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

Jon Grantham

April 2007

Outline

Pseudoprimes As of 1980

Quadratic Frobenius Test

Newer Tests

Reducing the QFT run time

Future Work

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 **pseudoprime base** a.
- Some numbers (1729) are pseudoprimes for all (coprime) bases.

Euler Pseudoprimes

- $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$.
- If $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)$, n is an **Euler pseudoprime to the base** a. (Robinson, 1957)
- A composite is an Euler pseudoprime for at most $\frac{1}{2}$ of the bases. (Solovay and Strassen, 1977)

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 $p \equiv 3, 4 \mod 5$, $F_{p-\left(\frac{p}{5}\right)}$ 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 Ballie-PSW pseudoprime. (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 (See Pomerance, 1984; Alford and G., unpublished.)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 $p < 50000$.
- 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.
- 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.)
- 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.

Müller's Tests

- Test for $n \equiv 1 \mod 4$. (2004)
- $\frac{1}{1048350 * 131040^{t-1}}$ error probability for t iterations.
- Test for $n \equiv 3 \mod 4$. (2003)
- $\frac{1}{331000}$ error probability.
- Both take 3 selfridges.

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 $\left(\frac{c}{n}\right) = -1$.
- 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 find a very small c without ERH.
- However, multiplying by a number of size n^ϵ takes ϵ of the time as a full-sized multiplication.
- If I can find $c < n^\epsilon$, QFT takes $2 + \epsilon$ selfridges.

Lemma

Lemma

If n is a sufficiently large composite number, at least $1/9$ of the numbers $0 < c < n^{1/2}$ have $\left(\frac{c}{n}\right) = -1$.

Proof.

Let p be the smallest prime divisor of n. We have that $p < \sqrt{n}$. Let $m = n/p$. Then for $u = 1$ or $u = -1$, at least $1/3$ of the numbers $< \sqrt{n}$ have $\left(\frac{c}{m}\right) = u$. At least $1/3$ of the numbers have $\left(\frac{c}{p}\right) = -u$, ensuring that $1/9$ have the $\left(\frac{c}{n}\right) = -1$. □

This is sloppy, you can get $1/9$ as close as you want to $1/2$.

MSQ Costing

- The cost of a QFT with $c < n^\epsilon$ is $(2 + \epsilon) * 1.3$ MSQs.
- Therefore, we have $2.5 * 1.3 = 3.25$ MSQs.
- Even under the MSQ scoring, we achieve a slight victory over the original (3.3 MSQ) test.
- Need a more complicated lemma to deal with Montgomery multiplication.

Future Work

- Reduce ϵ.
- Apply this technique to tests involving cube roots of 1.