International Journal of Number Theory

The exceptional set in the polynomial Goldbach problem

Paul Pollack
Mathematics Department, University of Illinois, 1409 West Green Street
Urbana, Illinois 61801, USA
pppollac@illinois.edu

Received (Day Month Year)
Accepted (Day Month Year)

Communicated by xxx

For each natural number N, let $R(N)$ denote the number of representations of N as a sum of two primes. Hardy and Littlewood proposed a plausible asymptotic formula for $R(2N)$ and showed, under the assumption of the Riemann Hypothesis for Dirichlet L-functions, that the formula holds "on average" in a certain sense. From this they deduced (under ERH) that all but $O_\epsilon(x^{1/2+\epsilon})$ of the even natural numbers in $[1, x]$ can be written as a sum of two primes. We generalize their results to the setting of polynomials over a finite field. Owing to Weil's Riemann Hypothesis, our results are unconditional.

Keywords: Goldbach conjecture, Hardy–Littlewood conjectures, polynomials over finite fields, exceptional set

Mathematics Subject Classification 2000: 11T55, 11P32

1. Introduction

For each natural number N, write $R(N)$ for the number of (ordered) representations of N as a sum of two primes. A famous conjecture of Goldbach asserts that $R(N) > 0$ for each even $N \geq 4$. The first substantial progress towards Goldbach's conjecture was made in the series of papers "Some problems of partitio numerorum" published in the early 1920s by Hardy and Littlewood. In part III of this series, one finds the prediction [8, Conjecture A] that as $N \to \infty$ through even values,

$$R(N) \sim \mathfrak{S}(N)\frac{N}{(\log N)^2}, \quad \text{where} \quad \mathfrak{S}(N) := 2\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{\substack{p\mid N\\ p>2}}\frac{p-1}{p-2}. \tag{1.1}$$

To this day, it remains a famous open problem to prove that this asymptotic formula holds for all N. However, in part V of the same series, Hardy & Littlewood proved that the Riemann Hypothesis for Dirichlet L-functions (ERH) implies that as $x \to \infty$,

$$\sum_{\substack{N \le x \\ N \text{ even}}} \left| R(N) - \mathfrak{S}(N) \frac{N}{(\log N)^2} \right|^2 \le x^{5/2+o(1)}. \tag{1.2}$$

(See [9, Theorem A].) It follows easily that (1.1) holds for almost all even N. Moreover, one can derive from (1.2) that there are $\le x^{1/2+o(1)}$ even values of $N \le x$ for which $R(N) = 0$ ([9, Theorem B]).

In this paper we use the circle method to study an analogue of the Goldbach problem for $\mathbf{F}_q[T]$, the ring of one-variable polynomials over the finite field with q elements. Let α and β be nonzero elements of $\mathbf{F}_q$, and let $\gamma := \alpha + \beta$. Let n be a positive integer. If $\gamma \ne 0$, we suppose that A is a univariate polynomial of degree n over $\mathbf{F}_q$ with leading coefficient γ; otherwise we suppose A is a nonzero polynomial of degree $< n$ over $\mathbf{F}_q$. We define $R(A) = R_{\alpha,\beta,n,\mathbf{F}_q}(A)$ by

$$R(A) := \sum_{\substack{P_1, P_2 \\ \alpha P_1 + \beta P_2 = A}} 1,$$

where the sum is over degree-n monic irreducibles P_1 and P_2 in $\mathbf{F}_q[T]$. Note when $\alpha + \beta = 0$, it is natural to view $R(A)$ as counting twin irreducible pairs $\{P_1, P_1 - \alpha^{-1}A\}$ (cf. [12]).

What is the right analogue of (1.1)? If we recall that a polynomial of degree n over $\mathbf{F}_q$ is irreducible with probability roughly $1/n$, then standard probabilistic arguments (cf. [5, §1.2.3]) suggest that $R(A) \approx \mathfrak{S}(A) q^n / n^2$, where now

$$\mathfrak{S}(A) := \prod_{P \mid A} \left(1 + \frac{1}{|P| - 1}\right) \prod_{P \nmid A} \left(1 - \frac{1}{(|P| - 1)^2}\right),$$

with both products extended over monic irreducibles P. In order to make this prediction more precise, we introduce the notion of an *even polynomial.* Define the *norm* of a nonzero polynomial $M \in \mathbf{F}_q[T]$ as $|M| = q^{\deg M}$, so that $|M| = \#\mathbf{F}_q[T]/(M)$. We say that M is *even* if M is divisible by every irreducible of norm 2. If $q > 2$, then every element of $\mathbf{F}_q[T]$ is even, while when $q = 2$, the polynomial M is even precisely when it is divisible by $T(T+1)$. As in the classical setting, it is easy to verify that if A is not even, then $R(A) = O(1)$; also in this case, $\mathfrak{S}(A) = 0$. So let us assume that A is even. Then we conjecture that whenever $q^n \to \infty$,

$$R(A) \sim \mathfrak{S}(A) \frac{q^n}{n^2}. \tag{1.3}$$

Note that this is a *uniform* conjecture, in the sense that we do not assume that any of the parameters q, n, α, β or A is fixed.

