Baillie-PSW Pseudoprimes

The Quest For $620

Junhyun Lim, Shaunak Mashalkar, Ed Schaefer

Motivation

Primes are enigmatic but useful

Motivation

Primes are enigmatic but useful

Especially important in the internet age

Motivation

Primes are enigmatic but useful

Especially important in the internet age

However, they can be difficult to find

Primality Tests

Primality Tests are ways to investigate arbitrary numbers

Primality Tests

Primality Tests are ways to investigate arbitrary numbers

Sieve of Eratosthenes and trial division are primality tests

Primality Tests

Primality Tests are ways to investigate arbitrary numbers

Sieve of Eratosthenes and trial division are primality tests

However, both of these tests are slow

Division Revision

Given $a, x \in \mathbb{Z}$ we have $a = bx + r$ for some $b \in \mathbb{Z}$ and $0 \leq r < x$

Division Revision

Given $a, x \in \mathbb{Z}$ we have $a = bx + r$ for some $b \in \mathbb{Z}$ and $0 \leq r < x$

If $r = 0$ or $a = bx$, then x divides a and we write $x|a$

Division Revision

Given $a, x \in \mathbb{Z}$ we have $a = bx + r$ for some $b \in \mathbb{Z}$ and $0 \leq r < x$

If $r = 0$ or $a = bx$, then x divides a and we write $x|a$

If $a = bx + r$ and $m = nx + r$, we write $a \equiv m \pmod{x}$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)}$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)}$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7 = 128$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7 = 128 \equiv 0 \pmod{8}$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7 = 128 \equiv 0 \pmod{8}$
- $n = 9$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7 = 128 \equiv 0 \pmod{8}$
- $n = 9$: $2^{(9-1)}$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7 = 128 \equiv 0 \pmod{8}$
- $n = 9$: $2^{(9-1)} = 2^8$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7 = 128 \equiv 0 \pmod{8}$
- $n = 9$: $2^{(9-1)} = 2^8 = 256$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7 = 128 \equiv 0 \pmod{8}$
- $n = 9$: $2^{(9-1)} = 2^8 = 256 = 252 + 4$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7 = 128 \equiv 0 \pmod{8}$
- $n = 9$: $2^{(9-1)} = 2^8 = 256 = 252 + 4 \equiv 4 \pmod{9}$

(Base-2) Fermat Primality Test

Suppose some integer $n > 2$

Compute $2^{(n-1)} \pmod{n}$ for composite n

- $n = 6$: $2^{(6-1)} = 2^5 = 32 = 30 + 2 \equiv 2 \pmod{6}$
- $n = 8$: $2^{(8-1)} = 2^7 = 128 \equiv 0 \pmod{8}$
- $n = 9$: $2^{(9-1)} = 2^8 = 256 = 252 + 4 \equiv 4 \pmod{9}$
- $n = 341$: $2^{340} \equiv 1 \pmod{341}$

(Base-2) Fermat Primality Test

The composite examples show no pattern

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: 2^{5-1}

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod{5}$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod{5}$
- $n = 7$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod{5}$
- $n = 7$: 2^{7-1}

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod n$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod 5$
- $n = 7$: $2^{7-1} = 2^6$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod 5$
- $n = 7$: $2^{7-1} = 2^6 = 64$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod n$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod 5$
- $n = 7$: $2^{7-1} = 2^6 = 64 = 63 + 1$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod{5}$
- $n = 7$: $2^{7-1} = 2^6 = 64 = 63 + 1 \equiv 1 \pmod{7}$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod{5}$
- $n = 7$: $2^{7-1} = 2^6 = 64 = 63 + 1 \equiv 1 \pmod{7}$
- $n = 11$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod{5}$
- $n = 7$: $2^{7-1} = 2^6 = 64 = 63 + 1 \equiv 1 \pmod{7}$
- $n = 11$: 2^{11-1}

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod{5}$
- $n = 7$: $2^{7-1} = 2^6 = 64 = 63 + 1 \equiv 1 \pmod{7}$
- $n = 11$: $2^{11-1} = 2^{10}$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod n$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod 5$
- $n = 7$: $2^{7-1} = 2^6 = 64 = 63 + 1 \equiv 1 \pmod 7$
- $n = 11$: $2^{11-1} = 2^{10} = 1024$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod 5$
- $n = 7$: $2^{7-1} = 2^6 = 64 = 63 + 1 \equiv 1 \pmod 7$
- $n = 11$: $2^{11-1} = 2^{10} = 1024 = 1023 + 1$

(Base-2) Fermat Primality Test

The composite examples show no pattern

What about $2^{(n-1)} \pmod{n}$ for prime n?

- $n = 5$: $2^{5-1} = 2^4 = 16 = 15 + 1 \equiv 1 \pmod{5}$
- $n = 7$: $2^{7-1} = 2^6 = 64 = 63 + 1 \equiv 1 \pmod{7}$
- $n = 11$: $2^{11-1} = 2^{10} = 1024 = 1023 + 1 \equiv 1 \pmod{11}$

(Base-2) Fermat Primality Test

Theorem

For any $n > 2$, if n is prime, then $2^{(n-1)} \equiv 1 \pmod{n}$

(Base-2) Fermat Primality Test

Theorem

For any $n > 2$, if n is prime, then $2^{(n-1)} \equiv 1 \pmod{n}$

Much faster than the first two tests

(Base-2) Fermat Primality Test

Theorem

For any $n > 2$, if n is prime, then $2^{(n-1)} \equiv 1 \pmod{n}$

Much faster than the first two tests, but *probabilistic*

(Base-2) Fermat Primality Test

Theorem

For any $n > 2$, if n is prime, then $2^{(n-1)} \equiv 1 \pmod{n}$

Much faster than the first two tests, but *probabilistic*

$11 | 341$, yet $2^{340} \equiv 1 \pmod{341}$ – a false positive!

False Positives

Definition

A *pseudoprime* is a composite number that gives a false positive on a primality test.

False Positives

Definition

A *pseudoprime* is a composite number that gives a false positive on a primality test.

A number that fools the X primality test is an X pseudoprime

False Positives

Definition
A *pseudoprime* is a composite number that gives a false positive on a primality test.

A number that fools the X primality test is an X pseudoprime

For a good probabilistic test, pseudoprimes are rare

False Positives

Probabilistic tests are chosen to be very fast

False Positives

Probabilistic tests are chosen to be very fast

We could potentially run multiple tests for accuracy

False Positives

Probabilistic tests are chosen to be very fast

We could potentially run multiple tests for accuracy

For two probable primality tests X and Y, does there exist a number that is both an X and Y pseudoprime?

