Finding Very Large Prime Numbers

Jeff Kinne

Indiana State University

Midwest Theory Day, November 23, 2013

Notes

- My "normal" research – computational complexity

Notes

- My "normal" research – computational complexity
- Today – computational number theory

Notes

- My "normal" research – computational complexity
- Today – computational number theory
- Research in progress with Geoff Exoo (Indiana State)

Notes

- My "normal" research – computational complexity
- Today – computational number theory
- Research in progress with Geoff Exoo (Indiana State)
- Links to more information at the end

Notes

- My "normal" research – computational complexity
- Today – computational number theory
- Research in progress with Geoff Exoo (Indiana State)
- Links to more information at the end

Prime Records

Selected Largest Prime Records

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
2013	17,425,170	GIMPS, Woltman

Current Largest Known Primes

Current Largest Known Primes

- Top ten are **Mersenne primes,** $2^k - 1$

Current Largest Known Primes

- Top ten are **Mersenne primes,** $2^k - 1$
- Great Internet Mersenne Prime Search (GIMPS)

Current Largest Known Primes

- Top ten are **Mersenne primes,** $2^k - 1$
- Great Internet Mersenne Prime Search (GIMPS)
  - $\sim$ 5000 users, $\sim$ 25000 computers

Current Largest Known Primes

- Top ten are **Mersenne primes,** $2^k - 1$
- Great Internet Mersenne Prime Search (GIMPS)
  - $\sim$ 5000 users, $\sim$ 25000 computers
  - All records since 1996

Current Largest Known Primes

- Top ten are **Mersenne primes,** $2^k - 1$
- Great Internet Mersenne Prime Search (GIMPS)
  - $\sim$ 5000 users, $\sim$ 25000 computers
  - All records since 1996
- **All of the current largest known primes $\Leftrightarrow$ $p \pm 1$ is factored**

Current Largest Known Primes

- Top ten are **Mersenne primes,** $2^k - 1$
- Great Internet Mersenne Prime Search (GIMPS)
  - $\sim$ 5000 users, $\sim$ 25000 computers
  - All records since 1996
- **All of the current largest known primes** $\Leftrightarrow p \pm 1$ **is factored**

Special Types

- Twin primes: p and $p + 2$ both prime

Current Largest Known Primes

- Top ten are **Mersenne primes,** $2^k - 1$
- Great Internet Mersenne Prime Search (GIMPS)
  - $\sim$ 5000 users, $\sim$ 25000 computers
  - All records since 1996
- **All of the current largest known primes** $\Leftrightarrow p \pm 1$ **is factored**

Special Types

- Twin primes: p and $p + 2$ both prime
- Sophie-Germain: p and $2p + 1$

Current Largest Known Primes

- Top ten are **Mersenne primes,** $2^k - 1$
- Great Internet Mersenne Prime Search (GIMPS)
  - $\sim$ 5000 users, $\sim$ 25000 computers
  - All records since 1996
- **All of the current largest known primes** $\Leftrightarrow$ $p \pm 1$ **is factored**

Special Types

- Twin primes: p and $p + 2$ both prime
- Sophie-Germain: p and $2p + 1$
- Factorial: $m! \pm 1$

Current Largest Known Primes

- Top ten are **Mersenne primes,** $2^k - 1$
- Great Internet Mersenne Prime Search (GIMPS)
  - $\sim$ 5000 users, $\sim$ 25000 computers
  - All records since 1996
- **All of the current largest known primes** $\Leftrightarrow$ $p \pm 1$ **is factored**

Special Types

- Twin primes: p and $p + 2$ both prime
- Sophie-Germain: p and $2p + 1$
- Factorial: $m! \pm 1$
- ...

