Note on Hayes's paper "A polynomial analog of the Goldbach conjecture"

Paul Pollack [1]

Mathematics Department
Dartmouth College
Hanover, NH 03755

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 $< n$. When M has degree $n-1$, our theorem implies the general validity of a result claimed by Hayes in 1962, but proven only under additional hypotheses. When M has degree zero, our theorem refines a result of Effinger, Hicks & Mullen.

1 Introduction

Our main result is the following:

Theorem 1 *Let k, n be integers with $0 \le k < n$. Let M be a polynomial of degree k over $\mathbf{F}_q$. Then the number $R(M)$ of prime pairs $P, P+M$ over $\mathbf{F}_q$, as P ranges over all (not necessarily monic) degree n primes over $\mathbf{F}_q$, satisfies*

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

where the implied constants are absolute.

When $k = n-1$, the study of $R(M)$ was initiated by Hayes [3]. After proving that $R(M) > 0$ for $q > q_0(n)$ [3, Theorem 1], he stated an asymptotic formula [3, Theorem 2] for $R(M)$ slightly weaker than that contained in our theorem. Hayes later pointed out a gap in his argument (see [4]). However, he noted that slight modifications permit one to salvage the result if one assumes either

Email address: paul.pollack@dartmouth.edu (Paul Pollack).

[1] Supported by an NSF Graduate Research Fellowship.

that M is squarefree or that $n+1$ is prime to the characteristic of $\mathbf{F}_q$. Our theorem shows that no such additional assumptions are necessary.

In the case $k = 0$, Effinger, Hicks & Mullen [1] have shown that $R(M) > 0$ for $q > q_1(n)$. Our theorem shows that a formula comparable to that stated by Hayes is valid in this context as well.

To obtain the upper bound in Theorem 1, we follow closely the argument offered by Hayes in [3]. There Hayes obtains, in the case $k = n-1$, an asymptotic formula for a quantity related to $R(M)$, but including some additional terms (corresponding to the terms of Lemma 2 below with $j > 1$). Hayes's strategy for finding a lower bound on $R(M)$ is to show that the contribution from these extra terms is negligible. We take a different (and much simpler!) approach to the lower bound, applying an averaging argument to the well-known formula for the number of prime polynomials of a given degree.

Before proceeding we observe that the estimates of Theorem 1 are only nontrivial when q is large compared to n. In particular, this result does not imply the existence of infinitely many prime pairs $P, P+M$ over a fixed finite field $\mathbf{F}_q$. At present such an assertion is known only when M is a constant polynomial; see [6] for a discussion of this and related results.

Notation

We write $\pi(n; q)$ for the number of monic primes of degree n over $\mathbf{F}_q$; thus $\pi(n; q) = q^n/n + O(q^{n/2}/n)$. If M is a nonzero polynomial over $\mathbf{F}_q$, we write $|M|$ for the total number of elements of the ring $\mathbf{F}_q[T]/(M)$ and $\phi(M)$ for size of the corresponding unit group. All sums and products indexed by P are to be taken only over monic primes P.

2 An explicit formula for primes in certain residue classes

Let $\mathcal{P}$ be the (multiplicative) monoid of monic polynomials over $\mathbf{F}_q$. If $l \geq 0$ and $M \in \mathcal{P}$, we define a relation $\mathbf{R}_{l,M}$ on $\mathcal{P}$ 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 $\mathcal{P}$, i.e., an equivalence relation satsifying

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

Thus there is a well-defined quotient monoid $\mathcal{P}/\mathbf{R}_{l,M}$. It can be shown that an element of $\mathcal{P}$ is invertible modulo $\mathbf{R}_{l,M}$ if and only if it is coprime to M

and that the units group $(\mathcal{P}/\mathbf{R}_{l,M})^\times$ has size $q^l\phi(M)$ (cf. [5, Theorem 8.6]).

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

$$L(u,\chi) := \prod_P (1 - \chi(P)u^{\deg P})^{-1}. \tag{1}$$

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

$$L(u,\chi) = \prod_{i=1}^{a(\chi)} (1 - \beta_i(\chi)u), \tag{2}$$

where from Weil's Riemann Hypothesis we know that $|\beta_i(\chi)| \leq q^{1/2}$ for $1 \leq i \leq a(\chi)$. (Compare this with the proof of [2, Theorem 5.7] and the discussion in [7, Chapter 2].) From the Euler product representation (1), we deduce

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

while from (2), 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 deduce that

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

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

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

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

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

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 2 *Let A be a polynomial prime to M. Then*

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

Here $a(\chi)\le l+\deg M$ for all χ, and each $|\beta_i(\chi)|\le q^{1/2}$.

