in S$ and reducible for all $s\in I(p;h)\setminus S$. By the principle of inclusion-exclusion, this is given by

$$\sum_{\substack{T\supseteq S\\ T\subseteq I(p;h)}}(-1)^{|T|-|S|}\#\{A : \text{every element of } A+T \text{ is irreducible}\}.$$

According to Theorem 5,

$$\#\{A : \text{every element of } A+T \text{ is irreducible}\} = \frac{p^n}{n^{|T|}} + O((hn)n!^h p^{n-1/2}).$$

We insert this estimate above, and sum over the $\binom{h}{k}$ k-element subsets S of $I(p;h)$ to find that

$$P_k(p;h,n) = \binom{h}{k}\left(\frac{p^n}{n^k} - \binom{h-k}{1}\frac{p^n}{n^{k+1}} + \cdots + (-1)^{h-k}\,\frac{p^n}{n^h}\right) + O\left(\binom{h}{k}2^{h-k}(hn)n!^h p^{n-1/2}\right).$$

The error term here is

$$\ll 2^{2h}(nh)n^{nh}p^{n-1/2} \ll \exp(Cn^2\log n)p^{n-1/2}$$

for a constant C depending on I, and the main term is

$$\binom{h}{k}\frac{p^n}{n^k}\left(1-\frac{1}{n}\right)^{h-k}.$$

The theorem follows upon inserting into this expression for the main term the estimates

$$\begin{aligned}\binom{h}{k} &= \frac{h^k}{k!}\left(1-\frac{1}{h}\right)\left(1-\frac{2}{h}\right)\cdots\left(1-\frac{k-1}{h}\right)\\ &= \frac{h^k}{k!}\left(1+O\left(\frac{k^2}{h}\right)\right) = \frac{h^k}{k!}\left(1+O_I\left(\frac{k^2}{n}\right)\right),\\ \left(1-\frac{1}{n}\right)^{h-k} &= \left(1+O_I\left(\frac{k}{n}\right)\right)\left(1-\frac{1}{n}\right)^h\\ &= \exp(-h/n)\left(1+O_I\left(\frac{k}{n}\right)\right)\left(1+O_I\left(\frac{1}{n}\right)\right)\\ &= \exp(-h/n)\left(1+O_I\left(\frac{k+1}{n}\right)\right),\end{aligned}$$

once we recall that we are writing λ for h/n. ∎

4. Smooth values of polynomials: Proof of Theorem 3. For a permutation σ on a finite set, let $L(\sigma)$ denote the length of the longest cycle in the decomposition of σ into disjoint cycles. The following result is extracted from the thesis of X. Gourdon (cf. [11, Chapitre VII, Théorème 1]).

LEMMA 4 (Gourdon). *Let n be a positive integer and suppose $m > 0$. Then the proportion of permutations σ on n letters with $L(\sigma) \le m$ is $\varrho(n/m) + O(1/m)$.*

Thus, by the results mentioned in the introduction just before Conjecture 2, the proportion of permutations on n letters with largest cycle length $\le n/u$ is close to the proportion of degree n polynomials over a finite field with largest prime factor of degree $\le n/u$. (The idea that the decomposition of random permutations should mimic the decomposition of random arithmetic structures seems to appear first in the work of Knuth and Trabb Pardo [20] in their study of the rth largest prime factor of a random integer.)

Remarks. (i) In the original theorem of Gourdon, m is restricted to integral values in the interval $[2, n]$. However, the restriction to integral values is inessential; for any real m with $2 \le m \le n$,

$$\varrho(n/m) - \varrho(n/\lfloor m \rfloor) = \int_{n/m}^{n/\lfloor m \rfloor} \frac{\varrho(u-1)}{u}\, du \ll \log \frac{m}{\lfloor m \rfloor} \ll \frac{1}{m}.$$

Moreover, for $m < 2$ or $m > n$, Lemma 4 is trivial.

(ii) By a simple inductive argument, Omar et al. obtain Lemma 4 under the additional hypothesis that $m \ge \varepsilon n$ for an arbitrary fixed $\varepsilon > 0$ (see [23, Theorem 1]). This result gives Theorem 3 with its first error term replaced with the less uniform bound $O_{B,U}(uq^n/n)$. However, it suffices to establish Theorem 4(a) as stated.

