There are Infinitely Many Perrin Pseudoprimes

Jon Grantham

Institute for Defense Analyses
Center for Computing Sciences
17100 Science Drive, Bowie, MD 20715

Abstract

This paper proves the existence of infinitely many Perrin pseudoprimes, as conjectured by Adams and Shanks in 1982. The theorem proven covers a general class of pseudoprimes based on recurrence sequences. The result uses ingredients of the proof of the infinitude of Carmichael numbers, along with zero-density estimates for Hecke L-functions.

Key words:
2000 MSC: 11Y11, 11N13, 11N25

1. Introduction

The search for fast primality tests has led to the examination of the generalization of the Fermat probable prime test: n is a probable prime if $2^{n-1} \equiv 1 \bmod n$. This test, and its generalizations, requires $O(\log n)$ multiplications. If such a generalization could be found with a finite list of exceptions (pseudoprimes), we would have a primality test which runs deterministically in time $\tilde{\mathrm{O}}(\log^2 n)$. (Recall that $\tilde{\mathrm{O}}$ is an extension to the O notation that ignores factors that are bounded by a fixed power of the logarithm.) By contrast, the Agrawal-Kayal-Saxena test [2] has recently been improved to $\tilde{\mathrm{O}}(\log^6 n)$ [16]. Non-deterministic variants of the AKS test [4], [5] have running time of $\tilde{\mathrm{O}}(\log^4 n)$; the same can be achieved heuristically for the ECPP test [19]. Although ECPP is the fastest method in practice, it is not proven to be in (random) polynomial time.

The Fermat test can be generalized in many ways, which fall into two broad categories. By thinking of it in terms of the first-order recurrence sequence defined by $a_{n+1} = 2a_n$, $a_0 = 1$, we can generalize to congruences on higher-order recurrence sequences. This approach is more traditional. Alternatively, one can think of the Fermat criterion as the extent to which the ring of integers mod n resembles a finite field. In that way, we can generalize to higher-degree finite fields. The latter approach was favored in the author's dissertation [9], Chapter 4 of which contained an earlier version of the results of this paper.

Email addresses: grantham@super.org (Jon Grantham)

In a 1982 paper [1], Adams and Shanks introduced a probable primality test based on third-order recurrence sequences, which they called the Perrin test. They asked if there are infinitely many Perrin pseudoprimes. They answered the question, "Almost certainly yes, but we cannot prove it. Almost certainly, there are infinitely many [Carmichael numbers which are Perrin pseudoprimes], and yet it has never been proved that there are infinitely many Carmichael numbers."

Carmichael numbers are composites which satisfy $a^{n-1} \equiv 1 \bmod n$ for all $(a, n) = 1$. The Carmichael question has been resolved [3]. The techniques of that proof can be combined with results about Hecke L-functions to show that there are infinitely many Perrin pseudoprimes. In fact, the main result of this paper applies to a more general class of pseudoprimes, including Lucas and Lehmer pseudoprimes.

2. Background

The following is a version of the Perrin test.

Consider sequences $A_n = A_n(r, s)$ defined by the following relations: $A_{-1} = s$, $A_0 = 3$, $A_1 = r$, and $A_n = rA_{n-1} - sA_{n-2} + A_{n-3}$. Let $f(x) = x^3 - rx^2 + sx - 1$ be the associated polynomial and Δ its discriminant. (Perrin's sequence is $A_n(0, -1)$.)

Definition. *The* **signature mod** m *of an integer* n *with respect to the sequence* $A_k(r, s)$ *is the* 6*-tuple* $(A_{-n-1}, A_{-n}, A_{-n+1}, A_{n-1}, A_n, A_{n+1}) \bmod m$.

Definitions. *An integer* n *is said to have an* **S-signature** *if its signature mod* n *is congruent to* $(A_{-2}, A_{-1}, A_0, A_0, A_1, A_2)$.

An integer n *is said to have a* **Q-signature** *if its signature mod* n *is congruent to* (A, s, B, B, r, C)*, where for some integer* a *with* $f(a) \equiv 0 \bmod n$*,* $A \equiv a^{-2} + 2a$*,* $B \equiv -ra^2 + (r^2 - s)a$*, and* $C \equiv a^2 + 2a^{-1}$.

An integer n *is said to have an* **I-signature** *if its signature mod* n *is congruent to* (r, s, D', D, r, s)*, where* $D' + D \equiv rs - 3$ *mod* n *and* $(D' - D)^2 \equiv \Delta$.

Definition. *A* **Perrin pseudoprime** *with parameters* (r, s) *is an odd composite* n *such that either*

1) $\left(\frac{\Delta}{n}\right) = 1$ *and* n *has an S-signature or an I-signature, or*

2) $\left(\frac{\Delta}{n}\right) = -1$ *and* n *has a Q-signature.*

The concept of Perrin pseudoprime can be generalized [10] to that of a Frobenius pseudoprime. Briefly, a Frobenius pseudoprime with respect to $f(x)$ is a composite for which $\mathbb{Z}[x]/(n, f(x))$ exhibits properties similar to that of a true finite field. Most pseudoprime tests based on recurrence sequences can be treated as special cases.

Definition. *Let* $f(x) \in \mathbb{Z}[x]$ *be a monic polynomial of degree* d *with discriminant* Δ*. An odd composite* $n > 1$ *is said to be a* **Frobenius pseudoprime** *with respect to* $f(x)$ *if* $(n, f(0)\Delta) = 1$*, and it is declared to be a probable prime by the following algorithm. All computations are done in* $(\mathbb{Z}/n\mathbb{Z})[x]$.

