PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 11, November 2008, Pages 3775–3784
S 0002-9939(08)09351-9
Article electronically published on May 20, 2008

A POLYNOMIAL ANALOGUE OF THE TWIN PRIME CONJECTURE

PAUL POLLACK

(Communicated by Ken Ono)

ABSTRACT. We consider the problem of counting the number of (not necessarily monic) 'twin prime pairs' $P, P+M \in \mathbf{F}_q[T]$ of degree n, where M is a polynomial of degree $< n$. We formulate an asymptotic prediction for the number of such pairs as $q^n \to \infty$ and then prove an explicit estimate confirming the conjecture in those cases where q is large compared with n^2. When M has degree $n-1$, our theorem implies the validity of a result conditionally proved by Hayes in 1963. When M has degree zero, our theorem refines a result of Effinger, Hicks and Mullen.

1. INTRODUCTION

1.1. **A uniform conjecture.** Let M be a nonzero polynomial over a finite field $\mathbf{F}_q$, and let $R(n; M, q)$ denote the number of 'twin prime pairs' $P, P+M$, where P runs over the irreducible polynomials of degree n. Reasoning in analogy with the usual heuristic arguments offered for configurations of rational primes (compare, e.g., with [11, pp. 409-411]), we are led to expect that for $n > \deg M$,

$$R(n; M, q) \approx R_0(n; M, q), \tag{1}$$

where

$$R_0(n; M, q) := (q-1)\frac{q^n}{n^2} \prod_{Q \mid M} \left(1 - \frac{1}{|Q|}\right)^{-1} \prod_{Q \nmid M} \left(1 - \frac{2}{|Q|}\right)\left(1 - \frac{1}{|Q|}\right)^{-2}.$$

(For a nonzero polynomial $N \in \mathbf{F}_q[T]$, we denote by $|N|$ the number of elements in the ring $\mathbf{F}_q[T]/(N)$, that is, $|N| = q^{\deg N}$.) Here and below Q denotes a generic *monic* irreducible over $\mathbf{F}_q$. The factor of $q-1$ in front stems from the fact that P is not restricted to monic values.

There are various ways one might attempt to make the approximation (1) precise; perhaps the most obvious is to fix q and M, and to read (1) as an asymptotic estimate as n tends to infinity. Various special cases of such a conjecture were proposed by Effinger, Hicks and Mullen (see [3]). Little is known in this direction; in fact it was only recently that Hall [4, p. 140] showed the existence of infinitely many twin prime pairs $P, P+M$ over $\mathbf{F}_q$ in the special case when M is constant

Received by the editors July 10, 2007, and, in revised form, September 19, 2007.
2000 *Mathematics Subject Classification.* Primary 11T55; Secondary 11N32.
The author was supported by an NSF Graduate Research Fellowship.

(and $q > 3$), but his clever proof yields very weak lower bounds on the number of such pairs. For a discussion of Hall's results and some generalizations, see [8].

A different approach is suggested by another result from the same paper of Effinger, Hicks and Mullen. A special case of these authors' Proposition 1 (op. cit.) is that for M a nonzero constant polynomial, one has $R(n; M, q) > 0$ for $q \geq 2n$. This suggests that $R(n; M, q)$ may be more amenable to study as a function of multiple parameters. Once in this frame of mind, it is easy to formulate a more uniform conjecture, justified by the same classical heuristic alluded to above:

Conjecture 1. *Let M be a nonzero polynomial of degree $< n$ over $\mathbf{F}_q$. Then*

$$R(n; M, q) = (1 + o(1))R_0(n; M, q) \quad \text{as} \quad q^n \to \infty,$$

uniformly in M. In other words, for every $\epsilon > 0$, there is a constant $B = B(\epsilon)$ with the property that whenever M is a nonzero polynomial over $\mathbf{F}_q$ of degree $< n$ and $q^n > B$, we have

$$|R(n; M, q) - R_0(n; M, q)| < \epsilon R_0(n; M, q).$$

The purpose of this paper is to prove an explicit estimate for $R(n; M, q)$ which confirms Conjecture 1 whenever q/n^2 tends to infinity (uniformly in the choice of $M \in \mathbf{F}_q[T]$ of degree $< n$).

