Finding Really Big Primes

Clayton Smith

November 6, 2003

Strategy

- Basic strategy: Choose n. Check whether n is prime. Repeat.

- By Prime Number Theorem, probability that n is prime is $\sim 1/\log n$.

- Expect $\sim \log n$ tests before finding a prime.

Strategy

- Problem: Proving that n is prime.

  Algorithms for generic n can only handle $\sim 5,000$ digits.

- It helps if n is near a number with many small factors.

- $n = k \cdot a^m \pm 1$ works well.

Mersenne Numbers

- $M_n = 2^n - 1$
- If $2^n - 1$ is prime, then n is prime.
- $2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)(\ldots)$

Mersenne Numbers

- Small examples:

$$
\begin{aligned}
2^2 - 1 &= 3 \\
2^3 - 1 &= 7 \\
2^5 - 1 &= 31 \\
2^7 - 1 &= 127 \\
2^{11} - 1 &= 2047 = 23 \cdot 89 \\
&\vdots
\end{aligned}
$$

- Only 39 Mersenne primes are known.

Factors of Mersenne Numbers

Theorem: Let p and q be odd primes, and suppose q divides $M_p = 2^p - 1$. Then

$$q \equiv 1 \pmod{p}$$

and

$$q \equiv \pm 1 \pmod{8}.$$

These can easily be combined using the Chinese Remainder Theorem.

Example: $2^{31} - 1 = 2147483647$

If q divides $2^{31} - 1$ then

$$q \equiv 1 \pmod{31}$$

and

$$q \equiv \pm 1 \pmod{8}.$$

Applying CRT, this gives $q \equiv 1$ or $63 \pmod{248}$. There are 374 such q less than $\sqrt{2^{31} - 1}$, and only 84 of these are prime.

In 1772, Euler used this method to show that $2^{31} - 1$ is prime.

Primality Test for Mersenne Numbers

Consider the sequence $(v_k)_{k=0,1,\ldots}$ defined by

$$v_0 = 4$$
$$v_{k+1} = v_k^2 - 2.$$

Let p be an odd prime. Then $M_p = 2^p - 1$ is prime if and only if $v_{p-2} \equiv 0 \pmod{M_p}$.

Lucas first used this test in 1876 to show that $2^{127} - 1$ is prime. (This number has 39 decimal digits.)

Example: $2^7 - 1 = 127$

Working mod $2^7 - 1$:

$$
\begin{aligned}
v_0 &= 4 \\
v_1 &= 4^2 - 2 = 14 \\
v_2 &= 14^2 - 2 = 194 = 67 \\
v_3 &= 67^2 - 2 = 4487 = 42 \\
v_4 &= 42^2 - 2 = 1760 = 111 \\
v_5 &= 111^2 - 2 = 12319 = 0
\end{aligned}
$$

Thus $2^7 - 1$ is prime.

Efficiency

- Squaring is hardest part; naive algorithm $O(p^2)$, can be reduced to $O(p \log p \log \log p)$ using FFT.

- Modular reduction is easy in binary; can be eliminated entirely.

- $p - 2$ squarings, so total runtime is

$$O(p^2 \log p \log \log p)$$

Efficiency

- Faster than even a single probabilistic primality test.

- About 10 days to test a 6-million digit number on a 2.4 GHz Pentium.

GIMPS

- Great Internet Mersenne Prime Search
- Distributed computing project
- Founded in 1996 by George Woltman
- http://www.mersenne.org/

GIMPS

- 40,000 computers, 8.5 teraflops
- 5 new Mersenne primes found
- 4 largest known primes

Testing Procedure

- Trial factoring
- $p - 1$ factoring
- Lucas-Lehmer test
- Double check

EFF Prizes

- $50,000 for first million-digit prime; claimed in 1999 by GIMPS member Nayan Hajratwala
- $100,000 for first ten-million-digit prime
- $150,000 for first hundred-million digit prime
- $250,000 for first billion-digit prime

Largest Known Prime

- $2^{13,466,917} - 1$
- 4,053,946 digits
- Found on November 14, 2001 by Michael Cameron of Owen Sound, Ontario

Open Problems

- Are there infinitely many Mersenne primes?

- Are there infinitely many Mersenne composites?