Factorization Step *Let* $f_0(x) = f(x) \bmod n$. *For* $1 \leq i \leq d$, *let* $F_i(x) = \text{gcmd}(x^{n^i} - x, f_{i-1}(x))$ *and* $f_i(x) = f_{i-1}(x)/F_i(x)$. *If any of the* gcmd*s fail to exist, declare* n *to be composite and stop. If* $f_d(x) \neq 1$, *declare* n *to be composite and stop.*

Frobenius Step *For* $2 \leq i \leq d$, *compute* $F_i(x^n) \bmod F_i(x)$. *If it is nonzero for some* i, *declare* n *to be composite and stop.*

Jacobi Step *Let* $S = \sum_{2|i} deg(F_i(x))/i$.

If $(-1)^S \neq \left(\frac{\Delta}{n}\right)$, *declare* n *to be composite and stop.*

If n *has not been declared composite, declare* n *to be a Frobenius probable prime.*

(The gcmd of two polynomials is the greatest common monic divisor; see [10] for a full treatment.)

Haddad [12] has shown that cubic variant of this test has running times which track well with asymptotics when implemented with Arjen Lenstra's Large Integer Package.

The following general result gives the infinitude of Perrin pseudoprimes as a corollary.

Theorem 2.1. *Let* $f(x) \in \mathbb{Z}[x]$ *be a monic, squarefree polynomial with splitting field* K. *There are infinitely many Frobenius pseudoprimes with respect to* $f(x)$. *In fact, there are* $\gg N^c$ *Carmichael-Frobenius numbers with respect to* K *which are less than* N, *for some* $c = c(K) > 0$.

A Carmichael-Frobenius number is a Frobenius pseudoprime with respect to all polynomials with splitting field K (a Carmichael number is thus a Carmichael-Frobenius number with respect to $\mathbb{Q}$). Proving the theorem for the general case allows specialization to other cases. The constant $c(K)$ can, in principle, be made effective.

In particular, the results of [10] combined with Theorem 2.1 show that there are infinitely many Perrin pseudoprimes, if we take $f(x) = x^3 - x - 1$. Gurak [11] defines pseudoprimes using congruences for higher-order recurrence sequences. Szekeres [20] defines pseudoprimes with respect to a polynomial as those for which every symmetric polynomial of its roots is invariant under the map $x \mapsto x^n$. From [10], we have that there are infinitely many pseudoprimes in the senses of both Gurak and Szekeres.

By Proposition 6.1 of [10], in order to prove Theorem 2.1, it suffices to show that there are infinitely many Carmichael numbers n, such that for all $p|n$, $f(x)$ splits completely mod p. The proof will involve modifying the construction in [3] to ensure that each of the prime factors of the Carmichael numbers constructed has this property.

The main result that will be used in this proof is a version of the "prime ideal theorem for arithmetic progressions" that gives a uniform error term, except for a possible exceptional progression arising from a Siegel zero.

3. Distribution of Primes

Theorems about the distribution of primes in arithmetic progressions are traditionally proved using Dirichlet characters — homomorphisms from the integers mod q to the complex roots of unity. (The map is defined to be zero on integers not coprime to q.) Because we want to prove a theorem about primes in a particular arithmetic progression which split completely, we employ a slightly different sort of Dirichlet character.

We recall the definitions of [15].

Definitions. *Let K be an algebraic number field and $\mathfrak{O}_K$ its ring of integers. A* **cycle** *of K is a formal product $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$ extending over all of the primes of K, where the $m(\mathfrak{p})$ are nonnegative integers, almost all 0, with $m(\mathfrak{p}) = 0$ for complex $\mathfrak{p}$ and $m(\mathfrak{p}) \leq 1$ for real $\mathfrak{p}$. Let $\mathfrak{I}$ be the group of fractional ideals of $\mathfrak{O}_K$. Let $\mathfrak{I}(\mathfrak{m})$ be the subgroup of $\mathfrak{I}$ generated by the finite primes $\mathfrak{p}$ for which $m(\mathfrak{p}) = 0$. Let $P_{\mathfrak{m}}$ be the subgroup of $\mathfrak{I}(\mathfrak{m})$ generated by the nonzero ideals of the form $\mathfrak{O}_K\alpha$, where $\alpha \in \mathfrak{O}_K$ is such that $\alpha \equiv 1 \bmod \mathfrak{p}^{m(\mathfrak{p})}$ for each finite prime $\mathfrak{p}$, and $\alpha > 0$ under each embedding of K in the field of real numbers corresponding to a real prime $\mathfrak{p}$ with $m(\mathfrak{p}) = 1$. The* **norm** *of a cycle $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$ is the number $N(\mathfrak{m}) = \prod N(\mathfrak{p})^{m(\mathfrak{p})}$, where $\mathfrak{p}$ in the second product ranges over only the finite primes, and $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$ in K.*

A **Dirichlet character of** *K is a pair consisting of a cycle $\mathfrak{m}$ of K and a group homomorphism $\chi : \mathfrak{I}(\mathfrak{m}) \mapsto \mathbb{C}^*$ such that $P_{\mathfrak{m}}$ is contained in the kernel. We call $\mathfrak{m}$ the* **modulus** *of χ.*

Given two Dirichlet characters χ and χ' with moduli $\mathfrak{m}$ and $\mathfrak{m}'$, we say that χ is **induced** *by χ' if $\mathfrak{m}'(\mathfrak{p}) \leq \mathfrak{m}(\mathfrak{p})$ for all $\mathfrak{p}$ and χ is the composition of the inclusion $\mathfrak{I}(\mathfrak{m}) \subset \mathfrak{I}(\mathfrak{m}')$ with χ'. A Dirichlet character is* **primitive** *if it is not induced by any character other than itself. The modulus of the unique primitive character inducing a Dirichlet character χ is called the* **conductor** *of χ.*

For a Dirichlet character χ of K, $L(s, \chi)$ is $\sum \chi(\mathfrak{i})N(\mathfrak{i})^{-s}$, where the sum is over the nonzero ideals of the ring of integers of K and $\operatorname{Re} s > 1$. This sum is absolutely convergent, and $L(s, \chi')$ can be extended to a meromorphic function on the complex plane. It has a simple pole at $s = 1$ if χ' is principal and is holomorphic otherwise.