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$F_2 = F_0 + F_1$

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$$F_2 = F_0 + F_1 = 0 + 1$$

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$$F_2 = F_0 + F_1 = 0 + 1 = 1$$

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$F_2 = F_0 + F_1 = 0 + 1 = 1$

F_3

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$$F_2 = F_0 + F_1 = 0 + 1 = 1$$

$$F_3 = F_1 + F_2$$

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$$F_2 = F_0 + F_1 = 0 + 1 = 1$$

$$F_3 = F_1 + F_2 = 1 + 1$$

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$$F_2 = F_0 + F_1 = 0 + 1 = 1$$

$$F_3 = F_1 + F_2 = 1 + 1 = 2$$

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$F_2 = F_0 + F_1 = 0 + 1 = 1$

$F_3 = F_1 + F_2 = 1 + 1 = 2$, $F_4 = 3$

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$F_2 = F_0 + F_1 = 0 + 1 = 1$

$F_3 = F_1 + F_2 = 1 + 1 = 2$, $F_4 = 3$, $F_5 = 5$

The Fibonacci Sequence

Definition

Fibonacci Sequence: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

$$F_2 = F_0 + F_1 = 0 + 1 = 1$$

$$F_3 = F_1 + F_2 = 1 + 1 = 2,\ F_4 = 3,\ F_5 = 5$$

$$F_0 = 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610 = F_{15}$$

Fibonacci and Primes

If $p \equiv \pm 1 \pmod{5}$, then $p | F_{p-1}$

Fibonacci and Primes

If $p \equiv \pm 1 \pmod{5}$, then $p | F_{p-1}$

- $11 | F_{10} = 55 = (11)(5)$

Fibonacci and Primes

If $p \equiv \pm 1 \pmod 5$, then $p | F_{p-1}$

- $11 | F_{10} = 55 = (11)(5)$
- $19 | F_{18} = 2584 = (19)(136)$

Fibonacci and Primes

If $p \equiv \pm 1 \pmod 5$, then $p | F_{p-1}$

- $11 | F_{10} = 55 = (11)(5)$
- $19 | F_{18} = 2584 = (19)(136)$
- $29 | F_{28} = 317811 = (29)(10959)$

Fibonacci and Primes

If $p \equiv \pm 2 \pmod 5$, then $p | F_{p+1}$

Fibonacci and Primes

If $p \equiv \pm 2 \pmod{5}$, then $p | F_{p+1}$

- $2 | F_3 = 2$

Fibonacci and Primes

If $p \equiv \pm 2 \pmod 5$, then $p | F_{p+1}$

- $2 | F_3 = 2$
- $13 | F_{14} = 377 = (13)(29)$

Fibonacci and Primes

If $p \equiv \pm 2 \pmod 5$, then $p | F_{p+1}$

- $2 | F_3 = 2$
- $13 | F_{14} = 377 = (13)(29)$
- $323 | F_{324}$

Fibonacci and Primes

If $p \equiv \pm 2 \pmod 5$, then $p | F_{p+1}$

- $2 | F_3 = 2$
- $13 | F_{14} = 377 = (13)(29)$
- $323 | F_{324}$ – *Not a prime number:* $323 = (17)(19)$

Jacobi Symbols

Jacobi Symbols: For odd n, we have:

$$\left(\frac{5}{n}\right) = \begin{cases} 0 \text{ if } n = 5m, m \in \mathbb{Z} \\ 1 \text{ if } n \equiv \pm 1 \pmod 5 \\ -1 \text{ if } n \equiv \pm 2 \pmod 5 \end{cases}$$

We will use this to simplify notation

This is not the complete definition

Jacobi Symbols

Jacobi Symbols: For odd n, we have:

$$\left(\frac{5}{n}\right) = \begin{cases} 0 \text{ if } n = 5m, m \in \mathbb{Z} \\ 1 \text{ if } n \equiv \pm 1 \pmod 5 \\ -1 \text{ if } n \equiv \pm 2 \pmod 5 \end{cases}$$

For $n = ab$ where $n, a, b \in \mathbb{Z}$ are odd:

$$\left(\frac{5}{n}\right) = \left(\frac{5}{a}\right)\left(\frac{5}{b}\right)$$

Fibonacci Primality Test

Let $n > 1$ be an arbitrary integer

Fibonacci Primality Test

Let $n > 1$ be an arbitrary integer

If n divides $F_{n-\left(\frac{5}{n}\right)}$ then n is *probably* prime

Fibonacci Primality Test

Let $n > 1$ be an arbitrary integer

If n divides $F_{n-\left(\frac{5}{n}\right)}$ then n is *probably* prime

Reminder:

- If $n \equiv \pm 1 \pmod{5}$, $F_{n-\left(\frac{5}{n}\right)} = F_{n-1}$

Fibonacci Primality Test

Let $n > 1$ be an arbitrary integer

If n divides $F_{n-\left(\frac{5}{n}\right)}$ then n is *probably* prime

Reminder:

- If $n \equiv \pm 1 \pmod 5$, $F_{n-\left(\frac{5}{n}\right)} = F_{n-1}$
- If $n \equiv \pm 2 \pmod 5$, $F_{n-\left(\frac{5}{n}\right)} = F_{n-(-1)} = F_{n+1}$

Fibonacci & Fermat

We now have two probable primality tests

Fibonacci & Fermat

We now have two probable primality tests

Is there a common pseudoprime between them?

Fibonacci & Fermat

We now have two probable primality tests

Is there a common pseudoprime between them? **Yes**

Fibonacci & Fermat

We now have two probable primality tests

Is there a common pseudoprime between them? **Yes**

There are actually several

Common False Positives

Common False Positives

79624621

Common False Positives

79624621, 17969789

Common False Positives

79624621, 17969789, 3807749821

Common False Positives

79624621, 17969789, 3807749821 – all $\pm 1 \pmod 5$

Common False Positives

79624621, 17969789, 3807749821 – all $\pm 1 \pmod 5$

What about $\pm 2 \pmod 5$?

Common False Positives

79624621, 17969789, 3807749821 – all $\pm 1 \pmod 5$

What about $\pm 2 \pmod 5$? **No known examples**

Common False Positives

79624621, 17969789, 3807749821 – all $\pm 1 \pmod 5$

What about $\pm 2 \pmod 5$? **No known examples**

However there is no proof that one cannot exist

The Mythical $\pm 2 \pmod 5$ Example

Is it impossible to find a counterexample?

The Mythical $\pm 2 \pmod 5$ Example

Is it impossible to find a counterexample?