Proof of Theorem 3. Let $P_1, \dots, P_K$ be the distinct monic irreducible factors of F, numbered so that $\deg P_i = d_i$. Then $F(h(T))$ has all its prime factors of degree $\le n/u$ precisely when the same is true for each of the polynomials $P_i(h(T))$. For $1 \le i \le K$, let λ_i run over the cycle types of permutations on n letters corresponding to permutations σ with $L(\sigma) \le n/d_i u$. By Theorem 5, we have

$$\Psi(F; n, n/u) = \sum_{\lambda_1,\dots,\lambda_K} q^n \prod_{i=1}^{K} T(\lambda_i) + O_B\Big(\sum_{\lambda_1,\dots,\lambda_K} nn!^B q^{n-1/2} \Big).$$

Since the number of possibilities for each λ_i is (crudely) bounded above by 2^n, the error here is

$$\ll_B 2^{nK} nn!^B q^{n-1/2} \le 2^{2nB} n!^B q^{n-1/2} \ll_B n!^{2B} q^{n-1/2}.$$

Using Lemma 4, we see that the main term here is

$$\begin{aligned} q^n \prod_{i=1}^{K} \Big(\sum_{\lambda_i} T(\lambda_i) \Big) &= q^n \prod_{i=1}^{K} (\varrho(d_i u) + O(d_i u/n)) \\ &= q^n \varrho(d_1 u) \cdots \varrho(d_K u) + O_B(uq^n/n). \end{aligned}$$

Combining these two estimates completes the proof of Theorem 3. ∎

5. Smoothness of neighboring polynomials: Proof of Theorem 4

Proof of Theorem 4(a). We may assume $n \ge 2$, since the estimate is trivial for $n = 1$ (or for any absolutely bounded n). By Lemma 4, the proportion of permutations σ on n letters for which

$$\alpha n \le L(\sigma) \le \beta n \tag{15}$$

is given by

$$\varrho(\beta^{-1}) - \varrho(\alpha^{-1}) + O(\kappa/n),$$

where $\kappa = \kappa([\alpha,\beta])$, provided we adopt the convention that $\varrho(0^{-1}) = 0$. (Recall that if $I = [\alpha,\beta]$, then $\kappa(I) = 1/\alpha$ if $\alpha \neq 0$ and $\kappa(I) = 1/\beta$ otherwise.) For each $s \in S$, let λ_s run over the cycle types of permutations satisfying (15) with $[\alpha,\beta] = [\alpha_s,\beta_s]$. Proceeding as in the proof of Theorem 3, we find that the number of polynomials $A(T)$ satisfying the conclusion of part (a) is

$$q^n \prod_{s\in S}\Big(\sum_{\lambda_s} T(\lambda_s)\Big) + O\Big(\sum_{\lambda_1,\dots,\lambda_k} (nk)n!^k q^{n-1/2}\Big).$$

The error term here is

$$\ll 2^{nk}(nk)n!^k q^{n-1/2} \ll n!^{2k} q^{n-1/2}.$$

Moreover, since $\kappa([\alpha_s,\beta_s]) \le C$ for each s, the main term here is

$$q^n \prod_{s\in S}(\varrho(\beta_s^{-1}) - \varrho(\alpha_s^{-1}) + O(C/n)) = q^n \prod_{s\in S}(\varrho(\beta_s^{-1}) - \varrho(\alpha_s^{-1})) + O_{k,C}(q^n/n).$$

Combining these estimates finishes the proof. ∎

To prove part (b), we require the following auxiliary result (see [25, Theorem 2]):

THEOREM B. *Let $f_1(T),\dots,f_r(T)$ be irreducible polynomials over $\mathbb{F}_q$. If q is large compared to the sum of the degrees of the f_i, then there is a prime l dividing $q-1$ and an element $\beta \in \mathbb{F}_q$ for which every substitution*

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

leaves all of $f_1,\dots,f_r$ irreducible.

Proof of Theorem 4(b). Let n be the least positive integer which is prime to q and exceeds $2\varepsilon^{-1}$; then $n = O_\varepsilon(1)$. For each $s \in S$, choose a $\lfloor \frac{1}{2}(\alpha_s+\beta_s)n \rfloor$-cycle σ_s from S_n. Since $n \ge 2\varepsilon^{-1} \ge 2(\beta_s-\alpha_s)^{-1}$, we have

$$\alpha_s n \le L(\sigma_s) \le \beta_s n$$

for each $s \in S$. Let λ_s be the cycle type of σ_s. By Theorem 5 (applied to the k linear polynomials $f_s(T) = T + s$), if q is chosen large enough (depending on k and ε), then we can find a monic, degree n polynomial $A(T)$ for which $A(T)+s$ has cycle type λ_s for all $s \in S$. For this choice of $A(T)$, we have

$$\alpha_s n \le L(A(T)+s) \le \beta_s n$$

for all $s \in S$. We have thus constructed a polynomial satisfying (5).