Let K be the splitting field of f, $n = [K : \mathbb{Q}]$, and $d = \operatorname{disc}(K)$. Let χ be a Dirichlet character mod q (in the traditional sense). We associate to it a Dirichlet character of K in the following way.

Given an ideal $\mathfrak{i} \subset \mathfrak{O}_K$, let $\chi'(\mathfrak{i}) = \chi(N(\mathfrak{i}))$. Then χ' is an example of a Dirichlet character of K with conductor dividing $N(q)$.

Let $\Psi(x, \chi') = \sum_{N(\mathfrak{i})<x} \chi'(\mathfrak{i})\Lambda(\mathfrak{i})$, where $\Lambda(\mathfrak{i}) = \log N(\mathfrak{p})$ if $\mathfrak{i} = \mathfrak{p}^k$ for some prime ideal $\mathfrak{p}$, and 0 otherwise. Then

$$\frac{1}{\phi(q)} \sum_{\chi \bmod q} \bar{\chi}(a)\Psi(x, \chi') = \sum_{\substack{N(\mathfrak{i})<x \\ N(\mathfrak{i}) \equiv a \bmod q}} \Lambda(\mathfrak{i}).$$

We will prove some results about $L(s,\chi')$ that enable us to obtain results about $\Psi(x,\chi')$, and thus about the distribution of primes that split completely in K and lie in a particular residue class.

Lemma 3.1. *Fix a number field K. Let χ be a* **real** *Dirichlet character of $K \bmod \mathfrak{m}$. Let $M = N(\mathfrak{m})$. Let s be a real number in the range $2 > s > 1$. If χ is principal, then*

$$\frac{L'}{L}(s,\chi) > -\frac{1}{s-1} - c_1 \log 2M,$$

for some $c_1 > 0$, depending on K. If χ is non-principal, and if $L(s,\chi)$ has some real zero $\rho > 0$,

$$\frac{L'}{L}(s,\chi) > \frac{1}{s-\rho} - c_1 \log 2M,$$

and

$$\frac{L'}{L}(s,\chi) > -c_1 \log 2M,$$

if it has no real zero.

Proof. Assume χ is non-principal. From equation (5.9) of [17],

$$\frac{L'}{L}(s,\chi) = B(\chi) + \sum_\rho \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{2}\log A(\chi) - \frac{\gamma_\chi'}{\gamma_\chi}(s),$$

where the sum is over all the non-trivial zeroes of $L(s,\chi)$, $A(\chi) = dM$, $d = \operatorname{disc}(K)$, and $\gamma_\chi(s) = \left[\pi^{-\frac{s+1}{2}}\Gamma\left(\frac{s+1}{2}\right)\right]^b \left[\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\right]^a$ for nonnegative integers a and b depending on χ such that $a + b = n = [K:\mathbb{Q}]$. The exact dependence, described in [17], is irrelevant here.

The $\log A(\chi)$ term can be bounded because $\log A(\chi) = \log dM \ll \log 2M$.

$B(\chi)$ is defined implicitly in [17]. By Lemma 5.1 of that paper, we have

$$B(\chi) = -\operatorname{Re}\sum_\rho \frac{1}{\rho}.$$

We have from Lemma 5.3 of [17] that

$$\left|\frac{\gamma_\chi'}{\gamma_\chi}(s)\right| \ll n\log(s+2),$$

where the implied constant is absolute.

Thus $\frac{L'}{L}(s,\chi) > \sum_\rho \operatorname{Re}\frac{1}{s-\rho} - c_1\log 2M$, for some $c_1 > 0$. We have that $\operatorname{Re}\frac{1}{s-\rho} = \frac{s-\operatorname{Re}\rho}{|s-\rho|^2} > 0$, so we can omit any part of the sum. We omit anything but one possible real zero.

Thus

$$\frac{L'}{L}(s,\chi) > \frac{1}{s-\rho} - c_1 \log 2M,$$

if $L(s,\chi)$ has a real zero ρ, and

$$\frac{L'}{L}(s,\chi) > -c_1 \log 2M,$$

independent of the existence of real zeros.

Now assume χ is principal. From (5.9) of [17]

$$\frac{L'}{L}(s,\chi) = \sum_\rho \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) - \frac{1}{s} - \frac{1}{s-1} - \frac{1}{2}\log A(\chi) + \frac{\gamma_\chi'}{\gamma_\chi}(s).$$

By the same arguments as in the non-principal case (and the fact that $\frac{1}{s} < 1$), we have that

$$\frac{L'}{L}(s,\chi) > -\frac{1}{s-1} - c_1 \log 2M.$$

□

The following version of the Landau-Page Lemma for Dirichlet L-functions over a number field shows that there is at most one "Siegel zero" for characters of a bounded modulus.

