On Beating Large Prime Records

Jeff Kinne, Geoff Exoo

Indiana State University

Indiana Academy of Sciences, March 15, 2014

What is a prime number?

What is a prime number?

No divisors/factors except 1 and itself.

What is a prime number?

No divisors/factors except 1 and itself. **5**

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes.

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes. **9**

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes. **9** - no.

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes. **9** - no.
2, 3, 5, 7, 11, 13, 17, 19, ...

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes. **9** - no.
2, 3, 5, 7, 11, 13, 17, 19, ...

Goal:

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes. **9** - no.
2, 3, 5, 7, 11, 13, 17, 19, ...

Goal: find really, really, really large prime numbers

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes. **9** - no.
2, 3, 5, 7, 11, 13, 17, 19, ...

Goal: find really, really, really large prime numbers

Why:

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes. **9** - no.
2, 3, 5, 7, 11, 13, 17, 19, ...

Goal: find really, really, really large prime numbers

Why: cryptography, error correction...

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes. **9** - no.
2, 3, 5, 7, 11, 13, 17, 19, ...

Goal: find really, really, really large prime numbers

Why: cryptography, error correction...
But, really – for the shear thrill of it

What is a prime number?

No divisors/factors except 1 and itself. **5** - yes. **9** - no.
2, 3, 5, 7, 11, 13, 17, 19, ...

Goal: find really, really, really large prime numbers

Why: cryptography, error correction...
But, really – for the shear thrill of it
History: ancient Greeks, ... Renaissance mathematicians, ...

Selected Largest Prime Records

Selected Largest Prime Records

year	digits	discoverer/notes
1588	6	Cataldi
1772	10	Euler
1867	13	Landry

Selected Largest Prime Records

year	digits	discoverer/notes
1588	6	Cataldi
1772	10	Euler
1867	13	Landry
1876	39	Lucas, **1st record w/ Lucas thm**

Selected Largest Prime Records

year	digits	discoverer/notes
1588	6	Cataldi
1772	10	Euler
1867	13	Landry
1876	39	Lucas, **1st record w/ Lucas thm**
1951	44	Ferrier, **mechanical calc**

Selected Largest Prime Records

year	digits	discoverer/notes
1588	6	Cataldi
1772	10	Euler
1867	13	Landry
1876	39	Lucas, **1st record w/ Lucas thm**
1951	44	Ferrier, **mechanical calc**
1951	79	Miller & Wheeler, **EDSAC1 computer**

Selected Largest Prime Records

year	digits	discoverer/notes
1588	6	Cataldi
1772	10	Euler
1867	13	Landry
1876	39	Lucas, **1st record w/ Lucas thm**
1951	44	Ferrier, **mechanical calc**
1951	79	Miller & Wheeler, **EDSAC1 computer**
1953	687	Robinson, **SWAC**
1963	2,917	Gillies, **ILLIAC 2**
1973	6,002	Tuckerman, **IBM360/91**
1983	39,751	Slowinski, **Cray X-MP**
1993	227,832	Slowinski et al., **Cray-2**

Selected Largest Prime Records

year	digits	discoverer/notes
1588	6	Cataldi
1772	10	Euler
1867	13	Landry
1876	39	Lucas, **1st record w/ Lucas thm**
1951	44	Ferrier, **mechanical calc**
1951	79	Miller & Wheeler, **EDSAC1 computer**
1953	687	Robinson, **SWAC**
1963	2,917	Gillies, **ILLIAC 2**
1973	6,002	Tuckerman, **IBM360/91**
1983	39,751	Slowinski, **Cray X-MP**
1993	227,832	Slowinski et al., **Cray-2**
2003	6,320,430	GIMPS, Woltman, **thousands of PC's**

Selected Largest Prime Records

year	digits	discoverer/notes
1588	6	Cataldi
1772	10	Euler
1867	13	Landry
1876	39	Lucas, **1st record w/ Lucas thm**
1951	44	Ferrier, **mechanical calc**
1951	79	Miller & Wheeler, **EDSAC1 computer**
1953	687	Robinson, **SWAC**
1963	2,917	Gillies, **ILLIAC 2**
1973	6,002	Tuckerman, **IBM360/91**
1983	39,751	Slowinski, **Cray X-MP**
1993	227,832	Slowinski et al., **Cray-2**
2003	6,320,430	GIMPS, Woltman, **thousands of PC's**
2013	17,425,170	GIMPS, Woltman, **thousands of PC's**

Is there a **largest** prime number?