Yes: We have a fast primality test for half of all candidates

The Mythical $\pm 2 \pmod 5$ Example

Is it impossible to find a counterexample?

Yes: We have a fast primality test for half of all candidates

No: The implications are a mystery but likely significant

The Quest For \$620

Does there exist an odd composite number that is $\pm 2 \pmod 5$, a base-2 Fermat pseudoprime, and a Fibonacci pseudoprime?

The Quest For \$620

Does there exist an odd composite number that is $\pm 2 \pmod 5$, a base-2 Fermat pseudoprime, and a Fibonacci pseudoprime?

There are already methods to generate Fermat pseudoprimes

The Quest For \$620

Does there exist an odd composite number that is $\pm 2 \pmod{5}$, a base-2 Fermat pseudoprime, and a Fibonacci pseudoprime?

There are already methods to generate Fermat pseudoprimes

Our approach generates Fibonacci pseudoprimes instead

The Quest For \$620

Does there exist an odd composite number that is $\pm 2 \pmod 5$*, a base-2 Fermat pseudoprime, and a Fibonacci pseudoprime?*

There are already methods to generate Fermat pseudoprimes

Our approach generates Fibonacci pseudoprimes instead

We then filter for $\pm 2 \pmod 5$ and run a base-2 Fermat test

Fibonacci and Divisibility: Part 1

Theorem

$F_m|F_n$ if and only if $m|n$ or $m = 2$ (If $m = 2$, $F_m = 1$)

Fibonacci and Divisibility: Part 1

Theorem

$F_m|F_n$ if and only if $m|n$ or $m = 2$ (If $m = 2$, $F_m = 1$)

$F_3 = 2$

Fibonacci and Divisibility: Part 1

Theorem

$F_m | F_n$ *if and only if* $m | n$ *or* $m = 2$ *(If* $m = 2$*,* $F_m = 1$*)*

$F_3 = 2$: 1, 1, **2**, 3, 5, **8**, 13, 21, **34**, 55, 89, **144**, 233, 377, **610**

Fibonacci and Divisibility: Part 1

Theorem

$F_m|F_n$ *if and only if* $m|n$ *or* $m = 2$ *(If* $m = 2$*,* $F_m = 1$*)*

$F_3 = 2$: 1, 1, **2**, 3, 5, **8**, 13, 21, **34**, 55, 89, **144**, 233, 377, **610**

$F_4 = 3$

Fibonacci and Divisibility: Part 1

Theorem

$F_m | F_n$ if and only if $m | n$ or $m = 2$ (If $m = 2$, $F_m = 1$)

$F_3 = 2$: 1, 1, **2**, 3, 5, **8**, 13, 21, **34**, 55, 89, **144**, 233, 377, **610**

$F_4 = 3$: 1, 1, 2, **3**, 5, 8, 13, **21**, 34, 55, 89, **144**, 233, 377, 610

Fibonacci and Divisibility: Part 1

Theorem

$F_m|F_n$ if and only if $m|n$ or $m = 2$ (If $m = 2$, $F_m = 1$)

$F_3 = 2$: 1, 1, **2**, 3, 5, **8**, 13, 21, **34**, 55, 89, **144**, 233, 377, **610**

$F_4 = 3$: 1, 1, 2, **3**, 5, 8, 13, **21**, 34, 55, 89, **144**, 233, 377, 610

$F_5 = 5$

Fibonacci and Divisibility: Part 1

Theorem

$F_m | F_n$ if and only if $m | n$ or $m = 2$ (If $m = 2$, $F_m = 1$)

$F_3 = 2$: 1, 1, **2**, 3, 5, **8**, 13, 21, **34**, 55, 89, **144**, 233, 377, **610**

$F_4 = 3$: 1, 1, 2, **3**, 5, 8, 13, **21**, 34, 55, 89, **144**, 233, 377, 610

$F_5 = 5$: 1, 1, 2, 3, **5**, 8, 13, 21, 34, **55**, 89, 144, 233, 377, **610**

Greatest Common Divisor

$\gcd(a, b)$ is the largest $n \in \mathbb{Z}^+$ such that $n|a$ and $n|b$

Greatest Common Divisor

$\gcd(a, b)$ is the largest $n \in \mathbb{Z}^+$ such that $n|a$ and $n|b$

For $b = ax + r$, $\gcd(a, b) = \gcd(a, ax + r) = \gcd(a, r)$

Greatest Common Divisor

$\gcd(a, b)$ is the largest $n \in \mathbb{Z}^+$ such that $n|a$ and $n|b$

For $b = ax + r$, $\gcd(a, b) = \gcd(a, ax + r) = \gcd(a, r)$

$\gcd(68, 60) = \gcd(8, 60)$

Greatest Common Divisor

$\gcd(a, b)$ is the largest $n \in \mathbb{Z}^+$ such that $n|a$ and $n|b$

For $b = ax + r$, $\gcd(a, b) = \gcd(a, ax + r) = \gcd(a, r)$

$\gcd(68, 60) = \gcd(8, 60) = \gcd(8, 4) = 4$

Fibonacci and Divisibility: Part 2

Theorem

Let m, n *be positive integers. Then* $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

Fibonacci and Divisibility: Part 2

Theorem

Let m, n be positive integers. Then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

L:	1	2	3	4	5	6	7	8	9	10	11	12	...
F_L:	1	1	2	3	5	8	13	21	34	55	89	144	...

Fibonacci and Divisibility: Part 2

Theorem

Let m, n be positive integers. Then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

L:	1	2	3	4	**5**	6	**7**	8	9	10	11	12	...
F_L:	1	1	2	3	**5**	8	**13**	21	34	55	89	144	...

Fibonacci and Divisibility: Part 2

Theorem

Let m, n be positive integers. Then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

L:	***1***	2	3	4	**5**	6	**7**	8	9	10	11	12	…
F_L:	***1***	1	2	3	**5**	8	**13**	21	34	55	89	144	…

Fibonacci and Divisibility: Part 2

Theorem

Let m, n *be positive integers. Then* $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

L:	5	6	7	8	9	10	11	12	13	14	15	…
F_L:	5	8	13	21	34	55	89	144	233	377	610	…

Fibonacci and Divisibility: Part 2

Theorem

Let m, n *be positive integers. Then* $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

L:	5	**6**	7	8	9	10	11	**12**	13	14	15	...
F_L:	5	**8**	13	21	34	55	89	**144**	233	377	610	...

Fibonacci and Divisibility: Part 2

Theorem

Let m, n be positive integers. Then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

L:	5	***6***	7	8	9	10	11	**12**	13	14	15	...
F_L:	5	***8***	13	21	34	55	89	**144**	233	377	610	...