1.2. **Statement of the main result.** Again considering the right-hand side of the approximation (1), we observe that each factor in the second product is $1+O(|Q|^{-2})$. From this one may deduce that

$$R_0(n; M, q) = (1 + O(1/q))\frac{q^{n+1}}{n^2} \prod_{Q|M} \left(1 - \frac{1}{|Q|}\right)^{-1}.$$

In particular, Conjecture 1 would imply that as $q \to \infty$, we have

$$R(n; M, q) = (1 + o(1))\frac{q^{n+1}}{n^2} \prod_{Q|M} \left(1 - \frac{1}{|Q|}\right)^{-1}, \tag{2}$$

uniformly in n and M (with $0 \leq \deg M < n$).

We can now state our main result. We write $\phi(M)$ for the number of units in the ring $\mathbf{F}_q[T]/(M)$; note that $\prod_{Q|M}(1 - 1/|Q|)^{-1} = |M|/\phi(M)$.

Theorem 1. *Let $k \geq 0$ and $n \geq 2$ be integers with $0 \leq k < n$. Let M be a polynomial of degree k over $\mathbf{F}_q$. Then*

$$-\frac{q^n}{n} - 4\frac{|M|}{\phi(M)}\frac{q^{n/p+1}}{n^2} \leq R(n; M, q) - \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} \leq q^n - \frac{q^n}{n} + 2\frac{q^{n/p}}{n},$$

where p is the least prime divisor of n.

In the omitted case $k = 0$ and $n = 1$, it is easy to see that one has the exact expression $R(n; M, q) = q^2 - q$.

Remark. As a consequence of Theorem 1, we see that

$$1 + O(n/q) \leq \frac{R(n; M, q)}{(|M|/\phi(M))q^{n+1}/n^2} \leq 1 + O(n^2/q).$$

Thus if q^n tends to infinity in such a way that n^2/q tends to zero, we have the asymptotic for $R(n; M, q)$ predicted by (2), while the lower bound aspect of this

asymptotic already holds if n/q tends to zero. These estimates can be compared with the uniform upper bound

$$R(n; M, q) \leq 8\frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2}, \tag{3}$$

which follows from an application of Selberg's upper-bound sieve, as developed in the polynomial setting by Webb (see [13]). Full details of the proof of (3) are supplied in the Appendix.

When $k = n - 1$, a weaker version of Theorem 1 was stated by Hayes [5, Theorem 2]. However, the proof of his lower bound on $R(n; M, q)$ contained a gap [6], and he salvaged his main result only under additional hypotheses. Our argument for the upper bound in Theorem 1 closely follows Hayes. Our proof of the lower bound rests on a simple averaging argument applied to the well-known formula for the number of prime polynomials of a given degree.

Finally, we remark that if we let P run over only monic primes, then we still believe the analogue of Conjecture 1, but obtaining an analogue of Theorem 1 appears substantially more difficult. A somewhat weaker result in the case of constant polynomials M is contained in the main theorem of [9].

Notation. We use p to denote the least prime factor of the integer n. (Thus p is not necessarily the characteristic of $\mathbf{F}_q$.) We write $\pi(n; q)$ for the number of monic primes of degree n over $\mathbf{F}_q$; for future use we record the well-known estimates

$$\frac{q^n}{n} - 2\frac{q^{n/p}}{n} \leq \pi(n; q) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} \leq \frac{q^n}{n}. \tag{4}$$

All sums and products indexed by Q are to be taken only over monic primes Q.