3 Proof of Theorem 1

3.1 Lower bound

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 $n+1$ congruent to $h(T)$ modulo $\mathbf{R}_{n-1-k,M}$. Since every prime of degree n belongs to some unit residue class modulo $\mathbf{R}_{n-1-k,M}$, we have

$$\sum_h N_h = \pi(n;q) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right),$$

so that by the Cauchy-Schwarz inequality,

$$\sum_h 1^2\sum_h N_h^2 \ge \left(\sum_h N_h\right)^2 = \frac{q^{2n}}{n^2} + O\left(\frac{q^{3n/2}}{n^2}\right),$$

and so

$$\begin{aligned}\sum_h N_h^2 &\ge \frac{1}{q^{n-1-k}\phi(M)}\frac{q^{2n}}{n^2} + O\left(\frac{q^{3n/2}}{q^{n-1-k}\phi(M)n^2}\right)\\ &= \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} + O\left(\frac{q^{n/2+k+1}}{\phi(M)n^2}\right).\end{aligned}$$

But $\sum_h N_h^2$ is precisely the number of monic prime pairs P,Q of degree n whose difference is a multiple of M having degree $\le k=\deg M$. If $Q-P$ is nonzero for such a pair, then necessarily $Q-P=\alpha M$ for some $\alpha\in\mathbf{F}_q^\times$. But then $\alpha^{-1}P$ and $\alpha^{-1}Q$ form a pair of primes differing by M. Thus, removing the pairs where $Q=P$, we find that

$$R(M) \ge \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} + O\left(\frac{1}{\phi(M)}\frac{q^{n/2+1+k}}{n^2}\right) + O\left(\frac{q^n}{n}\right). \tag{3}$$

So to prove the lower bound of the theorem we only have to show that the last O-term is dominant. For this we appeal to the following uniform lower bound on $\phi(M)$:

Lemma 3 *For every $\epsilon > 0$, there is a constant C depending only on ϵ (and not on q) for which*

$$\phi(M) \geq C|M|^{1-\epsilon}$$

for every nonzero polynomial M over $\mathbf{F}_q$.

PROOF. We have

$$\phi(M)/|M|^{1-\epsilon} = \prod_{P^k \| M} \frac{\phi(P^k)}{|P^k|^{1-\epsilon}} = \prod_{P^k \| M} \left(1 - \frac{1}{|P|}\right) |P|^{\epsilon k} \geq \prod_{|P^k| < 2^{1/\epsilon}} \left(\frac{1}{2}|P|^{\epsilon k}\right).$$

So it suffices to show that the final product is bounded away from zero, uniformly in q. But this is clear: the product is finite for each fixed q and empty once $q > 2^{1/\epsilon}$.

As a corollary, we have $\phi(M) \gg q^{(k+1)/2}$ for M of degree k. This is clear for $k = 1$ (as in this case $\phi(M) = q - 1 \geq q/2$), while for $n > 1$, Lemma 3 guarantees that $\phi(M) \gg |M|^{3/4} = q^{3k/4} \geq q^{(k+1)/2}$. Thus

$$\frac{1}{\phi(M)} \frac{q^{n/2+1+k}}{n^2} \ll \frac{q^{(k+1+n)/2}}{n^2} \ll \frac{q^n}{n^2},$$

implying that the first O-term in (3) may be omitted.

3.2 Upper bound

From Lemma 2, if h is a representative of a unit residue class modulo $\mathbf{R}_{n-1-k,M}$, then

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

Now square both sides and sum over h:

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

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

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

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

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

Hence

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

completing the proof of the upper bound (since $|M| = q^k$).

References

[1] G. Effinger, K. Hicks, and G. L. Mullen. Twin irreducible polynomials over finite fields. In *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, pages 94–111. Springer, Berlin, 2002.

[2] G. W. Effinger and D. R. Hayes. *Additive number theory of polynomials over a finite field*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1991. Oxford Science Publications.

[3] D. R. Hayes. A polynomial analog of the Goldbach conjecture. *Bull. Amer. Math. Soc.*, 69:115–116, 1963.

[4] D. R. Hayes. Correction to "A polynomial analog of the Goldbach conjecture". *Bull. Amer. Math. Soc.*, 69:493, 1963.

[5] D. R. Hayes. The distribution of irreducibles in GF[q, x]. *Trans. Amer. Math. Soc.*, 117:101–127, 1965.

[6] P. Pollack. An explicit approach to Hypothesis H for polynomials over a finite field. In *Proceedings of the Anatomy of Integers Conference, Montréal, March 2006*. To appear.

[7] G. Rhin. Répartition modulo 1 dans un corps de séries formelles sur un corps fini. *Dissertationes Math. (Rozprawy Mat.)*, 95:75, 1972.