Our Results So Far

Our Results So Far

- Primes with 712K, 470K, 349K digits

Our Results So Far

- Primes with 712K, 470K, 349K digits (190th, 865th, 3356th largest known)

Our Results So Far

- Primes with 712K, 470K, 349K digits (190th, 865th, 3356th largest known)
- Sophie Germain prime with 31K digits (16th largest known)

Our Results So Far

- Primes with 712K, 470K, 349K digits
  (190th, 865th, 3356th largest known)
- Sophie Germain prime with 31K digits (16th largest known)
- Computing resources: 60 machines running continuously, another 50 on the weekends

Verifying Large Primes

Randomized Prime Tests

	Miller-Rabin	**Fermat**[1]
run time[2]	b^2	"
$b = 40$	2^{10}	
$b = 1000$	2^{20}	
$b = 1\text{mil}$	2^{40}	

[1] some false positives
[2] ignoring poly-log factors

Fermat Test

Pick $1 < a < N$ at random. N prime $\Rightarrow a^{N-1} \equiv 1 \mod N$.

Randomized Prime Tests

	Miller-Rabin	Fermat[1]
run time[2]	b^2	"
$b = 40$	2^{10}	
$b = 1000$	2^{20}	
$b = 1\text{mil}$	2^{40}	

[1] some false positives
[2] ignoring poly-log factors

Deterministic Prime Tests

	trial div	MR w GRH	AKS	GNFS
run time[2]	$2^{b/2}$	b^4	b^6	$2^{O(b^{\frac{1}{3}} \log^{\frac{2}{3}}(b))}$
$b = 40$	2^{20}	2^{20}	2^{30}	$2^{O(8)}$
$b = 1000$	2^{500}	2^{40}	2^{60}	$2^{O(50)}$
$b = 1000000$	$2^{500,000}$	2^{80}	2^{120}	$2^{O(575)}$

Deterministic Prime Tests

Deterministic Prime Tests

For certain classes of integers, $\widetilde{O}(b^2)$ time

Deterministic Prime Tests

For certain classes of integers, $\widetilde{O}(b^2)$ time

Theorem (Lucas)

$N > 1$ is prime $\Leftrightarrow$

Deterministic Prime Tests

For certain classes of integers, $\widetilde{O}(b^2)$ time

Theorem (Lucas)

$N > 1$ is prime $\Leftrightarrow \exists\ a$, $1 < a < N$ s.t.

- $a^{N-1} \equiv 1 \mod N$, *and*

Deterministic Prime Tests

For certain classes of integers, $\widetilde{O}(b^2)$ time

Theorem (Lucas)

$N > 1$ is prime $\Leftrightarrow \exists\ a$, $1 < a < N$ s.t.

- $a^{N-1} \equiv 1 \mod N$, *and*
- $\forall$ **prime** q **s.t.** $q \big| (N-1)$,

Deterministic Prime Tests

For certain classes of integers, $\widetilde{O}(b^2)$ time

Theorem (Lucas)

$N > 1$ is prime $\Leftrightarrow \exists\ a$, $1 < a < N$ s.t.

- $a^{N-1} \equiv 1 \mod N$, *and*
- $\forall$ **prime** q **s.t.** $q|(N-1)$, $a^{(N-1)/q} \not\equiv 1 \mod N$

Deterministic Prime Tests

For certain classes of integers, $\widetilde{O}(b^2)$ time

Theorem (Lucas)

$N > 1$ is prime $\Leftrightarrow \exists$ a, $1 < a < N$ s.t.

- $a^{N-1} \equiv 1 \mod N$, *and*
- **$\forall$ prime q s.t. $q | (N-1)$**, $a^{(N-1)/q} \not\equiv 1 \mod N$

Example:

- $N = 29$

Deterministic Prime Tests

For certain classes of integers, $\widetilde{O}(b^2)$ time

Theorem (Lucas)

$N > 1$ is prime $\Leftrightarrow \exists\ a,\ 1 < a < N$ s.t.

- $a^{N-1} \equiv 1 \mod N$, *and*
- $\forall$ **prime q s.t. $q|(N-1)$**, $a^{(N-1)/q} \not\equiv 1 \mod N$

Example:

- $N = 29$
- $2^{28} \equiv 1 \mod 29$

Deterministic Prime Tests

For certain classes of integers, $\widetilde{O}(b^2)$ time

Theorem (Lucas)

$N > 1$ is prime $\Leftrightarrow \exists\ a$, $1 < a < N$ s.t.