If q is large, we can use this polynomial $A(T)$ to construct an infinite sequence of solutions to (5): For each $s \in S$, let $P_s(T)$ be a monic prime of maximal degree dividing $A(T)+s$. Then the degree of $\prod_{s\in S} P_s(T)$ is $O_{k,\varepsilon}(1)$, and so by Theorem B, if q is large enough (again depending only on k and ε) one can find a prime l and a $\beta \in \mathbb{F}_q$ for which all the polynomials

$P_s(T^{l^k} - \beta)$ are irreducible for every $k \geq 0$. It is now easy to check that all the polynomials $A(T^{l^k} - \beta)$, with $k = 0, 1, 2, \ldots$, have the desired property. ∎

6. Proof of Theorem 5. We recall the basic setup of [27], referring to that paper for details and proofs. Our strategy is to count, for fixed values of

$$h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T \in \mathbb{F}_q[T], \tag{16}$$

the number of $a \in \mathbb{F}_q$ for which $f_i(h(T) - a)$ has cycle type $d_i \times \lambda_i$ for every $1 \leq i \leq r$. We then sum over h to complete the proof.

Fix an algebraically closed field Ω of infinite transcendence degree containing $\mathbb{F}_q(u)$; all fields appearing below are to be understood as subfields of Ω. Let $d_1, \ldots, d_r$ be the degrees of the polynomials $f_1, \ldots, f_r$, respectively, and fix roots $\theta_1, \ldots, \theta_r$ of $f_1, \ldots, f_r$ (respectively) from Ω. For each integer j, define $\theta_i^{(j)} := \theta_i^{q^j}$. Now define the function fields $K_{i,j}/\mathbb{F}_q$, $L_{i,j}/\mathbb{F}_q$ and $M_i/\mathbb{F}_q$ (for $1 \leq i \leq r$, $1 \leq j \leq d_i$) as follows (suppressing the dependence on h):

$K_{i,j}$	field obtained by adjoining a fixed root of $h(T) - u - \theta_i^{(j)}$ to $\mathbb{F}_{q^{d_i}}(u)$,
$L_{i,j}$	normal closure of $K_{i,j}$ over $\mathbb{F}_{q^{d_i}}(u)$, that is, the splitting field of $h(T) - u - \theta_i^{(j)}$ over $\mathbb{F}_{q^{d_i}}(u)$,
M_i	compositum of the fields $L_{i,j}$ for $j = 1, \ldots, d_i$, that is, the splitting field of $f_i(h(T) - u)$ over $\mathbb{F}_{q^{d_i}}(u)$.

Let D be the least common multiple of $d_1, \ldots, d_r$, and set $\widetilde{K}_{i,j} := K_{i,j}\mathbb{F}_{q^D}$, $\widetilde{L}_{i,j} := L_{i,j}\mathbb{F}_{q^D}$ and $\widetilde{M}_i := M_i\mathbb{F}_{q^D}$. Finally, let $\widetilde{M}$ be the compositum of $\widetilde{M}_1, \ldots, \widetilde{M}_r$. (Thus $\widetilde{M}$ is the splitting field of $\prod_{i=1}^r f_i(h(T) - u)$ over $\mathbb{F}_{q^D}(u)$.) The assumption that p does not divide n implies that the extensions $M_i/\mathbb{F}_q(u)$ (for $1 \leq i \leq r$) are all Galois, as are all the $\widetilde{M}_i/\mathbb{F}_q(u)$ and $\widetilde{M}/\mathbb{F}_q(u)$ (see [27, Lemma 5]).

The groups $\mathrm{Gal}(\widetilde{M}/\mathbb{F}_q(u))$ and $\mathrm{Gal}(M_i/\mathbb{F}_q(u))$ are related as follows. Let $S_{i,j}$ denote the full set of roots of $h(T) - u - \theta_i^{(j)}$ (thus $S_{i,j}$ is periodic in j with period d_i). Then we have for each $k = 1, \ldots, r$ a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\widetilde{M}/\mathbb{F}_q(u)) & \xrightarrow{\iota_1} & \mathrm{Gal}(\mathbb{F}_{q^D}/\mathbb{F}_q) \times \prod_{i=1}^r \mathrm{Sym}(\bigcup_{j=1}^{d_i} S_{i,j}) \\ {\scriptstyle \sigma \mapsto \sigma|_{M_k}}\downarrow & & \downarrow{\scriptstyle \pi} \\ \mathrm{Gal}(M_k/\mathbb{F}_q(u)) & \xrightarrow{\iota_2} & \mathrm{Gal}(\mathbb{F}_{q^{d_k}}/\mathbb{F}_q) \times \mathrm{Sym}(\bigcup_{j=1}^{d_k} S_{k,j}) \end{array} \tag{17}$$

Here the maps ι_1, ι_2 are given by

$$\iota_1 \colon \sigma \mapsto (\sigma|_{\mathbb{F}_{q^D}}, \sigma|_{\bigcup_{j=1}^{d_1} S_{1,j}}, \ldots, \sigma|_{\bigcup_{j=1}^{d_r} S_{r,j}}), \qquad \iota_2 \colon \sigma \mapsto (\sigma|_{\mathbb{F}_{q^{d_k}}}, \sigma|_{\bigcup_{j=1}^{d_k} S_{k,j}}),$$

and

$$\pi\colon (\tau, \sigma_1, \dots, \sigma_r) \mapsto (\tau|_{\mathbb{F}_{q^{d_k}}}, \sigma_k).$$

(Note that ι_1 and ι_2 are embeddings while π is a surjection.)