Our attack on this conjecture goes via the circle method, as developed in the polynomial setting by Hayes [10]. In this paper, Hayes proves a three-irreducible analogue of our conjecture (1.3), following the approach of [8]. Whereas Hardy & Littlewood needed an unproved hypothesis on the zeros of L-functions in their work, Hayes's results and ours are unconditional, owing to Weil's proof of the geometric Riemann Hypothesis.

Our principal result is an analogue of (1.2):

Theorem 1.1. *Let α and β be nonzero elements of $\mathbf{F}_q$, and let $R(A)$ be defined as above. Then*

$$\sum_{A}{}' \left| R(A) - \mathfrak{S}(A)\frac{q^n}{n^2} \right|^2 \ll q^{(5n+1)/2} n^{-1}. \tag{1.4}$$

Here the $'$ indicates that the sum is taken over degree-n polynomials with leading coefficient γ in the case $\gamma \neq 0$, and over all nonzero polynomials of degree $< n$ when $\gamma = 0$. The implied constant is absolute.

From this, it is a simple matter (see §4) to deduce the following estimate for the size of the exceptional set in Goldbach's problem:

Theorem 1.2. *Let α and β be nonzero elements of $\mathbf{F}_q$, and let $\gamma := \alpha + \beta$. Suppose first that $\gamma \neq 0$. Then the number of even polynomials of degree n and leading coefficient γ that cannot be written in the form $\alpha P_1 + \beta P_2$ for degree-n monic irreducible polynomials P_1, P_2 is*

$$\ll q^{(n+1)/2} n^3.$$

If $\gamma = 0$, then the same bound holds for the number of even polynomials of degree $< n$ that cannot be represented in this form. Here the implied constant is absolute.

The bound of Theorem 1.2 is a bit more explicit than the $x^{1/2+o(1)}$ bound of Hardy and Littlewood quoted above. It may be compared with the result of Goldston (see [7, bottom of p. 122]) that on ERH, the number $E(x)$ of even $N \leq x$ lacking a representation as a sum of two primes is $\ll x^{1/2}(\log x)^4$.

The author has proposed a different attack on (1.3) in [13, Chapter 7]. That approach, which rests an explicit version of the Chebotarev density theorem for function fields, shows that (1.3) holds if q tends to infinity much faster than n and satisfies $\gcd(q, 2n) = 1$. One consequence is that for an appropriate constant C, the exceptional set considered in Theorem 1.2 is empty if $\gcd(q, 2n) = 1$ and $q > Cn!^4 n^2$. We do not go into details here; related results will appear in joint work of the author with Andreas Bender [3]. See also [1], [2].

We conclude this introduction by remarking that since the era of Hardy and Littlewood, there has been substantial progress towards estimating $E(x)$ unconditionally. In the late '30s, Chudakov [4], van der Corput [14], and Estermann [6] independently adapted methods of Vinogradov to show that $E(x) \ll_A x/(\log x)^A$ for each positive A. The current record is due to Pintz (see [11]), who has shown that $E(x) \ll x^{\theta}$ for a certain $\theta < 2/3$.

2. Preliminaries

2.1. *Notation and conventions*

We recall briefly the set-up of Hayes [10]. We write $\mathbf{F}_q(T)_\infty$ for the completion of $\mathbf{F}_q(T)$ at the prime associated to the $(1/T)$-adic valuation, which we identify with the field of finite-tailed Laurent series in $1/T$:

$$\mathbf{F}_q(T)_\infty = \mathbf{F}_q((1/T)) = \left\{ \sum_{i=-\infty}^{n} a_i T^i : a_i \in \mathbf{F}_q, n \in \mathbf{Z} \right\}.$$

We let $|\cdot|$ denote the induced absolute value on $\mathbf{F}_q(T)_\infty$, so that

$$\left| \sum_{i=-\infty}^{n} a_i T^i \right| = q^n \quad \text{if } a_n \neq 0.$$

(Note that this agrees with the previous definition of $|M|$ for $M \in \mathbf{F}_q[T]$.) The *unit interval* $\mathcal{U}$ is defined as

$$\mathcal{U} := \left\{ \sum_{i<0} a_i T^i : a_i \in \mathbf{F}_q \right\}.$$

Then $\mathcal{U}$ is a compact abelian group; we use ν to denote the Haar measure on $\mathcal{U}$, normalized so that $\nu(\mathcal{U}) = 1$. For notational simplicity, we always abbreviate $\int f(\theta)\, d\nu(\theta)$ to $\int f(\theta)\, d\theta$.