- $a^{N-1} \equiv 1 \mod N$, *and*
- $\forall$ **prime q s.t.** $q | (N-1)$, $a^{(N-1)/q} \not\equiv 1 \mod N$

Example:

- $N = 29$
- $2^{28} \equiv 1 \mod 29$
- $2^4 \equiv 16 \mod 29$,

Deterministic Prime Tests

For certain classes of integers, $\widetilde{O}(b^2)$ time

Theorem (Lucas)

$N > 1$ is prime $\Leftrightarrow \exists\ a,\ 1 < a < N$ s.t.

- $a^{N-1} \equiv 1 \mod N$, *and*
- $\forall$ **prime** q **s.t.** $q|(N-1)$, $a^{(N-1)/q} \not\equiv 1 \mod N$

Example:

- $N = 29$
- $2^{28} \equiv 1 \mod 29$
- $2^4 \equiv 16 \mod 29$, $2^{14} \equiv 28 \mod 29$

Strategy for the Search

Basic Framework

Basic Framework

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

Basic Framework

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

Basic Framework

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

Basic Framework

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

Basic Framework

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

Prime Number Theorem

Basic Framework

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

Prime Number Theorem

Number of primes at most $x = \Pi(x) \sim \frac{x}{\ln x}$

Basic Framework

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

Prime Number Theorem

Number of primes at most $x = \Pi(x) \sim \frac{x}{\ln x}$

- $\Pr[d \text{ digit } N \text{ is prime }] \approx \frac{1}{d \ln 10}$

Basic Framework

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

Prime Number Theorem

Number of primes at most $x = \Pi(x) \sim \frac{x}{\ln x}$

- $\Pr[d \text{ digit } N \text{ is prime }] \approx \frac{1}{d \ln 10}$ **(heuristic, GRH)**

Basic Framework

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

Prime Number Theorem

Number of primes at most $x = \Pi(x) \sim \frac{x}{\ln x}$

- $\Pr[d \text{ digit } N \text{ is prime }] \approx \frac{1}{d \ln 10}$ **(heuristic, GRH)**
- Test $d(\ln 10)(\ln 2)$ numbers $\Leftrightarrow$ 50% chance to find 1 prime

Basic Framework

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

Prime Number Theorem

Number of primes at most $x = \Pi(x) \sim \frac{x}{\ln x}$

- $\Pr[d$ digit N is prime $] \approx \frac{1}{d \ln 10}$ **(heuristic, GRH)**
- Test $d(\ln 10)(\ln 2)$ numbers $\Leftrightarrow$ 50% chance to find 1 prime
- $d = 13 \Leftrightarrow$ test about 21 numbers

Basic Framework

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

Prime Number Theorem

Number of primes at most $x = \Pi(x) \sim \frac{x}{\ln x}$

- $\Pr[d \text{ digit } N \text{ is prime }] \approx \frac{1}{d \ln 10}$ **(heuristic, GRH)**
- Test $d(\ln 10)(\ln 2)$ numbers $\Leftrightarrow$ 50% chance to find 1 prime
- $d = 13 \Leftrightarrow$ test about 21 numbers
- $d = 1,000,000 \Leftrightarrow$ test about 1.6 million

For about $d(\ln 10)(\ln 2)$ many N...

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow \widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx \widetilde{O}(d^2)$ time

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Mertens' formula)

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Mertens' formula)

$\prod_{p \leq T} \left(1 - \frac{1}{p}\right)$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Mertens' formula)

$$\prod_{p\leq T}\left(1-\frac{1}{p}\right)\sim\frac{e^{-\gamma}}{\ln(T)}$$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Mertens' formula)

$$\prod_{p \leq T} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln(T)}$$

- T – threshold for trial division

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Mertens' formula)

$$\prod_{p\leq T}\left(1-\frac{1}{p}\right)\sim\frac{e^{-\gamma}}{\ln(T)}$$

- T – threshold for trial division
- $\gamma = 0.57721$, $e^{-\gamma} = 0.56145\ldots$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow \widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Mertens' formula)

$$\prod_{p \le T}\left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln(T)}$$