For most choices of $h(T)$ it is possible to describe, in a simple and explicit way, the images of ι_1 and ι_2. Indeed, assume that

$$\operatorname{disc}_u^{n-1} \operatorname{disc}_T^n(h(T) - u - \theta_i^{(j)}) \neq 0 \quad \text{for all } 1 \le i \le r,\ 1 \le j \le d_i, \tag{18}$$

$$\operatorname{res}_u^{n-1,n-1}(\operatorname{disc}_T^n(h(T) - u - \theta_i^{(j)}), \operatorname{disc}_T^n(h(T) - u - \theta_{i'}^{(j')})) \neq 0 \tag{19}$$
$$\text{whenever } i, i', j, j' \text{ are as above and } (i,j) \neq (i',j').$$

(Here the subscripts indicate the variable with respect to which the resultants and discriminants are to be computed, and the superscripts indicate the formal degrees of the arguments.) Together these conditions exclude at most

$$4n^2 q^{n-2}\left(1 + \binom{B}{2}\right)$$

values of $h(T)$ of the form (16) (see [27, Lemma 6]) and for the remaining choices of $h(T)$ the following holds (see [27, Lemma 7]): Let Frob denote the qth power map; then the image of ι_1 consists of all pairs $(\mathrm{Frob}^l, \sigma) \in \mathrm{Gal}(\mathbb{F}_{q^D}/\mathbb{F}_q) \times \prod_{i=1}^r \mathrm{Sym}(\bigcup_{j=1}^{d_i} S_{i,j})$ which obey the compatibility condition

$$\sigma(S_{i,j}) \subset S_{i,j+l} \quad \text{for all } 1 \le i \le r \text{ and all } j. \tag{20}$$

Similarly, for each $k = 1, \dots, r$, the image of ι_2 consists of all pairs $(\mathrm{Frob}^l, \sigma) \in \mathrm{Gal}(\mathbb{F}_{q^{d_k}}/\mathbb{F}_q) \times \mathrm{Sym}(\bigcup_{j=1}^{d_k} S_{k,j})$ satisfying

$$\sigma(S_{k,j}) \subset S_{k,j+l} \tag{21}$$

for all j.

The following result supersedes Lemma 12 of [27].

LEMMA 5. *Let $g(T)$ be a squarefree polynomial of degree n over $\mathbb{F}_{q^d}$ which is coprime to all its conjugates over $\mathbb{F}_q$, that is,* $\gcd(g(T), \sigma(g(T))) = 1$ *for every $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$. If λ is the factorization type of $g(T)$, then $d \times \lambda$ is the factorization type of* $\mathrm{Nm}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(g(T)) := \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)} \sigma(g(T))$.

Proof. Since $g(T)$ is squarefree, so are all the polynomials $\sigma(g(T))$, and as $g(T)$ is coprime to its conjugates, $\mathrm{Nm}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(g(T))$ is also squarefree.

Suppose that Q is a monic prime of $\mathbb{F}_{q^d}[T]$ that divides $g(T)$, and let P be the monic prime of $\mathbb{F}_q[T]$ that lies below Q. Let $f(Q/P)$ be the inertial degree of Q over P. Since $\mathrm{Nm}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(Q) = P^{f(Q/P)}$ divides the squarefree polynomial $\mathrm{Nm}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(g(T))$, we must have $f(Q/P) = 1$ and $\mathrm{Nm}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(Q) = P$. In particular, $\deg P = d \deg Q$.

Thus, if we start with a factorization of $g(T)$ exhibiting cycle type λ, taking norms gives us a corresponding factorization of $\mathrm{Nm}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(g(T))$ with cycle type $d \times \lambda$. ∎

The next lemma replaces [27, Lemma 13]. For $a \in \mathbb{F}_q$, we use P_a to denote the prime of $\mathbb{F}_q(u)$ corresponding to the $(u-a)$-adic valuation.

LEMMA 6. *Assume $h(T)$ obeys the nondegeneracy conditions* [27, eqs. (2.2) and (2.3)]. *If $\lambda_1, \dots, \lambda_r$ are arbitrary partitions of n, then* $\mathrm{Gal}(\widetilde{M}/\mathbb{F}_q(u))$ *contains a conjugacy class $\mathcal{C}$, of size*

$$n!^{d_1+\cdots+d_r} \prod_{i=1}^{r} T(\lambda_i),$$

with the following property: *Suppose that a is an element of $\mathbb{F}_q$ which is not a zero of any of the polynomials*

$$\mathrm{disc}_T(h(T) - u - \theta_i^{(j)}) \quad \text{for } 1 \le i \le r,\ 1 \le j \le d_i. \tag{22}$$

Then $f_i(h(T)-a)$ has factorization type λ_i for every $1 \le i \le r$ exactly when $\mathcal{C}$ coincides with the Frobenius conjugacy class $(\widetilde{M}/\mathbb{F}_q(u), P_a)$.