For $\theta \in \mathcal{U}$ and integers $r \geq 1$, we define

$$B(\theta, r) = \{\eta \in \mathcal{U} : |\eta - \theta| < q^{-r}\}.$$

Then the ν-measure of $B(\theta, r)$ is q^{-r} (see [10, Corollary 3.2]).

We write $e\colon \mathbf{F}_q(T)_\infty \to S^1$ for the map defined by

$$e\left(\sum_{i=-\infty}^{n} a_i T^i \right) = \exp\left(\frac{2\pi i}{p} \mathrm{Tr}(a_{-1}) \right),$$

where the trace is from $\mathbf{F}_q$ to its prime field $\mathbf{F}_p$.

2.2. *Two lemmas on arithmetic functions*

A complex-valued function f, defined on the multiplicative semigroup $\mathcal{M}$ of monic polynomials over $\mathbf{F}_q$, is said to be *multiplicative* if $f(AB) = f(A)f(B)$ whenever A and B are relatively prime. Two examples of multiplicative functions which appear repeatedly are the analogues of the Euler totient function and the Möbius function: Here $\phi(M) = \#(\mathbf{F}_q[T]/(M))^\times$, and

$$\mu(M) = \begin{cases} 0 & \text{if } P^2 \mid M \text{ for some irreducible } P, \\ (-1)^k & \text{if } M \text{ is the product of } k \text{ distinct monic irreducibles.} \end{cases}$$

The following crude lemma is often useful:

Lemma 2.1. *If G is a nonnegative multiplicative function, then*

$$\sum_{\substack{\deg A \le d \\ A \text{ monic}}} G(A) \ll q^d \prod_{\deg P \le d} \left(1 + \frac{|G(P) - 1|}{|P|} + \frac{|G(P^2) - G(P)|}{|P|^2} + \dots\right),$$

where the implied constant is absolute.

Proof. Define $g\colon \mathcal{M} \to \mathbf{C}$ so that

$$G(A) = \sum_{\substack{D|A \\ D \text{ monic}}} g(D).$$

By Möbius inversion, $g(A) = \sum_{D|A, D \text{ monic}} G(D)\mu(A/D)$. Since g is multiplicative and $g(P^k) = G(P^k) - G(P^{k-1})$, we have that

$$\begin{aligned}\sum_{\substack{\deg A \le d \\ A \text{ monic}}} G(A) &= \sum_{\substack{\deg A \le d \\ A \text{ monic}}} \sum_{\substack{D|A \\ D \text{ monic}}} g(D) \le (q^d + q^{d-1} + \dots + q^{\deg D}) \sum_{\substack{\deg D \le d \\ D \text{ monic}}} \frac{|g(D)|}{|D|} \\ &\le 2q^d \prod_{\deg P \le d} \left(1 + \frac{|G(P) - 1|}{|P|} + \frac{|G(P^2) - G(P)|}{|P|^2} + \dots\right). \qquad \square\end{aligned}$$

Lemma 2.2. *For every real $i \ge 1$, we have*

$$\sum_{\substack{\deg A = d \\ A \text{ monic}}} \frac{1}{\phi(A)^i} = O(q^{(1-i)d}),$$

where the implied constant depends only on i.

