Average Number of Quadratic Frobenius Pseudoprimes

Andrew Fiori

PIMS Postdoctoral Fellow - University of Calgary

Summer 2016

This work is joint with Andrew Shallue.

Context and Motivation

- A number n is a base a pseudoprime if $a^n = a \pmod{n}$.
- Let $F(n) = |\{a \pmod{n} \mid n \text{ is a base } a \text{ pseudoprime}\}|$. Erdős and Pomerance showed that, with $\alpha = \frac{23}{15}$ we have:

$$x^{2-\alpha^{-1}-o(1)} < \sum_{n<x} F(n) < x^2 e^{-\log(x)\frac{\log\log\log(x)}{\log\log(x)}}.$$

- Rather than a base $a \pmod{n}$ we will consider a base $f(x) = x^2 + ax + b \pmod{b}$, and the more elaborate Frobenius pseudoprime test. We will then look at

$$F_{\pm 1}(n) = \{f \pmod{n} \mid \left(\frac{\Delta_f}{n}\right) = \pm 1,\ n \text{ is a base } f \text{ pseudoprime}\}$$

- We are broadly motivated by the question:
  How likely is it that a randomly chosen pair (f, n) passes the primality test even though n is not prime?
  Note: a Frobenius pseudoprime for f, is a Lucas pseudoprime for the associated recurrence.

What are Frobenius Pseudoprimes

Fix a polynomial $f(x)$. If p is a prime number, and $(\Delta_f f(0), p) = 1$ then we know that:

- For all d we have that:

$$d \mid \deg\left(\gcd_{\text{mod-p}}\left(f(x), \frac{x^{p^d}-1}{x^{p^{d-1}}-1}\right)\right)$$

- The map $x \mapsto x^p$ permutes the roots of each:

$$f_d(x) = \gcd_{\text{mod-p}}\left(f(x), \frac{x^{p^d}-1}{x^{p^{d-1}}-1}\right).$$

- We have the factorization $f(x) = \prod f_d(x) \pmod{p}$.
- The factorization structure of $f(x)$, that is the collection of degrees above, determines $\left(\frac{\Delta_f}{p}\right)$.

Without getting into the technical details, we will call a number n a Frobenius pseudoprime if it satisfies these four conditions.

What are our main results?

We have the following closed form expressions for $F_{\pm}(n)$:

$$F_+(n) = \frac{1}{2}\prod_{p|n}\frac{1}{2}\left((n-1,p^2-1)+(n-1,p-1)^2-2(n-1,p-1)\right)$$
$$+\frac{1}{2}\prod_{p|n}\frac{1}{2}\left((n-1,p-1)^2-(n-1,p^2-1)\right)$$

$$F_-(n) = \frac{1}{2}\prod_{p|n}\frac{1}{2}\left((\frac{n}{p}-1,p^2-1)+(n^2-1,p-1)-2(n-1,p-1)\right)$$
$$-\frac{1}{2}\prod_{p|n}\frac{1}{2}\left(-(\frac{n}{p}-1,p^2-1)+(n^2-1,p-1)\right)$$

We have the following bounds on the average:

$$x^{3-\alpha^{-1}-o(1)} < \sum_{n<x} F_+(n) < x^3 e^{-\log(x)\frac{\log\log\log(x)}{\log\log(x)}}$$

$$x^{2-\alpha^{-1}-o(1)} < \sum_{n<x} F_-(n) < x^3 e^{-\log(x)\frac{\log\log\log(x)}{\log\log(x)}}$$

Some basic questions we can thus partially answer

1) Fix n, are there quadratic $f(x)$ with (f, n) a Frobenius liar pair?
   Yes.
2) Fix n, are there quadratic $f(x)$ with $\left(\frac{\Delta_f}{n}\right) = \pm 1$?
   Yes for $+1$
   Sometimes no for -1 (for example 21) but they exist on average.
3) Given f, are there n for which (f, n) gives a Frobenius liar pair?
   Yes.
   We just need a Carmichael number n for which f splits at all $p|n$.
4) Given f, are there n with $\left(\frac{\Delta_f}{n}\right) = \pm 1$ and the pair is a liar?
   Yes for $+1$
   Unclear for -1 case, and our result doesn't even tell us on average.

What is needed to improve our $\left(\frac{\Delta_f}{n}\right) = -1$ result.

Firstly, the idea of the proof is that of Erdős and Pomerance. Given primes p for which $p-1$ is smooth one constructs n for which

$$(n-1, p-1) \qquad (n-1, p^2-1) \qquad (n^2-1, p-1) \qquad (n^2-1, p^2-1, n-p)$$

are large. To improve the results in the -1 case, we want p^2-1 to be smooth to maximize: $(n^2-1, p^2-1, n-p)$. But this is not sufficient because of the $n-p$ term.

Conjecture:
If p is a prime and p^2-1 is 'smooth' the expected number of prime factors of p^2-1 is $\log((p^2-1)^{o(1)})$.

Assuming this conjecture we can show, with $\beta = \frac{4}{3}$ that:

$$x^{3-\beta^{-1}-o(1)} < \sum_{n<x} F_-(n)$$

This would tell us we expect n to exist on average.

The End.

Thank you.