2. An explicit formula for primes in certain residue classes

Let $\mathcal{M}$ be the (multiplicative) monoid of monic polynomials over $\mathbf{F}_q$. If $l \geq 0$ and $M \in \mathcal{M}$, we define a relation $\mathbf{R}_{l,M}$ on $\mathcal{M}$ by saying that $A \equiv B \pmod{\mathbf{R}_{l,M}}$ if and only if A and B have the same first l next-to-leading coefficients and $A \equiv B \pmod{M}$. Then $\mathbf{R}_{l,M}$ is a congruence relation on $\mathcal{M}$, i.e., an equivalence relation satisfying

$$A \equiv B \bmod \mathbf{R}_{l,M} \Rightarrow AC \equiv BC \bmod \mathbf{R}_{l,M} \quad \text{for all} \quad A, B, C \in \mathcal{M}.$$

Thus there is a well-defined quotient monoid $\mathcal{M}/\mathbf{R}_{l,M}$. It can be shown that an element of $\mathcal{M}$ is invertible modulo $\mathbf{R}_{l,M}$ if and only if it is coprime to M. The units of this monoid form an abelian group of size $q^l\phi(M)$, which we denote by $(\mathcal{M}/\mathbf{R}_{l,M})^\times$ (cf. [7, Theorem 8.6]).

Now fix $l \geq 0$ and $M \in \mathcal{M}$. Let χ be a character of $(\mathcal{M}/\mathbf{R}_{l,M})^\times$, and lift χ to a function on $\mathcal{M}$ (defining χ to vanish at elements of $\mathcal{M}$ that are nonunits of $\mathcal{M}/\mathbf{R}_{l,M}$). For $u \in \mathbf{C}$ with $|u| < 1/q$, define

$$L(u, \chi) := \prod_Q (1 - \chi(Q)u^{\deg Q})^{-1}. \tag{5}$$

If χ is nontrivial, then $L(u,\chi)$ is a polynomial in u, and for some integer $a(\chi) \leq l + \deg M$, we have a factorization

$$L(u,\chi) = \prod_{i=1}^{a(\chi)} (1 - \beta_i(\chi)u), \tag{6}$$

where from Weil's Riemann Hypothesis and the work of Rhin [10, Chapter 2] we know that $|\beta_i(\chi)| \leq q^{1/2}$ for $1 \leq i \leq a(\chi)$. (Cf. the proof of [2, Theorem 5.7].) From the Euler product representation (5), we deduce

$$\begin{aligned} u\frac{L'(u,\chi)}{L(u,\chi)} &= \sum_Q \deg Q \frac{\chi(Q)u^{\deg Q}}{1-\chi(Q)u^{\deg Q}} \\ &= \sum_{N=1}^{\infty} u^N \sum_{\deg Q^j = N} \chi(Q^j)\deg Q, \end{aligned}$$

while from (6), we have

$$u\frac{L'(u,\chi)}{L(u,\chi)} = -\sum_{i=1}^{a(\chi)} \frac{\beta_i(\chi)u}{1-\beta_i(\chi)u} = -\sum_{N=1}^{\infty} u^N \left(\sum_{i=1}^{a(\chi)} \beta_i(\chi)^N \right).$$

Comparing coefficients in these two expansions, we conclude that

$$\sum_{\deg Q^j = N} \chi(Q^j)\deg Q = -\sum_{i=1}^{a(\chi)} \beta_i(\chi)^N.$$

On the other hand, if $\chi = \chi_0$, then

$$L(u,\chi) = \frac{1}{1-qu} \prod_{Q|M} (1-u^{\deg Q}) = \frac{1}{1-qu} \prod_{i=1}^{a(\chi_0)} (1-\beta_i(\chi_0)u),$$

for certain roots of unity $\beta_i(\chi_0)$ (say), the number of which, say $a(\chi_0)$, is exactly $\sum_{Q|M} \deg Q \leq \deg M$. Proceeding as above we find

$$\sum_{\deg Q^j = N} \chi_0(Q^j)\deg Q = q^N - \sum_{i=1}^{a(\chi_0)} \beta_i(\chi_0)^N.$$

It is worth noting for future use that the right hand sum is always nonnegative, since $\sum_{\deg Q^j = N} \deg Q = q^N$.