Proof. Define a multiplicative function G on $\mathcal{M}$ by setting

$$G(A) := \left(\frac{|A|}{\phi(A)}\right)^i = \prod_{P|A} \left(1 - \frac{1}{|P|}\right)^{-i}.$$

Since $|A| = q^d$ when $\deg A = d$, to prove the lemma it is enough to show that

$$\sum_{\substack{\deg A = d \\ A \text{ monic}}} G(A) = O(q^d). \tag{2.1}$$

For each monic irreducible P we have $|G(P) - 1| \ll_i 1/|P|$. Moreover, since $G(A)$ depends only on the irreducibles dividing A, every difference $G(P^k) - G(P^{k-1})$ with $k > 1$ vanishes. By Lemma 2.1,

$$\sum_{\substack{\deg A = d \\ A \text{ monic}}} G(A) \ll q^d \prod_{\deg P \le d} \left(1 + O\left(\frac{1}{|P|^2}\right)\right) \le q^d \exp\left(O\left(\sum_P \frac{1}{|P|^2}\right)\right).$$

Now (2.1) follows since $\sum |P|^{-2} \le \sum_{M \in \mathcal{M}} |M|^{-2} = \sum_n q^{-n} \le 2$. $\square$

2.3. *The fundamental approximation*

Let n be a positive integer. To study additive problems concerning degree-n irreducibles, one is led to investigate the behavior of the function $f\colon \mathcal{U} \to \mathbf{C}$ defined by

$$f(\theta) := \sum_{\deg P = n} e(P\theta),$$

where the sum is over monic irreducibles of degree n. We introduce the decomposition

$$\mathcal{U} = \bigcup_{\substack{\deg H \le n/2 \\ H \text{ monic}}} \bigcup_{\substack{\deg G < \deg H \\ \gcd(G,H)=1}} \mathcal{I}_{G/H},$$

$$\text{where} \quad \mathcal{I}_{G/H} = \left\{ \eta \in \mathcal{U} : |\eta - G/H| < \frac{1}{q^{\deg H} q^{\lfloor n/2 \rfloor}} \right\}.$$

(Thus $\mathcal{I}_{G/H} = B(G/H, \lfloor n/2 \rfloor + \deg H)$.) The sets $\mathcal{I}_{G/H}$, with G and H as above, form a disjoint open cover of $\mathcal{U}$ ([10, Theorem 4.3]). We define $\mathcal{U}_1$ (the 'major arcs') as the union of those intervals $\mathcal{I}_{G/H}$ with $\deg H \le n/4$, and we take $\mathcal{U}_2 := \mathcal{U} \setminus \mathcal{U}_1$ (the 'minor arcs').

The function f can be well-approximated on each $I_{G/H}$ by a simpler function g. For $\theta \in \mathcal{I}_{G/H}$, set

$$g(\theta) := \begin{cases} \frac{\mu(H)}{\phi(H)} \frac{q^n}{n} e\left(T^n(\theta - G/H)\right) & \text{if } |\theta - G/H| < 1/q^n, \\ 0 & \text{otherwise.} \end{cases}$$

The following fundamental estimate is proved by Hayes as a consequence of Weil's Riemann Hypothesis (see [10, Theorem 5.3 and Lemma 7.1]):

Lemma 2.3. *For all $\theta \in \mathcal{U}$, we have $|f(\theta) - g(\theta)| < 2q^{(3n+1)/4}$.*

3. Proof of Theorem 1.1

For distinct polynomials A, the functions $e(A\theta)$ define orthonormal elements of $L^2(\mathcal{U})$ (see [10, Theorem 3.5]). Thus

$$\int_{\mathcal{U}} f(\alpha\theta) f(\beta\theta) e(-A\theta)\, d\theta = \sum_{P_1, P_2} \int_{\mathcal{U}} e((\alpha P_1 + \beta P_2)\theta) e(-A\theta)\, d\theta = R(A).$$

We decompose $R(A) = R_1(A) + R_2(A)$, where in R_1 the integration is taken over $\mathcal{U}_1$ and in R_2 the integration is taken over $\mathcal{U}_2$. Then

$$\sum_A{}' \left| R(A) - \mathfrak{S}(A) \frac{q^n}{n^2} \right|^2 \ll \sum_A{}' |R_2(A)|^2 + \sum_A{}' \left| R_1(A) - \mathfrak{S}(A) \frac{q^n}{n^2} \right|^2. \tag{3.1}$$

Lemma 3.1. *We have*

$$\int_{\mathcal{U}} |f(\theta)|^2\, d\theta \le q^n/n \quad \textit{and} \quad \int_{\mathcal{U}} |g(\theta)|^2\, d\theta \ll q^n/n.$$

Proof. The first estimate is almost immediate. Writing $\pi(q;n)$ for the number of monic irreducible polynomials of degree n over $\mathbf{F}_q$, we have by a well-known theorem of Gauss that $\pi(q;n) \le q^n/n$. Thus

$$\int_{\mathcal{U}} |f(\theta)|^2 \, d\theta = \sum_{P_1, P_2} \int_{\mathcal{U}} e(\theta(P_1 - P_2)) \, d\theta = \sum_{P_1} 1 = \pi(q;n) \le \frac{q^n}{n}.$$