Fibonacci and Divisibility: Part 2

Theorem

Let m, n be positive integers. Then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

L:	5	6	7	8	9	10	11	12	13	14	15	...
F_L:	5	8	13	21	34	55	89	144	233	377	610	...

Fibonacci and Divisibility: Part 2

Theorem

Let m, n be positive integers. Then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

L:	5	6	7	8	9	**10**	11	12	13	14	**15**	...
F_L:	5	8	13	21	34	**55**	89	144	233	377	**610**	...

Fibonacci and Divisibility: Part 2

Theorem

Let m, n be positive integers. Then $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

L:	***5***	6	7	8	9	**10**	11	12	13	14	**15**	...
F_L:	***5***	8	13	21	34	**55**	89	144	233	377	**610**	...

A Brief Lemma

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Then $\gcd(L, p - \left(\frac{5}{p}\right)) > 2$

A Brief Lemma

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Then $\gcd(L, p - \left(\frac{5}{p}\right)) > 2$

Proof: We know that for prime p, $p|F_{p-\left(\frac{p}{5}\right)}$

A Brief Lemma

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Then $\gcd(L, p - \left(\frac{5}{p}\right)) > 2$

Proof: We know that for prime p, $p|F_{p-\left(\frac{p}{5}\right)}$

So $p|\gcd(F_L, F_{p-\left(\frac{p}{5}\right)})$

A Brief Lemma

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Then $\gcd(L, p - \left(\frac{5}{p}\right)) > 2$

Proof: We know that for prime p, $p|F_{p-\left(\frac{p}{5}\right)}$

So $p|\gcd(F_L, F_{p-\left(\frac{p}{5}\right)})$ or $p|F_{\gcd(L, p-\left(\frac{p}{5}\right))}$

A Brief Lemma

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Then $\gcd(L, p - \left(\frac{5}{p}\right)) > 2$

Proof: Just showed $p|F_{\gcd(L,p-\left(\frac{p}{5}\right))}$.

A Brief Lemma

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Then $\gcd(L, p - \left(\frac{5}{p}\right)) > 2$

Proof: Just showed $p|F_{\gcd(L,p-\left(\frac{p}{5}\right))}$. Recall: $F_1 = F_2 = 1$

A Brief Lemma

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Then $\gcd(L, p - \left(\frac{5}{p}\right)) > 2$

Proof: Just showed $p|F_{\gcd(L,p-(\frac{p}{5}))}$. Recall: $F_1 = F_2 = 1$

Since $p \nmid 1$, $\gcd(L, p - (\frac{p}{5})) > 2$ and we are done

Interlude

Just proved: Let L be a positive integer and p be prime with $p|F_L$. Then $\gcd(L, p - \left(\frac{5}{p}\right)) > 2$.

Interlude

Just proved: Let L be a positive integer and p be prime with $p|F_L$. Then $\gcd(L, p - \left(\frac{5}{p}\right)) > 2$.

Given $a, b \in \mathbb{Z}$, $\gcd(a, b) \leq |a|$ and $|b|$ unless $|a|$ or $|b| = 0$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: Write $p \equiv \epsilon \pmod{L}$ where $\epsilon \in \{-1, 1\}$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: Write $p \equiv \epsilon \pmod{L}$ where $\epsilon \in \{-1, 1\}$

This means $p = kL + \epsilon$ for some $k \in \mathbb{Z}$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: We have $p = kL + \epsilon$, where $\epsilon \in \{-1, 1\}$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: We have $p = kL + \epsilon$, where $\epsilon \in \{-1, 1\}$

We write $2 < \gcd(L, p - \left(\frac{p}{5}\right))$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: We have $p = kL + \epsilon$, where $\epsilon \in \{-1, 1\}$

We write $2 < \gcd(L, p - \left(\frac{p}{5}\right))$ as $\gcd(L, kL + \epsilon - \left(\frac{p}{5}\right))$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: We simplify $2 < \gcd(L, kL + \epsilon - \left(\frac{p}{5}\right))$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: We simplify $2 < \gcd(L, kL + \epsilon - \left(\frac{p}{5}\right))$ to $\gcd(L, \epsilon - \left(\frac{p}{5}\right))$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p | F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: We simplify $2 < \gcd(L, kL + \epsilon - \left(\frac{p}{5}\right))$ to $\gcd(L, \epsilon - \left(\frac{p}{5}\right))$

$2 < \gcd(L, kL + \epsilon - \left(\frac{p}{5}\right)) \leq \left|\epsilon - \left(\frac{p}{5}\right)\right|$, or $\left|\epsilon - \left(\frac{p}{5}\right)\right| = 0$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: Now note that ϵ and $\left(\frac{p}{5}\right)$ are both either -1 or 1

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: Now note that ϵ and $\left(\frac{p}{5}\right)$ are both either -1 or 1

So $\left|\epsilon - \left(\frac{p}{5}\right)\right| \leq 2$

Important Jacobi Symbol Property

Lemma

Let L be a positive integer and p be prime with $p|F_L$. Assume $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \left(\frac{p}{5}\right) \pmod{L}$

Proof: Now note that ϵ and $\left(\frac{p}{5}\right)$ are both either -1 or 1

So $\left|\epsilon - \left(\frac{p}{5}\right)\right| \leq 2$ which forces $\epsilon - \left(\frac{p}{5}\right) = 0$

The Method

Theorem

Let L be a positive integer. Let $p_1, p_2, \ldots, p_k$, for some $k \geq 2$, be distinct primes dividing F_L such that $p_i \equiv \pm 1 \pmod{L}$ for each i and no p_i is equal to 2 or 5. Let $P = \prod_{i=1}^{k} p_i$. Then P is a Fibonacci pseudoprime.

Theorem

For distinct $p_1, p_2, \ldots, p_k$*,* $k \geq 2$*, if* $p_i | F_L$*,* $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i*, then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, if $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ and $p \neq 2, 5$ for all i, then $P = \prod_{i=1}^{k} p_i$ is a Fibonacci pseudoprime.

Need To Show: $P | F_{P - \left(\frac{5}{P}\right)}$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, if $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ and $p \neq 2, 5$ for all i, then $P = \prod_{i=1}^{k} p_i$ is a Fibonacci pseudoprime.