Lemma 3.2. *Given a number field K, there is a computable constant $c_2 > 0$, depending on K, such that for all $T \geq 2$, there is at most one primitive character χ_1 with modulus $\mathfrak{m}$, $1 \leq N(\mathfrak{m}) < T$ for which $L(s,\chi_1)$ has a zero $\beta_1 + i\gamma_1$ satisfying $\beta_1 \geq 1 - c_2/\log T$ and $|\gamma_1| < T$.*

Proof. We follow the proof in [6], p. 94.

Lemma 3.5 of [15] allows us to consider only real zeros of real non-principal characters.

Let χ_1 and χ_2 be primitive characters mod $\mathfrak{m}_1$ and $\mathfrak{m}_2$, respectively, where $N(\mathfrak{m}_1)$ and $N(\mathfrak{m}_2)$ are at most T.

Consider the expression

$$-\frac{L'}{L}(s,\chi_0) - \frac{L'}{L}(s,\chi_1) - \frac{L'}{L}(s,\chi_2) - \frac{L'}{L}(s,\chi_1\chi_2),$$

where χ_0 is the principal character modulo the gcd of $\mathfrak{m}_1$ and $\mathfrak{m}_2$. (We define $\gcd(\prod \mathfrak{p}^{m_1(\mathfrak{p})}, \prod \mathfrak{p}^{m_2(\mathfrak{p})}) = \prod \mathfrak{p}^{\min(m_1(\mathfrak{p}),m_2(\mathfrak{p}))}$.) This expression is equal to

$$\sum \Lambda(\mathfrak{i})(\chi_0(\mathfrak{i}) + \chi_1(\mathfrak{i}))(\chi_0(\mathfrak{i}) + \chi_2(\mathfrak{i}))N(\mathfrak{i})^{-s} > 0, \tag{1}$$

for $\operatorname{Re} s > 1$.

Assume that $L(s,\chi_1)$ and $L(s,\chi_2)$ have real zeros, β_1 and β_2 respectively. Applying the previous lemma to (1) for real $s > 1$, we obtain

$$-\frac{1}{s-\beta_1} - \frac{1}{s-\beta_2} + \frac{1}{s-1} + c_3 \log T > 0,$$

for some $c_3 > 0$ depending on K, but not T. Rearranging, we get

$$\frac{1}{s-\beta_1} + \frac{1}{s-\beta_2} < \frac{1}{s-1} + c_3 \log T.$$

Let $c_2 = \frac{1}{6c_3}$ and assume that each $\beta_i \geq 1 - \frac{c_2}{\log T}$.
Taking $s = 1 + 3c_2/\log T$ gives us $\frac{1}{s-\beta_i} \geq \frac{\log T}{4c_2}$ and $\frac{1}{s-1} = \frac{\log T}{3c_2}$.
We now have that

$$\frac{\log T}{2c_2} < \frac{\log T}{3c_2} + c_3 \log T.$$

Simplifying, we get $\frac{1}{6c_2} < c_3$. Substituting the value of c_2 gives the desired contradiction. □

For each Dirichlet character χ of a field K and real numbers σ, T, in the ranges $\frac{1}{2} \leq \sigma \leq 1$, $T \geq 0$, let $N(\sigma, T, \chi)$ be the number of zeros $s = \beta + i\gamma$ of the Dirichlet L-function $L(s, \chi)$ inside the box $\sigma < \beta < 1$ and $|\gamma| < T$. Let $\mathcal{A}$ be the set of real numbers $A > 2$ for which there exists a number $C_A \geq 1$, such that for all $\sigma \geq 1 - \frac{1}{A}$ and $T \geq 1$, we have

$$N(\sigma, T, \mathfrak{m}) := \sum_{\chi \bmod \mathfrak{m}} N(\sigma, T, \chi) \leq C_A (N(\mathfrak{m}) T^n)^{A(1-\sigma)},$$

for all moduli $\mathfrak{m}$.

Hilano [14] has shown that every $A \geq 2890$ is in $\mathcal{A}$. The existence of such an A was first shown by Fogels [7].

Theorem 3.3. *Let K be a number field. For any given $\epsilon > 0$, there exist numbers x_ϵ, $\eta_\epsilon > 0$, and an integer $q_\epsilon(x)$, all depending on K, such that whenever $x \geq x_\epsilon$ and $x^{1/2} < y < x$,*

$$\left| \sum_{\substack{N(\mathfrak{i}) < y \\ N(\mathfrak{i}) \equiv a \bmod q}} \Lambda(\mathfrak{i}) - \frac{y}{\phi(q)} \right| \leq \epsilon \frac{y}{\phi(q)}$$

for all integers q not divisible by $q_\epsilon(x)$, with $(a, q) = 1$ and q in the range $1 \leq q \leq x^{\eta_\epsilon}$. Furthermore $q_\epsilon(x) > \log x$.

Proof. Let $\nu = 3 \log(36 C_A/\epsilon)$. Let $\eta_\epsilon = \min(\frac{1}{8An^2}, \frac{c_2}{n\nu})$. We can require $x_\epsilon > \max(e^{4A\nu/\eta_\epsilon}, 18(C_A/\epsilon)^{2/\eta_\epsilon})$.