To handle the second estimate, observe that

$$\begin{aligned}\int_{\mathcal{U}} |g(\theta)|^2 \, d\theta &= \sum_{\substack{\deg H \le n/2 \\ H \text{ monic}}} \sum_{\substack{\deg G < \deg H \\ (G,H)=1}} \int_{B(G/H,n)} \left(\frac{\mu(H)}{\phi(H)}\right)^2 \frac{q^{2n}}{n^2} \, d\theta \\ &\le \frac{q^n}{n^2} \sum_{\substack{\deg H \le n/2 \\ H \text{ monic}}} \left(\frac{\mu(H)}{\phi(H)}\right)^2 \sum_{\substack{\deg G < \deg H \\ (G,H)=1}} 1 = \frac{q^n}{n^2} \sum_{\substack{\deg H \le n/2 \\ H \text{ monic, squarefree}}} \frac{1}{\phi(H)}\end{aligned}$$

and that the final sum here is $\ll n$ by Lemma 2.2. □

Now recall the following elementary result from linear algebra:

Lemma 3.2 (Bessel's inequality). *Let $e_1, \ldots, e_n$ be a finite collection of orthonormal vectors in a complex inner product space V. Then for any $x \in V$,*

$$\sum_{k=1}^{n} |\langle x, e_k \rangle|^2 \le \|x\|^2.$$

Lemma 3.3. *We have*

$$\sum_{A}{}' |R_2(A)|^2 \ll q^{(5n+1)/2} n^{-1}.$$

Proof. We view $R_2(A)$ as the A-th Fourier coefficient of the function $f(\alpha\theta)f(\beta\theta)\mathbf{1}_{\mathcal{U}_2}$, where $\mathbf{1}_{\mathcal{U}_2}$ is the indicator function of the set $\mathcal{U}_2$. So by Bessel's inequality, with the functions $e(A\theta)$ playing the role of the e_i, we see that

$$\sum_{A}{}' |R_2(A)|^2 \le \int_{\mathcal{U}_2} |f(\alpha\theta)f(\beta\theta)|^2 \, d\theta,$$

which, by the Schwarz inequality, is bounded by

$$\left(\int_{\mathcal{U}_2} |f(\alpha\theta)|^4 \, d\theta\right)^{1/2} \left(\int_{\mathcal{U}_2} |f(\beta\theta)|^4 \, d\theta\right)^{1/2}.$$

Since multiplication by elements of $\mathbf{F}_q^{\times}$ preserves the ν-measure of Borel subsets of $\mathcal{U}$, both of the above integrals coincide with $\int_{\mathcal{U}_2} |f(\theta)|^4 \, d\theta$. Now

$$\int_{\mathcal{U}_2} |f(\theta)|^4 \, d\theta \ll \int_{\mathcal{U}_2} |g(\theta)|^4 \, d\theta + \int_{\mathcal{U}_2} |f(\theta) - g(\theta)|^4 \, d\theta.$$

By Lemmas 2.3 and 3.1,

$$\int_{\mathcal{U}_2} |f(\theta)-g(\theta)|^4\,d\theta \ll \sup|f(\theta)-g(\theta)|^2 \int_{\mathcal{U}_2} (|f(\theta)|^2+|g(\theta)|^2)\,d\theta$$
$$\ll q^{(3n+1)/2}\,(q^n/n+q^n/n) \ll q^{(5n+1)/2} n^{-1}.$$

By Lemma 2.2,

$$\int_{\mathcal{U}_2} |g(\theta)|^4\,d\theta = \frac{q^{4n}}{n^4} \sum_{\substack{n/4<\deg H\leq n/2\\ H \text{ monic}}} \left(\frac{\mu(H)}{\phi(H)}\right)^4 \sum_{\substack{\deg G<\deg H\\ (G,H)=1}} \int_{B(G/H,n)} 1\,d\theta$$
$$= \frac{q^{3n}}{n^4} \sum_{\substack{n/4<\deg H\leq n/2\\ H \text{ monic, squarefree}}} \frac{1}{\phi(H)^3} \ll \frac{q^{3n}}{n^4} \sum_{n/4<r\leq n/2} \frac{1}{q^{2r}} \ll \frac{q^{5n/2}}{n^4}.$$

Lemma 3.3 follows upon collecting the estimates. □

For H a monic polynomial over $\mathbf{F}_q$ and A any element of $\mathbf{F}_q[T]$, define $c_H(A)$ by

$$c_H(A) := \sum_{\substack{G \bmod H\\ (G,H)=1}} e(AG/H).$$

(Here G runs over a reduced residue system modulo H, which will usually be chosen as the set of polynomials of degree $< \deg H$ and coprime to H.) Then $c_H(A)$ is a polynomial analogue of the usual Ramanujan sum. It is multiplicative in H for fixed A and satisfies

$$c_H(A) = \frac{\phi(H)\mu(H/(H,A))}{\phi(H/(H,A))}. \tag{3.2}$$

(Compare [10, Theorem 6.1].)

