There are Infinitely Many Perrin Pseudoprimes *

Jon Grantham

April 24, 2005

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 proof uses ingredients of the recent proof that are are infinitely many Carmichael numbers, along with zero-density estimates for Hecke L-functions.

1 Background

In a 1982 paper [**?**], Adams and Shanks introduced a probable primality test based on third order recurrence sequences. The following is a version of it.

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

Definition 1.2 *An integer* n *is said to have an* **S-signature** *if its signature mod* n *is congruent to* $(A_{-2}, A_{-1}, A_0, A_0, A_1, A_2)$.

*In memory of Daniel Shanks

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 $f(a) \equiv 0 \mod n$, $A \equiv a^{-2} + 2a$, $B \equiv -ra^2 + (r^2 - s)a$, 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 1.3 *A* **Perrin pseudoprime** *with parameters (r, s) is an odd composite n and 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.

Adams and Shanks asked if there are infinitely 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."

In 1994, Alford, Granville and Pomerance [**?**] proved that there are infinitely many Carmichael numbers. A simple modification of that proof shows that there are infinitely many Lucas and Lehmer pseudoprimes. (If the characteristic polynomial is $f(x)$, require all prime divisors p of the Carmichael numbers to have $p \equiv 1 \mod 4 \operatorname{disc}(f)$).

In this paper, the techniques of that proof are combined with results about Hecke L-functions to show that there are infinitely many Perrin pseudoprimes. In fact, a more general result can be proven.

Theorem 1.1 *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 $c = c(K) > 0$.*

The concept of Frobenius pseudoprime, introduced in [**?**], essentially provides a generalization of most pseudoprime definitions based on recurrence sequences. A Carmichael-Frobenius number is a pseudoprime with respect to all polynomials with splitting field K. Proving the theorem with respect to the generalization allows specialization to other cases.

In particular, we know from [**?**] that Theorem 1.1 shows that there are infinitely many Perrin pseudoprimes, if we take $f(x) = x^3 - x - 1$. Also

from [?], we have that there are infinitely many pseudoprimes in the senses of Gurak [?] and Szekeres [?].

By Proposition 6.1 of [?], in order to prove Theorem 1.1, 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 [?] 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.

2 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.) Since 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 [?].

Definition 2.1 *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, $m(\mathfrak{p}) = 0$ 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 $\alpha \equiv 1 \mod \mathfrak{p}^{m(\mathfrak{p})}$ 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*