Is there a **largest** prime number?
- **Euclid: No, there are infinitely many prime numbers**

Is there a **largest** prime number?
- **Euclid: No, there are infinitely many prime numbers**

If you pick a random integer, what are the chances it is prime?

Is there a **largest** prime number?
- **Euclid: No, there are infinitely many prime numbers**

If you pick a random integer, what are the chances it is prime?

Prime number theorem

Is there a **largest** prime number?
- **Euclid: No, there are infinitely many prime numbers**

If you pick a random integer, what are the chances it is prime?

Prime number theorem

Pick a random integer between 1 and x.

Is there a **largest** prime number?
- **Euclid: No, there are infinitely many prime numbers**

If you pick a random integer, what are the chances it is prime?

Prime number theorem

Pick a random integer between 1 and x.
The chance it is prime is about $\frac{1}{\ln x}$.

Is there a **largest** prime number?
- **Euclid: No, there are infinitely many prime numbers**

If you pick a random integer, what are the chances it is prime?

Prime number theorem

Pick a random integer between 1 and x.
The chance it is prime is about $\frac{1}{\ln x}$.

Note: $\frac{1}{\ln(100)} = 0.21...$

x = 22222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

Is this 100 digit number prime?

x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

Is this 100 digit number prime? – use trial division

x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

Is this 100 digit number prime? – use trial division

- If even, done $\Rightarrow$ not prime

$x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221$

Is this 100 digit number prime? – use trial division

- If even, done $\Rightarrow$ not prime
- If multiple of 3, done $\Rightarrow$ not prime

$x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221$

Is this 100 digit number prime? – use trial division

- If even, done $\Rightarrow$ not prime
- If multiple of 3, done $\Rightarrow$ not prime
- If multiple of 5, done $\Rightarrow$ not prime

x = 222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

Is this 100 digit number prime? – use trial division

- If even, done $\Rightarrow$ not prime
- If multiple of 3, done $\Rightarrow$ not prime
- If multiple of 5, done $\Rightarrow$ not prime
- ...

x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

Is this 100 digit number prime? – use trial division

- If even, done $\Rightarrow$ not prime
- If multiple of 3, done $\Rightarrow$ not prime
- If multiple of 5, done $\Rightarrow$ not prime
- ...
- Check multiples up to ...

x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

Is this 100 digit number prime? – use trial division

- If even, done $\Rightarrow$ not prime
- If multiple of 3, done $\Rightarrow$ not prime
- If multiple of 5, done $\Rightarrow$ not prime
- ...
- Check multiples up to ... **sqrt of the number**

x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

Is this 100 digit number prime? – use trial division

- If even, done ⇒ not prime
- If multiple of 3, done ⇒ not prime
- If multiple of 5, done ⇒ not prime
- ...
- Check multiples up to ... **sqrt of the number**
- If no divisors found, number is prime

x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

Is this 100 digit number prime? – use trial division

- If even, done $\Rightarrow$ not prime
- If multiple of 3, done $\Rightarrow$ not prime
- If multiple of 5, done $\Rightarrow$ not prime
- ...
- Check multiples up to ... **sqrt of the number**
- If no divisors found, number is prime

- **Very fast on most composite numbers**

x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221

Is this 100 digit number prime? – use trial division

- If even, done $\Rightarrow$ not prime
- If multiple of 3, done $\Rightarrow$ not prime
- If multiple of 5, done $\Rightarrow$ not prime
- ...
- Check multiples up to ... **sqrt of the number**
- If no divisors found, number is prime

- **Very fast on most composite numbers**
- **Very slow** to prove a number **prime**

$x = 2222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222222221$

Is this 100 digit number prime? – use trial division

- If even, done $\Rightarrow$ not prime
- If multiple of 3, done $\Rightarrow$ not prime
- If multiple of 5, done $\Rightarrow$ not prime
- ...
- Check multiples up to ... **sqrt of the number**
- If no divisors found, number is prime

- **Very fast on most composite numbers**
- **Very slow** to prove a number **prime**
  (sqrt of 100 digit number $\approx 10^{50}$)

"Big" to a computer?