Need To Show: $P | F_{P - \left(\frac{5}{P}\right)}$

Same as: $P | x$ and $x | F_{P - \left(\frac{5}{P}\right)}$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Need To Show: $P | F_{P - \left(\frac{5}{P}\right)}$

Same as: $P | x$ and $x | F_{P - \left(\frac{5}{P}\right)}$

We can do this by choosing $x = F_L$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We need to show $P | F_L$ and $F_L | F_{P - \left(\frac{5}{P}\right)}$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We need to show $P | F_L$ and $F_L | F_{P - \left(\frac{5}{P}\right)}$

Since $p_i | F_L$ for each i and each p_i is distinct

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We need to show $P | F_L$ and $F_L | F_{P - \left(\frac{5}{P}\right)}$

Since $p_i | F_L$ for each i and each p_i is distinct, we have $P | F_L$

Theorem

For distinct $p_1, p_2, \ldots, p_k$*,* $k \geq 2$*, if* $p_i | F_L$*,* $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i*, then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: Now we need to show $F_L | F_{P - \left(\frac{5}{P}\right)}$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: Now we need to show $F_L | F_{P - \left(\frac{5}{P}\right)}$

Jacobi symbol property

Theorem

For distinct $p_1, p_2, \ldots, p_k$*,* $k \geq 2$*, if* $p_i | F_L$*,* $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i*, then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: Now we need to show $F_L | F_{P - \left(\frac{5}{P}\right)}$

Jacobi symbol property gives us $p_i \equiv \left(\frac{5}{p_i}\right) \pmod{L}$ for all i

Theorem

For distinct $p_1, p_2, \ldots, p_k$*,* $k \geq 2$*, if* $p_i | F_L$*,* $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i*, then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: Now we need to show $F_L | F_{P - \left(\frac{5}{P}\right)}$

Jacobi symbol property gives us $p_i \equiv \left(\frac{5}{p_i}\right) \pmod{L}$ for all i

Taking products gives $P \equiv \left(\frac{5}{P}\right) \pmod{L}$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We used $p_i \equiv \left(\frac{5}{p_i}\right) \pmod{L}$ to get $P \equiv \left(\frac{5}{P}\right) \pmod{L}$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We used $p_i \equiv \left(\frac{5}{p_i}\right) \pmod{L}$ to get $P \equiv \left(\frac{5}{P}\right) \pmod{L}$

This means $P - \left(\frac{5}{P}\right) \equiv 0 \pmod{L}$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We used $p_i \equiv \left(\frac{5}{p_i}\right) \pmod{L}$ to get $P \equiv \left(\frac{5}{P}\right) \pmod{L}$

This means $P - \left(\frac{5}{P}\right) \equiv 0 \pmod{L}$ or $L | \left(P - \left(\frac{5}{P}\right)\right)$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We have $L | \left(P - \left(\frac{5}{P}\right)\right)$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We have $L| \left(P - \left(\frac{5}{P}\right)\right)$ and want $F_L | F_{\left(P - \left(\frac{5}{P}\right)\right)}$

Theorem

For distinct $p_1, p_2, \ldots, p_k$*,* $k \geq 2$*, if* $p_i | F_L$*,* $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i*, then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We have $L | \left(P - \left(\frac{5}{P}\right)\right)$ and want $F_L | F_{\left(P - \left(\frac{5}{P}\right)\right)}$

We can use $L | \left(P - \left(\frac{P}{5}\right)\right)$ as indices to get $F_L | F_{\left(P - \left(\frac{P}{5}\right)\right)}$

Theorem

For distinct $p_1, p_2, \ldots, p_k$, $k \geq 2$, *if* $p_i | F_L$, $p_i \equiv \pm 1 \pmod{L}$ *and* $p \neq 2, 5$ *for all* i, *then* $P = \prod_{i=1}^{k} p_i$ *is a Fibonacci pseudoprime.*

Proof: We have $L|\left(P - \left(\frac{5}{P}\right)\right)$ and want $F_L | F_{\left(P - \left(\frac{5}{P}\right)\right)}$

We can use $L|\left(P - \left(\frac{P}{5}\right)\right)$ as indices to get $F_L | F_{\left(P - \left(\frac{P}{5}\right)\right)}$

Since $P | F_L$ and $F_L | F_{\left(P - \left(\frac{P}{5}\right)\right)}$, we know $P | F_{\left(P - \left(\frac{P}{5}\right)\right)}$

CS Introduction

Restating the burning question…

CS Introduction

Restating the burning question…

Question

Does there exist an odd composite number that is $\pm 2 \pmod 5$*, a base-2 Fermat pseudoprime, and a Fibonacci pseudoprime?*

CS Introduction

Restating the burning question...

Question

Does there exist an odd composite number that is $\pm 2 \pmod 5$, a base-2 Fermat pseudoprime, and a Fibonacci pseudoprime?

Previously...

CS Introduction

Restating the burning question...

Question

Does there exist an odd composite number that is $\pm 2 \pmod 5$*, a base-2 Fermat pseudoprime, and a Fibonacci pseudoprime?*

Previously...

It was shown that our candidate number doesn't exist in the range of 10^{17}. (Jeff Gilchrist, 2009)

Plan of Attack

Plan of Attack

- Find base-2 Fermat pseudoprimes and check that they're Fibonacci pseudoprimes. (Feitsma, Galway, Wagstaff)

Plan of Attack

- Find base-2 Fermat pseudoprimes and check that they're Fibonacci pseudoprimes. (Feitsma, Galway, Wagstaff)
- Create Fibonacci pseudoprimes that are $\pm 2 \pmod 5$ and check that they are base-2 Fermat pseudoprimes?

Modular Observations (1)

Consider the multiplication tables in $\mathbb{Z}_5$.

Modular Observations (1)

Consider the multiplication tables in $\mathbb{Z}_5$.

$\times$	1	4	2	3
1	1	4	2	3
4	4	1	3	2
2	2	3	4	1
3	3	2	1	4

$\times$	1	-1	2	-2
1	1	-1	2	-2
-1	-1	1	-2	2
2	2	-2	-1	1
-2	-2	2	1	-1

Modular Observations (2)

The following cases generate products that are $\pm 2 \mod 5$.

Modular Observations (2)

The following cases generate products that are $\pm 2 \mod 5$.

Table: Multiplication in $\mathbb{Z}_5$

$\times$	1	-1	2	-2
1	1	-1	2	-2
-1	-1	1	-2	2
2	2	-2	-1	1
-2	-2	2	1	-1

Modular Observations (2)

The following cases generate products that are $\pm 2 \mod 5$.

Cases:

Table: Multiplication in $\mathbb{Z}_5$

$\times$	1	-1	2	-2
1	1	-1	2	-2
-1	-1	1	-2	2
2	2	-2	-1	1
-2	-2	2	1	-1

Modular Observations (2)

The following cases generate products that are $\pm 2 \mod 5$.