Proof. Since a is not a root of any of the polynomials (22), P_a is unramified in $\widetilde{M}$ and the polynomials $h(T) - a - \theta_i^{(j)}$ are squarefree for all i and j. Now fix $1 \le i \le r$. Applying Lemma 5 with $g(T) = h(T) - a - \theta_i^{(1)}$, we see that

$$h(T) - a - \theta_i^{(1)} \text{ has type } \lambda_i \text{ over } \mathbb{F}_{q^{d_i}} \\ \Leftrightarrow\ f_i(h(T)-a) \text{ has type } d \times \lambda_i \text{ over } \mathbb{F}_q.$$

There is a unique prime Q_a of $\mathbb{F}_{q^{d_i}}(u)$ that lies over P_a, and for this prime we have

$$f(Q_a/P_a) = d_i \quad \text{and} \quad e(Q_a/P_a) = 1. \tag{23}$$

By Kummer's theorem [31, Theorem 3.3.7], the factorization of $h(T) - a - \theta_i^{(1)}$ mirrors the factorization of Q_a in $K_{i,1}$. So if $\lambda_i = (t_1, \dots, t_s)$, then $f_i(h(T)-a)$ has type $d_i \times \lambda_i$ if and only if Q_a factors in $K_{i,1}$ into primes of relative degrees $t_1, \dots, t_s$. By (23), this in turn occurs exactly when P_a factors in $K_{i,1}$ into primes of degrees $d_i t_1, \dots, d_i t_s$.

This last possibility can be recast in terms of the action of Frobenius. Let σ denote any element of the Frobenius conjugacy class $(M_i/\mathbb{F}_q(u), P_a)$; then necessarily

$$\sigma \text{ restricts to the } q\text{th power map on } \mathbb{F}_{q^{d_i}}, \tag{24}$$

so that the image of σ under ι_2 has the form (Frob, σ') for some permutation σ' of $\bigcup_{j=1}^{d_i} S_{i,j}$ (obeying the compatibility condition (21) with $k = i$ and $l = 1$). Then P_a factors as indicated above if and only if σ has cycles of lengths $d_i t_1, \dots, d_i t_s$ when acting by right-multiplication on

the right-cosets of $H = \mathrm{Gal}(M_i/K_{i,1})$ in the group $\mathrm{Gal}(M_i/\mathbb{F}_q(u))$. We claim that this is equivalent to σ', considered as a permutation of the nd_i-element set $\bigcup_{j=1}^{d_i} S_{i,j}$, decomposing as a product of s disjoint cycles of lengths $d_i t_1, \ldots, d_i t_s$. To prove this, we exhibit a bijective length-preserving correspondence between the cycles in the decomposition of σ' and the cycles appearing when σ acts by right-multiplication on the right-cosets of H.

We set this correspondence up as follows. Write $K_{i,1} = \mathbb{F}_{q^{d_i}}(u)(\alpha)$, where $\alpha \in S_{i,1}$. Let C' be a cycle appearing in the decomposition of σ', and let β be an element appearing in C'. Choose an element τ of $\mathrm{Gal}(M_i/\mathbb{F}_q(u))$ with $\tau(\beta) = \alpha$. (The existence of such an element follows from our description of the image of ι_2 above.) We define our bijection by sending

$$C' \mapsto C, \text{ where } C \text{ is that cycle of the right-action containing } H\tau. \tag{25}$$

We must check that this does not depend on the particular choice of τ and β. To this end, suppose that $\tau_1(\beta) = \tau_2(\beta) = \alpha$. Then $\tau_1\tau_2^{-1}$ fixes both α and $\mathbb{F}_q(u)$, so must also fix the entire field

$$\mathbb{F}_q(u)(\alpha) = \mathbb{F}_q(u)(h(\alpha), \alpha) = \mathbb{F}_q(u)(\theta_i^{(1)})(\alpha) = \mathbb{F}_{q^{d_i}}(u)(\alpha) = K_{i,1}.$$

Thus $\tau_1\tau_2^{-1} \in \mathrm{Gal}(M/K_{i,1}) = H$, and so $H\tau_1 = H\tau_2$, proving that our map is independent of the choice of τ. Now suppose β_1 and β_2 both appear in the cycle C'; then $\beta_2 = \sigma^j(\beta_1)$ for some j. If $\tau(\beta_1) = \alpha$, then $(\tau\sigma^j)(\beta_2) = \alpha$. Thus (25) associates to C' both the cycle containing $H\tau$ and the cycle containing $H\tau\sigma^j$. But these coincide, since our action is right-multiplication by σ.