Lemma 3.4. *We have*

$$R_1(A) = \mathfrak{S}'(A)\frac{q^n}{n^2} + E(A),$$

where

$$\mathfrak{S}'(A) := \sum_{\substack{\deg H\leq n/4\\ H \text{ monic}}} \left(\frac{\mu(H)}{\phi(H)}\right)^2 c_H(A)$$

and

$$E(A) := \int_{\mathcal{U}_1} (f(\alpha\theta)f(\beta\theta)-g(\alpha\theta)g(\beta\theta))e(-A\theta)\,d\theta.$$

Proof. We have

$$R_1(A) = \int_{\mathcal{U}_1} g(\alpha\theta)g(\beta\theta)e(-A\theta)\,d\theta + \int_{\mathcal{U}_1} (f(\alpha\theta)f(\beta\theta)-g(\alpha\theta)g(\beta\theta))e(-A\theta)\,d\theta$$
$$= \int_{\mathcal{U}_1} g(\alpha\theta)g(\beta\theta)e(-A\theta)\,d\theta + E(A),$$

and we need to show that the remaining integral is $\mathfrak{S}'(A)q^n/n^2$. Inserting the definition of g, we can rewrite this integral as

$$\frac{q^{2n}}{n^2} \sum_{\substack{\deg H \le n/4 \\ H \text{ monic}}} \left(\frac{\mu(H)}{\phi(H)}\right)^2 \sum_{\substack{\deg G < \deg H \\ (G,H)=1}} \int_{B(G/H,n)} e((\alpha+\beta)T^n(\theta - G/H))e(-A\theta)\, d\theta.$$

Write $e(-A\theta) = e(-AG/H)e(-A(\theta - G/H))$ and make the change of variables $\theta \mapsto \theta + G/H$, so that the integration takes place over $B(0,n)$. This transforms the expression into

$$\frac{q^{2n}}{n^2} \sum_{\substack{\deg H \le n/4 \\ H \text{ monic}}} \left(\frac{\mu(H)}{\phi(H)}\right)^2 \sum_{\substack{\deg G < \deg H \\ (G,H)=1}} e(-AG/H) \int_{B(0,n)} e(((\alpha+\beta)T^n - A)\theta)\, d\theta.$$

By the choice of A, the polynomial $(\alpha+\beta)T^n - A$ has degree $< n$; it follows that

$$|((\alpha+\beta)T^n - A)\theta| < q^{-1} \quad \text{for each } \theta \in B(0,n).$$

Recalling the definition of $e(\cdot)$, we see that the integrand here is identically 1. Since the measure of $B(0,n)$ is q^{-n}, the above simplifies to

$$\frac{q^n}{n^2} \sum_{\substack{\deg H \le n/4 \\ H \text{ monic}}} \left(\frac{\mu(H)}{\phi(H)}\right)^2 \sum_{\substack{\deg G < \deg H \\ (G,H)=1}} e(-AG/H).$$

But the rightmost sum here is precisely $c_H(-A) = c_H(A)$. □

Lemma 3.5. *We have*

$$\sum_A{}' |\mathfrak{S}(A) - \mathfrak{S}'(A)|^2 \ll q^{n/2}n^3.$$

Proof. Since $c_H(A)$ is multiplicative in H, we have

$$\sum_{H \text{ monic}} \left(\frac{\mu(H)}{\phi(H)}\right)^2 c_H(A) = \prod_P \left(1 + \frac{1}{(|P|-1)^2} c_P(A)\right) = \mathfrak{S}(A).$$

