The $620 problem

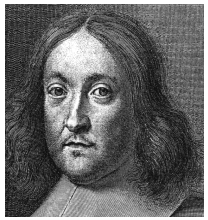
Jon Grantham

Institute for Defense Analyses
Center for Computing Sciences

June 11, 2015

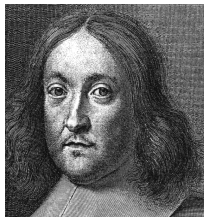
Pseudoprimes

- For all odd primes p, Fermat's Little Theorem tells us that $2^{p-1} \equiv 1 \pmod{p}$.
- An odd composite with this property is called a **Fermat pseudoprime**.



Pseudoprimes

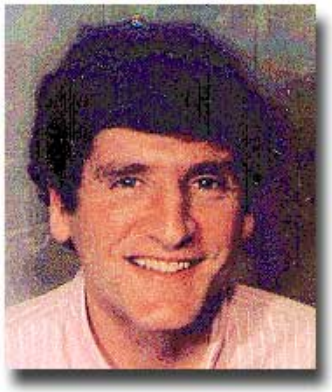
- For all odd primes p, Fermat's Little Theorem tells us that $2^{p-1} \equiv 1 \pmod{p}$.
- An odd composite with this property is called a **Fermat pseudoprime**.



- For all primes $p \neq 5$, p divides F_{p-1} if $p \equiv \pm 1 \pmod{5}$, otherwise $p | F_{p+1}$.
- (F_k is the kth Fibonacci number.)
- A composite satisfying this property is a **Fibonacci pseudoprime**.

Where did the $620 come from?

- In a 1980 paper, Pomerance, Selfridge and Wagstaff asked whether there was a number $n \equiv 2, 3 \pmod 5$ that was both types of pseudoprimes.



- They later offered $620 for such a number, or a proof that none exists.

Pomerance's Heuristic

- In 1984, Pomerance gave a heuristic as to why infinitely many such numbers should exist.

Pomerance's Heuristic

- In 1984, Pomerance gave a heuristic as to why infinitely many such numbers should exist.

- `http://www.pseudoprime.com/dopo.pdf`

Pomerance's Heuristic

- In 1984, Pomerance gave a heuristic as to why infinitely many such numbers should exist.

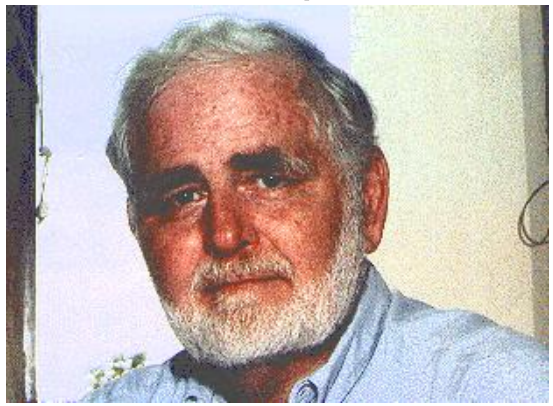
- `http://www.pseudoprime.com/dopo.pdf`
- It's a modification of the Erdös heuristic on Carmichael numbers.
- Let Q_1 be the set of primes $1 \pmod 4$ (except 5) up to a bound B. Similarly, Q_3.
- Look for primes $p \equiv 3, 27 \pmod{40}$ with $p - 1$ $2Q_1$-smooth and $p + 1$ $4Q_3$-smooth.
- Let P be a set of those primes.

Pomerance's Heuristic (continued)

- 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 n 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.

Likely sets

- If $2^{|P|} > \varphi(4M_1M_3)$, heuristics say likely solution.
- In mid-1990s at SERMON, Alford and I and presented a set $|P| = 2030$, $\varphi(4M_1M_3) \approx 2^{1812}$.



- So a "likely set" of size 1812.
- Best known algorithm for finding a solution square-root, so 2^{906} work.

Chen/Greene

- In a 2003 paper, Chen/Greene find a likely set of size 1241.

- Key ingredients:
  - Require $ord_2(p)|2M_1$, rather than $p-1|2M_1$.
  - Similarly with "Fibonacci order".
  - Allow prime powers in Q_1 and Q_3.
  - Drop congruence restrictions (lose strong pseudoprime).
  - Carefully assign small primes to Q_1 and Q_3 for "balance".