Table: Multiplication in $\mathbb{Z}_5$

$\times$	1	-1	2	-2
1	1	-1	2	-2
-1	-1	1	-2	2
2	2	-2	-1	1
-2	-2	2	1	-1

Cases:

- Trivially, multiplying any number of $\pm 1 \mod 5$ elements to a $\pm 2 \mod 5$ will generate a $\pm 2 \mod 5$ element.

Modular Observations (2)

The following cases generate products that are $\pm 2 \mod 5$.

Table: Multiplication in $\mathbb{Z}_5$

$\times$	1	-1	2	-2
1	1	-1	2	-2
-1	-1	1	-2	2
2	2	-2	-1	1
-2	-2	2	1	-1

Cases:

- Trivially, multiplying any number of $\pm 1 \mod 5$ elements to a $\pm 2 \mod 5$ will generate a $\pm 2 \mod 5$ element.
- Multiplying an odd number of $\pm 2 \mod 5$ elements will generate a $\pm 2 \mod 5$ element.

Implementing The Algorithm (1)

Pseudoprime Algorithm:
Input: L, of F_L
Output: Fibonacci Pseudoprimes associated to F_L that are also $\pm 2 \pmod 5$

Implementing The Algorithm (1)

Pseudoprime Algorithm:
Input: L, of F_L
Output: Fibonacci Pseudoprimes associated to F_L that are also $\pm 2 \pmod 5$

1. Factorize F_L, and filter out the prime factors that are $\pm 1 \pmod L$

Implementing The Algorithm (1)

Pseudoprime Algorithm:
Input: L, of F_L
Output: Fibonacci Pseudoprimes associated to F_L that are also $\pm 2 \pmod 5$

1. Factorize F_L, and filter out the prime factors that are $\pm 1 \pmod L$
2. Partition the prime factors to $\pm 1 \pmod 5$, and $\pm 2 \pmod 5$.

Implementing The Algorithm (1)

Pseudoprime Algorithm:
Input: L, of F_L
Output: Fibonacci Pseudoprimes associated to F_L that are also $\pm 2 \pmod 5$

1. Factorize F_L, and filter out the prime factors that are $\pm 1 \pmod L$
2. Partition the prime factors to $\pm 1 \pmod 5$, and $\pm 2 \pmod 5$.
3. Combine the $\pm 1 \pmod 5$ factors with an odd number of $\pm 2 \pmod 5$ factors to generate candidate pseudoprimes.

A Note on Factorization

Factoring is hard!

A Note on Factorization

Factoring is hard!
...And our numbers were too big.

$$F_{9999} \approx 10^{2090}$$

Speaking of Big Numbers

Languages don't typically deal with ridiculously large numbers.

Speaking of Big Numbers

Languages don't typically deal with ridiculously large numbers.
Our Options:

- C++ (with gmp)
- Haskell
- Python
- ...Probably a few others!

Parsing Mersennus

Thankfully, a part of the work was done by **Mersennus**.

Parsing Mersennus

Thankfully, a part of the work was done by **Mersennus.**
Partial factorizations for up to F_{9999} had been completed.

Mersennus Formatting

Mersennus didn't have the best formatting of data.

Mersennus Formatting

Mersennus didn't have the best formatting of data.

1. The factorization of the even index Fibonacci numbers were formatted differently from the odd index ones.

Mersennus Formatting

Mersennus didn't have the best formatting of data.

1. The factorization of the even index Fibonacci numbers were formatted differently from the odd index ones.
2. The factorizations for larger Fibonacci numbers were incomplete.

For example

Here's an example of a data point from Mersennus.

For example

Here's an example of a data point from Mersennus.

F81 (3,9,27) 2269.4373.P5

For example

Here's an example of a data point from Mersennus.

F81 (3,9,27) 2269.4373.P5

F81 = F_{81}

For example

Here's an example of a data point from Mersennus.

F81 (3,9,27) 2269.4373.P5

F81 = F_{81}
2269.4373.P5 = prime factors split by .

For example

Here's an example of a data point from Mersennus.

F81 (3,9,27) 2269.4373.P5

F81 = F_{81}
2269.4373.P5 = prime factors split by .
We will ignore what P5 and (3,9,27) are for now...

Fibonacci Relations

Mersennus uses relations for data compression.

Fibonacci Relations

Mersennus uses relations for data compression.

1. $F_m | F_n \iff m|n$ or $m = 2$

Fibonacci Relations

Mersennus uses relations for data compression.

1. $F_m | F_n \iff m|n$ or $m = 2$
2. $F_{2n} = F_n L_n$

Where L_n are the Lucas numbers. $(2, 1, 3, 4, 7, 11, \ldots)$

Fibonacci Relations

Mersennus uses relations for data compression.

1. $F_m | F_n \iff m|n$ or $m = 2$
2. $F_{2n} = F_n L_n$

Where L_n are the Lucas numbers. $(2, 1, 3, 4, 7, 11, \dots)$
For each n, Mersennus only lists new prime factors that can not be deduced from (1) and (2) above.

Compression with (1)

Consider

F39 (3,13) 135721

Compression with (1)

Consider

$$\text{F39 (3,13) 135721}$$

Here (3,13) are the non-trivial factors of 39.

Compression with (1)

Consider

F39 (3,13) 135721

Here (3,13) are the non-trivial factors of 39.

$$m|n \implies F_m|F_n$$

Compression with (1)

Consider

F39 (3,13) 135721

Here (3,13) are the non-trivial factors of 39.

$$m|n \implies F_m|F_n$$

$$F_3|F_{39},\ F_{13}|F_{39}$$

Compression with (1)

Consider

F39 (3,13) 135721

Here (3,13) are the non-trivial factors of 39.

$$m|n \implies F_m|F_n$$
$$F_3|F_{39},\ F_{13}|F_{39}$$

Thus (3, 13) indicates the set of prime factors of F_3, F_{13} that we already know.

Compression with (1)

Consider

F39 (3,13) 135721

Here (3,13) are the non-trivial factors of 39.

$$m|n \implies F_m|F_n$$
$$F_3|F_{39},\ F_{13}|F_{39}$$

Thus (3, 13) indicates the set of prime factors of F_3, F_{13} that we already know.

135721 is the only new prime factor of F_{39}.

Proof of (2)

Prove $F_{2n} = F_n L_n$ holds.

Proof of (2)

Prove $F_{2n} = F_n L_n$ holds.

Let $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$.

Proof of (2)

Prove $F_{2n} = F_n L_n$ holds.

Let $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$.

