IDA

An Unconditional Improvement to the Running Time of the Quadratic Frobenius Test

Jon Grantham

PAJAMAS

September 2020

Center for Computing Sciences
17100 Science Drive • Bowie, Maryland 20715

Outline

1. Pseudoprimes As of 1980
2. Quadratic Frobenius Test
3. Newer Tests
4. Reducing the QFT run time

Pseudoprimes

- $a^p \equiv a \mod p$, for p prime.

Pseudoprimes

- $a^p \equiv a \mod p$, for p prime.
- Equivalently, $a^{p-1} \equiv 1$.

Pseudoprimes

- $a^p \equiv a \mod p$, for p prime.
- Equivalently, $a^{p-1} \equiv 1$.
- If $a^{n-1} \equiv 1$ and n is composite, n is a **(Fermat) pseudoprime base** a.

Pseudoprimes

- $a^p \equiv a \mod p$, for p prime.
- Equivalently, $a^{p-1} \equiv 1$.
- If $a^{n-1} \equiv 1$ and n is composite, n is a **(Fermat) pseudoprime base** a.
- Some numbers (1729) are pseudoprimes for all (coprime) bases.

Strong Pseudoprimes

- If $p = 2^r s + 1$ with s odd, then either $a^s \equiv 1$, or $a^{2^t s} \equiv -1$ with $r > t \geq 0$.

Strong Pseudoprimes

- If $p = 2^r s + 1$ with s odd, then either $a^s \equiv 1$, or $a^{2^t s} \equiv -1$ with $r > t \geq 0$.
- A composite satisfying this test is a **strong pseudoprime to the base** a. (Dubois; Selfridge)

Strong Pseudoprimes

- If $p = 2^r s + 1$ with s odd, then either $a^s \equiv 1$, or $a^{2^t s} \equiv -1$ with $r > t \geq 0$.
- A composite satisfying this test is a **strong pseudoprime to the base** a. (Dubois; Selfridge)
- A composite is a strong pseudoprime for at most $\frac{1}{4}$ of the bases. (Monier, 1980; Rabin, 1980)

Baillie-PSW Pseudoprimes

- If p is prime, $F_{p-\left(\frac{p}{5}\right)}$ is divisible by p.

Baillie-PSW Pseudoprimes

- If p is prime, $F_{p-\left(\frac{p}{5}\right)}$ is divisible by p.
- A composite satsifying this test is a **Fibonacci pseudoprime**.

Baillie-PSW Pseudoprimes

- If p is prime, $F_{p-\left(\frac{p}{5}\right)}$ is divisible by p.
- A composite satsifying this test is a **Fibonacci pseudoprime**.
- A composite with $\left(\frac{n}{5}\right) = -1$ which is also a strong pseudoprime to the base 2 is a Baillie-PSW pseudoprime. (Baillie, Wagstaff, 1980; Pomerance, Selfridge and Wagstaff, 1980)

Baillie-PSW Pseudoprimes

- If p is prime, $F_{p-\left(\frac{p}{5}\right)}$ is divisible by p.
- A composite satsifying this test is a **Fibonacci pseudoprime**.
- A composite with $\left(\frac{n}{5}\right) = -1$ which is also a strong pseudoprime to the base 2 is a Baillie-PSW pseudoprime. (Baillie, Wagstaff, 1980; Pomerance, Selfridge and Wagstaff, 1980)
- No such number is known; \$620 is offered for a solution, which probably exists. (See Pomerance, 1984; Alford and G., unpublished.)

Reformulation

The QFT, reformulated in the style of Damgard and Frandsen:

- Make sure n is not divisible by $p < 50000$.

Reformulation

The QFT, reformulated in the style of Damgard and Frandsen:

- Make sure n is not divisible by $p < 50000$.
- Make sure that n is not a perfect square.

Reformulation

The QFT, reformulated in the style of Damgard and Frandsen:

- Make sure n is not divisible by $p < 50000$.
- Make sure that n is not a perfect square.
- Choose c with $\left(\frac{c}{n}\right) = -1$.

Reformulation

The QFT, reformulated in the style of Damgard and Frandsen:

- Make sure n is not divisible by $p < 50000$.
- Make sure that n is not a perfect square.
- Choose c with $\left(\frac{c}{n}\right) = -1$.
- Choose a, b such that $\left(\frac{b^2 - ca^2}{n}\right) = 1$. Let $z = ax + b$.

