Fast Tabulation of Challenge Pseudoprimes

Andrew Shallue
Jonathan Webster

Illinois Wesleyan University
Butler University

ANTS-XIII, 2018

Outline

- Elementary theorems and definitions
- Challenge pseudoprime
- Algorithmic theory
- Sketch of analysis
- Future work

Fermat's Little Theorem

Theorem

If p is prime and $\gcd(b,p) = 1$ *then*

$$b^{p-1} \equiv 1 \pmod{p}.$$

Fermat's Little Theorem

Theorem

If p is prime and $\gcd(b, p) = 1$ *then*

$$b^{p-1} \equiv 1 \pmod{p}.$$

Definition

If n is a composite integer with $\gcd(b, n) = 1$ and

$$b^{n-1} \equiv 1 \pmod{n}$$

then we call n a *base b Fermat pseudoprime*.

Lucas Sequences

Definition

Let P, Q be integers, and let $D = P^2 - 4Q$ (called the discriminant). Let α and β be the two roots of $x^2 - Px + Q$. Then we have an integer sequence U_k defined by

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}$$

called the (P, Q)-Lucas sequence.

Definition

Equivalently, we may define this as a recurrence relation:

$$U_0 = 0, \quad U_1 = 1, \quad \textit{and} \quad U_n = PU_{n-1} - QU_{n-2}.$$

An Analogous Theorem

Theorem

Let the (P, Q)-Lucas sequence be given, and let $\epsilon(n) = (D|n)$ be the Jacobi symbol. If p is an odd prime and $\gcd(p, 2QD) = 1$, then

$$U_{p-\epsilon(p)} \equiv 0 \pmod{p}$$

An Analogous Theorem

Theorem

Let the (P, Q)-Lucas sequence be given, and let $\epsilon(n) = (D|n)$ be the Jacobi symbol. If p is an odd prime and $\gcd(p, 2QD) = 1$, then

$$U_{p-\epsilon(p)} \equiv 0 \pmod{p}$$

Definition

If n is a composite integer with $\gcd(n, 2QD) = 1$ such that

$$U_{n-\epsilon(n)} \equiv 0 \pmod{n}$$

then we call n a (P, Q)-*Lucas pseudoprime.*

Challenge Pseudoprimes

Definition

A composite number n is a (b, P, Q)-challenge pseudoprime if it is

- a base b Fermat pseudoprime,
- a (P, Q)-Lucas pseudoprime, and
- $\epsilon(n) = -1$.

Examples

Previously seen...

Examples

Previously seen...

- Pomerance, Selfridge, and Wagstaff offer \$620 for a $(2, 1, -1)$-challenge pseudoprime.

Examples

Previously seen...

- Pomerance, Selfridge, and Wagstaff offer \$620 for a $(2, 1, -1)$-challenge pseudoprime.
- Jon Grantham offers \$6.20 for a $(5, 5, -5)$-challenge pseudoprime.

Examples

Previously seen...

- Pomerance, Selfridge, and Wagstaff offer \$620 for a $(2, 1, -1)$-challenge pseudoprime.
- Jon Grantham offers \$6.20 for a $(5, 5, -5)$-challenge pseudoprime.
- Baillie-PSW test is built around $(2, P, Q)$-challenge pseudoprimes.

Examples

Previously seen...

- Pomerance, Selfridge, and Wagstaff offer \$620 for a $(2, 1, -1)$-challenge pseudoprime.
- Jon Grantham offers \$6.20 for a $(5, 5, -5)$-challenge pseudoprime.
- Baillie-PSW test is built around $(2, P, Q)$-challenge pseudoprimes.
- Williams numbers are (b, P, Q)-challenge pseudoprimes for fixed D.

How Can We Find These?

How Can We Find These?

We can't.

How Can We Find These?

We can't.

Two theoretical approaches:

- Constructive: Computationally infeasible subset product problem.
  - Grantham and Alford
  - Chen and Greene

How Can We Find These?

We can't.

Two theoretical approaches:

- Constructive: Computationally infeasible subset product problem.
    - Grantham and Alford
    - Chen and Greene
- Enumerate: List base *b* Fermat pseudoprime and hope you get lucky.