Combining these results with the orthogonality relations for characters, we deduce the following explicit formula for primes in residue classes modulo $\mathbf{R}_{l,M}$:

Lemma 1. *Let A be a polynomial prime to M. Then*

$$q^l \phi(M) \sum_{\substack{Q^j \equiv A \pmod{\mathbf{R}_{l,M}} \\ \deg Q^j = N}} \deg Q = q^N - \sum_{\chi} \bar{\chi}(A) \sum_{i=1}^{a(\chi)} \beta_i(\chi)^N,$$

where χ runs over all characters modulo $\mathbf{R}_{l,M}$. Here $a(\chi) \leq l + \deg M$ for all χ, and each $|\beta_i(\chi)| \leq q^{1/2}$.

3. Proof of Theorem 1

3.1. **A heuristic.** Let M be a polynomial of degree k over $\mathbf{F}_q$ and suppose $n > k$. Let $h(T)$ range over a set of representatives of the units modulo $\mathbf{R}_{n-1-k,M}$, and let N_h be the number of monic primes of degree n congruent to $h(T)$ modulo $\mathbf{R}_{n-1-k,M}$. (If we choose our representatives $h(T)$ from the set of monic, degree n polynomials, then N_h can be interpreted as the number of prime polynomials in the q-element set $\{h(T)+\alpha M\}$, where α ranges over $\mathbf{F}_q$.) Then $\sum_h N_h^2$ is precisely the number of monic prime pairs Q, Q' of degree n whose difference is an $\mathbf{F}_q$-multiple of M. If $Q'-Q$ is nonzero for such a pair, then necessarily $Q'-Q=\alpha M$ for some $\alpha \in \mathbf{F}_q^\times$. But then $\alpha^{-1}Q$ and $\alpha^{-1}Q'$ form a pair of primes differing by M. Thus, removing the pairs where $Q=Q'$, we find that

$$R(n;M,q) = \sum_h N_h^2 - \pi(n;q). \tag{7}$$

There are a total of $q^n\phi(M)/|M|$ monic, degree n polynomials which are prime to M, of which about q^n/n are irreducible. Thus, a random monic, degree n polynomial coprime to M is irreducible with probability about $n^{-1}|M|/\phi(M)$. Hence it is natural to guess that N_h is roughly $(q/n)|M|/\phi(M)$ for each h, and this leads us to expect that

$$\sum_h N_h^2 \approx (q/n)^2(|M|/\phi(M))^2 \#(\mathcal{M}/\mathbf{R}_{n-1-k,M})^\times$$
$$= \frac{q^2}{n^2}\frac{|M|^2}{\phi(M)^2} q^{n-1-k}\phi(M) = \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2}.$$

3.2. **Lower bound.** To obtain a lower bound it is not necessary to understand the numbers N_h individually. Since every monic prime of degree n belongs to some unit residue class modulo $\mathbf{R}_{n-1-k,M}$, we have $\sum_h N_h = \pi(n;q)$, so that by the Cauchy-Schwarz inequality and (4),

$$\sum_h 1^2 \sum_h N_h^2 \geq \left(\sum_h N_h\right)^2 \geq \frac{q^{2n}}{n^2} - 4\frac{q^{n(1+1/p)}}{n^2},$$

and so

$$\sum_h N_h^2 \geq \frac{1}{q^{n-1-k}\phi(M)}\left(\frac{q^{2n}}{n^2} - 4\frac{q^{n(1+1/p)}}{n^2}\right)$$
$$= \frac{|M|}{\phi(M)}\left(\frac{q^{n+1}}{n^2} - 4\frac{q^{n/p+1}}{n^2}\right).$$

The relation (7) now implies that

$$R(n;M,q) \geq \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} - 4\frac{|M|}{\phi(M)}\frac{q^{n/p+1}}{n^2} - \pi(n;q). \tag{8}$$

The upper estimate $\pi(n;q) \leq q^n/n$ completes the proof of the lower bound.