Suppose now that two cycles C_1' and C_2' are mapped to the same cycle C. Choose elements β_1 and β_2 which appear in the cycles C_1' and C_2' respectively, and choose τ_1 and τ_2 from $\mathrm{Gal}(M_i/\mathbb{F}_q(u))$ with $\tau_1(\beta_1) = \alpha$ and $\tau_2(\beta_2) = \alpha$. It follows that $H\tau_1$ and $H\tau_2$ appear in the same cycle of our right-action, so that $H\tau_1 = H\tau_2\sigma^j$ for some j. Hence the *left*-cosets $\tau_1^{-1}H$ and $\sigma^{-j}\tau_2^{-1}H$ coincide. But elements of the former coset send α to β_1 and elements of the latter send α to $\sigma^{-j}(\beta_2)$. It follows that β_1 and β_2 belong to the same cycle of σ; i.e., $C_1' = C_2'$. This proves injectivity.

Now we show that the association (25) takes cycles C' to cycles C of the same length. Writing $|\cdot|$ for the length of a cycle in both cases, we observe that for an arbitrary integer j,

$$\begin{aligned} |C| \text{ divides } j &\Leftrightarrow H\tau\sigma^j = H\tau \Leftrightarrow \tau^{-1}H = \sigma^{-j}\tau^{-1}H \\ &\Leftrightarrow \tau^{-1}(\alpha) = \sigma^{-j}\tau^{-1}(\alpha) \Leftrightarrow \beta = \sigma^{-j}(\beta) \Leftrightarrow |C'| \text{ divides } j. \end{aligned}$$

This forces $|C| = |C'|$.

Surjectivity of our map now follows, as the lengths of the cycles of C and the lengths of the cycles of C' must both sum to n. This completes the proof that (25) defines a bijective, length-preserving map.

At this point we have reduced the problem to a consideration of those permutations σ' of $\bigcup_{j=1}^{d_i} S_{i,j}$ which obey the compatibility condition (21) (with $k = i$ and $l = 1$) and which decompose into disjoint cycles of lengths $d_i t_1, \dots, d_i t_s$. Such cycles can be explicitly constructed as follows: Take any permutation of $S_{i,1}$ of cycle type λ_i; there are $T(\lambda_i)n!$ of these. This permutation serves as a template for a permutation σ' with the desired properties: use the given permutation to fill in every dth element in the cycles of σ', and fill in the remaining spots arbitrarily, subject only to the compatibility condition. The latter task can be done in $n!^{d_i-1}$ ways, and this shows that the total number of such σ' is $T(\lambda)n!^{d_i}$.

Suppose $\gamma \in \mathrm{Gal}(\widetilde{M}/\mathbb{F}_q(u))$ belongs to the Frobenius conjugacy class $(\widetilde{M}/\mathbb{F}_q(u), P_a)$. Then in order that $f_i(h(T) - a)$ have cycle type $d_i \times \lambda_i$ for every $i = 1, \dots, r$, it is necessary and sufficient that $\gamma|_{M_i}$ obey the conditions imposed on σ' above for every i. That is, it is necessary and sufficient that γ (identified with its image under ι_1) have the form $(\mathrm{Frob}, \sigma_1, \dots, \sigma_r)$, where each σ_i is one of the previously constructed $n!^{d_i} T(\lambda_i)$ permutations on $\bigcup_{j=1}^{d_i} S_{i,j}$. There are $n!^{d_1+\cdots+d_r} \prod_{i=1}^{r} T(\lambda_i)$ possible tuples $(\mathrm{Frob}, \sigma_1, \dots, \sigma_r)$, and because the σ_i obey the stated compatibility conditions, these tuples correspond to distinct, well-defined elements of $\mathrm{Gal}(\widetilde{M}/\mathbb{F}_q(u))$.

For a set S, let $\mathrm{Sym}(S)$ denote the group of permutations on S. Then (see [27, Lemma 8(i), (ii)])

$$\mathrm{Gal}(\widetilde{M}/\mathbb{F}_q(u)) \supset \mathrm{Gal}(\widetilde{M}/\mathbb{F}_{q^D}(u)) = \prod_{\substack{1 \le i \le r \\ 1 \le j \le d_i}} \mathrm{Sym}(S_{i,j}), \tag{26}$$

where each $\mathrm{Sym}(S_{i,j})$ is thought of as a subgroup of $\mathrm{Sym}(\bigcup_{1 \le i \le r,\, 1 \le j \le d_i} S_{i,j})$. From (26) and our construction of the σ_i, it is easy to convince oneself that the set of elements $\mathcal{C}$ (say) constructed above constitutes a single conjugacy class of $\mathrm{Gal}(\widetilde{M}/\mathbb{F}_q(u))$. ∎

We can now complete the proof of Theorem 5 much as in [27]. We once again require the following version of the Chebotarev density theorem. (This result is implicit in the proof of [9, Proposition 6.4.8].)