We can deduce the following explicit formula from [15], proof of Theorem 3.1: (equations 3.2, 3.3 and the equation following the "Hence" on p. 493).

$$\begin{aligned} \sum_{\substack{N(\mathfrak{a}) < y \\ N(\mathfrak{a}) \equiv a \bmod q}} \Lambda(\mathfrak{a}) = \frac{y}{\phi(q)} - \frac{1}{\phi(q)} \sum_{\chi \bmod q} \bar{\chi}(a) \sum_{\substack{L(\beta+i\gamma, \chi) = 0 \\ \beta \geq 1/2, |\gamma| \leq T}} \frac{y^{\beta+i\gamma}}{\beta + i\gamma} + \\ O\Big(n \log y + n \frac{y \log y (\log y + \log dq + \log T)}{T} + \\ n \log dq + n y^{\frac{1}{2}} \log y (\log q + \log y) \Big). \end{aligned} \tag{2}$$

We have that $\eta_\epsilon < 1/16$ (since by definition, $A > 2$), so $\log q < \log y$ and $q < y^{1/3}$. We take $T = x$, so $y < T < y^2$.

The error term in (2) is

$$O\left(ny^{1/2}(\log^2 y + \log y \log d) + n \log d\right).$$

Because d, n are fixed, the error is $O(y^{1/2}\log^2 y) = O(\frac{y^{6/7}}{q})$, which is less than $\frac{\epsilon}{3}\frac{y}{\phi(q)}$ for y sufficiently large.

The double sum may be bounded by noting that $|y^{\beta+i\gamma}| = y^\beta$, and $\beta + i\gamma \geq \sqrt{1/4+\gamma^2} \geq (1+|\gamma|)/3$.

Thus

$$\left| \sum_{\substack{N(\mathfrak{a})<y \\ N(\mathfrak{a})\equiv 1 \bmod q}} \Lambda(\mathfrak{a}) - \frac{y}{\phi(q)} \right| \leq \frac{3}{\phi(q)} \sum_{\chi \bmod q} \sum_{\substack{L(\beta+i\gamma,\chi)=0 \\ \beta\geq 1/2, |\gamma|\leq x}} \frac{y^\beta}{1+|\gamma|} + \frac{\epsilon}{3}\frac{y}{\phi(q)}. \quad (3)$$

Write $\sum_\sigma^\alpha$ for a sum over all zeros of $\beta+i\gamma$ of $L(s,\chi)$ and over all characters $\chi \bmod q$ where $\sigma \leq \beta < \alpha$ and $|\gamma| < x$. (Each $\beta+i\gamma$ is counted with multiplicity equal to the number of those L-functions for which it is a zero.) To estimate the double sum in (3) we use the upper bounds $y^\beta \leq y^{1-1/(2An)}$ for $\beta \leq 1-1/(2An)$, and $y^\beta \leq y$ for $\tau \leq \beta \leq 1$, where $\tau = 1 - \nu/\log x$. In the range $1-1/(2An) \leq \beta \leq \tau$, we use the identity $y^\beta = y^{1-1/(2An)} + \log y \int_{1-1/(2An)}^\beta y^\sigma d\sigma$.

Therefore, the double sum in (3) is at most

$$\begin{aligned}
&\sum_{1/2}^{1-1/(2An)} \frac{y^{1-1/(2An)}}{1+|\gamma|} + \log y \sum_{1-1/(2An)}^{\tau} \frac{1}{1+|\gamma|} \int_{1-1/(2An)}^\beta y^\sigma d\sigma + y\sum_\tau^1 \frac{1}{1+|\gamma|} \\
&\leq y^{1-1/(2An)} \sum_{1/2}^1 \frac{1}{1+|\gamma|} + \log y \int_{1-1/(2An)}^\tau y^\sigma \left(\sum_\sigma^1 \frac{1}{1+|\gamma|}\right) d\sigma \\
&+ y\sum_\tau^1 \frac{1}{1+|\gamma|}.
\end{aligned} \quad (4)$$

For $\sigma \geq 1/2$, we have, by partial summation,

$$\sum_\sigma^1 \frac{1}{1+|\gamma|} \leq N(\sigma,2,q) + \frac{N(\sigma,x,q)}{x} + \int_2^x \frac{N(\sigma,t,q)}{t^2} dt.$$

By [13], $N(1/2,t,q) < c_4 n q^n t \log qt$. For t in the range $2 \leq t \leq x$, we have $N(1/2,t,q)/t \leq c_4 n q^n \log qx$.

Applying this,

$$\sum_{1/2}^1 \frac{y^{1-\frac{1}{2An}}}{1+|\gamma|} \leq 2c_4 n q^n y^{1-\frac{1}{2An}} \log qx \left(2 + \int_2^x \frac{dt}{t}\right) \leq 5c_4 n q^n y^{1-\frac{1}{2An}} \log^2 qx.$$

Because we insist that $\eta_\epsilon < \frac{1}{8An^2}$, the first term in (4) is $O(y^{1-1/(3An)})$, which is $< \frac{\epsilon}{18}y$ for y sufficiently large.