First View on Fermat's Little Theorem

Problem

Given an preproduct k, find a prime p such that $n = kp$ is a base b-Fermat pseudoprime.

Examining the exponent in Fermat's Little Theorem:

$$n - 1 = kp - 1 = k(p - 1) + k - 1$$

First View

Since $\ell_b(p)$ divides $n - 1$ and $p - 1$, $\ell_b(p) | k - 1$. So

$$p | b^{k-1} - 1.$$

Second View on Fermat's Little Theorem

Problem

Given an preproduct k, find a prime p such that $n = kp$ is a base b-Fermat pseudoprime.

Note, $b^{kp-1} \equiv 1 \pmod{p_i}$ for all $p_i | k$, so

$$kp \equiv 1 \pmod{\ell_b(p_i)}.$$

Second View

Let $L = \mathrm{lcm}(\ell_b(p_1), \ldots, \ell_b(p_t))$, then

$$p \equiv k^{-1} \pmod{L}.$$

Two Views on the Analogous Theorem

First View

$$p | U_{k-\epsilon(k)}.$$

Second View

Let $W = \mathrm{lcm}(\omega(p_1), \ldots, \omega(p_t))$, then

$$p \equiv -k^{-1} \pmod{W}.$$

Finding k

Definition

A number k is *admissible* if

$$\gcd(L,k)=1, \quad \gcd(W,k)=1, \quad \text{and} \quad \gcd(L,W)<3.$$

Finding k

Definition

A number k is *admissible* if

$$\gcd(L, k) = 1, \quad \gcd(W, k) = 1, \quad \text{and} \quad \gcd(L, W) < 3.$$

Consequences:

- Primes with $\epsilon(p) = -1$ will always be admissible.
- Primes with $\epsilon(p) = 1$ will rarely be admissible.

Tabulation of Challenge Pseudoprimes

Create all admissible k up to some bound.

1. If k is small, then find p as a divisor of $\gcd(b^{k-1} - 1, U_{k-\epsilon(k)})$
2. If $\mathrm{lcm}(L, W)$ is large, then find p by sieving

$$p \equiv \begin{cases} k^{-1} & \mod L \\ -k^{-1} & \mod W \end{cases}$$

Note:

1. GCD computation time monotonically increases with k.
2. Sieve time does not monotonically decrease with k.

Analysis: A Sketch

We want an estimate of

$$\sum_{p<\sqrt{B}} \min\{\text{gcd cost}, \text{sieve cost}\}.$$

We estimate

$$\sum_{p<X} \text{gcd cost} + \sum_{X<p<\sqrt{B}} \text{sieve cost}.$$

Analysis: A Sketch (cont.)

This is

$$\sum_{p<X} O(p) + \sum_{X<p<\sqrt{B}} O\left(\frac{B}{p\ell_b(p)\omega(p)}\right).$$

The interval length is B/p and the sieve step size is $\ell_b(p)\omega(p)$.

This requires we balance:

$$O(X^2) + O(B/X)$$

for a run-time of

$$O(B^{2/3}).$$

Actual Results

Theorem

There exists an algorithm which tabulates challenge pseudoprimes up to B with t prime factors using $O(B^{1-\frac{1}{3t-1}})$ bit operations. Under the heuristic assumption that factoring plays a minimal role, then the time is $O(B^{1-\frac{1}{2t-1}})$.

Actual Results

Theorem

There exists an algorithm which tabulates challenge pseudoprimes up to B with t prime factors using $O(B^{1-\frac{1}{3t-1}})$ bit operations. Under the heuristic assumption that factoring plays a minimal role, then the time is $O(B^{1-\frac{1}{2t-1}})$.

Theorem

There are no $(2, 1, -1)$ challenge pseudoprimes with 2 or 3 prime factors less than 2^{80}.

Challenging Challenges

- \$20 for a $(2, 1, -1)$ challenge pseudoprime with an even number of prime factors.
- \$20 for a $(2, 1, -1)$ challenge pseudoprime with exactly three prime factors.
- \$6 for a $(2, 1, -1)$ challenge pseudoprime divisible by 3.

Future Work

- Strong challenge pseudoprimes
  - Fewer admissible k.
  - Smaller gcds.
  - Large sieving moduli.
- Improved analysis.

Thank you for your time.