Reformulation

The QFT, reformulated in the style of Damgard and Frandsen:

- Make sure n is not divisible by $p < 50000$.
- Make sure that n is not a perfect square.
- Choose c with $\left(\frac{c}{n}\right) = -1$.
- Choose a, b such that $\left(\frac{b^2 - ca^2}{n}\right) = 1$. Let $z = ax + b$.
- Make sure $z^{\frac{n+1}{2}} \mod x^2 - c$ is an integer.

Reformulation

The QFT, reformulated in the style of Damgard and Frandsen:

- Make sure n is not divisible by $p < 50000$.
- Make sure that n is not a perfect square.
- Choose c with $\left(\frac{c}{n}\right) = -1$.
- Choose a, b such that $\left(\frac{b^2 - ca^2}{n}\right) = 1$. Let $z = ax + b$.
- Make sure $z^{\frac{n+1}{2}} \mod x^2 - c$ is an integer.
- Make sure $z^{n+1} \equiv b^2 - ca^2$.

Reformulation

The QFT, reformulated in the style of Damgard and Frandsen:

- Make sure n is not divisible by $p < 50000$.
- Make sure that n is not a perfect square.
- Choose c with $\left(\frac{c}{n}\right) = -1$.
- Choose a, b such that $\left(\frac{b^2 - ca^2}{n}\right) = 1$. Let $z = ax + b$.
- Make sure $z^{\frac{n+1}{2}} \mod x^2 - c$ is an integer.
- Make sure $z^{n+1} \equiv b^2 - ca^2$.
- Let $n^2 - 1 = 2^r s$, s odd. Verify that $x^s \equiv 1$, or $x^{2^j s} \equiv -1$ for some $0 \leq j < r - 1$.

Running Time

- The strong pseudoprime test requires $(1 + o(1)) \log n$ modular multiplications.

Running Time

- The strong pseudoprime test requires $(1 + o(1)) \log n$ modular multiplications.
- The unit of time required to perform one such test is called a **selfridge**.

Running Time

- The strong pseudoprime test requires $(1 + o(1)) \log n$ modular multiplications.
- The unit of time required to perform one such test is called a **selfridge**.
- The term originated with Atkin, who had a somewhat different formalization.

Running Time

- The strong pseudoprime test requires $(1 + o(1)) \log n$ modular multiplications.
- The unit of time required to perform one such test is called a **selfridge**.
- The term originated with Atkin, who had a somewhat different formalization.
- In particular, my formalization does not distinguish between modular multiplications and modular squares, which are often cheaper.

Running Time

- The strong pseudoprime test requires $(1 + o(1)) \log n$ modular multiplications.
- The unit of time required to perform one such test is called a **selfridge**.
- The term originated with Atkin, who had a somewhat different formalization.
- In particular, my formalization does not distinguish between modular multiplications and modular squares, which are often cheaper.
- This annoyed Atkin.

Running Time

- The strong pseudoprime test requires $(1 + o(1)) \log n$ modular multiplications.
- The unit of time required to perform one such test is called a **selfridge**.
- The term originated with Atkin, who had a somewhat different formalization.
- In particular, my formalization does not distinguish between modular multiplications and modular squares, which are often cheaper.
- This annoyed Atkin.
- Both the QFT in its original form and the reformulation above have running time of 3 selfridges.

Accuracy

- Any composite passes the QFT with probability $< \frac{1}{7710}$. (G, 1998.)

Accuracy

- Any composite passes the QFT with probability $< \frac{1}{7710}$. (G, 1998.)
- Not known to be sharp.

Accuracy

- Any composite passes the QFT with probability $< \frac{1}{7710}$. (G, 1998.)
- Not known to be sharp.
- By comparision, 3 iterations of the strong probable prime test also take 3 selfridges and give error bound $\frac{1}{64}$.

Accuracy

- Any composite passes the QFT with probability $< \frac{1}{7710}$. (G, 1998.)
- Not known to be sharp.
- By comparision, 3 iterations of the strong probable prime test also take 3 selfridges and give error bound $\frac{1}{64}$.
- A different, but related question is what the probability that a random composite will pass this test.

Accuracy

- Any composite passes the QFT with probability $< \frac{1}{7710}$. (G, 1998.)
- Not known to be sharp.
- By comparision, 3 iterations of the strong probable prime test also take 3 selfridges and give error bound $\frac{1}{64}$.
- A different, but related question is what the probability that a random composite will pass this test.
- As usual, I will ignore that question in this talk.

Extended QFT

- Due to Damgard and Frandsen (2006).
- $\frac{256}{331776^t}$ error probability for t iterations.
- Each iteration takes 2 selfridges, plus a start-up cost of 2 selfridges.
- Uses ERH to establish run time.
- Uses properties of 24th roots to establish error probability.