"Big" to a computer?

- 3Gz CPU means

"Big" to a computer?

- 3Gz CPU means $< 3 \cdot 10^9$ instructions/second

“Big” to a computer?

- 3Gz CPU means $< 3 \cdot 10^9$ instructions/second
- If you have 1000 CPU’s,

"Big" to a computer?

- 3Gz CPU means $< 3 \cdot 10^9$ instructions/second
- If you have 1000 CPU's, $< 3 \cdot 10^{12}$ instructions/second

“Big” to a computer?

- 3Gz CPU means $< 3 \cdot 10^9$ instructions/second
- If you have 1000 CPU's, $< 3 \cdot 10^{12}$ instructions/second

  $< 9.5 \cdot 10^{19}$ **instructions/year**

"Big" to a computer?

- 3Gz CPU means $< 3 \cdot 10^9$ instructions/second
- If you have 1000 CPU's, $< 3 \cdot 10^{12}$ instructions/second
  $< 9.5 \cdot 10^{19}$ **instructions/year**

- Trial divison **too slow for prime proof!**

"Big" to a computer?

- 3Gz CPU means $< 3 \cdot 10^9$ instructions/second
- If you have 1000 CPU's, $< 3 \cdot 10^{12}$ instructions/second
  $< 9.5 \cdot 10^{19}$ **instructions/year**

- Trial divison **too slow for prime proof!**
- We need a faster method...

Other Prime Tests

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1,

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1, 3,

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1, 3, 7,

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1, 3, 7, 15, ...

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1, 3, 7, 15, ...
- **In general**:

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1, 3, 7, 15, ...
- **In general**: $p_1 \cdot p_2 \cdot p_3 \cdot \, \ldots \, \cdot p_j \pm 1$.

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1, 3, 7, 15, ...
- **In general**: $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_j \pm 1$.
  $2^{57885161} - 1$

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1, 3, 7, 15, ...
- **In general**: $p_1 \cdot p_2 \cdot p_3 \cdot \ \dots \ \cdot p_j \pm 1$.
  $2^{57885161} - 1$
  $19249 \cdot 2^{13018586} + 1$

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1, 3, 7, 15, ...
- **In general**: $p_1 \cdot p_2 \cdot p_3 \cdot \, \ldots \, \cdot p_j \pm 1$.
  $2^{57885161} - 1$
  $19249 \cdot 2^{13018586} + 1$
  $475856^{524288} + 1$

Other Prime Tests

Fermat, Miller-Rabin, Solovay-Strassen, AKS, Elliptic curves, ...
All either **randomized** or **not fast enough**

Deterministic primality tests that work for all integers
- **limited to a few hundred digits**

Millions of digits...

- Fast prime proofs that work **only for special integers**
- **Mersenne number**: $2^k - 1$.
  1, 3, 7, 15, ...
- **In general**: $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_j \pm 1$.
  $2^{57885161} - 1$
  $19249 \cdot 2^{13018586} + 1$
  $475856^{524288} + 1$
  ...

Our Results So Far

Our Results So Far

- 208th largest prime overall,

Our Results So Far

- 208th largest prime overall, **712,748 digits** long

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** :

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p + 2$ are both prime.

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p + 2$ are both prime.
  3 and 5 - yes.

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5 - yes. 7 and 9

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5 - yes. 7 and 9 - no.

