MATHEMATICS OF COMPUTATION
Volume 89, Number 321, January 2020, Pages 493–514
https://doi.org/10.1090/mcom/3452
Article electronically published on May 24, 2019

AVERAGE LIAR COUNT FOR DEGREE-2 FROBENIUS PSEUDOPRIMES

ANDREW FIORI AND ANDREW SHALLUE

ABSTRACT. In this paper we obtain lower and upper bounds on the average number of liars for the Quadratic Frobenius Pseudoprime Test of Grantham [Math. Comp. 70 (2001), pp. 873–891], generalizing arguments of Erdős and Pomerance [Math. Comp. 46 (1986), pp. 259–279] and Monier [Theoret. Comput. Sci. 12 (1980), 97–108]. These bounds are provided for both Jacobi symbol ±1 cases, providing evidence for the existence of several challenge pseudoprimes.

1. INTRODUCTION

A pseudoprime is a composite number that satisfies some necessary condition for primality. Since primes are necessary building blocks for so many algorithms, and since the most common way to find primes in practice is to apply primality testing algorithms based on such necessary conditions, it is important to gather what information we can about pseudoprimes. In addition to the practical benefits, pseudoprimes have remarkable divisibility properties that make them fascinating objects of study.

The most common necessary condition used in practice is that the number has no small divisors. Another common necessary condition follows from a theorem of Fermat, that if n is prime and $\gcd(a,n) = 1$, then $a^{n-1} = 1 \pmod{n}$. If $\gcd(a,n) = 1$ and $a^{n-1} = 1 \pmod{n}$ for composite n, we call a a Fermat liar and denote by $F(n)$ the set of Fermat liars with respect to n, or more precisely the set of their residue classes modulo n.

For the purposes of generalization, it is useful to translate the Fermat condition to polynomial rings. Let n be prime, let $R = \mathbb{Z}/n\mathbb{Z}$, assume $a \in R^\times$, and construct the polynomial ring $R[x]/\langle x-a\rangle$. Then a little work shows that $x^n = x$ in $R[x]/\langle x-a\rangle$ [Gra01, Proof of Theorem 4.1]. After all, as $x = a$ in $R[x]/\langle x-a\rangle$, we have $R[x]/\langle x-a\rangle \cong R$ as fields, and $a^n = a$ in R. The advantage of this view is that $x - a$ may be replaced by an arbitrary polynomial.

In the following definition gcmd stands for "greatest common monic divisor", and it implicitly depends on a modulus n. Following [Gra01], for monic polynomials

Received by the editor July 18, 2017, and, in revised form, May 26, 2018, October 26, 2018, February 8, 2019, March 8, 2019, and March 24, 2019.

2010 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11A41.

Key words and phrases. Primality testing, pseudoprime, Frobenius pseudoprime, Lucas pseudoprime.

The first author gratefully acknowledges support from the Pacific Institute for Mathematical Sciences (PIMS).

The second author was supported by an Artistic and Scholarly Development grant from Illinois Wesleyan University.

$g_1(x), g_2(x), f(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ we say that $\operatorname{gcmd}(g_1(x), g_2(x)) = f(x)$ if the ideal generated by $g_1(x), g_2(x)$ is principal and equals the ideal generated by $f(x)$ in $(\mathbb{Z}/n\mathbb{Z})[x]$.

Definition 1 ([Gra01], Section 3)**.** Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree d and discriminant Δ. Then odd composite n is a Frobenius pseudoprime with respect to $f(x)$ if the following conditions all hold:

(1) (Integer Divisibility) We have $\gcd(n, f(0)\Delta) = 1$.
(2) (Factorization) Let $f_0(x) = f(x) \pmod{n}$. Define $F_i(x) = \operatorname{gcmd}(x^{n^i} - x, f_{i-1}(x))$ and $f_i(x) = f_{i-1}(x)/F_i(x)$ for $1 \le i \le d$. All of the gcmds exist and $f_d(x) = 1$.
(3) (Frobenius) For $2 \le i \le d$, $F_i(x) \mid F_i(x^n)$.
(4) (Jacobi) Let $S = \sum_{2|i} \deg(F_i(x))/i$. Have $(-1)^S = (\Delta \mid n)$, where $(\Delta \mid n)$ is the Jacobi symbol.

If n is prime, then $(\mathbb{Z}/n\mathbb{Z})$ is a field, making $(\mathbb{Z}/n\mathbb{Z})[x]$ a principal ideal domain, from which it follows that $\operatorname{gcmd}(g_1(x), g_2(x))$ must exist. As an example of nonexistence note that the ideal $\langle x+2, x\rangle \subseteq (\mathbb{Z}/6\mathbb{Z})[x]$ is nonprincipal and thus $\operatorname{gcmd}(x+2, x)$ does not exist modulo 6. Grantham shows that if $\operatorname{gcmd}(g_1(x), g_2(x))$ exists in $(\mathbb{Z}/n\mathbb{Z})[x]$, then for each prime $p \mid n$, the usual $\gcd(g_1(x), g_2(x))$, when taken over $\mathbb{Z}/p\mathbb{Z}$, will have the same degree [Gra01, Corollary 3.3]. Furthermore, the Euclidean algorithm when applied to $g_1(x), g_2(x)$ will either correctly compute their gcmd, or find a proper factor of n when the leading coefficient of a remainder fails to be a unit [Gra01, Proposition 3.5]. Returning to the earlier example, if we apply the Euclidean algorithm in an attempt to compute $\gcd(x, x+2)$ modulo 6, the first recursive step yields $\gcd(x+2, 2)$, and then in performing the resulting division the attempt to invert 2 fails and yields a factor of 6.

Example. Suppose $d = 1$ and n is a Frobenius pseudoprime with respect to $f(x) = x - a$. Then $\gcd(a, n) = 1$ and $\operatorname{gcmd}(x^n - x, x - a) = x - a$, which implies a is a unit and $a^n = a \pmod{n}$. Hence a is a Fermat liar with respect to n. Conversely, if a is a Fermat liar, then $\gcd(a, n) = 1$ and $\operatorname{gcmd}(x^n - x, x - a) = x - a$, from which we conclude that n is a Frobenius pseudoprime with respect to $x - a$.

A Frobenius liar is then a polynomial, and to count the liars with respect to n we restrict our polynomials to members of $(\mathbb{Z}/n\mathbb{Z})[x]$. We denote by $L_d(n)$ the set of Frobenius liars of degree d with respect to n, and note by the example above that $L_1(n) = F(n)$. We will further divide the set $L_2(n)$ into $L_2^+(n)$ and $L_2^-(n)$. A degree 2 polynomial $f(x)$ with discriminant Δ will be in $L_2^+(n)$ (respectively, $L_2^-(n)$) if $(\Delta \mid n) = 1$ (respectively, -1). Notice that if $(\Delta \mid n) = 0$, $f(x)$ is not a liar since it fails the Integer Divisibility step. Let $\operatorname{Frob}_2(y, f(x))$ be the set of degree-2 Frobenius pseudoprimes with respect to $f(x)$, up to bound y, and similarly divide them into $+$ and $-$ sets according to the Jacobi symbol. Further, let $\operatorname{Frob}_2(f(x))$ be the (possibly infinite) set of all such pseudoprimes. As an abuse of notation, the same symbols will be used for the size of each set.

The main goal of this work is to generalize [EP86, Theorem 2.1], which bounds the average number of Fermat liars. We prove the following two theorems.

Theorem 2. *For all α satisfying Proposition 21, in particular $\alpha \leq \frac{10}{3}$, we have that as $y \to \infty$,*

$$y^{3-\alpha^{-1}-o(1)} \leq \sum_{n \leq y} L_2^+(n) \leq y^3 \cdot \mathcal{L}(y)^{-1+o(1)},$$

where the sum is restricted to odd composite n. Moreover, the same bounds hold if we replace $L_2^+(n)$ by $L_2(n)$. Here $\mathcal{L}(y) = \exp((\log y)(\log\log\log y)/\log\log y)$, with log *denoting the natural logarithm.*

Theorem 3. *For all α satisfying Proposition 22, in particular $\alpha \leq \frac{4}{3}$, we have that as $y \to \infty$,*

$$y^{3-\alpha^{-1}-o(1)} \leq \sum_{n \leq y} L_2^-(n) \leq y^3 \cdot \mathcal{L}(y)^{-1+o(1)},$$

where the sum is restricted to odd composite n.

As a comparison, if n is prime, then the size of $L_2(n)$ is $(n-1)^2$, $L_2^+(n) = \frac{1}{2}(n-1)(n-2)$, and $L_2^-(n) = \frac{1}{2}n(n-1)$. Thus the average count of liars for composites is rather large.

Remark 4. We obtain the same results if we restrict to composite n coprime to some fixed value.

These theorems count pairs $(f(x), n)$, where $n \leq y$ and n is a degree-2 Frobenius pseudoprime with respect to $f(x)$. We thus have the following corollary on the average count of degree-2 Frobenius pseudoprimes with Jacobi symbol -1.

Corollary 5. *Suppose α satisfies the conditions outlined in Theorem 3. Then as $y \to \infty$ we have*

$$\sum_{a,b \leq y} \mathrm{Frob}_2^-(y, x^2 + ax + b) \geq y^{3-\alpha^{-1}-o(1)}.$$

In [Gra01, Section 8], Grantham offers \$6.20 for exhibiting a Frobenius pseudoprime with respect to $x^2 + 5x + 5$ that is congruent to 2 or 3 modulo 5. The proper generalization for these Grantham challenge pseudoprimes are the sets $\mathrm{Frob}_2^-(x^2 + ax + b)$, since the condition of being $2, 3 \pmod 5$ is equivalent to $(5 \mid n) = -1$. Grantham later proved [Gra10, Theorem 2.1] that the sets $\mathrm{Frob}(f(x))$ are infinite for all monic, squarefree polynomials $f(x) \in \mathbb{Z}[x]$, but his construction is limited to composite n for which $(\Delta \mid n) = 1$ and $(\Delta \mid p) = 1$ for all $p \mid n$. Our work is limited to degree 2 polynomials, but expands the cases to include Jacobi symbol -1 for both n and $p \mid n$. Corollary 5 is consistent with the conjecture that the sets $\mathrm{Frob}_2^-(f(x))$ are infinite as well, and provides good evidence that there are infinitely many Grantham challenge pseudoprimes.