If $\sigma \geq 1 - 1/(2An)$, then $An(1-\sigma) \leq 1/2$, so that for any t in the range $1 \leq t \leq x$, Theorem 9 of [14] shows that $N(\sigma, t, d) \leq C_A q^{An(1-\sigma)} t^{1/2}$. We deduce that

$$\sum_{\sigma}^{1} \frac{1}{1+|\gamma|} \leq C_A q^{An(1-\sigma)} \left(3 + \int_2^x \frac{dt}{t^{3/2}}\right) \leq 5C_A q^{An(1-\sigma)}.$$

Using this bound, the middle term in (4) is

$$\begin{aligned} &\leq 5C_A q^{An} \log y \int_{1-1/(2An)}^{\tau} \left(\frac{y}{q^{An}}\right)^{\sigma} d\sigma \\ &\leq 5C_A q^{An} \frac{\log y}{log(y/q^{An})} \frac{y}{q^{An}} \left(\frac{y}{q^{An}}\right)^{-(1-\tau)}. \end{aligned} \tag{5}$$

We have that $q^{An} < x^{An\eta} < y^{1/3}$, so $\frac{\log y}{\log(y/q^{An})} < 3/2$. Also,

$$\left(\frac{y}{q^{An}}\right)^{-(1-\tau)} = \left(\frac{y}{q^{An}}\right)^{-\nu/\log x} < e^{-\frac{2}{3}\log y \nu/\log x} < e^{\frac{1}{3}\nu}.$$

Thus the middle term in (4) is $\leq 4C_A y e^{-\frac{1}{3}\nu}$, which, by the way we chose ν, is $\leq \frac{\epsilon}{9}y$.

We apply Lemma 2.2 with $T = x^{n\eta_\epsilon}$ and call the exceptional modulus $q_\epsilon(x)$. Then for all moduli less than x^{η_ϵ} and not divisible by $q_\epsilon(x)$, the L-function has no zeros $\beta + i\gamma$ with $\beta \geq \tau = 1 - \nu/\log x$ and $|\gamma| < x^{n\eta_\epsilon}$.

So the third term in (4) is

$$y \sum_{\tau}^{1} \frac{1}{1+|\gamma|} \leq y \frac{N(\tau, x, q)}{x^{n\eta_\epsilon}} \leq C_A y (q^n x^n)^{A(1-\tau)} / x^{n\eta_\epsilon} < C_A y x^{2An\nu/\log x} / x^{n\eta_\epsilon}.$$

This is less than $C_A y x^{-\eta_\epsilon/2}$, by our choice of x. Also, since $x > x_\epsilon$, by our choice of x, this is less than $C_A y (18C_A/\epsilon)^{2/\eta_\epsilon - \eta_\epsilon/2} = \epsilon y/18$. Putting these bounds together, we get the desired theorem. □

Theorem 2.1 of [3] shows, essentially, that the number of primes in an arithmetic progression less than x cannot be too far away from what you expect. Furthermore, it shows this for "most" moduli up to $x^{\frac{5}{12}}$. Our replacement is the following

Theorem 3.4. *Let $f(t) \in \mathbb{Z}[t]$ be a monic polynomial with splitting field K, $[K:\mathbb{Q}] = n$. Then we have real numbers $x_{1/3}, \eta_{1/3} > 0$ and an integer $q_{1/3}(x) > \log x$, depending on K as described in Theorem 3.3, such that the following statement holds. If $q \leq x^{\eta_{1/3}}$, $\gcd(a,q) = 1$, $q_{1/3}(x) \nmid q$, $x \geq x_{1/3}$ and $x^{1/2} < y < x$, then the number of primes $p < y$ that are $a \bmod q$ and such that $f(t)$ splits into linear factors mod p (equivalently, p splits completely in K) is at least $\frac{1}{2\phi(q)n}\pi(x)$.*

Proof. The previous theorem gives that

$$\sum_{\substack{N(\mathfrak{a})<y \\ N(\mathfrak{a})\equiv a \bmod q}} \Lambda(\mathfrak{a}) \geq \frac{(2/3)y}{\phi(q)}.$$

The sum contains two types of summands not arising from primes. The first, prime ideal powers, can be dispensed of in the usual way, by noting that their contribution to the sum is $O(y^{1/2})$. The second type is primes that do not split completely, for which we have $N(p) = p^k$, for $k > 1$, so they also contribute $O(y^{1/2})$. We pass to the estimate on the number of primes by standard techniques ([6], p. 112). □

Henceforth, let $\eta = \eta_{1/3}$ and $q(x) = q_{1/3}(x)$.

4. Prachar's Theorem

We use the following variant of Prachar's Theorem (c.f. Theorem 3.1 of [3]).

Theorem 4.1. *If L is a squarefree number not divisible by any prime exceeding $x^{\frac{1-\eta}{2}}$ and for which $\sum_{prime\ q|L} \frac{1}{q} \leq \frac{1-\eta}{32n}$, then there is a positive integer $k \leq x^{1-\eta}$ with $(k, L) = 1$ such that*

$$\#\{d|L : dk + 1 \leq x, dk + 1 \text{ is prime, splits fully in } K\} \geq \frac{\#\{d|L : 1 \leq d \leq x^{\eta}\}}{8n \log x}.$$

Proof. Let $\pi_K(x; q)$ denote the number of primes less than x that are 1 mod q and split completely in K.

From Theorem 3.4, we see that for each divisor d of L with $1 \leq d \leq x^{\eta}$ and $(d, q(x)) = 1$,

$$\pi_K(dx^{1-\eta}; d) \geq \frac{\pi(dx^{1-\eta})}{2n\phi(d)} \geq \frac{dx^{1-\eta}}{2n\phi(d)\log x}.$$

Because any prime factor q of L is at most $x^{\frac{1-\eta}{2}}$, we can use Montgomery and Vaughan's explicit version of the Brun-Titchmarsh theorem [18] to get

$$\pi_K(dx^{1-\eta}; dq) \leq \pi(dx^{1-\eta}; dq, 1) \leq \frac{8}{q(1-\eta)} \frac{dx^{1-\eta}}{\phi(d)\log x}.$$

So the number of primes $p \leq dx^{1-\eta}$ with $p \equiv 1 \bmod d$ and $(\frac{p-1}{d}, L) = 1$ that split completely is at least

$$\pi_K(dx^{1-\eta}; d) - \sum_{\text{prime } q|L} \pi_K(dx^{1-\eta}; dq)$$

$$\geq \left(\frac{1}{2n} - \frac{8}{1-\eta} \sum_{\text{prime } q|L} \frac{1}{q} \right) \frac{dx^{1-\eta}}{\phi(d)\log x} \geq \frac{x^{1-\eta}}{4n \log x},$$

for any divisor not divisible by $q(x)$. But at least half of the divisors of L will not be divisible by $q(x)$.