- T – threshold for trial division
- $\gamma = 0.57721$, $e^{-\gamma} = 0.56145\ldots$
- $T = 10^6 \Rightarrow$ Pr **pass trial division** $\approx \frac{1}{25}$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Mertens' formula)

$$\prod_{p \le T} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln(T)}$$

- T – threshold for trial division
- $\gamma = 0.57721$, $e^{-\gamma} = 0.56145\ldots$
- $T = 10^6 \Rightarrow$ Pr **pass trial division** $\approx \frac{1}{25}$ **(heuristic, GRH)**

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Mertens' formula)

$$\prod_{p\leq T}\left(1-\frac{1}{p}\right)\sim\frac{e^{-\gamma}}{\ln(T)}$$

- T – threshold for trial division
- $\gamma = 0.57721$, $e^{-\gamma} = 0.56145\ldots$
- $T = 10^6 \Rightarrow$ Pr **pass trial division** $\approx \frac{1}{25}$ **(heuristic, GRH)**
- $T = 10^{12} \Rightarrow$ Pr **pass trial division** $\approx \frac{1}{50}$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow \widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Pomerance)

Let $\mathcal{P}_a(x) = \#$ composites $N \leq x$ s.t. $a^{N-1} \equiv 1 \mod N$.

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Pomerance)

Let $\mathcal{P}_a(x) = \#$ composites $N \leq x$ s.t. $a^{N-1} \equiv 1 \mod N$.

$$\mathcal{P}_a(x)/x \leq 1/e^{\ln(x)\ln\ln\ln(x)/(2\ln\ln(x))}$$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Pomerance)

Let $\mathcal{P}_a(x) = \#$ composites $N \leq x$ s.t. $a^{N-1} \equiv 1 \mod N$.

$$\mathcal{P}_a(x)/x \leq 1/e^{\ln(x)\ln\ln\ln(x)/(2\ln\ln(x))}$$

- ***N* passes Fermat test** $\Leftrightarrow$ Pr ***N* composite**

$$\leq \frac{d\ln(10)}{e^{d\ln(10)\ln\ln(d\ln(10))/(2\ln(d\ln(10)))}}$$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Pomerance)

Let $\mathcal{P}_a(x) = \#$ composites $N \leq x$ s.t. $a^{N-1} \equiv 1 \mod N$.

$$\mathcal{P}_a(x)/x \leq 1/e^{\ln(x)\ln\ln\ln(x)/(2\ln\ln(x))}$$

- ***N* passes Fermat test** $\Leftrightarrow$ $\Pr$ ***N* composite**

$$\leq \frac{d\ln(10)}{e^{d\ln(10)\ln\ln(d\ln(10))/(2\ln(d\ln(10)))}}$$

- $d = 1000 \Rightarrow \frac{1}{10^{129}}$,

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Theorem (Pomerance)

Let $\mathcal{P}_a(x) = \#$ composites $N \leq x$ s.t. $a^{N-1} \equiv 1 \mod N$.

$$\mathcal{P}_a(x)/x \leq 1/e^{\ln(x)\ln\ln\ln(x)/(2\ln\ln(x))}$$

- ***N* passes Fermat test** $\Leftrightarrow$ $\Pr$ ***N* composite**

$$\leq \frac{d\ln(10)}{e^{d\ln(10)\ln\ln(d\ln(10))/(2\ln(d\ln(10)))}}$$

- $d = 1000 \Rightarrow \frac{1}{10^{129}}$, $d = 1,000,000 \Rightarrow \frac{1}{10^{90,000}}$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Time to find d digit prime **(heuristic)**

$$\widetilde{O}(d^3)$$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx$ $\widetilde{O}(d^2)$ time **(heuristic, GRH)**

Time to find d digit prime (heuristic)

$$\widetilde{O}(d^3)$$

- $d = 17M$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow \widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow\approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

Time to find d digit prime **(heuristic)**

$$\widetilde{O}(d^3)$$

- $d = 17M \Rightarrow \widetilde{O}(4.9 \cdot 10^{21})$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow \widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