Further motivation for the present work comes from other challenge pseudoprimes. PSW challenge pseudoprimes [Guy04, Section A12], also known as \$620 problem numbers, are composite n that are simultaneously base-2 Fermat pseudoprimes, Fibonacci pseudoprimes, and congruent to $2, 3$ modulo 5. Potentially even more rare are Baillie pseudoprimes [BW80, Section 6] (also called Baillie-PSW pseudoprimes due to the challenge posed in [PSW80, Section 10]), composite n that are simultaneously base-2 strong pseudoprimes and strong Lucas pseudoprimes with respect to a polynomial $x^2 - Px + Q$ chosen in a prescribed way to ensure $\left(P^2 - 4Q \mid n\right) = -1$. Though it is unresolved whether these sought-after numbers are Frobenius pseudoprimes, strong Frobenius pseudoprimes, or something more restrictive still, quadratic Frobenius pseudoprimes provide a natural generalization for the types of conditions requested.

From this we conclude that the division of $L_2(n)$ into $(\Delta \mid n) = \pm 1$ cases is of fundamental importance, and in particular that bounding $\sum_{n \leq y} L_2^-(n)$ is of strong interest.

Since $\mathrm{Frob}_2(x^2 - Px + Q)$ is a subset of the set of (P, Q)-Lucas pseudoprimes [Gra01, Theorem 4.9], Corollary 5 gives an immediate lower bound on the average count of Lucas pseudoprimes. We do not explore the connection to Lucas pseudoprimes further in this work.

2. Degree-2 Frobenius pseudoprimes

This work focuses on the degree 2 case. We reproduce the definition and give some basic facts about Frobenius pseudoprimes and liars. From now on n will be an odd composite natural number.

Definition 6. Let $f(x) \in \mathbb{Z}[x]$ be a degree 2 monic polynomial with discriminant Δ, and let n be an odd composite. Then n is a degree-2 Frobenius pseudoprime with respect to $f(x)$ if the following four conditions hold:

(1) (Integer Divisibility) We have $\gcd(n, f(0)\Delta) = 1$.
(2) (Factorization) Let $F_1(x) = \mathrm{gcmd}(x^n - x, f(x))$, $f_1(x) = f(x)/F_1(x)$, $F_2(x) = \mathrm{gcmd}(x^{n^2} - x, f_1(x))$, and $f_2(x) = f_1(x)/F_2(x)$. All these polynomials exist and $f_2(x) = 1$.
(3) (Frobenius) We have $F_2(x) \mid F_2(x^n)$.
(4) (Jacobi) We have $(-1)^S = (\Delta \mid n)$, where $S = \deg(F_2(x))/2$.

Alternatively, in this case we call $f(x)$ a degree-2 Frobenius liar with respect to n.

The first condition ensures that $\Delta \neq 0$ and 0 is not a root of $f(x)$. Since the discriminant is nonzero, $f(x)$ is squarefree. Thus the roots of $f(x)$ are nonzero and distinct modulo p for all $p \mid n$.

Example. Consider $f(x) = x^2 - 1$ with $\Delta = 4$. If n is odd, $F_1(x) = f(x)$ and $F_2(x) = 1$, so the Frobenius step is trivially satisfied. Since $S = 0$, n will be a Frobenius pseudoprime as long as $(\Delta \mid n) = 1$. Since 4 is a square modulo n for all $n \geq 5$, we conclude that all odd $n \geq 5$ have at least one degree-2 Frobenius liar.

Example. Next consider $f(x) = x^2 + 1$ with $\Delta = -4$. Observe that $n = 1 \pmod 4$ if and only if $(-1)^{(n-1)/2} = 1$, which is true if and only if $\mathrm{gcmd}(x^n - x, f(x)) \neq 1$. In this case $F_2(x) = 1$ and $(-1)^S = 1 = (-1 \mid n) = (\Delta \mid n)$. In the other case, $n = 3 \pmod 4$ if and only if $\mathrm{gcmd}(x^n - x, f(x)) = 1$. However, $(-1)^{(n^2-1)/2} = 1$, and so $\mathrm{gcmd}(x^{n^2} - x, f(x)) = f(x)$. For the Frobenius step, we know $x^2 + 1 \mid x^{2n} + 1$ since if a is a root of $x^2 + 1$, n odd implies that $(a^2)^n = -1$, and hence a is also a root of $x^{2n} + 1$. Finally, the Jacobi step is satisfied since $(-1)^S = -1 = (\Delta \mid n)$. This demonstrates that $x^2 + 1$ is also a liar for all odd composite n. The minimum number of degree-2 Frobenius liars for odd composite n is in fact 2, first achieved by $n = 15$.

If we fix n and instead restrict to liars with $(\Delta \mid n) = -1$, then it is possible that no such liars exist. See Section 3.4 for a more in-depth discussion of this case.

We next give several reinterpretations of the conditions under which a number $n = \prod_i p_i^{r_i}$ is a degree-2 Frobenius pseudoprime with respect to a monic polynomial f. We treat cases $(\Delta \mid n) = +1$ and $(\Delta \mid n) = -1$ separately.

2.1. **The case $(\Delta \mid n) = +1$.** Supposing we already know that $(\Delta \mid n) = +1$, n is a degree-2 Frobenius pseudoprime with respect to monic $f(x)$ if and only if

(1) (Integer Divisibility) we have $\gcd(n, f(0)\Delta) = 1$ and
(2) (Factorization) $\operatorname{gcmd}(x^n - x, f(x)) = f(x) \pmod{n}$.

All other conditions follow immediately. In particular, because $f(x) \mid x^n - x$ modulo n, it is not possible for the Euclidean algorithm to discover any nontrivial factors of n. We observe that these conditions can be interpreted locally, giving us the following result.

Proposition 7. *Positive integer $n = \prod_i p_i^{r_i}$ satisfies Definition 6 in the case $(\Delta \mid n) = 1$ if and only if*

(1) *(Integer Divisibility) Δ is a unit modulo n and 0 is not a root of $f(x)$ modulo p_i for all i and*
(2) *(Factorization) $\operatorname{gcmd}(x^n - x, f(x)) = f(x) \pmod{p_i^{r_i}}$ for all i.*

Proof. First assume that n is a degree-2 Frobenius pseudoprime with respect to $f(x)$ according to Definition 6 and that $(\Delta \mid n) = 1$. Then $\gcd(n, f(0)\Delta) = 1$, so $\gcd(\Delta, n) = 1$ making Δ a unit, and $\gcd(f(0), n) = 1$. It follows that $f(0) \not\equiv 0 \pmod{p}$ for all $p \mid n$.

The Jacobi condition in Definition 6 along with the assumption that $(\Delta \mid n) = 1$ ensures $S = 0$, and so $\deg(F_2(x)) = 0$. All the polynomials in condition (2) are monic, so $F_2(x) = 1$, which implies $f_1(x) = 1$, so that $\operatorname{gcmd}(x^n - x, f(x)) = f(x)$. Since this identity is true modulo n, it is true modulo $p_i^{r_i}$ for all i.

Conversely, if $\operatorname{gcmd}(x^n - x, f(x)) = f(x) \pmod{p_i^{r_i}}$ for all i, then the identity is true modulo n by the Chinese remainder theorem. It follows that $f_1(x) = 1$, and so $F_2(x) = 1$. Thus condition (2) of Definition 6 is true, condition (3) follows trivially, and condition (4) is true since $S = 0$.

We are assuming that Δ is a unit modulo n, from which it follows that $\gcd(\Delta, n) = 1$. Furthermore, $f(0) \not\equiv 0 \pmod{p}$ for all $p \mid n$ implies $\gcd(f(0), n) = 1$. Thus condition (1) is satisfied. □

2.2. **The Case $(\Delta \mid n) = -1$.** When $(\Delta \mid n) = -1$ we need a couple more conditions.

Proposition 8. *Positive integer $n = \prod_i p_i^{r_i}$ satisfies Definition 6 in the case $(\Delta \mid n) = -1$ if and only if it satisfies the following conditions:*

(1) *(Integer Divisibility) discriminant Δ is a unit modulo n and 0 is not a root of $f(x) \pmod{p_i}$ for all i,*
(2) *(Factorization 1) $\operatorname{gcmd}(x^n - x, f(x)) = 1 \pmod{p_i^{r_i}}$ for all i,*
(3) *(Factorization 2) $\operatorname{gcmd}(x^{n^2} - x, f(x)) = f(x) \pmod{p_i^{r_i}}$ for all i,*
(4) *(Frobenius) if α is a root of $f(x)$ modulo $p_i^{r_i}$, then so too is α^n for all i.*

In particular, these conditions are sufficient to ensure that $\operatorname{gcmd}(x^n - x, f(x))$ and $\operatorname{gcmd}(x^{n^2} - x, f(x))$ exist modulo n.

Proof. Following the argument from Proposition 7, condition (1) from Definition 6 holds if and only if Δ is a unit modulo n and 0 is not a root of $f(x) \pmod{p_i}$ for all i.

Now, if we assume n satisfies Definition 6, then by condition (4) we must have $S = 1$, and hence $\deg(F_2(x)) = 2$. Thus $\mathrm{gcmd}(x^{n^2} - x, f_1(x)) = f(x)$, and since $f_2(x) = 1$ we further have $f_1(x) = f(x)$. This is only possible if $\mathrm{gcmd}(x^n - x, f(x)) = 1$. Since these identities hold modulo n, they hold modulo $p_i^{r_i}$ for all i. Finally, $F_2(x) \mid F_2(x^n)$ means that $f(x) \mid f(x^n) \pmod{n}$; hence if α is a root of $f(x)$ modulo $p_i^{r_i}$, then α^n is a root as well.