MSQ costing

- Damgard and Frandsen cost in terms of Modular Squarings (MSQs).
- They assume that a modular multiplication costs 1.3 MSQs.
- Based on an implementation of Montgomery multiplication.
- Under this, their test has a start-up cost of 2.3 MSQs and a per-test cost of 2.6.
- The QFT has a cost of 3.3 MSQs. (But the reformulation is 3.9.)

Conditional Improvement

- Under ERH, can find a small c with $\left(\frac{c}{n}\right) = -1$.

Conditional Improvement

- Under ERH, can find a small c with $\left(\frac{c}{n}\right) = -1$.
- Then reduction modulo $x^2 - c$ requires c subtractions rather than multiplication by c.

Conditional Improvement

- Under ERH, can find a small c with $\left(\frac{c}{n}\right) = -1$.
- Then reduction modulo $x^2 - c$ requires c subtractions rather than multiplication by c.
- Same technique as Damgard and Frandsen.

Conditional Improvement

- Under ERH, can find a small c with $\left(\frac{c}{n}\right) = -1$.
- Then reduction modulo $x^2 - c$ requires c subtractions rather than multiplication by c.
- Same technique as Damgard and Frandsen.
- Reduces running time to 2 selfridges.

Unconditional Improvement

- Can't guarantee a very small c without ERH.

Unconditional Improvement

- Can't guarantee a very small c without ERH.
- However, multiplying by a number of size n^{δ} takes δ of the time as a full-sized multiplication.

Unconditional Improvement

- Can't guarantee a very small c without ERH.
- However, multiplying by a number of size n^δ takes δ of the time as a full-sized multiplication.
- If I can find $c < n^\delta$, QFT takes $2 + \delta$ selfridges.

Lemma

Lemma

If n is a sufficiently large composite number and $\delta > \frac{1}{3\sqrt{e}}$, a positive proportion of the numbers $0 < c < n^{\delta}$ have $\left(\frac{c}{n}\right) = 0$ or -1.

Lemma

Lemma

If n is a sufficiently large composite number and $\delta > \frac{1}{3\sqrt{e}}$, a positive proportion of the numbers $0 < c < n^{\delta}$ have $\left(\frac{c}{n}\right) = 0$ or -1.

Proof.

A character sum estimate from Burgess (1986) shows that for any $\epsilon > 0$, $\sum_{k<n^{\gamma}} \left(\frac{k}{n}\right) < (n^{\gamma})^{2/3} n^{1/9+\epsilon}$. We can then take $\gamma = 1/3 + 6\epsilon$ to get $\sum_{k<n^{\gamma}} \left(\frac{k}{n}\right) < n^{1/3+5\epsilon} = o(n^{\gamma})$.

Lemma

Lemma

If n is a sufficiently large composite number and $\delta > \frac{1}{3\sqrt{e}}$, a positive proportion of the numbers $0 < c < n^{\delta}$ have $\left(\frac{c}{n}\right) = 0$ or -1.

Proof.

A character sum estimate from Burgess (1986) shows that for any $\epsilon > 0$, $\sum_{k<n^{\gamma}} \left(\frac{k}{n}\right) < (n^{\gamma})^{2/3} n^{1/9+\epsilon}$. We can then take $\gamma = 1/3 + 6\epsilon$ to get $\sum_{k<n^{\gamma}} \left(\frac{k}{n}\right) < n^{1/3+5\epsilon} = o(n^{\gamma})$.
A result of Granville and Soundararajan (in Banks, et. al., 2008) shows that if $\sum_{n\leq x} f(n) = o(x)$, then $\left|\sum_{n\leq x^{1/\sqrt{e}}} f(n)\right| < Cx^{1/\sqrt{e}}$, for some $C < 1$.

□

MSQ Costing

- The cost of a QFT with $c < n^{\delta}$ is $(2 + \delta) * 1.3$ MSQs.
- Therefore, we have $(2 + \frac{1}{3\sqrt{e}}) * 1.3 \approx 2.86$ MSQs.
- Even under the MSQ scoring, we achieve an improvement over the original (3.3 MSQ) test.

The End

- `https://arxiv.org/abs/1908.02394`
- *J. Number Theory* 210 (2020), 476–480.
- Thanks to Paul Pollack for helpful e-mail exchanges about Burgess bounds.

The End

- `https://arxiv.org/abs/1908.02394`
- *J. Number Theory* 210 (2020), 476–480.
- Thanks to Paul Pollack for helpful e-mail exchanges about Burgess bounds.

- Questions?