RECENT DEVELOPMENTS IN PRIMALITY TESTING

Jon Grantham
Institute for Defense Analyses
Center for Computing Sciences
Bowie, MD

grantham@super.org

http://www.clark.net/pub/grantham/pseudo/

Outline

Old Results in Primality Proving

- The $n-1$ Test and its Relatives
- The APR Test

Old Results in Probable Primality Testing

- Pseudoprimes
- From Pseudoprimes to Provable Primes

New Results in Primality Proving

- Updates
- Elliptic Curve Methods
- New Life for the $n-1$ Test

New Results in Probable Prime Testing

- Perrin Pseudoprimes
- Carmichael Numbers
- Frobenius Pseudoprimes

Not-So-Recent Developments in Primality Proving

The Pocklington-Lehmer $n-1$ Test

Let n be an integer with $n-1 = FR$ and $F > \sqrt{n}$. If there exists an a with $a^{n-1} \equiv 1 \bmod n$ and

$$\gcd(a^{\frac{n-1}{q}} - 1, n) = 1$$

for each prime $q|F$, then n is prime.

Why? For each prime $p|n$, we have $(a^R)^F \equiv 1 \bmod p$, but $(a^R)^{F/q} \not\equiv 1$ for any $q|F$. Thus a^R has order F mod p. But $a^{p-1} \equiv 1 \bmod p$, and thus $F|(p-1)$. Therefore, $p-1 \geq F > \sqrt{n}$ for each $p|n$. This can only happen if n is prime.

The $n-1$ method and its relatives

With the $n-1$ method,and the $n+1$, n^2+1, n^2-n+1 or n^2-n-1 methods (Lucas; Pocklington; Lehmer; Robinson; Brillhart, Lehmer, Selfridge; Williams), the time required to prove primality is polynomial, **once you find the factorization of a factor of $n-1$ (or $n+1$, etc.) that is greater than $n^{1/3}$** (or $n^{1/2}$, depending on the test).

This is a practical test. A version of the $n+1$ test has been used to prove primality or compositeness of Mersenne numbers ($2^p - 1$), including the current world record prime, $2^{1398269}-1$, which was proved prime in 88 hours on a Pentium-90.

The APR Test

The APR test (or the APRCL test) (Adleman, Pomerance, Rumely; Cohen, H. Lenstra) was first described in 1980. It involves testing congruences in cyclotomic extensions of the rationals.

The APR test turns out to have a running time of $O\left((\log n)^{c \log\log\log n}\right)$. In one version, the running time is probabilistic; in another, the running time is deterministic.

The probabilistic version of the APR test is practical.

Not-So-Recent Developments in Probable Prime Testing

Pseudoprimes

By Fermat's Little Theorem, if p is a prime not dividing a,

$$a^{p-1} \equiv 1 \bmod p.$$

The converse is not true. $2^{340} \equiv 1 \bmod 341$, but 341 is not prime. We call 341 a **pseudoprime** to the base 2.

The pseudoprime test, however, is often "good enough." In particular, it provides a useful way of exposing composites.

Other Pseudoprimes

We also know if $p \not| 2a$,
$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p.$$

The converse does not hold; for example, $2^{280} \equiv \left(\frac{2}{561}\right)$. We call 561 an **Euler pseudoprime** to the base 2. (Robinson)

If $n \equiv 1 \bmod 4$, we can look at $a^{(n-1)/2^k}$ for $k > 1$. A **strong pseudoprime** to the base a is an odd composite $n = 2^r s + 1$, with s odd, such that either $a^s \equiv 1 \bmod n$, or $a^{2^t s} \equiv -1$ for some integer t, with $r > t \geq 0$. (Dubois; Selfridge)

Composites n dividing $F_{n-\left(\frac{n}{5}\right)}$ are **Fibonacci pseudoprimes**. This generalizes to the concept of **Lucas pseudoprimes**.

Pseudoprimes to Multiple Bases

There are numbers which are pseudoprimes to every base. We call these numbers **Carmichael numbers**.

No numbers are Euler pseudoprimes to all bases. In fact, for every composite n, for at least $\frac{1}{2}n$ bases less than n, n is **not** an Euler pseudoprime. (Solovay-Strassen)

Even better — no composite n can be a strong pseudoprime to more than $\frac{1}{4}n$ bases. (Monier; Rabin)

This means that if we chose bases at random, a composite has at most a $\frac{1}{4}$ chance of passing 1 iteration of this test, and a $\frac{1}{4^k}$ chance of passing k iterations.

When Probable becomes Provable

Miller proved a result which is equivalent to this:

Assuming the ERH, if n is composite, there is a base $b < c\log^2 n$ for which n fails the strong pseudoprime test to the base b.

Since a strong pseudoprime test takes $O(\log^3 n)$ bit operations, we have a method of primality proving that can be done in $O(\log^5 n)$ bit operations. . . if we can prove the Extended Riemann Hypothesis.