3.3. **Upper bound.** From Lemma 1, if h is a representative of a unit residue class modulo $\mathbf{R}_{n-1-k,M}$, then

$$q^{n-1-k}\phi(M)nN_h \le q^{n-1-k}\phi(M) \sum_{\substack{Q^j \equiv h \pmod{\mathbf{R}_{n-1-k,M}} \\ \deg Q^j = n}} \deg Q$$
$$= q^n - \sum_{\chi} \overline{\chi}(h) \sum_{i=1}^{a(\chi)} \beta_i(\chi)^n.$$

Now square both sides and sum over h:

$$n^2 q^{2(n-1-k)}\phi(M)^2 \sum_h N_h^2 \le \sum_h q^{2n} - 2q^n \sum_h \sum_{\chi} \overline{\chi}(h) \sum_{i=1}^{a(\chi)} \beta_i(\chi)^n$$
$$+ \sum_h \sum_{\chi,\chi'} \overline{\chi}(h)\overline{\chi}'(h) \sum_{\substack{1\le i\le a(\chi) \\ 1\le j\le a(\chi')}} \beta_i(\chi)^n \beta_j(\chi')^n.$$

Interchanging the sums over h with the sums over χ and χ', and using the orthogonality relations once again, we find that the right-hand side simplifies to

$$q^{n-1-k}\phi(M)q^{2n} - 2q^n q^{n-1-k}\phi(M) \sum_{i=1}^{a(\chi_0)} \beta_i(\chi_0)^n$$
$$+ \sum_h \sum_{\chi} \sum_{\substack{1\le i\le a(\chi) \\ 1\le j\le a(\chi^{-1})}} \beta_i(\chi)^n \beta_j(\chi^{-1})^n.$$

As noted above, the first sum appearing here is nonnegative, and so the entire term it belongs to is nonpositive and can therefore be ignored, since we are looking for an upper bound. Moreover, since $|\beta_i(\chi)|$ and $|\beta_j(\chi^{-1})|$ are bounded by $q^{1/2}$, and both $a(\chi)$ and $a(\chi^{-1})$ are bounded by $n-1$, the triple sum here is bounded in absolute value by

$$(q^{n-1-k}\phi(M))^2 (q^{n/2})^2 n^2 = q^{3n-2-2k}\phi(M)^2 n^2.$$

Thus

$$\sum_h N_h^2 \le \frac{q^{3n-1-k}\phi(M) + q^{3n-2-2k}\phi(M)^2 n^2}{n^2 q^{2n-2-2k}\phi(M)^2},$$

so that

$$R(n;M,q) = \sum_h N_h^2 - \pi(n;q)$$
$$\le \frac{|M|}{\phi(M)} \frac{q^{n+1}}{n^2} + q^n - \pi(n;q).$$

Inserting the lower estimate for $\pi(n;q)$ from (4) completes the proof of the upper bound.

Appendix: An upper bound for twin prime pairs in $\mathbf{F}_q[T]$

In this section we establish the following estimate:

Lemma 2. *Let $n \geq 2$ be an integer, and let $M \neq 0$ be a polynomial of degree $< n$ over the finite field $\mathbf{F}_q$. Then*

$$\#\{P : P, P+M \text{ are both monic irreducibles of degree } n\} \leq 8\frac{|M|}{\phi(M)}\frac{q^n}{n^2}.$$

As a corollary, we have

$$R(n; M, q) \leq 8\frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2}$$

whenever $0 \leq \deg M < n$.