2005 talk at SERMON

- Generate primes p with $p-1$ and $p+1$ 827-smooth.
- Assign primes randomly to Q_1 and Q_3.
- Repeat, choose Q_1 and Q_3 with largest number of primes.
- Try small alterations to Q_1 and Q_3 to see if they help.
- Generate "likely set" of size 1182.

2013 talk at SERMON

- Find all primes p with $p^2 - 1$ 1163-smooth with at most 7 primes dividing $p - 1$ (some arbitrary limit on prime powers).
- Needed to increase from 827 partially to get solution without $ord_2(p)$ or Fibonacci order.

2013 talk at SERMON

- Find all primes p with $p^2 - 1$ 1163-smooth with at most 7 primes dividing $p - 1$ (some arbitrary limit on prime powers).
- Needed to increase from 827 partially to get solution without $ord_2(p)$ or Fibonacci order.
- Look at many random selections of Q_1 and Q_3.
- Try alterations of up to 2 primes at a time to see if it improves.

2013 talk at SERMON

- Find all primes p with $p^2 - 1$ 1163-smooth with at most 7 primes dividing $p - 1$ (some arbitrary limit on prime powers).
- Needed to increase from 827 partially to get solution without $ord_2(p)$ or Fibonacci order.
- Look at many random selections of Q_1 and Q_3.
- Try alterations of up to 2 primes at a time to see if it improves.
- It always does, at first.
- Use hill-climbing to get local maximum.

2013 talk at SERMON

- Find all primes p with $p^2 - 1$ 1163-smooth with at most 7 primes dividing $p - 1$ (some arbitrary limit on prime powers).
- Needed to increase from 827 partially to get solution without $ord_2(p)$ or Fibonacci order.
- Look at many random selections of Q_1 and Q_3.
- Try alterations of up to 2 primes at a time to see if it improves.
- It always does, at first.
- Use hill-climbing to get local maximum.
- Throw away least-used prime (not always 1163!)
- Repeat as long as you keep likely set.

2013 talk at SERMON

- Find all primes p with $p^2 - 1$ 1163-smooth with at most 7 primes dividing $p - 1$ (some arbitrary limit on prime powers).
- Needed to increase from 827 partially to get solution without $ord_2(p)$ or Fibonacci order.
- Look at many random selections of Q_1 and Q_3.
- Try alterations of up to 2 primes at a time to see if it improves.
- It always does, at first.
- Use hill-climbing to get local maximum.
- Throw away least-used prime (not always 1163!)
- Repeat as long as you keep likely set.
- \$620 minimal set:

2013 talk at SERMON

- Find all primes p with $p^2 - 1$ 1163-smooth with at most 7 primes dividing $p - 1$ (some arbitrary limit on prime powers).
- Needed to increase from 827 partially to get solution without $ord_2(p)$ or Fibonacci order.
- Look at many random selections of Q_1 and Q_3.
- Try alterations of up to 2 primes at a time to see if it improves.
- It always does, at first.
- Use hill-climbing to get local maximum.
- Throw away least-used prime (not always 1163!)
- Repeat as long as you keep likely set.
- \$620 minimal set:1148.

2013 talk at SERMON

- Find all primes p with $p^2 - 1$ 1163-smooth with at most 7 primes dividing $p - 1$ (some arbitrary limit on prime powers).
- Needed to increase from 827 partially to get solution without $ord_2(p)$ or Fibonacci order.
- Look at many random selections of Q_1 and Q_3.
- Try alterations of up to 2 primes at a time to see if it improves.
- It always does, at first.
- Use hill-climbing to get local maximum.
- Throw away least-used prime (not always 1163!)
- Repeat as long as you keep likely set.
- \$620 minimal set:1148.
- It turns out that the set of smallest primes is not optimal!

Zhang

- Zhang 2015 Math. Comp. paper.
- Optimal choice of prime powers
- Likely set of size 1004, but allows 5 to divide $p \pm 1$.

Future directions

- Generate more primes.
- Use Zhang for choice of prime powers
- Smarter hill-climbing?
- Subset-product algorithms.
- Give up?

Thanks, Carl!