Thus we have at least

$$\frac{x^{1-\eta}}{8n\log x}\#\{d|L : 1 \le d \le x^{\eta}\}$$

pairs (p,d) where $p \le d^{1-\eta}$ is prime, $p \equiv 1 \bmod d$, p splits completely in K, $(\frac{p-1}{d}, L) = 1$, $d|L$ and $1 \le d \le x^{\eta}$. Each such pair (p,d) corresponds to an integer $\frac{p-1}{d} \le x^{1-\eta}$ which is coprime to L, so there is at least one integer $k \le x^{1-\eta}$ with $(k,L) = 1$ such that k has at least

$$\frac{1}{8n\log x}\#\{d|L : 1 \le d \le x^{\eta}\}$$

representations as $\frac{p-1}{d}$ with (p,d) as above. Thus for this integer k we have $\#\{d|L : dk+1 \le x, dk+1 \text{ prime, split completely in } K\} \ge \frac{1}{8n\log x}\#\{d|L : 1 \le d \le x^{\eta}\}$. □

5. Infinitely Many Frobenius Pseudoprimes

We recall the results from Section 1 of [3].

Theorem 5.1 (Theorem 1.1 of [3])**.** *Let $n(G)$ be the length of the longest sequence of (not necessarily distinct) elements of G for which no non-empty subsequence has product the identity. If G is a finite abelian group and m is the maximal order of an element in G, then $n(G) < m(1+\log(\frac{|G|}{m}))$.*

This theorem is due to van Emde Boas and Kruyswijk, and to Meshulam.

Proposition 5.2 (Proposition 1.2 of [3])**.** *Let G be a finite abelian group, and let $r > t > n = n(G)$ be integers. Then any sequence of r elements of G contains at least $\frac{\binom{r}{t}}{\binom{r}{n}}$ distinct subsequences of length at most t and at least $t-n$, whose product is the identity.*

We now prove our main result, which was stated earlier as Theorem 2.1.

Theorem 5.3. *Let K be a number field, and let η be the positive real number depending on K defined in Theorem 3.3. For any $\epsilon > 0$, the number of Carmichael-Frobenius numbers less than x, with respect to a number field K, is at least $x^{\eta/3-\epsilon}$, for sufficiently large x, depending on ϵ and K.*

Proof. Let $\mathcal{Q}$ be the set of primes $q \in (\frac{y^3}{\log y}, y^3]$ for which $q-1$ is free of prime factors exceeding y. Friedlander [8] has proven that there is a constant $C > 0$ for which

$$|\mathcal{Q}| \ge C\frac{y^3}{\log y}$$

for all sufficiently large y. Let L be the product of the primes $q \in \mathcal{Q}$; then

$$\log L \leq |\mathcal{Q}| \log(y^3) \leq \pi(y^3) \log(y^3) \leq 2y^3,$$

for all large y. Carmichael's lambda function, $\lambda(L)$, is the exponent of the group of integers modulo L. Because L is squarefree, it is the least common multiple of $\{q-1\}$ for those primes q that divide L. Because each such $q-1$ is free of prime factors exceeding y, we know that if the prime power p^a divides $\lambda(L)$ then $p \leq y$ and $p^a \leq y^3$. We let p^{a_p} be the largest power of p with $p^{a_p} \leq y^3$, then

$$\lambda(L) \leq \prod_{p \leq y} p^{a_p} \leq \prod_{p \leq y} y^3 = y^{3\pi(y)} \leq e^{6y}$$

for all large y.

Let G be the group $(\mathbb{Z}/L\mathbb{Z})^*$. From Theorem 5.1 and the above equations,

$$n(G) < \lambda(L)\left(1 + \log \frac{\phi(L)}{\lambda(L)}\right) \leq \lambda(L)(1 + \log L) \leq e^{9y}$$

for all large y.

Recall that $\eta < 1/16$. We can choose y large enough so that $\sum \frac{1}{q} \leq \frac{1-\eta}{32n}$ as needed to apply Theorem 4.1. Let $\delta = \frac{3\epsilon}{8n\eta}$, and let $x = e^{y^{1+\delta}}$. Then, for y large enough, there is an integer k coprime to L for which the set $\mathcal{P}$ of primes $p \leq x$ with $p = dk + 1$ for some divisor d of L, and that split in K, satisfies

$$|\mathcal{P}| \geq \frac{\#\{d|L : 1 \leq d \leq x^\eta\}}{8n \log x}.$$

The product of any

$$u := \left[\frac{\log(x^\eta)}{\log y^3}\right] = \left[\frac{\eta \log x}{3 \log y}\right]$$

distinct prime factors of L is a divisor d of L with $d \leq x^\eta$. We deduce from above that

$$\#\{d|L : 1 \leq d \leq x^\eta\} \geq \binom{\omega(L)}{u} \geq \left(\frac{\omega(L)}{u}\right)^u$$

$$\geq \left(\frac{Cy^3}{\eta \log x}\right)^u = \left(\frac{C}{\eta} y^{2-\delta}\right)^u.$$

We notice that $\frac{(2-\delta)\eta}{3} = \frac{2\eta}{3} - \frac{\epsilon}{8n}$. So for all sufficiently large values of y,

$$|\mathcal{P}| \geq \frac{\left(\frac{C}{\eta} y^{2-\delta}\right)^u}{8n \log x} \geq x^{\frac{2\eta}{3} - \frac{\epsilon}{3}}.$$

Take $\mathcal{P}' = \mathcal{P} \backslash \mathcal{Q}$. Because $|\mathcal{Q}| \leq y^3$, we have that $|\mathcal{P}'| \geq x^{\frac{2\eta}{3} - \frac{\epsilon}{2}}$, for all sufficiently large values of y.