Conversely, assume n satisfies conditions (2), (3), (4) from the statement of the proposition. By the Chinese remainder theorem, conditions (2) and (3) mean that $\mathrm{gcmd}(x^n - x, f(x)) = 1 \pmod{n}$ and $\mathrm{gcmd}(x^{n^2} - x, f(x)) = f(x) \pmod{n}$. In the language of Definition 6, we have $F_1(x) = 1$, $F_2(x) = f(x)$, and $f_2(x) = 1$ as required. It follows that the Jacobi step is satisfied. Finally, condition (3) means that $f(x) \mid f(x^n) \pmod{p_i^{r_i}}$ for all i, and so the Frobenius step is satisfied modulo n.

If all gcmd calculations exist modulo n, then they exist modulo $p_i^{r_i}$ for all i, so to finish the proof we need to show that the latter condition is sufficient to ensure that $\mathrm{gcmd}(x^n - x, f(x))$ and $\mathrm{gcmd}(x^{n^2} - x, f(x))$ exist. Since $\mathrm{gcmd}(x^n - x, f(x)) = 1 \pmod{p_i^{r_i}}$ for all i, by [Gra01, Proposition 3.4] we know that $\mathrm{gcmd}(x^n - x, f(x)) = 1 \pmod{n}$ and thus exists. If $\mathrm{gcmd}(x^{n^2} - x, f(x)) = f(x) \pmod{p_i^{r_i}}$, then $p_i^{r_i}$ divides $x^{n^2} - x - f(x)g_i(x)$ for some polynomial $g_i(x)$. However, using the Chinese remainder theorem on each coefficient in turn, we can construct a polynomial $g(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ such that $g(x) = g_i(x) \pmod{p_i^{r_i}}$ for all i. Then for all i, $p_i^{r_i}$ divides $x^{n^2} - x - f(x)g(x)$ and hence n divides $x^{n^2} - x - f(x)g(x)$. This shows that $\mathrm{gcmd}(x^{n^2} - x, f(x)) = f(x) \pmod{n}$, and in particular that it exists. □

Remark 9. Earlier we commented that if the gcmd does not exist, the Euclidean algorithm will find a factor of n. Here we note that even if the gcmd exists, the Euclidean algorithm might detect a factor of n while computing it. For example, consider $n = 14$ and $\mathrm{gcmd}(x^{14} - x, x^2 + x + 1)$ modulo 14. When dividing $x^{14} - x$ by $x^2 + x + 1$ we get a remainder of $-2x - 1$, so the second step of the Euclidean algorithm will attempt to invert 2 and find 2 as a factor of 14. However, $4(x^2+x+1)+(2x+1)(-2x-1) = 3$, a unit modulo 14, and thus $\mathrm{gcmd}(x^{14}-x, x^2+x+1) = 1$.

That said, for the calculations involved in checking for degree-2 Frobenius pseudoprimes this failure mode can only happen in the $(\Delta \mid n) = -1$ case and only if either n is even or if one of the conditions (1)–(4) of Proposition 8 would already fail. When n is even, it will only discover a power of 2 (and the complementary factor). The rest of this remark justifies these claims.

First, assume the Euclidean algorithm would discover factors of n. If the Factorization 1 and Factorization 2 conditions are passed, then it implies there exist primes p_i and p_j such that at some iteration of the Euclidean algorithm to compute $\mathrm{gcmd}(x^n - x, f(x))$, the degrees of the polynomials being considered differ.

We note that given $\mathrm{gcmd}(x^n - x, f(x)) = 1 \pmod{n}$ we must have for each $p \mid n$ that

$$x^n - x = f(x)g(x) + ax + b \pmod{p},$$

where either $a = 0$ and b is a unit, or a is a unit. However, if $a = 0$, then condition (Frobenius) implies that the roots of $f(x)$ modulo p are α and $\alpha + b$. But this can only happen for $p = 2$. In particular, if n is odd, then we must have that $a \neq 0$ is a unit for all $p \mid n$, and thus

$$x^n - x = f(x)g(x) + ax + b \pmod{n}.$$

Given that $\operatorname{gcmd}(x^n - x, f(x)) = 1 \pmod{n}$ we then have that

$$f(x) = (ax+b)h(x) + e \pmod{n},$$

where e is a unit. It follows that the only possible discrepancy between p_i and p_j is if one of the primes is 2.

Finally, the Euclidean algorithm will not discover a factor of n while computing $\operatorname{gcmd}(f(x), g(x))$ if the result is $f(x)$.

3. Monier formula for degree-2 Frobenius pseudoprimes

In this section we give explicit formulas, analogous to those of Monier [Mon80, Proposition 1], for the quantity $L_2(n)$ of polynomials $f(x)$ modulo $n = \prod_i p_i^{r_i}$ for which n is a degree-2 Frobenius pseudoprime. The key step will be reinterpreting the conditions of the previous section in terms of conditions on the roots α and β of $f(x)$ modulo $p_i^{r_i}$ for each i.

As in the previous section, it shall be useful to distinguish the cases $(\Delta \mid n) = \pm 1$, and as such we will give separate formulas for $L_2^{\pm}(n)$.

Notation. For each fixed value of n, denote by $L_2^{+}(n)$ the total number of quadratic polynomials $f \pmod{n}$ such that (f, n) is a liar pair and $(\Delta \mid n) = +1$.

For each fixed value of n, denote by $L_2^{-}(n)$ the total number of quadratic polynomials $f \pmod{n}$ such that (f, n) is a liar pair and $(\Delta \mid n) = -1$.

At the heart of the formula is the size and structure of the ring $R := (\mathbb{Z}/p^r\mathbb{Z})[x]/\langle f(x)\rangle$, so we spend a little time discussing some basic facts.

Recall that in the case where $r = 1$, if $(\Delta \mid p) = 1$, then $R \simeq \mathbb{F}_p \times \mathbb{F}_p$ and $|R^\times| = (p-1)^2$, while if $(\Delta \mid p) = -1$, then $R \simeq \mathbb{F}_{p^2}$ and $R^\times$ is cyclic of order $p^2 - 1$. When $r > 1$ we have the canonical surjective homomorphism

$$\phi : (\mathbb{Z}/p^r\mathbb{Z})[x]/\langle f(x)\rangle \to (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$$

and a similar map on the unit groups. Furthermore, $f(x)$ will split in $\mathbb{Z}/p^r\mathbb{Z}$ if and only if $(\Delta \mid p) = 1$. Thus $|R^\times| = p^{2r-2}(p-1)^2$ if $(\Delta \mid p) = 1$ and $|R^\times| = p^{2r-2}(p^2-1)$ if $(\Delta \mid p) = -1$. In the latter case, since $R^\times$ maps surjectively onto a cyclic group of order $p^2 - 1$ with kernel a p-group, it has a cyclic subgroup C of order $p^2 - 1$. This fact follows from the fundamental theorem of abelian groups [Lan02, Exercise 1.43] and implies that there is a section of ϕ yielding a bijective homomorphism from C to $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$.

3.1. The case $(\Delta \mid n) = +1$.

We note that in this case there must be an even number of primes p_i for which r_i is odd and $(\Delta \mid p_i) = -1$.

In order to count the number of $f(x)$ modulo n, we shall count for each i the number of modulo $p_i^{r_i}$ liars for which $(\Delta \mid p_i) = \pm 1$. By the Chinese remainder theorem, the desired count is then the product for all combinations which ensure the above parity condition.

Lemma 10. *Suppose $p^r \| n$. The number of degree 2 polynomials over $(\mathbb{Z}/p^r\mathbb{Z})$ with $(\Delta \mid n) = +1$ and $(\Delta \mid p) = +1$ for which n is a quadratic Frobenius pseudoprime at p is exactly*

$$L_2^{++}(n,p) = \frac{1}{2}\left(\gcd(n-1,p-1)^2 - \gcd(n-1,p-1)\right).$$

Proof. Referring to Proposition 7, $\mathrm{gcmd}(x^n - x, f(x)) = f(x) \pmod{p^r}$ means that $\alpha^n = \alpha$ and $\beta^n = \beta$ modulo p^r for roots α, β of $f(x)$. In addition, the roots are distinct and nonzero by the integer divisibility condition.

The group $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic, so it has $\gcd(n-1, p^{r-1}(p-1)) = \gcd(n-1, p-1)$ elements whose order divides both $n-1$ and $p-1$. Choosing two such elements, which are not congruent modulo p, gives the result. □

Lemma 11. *Suppose $p^r || n$. The number of degree 2 polynomials over $(\mathbb{Z}/p^r\mathbb{Z})$ with $(\Delta \mid n) = +1$ and $(\Delta \mid p) = -1$ for which n is a quadratic Frobenius pseudoprime at p is exactly*

$$L_2^{+-}(n,p) = \frac{1}{2}\left(\gcd(n-1, p^2-1) - \gcd(n-1, p-1)\right).$$

Proof. We again refer to Proposition 7. Since $(\Delta \mid p) = -1$, $R := (\mathbb{Z}/p^r\mathbb{Z})[x]/\langle f(x)\rangle$ maps surjectively onto $\mathbb{F}_{p^2}$ and the cofactor has size p^{2r-2}. Furthermore, the distinct, nonzero roots α, β of $f(x)$ are not lifts of elements of $\mathbb{F}_p$, and $\alpha^{p^r} = \beta \pmod{p^r}$. The factorization condition implies that $\alpha^n = \alpha \pmod{p^r}$, so that the order of α in $R^\times$ divides $n-1$.

All elements of $R^\times$ have order dividing $p^{2r-2}(p^2-1)$. Hence the number of options for α is exactly $\gcd(p^2-1, n-1) - \gcd(p-1, n-1)$, and we divide by 2 since the polynomial $f(x) \pmod{p^r}$ is symmetric in α and β. □

In order to capture the requirement that we have an even number of contributions from primes where $(\Delta \mid p_i) = -1$ with r_i odd, we antisymmetrize with respect to these terms to obtain the formula for $L_2^+(n)$.

