LARGE PRIME NUMBERS

1. Fermat Pseudoprimes

Fermat's Little Theorem states that for any positive integer n,

$$\textit{if } n \textit{ is prime then } b^n \,\%\, n = b \textit{ for } b = 1, \dots, n-1.$$

In the other direction, all we can say is that

$$\textit{if } b^n \,\%\, n = b \textit{ for } b = 1, \dots, n-1 \textit{ then } n \textit{ might be prime.}$$

If $b^n \,\%\, n = b$ where $b \in \{1, \dots, n-1\}$ then n is called a **Fermat pseudoprime base** b.

There are 669 primes under 5000, but only five values of n (561, 1105, 1729, 2465, and 2821) that are Fermat pseudoprimes base b for $b = 2, 3, 5$ without being prime. This is a false positive rate of less than 1%. The false positive rate under 500,000 just for $b = 2, 3$ is 0.118%.

On the other hand, the bad news is that checking more bases b doesn't reduce the false positive rate much further. There are infinitely many **Carmichael numbers**, numbers n that are Fermat pseudoprimes base b for all $b \in \{1, \dots, n-1\}$ but are not prime.

In sum, Fermat pseudoprimes are reasonable candidates to be prime.

2. Strong Pseudoprimes

The **Miller–Rabin test** on a positive integer n and a positive test base b in $\{1, \ldots, n-1\}$ proceeds as follows.

(1) Factor $n - 1 = 2^s \cdot m$ where m is odd.
(2) Replace b by $b^m \,\%\, n$.
(3) If $b = 1$ or $b = n - 1$, return the result that the test suggests that n is prime. Otherwise continue.
(4) Set $r = 0$.
(5) If $r < s$, proceed to step (6). Otherwise return the result that n is composite.
(6) Replace b by $b^2 \,\%\, n$.
(7) If $b = n - 1$, return the result that the test suggests that n is prime. Otherwise continue.
(8) If $b = 1$, return the result that n is composite. Otherwise continue.
(9) Increment r and return to step (5).

The idea behind the test is that if n has distinct prime factors then the equation $x^2 \,\%\, n = 1$ has at least four solutions. So if we find some b such that $b \,\%\, n$ is not 1 or $n - 1$, and yet $b^2 \,\%\, n = 1$, then n is composite.

A positive integer n that passes the Miller-Rabin test for some b is a **strong pseudoprime base** b.

For any n, at least $3/4$ of the b-values in $\{1, \ldots, n-1\}$ have the property that if n is a strong pseudoprime base b then n is really prime. But according to the theory, up to $1/4$ of the b-values have the property that n could be a strong pseudoprime base b but not be prime. In practice, the percentage of such b's is much lower. For n up to 500,000, if n is a strong pseudoprime base 2 and base 3 then n is prime.

3. Generating Candidate Large Primes

Given n, a simple approach to finding a candidate prime above $2n$ is as follows. Take the first of $N = 2n + 1$, $N = 2n + 3$, $N = 2n + 5$, ... to pass the following test.

(1) Try trial division for a few small primes. If N passes, continue.
(2) Check whether N is a Fermat pseudoprime base 2. If N passes, continue.
(3) Check whether N is a strong pseudoprime base b as b runs through the first 20 primes.

Any N that passes the test is extremely likely to be prime. And such an N should appear quickly. Indeed, using only the first *three* primes in step (3) of the previous test finds the following correct candidate primes:

The first candidate prime after	10^{50}	is	$10^{50} + 151$.
The first candidate prime after	10^{100}	is	$10^{100} + 267$.
The first candidate prime after	10^{200}	is	$10^{200} + 357$.
The first candidate prime after	10^{500}	is	$10^{500} + 331$.
The first candidate prime after	10^{1000}	is	$10^{1000} + 453$.

4. Certifiable Large Primes

The **Lucas–Pocklington–Lehmer Criterion** is as follows. *Suppose that* $N = p \cdot U + 1$ *where* p *is prime and* $p > U$. *Suppose also that there is a base* b *such that* $b^{N-1} \,\%\, N = 1$ *but* $\gcd(b^U - 1, N) = 1$. *Then* N *is prime.*

The proof is just Fermat's Little Theorem and some other basic number theory.

As an example of using the result, start with

$$p = 1000003.$$

This is small enough that its primality is easily verified by trial division. A candidate prime above $1000 \cdot p$ of the form $p \cdot U + 1$ is

$$N = p \cdot 1032 + 1 = 1032003097.$$

And $2^{N-1} \,\%\, N = 1$ and $\gcd(2^{1032} - 1, N) = 1$, so the LPL Criterion is satisfied, and N is prime. Rename it p.

A candidate prime above $10^9 \cdot p$ of the form $p \cdot U + 1$ is

$$N = p \cdot (10^9 + 146) + 1 = 1032003247672452163.$$

Again $b = 2$ works in the LPL Criterion, so N is prime. Again rename it p.

A candidate prime above $10^{17} \cdot p$ of the form $p \cdot U + 1$ is

$$N = p \cdot (10^{17} + 24) + 1 = 103200324767245241068077944138851913.$$

Again $b = 2$ works in the LPL Criterion, so N is prime. Again rename it p.

A candidate prime above $10^{34} \cdot p$ of the form $p \cdot U + 1$ is

$$\begin{aligned} N = p \cdot (10^{34} + 224) + 1 = &1032003247672452410680779441388542\,2 \\ &4687274786293399924945948710282851\,3. \end{aligned}$$

Again $b = 2$ works in the LPL Criterion, so N is prime. Again rename it p.

A candidate prime above $10^{60} \cdot p$ of the form $p \cdot U + 1$ is

$$\begin{aligned} N = p \cdot (10^{60} + 1362) + 1 = &10320032476724524106807794413885422 \\ &468727478629339992494608926912518428 \\ &801833472215991711945402406825893161 \\ &06977763821434052434707. \end{aligned}$$

Again $b = 2$ works in the LPL Criterion, so N is prime. Again rename it p.

A candidate prime above $10^{120} \cdot p$ of the form $p \cdot U + 1$ is

$$
\begin{aligned}
N = p \cdot (10^{120} + 796) + 1 = &10320032476724524106807794413885422\\
&46872747862933999249460892691251842 8\\
&80183347221599171194540240682589316 1\\
&06977763822255527019854272118901900 4\\
&35345279628510707298895463402570870 5\\
&82236466932625944388392940270854031 5\\
&8334109562115430000186150573802677 3.
\end{aligned}
$$

Again $b = 2$ works in the LPL Criterion, so N is prime.