We may view $\mathcal{P}'$ as a subset of the group $G = (\mathbb{Z}/L\mathbb{Z})^*$ by considering the residue class of each $p \in \mathcal{P}'$ mod L. If $\mathcal{S}$ is a subset of $\mathcal{P}'$ that contains more than one element, and if

$$\prod(\mathcal{S}) := \prod_{p \in \mathcal{S}} p \equiv 1 \bmod L,$$

then $\prod(\mathcal{S})$ is congruent to 1 mod kL and is a Carmichael number by Korselt's criterion. Because all of its prime factors split completely in K, it is a Frobenius pseudoprime.

Let $t = e^{y^{\frac{1+\delta}{2}}}$. Then, by Proposition 5.2, we see that the number of Frobenius pseudoprimes of the form $\prod(\mathcal{S})$, where $\mathcal{S} \subset \mathcal{P}'$ and $|\mathcal{S}| \leq t$, is at least

$$\frac{\binom{|\mathcal{P}'|}{[t]}}{\binom{|\mathcal{P}'|}{n(G)}} \geq \frac{\left(\frac{|\mathcal{P}'|}{[t]}\right)^{[t]}}{|\mathcal{P}'|^{n(G)}} \geq \left(x^{\frac{2\eta}{3}-\frac{\epsilon}{2}}\right)^{[t]-n(G)} [t]^{-[t]} \geq x^{t\left(\frac{2\eta}{3}-\epsilon\right)}$$

for all sufficiently large values of y. We note that we have formed each Frobenius pseudoprime $\prod(\mathcal{P}) \leq x^t$. Thus for $X = x^t$ we have the number of Frobenius pseudoprimes $\leq x$ is at least $X^{\frac{2\eta}{3}-\epsilon}$ for all sufficiently large values of X. Because y can be uniquely determined from X, the theorem is proven.

□

References

[1] W. W. Adams and D. Shanks. Strong primality tests that are not sufficient. *Math. Comp.*, 39:255–300, 1982.

[2] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Ann. of Math.*, 160:781–793, 2004.

[3] W. R. Alford, Andrew Granville, and Carl Pomerance. There are infinitely many carmichael numbers. *Annals of Mathematics*, 140:703–722, 1994.

[4] Roberto M. Avanzi and Preda Mihăilescu. Efficient "quasi"-deterministic primality test improving AKS. http://caccioppoli.mac.rub.de/website/papers/aks-mab.pdf, 2009.

[5] Daniel J. Bernstein. Proving primality in essentially quartic random time. *Math. Comp.*, 76:389–403, 2007.

[6] Harold Davenport. *Multiplicative Number Theory.* Springer-Verlag, New York, second edition edition, 1980.

[7] E. Fogels. On the zeros of L-functions. *Acta Arith.*, 11:67–96, 1965.

[8] J. B. Friedlander. Shifted primes without large prime factors. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 393–401. Kluwer Acad. Publ., Dordrecht, 1989.

[9] J. Grantham. *Frobenius Pseudoprimes*. PhD thesis, University of Georgia, 1997.

[10] J. Grantham. Frobenius pseudoprimes. *Math. Comp.*, 70:873–891, 2001.

[11] S. Gurak. Pseudoprimes for higher-order linear recurrence sequences. *Math. Comp.*, 55:783–813, 1990.

[12] Jihad Michael Haddad. A comparison of the frobenius primality test with the strong primality test. Technical report, University of Odense, 1998. Bachelor Project.

[13] Teluhiko Hilano. On the zeros of Hecke's L-functions. *Sci. Papers College Gen. Ed. Univ. Tokyo*, 24:9–24, 1974.

[14] Teluhiko Hilano. On the zeros of Heck's [sic] L-functions. *Proc. Japan Acad.*, 50:23–28, 1974.

[15] H.W. Lenstra Jr. and Carl Pomerance. A rigorous time bound for factoring numbers. *J. Amer. Math. Soc.*, 5:483–516, 1992.

[16] H.W. Lenstra Jr. and Carl Pomerance. Primality testing with gaussian periods. http://math.dartmouth.edu/~carlp/aks0221109.pdf, 2009.

[17] J.C. Lagarias and A.M. Odlyzko. Effective versions of the chebotarev density theorem. In A. Frolich, editor, *Algebraic Number Fields: L-functions and Galois Properties*, pages 409–464. Academic Press, London, 1977.

[18] H. L. Montgomery and R. C. Vaughan. Error terms in additive prime number theory. *Quart. J. Math. Oxford Ser. (2)*, 24:207–216, 1973.

[19] F. Morain. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. *Math. Comp.*, 76:493–505, 2007.

[20] G. Szekeres. Higher order pseudoprimes in primality testing. In *Combinatorics, Paul Erdős is eighty*, volume 2, pages 451–458. János Bolyai Math Soc., Budapest, 1996.