Theorem 12. *The number of degree 2 polynomials over $(\mathbb{Z}/n\mathbb{Z})$ with $(\Delta \mid n) = +1$ for which n is a quadratic Frobenius pseudoprime is exactly*

$$\frac{1}{2}\prod_i \left(L_2^{++}(n,p_i) + L_2^{+-}(n,p_i)\right)$$
$$+ \frac{1}{2}\prod_{2 \mid r_i}\left(L_2^{++}(n,p_i) + L_2^{+-}(n,p_i)\right)\prod_{2 \nmid r_i}\left(L_2^{++}(n,p_i) - L_2^{+-}(n,p_i)\right).$$

Corollary 13. *If n is squarefree, the formula in Theorem 12 becomes*

$$L_2^+(n) = \frac{1}{2}\prod_{p \mid n}\frac{1}{2}\left(\gcd(n-1,p^2-1) + \gcd(n-1,p-1)^2 - 2\gcd(n-1,p-1)\right)$$
$$+ \frac{1}{2}\prod_{p \mid n}\frac{1}{2}\left(\gcd(n-1,p-1)^2 - \gcd(n-1,p^2-1)\right).$$

3.2. **The case $(\Delta \mid n) = -1$.** In this case there must be an odd number of primes p_i for which r_i is odd and $(\Delta \mid p_i) = -1$. As above, the liar count is first computed locally.

Lemma 14. *The number of degree 2 polynomials over $(\mathbb{Z}/p^r\mathbb{Z})$ with $(\Delta \mid n) = -1$ and $(\Delta \mid p) = +1$ for which n is a quadratic Frobenius pseudoprime at p is exactly*

$$L_2^{-+}(n,p) = \frac{1}{2}\left(\gcd(n^2-1, p-1) - \gcd(n-1, p-1)\right).$$

Proof. Since $(\Delta \mid p) = 1$, the roots α, β of $f(x)$ are in $(\mathbb{Z}/p^r\mathbb{Z})$. Referring to Proposition 8, the roots are distinct and nonzero by the integer divisibility condition.

Furthermore, $\mathrm{gcmd}(x^n - x, f(x)) = 1$ means that $\alpha^n \neq \alpha \pmod{p^r}$, but we do have $\alpha^{n^2} = \alpha \pmod{p^r}$ by the factorization 2 condition. The Frobenius condition implies that α^n is a root of $f(x)$, and thus $\alpha^n = \beta$.

The group $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic of order $p^{r-1}(p-1)$, and so the number of elements with order dividing both n^2-1 and $p^{r-1}(p-1)$ is $\gcd(n^2-1, p-1)$. We subtract off the subset of elements with order dividing $n-1$, then divide by 2 since $f(x) \pmod{p^r}$ is symmetric in α and β. □

Lemma 15. *The number of degree* 2 *polynomials over* $(\mathbb{Z}/p^r\mathbb{Z})$ *with* $(\Delta \mid n) = -1$ *and* $(\Delta \mid p) = -1$ *for which* n *is a quadratic Frobenius pseudoprime at* p *is exactly*

$$L_2^{--}(n,p) = \frac{1}{2}\left(\gcd(p^2-1, n^2-1, n-p) - \gcd(n-1, p-1)\right).$$

Proof. Since $(\Delta \mid p) = -1$, $R := (\mathbb{Z}/p^r\mathbb{Z})[x]/\langle f(x)\rangle$ maps surjectively onto $\mathbb{F}_{p^2}$ and $R^\times$ has order $p^{2r-2}(p^2-1)$. Furthermore, roots α, β of $f(x)$ are not in $\mathbb{Z}/p^r\mathbb{Z}$, and by the divisibility condition in Proposition 8 we know that those roots are distinct units modulo p. The factorization conditions tell us that $\alpha^{n^2} = \alpha \pmod{p^r}$ and the Frobenius condition implies $\alpha^n = \beta \pmod{p^r}$.

We claim a further relation on the roots, namely that $\alpha^p = \beta \pmod{p}$ implies $\alpha^p = \beta \pmod{p^r}$. If $\alpha^p = \beta \pmod{p}$, then $\alpha^p/\beta \in \mathrm{Ker}(\phi)$, a p-group, and thus has order divisible by p unless it is the identity in $R^\times$. However, the multiplicative orders of α, β divide n^2-1, and thus $\alpha^p/\beta \in C$, the cyclic group in $R^\times$ of order p^2-1. It follows that the order of α^p/β in $R^\times$ must be 1, making it the identity modulo p^r.

We conclude that the order of α in $R^\times$ must divide n^2-1, $p^{2r-2}(p^2-1)$, and $n-p$. The number of options for α is thus exactly $\gcd(p^2-1, n^2-1, n-p) - \gcd(p-1, n-1)$, and we divide by 2 since the polynomial $f(x) \pmod{p^r}$ is symmetric in α and β. □

In order to capture the requirement that we have an odd number of contributions from primes where $(\Delta \mid p_i) = -1$ when r_i is odd, we antisymmetrize with respect to these terms to obtain the formula for $L_2^-(n)$.

Theorem 16. *The number of degree* 2 *polynomials over* $(\mathbb{Z}/n\mathbb{Z})$ *with* $(\Delta \mid n) = -1$ *for which* n *is a quadratic Frobenius pseudoprime is exactly*

$$\frac{1}{2}\prod_i \left(L_2^{-+}(n,p_i) + L_2^{--}(n,p_i)\right) - \frac{1}{2}\prod_{2\mid r_i}\left(L_2^{-+}(n,p_i) + L_2^{--}(n,p_i)\right)\prod_{2\nmid r_i}\left(L_2^{-+}(n,p_i) - L_2^{--}(n,p_i)\right).$$

Corollary 17. *If* n *is squarefree, the formula in Theorem* 16 *becomes*

$$L_2^-(n) = \frac{1}{2}\prod_{p\mid n}\frac{1}{2}\left(\gcd(n^2-1, p-1) + \gcd(n^2-1, p^2-1, n-p) - 2\gcd(n-1, p-1)\right) - \frac{1}{2}\prod_{p\mid n}\frac{1}{2}\left(\gcd(n^2-1, p-1) - \gcd(n^2-1, p^2-1, n-p)\right).$$

3.3. **Upper bounds.** In this section we give simpler upper bounds for $L_2^+(n)$ and $L_2^-(n)$, which will be needed in Section 6.

Lemma 18. *If n is a composite integer, then*

$$L_2^+(n) \le \prod_{p \mid n} \max(\gcd(n-1, p^2-1), \gcd(n-1, p-1)^2) \text{ and}$$

$$L_2^-(n) \le \prod_{p \mid n} \gcd(n^2-1, p^2-1).$$

Proof. For each prime factor p of n, we choose the greater of $L_2^{++}(n,p)$ and $L_2^{+-}(n,p)$. That is,

$$\begin{aligned} L_2^+(n) &\le \prod_i \max(L_2^{++}(n,p_i), L_2^{+-}(n,p_i)) \\ &\le \prod_{p \mid n} \max(\gcd(n-1,p-1)^2, \gcd(n-1,p^2-1)). \end{aligned}$$

For $L_2^-(n)$ a similar argument gives the simpler upper bound

$$\prod_{p \mid n} \max(\gcd(n^2-1, p^2-1, n-p), \gcd(n^2-1, p-1)) \le \prod_{p \mid n} \gcd(n^2-1, p^2-1). \qquad \square$$

3.4. **The vanishing of $L_2^-(n)$.** A major theme of this work is that odd composites have many quadratic Frobenius liars on average, even if we restrict to the case $(\Delta \mid n) = -1$. With this in mind, it is useful to note that $L_2^-(n)$ can be 0. For example, $L_2^-(9) = 0$ and $L_2^-(21) = 0$.

As a first general example, write $n = ps$ with $\gcd(p,s) = 1$. If the quantities

$$\gcd(p^2-1, n^2-1, n-p) - \gcd(n-1, p-1) \quad \text{and} \quad \gcd(n^2-1, p-1) - \gcd(n-1, p-1)$$

are both zero, then it is immediate from Theorem 16 that $L_2^-(n) = 0$. These conditions are met if whenever $\ell^r \mid \gcd(p^2-1, n^2-1, n-p)$ or $\ell^r \mid \gcd(n^2-1, p-1)$ we also have $\ell^r \mid \gcd(n-1, p-1)$. For odd primes $\ell \mid p^2-1$ this is accomplished by the requirement that

$$s \not\equiv -p^{-1} \pmod{\ell},$$

as this implies that if $\ell \mid p^2-1$ then $\ell \nmid sp+1$. For the prime 2, if we write $p = 1 + 2^r \pmod{2^{r+1}}$, then the requirement

$$s = 1 + 2^r \pmod{2^{r+1}}$$

implies that the exact power of 2 dividing each of $\gcd(p^2-1, n^2-1, n-p)$, $\gcd(n^2-1, p-1)$, and $\gcd(n-1, p-1)$ is 2^r.

A more general example comes from Carmichael numbers, which are squarefree n with $\gcd(n-1, p-1) = p-1$ for all primes $p \mid n$.

Remark 19. If n is a classical Carmichael number, then $L_2^{-+}(n,p) = 0$ for all p and

$$L_2^-(n) = \prod_{p \mid n} \frac{1}{2} \left(\gcd(n^2-1, p^2-1, n-p) - \gcd(n-1, p-1) \right)$$

if n has an odd number of prime factors, and 0 otherwise (see Corollary 17). In particular, the only f for which (f, n) is a liar pair with $(\Delta \mid n) = -1$ have f inert at all primes dividing n. Furthermore, if $n = 1 \pmod 4$, then for each $p \mid n$ with $p = 3 \pmod 4$ we naively estimate the probability that $L_2^{--}(n,p) = 0$ as $\prod'_{\ell \mid p+1} \frac{\ell-2}{\ell-1}$, where the product is over odd primes ℓ.

As a final example, let n be a rigid Carmichael number of order 2 in the sense of [How00], so that n is squarefree and $p^2-1 \mid n-1$ for every prime factor p of n. Then $\gcd(n^2-1, p^2-1, n-p) = \gcd(n-1, p-1)$ and $\gcd(n^2-1, p-1) = \gcd(n-1, p-1)$, so that $L_2^-(n) = 0$.

4. Number theoretic background

Notation. Let L be an upper bound for Linnik's constant. That is, the constant L satisfies:

$$\text{if } (a, m) = 1, \text{ then there exists prime } p = a \pmod{m} \text{ with } p < m^L.$$

It is known that $L \leq 5$. (See [Xyl11, Theorem 2.1].)