Time to find d digit prime **(heuristic)**

$$\widetilde{O}(d^3)$$

- $d = 17M \Rightarrow \widetilde{O}(4.9 \cdot 10^{21}) \Rightarrow \approx$ **150,000 CPU years** (with 10^9 operations/second/CPU)

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow \widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

Time to find d digit prime (heuristic)

$$\widetilde{O}(d^3)$$

- $d = 17M \Rightarrow \widetilde{O}(4.9 \cdot 10^{21}) \Rightarrow \approx$ **150,000 CPU years** (with 10^9 operations/second/CPU)
  - Actually took 4 years, $\approx 25,000$ computers

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow \widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

Time to find d digit prime (heuristic)

$$\widetilde{O}(d^3)$$

- $d = 17M \Rightarrow \widetilde{O}(4.9 \cdot 10^{21}) \Rightarrow \approx$ **150,000 CPU years** (with 10^9 operations/second/CPU)
  - Actually took 4 years, $\approx 25,000$ computers
- $d = 712K$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

Time to find d digit prime (heuristic)

$$\widetilde{O}(d^3)$$

- $d = 17M \Rightarrow \widetilde{O}(4.9 \cdot 10^{21}) \Rightarrow \approx$ **150,000 CPU years** (with 10^9 operations/second/CPU)
  - Actually took 4 years, $\approx 25,000$ computers
- $d = 712K \Rightarrow \widetilde{O}(3.6 \cdot 10^{17})$

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow \widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

Time to find d digit prime (heuristic)

$$\widetilde{O}(d^3)$$

- $d = 17M \Rightarrow \widetilde{O}(4.9 \cdot 10^{21}) \Rightarrow \approx$ **150,000 CPU years** (with 10^9 operations/second/CPU)
  - Actually took 4 years, $\approx 25,000$ computers
- $d = 712K \Rightarrow \widetilde{O}(3.6 \cdot 10^{17}) \Rightarrow \approx$ **11 CPU years**

For about $d(\ln 10)(\ln 2)$ many N...

- Test for small factors $\Leftrightarrow$ $O(d)$ time (or less) each test
  - $\sim \frac{1}{50th}$ pass trial division **(heuristic, GRH)**
- Fermat test $\Leftrightarrow$ $\widetilde{O}(d^2)$ time
- Lucas test $\Leftrightarrow \approx \widetilde{O}(d^2)$ time **(heuristic, GRH)**

Time to find d digit prime **(heuristic)**

$$\widetilde{O}(d^3)$$

- $d = 17M \Rightarrow \widetilde{O}(4.9 \cdot 10^{21}) \Rightarrow \approx$ **150,000 CPU years** (with 10^9 operations/second/CPU)
  - Actually took 4 years, $\approx 25,000$ computers
- $d = 712K \Rightarrow \widetilde{O}(3.6 \cdot 10^{17}) \Rightarrow \approx$ **11 CPU years**
  - Actually took 1 month, ≈ 150 cores

Practical considerations

Practical considerations

- Heuristic is “good enough”

Practical considerations

- Heuristic is "good enough"
- Constant factors matter

Practical considerations

- Heuristic is "good enough"
- Constant factors matter
- Which math library matters: GMP, gwNum

Practical considerations

- Heuristic is "good enough"
- Constant factors matter
- Which math library matters: GMP, gwNum
- How many processes/computer: **for 4 core CPU, 2 processes**
  (using double-wide floating point FFT for multiplication)

Practical considerations

- Heuristic is "good enough"
- Constant factors matter
- Which math library matters: GMP, gwNum
- How many processes/computer: **for 4 core CPU, 2 processes**
  (using double-wide floating point FFT for multiplication)
- **Choose goal based on available CPUs**

Thank You, The End

Thank You, The End

Links

- Prime Pages, by Chris Caldwell – THE source of information on prime records, and the official prime records database
- On the Distribution of Pseudoprimes by Pomerance – scarcity of Fermat pseudoprimes
- An Amazing Prime Heuristic – same heuristic arguments we presented today
- Software/libraries we use: GMP, OpenPFGW