Explicit Chebotarev density theorem for first degree primes. *Suppose that $M/\mathbb{F}_q(u)$ is a finite Galois extension having full field of constants $\mathbb{F}_{q^D}$. Let $\mathcal{C}$ be a conjugacy class of $\mathrm{Gal}(M/\mathbb{F}_q(u))$ every element of which restricts to the qth power map on $\mathbb{F}_{q^D}$. Let*

$$\mathcal{P} := \left\{ \textit{degree 1 primes } P \textit{ of } \mathbb{F}_q(u) \textit{ unramified in } M : \left(\frac{M/\mathbb{F}_q(u)}{P} \right) = \mathcal{C} \right\}.$$

Then

$$\left|\#\mathcal{P} - \frac{\mathcal{C}}{[M:\mathbb{F}_{q^D}(u)]}\,q\right| \le 2\,\frac{\#\mathcal{C}}{[M:\mathbb{F}_{q^D}(u)]}\,(gq^{1/2}+g+[M:\mathbb{F}_{q^D}(u)]),$$

where g denotes the genus of $M/\mathbb{F}_{q^D}$.

Proof of Theorem 5. As always, we may assume $n \ge 2$, since Theorem 5 is trivial otherwise. Let X be the number of polynomials $h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T \in \mathbb{F}_q[T]$ satisfying both nondegeneracy conditions [27, eqs. (2.2) and (2.3)].

Suppose $h(T)$ is one of the polynomials counted by X, and let N_h be the number of $a \in \mathbb{F}_q$ with the property that $f_i(h(T)-a)$ has cycle type λ_i for all $1 \le i \le r$. For all but at most $(n-1)B$ values of a, Lemma 6 asserts that this property is equivalent to $(\widetilde{M}/\mathbb{F}_q(u), P_a)$ coinciding with the conjugacy class $\mathcal{C}$ of that lemma. Since

$$|\mathcal{C}| = n!^{d_1+\cdots+d_r}\prod_{i=1}^{r} T(\lambda_i) \quad \text{and} \quad [\widetilde{M}:\mathbb{F}_{q^D}(u)] = n!^{d_1+\cdots+d_r},$$

the Chebotarev density theorem in the above explicit form gives us

$$\left|N_h - q\prod_{i=1}^{r} T(\lambda_i)\right| \le \Big(2\prod_{i=1}^{r} T(\lambda_i)\Big)(gq^{1/2}+g+n!^{d_1+\cdots+d_r}) + (n-1)B.$$

Since $g \le Bnn!^B$ [27, Corollary 15], the right-hand side of this inequality is $O((Bn)n!^Bq^{n-1/2})$. Thus the total number of polynomials $\widetilde{h}(T)$ for which $f_i(\widetilde{h}(T))$ has cycle type λ_i for all $1 \le i \le r$ is

$$Xq\prod_{i=1}^{r} T(\lambda_i) + O(X(Bn)n!^Bq^{1/2}) + O((q^{n-1}-X)q).$$

Making use of the bounds

$$q^{n-1} - 4n^2q^{n-2}\left(1+\binom{B}{2}\right) \le X \le q^{n-1},$$

we find that this number is

$$q^n\prod_{i=1}^{r} T(\lambda_i) + O((Bn)n!^Bq^{n-1/2}) + O(n^2B^2q^{n-1}).$$

The proof is completed by the (easy) verification that the first O-term is dominant (using $n \ge 2$). ∎

Acknowledgements. I would like to thank Andrew Granville for suggesting that some form of Theorem 2 should follow from the results of [27]. I am also indebted to my advisor, Carl Pomerance, for suggestions that made this a stronger and more readable paper.

References

[1] R. Arratia, A. D. Barbour, and S. Tavaré, *Logarithmic Combinatorial Structures*: *A Probabilistic Approach*, EMS Monogr. Math., Eur. Math. Soc., Zürich, 2003.

[2] A. Balog and T. D. Wooley, *On strings of consecutive integers with no large prime factors*, J. Austral. Math. Soc. Ser. A 64 (1998), 266–276.

[3] V. Brun, *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ *où les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie*, Bull. Sci. Math. 43 (1919), 100–104, 124–128.

[4] M. Car, *Théorèmes de densité dans* $\mathbf{F}_q[X]$, Acta Arith. 48 (1987), 145–165.

[5] R. Crandall and C. Pomerance, *Prime Numbers*: *A Computational Perspective*, 2nd ed., Springer, New York, 2005.