For each value x denote by $M(x)$ the least common multiple of all integers up to $\frac{\log x}{\log\log x}$.

For each value x and for each $\alpha > 0$ denote by $P_\alpha^{(+)}(x)$ the set

$$\{\text{prime } p < (\log x)^\alpha \text{ such that } (p-1) \mid M(x)\}$$

and by $P_\alpha^{(-)}(x)$ the set

$$\left\{\text{prime } p < (\log x)^\alpha \text{ such that } (p^2-1) \mid M(x)\right\}.$$

Now, given functions $M_1(x)$ and $M_2(x)$ of x which satisfy

$$M(x) = M_1(x)M_2(x) \qquad \text{and} \qquad \gcd(M_1(x), M_2(x)) = 2,$$

we define for each value x and for each $\alpha > 0$ the set

$$\begin{aligned} &P_\alpha\left(M_1(x), M_2(x), x\right) \\ &\quad = \{\text{prime } p < (\log x)^\alpha \text{ such that } (p-1) \mid M_1(x) \text{ and } (p+1) \mid M_2(x)\}. \end{aligned}$$

Proposition 20. *We have $M(x) = x^{o(1)}$ as $x \to \infty$.*

Proof. We bound $M(x)$ by

$$\prod_{p<\frac{\log x}{\log\log x}} p^{\left\lfloor \frac{\log\log x - \log\log\log x}{\log p} \right\rfloor} < \prod_{p<\frac{\log x}{\log\log x}} \frac{\log x}{\log\log x} = \left(\frac{\log x}{\log\log x}\right)^{\pi\left(\frac{\log x}{\log\log x}\right)} = x^{o(1)}.$$

□

The next two propositions follow from results on the smoothness of shifted primes. The conclusion is that the sets $P_\alpha^{(+)}(x)$ and $P_\alpha^{(-)}(x)$ are relatively large. As a comparison, by the prime number theorem the asymptotic count of all primes $p < (\log x)^\alpha$ is $\frac{(\log x)^\alpha}{\alpha \log\log x}$.

Proposition 21. *For all $\alpha \leq 10/3$ we have that $\left|P_\alpha^{(+)}(x)\right| \geq (\log x)^{\alpha - o(1)}$ as $x \to \infty$.*

Proof. This is Theorem 1 of [BH98] under the assumption that $1/\alpha > 0.2961$. □

Proposition 22. *For all $\alpha \leq 4/3$ we have that $\left|P_\alpha^{(-)}(x)\right| \geq (\log x)^{\alpha - o(1)}$ as $x \to \infty$.*

Proof. We apply [DMT01, Theorem 1.2]. The constant $\alpha = 4/3$ arises from the formula $(g - 1/(2k))^{-1}$ because $x^2 - 1$ has $k = 2$ factors of degree $g = 1$, and 1 is the highest degree among the irreducible factors. □

The next proposition is a novel contribution to the theory of pseudoprime construction. Recall that $\omega(n)$ is the count of distinct prime factors of n.

Proposition 23. *Given α such that $\left|P_\alpha^{(-)}(x)\right| \geq (\log x)^{\alpha - o(1)}$ as $x \to \infty$, then there exist $M_1(x)$, $M_2(x)$ such that as $x \to \infty$ we have*

$$|P_\alpha\left(M_1(x), M_2(x), x\right)| \geq (\log x)^{\alpha - o(1)}.$$

Proof. Let M be the fixed choice of $M(x)$ that follows from a fixed choice of x. Each prime $p \in P_\alpha^{(-)}(x)$ is also in $P_\alpha\left((p-1)d_1, (p+1)d_2, x\right)$ for all pairs (d_1, d_2) satisfying

$$d_1 d_2 = \frac{M}{p^2-1} \quad \text{and} \quad \gcd(d_1, d_2) = 1.$$

The number of pairs (M_1, M_2) satisfying the conditions laid out in the notation comment at the beginning of the section is

$$2^{\pi(\log x/\log\log x)}$$

since each prime up to $\frac{\log x}{\log\log x}$ is assigned to either M_1 or M_2. To count the number of choices for d_1 and d_2 we subtract from the exponent the count of prime factors of p^2-1. This work yields

$$\sum_{M_1, M_2} |P_\alpha\left(M_1, M_2, x\right)| = \sum_{p \in P_\alpha^{(-)}(x)} 2^{\omega\left(\frac{M}{p^2-1}\right)} > 2^{\pi\left(\frac{\log x}{\log\log x}\right) - \omega_{\max}(p^2-1)} (\log x)^{\alpha - o(1)},$$

where $\omega_{\max}(p^2-1)$ denotes the maximum number of distinct prime factors of p^2-1 for all p under consideration.

For integers up to x, the integer n that maximizes $\omega(n)$ is formed by taking the product of all small distinct primes. By the argument in [HW08, Section 22.10], it follows that for $n \leq x$ we have $\omega(n) \leq (1 + o(1))\frac{\log x}{\log\log x}$. Thus

$$2^{\omega_{\max}(p^2-1)} \leq 2^{\frac{(1+o(1))\alpha \log\log x}{\log\log((\log x)^\alpha)}} \leq (\log x)^{o(1)}.$$

Now, if $|P_\alpha(M_1, M_2, x)| \leq (\log x)^{\alpha - o(1)}$ for all pairs (M_1, M_2) we would conclude that

$$\sum_{M_1, M_2} |P_\alpha(M_1, M_2, x)| \leq 2^{\pi\left(\frac{\log x}{\log\log x}\right)} (\log x)^{\alpha - o(1)},$$

but since this contradicts the earlier lower bound we instead conclude that $|P_\alpha(M_1, M_2, x)| \geq (\log x)^{\alpha - o(1)}$ for at least one pair (M_1, M_2). □

Remark 24. From the proof we expect that the result will in fact hold for most choices of M_1 and M_2.

The proof we have given does not actually imply any relationship between $M_i(x)$ for different values of x. In particular, though one perhaps expects that that there exists a complete partitioning of all primes into two sets and that the M_i are simply constructed by considering only those primes in the given range, we do not show this.

It is generally expected (see for example [EP86, proof of Theorem 2.1]) that the values α under consideration can be taken arbitrarily large. In particular, we expect the following to hold.

Conjecture 25. *In each of the above three propositions, the result holds for all $\alpha > 0$.*

The following lemma will be useful in the next section.

Lemma 26. *Fix n and $p \mid n$. If $n = -1 \pmod q$ and $p = 1 \pmod q$ for $q \geq 3$, then*

$$\gcd(n^2-1, p-1) - \gcd(n-1, p-1) > 0.$$

If $n = -1 \pmod q$ and $p = -1 \pmod q$ for $q \geq 3$, then

$$\gcd(n^2-1, p^2-1, n-p) - \gcd(n-1, p-1) > 0.$$

If $n = p = 1 \pmod 2$, then

$$\gcd(n-1, p-1)^2 - \gcd(n-1, p-1) > 0.$$

Proof. For $n = -1 \pmod q$ and $p = 1 \pmod q$ we have $q \mid \gcd(n+1, p-1)$, while $q \nmid \gcd(n-1, p-1)$.

If $n = -1 \pmod q$ and $p = -1 \pmod q$, then $q \mid \gcd(n^2-1, p^2-1, n-p)$ and $q \nmid \gcd(n-1, p-1)$.

Finally, for $n = p = 1 \pmod 2$ it follows that $\gcd(n-1, p-1) > 1$, and so

$$\gcd(n-1, p-1)(\gcd(n-1, p-1) - 1)$$

is nonzero. □

5. Lower bounds on the average number of degree-2 Frobenius pseudoprimes

In this section we will prove the lower bound portion of the two theorems in the introduction. Specifically, we shall prove the following results.

Theorem 27. *For any value of $\alpha > 1$ satisfying Proposition 21 we have the asymptotic inequality*

$$\sum_{n<x} L_2^+(n) \geq x^{3-\alpha^{-1}-o(1)}$$

as $x \to \infty$.

Theorem 28. *For any value of $\alpha > 1$ satisfying Proposition 22 we have the asymptotic inequality*

$$\sum_{n<x} L_2^-(n) \geq x^{3-\alpha^{-1}-o(1)}$$

as $x \to \infty$.

The proofs of the above two theorems are at the end of this section. We shall first introduce some notation and prove several necessary propositions.

Notation. For fixed $0 < \epsilon < \alpha - 1$ and for all $x > 0$ let

- $k_\alpha^{(+)}(x) = \left\lfloor \frac{\log x - L \log M}{\alpha \log\log x} \right\rfloor$,
- $k_\alpha^{(-)}(x) = \left\lfloor \frac{\log x - 2L \log M}{\alpha \log\log x} \right\rfloor$,
- $S_{\alpha,\epsilon}^{(+)}(x)$ be the set of integers s which are the product of $k_\alpha^{(+)}(x)$ distinct elements from
$$P_\alpha^{(+)}(x) \setminus P_{\alpha-\epsilon}^{(+)}(x),$$
- $S_{\alpha,\epsilon}^{(-)}(M_1(x), M_2(x), x)$ be the set of integers s which are the product of the largest odd number not larger than $k_\alpha^{(-)}(x)$ many distinct elements from
$$P_\alpha(M_1(x), M_2(x), x) \setminus P_{\alpha-\epsilon}(M_1(x), M_2(x), x).$$

The following two claims are immediate consequences of the construction.

Claim. The elements s of $S^{(+)}_{\alpha,\epsilon}(x)$ all satisfy

$$\left((\log x)^{-k^{(+)}_{\alpha}(x)\epsilon}\right)\frac{x^{1-o(1)}}{M^L} \leq s < \frac{x}{M^L}$$

as $x \to \infty$.

Claim. The elements s of $S^{(-)}_{\alpha,\epsilon}(x)$ all satisfy

$$\left((\log x)^{-k^{(-)}_{\alpha}(x)\epsilon}\right)\frac{x^{1-o(1)}}{M^L} \leq s < \frac{x}{M^{2L}}$$

as $x \to \infty$.

The next two propositions follow from the lower bound on the size of $P^{(\pm)}_{\alpha}$ and the definition of $k^{(\pm)}_{\alpha}$.