(The factorization here is justified by the absolute convergence of the left-hand sum, which follows from (3.2).) Hence

$$\begin{aligned}
|\mathfrak{S}(A) - \mathfrak{S}'(A)| &= \sum_{\substack{\deg H > n/4 \\ H \text{ monic}}} \left(\frac{\mu(H)}{\phi(H)}\right)^2 \frac{\phi(H)\mu(H/(H,A))}{\phi(H/(H,A))} \\
&= \sum_{\substack{D|A \\ D \text{ squarefree, monic}}} \sum_{\substack{\deg H > n/4 \\ H \text{ monic} \\ D|H,\ (H/D,A)=1}} \frac{\mu(H)^2}{\phi(H)} \frac{\mu(H/D)}{\phi(H/D)} \\
&= \sum_{\substack{D|A \\ D \text{ monic, squarefree}}} \frac{1}{\phi(D)} \sum_{\substack{\deg E > n/4 - \deg D \\ E \text{ monic},\ (E,A)=1}} \frac{\mu(E)}{\phi(E)^2}.
\end{aligned}$$

Appealing to Lemma 2.2, this last double sum is

$$\ll q^{-n/4} \sum_{\substack{D\mid A\\ D \text{ monic, squarefree}}} \frac{|D|}{\phi(D)}.$$

Thus

$$|\mathfrak{S}(A)-\mathfrak{S}'(A)|^2 \ll q^{-n/2}K(A), \quad \text{where} \quad K(A) := \left(\sum_{\substack{D\mid A\\ D \text{ monic, squarefree}}} \frac{|D|}{\phi(D)}\right)^2.$$

Applying Lemma 2.1,

$$\sideset{}{'}\sum_{A} K(A) \leq q^n \prod_{\deg P\leq n}\left(1+\frac{|K(P)-1|}{|P|}\right). \tag{3.3}$$

Now

$$\frac{K(P)-1}{|P|} = \frac{2}{|P|-1} + \frac{|P|}{(|P|-1)^2} = \frac{3}{|P|} + O\left(\frac{1}{|P|^2}\right),$$

and so the product on the right-hand side of (3.3) is

$$\leq \exp\left(\sum_{\deg P\leq n}\frac{3}{|P|}+O(1)\right) \ll \exp\left(\sum_{r\leq n}\frac{3}{q^r}\frac{q^r}{r}\right) = \exp(3\log n + O(1)) \ll n^3.$$

Piecing everything together,

$$\sideset{}{'}\sum_{A} |\mathfrak{S}(A)-\mathfrak{S}'(A)|^2 \ll q^{-n/2}q^n n^3 = q^{n/2}n^3,$$

as desired. □

Lemma 3.6. *We have*

$$\sideset{}{'}\sum_{A} |E(A)|^2 \ll q^{(5n+1)/2}n^{-1}.$$

Proof. By another application of Bessel's inequality,

$$\sideset{}{'}\sum_{A} |E(A)|^2 \leq \int_{\mathcal{U}_1} |f(\alpha\theta)f(\beta\theta)-g(\alpha\theta)g(\beta\theta)|^2\, d\theta.$$

Since

$$|f(\alpha\theta)f(\beta\theta)-g(\alpha\theta)g(\beta\theta)|^2 \ll |f(\alpha\theta)-g(\alpha\theta)|^2|f(\beta\theta)|^2 + |f(\beta\theta)-g(\beta\theta)|^2|g(\alpha\theta)|^2,$$

we have by Lemmas 2.3 and 3.1,

$$\begin{aligned}\int_{\mathcal{U}_1} |f(\alpha\theta)f(\beta\theta)-g(\alpha\theta)g(\beta\theta)|^2 &\ll \sup|f-g|^2\left(\int_{\mathcal{U}}|f(\beta\theta)|^2+\int_{\mathcal{U}}|g(\alpha\theta)|^2\right)\\ &\ll q^{(3n+1)/2}\left(\int_{\mathcal{U}}|f(\theta)|^2+\int_{\mathcal{U}}|g(\theta)|^2\right) \ll q^{(3n+1)/2}q^n n^{-1} = q^{(5n+1)/2}n^{-1},\end{aligned}$$

as desired. □

Lemma 3.7. *We have*

$$\sum_{A}{}' |R_1(A) - \mathfrak{S}(A)q^n/n^2|^2 \ll q^{(5n+1)/2}n^{-1}.$$

Proof. Observe that the sum to be estimated is

$$\ll \sum_{A}{}' \left|R_1(A) - \mathfrak{S}'(A)\frac{q^n}{n^2}\right|^2 + \sum_{A}{}' \left|\mathfrak{S}'(A)\frac{q^n}{n^2} - \mathfrak{S}(A)\frac{q^n}{n^2}\right|^2$$

$$= \sum_{A}{}' |E(A)|^2 + \frac{q^{2n}}{n^4}\sum_{A}{}' |\mathfrak{S}(A) - \mathfrak{S}'(A)|^2.$$

By Lemmas 3.5 and 3.6, this is

$$\ll q^{(5n+1)/2}n^{-1} + \frac{q^{2n}}{n^4}q^{n/2}n^3 \ll q^{(5n+1)/2}n^{-1},$$

as claimed. □

Theorem 1.1 follows immediately upon combining (3.1) with the results of Lemmas 3.3 and 3.7.