[6] K. Dickmann, *On the frequency of numbers containing prime factors of a certain relative magnitude*, Ark. Mat. Astronom Fys. A 22 (1930), no. 10, 14 pp.

[7] P. Erdős, *Problems and results on number theoretic properties of consecutive integers and related questions*, in: Proc. Fifth Manitoba Conference on Numerical Mathematics (Univ. of Manitoba, Winnipeg, 1975), Congressus Numerantium 16, Utilitas Math., Winnipeg, 1976, 25–44.

[8] P. Erdős and C. Pomerance, *On the largest prime factors of* n *and* $n+1$, Aequationes Math. 17 (1978), 311–321.

[9] M. D. Fried and M. Jarden, *Field Arithmetic*, 2nd ed., Ergeb. Math. Grenzgeb. (3) 11, Springer, Berlin, 2005.

[10] P. X. Gallagher, *On the distribution of primes in short intervals*, Mathematika 23 (1976), 4–9; corrigendum, ibid. 28 (1981), 86.

[11] X. Gourdon, *Combinatoire, algorithmique et géométrie des polynômes*, Ph.D. thesis, École Polytechnique, 1996.

[12] A. Granville, *Anatomy of integers and permutations*, preprint, http://www.dms.umontreal.ca/∼andrew/PDF/Anatomy.pdf.

[13] —, *Harald Cramér and the distribution of prime numbers*, Harald Cramér Sympos. (Stockholm, 1993), Scand. Actuar. J. 1995, 12–28.

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

[15] A. J. Hildebrand, *On a conjecture of Balog*, Proc. Amer. Math. Soc. 95 (1985), 517–523.

[16] —, *On integer sets containing strings of consecutive integers*, Mathematika 36 (1989), 60–70.

[17] —, *Multiplicative properties of consecutive integers*, in: Analytic Number Theory (Kyoto, 1996), London Math. Soc. Lecture Note Ser. 247, Cambridge Univ. Press, Cambridge, 1997, 103–117.

[18] C.-N. Hsu, *A large sieve inequality for rational function fields*, J. Number Theory 58 (1996), 267–287.

[19] D. Klyve, *Explicit bounds on twin primes and Brun's constant*, Ph.D. thesis, Dartmouth College, 2007.

[20] D. E. Knuth and L. Trabb Pardo, *Analysis of a simple factorization algorithm*, Theoret. Comput. Sci. 3 (1976/77), 321–348.

[21] G. Martin, *An asymptotic formula for the number of smooth values of a polynomial*, J. Number Theory 93 (2002), 108–182.

[22] A. Masuda and D. Panario, *Sequences of consecutive smooth polynomials over a finite field*, Proc. Amer. Math. Soc. 135 (2007), 1271–1277.

[23] M. Omar, D. Panario, B. Richmond, and J. Whitely, *Asymptotics of largest components in combinatorial structures*, Algorithmica 46 (2006), 493–503.

[24] D. Panario, X. Gourdon, and P. Flajolet, *An analytic approach to smooth polynomials over finite fields*, in: Algorithmic Number Theory (Portland, OR, 1998), Lecture Notes in Comput. Sci. 1423, Springer, Berlin, 1998, 226–236.

[25] P. Pollack, *An explicit approach to Hypothesis H for polynomials over a finite field*, in: Anatomy of Integers, CRM Proc. Lecture Notes 46, Amer. Math. Soc., 2008, 47–64.

[26] —, *A polynomial analogue of the twin prime conjecture*, Proc. Amer. Math. Soc. 136 (2008), 3775–3784.

[27] —, *Simultaneous prime specializations of polynomials over finite fields*, Proc. London Math. Soc. 97 (2008), 545–567.

[28] H. Riesel and R. C. Vaughan, *On sums of primes*, Ark. Mat. 21 (1983), 46–74.

[29] P. Sebah and X. Gourdon, *Introduction to twin primes and Brun's constant computation*, reported online at http://numbers.computation.free.fr/Constants/constants.html.

[30] V. T. Sós, *Turbulent years*: *Erdős in his correspondence with Turán from 1934 to 1940*, Paul Erdős and His Mathematics, I (Budapest, 1999), Bolyai Soc. Math. Stud. 11, János Bolyai Math. Soc., Budapest, 2002, 85–146.

[31] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer, Berlin, 1993.

[32] W. A. Webb, *Sieve methods for polynomial rings over finite fields*, J. Number Theory 16 (1983), 343–355.

Department of Mathematics
University of Illinois at Urbana-Champaign
273 Altgeld Hall, MC-382
1409 West Green Street
Urbana, IL 61801, U.S.A.
E-mail: pppollac@illinois.edu

Received on 8.5.2008
and in revised form on 1.7.2008 (5704)