Proposition 29. *If α satisfies the conditions of Proposition* 21, *then*

$$\left|S^{(+)}_{\alpha,\epsilon}(x)\right| \geq x^{1-\alpha^{-1}+o(1)}$$

as $x \to \infty$.

Proof. A standard bound on a binomial coefficient is given by $\binom{n}{k} \geq (n/k)^k$. We are choosing $k^{(+)}_{\alpha}$ many primes from a set of size at least $(\log x)^{\alpha-o(1)} - (\log x)^{\alpha-\epsilon} = (\log x)^{\alpha-o(1)}$. Noting that $M = x^{o(1)}$ by Proposition 20, the resulting lower bound on $\left|S^{(+)}_{\alpha,\epsilon}(x)\right|$ is

$$\left(\frac{(\log x)^{\alpha-o(1)}}{(\log x)^{1+o(1)}}\right)^{\frac{\log x - L\log M}{\alpha\log\log x}-1} \geq \left((\log x)^{\alpha-1+o(1)}\right)^{(\alpha^{-1}+o(1))\frac{\log x}{\log\log x}} = x^{1-\alpha^{-1}+o(1)}.$$

□

Proposition 30. *If α, $M_1(x)$, and $M_2(x)$ satisfy the conditions of Proposition* 23, *then*

$$\left|S^{(-)}_{\alpha,\epsilon}(M_1(x), M_2(x), x)\right| \geq x^{1-\alpha^{-1}+o(1)}$$

as $x \to \infty$.

Proof. The proof is identical to that of Proposition 29. □

The next two propositions construct a composite n with many degree-2 Frobenius liars. The strategy in the plus one case is to start with a composite s that is the product of many primes p such that $p-1$ is smooth, and then find a prime q such that $n = sq$ is congruent to 1 modulo M. While the liar count primarily comes from the primes p dividing s, we need to ensure at least one modulo q liar, otherwise the entire modulo n liar count becomes 0.

Lemma 31. *As before, let L be an upper bound for Linnik's constant. Given any element s of $S^{(+)}_{\alpha,\epsilon}(x)$ there exists a prime $q < M^L$ such that*

- $sq = 1 \pmod{M}$,
- $\gcd(q,s) = 1$, *and*
- $\frac{1}{2}\left(\gcd(q-1, sq-1)^2 - \gcd(q-1, sq-1)\right) > 0$.

Moreover, the number of liars of $n = sq$ with $(\Delta \mid n) = +1$ is at least $x^{2-\epsilon\frac{2}{\alpha}-o(1)}$ as $x \to \infty$.

Proof. By construction, every $s \in S_{\alpha,\epsilon}^{(+)}(x)$ satisfies $\gcd(s, M) = 1$ since primes dividing s are larger than $\log x$. Then by the definition of L, we can choose $M < q < M^L$ to be the smallest prime such that $sq = 1 \pmod{M}$. Since $q > M$ and the factors of s are all smaller than M, we have $\gcd(q, s) = 1$. With q, n both odd, the third condition follows from Lemma 26.

For a lower bound on $L_2^+(n)$ where $n = sq$ we count only the liars from primes $p \mid s$ with $(\Delta \mid p) = +1$. This gives

$$\prod_{p|s} L_2^{++}(n,p) = \prod_{p|s} \frac{1}{2}(\gcd(n-1,p-1)^2 - \gcd(n-1,p-1))$$

by Lemma 10. By construction, for $p \mid s$ we have $p-1 \mid M$ and $M \mid n-1$, so the product becomes

$$\begin{aligned} 2^{-k_\alpha^{(+)}(x)} \prod_{p|s}(p-1)(p-2) &\geq 2^{-k_\alpha^{(+)}(x)} \cdot s^{2-o(1)} \\ &\geq x^{-o(1)}\left((\log x)^{-k_\alpha^{(+)}(x)\epsilon(2-o(1))}\right)\frac{x^{2-o(1)}}{M^{L(2-o(1))}} \\ &\geq x^{-o(1)}x^{-\epsilon\cdot\frac{2}{\alpha}(1+o(1))}\frac{x^{2-o(1)}}{x^{o(1)}} = x^{2-\epsilon\frac{2}{\alpha}-o(1)}, \end{aligned}$$

where the upper bound on M comes from Proposition 20. □

In the minus one case we have two different divisibility conditions to satisfy, and as a result require two primes q_1 and q_2 to complete the composite number n.

Lemma 32. *Let L be an upper bound for Linnik's constant. Given any element s of $S_{\alpha,\epsilon}^{(-)}(x)$ there exists a number $q < M^{2L}$ such that*

- $sq = 1 \pmod{M_1}$,
- $sq = -1 \pmod{M_2}$,
- $\gcd(q, s) = 1$, *and*
- $\prod_{p|q} \frac{1}{2}\left(\gcd((sq)^2 - 1, p-1) - \gcd(sq-1, p-1)\right) > 0$.

Moreover, the number of liars of $n = sq$ with $(\Delta \mid n) = -1$ is at least

$$2^{-k_\alpha^{(-)}(x)} \prod_{p|s} \left(p^2 - 1\right) = x^{2-\epsilon\frac{2}{\alpha}-o(1)}$$

as $x \to \infty$.

Proof. We construct q as the product of two primes q_1 and q_2. Let ℓ_1, ℓ_2 be two distinct odd primes which divide M_2 and write $M_2 = M_2'\ell_1^{r_1}\ell_2^{r_2}$ where $\gcd(M_2', \ell_1\ell_2) = 1$. Choose q_1 to be the smallest prime greater than M satisfying the following four conditions:

$$\begin{aligned} sq_1 &= 1 \pmod{M_1}, & sq_1 &= -1 \pmod{M_2'}, \\ q_1 &= 1 \pmod{\ell_1^{r_1}}, & sq_1 &= -1 \pmod{\ell_2^{r_2}}, \end{aligned}$$

and choose q_2 to be the smallest prime greater than M satisfying the following four conditions:

$$\begin{aligned} q_2 &= 1 \pmod{M_1}, & q_2 &= 1 \pmod{M_2'}, \\ sq_2 &= -1 \pmod{\ell_1^{r_1}}, & q_2 &= 1 \pmod{\ell_2^{r_2}}. \end{aligned}$$

Note that $q_1, q_2 > M$ implies they are greater than any factor of s, and thus relatively prime to s, and $\gcd(s, M) = 1$ since primes dividing s are greater than $\log x$. Then q_1, q_2 exist due to the definition of Linnik's constant, with $q_1, q_2 < (M_1M_2'\ell_1^{r_1}\ell_2^{r_2})^L$ so that $q < M^{2L}$. Note $sq_1q_2 = 1 \pmod{M_1}$, which satisfies the first bulleted condition. In addition, $sq_1q_2 = -1 \pmod{M_2'}$, $sq_1q_2 = -1 \pmod{\ell_1^{r_1}}$, and $sq_1q_2 = -1 \pmod{\ell_2^{r_2}}$ so that $sq = -1 \pmod{M_2}$. For the fourth bullet point, $sq_1q_2 = -1 \pmod{\ell_1^{r_1}}$ and $q_1 = 1 \pmod{\ell_1^{r_1}}$ gives the result by Lemma 26.

To bound $L_2^-(n)$ we select only n where $(\Delta \mid p) = +1$ for all $p \mid q$ and $(\Delta \mid p) = -1$ for all $p \mid s$. By Lemma 15 we have

$$\begin{aligned}\prod_{p\mid s} L_2^{--}(n,p) &= \prod_{p\mid s} \frac{1}{2}\left(\gcd(p^2-1, n^2-1, n-p) - \gcd(n-1,p-1)\right)\\ &= 2^{-k_\alpha^{(-)}(x)} \prod_{p\mid s}(p^2-1)-(p-1),\end{aligned}$$

since by construction $p-1 \mid n-1$ and $p+1 \mid n+1$. This product is $x^{2-\epsilon\frac{2}{\alpha}-o(1)}$ by the same argument as that in Lemma 31. □

Proof of Theorems 27 *and* 28. In each case the theorem is an immediate consequence of the lower bounds on the number of liars for each value of $n = sq$ constructed in Lemma 31 or 32, together with the size of the set S under consideration.

More specifically, for each element s of $S_{\alpha,\epsilon}^{(\pm)}(x)$, by Lemma 31 or 32 we can associate a distinct number $n < x$ with $L_2^{\pm}(n) \geq x^{2-\epsilon\frac{2}{\alpha}-o(1)}$. For each of the plus, minus cases we have that

$$\left|S_{\alpha,\epsilon}^{(\pm)}(x)\right| \geq x^{1-\alpha^{-1}-o(1)}$$

for α satisfying as appropriate Proposition 21 or 22. We conclude that for all $\epsilon > 0$ and appropriately chosen α we have

$$\sum_{n<x} L_2^{\pm}(n) \geq x^{3-\alpha^{-1}-\epsilon\frac{2}{\alpha}-o(1)}.$$

Allowing ϵ to go to 0, we obtain the result. □

6. Upper bounds on the average number of degree-2 Frobenius pseudoprimes

Our proof will follow [EP86, Theorem 2.2] quite closely. First we need a key lemma, the proof of which follows a paper of Pomerance [Pom81, Theorem 1].

Notation. Given an integer m, define

$$\lambda(m) = \operatorname*{lcm}_{p\mid m}(p-1) \qquad \text{and} \qquad \lambda_2(m) = \operatorname*{lcm}_{p\mid m}(p^2-1).$$

Note that $\lambda(m)$ is not Carmichael's function, though it is equivalent when m is squarefree. Moreover, given $x > 0$ we shall define

$$\mathcal{L}(x) = \exp\left(\frac{\log x \log_3 x}{\log_2 x}\right),$$

where $\log_2 x = \log\log x$ and $\log_3 x = \log\log\log x$. Here log is the natural logarithm.