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5 - yes. 7 and 9 - no.
  14th largest :

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5 - yes. 7 and 9 - no.
  14th largest : $2^{1799} \cdot 3^{137} \cdot 474579581429^{465} \cdot 443749004359^{326} \cdot 644541865141^{488} \cdot 561014826899^{421} \cdot 725590842793^{493} \cdot 623163115793^{476} \cdot 383657519591^{332} - 1$

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5 - yes. 7 and 9 - no.
  14th largest : $2^{1799} \cdot 3^{137} \cdot 474579581429^{465} \cdot 443749004359^{326} \cdot 644541865141^{488} \cdot 561014826899^{421} \cdot 725590842793^{493} \cdot 623163115793^{476} \cdot 383657519591^{332} - 1$
- **Sophie Germain Prime** :

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5 - yes. 7 and 9 - no.
  14th largest : $2^{1799} \cdot 3^{137} \cdot 474579581429^{465} \cdot 443749004359^{326} \cdot 644541865141^{488} \cdot 561014826899^{421} \cdot 725590842793^{493} \cdot 623163115793^{476} \cdot 383657519591^{332} - 1$
- **Sophie Germain Prime** : p and $2p+1$ are both prime.

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5 - yes. 7 and 9 - no.
  14th largest : $2^{1799} \cdot 3^{137} \cdot 474579581429^{465} \cdot 443749004359^{326} \cdot 644541865141^{488} \cdot 561014826899^{421} \cdot 725590842793^{493} \cdot 623163115793^{476} \cdot 383657519591^{332} - 1$
- **Sophie Germain Prime** : p and $2p+1$ are both prime.
  12th largest :

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5 - yes. 7 and 9 - no.
  14th largest : $2^{1799} \cdot 3^{137} \cdot 474579581429^{465} \cdot 443749004359^{326} \cdot 644541865141^{488} \cdot 561014826899^{421} \cdot 725590842793^{493} \cdot 623163115793^{476} \cdot 383657519591^{332} - 1$
- **Sophie Germain Prime** : p and $2p+1$ are both prime.
  12th largest : $2^{1562} \cdot 3^{109} \cdot 828814575031^{420} \cdot 955637315837^{480} \cdot 672198801383^{498} \cdot 162946224587^{484} \cdot 258724139309^{335} \cdot 327170641169^{422} \cdot 880151556857^{437} - 1$

Our Results So Far

- 208th largest prime overall, **712,748 digits** long
- **Twin Prime** : p and $p+2$ are both prime.
  3 and 5 - yes. 7 and 9 - no.
  14th largest : $2^{1799} \cdot 3^{137} \cdot 474579581429^{465} \cdot 443749004359^{326} \cdot 644541865141^{488} \cdot 561014826899^{421} \cdot 725590842793^{493} \cdot 623163115793^{476} \cdot 383657519591^{332} - 1$
- **Sophie Germain Prime** : p and $2p+1$ are both prime.
  12th largest : $2^{1562} \cdot 3^{109} \cdot 828814575031^{420} \cdot 955637315837^{480} \cdot 672198801383^{498} \cdot 162946224587^{484} \cdot 258724139309^{335} \cdot 327170641169^{422} \cdot 880151556857^{437} - 1$

Computing resources

Computing resources

Computing resources

Computing resources

Computing resources

Computing resources

Computing resources

- 75 PCs running continuously
- Another 75 or so on the weekends

Computing resources

- 75 PCs running continuously
- Another 75 or so on the weekends
- **Use more PCs...**

Computing resources

- 75 PCs running continuously
- Another 75 or so on the weekends
- **Use more PCs...**
- **Use graphic cards/GPUs...**

Fermat prime test

Fermat prime test

- Is x prime?

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$.

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$.

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. a^{x-1}

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6$

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$.

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 =$

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$.

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$.

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$. a^{x-1}

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$. $a^{x-1} = 2^5$

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$. $a^{x-1} = 2^5 = 32$.

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$. $a^{x-1} = 2^5 = 32$. $32 \mod 6 =$

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$. $a^{x-1} = 2^5 = 32$. $32 \mod 6 = 2$.