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

Proof of (2)

Prove $F_{2n} = F_n L_n$ holds.

Let $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$.

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$
$$L_n = \alpha^n + \beta^n$$

Proof of (2)

Prove $F_{2n} = F_n L_n$ holds.

Let $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$.

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$
$$L_n = \alpha^n + \beta^n$$

Note, when $n = 2k$,

Proof of (2)

Prove $F_{2n} = F_n L_n$ holds.

Let $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$.

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$
$$L_n = \alpha^n + \beta^n$$

Note, when $n = 2k$,

$$F_{2k} = \frac{\alpha^{2k} - \beta^{2k}}{\alpha - \beta}$$

Proof of (2)

Prove $F_{2n} = F_n L_n$ holds.

Let $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$.

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$
$$L_n = \alpha^n + \beta^n$$

Note, when $n = 2k$,

$$\begin{aligned} F_{2k} &= \frac{\alpha^{2k} - \beta^{2k}}{\alpha - \beta} \\ &= \frac{(\alpha^k - \beta^k)(\alpha^k + \beta^k)}{\alpha - \beta} \end{aligned}$$

Proof of (2)

Prove $F_{2n} = F_n L_n$ holds.

Let $\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$.

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$
$$L_n = \alpha^n + \beta^n$$

Note, when $n = 2k$,

$$\begin{aligned} F_{2k} &= \frac{\alpha^{2k} - \beta^{2k}}{\alpha - \beta} \\ &= \frac{(\alpha^k - \beta^k)(\alpha^k + \beta^k)}{\alpha - \beta} = F_k L_k \end{aligned}$$

Useless Indices

There are also Fibonacci indices we don't need.

Useless Indices

There are also Fibonacci indices we don't need.

Lemma

Let L be a positive integer with $5|L$. Let p be an odd prime with $p|F_L$ with $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \pm 1 \pmod{5}$.

Useless Indices

There are also Fibonacci indices we don't need.

Lemma

Let L be a positive integer with $5|L$*. Let p be an odd prime with* $p|F_L$ *with* $p \equiv \pm 1 \pmod{L}$*. Then* $p \equiv \pm 1 \pmod{5}$*.*

Proof.

Since $5|L$ and $p \equiv \pm 1 \pmod{L}$, $p \equiv \pm 1 \pmod{5}$. □

Useless Indices

There are also Fibonacci indices we don't need.

Lemma

Let L be a positive integer with $5|L$. Let p be an odd prime with $p|F_L$ with $p \equiv \pm 1 \pmod{L}$. Then $p \equiv \pm 1 \pmod{5}$.

Proof.

Since $5|L$ and $p \equiv \pm 1 \pmod{L}$, $p \equiv \pm 1 \pmod{5}$. □

Can't use this to construct $\pm 2 \pmod{5}$ Fibonacci pseudoprimes!

Compressing Lucas Factors

There exist other compressions for Lucas factors.

Compressing Lucas Factors

There exist other compressions for Lucas factors.
Lucas factors in general don't satisfy the nice relation for Fibonacci numbers.

Compressing Lucas Factors

There exist other compressions for Lucas factors.
Lucas factors in general don't satisfy the nice relation for Fibonacci numbers.

$$m = 2 \text{ or } m|n \iff F_m|F_n$$

Compressing Lucas Factors

There exist other compressions for Lucas factors.
Lucas factors in general don't satisfy the nice relation for Fibonacci numbers.

$$m = 2 \text{ or } m|n \iff F_m|F_n$$

However, a similar, somewhat nice relation exists...

Lucas Relation

Being a sister sequence to the Fibonacci numbers, Lucas numbers satisfy the following property.

Lucas Relation

Being a sister sequence to the Fibonacci numbers, Lucas numbers satisfy the following property.

For $n, m \in \mathbb{Z}$ such that $m|n$,

Lucas Relation

Being a sister sequence to the Fibonacci numbers, Lucas numbers satisfy the following property.

For $n, m \in \mathbb{Z}$ such that $m|n$,

$$\frac{n}{m} \text{ is odd}$$

Lucas Relation

Being a sister sequence to the Fibonacci numbers, Lucas numbers satisfy the following property.

For $n, m \in \mathbb{Z}$ such that $m|n$,

$$\frac{n}{m} \text{ is odd} \implies L_m | L_n$$

For example

Recall

For $n, m \in \mathbb{Z}$ such that $m|n$,

$\frac{n}{m}$ is odd $\implies L_m|L_n$

For example

Recall

$$\text{For } n, m \in \mathbb{Z} \text{ such that } m|n,$$
$$\frac{n}{m} \text{ is odd } \implies L_m|L_n$$

Consider L_{39}.

For example

Recall

For $n, m \in \mathbb{Z}$ such that $m|n$,
$\frac{n}{m}$ is odd $\implies L_m | L_n$

Consider L_{39}.

L39 (3,13) 79.P3

For example

Recall

For $n, m \in \mathbb{Z}$ such that $m|n$,
$\frac{n}{m}$ is odd $\implies L_m | L_n$

Consider L_{39}.

L39 (3,13) 79.P3

Clearly $39/3 = 13$, $39/13 = 3$.

For example

Recall

For $n, m \in \mathbb{Z}$ such that $m|n$,
$\frac{n}{m}$ is odd $\implies L_m|L_n$

Consider L_{39}.

L39 (3,13) 79.P3

Clearly $39/3 = 13$, $39/13 = 3$.
Thus (3,13) indicates the set of prime factors of L_3, L_{13} that we already know.

Unique prime compression

Abbreviations are often used for large factors.

Unique prime compression

Abbreviations are often used for large factors.
Depending on the status of the factorization, they are listed as **"PXXX"** or **"CXXX"**.

Unique prime compression

Abbreviations are often used for large factors.
Depending on the status of the factorization, they are listed as **"PXXX"** or **"CXXX"**.

F39 (3,13) P6

Unique prime compression

Abbreviations are often used for large factors.
Depending on the status of the factorization, they are listed as **"PXXX"** or **"CXXX"**.

F39 (3,13) P6
F1423 12854269213.90131277469.C276

Finally Constructing The Fibonacci Factors

Finally Constructing The Fibonacci Factors

1. Process odd index Fibonacci prime factors and then the Lucas prime factors in two separate lists.

Finally Constructing The Fibonacci Factors

1. Process odd index Fibonacci prime factors and then the Lucas prime factors in two separate lists.
2. Enumerate through the even indices of the Fibonacci factors list, and append Lucas factors and Fibonacci factors that were previously acquired.

Quick Example!

Construct the prime factors of F_{78}:

Quick Example!

