# Collecting primes with $p^2 - 1$ $827$-smooth
# OR
# Reduced sets for likely solutions to the $620 problem

Jon Grantham
Institute for Defense Analyses
Center for Computing Sciences

*In memory of my friend Red Alford*

# Probable Primes and Pseudoprimes

- **Fermat's Little Theorem:**
  - If $p$ is prime, then $a^p \equiv a \bmod p$, for all integers $a$.
- The converse doesn't always follow...
- $2^{341} \equiv 2 \bmod 341$.
- A **probable prime to the base** $a$ is a number $n$ such that $a^n \equiv a \bmod n$.
- A **pseudoprime to the base** $a$ is a composite probable prime to the base $a$.
- (Sometimes called a **Fermat pseudoprime.**)
- There aren't that many pseudoprimes (compared to primes).

# Fibonacci pseudoprimes

- A **Fibonacci pseudoprime** is a composite $n$ such that $n | F_{n-(\frac{n}{5})}$, where $F_k$ is the $k^{th}$ Fibonacci number.
  - (Generalizes to Lucas sequences and Lucas pseudoprimes.)
- Pomerance, Selfridge and Wagstaff offer $620 for a base-$2$ pseudoprime that is also a Lucas pseudoprime and is $2$ or $3$ mod $5$. (Or a proof that none exists.)

# Carl's Heuristic

- In 1984, Carl Pomerance gave a heuristic (a modification of Erdos' heuristic for Carmichael numbers) that said that there should be infinitely many ($\gg x^{1-\epsilon}$) solutions to the $620 problem.
- The paper is available at
  - `http://www.pseudoprime.com/pseudo.html`
- We choose a set $Q$ of primes less than a bound $B$. Let $Q_1$ be the subset of $Q$ consisting of primes congruent to $1 \bmod 4$ (excepting $5$). Let $Q_3$ be the subset of $Q$ consisting of primes congruent to $-1 \bmod 4$. Then we search for primes $p \equiv 3, 27 \bmod 40$ with $(p-1)/2$ squarefree and consisting only of primes in $Q_1$ and $(p+1)/4$ squarefree and consisting only of primes in $Q_3$.
- Call this set of primes $P$.

# Carl's Heuristic, cont.

- Let $M_1 = \prod_{q \in Q_1} q$, and $M_3 = \prod_{q \in Q_3} q$.
- Let $P'$ be a subset of $P$, and let $n = \prod_{p \in P'} p$. Assume that $n$ has an odd number of prime factors, and further that $n \equiv 1 \bmod M_1$ and $n \equiv -1 \bmod 4M_3$. Then $n \equiv 2$ or $3 \bmod 5$, $n$ is a (strong) Fermat pseudoprime to the base $2$ and $m$ is a Fibonacci pseudoprime. (In fact, $n$ is also a Carmichael number.)
- **Why is $n$ a Fermat pseudoprime?** For each $p|n$ $p \in P$, so we have $p-1|2M_1$. Further, $2M_1|n-1$, by the assumptions on $n$. Therefore, $p-1|n-1$. Therefore $2^{n-1} \equiv 2^{(p-1)\frac{n-1}{p-1}} \equiv 1$.
- $n$ is a Fibonacci pseudoprime by a similar argument.

# Why does $n$ exist?

- We assume that all possible $n$s are randomly distributed $\mod 4M_1M_3$. (This is not accurate, but it is probably pessimistic.) If $2^{|P|} > \varphi(4M_1M_3)$, then there is likely an $n$ in the appropriate congruence class. If $2^{|P|} > 2\varphi(4M_1M_3)$, there is likely such an $n$ with an odd number of prime factors.
- We call such a set a **"likely solution"**.
- In the mid-1990s, Red Alford and I presented at SERMON a set $P$ with cardinality $2030$, where $2\varphi(4M_1M_3) \approx 2^{1812}$.

# How to find $n$?

- Heuristics say $2^{218}$ solutions! How to find $1$?
- Trim $P$ to minimum possible set. ($|P| = 1812$.)
- Naive way: form all possible subproducts; check if they win. Work: $2^{|P|}$.
- Less naive way: form all possible subproducts of odd cardinality. Work: $2^{|P|-1}$.
- Better way: categorize $P$ into equally sized subsets $P_1$ and $P_2$. Compute all possible subproducts of $P_1$ mod $4M_1M_3$. Compute all possible subproducts of $P_2$. Sort the two lists together in a clever way; if you get any matches, you win! Work: $2^{|P|/2}$.
- Practical way...Work: $2^{40}$. (Unfortunately not known to exist.)

# Relax!

- Carl's conditions were very strict. You can relax a number of them and still get a solution to the $620 problem (though perhaps not a Carmichael number). For example, you need $ord_2(p)|2M_1$, not necessarily $p-1|2M_1$ (though the latter implies the former).
- Similarly, you can look at the "Fibonacci order" instead of $p+1$.
- Also, if you look at primes that are $3 \bmod 4$ instead of $3 \bmod 8$, you lose the *strong* pseudoprime, but you get more primes to choose from. (You have to add powers of $2$ to $M_1$.)
- You don't need $(p^2-1)/8$ squarefree.
- You don't need to categorize primes by their value $\mathrm{mod} 4$; you can be smarter.

# Chen/Greene

- In a 2003 paper, Chen and Greene develop each of these ideas.
- They find a likely set with $1241$ elements.
- They use $70$ primes in each of $M_1$ and $M_3$. (Red and I used $100$ each.)
- They carefully assign primes to $M_1$ and $M_3$ to balance them out.
- This paper renewed my interest in reducing the size of likely sets.

# Don't be smart, be dumb!

- The general method for finding primes is constructing $p-1$ to be smooth, then testing $p$ for primality and $ord_f(p)$ for smoothness.
- (Alternatively, construct $p+1$...)
- Cycle through $k$-subsets of $Q_1$ and/or $Q_3$.
- It's almost as cheap to test $p+1$ for $M_1M_3$-smoothness as $M_3$-smoothness.
- Not horrifically more expensive to cycle through $k$-subsets of $Q$ than of $Q_1$.
- Let $Q_1$ and $Q_3$ choose themselves.

# Method to the madness

- Construct $k$-subsets of $Q$ with $B = 811$ for small $k$.
- Randomly separate $Q$ into $Q_1$ and $Q_3$. Repeat. Keep highest cardinality set.
- Try switching primes back and forth between $Q_1$ and $Q_3$...up to $9$ primes at a time. See if it improves.
- Construct $k$-subsets of $Q_1$ and $Q_3$ for slightly larger $k$.
- Try switching primes again.
- Don't have enough primes. Bump $B$ to $827$; search for primes $p$ where $p + 1$ is a multiple of $821$, $823$, or $827$.
- Find likely set of size $1182$. ($71$ primes in $Q_1$; $72$ in $Q_2$.)
- Celebrate! Write talk.
- Re-do more systematically. Write paper as if you knew the correct bound to begin with. (To do.)

# On the horizon

- Generate more primes?
- (Increase size of $k$ in both steps.)
- (Include primes $> 827$ as long as they don't divide the order.)
- Search smarter?
- One idea: let the primes be nodes on a graph. Connect two primes if they are "compatible".
  - $(\mathrm{gcd}(ord_2(q_1), ord_f(q_2))|2$, etc.)
  - Find maximal complete subgraph.
  - This is probably NP-complete...
- Other types (Perrin Q-pseudoprimes)