Lemma 33. *As $x \to \infty$ we have that*

$$\#\{m \leq x \ : \ \lambda_2(m) = n\} \leq x \cdot \mathcal{L}(x)^{-1+o(1)}.$$

Proof. For $c > 0$ we have

$$\sum_{\substack{m \le x \\ \lambda_2(m)=n}} 1 \le x^c \sum_{\lambda_2(m)=n} m^{-c} \le x^c \sum_{p|m \Rightarrow p^2-1|n} m^{-c} \le x^c \sum_{p|m \Rightarrow p-1|n} m^{-c}.$$

By the theory of Euler products, we can rewrite the sum as $\prod_{p-1|n}(1-p^{-c})^{-1}$. Call this product A. With $c = 1 - \frac{\log_3 x}{\log_2 x}$, the result follows if we can show that $\log A = o(\log x/\log_2 x)$.

Take x large enough so that $\frac{\log_3 x}{\log_2 x} \le \frac{1}{2}$; from this it follows that for all primes p, $\frac{1}{1-p^{-c}} \le 4$.

Following Pomerance in [Pom81, Theorem 1], via the Taylor series for $-\log(1-x)$ we can show that

$$\log A = \sum_{p-1|n} \frac{p^{-c}}{1-p^{-c}} \le 4 \sum_{d|n} d^{-c} \le 4 \prod_{p|n}(1-p^{-c})^{-1}$$

and similarly

$$\log\log A \le \log 4 + \sum_{p|n} \frac{p^{-c}}{1-p^{-c}} \le \log 4 + 4 \sum_{p|n} p^{-c}.$$

Since the sum is maximized with many small primes, an upper bound is

$$\log 4 + \sum_{p \le 4 \log x} 4p^{-c} = O\left(\frac{(\log x)^{1-c}}{(1-c)\log\log x}\right),$$

where the sum is evaluated using partial summation. With $c = 1 - \log_3 x/\log_2 x$ we achieve

$$\log\log A = O\left(\frac{\log_2 x}{\log_3 x}\right)$$

so that $\log A = o(\log x/\log_2 x)$, as requested. □

An interesting question is whether the upper bound in that lemma can be lowered. If so, a more clever upper bound would be required for the sum over primes p dividing m such that $p^2 - 1 \mid n$.

In [EP86, Theorem 2.2] the key idea is to parameterize composite n according to the size of the subgroup of Fermat liars, and then to prove a useful divisibility relation involving n. Here we reverse this strategy: we parameterize according to a divisibility condition and prove an upper bound on the size of the set of Frobenius liars.

Lemma 34. *Assume n is composite and let k be the smallest integer such that $\lambda_2(n) \mid k(n^2-1)$. Then*

$$L_2^-(n) \le \frac{1}{k} \prod_{p|n}(p^2-1).$$

Proof. We have $k = \lambda_2(n)/\gcd(\lambda_2(n), n^2-1)$. Our goal will be to show that

$$\frac{\lambda_2(n)}{\gcd(\lambda_2(n), n^2-1)} \prod_{p|n} \gcd(p^2-1, n^2-1) \Bigg| \prod_{p|n} p^2 - 1\ . \tag{1}$$

If this is true, then combined with Lemma 18 we have

$$L_2^-(n) \leq \prod_{p|n} \gcd(n^2-1, p^2-1) \leq \frac{1}{k} \prod_{p|n} p^2 - 1.$$

Fix arbitrary prime q and let q^{e_i} be the greatest power of q that divides $p_i^2 - 1$. Suppose we have ordered the r primes dividing n according to the quantity e_i. Let q^d be the power of q that divides $n^2 - 1$.

First consider the case where $d \geq e_r$, the largest of the e_i. Then q^{e_r} divides $\lambda_2(n)$ since it is defined as an lcm of the $p^2 - 1$, and q^{e_r} divides $\gcd(\lambda_2(n), n^2 - 1)$ since $d \geq e_r$. We are left with the observation that $\prod_{p|n} \gcd(p^2 - 1, n^2 - 1)$ is a divisor of $\prod_{p|n} p^2 - 1$, and thus in particular the q power divides.

Next consider the case where $d \geq e_i$ for $i \leq \ell$ and $d < e_i$ for $i > \ell$. Then q^{e_r} divides $\lambda_2(n)$ since it is defined as an lcm, and q^d divides $\gcd(\lambda_2(n), n^2 - 1)$ since $d < e_r$. The total power of q dividing the LHS is then $e_r - d + (\sum_{i=1}^{\ell} e_i) + (r - \ell)d$. We have

$$\begin{aligned}\left(\sum_{i=1}^{\ell} e_i\right) + e_r - d + d(r-\ell) &= \left(\sum_{i=1}^{\ell} e_i\right) + d(r-\ell-1) + (d + e_r - d) \\ &\leq \left(\sum_{i=1}^{\ell} e_i\right) + \left(\sum_{i=\ell+1}^{r-1} e_i\right) + e_r \\ &= \sum_{i=1}^{r} e_i,\end{aligned}$$

which is the power of q dividing $\prod p^2 - 1$. Since q was arbitrary, (1) holds, which finishes the proof. □

The result for $L_2^+(n)$ is similar. We do need a new piece of notation, namely given a prime p we shall define

$$d_n(p) = \begin{cases} (p-1)^2 & \text{if } \gcd(n-1, p-1)^2 > \gcd(n-1, p^2-1), \\ p^2 - 1 & \text{if } \gcd(n-1, p-1)^2 \leq \gcd(n-1, p^2-1). \end{cases}$$

Lemma 35. *Suppose n is composite and let k be the smallest integer such that $\lambda(n) \mid k(n-1)$. Then*

$$L_2^+(n) \leq \frac{1}{k} \prod_{p|n} d_n(p).$$

Proof. From Lemma 18 we know that

$$L_2^+(n) \leq \prod_{p|n} \max(\gcd(n-1, p^2-1), \gcd(n-1, p-1)^2),$$

and from the definition of k we know that k is exactly $\lambda(n)/\gcd(\lambda(n), n-1)$. It thus suffices to show that

$$\frac{\lambda(n)}{\gcd(\lambda(n), n-1)} \prod_{p|n} \max(\gcd(n-1, p^2-1), \gcd(n-1, p-1)^2) \;\Bigg|\; \prod_{p|n} d_n(p). \tag{2}$$

For an arbitrary prime q, let q^{e_i} be the power of q dividing $d_n(p)$, and let q^d be the power of q dividing $n - 1$. Order the e_i, and suppose that $d \geq e_i$ for $i \leq \ell$ and

$d < e_i$ for $i > \ell$. Then the exponent of q dividing $\prod_{p|n} d_n(p)$ is $\sum_{i=1}^r e_i$. Following the same argument as in Lemma 34, the exponent of q dividing the left-hand side of (2) is

$$(e_r - d) + \left(\sum_{i=1}^{\ell} e_i\right) + (r-\ell)d \le \sum_{i=1}^{r} e_i.$$

Since q was arbitrary, the division in (2) holds. □

Theorem 36. *As $x \to \infty$ we have that*

$$\sum_{n\le x}{}' L_2(n) \le x^3 \mathcal{L}(x)^{-1+o(1)},$$

where $\sum'$ signifies that the sum is only over composite integers.

Proof. Let $C_k(x)$ denote the set of composite $n \le x$ where k is the smallest integer such that $\lambda(n) \mid k(n-1)$, and let $D_k(x)$ denote the set of composite $n \le x$ where k is the smallest integer such that $\lambda_2(n) \mid k(n^2-1)$. By Lemma 34, if $n \in D_k(x)$, then $L_2^-(n) \le n^2/k$. Similarly, by Lemma 35, if $n \in C_k(x)$, then $L_2^+(n) \le n^2/k$. Then

$$\begin{aligned}
\sum_{n\le x}{}' L_2(n) &= \sum_{n\le x}{}' L_2^+(n) + L_2^-(n) \\
&= \sum_k \sum_{n\in C_k(x)} L_2^+(n) + \sum_k \sum_{n\in D_k(x)} L_2^-(n) \\
&\le \sum_k \sum_{n\in C_k(x)} \frac{n^2}{k} + \sum_k \sum_{n\in D_k(x)} \frac{n^2}{k} \\
&\le \sum_{n\le x} \frac{n^2}{\mathcal{L}(x)} + \sum_{k\le\mathcal{L}(x)} \sum_{n\in C_k(x)} \frac{n^2}{k} + \sum_{n\le x} \frac{n^2}{\mathcal{L}(x)} + \sum_{k\le\mathcal{L}(x)} \sum_{n\in D_k(x)} \frac{n^2}{k} \\
&= \frac{2x^3}{\mathcal{L}(x)} + x^2 \sum_{k\le\mathcal{L}(x)} \frac{|C_k(x)|}{k} + x^2 \sum_{k\le\mathcal{L}(x)} \frac{|D_k(x)|}{k},
\end{aligned}$$

and thus the proof is complete if we can prove that $|C_k(x)| \le x\mathcal{L}(x)^{-1+o(1)}$ and $|D_k(x)| \le x\mathcal{L}(x)^{-1+o(1)}$ hold uniformly for $k \le \mathcal{L}(x)$.

We focus first on the $D_k(x)$ result. For every $n \in D_k(x)$, either

(1) $n \le x/\mathcal{L}(x)$,
(2) n is divisible by some prime $p > \sqrt{k\mathcal{L}(x)}$, and/or
(3) $n \ge x/\mathcal{L}(x)$ and $p \mid n$ implies $p \le \sqrt{k\mathcal{L}(x)}$.

The number of integers in case (1) is at most $x\mathcal{L}(x)^{-1}$ by assumption.