Construct the prime factors of F_{78}:

$$F_{78} = F_{39}L_{39}$$

Quick Example!

Construct the prime factors of F_{78}:

$F_{78} = F_{39}L_{39}$

F39 (3,13) P6
L39 (3,13) 79.P3

Quick Example!

Construct the prime factors of F_{78}:

$F_{78} = F_{39} L_{39}$

F39 (3,13) P6
L39 (3,13) 79.P3

Prime factors of F_{39} are $\mathbf{F_3 = 2, F_{13} = 233}$, and 135721.

Quick Example!

Construct the prime factors of F_{78}:

$F_{78} = F_{39}L_{39}$

F39 (3,13) P6
L39 (3,13) 79.P3

Prime factors of F_{39} are $\mathbf{F_3 = 2, F_{13} = 233}$, and 135721.
Prime factors of L_{39} are $\mathbf{L_3 = 2^2}, 79, \mathbf{L_{13} = 521}$, and 859.

Quick Example!

Construct the prime factors of F_{78}:

$F_{78} = F_{39}L_{39}$

F39 (3,13) P6
L39 (3,13) 79.P3

Prime factors of F_{39} are $\mathbf{F_3 = 2, F_{13} = 233}$, and 135721.
Prime factors of L_{39} are $\mathbf{L_3 = 2^2}, 79, \mathbf{L_{13} = 521}$, and 859.

Append both for F_{78}: 2^3, 79, 233, 521, 859, 135721

Finally Constructing the Fibonacci Pseudoprimes

Review of Algorithm (given L of F_L):

Finally Constructing the Fibonacci Pseudoprimes

Review of Algorithm (given L of F_L):

1. Partition the prime factors of F_L that are $\pm 1 \pmod{L}$ to $\pm 1 \pmod{5}$, and $\pm 2 \pmod{5}$.

Finally Constructing the Fibonacci Pseudoprimes

Review of Algorithm (given L of F_L):

1. Partition the prime factors of F_L that are $\pm 1 \pmod{L}$ to $\pm 1 \pmod{5}$, and $\pm 2 \pmod{5}$.
2. Combine the $\pm 1 \pmod{5}$ prime factors with an odd number of $\pm 2 \pmod{5}$ prime factors to generate candidate pseudoprimes.

Finally Constructing the Fibonacci Pseudoprimes

Review of Algorithm (given L of F_L):

1. Partition the prime factors of F_L that are $\pm 1 \pmod{L}$ to $\pm 1 \pmod{5}$, and $\pm 2 \pmod{5}$.
2. Combine the $\pm 1 \pmod{5}$ prime factors with an odd number of $\pm 2 \pmod{5}$ prime factors to generate candidate pseudoprimes.
3. Test if they are base-2 Fermat pseudoprimes

Example of a Pseudoprime Construction

Given F_{78}: 2^3, 79, 233, 521, 859, 135721

Example of a Pseudoprime Construction

Given F_{78}: 2^3, 79, 233, 521, 859, 135721
Filter prime factors that are $\pm 1 \pmod{78}$:

79, 233, 859, 135721

Example of a Pseudoprime Construction

Given F_{78}: 2^3, 79, 233, 521, 859, 135721
Filter prime factors that are $\pm 1 \pmod{78}$:

79, 233, 859, 135721

Partition to $\pm 1 \pmod{5}$, and $\pm 2 \pmod{5}$.

$\pm 1 \pmod{5}$	$\pm 2 \pmod{5}$
79, 859, 135721	233

Example of a Pseudoprime Construction

Given F_{78}: 2^3, 79, 233, 521, 859, 135721

Filter prime factors that are $\pm 1 \pmod{78}$:

79, 233, 859, 135721

Partition to $\pm 1 \pmod{5}$, and $\pm 2 \pmod{5}$.

$\pm 1 \pmod{5}$	$\pm 2 \pmod{5}$
79, 859, 135721	233

Combine 233 with any number of $\pm 1 \pmod{5}$ prime factors to create 7 total pseudoprimes.

Example of a Pseudoprime Construction

Given F_{78}: 2^3, 79, 233, 521, 859, 135721
Filter prime factors that are $\pm 1 \pmod{78}$:

79, 233, 859, 135721

Partition to $\pm 1 \pmod{5}$, and $\pm 2 \pmod{5}$.

$\pm 1 \pmod{5}$	$\pm 2 \pmod{5}$
79, 859, 135721	233

Combine 233 with any number of $\pm 1 \pmod{5}$ prime factors to create 7 total pseudoprimes.
Example:

$$233 \times 859 \times 79 = 15811613$$

Checking Fermat Pseudoprimality

Recall

Checking Fermat Pseudoprimality

Recall

Theorem

For any $n > 2$, if n is prime, then $2^{(n-1)} \equiv 1 \pmod{n}$

Checking Fermat Pseudoprimality

Recall

Theorem

For any $n > 2$, if n is prime, then $2^{(n-1)} \equiv 1 \pmod{n}$

Given the Fibonacci pseudoprime 15811613, does

Checking Fermat Pseudoprimality

Recall

Theorem

For any $n > 2$, if n is prime, then $2^{(n-1)} \equiv 1 \pmod{n}$

Given the Fibonacci pseudoprime 15811613, does

$$2^{15811613-1} \equiv 1 \pmod{15811613}?$$

Checking Fermat Pseudoprimality

Recall

Theorem

For any $n > 2$, if n is prime, then $2^{(n-1)} \equiv 1 \pmod{n}$

Given the Fibonacci pseudoprime 15811613, does

$$2^{15811613-1} \equiv 1 \pmod{15811613}?$$

Unfortunately, $2^{15811613-1} \equiv 4899758 \pmod{15811613}$.

Results

As it turned out, none of our pseudoprimes were candidates for the \$620 prize.

Results

As it turned out, none of our pseudoprimes were candidates for the $620 prize.

But with these methods, we were able to create more than 10 million new Fibonacci pseudoprimes that were $\pm 2 \pmod 5$.

Results

As it turned out, none of our pseudoprimes were candidates for the $620 prize.

But with these methods, we were able to create more than 10 million new Fibonacci pseudoprimes that were $\pm 2 \pmod 5$.

Thank you for attending our talk!

Conclusion

Useful links: is this useful? Why is this here?

1. https://mersennus.net/fibonacci/
2. https://www.ams.org/journals/mcom/1988-50-181/S0025-5718-1988-0917832-6/S0025-5718-1988-0917832-6.pdf
3. Class notes - Camino, 174 home page
4. Jhttp://gilchrist.ca/jeff/factoring/pseudoprimes.html