4. Proof of Theorem 1.2

Lemma 4.1. *If A is even, then $\mathfrak{S}(A) \gg 1$, where the implied constant is absolute.*

Proof. Since A is even,

$$\mathfrak{S}(A) \geq \prod_{P \nmid A} \left(1 - (|P|-1)^{-2}\right) \geq \prod_{|P|>2} \left(1 - (|P|-1)^{-2}\right).$$

As

$$\sum_{P} \frac{1}{(|P|-1)^2} \leq \sum_{P} \frac{4}{|P|^2} \leq \sum_{d\geq 1} \frac{4}{q^{2d}}\frac{q^d}{d} < 4\sum_{d\geq 1}\frac{1}{q^d} = \frac{4}{q-1}, \qquad (4.1)$$

it follows that $\mathfrak{S}(A)$ is bounded below by a positive constant $\mathfrak{S}_q$ (say) depending only on q. Moreover, for $q \geq 9$,

$$\mathfrak{S}(A) \geq \prod_{|P|>2}\left(1 - \frac{1}{(|P|-1)^2}\right) \geq 1 - \sum_{P}\frac{1}{(|P|-1)^2} \geq 1 - \frac{4}{q-1} \geq \frac{1}{2}. \qquad (4.2)$$

Since $\mathfrak{S}_q > 0$ for each of the finitely many $q < 9$, the lemma follows. □

Suppose now that A is exceptional, so that A is included in the sum (1.4) but $R(A) = 0$. Then A contributes $\mathfrak{S}(A)^2q^{2n}/n^4 \gg q^{2n}/n^4$ to (1.4). So the number of such A must be

$$\ll \frac{q^{(5n+1)/2}n^{-1}}{q^{2n}/n^4} = q^{(n+1)/2}n^3,$$

which is the assertion of Theorem 1.2.

Acknowledgements

The author is supported by an NSF postdoctoral research fellowship. This work is adapted from the author's Ph.D. thesis at Dartmouth College [13]. He thanks his advisor, Carl Pomerance, for generosity with both time and ideas. He also thanks the referee for a careful reading of the manuscript.

References

[1] A. O. Bender, *Decompositions into sums of two irreducibles in* $\mathbf{F}_q[t]$, C. R. Math. Acad. Sci. Paris **346** (2008), no. 17-18, 931–934.
[2] ———, *Representing an element in* $\mathbf{F}_q[t]$ *as the sum of two irreducibles in* $\mathbf{F}_{q^s}[t]$, submitted, arXiv:0809.4381v1 [math.NT], 2008.
[3] A. O. Bender and P. Pollack, *On quantitative analogues of the Goldbach and twin prime conjectures over* $\mathbf{F}_q[t]$, submitted.
[4] N. G. Chudakov, *On the density of the set of even numbers which are not representable as a sum of two primes*, Izv. Akad. Nauk. SSSR **2** (1938), 25–40.
[5] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, second ed., Springer, New York, 2005.
[6] T. Estermann, *On Goldbach's problem: Proof that almost all even positive integers are sums of two primes*, Proc. London Math. Soc. **44** (1938), 307–314.
[7] D. A. Goldston, *On Hardy and Littlewood's contribution to the Goldbach conjecture*, Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989) (Salerno), Univ. Salerno, 1992, pp. 115–155.
[8] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), no. 1, 1–70.
[9] ———, *Some problems of 'Partitio numerorum'; V: A further contribution to the study of Goldbach's problem*, Proc. London Math. Soc. **22** (1923), 46–56.
[10] D. R. Hayes, *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. **11** (1966), 461–488.
[11] J. Pintz, *Landau's problems on primes*, J. Théor. Nombres Bordeaux **21** (2009), no. 2, 357–404.
[12] P. Pollack, *A polynomial analogue of the twin prime conjecture*, Proc. Amer. Math. Soc. **136** (2008), no. 11, 3775–3784.
[13] ———, *Prime polynomials over finite fields*, Ph.D. thesis, Dartmouth College, 2008.
[14] J. G. van der Corput, *Sur l'hypothése de Goldbach pour presque tous les nombres pairs*, Acta Arith **2** (1937), 266–290.