Turning to case (2), if $n \in D_k(x)$ and $p \mid n$, then p^2-1 is a divisor of $\lambda_2(n)$ and hence of $k(n^2-1)$. This means that

$$\left.\frac{p^2-1}{\gcd(k,p^2-1)}\,\right|\, n^2-1.$$

A straightforward application of the Chinese remainder theorem shows that the count of residues $x \pmod a$ with $x^2 = 1 \pmod a$ is at most $2^{\omega(a)+1}$ (for example, there are at most 4 when working modulo 8). Thus the count of $n \in D_k(x)$ with $p \mid n$ is at most

$$\left\lceil \frac{2x2^{\omega(p^2-1)}}{p(p^2-1)/\gcd(p^2-1,k)} \right\rceil \leq \frac{2xk2^{\omega(p^2-1)}}{p(p^2-1)} = \frac{xk\mathcal{L}(x)^{o(1)}}{p(p^2-1)}.$$

The equality $2^{\omega(p^2-1)+1} = \mathcal{L}(x)^{o(1)}$ follows from the fact that the maximum number of distinct prime factors dividing any integer $m \leq x^2$ is $(1+o(1))\log(x^2)/\log\log(x^2)$ (see the proof of Proposition 23 for the previous instance of this fact). We conclude that the maximum number of n in case (2) is

$$\sum_{p>\sqrt{k\mathcal{L}(x)}} \frac{2xk\mathcal{L}(x)^{o(1)}}{p^3} \leq xk\mathcal{L}(x)^{o(1)} \sum_{p>\sqrt{k\mathcal{L}(x)}} \frac{1}{p^3} = x\mathcal{L}(x)^{-1+o(1)}.$$

For n in case (3), since all primes dividing n are small we know that n has a divisor d satisfying

$$\frac{x}{\mathcal{L}(x)\sqrt{k\mathcal{L}(x)}} < d \leq \frac{x}{\mathcal{L}(x)}.$$

To construct such a divisor, remove primes from n until the remaining integer is smaller than $x/\mathcal{L}(x)$; since each prime dividing n is at most $\sqrt{k\mathcal{L}(x)}$, the lower bound follows. Let A be the set of $d \in \mathbb{Z}$ that fall between the bounds given. We have $\lambda_2(d) \mid \lambda_2(n) \mid k(n^2-1)$, and so by a similar argument we know that the number of $n \in D_k(x)$ with $d \mid n$ is at most

$$\frac{x\mathcal{L}(x)^{o(1)}}{d\lambda_2(d)/\gcd(k,\lambda_2(d))}.$$

Unlike the case where d is prime, here we might have $\gcd(d,\lambda_2(d)) \neq 1$. But then the set of $n \in D_k(x)$ with $d \mid n$ is empty, so the bound given remains true.

Now, the number of $n \in D_k(x)$ in case (3) is at most

$$\begin{aligned}\sum_{d\in A} \frac{x\mathcal{L}(x)^{o(1)}\gcd(k,\lambda_2(d))}{d\lambda_2(d)} &= x\mathcal{L}(x)^{o(1)} \sum_{d\in A} \frac{\gcd(k,\lambda_2(d))}{d\lambda_2(d)} \\ &= x\mathcal{L}(x)^{o(1)} \sum_{m\leq x} \frac{1}{m} \sum_{\substack{d\in A \\ \lambda_2(d)/\gcd(k,\lambda_2(d))=m}} \frac{1}{d} \\ &\leq x\mathcal{L}(x)^{o(1)} \sum_{m\leq x} \frac{1}{m} \sum_{u\mid k} \sum_{\substack{d\in A \\ \lambda_2(d)=mu}} \frac{1}{d}.\end{aligned}$$

Note that if $\lambda_2(d)/\gcd(k,\lambda_2(d)) = m$, then $\lambda_2(d) = mu$ for some $u \mid k$, and thus summing over all $u \mid k$ gives an upper bound.

To evaluate the inner sum we use partial summation and Lemma 33 to get

$$\begin{aligned}\sum_{\substack{d\in A \\ \lambda_2(d)=mu}} \frac{1}{d} &\leq \frac{1}{x/\mathcal{L}(x)} \sum_{\substack{d\in A \\ \lambda_2(d)=mu}} 1 + \int_{x/\mathcal{L}(x)\sqrt{k\mathcal{L}(x)}}^{x/\mathcal{L}(x)} \frac{1}{t^2} \sum_{\substack{d<t \\ \lambda_2(d)=mu}} 1 \,\mathrm{d}t \\ &\leq \frac{\mathcal{L}(x)}{x} \frac{x/\mathcal{L}(x)}{\mathcal{L}(x/\mathcal{L}(x))^{1+o(1)}} + \int_{x/\mathcal{L}(x)\sqrt{k\mathcal{L}(x)}}^{x/\mathcal{L}(x)} \frac{1}{t^2} \frac{t}{\mathcal{L}(t)^{1+o(1)}} \,\mathrm{d}t \\ &\leq \frac{1}{\mathcal{L}(x/\mathcal{L}(x))^{1+o(1)}} + \frac{\log x}{\mathcal{L}(x/\mathcal{L}(x)\sqrt{k\mathcal{L}(x)})} = \mathcal{L}(x)^{-1+o(1)}\end{aligned}$$

for large enough x and uniformly for $k \leq \mathcal{L}(x)$. Note that the count of divisors of an integer k is bounded above by $2^{(1+o(1))\log k/\log\log k}$ (see for instance [HW08, Theorem 317]). Thus the count in case (3) is

$$\frac{x}{\mathcal{L}(x)^{1+o(1)}}\sum_{m\leq x}\frac{1}{m}\sum_{u|k}1 \leq \frac{x\log x}{\mathcal{L}(x)^{1+o(1)}}2^{(1+o(1))\frac{\log k}{\log\log k}} = \frac{x}{\mathcal{L}(x)^{1+o(1)}}$$

uniformly for $k \leq \mathcal{L}(x)$ and large enough x.

Proving that $|C_k(x)| \leq x\mathcal{L}(x)^{-1+o(1)}$ uniformly for $k \leq \mathcal{L}(x)$ will be similar. Here the three cases are:

(1) $n \leq x/\mathcal{L}(x)$,
(2) n is divisible by some prime $p > k\mathcal{L}(x)$, and
(3) $n \geq \mathcal{L}(x)$ and $p \mid n$ implies $p \leq k\mathcal{L}(x)$.

If $n \in C_k(x)$, then $\lambda(n) \mid k(n-1)$. Thus the number of $n \in C_k(x)$ with $p \mid n$ is at most

$$\left\lceil \frac{x}{p(p-1)/\gcd(p-1,k)} \right\rceil \leq \frac{xk}{p^2},$$

and so the count of n in case (2) is $x\mathcal{L}(x)^{-1+o(1)}$.

For n in case (3) we know n has a divisor d satisfying

$$\frac{x}{k\mathcal{L}(x)^2} < d \leq \frac{x}{\mathcal{L}(x)},$$

and so the bound of $x\mathcal{L}(x)^{-1+o(1)}$ follows exactly from case (3) of [EP86, Theorem 2.2]. □

7. Conclusions and further work

A very naive interpretation of Theorems 2 and 3 is that for any given f, you should expect that there are n for which f is a liar. Moreover, one expects to find this in both the $+1$ and -1 cases. Likewise, one expects that given n, there will exist f which is a liar in both the $+1$ and -1 cases. To emphasize the extent to which one should be careful with the careless use of the word "expect" we remind the reader that in Section 3.4 we describe infinite families of n for which $L_2^-(n) = 0$. It would be interesting to know how often $L_2^-(n)$ vanishes for $n < x$.

It is useful to note that this vanishing described in Section 3.4 gives some heuristic evidence to suggest that the Baillie-PSW test is significantly more accurate than other primality tests. Further work to make these heuristics more precise may be worth pursuing.

In contrast to the above, the proof of Theorem 3 suggests that one should expect there to exist many Frobenius–Carmichael numbers (see [Gra01, Section 6] for a definition) relative to quadratic fields K for which $(n \mid \delta_K) = -1$. It is likely that this heuristic can be extended to show that for each fixed quadratic field K there exist infinitely many Frobenius–Carmichael numbers n relative to K with $(n \mid \delta_K) = -1$. A result of this form would be a nice extension of [Gra10], which proved infinitely many Frobenius–Carmichael numbers n for which $(n \mid \delta_K) = 1$. As such a number would also be a classical Carmichael number, such numbers would tend to lead to a failure of the Baillie–PSW test. If this could be done for all K it would show that all f admit n for which f is a liar and the Jacobi symbol is -1. It remains an open problem to prove that such numbers exist.

It remains unclear from our results if the expected value of $L_2^-(n)$ is actually less (in an asymptotic sense) than the expected value of $L_2^+(n)$. Various heuristics suggest that it ought to be the case. A result of this sort would put further weight behind the Baillie–PSW test.

Acknowledgments

The authors would like to thank Carl Pomerance for several comments which improved the results presented.

References

[BH98] R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), no. 4, 331–361.

[BW80] R. Baillie and S. S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), no. 152, 1391–1417.

[DMT01] C. Dartyge, G. Martin, and G. Tenenbaum, *Polynomial values free of large prime factors*, Period. Math. Hungar. **43** (2001), no. 1-2, 111–119.

[EP86] P. Erdős and C. Pomerance, *On the number of false witnesses for a composite number*, Math. Comp. **46** (1986), no. 173, 259–279.

[Gra01] J. Grantham, *Frobenius pseudoprimes*, Math. Comp. **70** (2001), no. 234, 873–891.

[Gra10] J. Grantham, *There are infinitely many Perrin pseudoprimes*, J. Number Theory **130** (2010), no. 5, 1117–1128.

[Guy04] R. K. Guy, *Unsolved Problems in Number Theory*, third ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004.

[How00] E. W. Howe, *Higher-order Carmichael numbers*, Math. Comp. **69** (2000), no. 232, 1711–1719.

[HW08] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, sixth ed., Oxford University Press, Oxford, 2008, revised by D. R. Heath-Brown and J. H. Silverman, with a foreword by Andrew Wiles.

[Lan02] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[Mon80] L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoret. Comput. Sci. **12** (1980), no. 1, 97–108.

[Pom81] C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), no. 156, 587–593.

[PSW80] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), no. 151, 1003–1026.

[Xyl11] T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, Bonner Mathematische Schriften [Bonn Mathematical Publications], 404, Universität Bonn, Mathematisches Institut, Bonn, 2011, dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn, Bonn, 2011.

Department of Mathematics and Computer Science, University of Lethbridge, C526 University Hall, 4401 University Drive, Lethbridge, Alberta, T1K 3M4, Canada
Email address: andrew.fiori@uleth.ca

Department of Mathematics, Illinois Wesleyan University, 1312 Park Street, Bloomington, Illinois 61701
Email address: ashallue@iwu.edu