Goals

• 5000\textsuperscript{th} largest known prime
  • Must be about 300,000 digits

• 20\textsuperscript{th} largest Sophie Germain prime
  • Must be about 30,000 digits
Prime Number

- Can only be divided by itself and one.
- Examples: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 …
• After various improvements to code efficiency...
• We are about ½ way through the search for 30,000 digit Sophie Germain prime after 2 weeks of computer time
• Searching for 300,000 digit prime will take another 2 weeks of computer time
Computers Used

About 220 cores:
- 20 dual-core 3.2Gz i5 machines,
- 30 quad-core 3.1Gz i5 machines,
- 15 quad-core 2.8Gz i5 machines.
Prime Number Test: Trial Division

• Division of $n$ by a sequence of number greater than 1 and less than $n$.
• Helps eliminate unwanted numbers

Example, 47
47 can only be divided by $\{1, 47\}$

Example, 49
49 can be divided by $\{1, 7, 49\}$
Prime Number Test: Fermat Test

- \( a^{n-1} \mod n = 1 \)
- If the number passes the test then it might be a prime, but if it does not, then it is not a prime.
- Example:

  - \( n = 4 \)
    - \( a = 3 \)
    - \( 3^3 \mod 4 = 27 \mod 4 = 3 \)
    - Failed
  - \( n = 5 \)
    - \( a = 3 \)
    - \( 3^4 \mod 5 = 81 \mod 5 = 1 \)
    - Passed
Prime Number Test: Lucas Test

• Find prime factors of n.
• Run a sequence of test (almost similar to the Fermat equation) on them.
• Example:

  \[ n = 47 \]
  \[ n - 1 = 46 \]
  Factors: \{2, 23\}
How rare are prime numbers?

\[ \pi(n) \sim \frac{n}{\ln(n)} \]

- 1 digit numbers: 4 are prime
- 2 digit numbers: 21 are prime
- 30,000 digit numbers: about 1/70,000 are prime
- 300,000 digit numbers: about 1/700,000 are prime
Sohpie Germain Primes

- \( n \) and \( 2n + 1 \) are both prime
- 30,000 digit numbers
  - \( \sim \left( \frac{1}{70,000} \right)^2 \) are Sophie Germain primes
How long does it take to get a prime and a SG

- Prime Number 300,000 digits
  - $9.8 \times 10^{149986}$ years (Trial Division)
  - 2695 years (Fermat Test)
- Sophie Germaine 30,000 digits
  - 6976 years (Trial Division)
  - 98 days (Fermat Test)
Is n prime?

Loop()
{
  1- Trial division try n/2
      n/3
      n/5..... n/9973
  2- Fermat's test: \( a^{n-1} \mod n = 1 \)
  3- Lucas theorem
}