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$. $a^{x-1} = 2^5 = 32$. $32 \mod 6 = 2$.
  6 is not prime.

Fermat prime test

- Is x prime?
- Let a between 2 and $x - 1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$. $a^{x-1} = 2^5 = 32$. $32 \mod 6 = 2$.
  6 is not prime.
- **Running time: pretty fast**,

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$. $a^{x-1} = 2^5 = 32$. $32 \mod 6 = 2$.
  6 is not prime.
- **Running time: pretty fast**, see google/wikipedia

Fermat prime test

- Is x prime?
- Let a between 2 and $x-1$.
- If $a^{x-1} \mod x \neq 1$, x is not prime.

- $x = 7$. $a = 2$. $a^{x-1} = 2^6 = 64$. $64 \mod 7 = 1$.
  7 might be prime.
- $x = 6$. $a = 2$. $a^{x-1} = 2^5 = 32$. $32 \mod 6 = 2$.
  6 is not prime.
- **Running time: pretty fast**, see google/wikipedia

Finding a very large prime

Finding a very large prime

- **Choose a number** N (such that $N \pm 1$ is factored)

Finding a very large prime

- **Choose a number N** (such that $N \pm 1$ is factored)
  - E.g., set $N = k \cdot 2^{3{,}330{,}000} + 1$, k small

Finding a very large prime

- **Choose a number N** (such that $N \pm 1$ is factored)
  - E.g., set $N = k \cdot 2^{3,330,000} + 1$, k small
- **Test N for small factors**

Finding a very large prime

- **Choose a number N** (such that $N \pm 1$ is factored)
  - E.g., set $N = k \cdot 2^{3,330,000} + 1$, k small
- **Test N for small factors** **[pick new N if any found]**

Finding a very large prime

- **Choose a number N** (such that $N \pm 1$ is factored)
    - E.g., set $N = k \cdot 2^{3,330,000} + 1$, k small
- **Test N for small factors** **[pick new N if any found]**
- **Run Fermat prime test on N**

Finding a very large prime

- **Choose a number N** (such that $N \pm 1$ is factored)
  - E.g., set $N = k \cdot 2^{3,330,000} + 1$, k small
- **Test N for small factors** **[pick new N if any found]**
- **Run Fermat prime test on N** **[pick new N if fails]**

Finding a very large prime

- **Choose a number N** (such that $N \pm 1$ is factored)
  - E.g., set $N = k \cdot 2^{3,330,000} + 1$, k small
- **Test N for small factors** **[pick new N if any found]**
- **Run Fermat prime test on N** **[pick new N if fails]**
- Run Lucas test to **prove** N prime

Finding a very large prime

- **Choose a number N** (such that $N \pm 1$ is factored)
  - E.g., set $N = k \cdot 2^{3,330,000} + 1$, k small
- **Test N for small factors** **[pick new N if any found]**
- **Run Fermat prime test on N** **[pick new N if fails]**
- Run Lucas test to **prove** N prime **[pick new N if fails]**

Finding a very large prime

- **Choose a number N** (such that $N \pm 1$ is factored)
  - E.g., set $N = k \cdot 2^{3,330,000} + 1$, k small
- **Test N for small factors** **[pick new N if any found]**
- **Run Fermat prime test on N** **[pick new N if fails]**
- Run Lucas test to **prove** N prime **[pick new N if fails]**
- Repeat until all tests passed

Thank You, The End

Thank You, The End

Links

- kinnejeff.com/talks.html – these slides, and a more detailed talk about this research
- Prime Pages, by Chris Caldwell – THE source of information on prime records, and the official prime records database
- Software/libraries we use: GMP, OpenPFGW

Ackowledgments

- **Funding** : Indiana Academy of Sciences; Indiana State University, Office of the President
- **Computing** : Indiana State University – Office of Information Technology; Departments of Mathematics and Computer Science, Chemistry and Physics, Languages Literatures and Linguistics, Electronics and Computer Engineering Technology, Built Environment