The estimate of Lemma 2 is analogous to an explicit upper bound on generalized twin prime pairs obtained by Riesel and Vaughan ([12, Lemma 5]), but working in the polynomial setting enables us to give a much simpler proof. We begin with a statement of Selberg's upper-bound sieve for polynomials (cf. [13, Theorem 1]).

Lemma 3 (Selberg's Λ^2-sieve for $\mathbf{F}_q[T]$)**.** *Let $\mathcal{A}$ be a multiset of polynomials over $\mathbf{F}_q$, and let $\mathcal{Q}$ be a finite set of monic irreducibles over $\mathbf{F}_q$. Suppose that f is a multiplicative function defined on the squarefree divisors of $\prod_{Q\in\mathcal{Q}} Q$ with $1 < f(Q) \leq |Q|$ for each $Q \in \mathcal{Q}$, and write*

$$\sum_{\substack{A\in\mathcal{A}\\ D|A}} 1 = \frac{\#\mathcal{A}}{f(D)} + R_D. \tag{9}$$

Let $\mathcal{D}$ be any nonempty subset of the monic divisors of $\prod_{Q\in\mathcal{Q}} Q$ which is divisor closed (i.e., every monic divisor of an element of $\mathcal{D}$ belongs to $\mathcal{D}$). Then

$$\sum_{\substack{A\in\mathcal{A}\\ \gcd(A,\prod_{Q\in\mathcal{Q}} Q)=1}} 1 \leq \frac{\#\mathcal{A}}{\sum_{D\in\mathcal{D}} f(D)^{-1}\prod_{Q|D}\left(1-f(Q)^{-1}\right)^{-1}} + \sum_{D_1,D_2\in\mathcal{D}} |X_{D_1}X_{D_2}R_{[D_1,D_2]}|,$$

where

$$X_D = \mu(D)f(D)\frac{\sum_{C\in\mathcal{D},D|C} f(C)^{-1}\prod_{Q|C}\left(1-f(Q)^{-1}\right)^{-1}}{\sum_{C\in\mathcal{D}} f(C)^{-1}\prod_{Q|C}\left(1-f(Q)^{-1}\right)^{-1}}.$$

Before proceeding we introduce a bit more notation. Let A be a nonzero polynomial over $\mathbf{F}_q$. Then we can express A uniquely in the form

$$A = \varepsilon Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r},$$

where $\varepsilon \in \mathbf{F}_q^\times$ and the Q_i are distinct monic irreducibles. We define the arithmetic functions $\Omega(\cdot), d(\cdot)$, and $\mathrm{rad}(\cdot)$ in analogy with their integer counterparts by setting

$$\Omega(A) := \sum_{i=1}^r e_i, \quad d(A) := \prod_{i=1}^r (e_i+1), \quad \mathrm{rad}(A) := \prod_{i=1}^r Q_i.$$

Proof of Lemma 2. In the case when $q = 2$, we may assume that $T(T+1)$ divides M, since otherwise there are no prime pairs $P, P+M$ of degree n. Thus $|Q| > 2$ for every prime Q not dividing M. Define the multiset

$$\mathcal{A} := \{A(A+M) : A \text{ monic}, \deg A = n\}.$$

Let $\mathcal{Q}$ be the set of monic primes of degree $\leq n/2$. Then the number of monic, degree n prime pairs $P, P+M$ is precisely the number of elements of $\mathcal{A}$ coprime to $\prod_{Q\in\mathcal{Q}} Q$, a quantity which may be estimated with Lemma 3.

We take $\mathcal{D}$ to be the (divisor-closed) set of squarefree, monic polynomials of degree $\leq n/2$. Define the multiplicative function f appearing in Lemma 3 by setting (for monic primes Q)

$$f(Q) = \begin{cases} |Q|/2 & \text{if } Q \text{ does not divide } M, \\ |Q| & \text{if } Q \text{ divides } M \end{cases}$$

and extending f to be a completely multiplicative function on the monoid of monic polynomials. It is easy to check that if the squarefree polynomial D has degree $\leq n$, then (9) holds without any error term, i.e., with $R_D = 0$.

