# Average Liar Counts for Degree 2 Frobenius Pseudoprimes

Andrew Fiori and Andrew Shallue

University of Calgary – Illinois Wesleyan University

West Coast Number Theory 2016

# Inspiration and summary

Erdős, Pomerance, "On the number of false witnesses for a composite number" (1986) proved that

$$y^{15/23} < \frac{1}{y} \sum_{n \leq y} F(n) \leq y \cdot \exp\left( \frac{-(1+o(1)) \log y \log\log\log y}{\log\log y} \right)$$

where the sum is over $n$ composite, and $F(n)$ is the count of Fermat liars for $n$.

We have proven a similar result for degree 2 Frobenius pseudoprimes.

Headline result: Grantham challenge pseudoprimes exist "on average"

# Why study pseudoprimes?

1. Primality tests based on necessary conditions are still used in practice.

2. Pseudoprimes exhibit fascinating divisibility properties.

3. Prize money!

# Definitions

Composite $n$ is a 2-**Fermat pseudoprime** if $2^{n-1} \equiv 1 \mod n$
First example: 341.

**Lucas pseudoprime**: let $P, Q$ be integers, $\Delta = P^2 - 4Q$ (discriminant), $\alpha, \beta$ the roots of $x^2 - Px + Q$. The Lucas U sequence is defined by

$$U(n) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \ .$$

Let $\epsilon(n) = (\Delta \mid n)$.

Composite $n$ is a $(P, Q)$-LucasU pseudoprime if $n \mid U(n - \epsilon(n))$.
First $(1, -1)$-Lucas pseudoprime: 323

# Degree 2 Frobenius pseudoprimes

## Definition (Grantham)

Let $f(x) \in \mathbb{Z}[x]$ be a degree 2 monic polynomial with discriminant $\Delta$. Suppose that all the following conditions hold for a composite $n$.

1. (Integer Divisibility) We have $\gcd(n, f(0)\Delta) = 1$.
2. (Factorization) Let $F_1(x) = \operatorname{gcmd}(x^n - x, f(x))$, $f_1(x) = f(x)/F_1(x)$, $F_2(x) = \operatorname{gcmd}(x^{n^2} - x, f_1(x))$, 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) Have $(-1)^S = (\Delta \mid n)$, where $S = \deg(F_2(x))/2$.

In this case we call $n$ a degree 2 Frobenius pseudoprime with respect to $f(x)$, and we call $f(x)$ a degree 2 Frobenius liar with respect to $n$.

# Connections

## Theorem (Grantham)

*If $a, b$ are integers, $f(x) = (x - a)(x - b)$, and $n$ is a Frobenius pseudoprime with respect to $f$, then $n$ is a Fermat pseudoprime to both $a$ and $b$.*

## Theorem (Grantham)

*If $f(x) = x^2 - Px + Q \in \mathbb{Z}[x]$ and $n$ is a Frobenius pseudoprime with respect to $f(x)$, then $n$ is a $(P, Q)$-LucasU pseudoprime.*

## Theorem (Grantham)

*If $n$ is a Frobenius pseudoprime with respect to $f(x)$, then $n$ is a Fermat pseudoprime to the base $f(0)$.*

# Motivation

PSW \$620 challenge pseudoprime: composite $n$ such that $n = \pm 2 \mod 5$ is a base 2 Fermat pseudoprime and a $(1, -1)$-LucasU pseudoprime (i.e. a Fibonacci pseudoprime).

Baillie-PSW pseudoprime: composite $n$ such that $n$ is a base-2 strong pseudoprime and a strong $(P, Q)$-Lucas pseudoprime where $(P, Q)$ chosen in a certain way to ensure symbol is $-1$.

Grantham \$6.20 challenge pseudoprime: composite $n$ such that $n = \pm 2 \mod 5$ and a Frobenius pseudoprime with respect to $x^2 + 5x + 5$.

# Notation

Let $L_2(n)$ be the set of degree 2 Frobenius liars for $n$.

Let $L_2^+(n)$ be subset of liars where $(\Delta \mid n) = +1$. Similarly $L_2^-(n)$ is the subset where $(\Delta \mid n) = -1$.

Let $\mathrm{Frob}_2(y, f(x))$ be the set of degree 2 Frobenius pseudoprimes with respect to $f(x)$, up to bound $y$.

# Results

## Theorem (Fiori, S.)

*For all $\alpha \leq 23/8$ we have*

$$y^{3-\alpha^{-1}-o(1)} < \sum_{n \leq y} L_2^+(n) \leq y^3 \cdot \exp\left(\frac{-(1+o(1))\log y \log\log\log y}{\log\log y}\right)$$

*where the sum is restricted to composite $n$.*

## Theorem (Fiori, S.)

*For all $\alpha \leq 4/3$ we have*

$$y^{3-\alpha^{-1}-o(1)} < \sum_{n \leq y} L_2^-(n) \leq y^3 \cdot \exp\left(\frac{-(1+o(1))\log y \log\log\log y}{\log\log y}\right)$$

*where the sum is restricted to composite $n$.*

# Satisfying challenges on average

Since $\sum_{n \le y} L_2^-(n) = \sum_{a,b \le y} \mathrm{Frob}_2^-(y, x^2 + ax + b)$ we have

$$\frac{1}{y^2} \sum_{a,b \le y} \mathrm{Frob}_2^-(y, x^2 + ax + b) \ge y^{1-\alpha^{-1}-o(1)}$$

So if we extend Grantham's challenge to any set $\mathrm{Frob}_2^-(y, f(x))$, there are infinitely many requested pseudoprimes on average.

# Upper bound strategy

Let $\lambda_2(n) = \operatorname{lcm}_{p|n} p^2 - 1$.

Let $D_k(x)$ be the set of composite $n \leq k$ where $k$ is the smallest integer such that $\lambda_2(n) \mid k(n^2 - 1)$.

## Lemma (Fiori, S.)

*Suppose $n$ is square-free, composite, and $n \in D_k(x)$. Then*

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

Following Erdős, Pomerance we have

$$\sum_{n \leq x}{}' L_2^-(n) = \sum_k \sum_{n \in D_k(x)} L_2^-(n)$$

# Bottleneck

Let $L(y) = \exp(\frac{(\log y)(\log\log\log y)}{\log\log y})$.

## Lemma (Fiori, S.)

*For all sufficiently large $y$ we have*

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

## Proof.

Follows Pomerance, Theorem 1 from "On the distribution of pseudoprimes." $\square$

# Questions and conclusions

The correct count of degree 2 Frobenius liars over all $n \leq y$ is probably $y^3 L(y)^{-1+o(1)}$. If we restrict to $-1$ liars, is the count different?

In particular, can the previous lemma be improved? Perhaps on average?

The search for challenge pseudoprimes continues.