Since the least common multiple of any pair $D_1, D_2 \in \mathcal{D}$ has degree $\leq n$, we obtain from Lemma 3 the following clean inequality:

$$\sum_{\substack{A\in\mathcal{A} \\ \gcd(A, \prod_{Q\in\mathcal{Q}} Q)=1}} 1 \leq \frac{\#\mathcal{A}}{\sum_{D\in\mathcal{D}} f(D)^{-1} \prod_{Q|D} \left(1 - f(Q)^{-1}\right)^{-1}}. \tag{10}$$

To proceed we need a lower bound on the denominator in this expression. For each $D \in \mathcal{D}$, write $D = D_1 D_2$, where D_1 divides M and D_2 is prime to M. Then we have

$$f(D)^{-1} \prod_{Q|D} \left(1 - f(Q)^{-1}\right)^{-1} = \prod_{Q|D_1} \frac{1}{|Q|-1} \prod_{Q|D_2} \frac{2}{|Q|-2},$$

using $|Q| > 2$ for every Q dividing D_2. Thus we have reduced the problem to obtaining a lower bound on

$$\sum_{D\in\mathcal{D}} \prod_{Q|D_1} \frac{1}{|Q|-1} \prod_{Q|D_2} \frac{2}{|Q|-2}$$
$$= \sum_{D\in\mathcal{D}} \prod_{Q|D_1} \left(\frac{1}{|Q|} + \frac{1}{|Q|^2} + \frac{1}{|Q|^3} + \cdots\right) \prod_{Q|D_2} \left(\frac{2}{|Q|} + \frac{4}{|Q|^2} + \frac{8}{|Q|^3} + \cdots\right).$$

We may rewrite this expression as

$$\sum_{A \text{ monic}} \frac{2^{\Omega(A_2)}}{|A|} \sum_{\substack{D\in\mathcal{D} \\ \mathrm{rad}(A)=D}} 1,$$

where A_2 denotes that part of A supported on the primes not dividing M. The inner sum is at least 1 whenever $\deg A \leq n/2$, which yields a lower bound of

$$\sum_{\substack{A_2 \text{ monic} \\ \deg A_2 \leq n/2 \\ \gcd(A_2, M)=1}} \frac{2^{\Omega(A_2)}}{|A_2|} \sum_{\substack{A_1 \text{ monic} \\ \deg A_1 \leq n/2 - \deg A_2 \\ \mathrm{rad}(A_1)|M}} \frac{1}{|A_1|}. \tag{11}$$

Now $2^{\Omega(A_2)} \geq d(A_2)$, while for the inner sum we have

$$\begin{aligned}\sum_{\substack{A_1 \text{ monic} \\ \deg A_1 \leq n/2 - \deg A_2 \\ \operatorname{rad}(A_1)|M}} \frac{1}{|A_1|} &= \frac{\phi(M)}{|M|} \sum_{\substack{A_1 \text{ monic} \\ \deg A_1 \leq n/2 - \deg A_2 \\ \operatorname{rad}(A_1)|M}} \frac{1}{|A_1|} \prod_{Q|M} \left(1 - \frac{1}{|Q|}\right)^{-1} \\ &= \frac{\phi(M)}{|M|} \sum_{\substack{A_1 \text{ monic} \\ \deg A_1 \leq n/2 - \deg A_2 \\ \operatorname{rad}(A_1)|M}} \frac{1}{|A_1|} \sum_{\substack{B \text{ monic} \\ \operatorname{rad}(B)|M}} \frac{1}{|B|} \\ &\geq \frac{\phi(M)}{|M|} \sum_{\substack{C \text{ monic} \\ \deg C \leq n/2 - \deg A_2 \\ \operatorname{rad}(C)|M}} \frac{d(C)}{|C|}.\end{aligned}$$

Assembling these results, we find that (11) is bounded below by

$$\frac{\phi(M)}{|M|} \sum_{\substack{A \text{ monic} \\ \deg A \leq n/2}} \frac{d(A)}{|A|}.$$

By a result of Carlitz, we have $\sum_{\substack{A \text{ monic} \\ \deg A = k}} d(A) = (k+1)q^k$ (see [1]), and so our final sum is just

$$\sum_{0 \leq k \leq n/2} (k+1) \geq \frac{n^2}{8},$$

so that (11) is bounded below by $(\phi(M)/|M|)n^2/8$. Since the numerator in (10) is $\#\mathcal{A} = q^n$, we obtain the stated result. □

Remark. Let $\mathcal{I}_q(n)$ denote the set of monic irreducibles of degree n over $\mathbf{F}_q$. Then our argument shows that for any nonzero polynomial M (without any restriction on its degree) there are at most $8(|M|/\phi(M))q^n/n^2$ values of $P \in \mathcal{I}_q(n)$ for which $P + M$ is free of prime factors of degree $\leq n/2$. As a consequence, there are at most

$$8\frac{|M|}{\phi(M)}\frac{q^n}{n^2} + q^{\lfloor n/2 \rfloor + 1}$$

values of $P \in \mathcal{I}_q(n)$ for which $P + M$ is irreducible, where the $q^{\lfloor n/2 \rfloor + 1}$ term can be omitted unless M has degree n and leading coefficient -1. (The extra term is due to irreducible values of $P + M$ which are nevertheless removed in the sieve because $\deg(P + M) \leq n/2$.)

Acknowledgements

I would like to thank my advisor, Carl Pomerance, for helpful suggestions regarding both the content and presentation of this paper. I would also like to thank the referee for a careful reading of the manuscript.

References

1. L. Carlitz, *The arithmetic of polynomials in a Galois field*, Proc. Nat. Acad. Sci. U.S.A. **17** (1931), 120–122.
2. G. W. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field*, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1991. MR1143282 (92k:11103)

3. G. W. Effinger, K. Hicks, and G. L. Mullen, *Twin irreducible polynomials over finite fields*, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, pp. 94–111. MR1995330 (2004h:11104)
4. C. Hall, *L-functions of twisted Legendre curves*, J. Number Theory **119** (2006), no. 1, 128–147. MR2228953 (2007b:11091)
5. D. R. Hayes, *A polynomial analog of the Goldbach conjecture*, Bull. Amer. Math. Soc. **69** (1963), 115–116. MR0142540 (26:109)
6. ———, *Correction to "A polynomial analog of the Goldbach conjecture"*, Bull. Amer. Math. Soc. **69** (1963), 493. MR0150132 (27:135)
7. ———, *The distribution of irreducibles in* GF$[q, x]$, Trans. Amer. Math. Soc. **117** (1965), 101–127. MR0169838 (30:81)
8. P. Pollack, *An explicit approach to Hypothesis H for polynomials over a finite field*, Proceedings of the Anatomy of Integers Conference, Montréal, March 2006, to appear.
9. ———, *Simultaneous prime specializations of polynomials over finite fields*, Proc. London Math. Soc. (to appear, published electronically at `http://plms.oxfordjournals.org/`), 2008.
10. G. Rhin, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Dissertationes Math. (Rozprawy Mat.) **95** (1972), 75. MR0349612 (50:2105)
11. P. Ribenboim, *The new book of prime number records*, Springer-Verlag, New York, 1996. MR1377060 (96k:11112)
12. H. Riesel and R. C. Vaughan, *On sums of primes*, Ark. Mat. **21** (1983), no. 1, 46–74. MR706639 (84m:10042)
13. W. A. Webb, *Sieve methods for polynomial rings over finite fields*, J. Number Theory **16** (1983), no. 3, 343–355. MR0707607 (84j:12021)

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