A hard problem in computational number theory (primality proving in deterministic polynomial time) was reduced to a hard problem in analytic number theory (ERH).

New Results in Primality Proving

Goldwasser-Kilian

Goldwasser and Kilian gave a test that heuristically runs in polynomial time. It runs in polynomial time for all but a small (infinite) class of primes.

Replace the group $(\mathbf{Z}/n\mathbf{Z})^*$ in the $n-1$ test with the group of points on an elliptic curve modulo n. Count the points with Schoof's algorithm (time: $O(\log^8 n)$).

The Goldwasser–Kilian algorithm isn't very practical, but represents an important conceptual breakthrough.

This method produces primality **certificates** which can be checked quickly without repeating the entire proof.

Atkin and Morain's ECPP

Atkin developed a similar algorithm; he and Morain implemented it.

They only use curves with complex multiplication. It is much faster to compute the order of these curves.

As a result, their algorithm is practical. They have made a version of it available under the name ECPP (Elliptic Curves and Primality Proving).

The ECPP program produces certificates that can be checked with a less complicated program.

Adleman-Huang

Adleman and Huang achieved an impressive theoretical milestone by modifying Goldwasser-Kilian.

Instead of using elliptic curves, they use Jacobians of curves $y^2 = f(x)$; $f(x)$ has degree 6. The number of points m will be larger than the prime. But, if m is prime, we may be able to prove its primality with the Goldwasser-Kilian method.

If we can't use that method to prove primality, we can just pick another polynomial $f(x)$ and try again.

While not practical, this method is the only known polynomial time primality proving algorithm. (It is not deterministic.)

New life for the $n-1$ test

H. Lenstra described a test based on polynomials over a finite field that has the same running time as the APR test.

Let $n > 1$ be an integer. Let I, E be integers with $E | n^I - 1$ and $E > \sqrt{n}$. Let $f(x) \in (\mathbf{Z}/n\mathbf{Z})[x]$ be a monic polynomial of degree I such that mod n, $f(x) | x^{n^I} - x$ and $\gcd(f(x), x^{n^{I/p}} - x) = 1$ for all $p | I$. Let $A = (\mathbf{Z}/n\mathbf{Z})[x]/(f(x))$. Let $\alpha \in A$ be such that $\alpha^E = 1$ and $\alpha^{E/q} - 1 \in A^*$ for all primes $q | E$. If $g(T) = (T - \alpha)(T - \alpha^n) \ldots (T - \alpha^{n^{I-1}}) \in (\mathbf{Z}/n\mathbf{Z})[T]$ and the least residue n^j mod E is not a proper divisor of n for $1 \leq j < I$, then n is prime.

Konyagin-Pomerance

In a recent paper, Konyagin and Pomerance gave several new versions of the $n-1$ test.

They gave a practical version if the factored part F of $n-1$ is greater than $n^{3/10}$.

They gave a version that, if F is greater than $n^{1/4+\epsilon}$, runs in deterministic polynomial time.

They gave a version that, if the factored part is greater than n^{ϵ} and consists entirely of small primes, runs in deterministic polynomial time. This method works for $\gg x^{1-\epsilon}$ primes less than x.

What's new in probable primality testing

Bach has shown that the bound in the ERH-conditional test can be taken to be $2\log^2 n$.

If k-bit integers ($k > 1$) are chosen at random until one is found which passes t strong pseudoprime tests, then the probability that the number is composite is less than 4^{-t}. (Damgard, Landrock, Pomerance; Burthe)

There are infinitely many Carmichael numbers! (Alford, Granville, Pomerance) Their proof uses a heuristic of Erdős, a version of the prime number theorem for arithmetic progressions, and other ingredients.

Perrin Pseudoprimes

In the 1982, Adams and Shanks introduced a test based on a third-order sequence known as Perrin's sequence:

$A_n = A_{n-2}+A_{n-3}$, $A_{-1} = -1$, $A_0 = 3$, $A_1 = 0$.

The test examines congruence properties mod n of the "signature"

$$(A_{-n-1}, A_{-n}, A_{-n+1}, A_{n-1}, A_n, A_{n+1}).$$

There are 3 types of acceptable signatures. The S-signature is

$$(1, -1, 3, 3, 0, 2).$$

Pseudoprimes for this test are relatively rare. Adams and Shanks conjectured, but could not prove, that there are infinitely many.

How it Generalizes and Strengthens

When $n \equiv 2$ or $3 \bmod 5$, the Fibonacci pseudoprime test asks whether $F_{n+1} \equiv 0$.

Equivalently, do we have

$x^{n+1} - (1-x)^{n+1} \equiv 0 \bmod (n, x^2 - x - 1)$?

When n is prime, $x^n \equiv 1 - x$, and $(1 - x)^n \equiv x$. So

$x^{n+1} - (1-x)^{n+1} \equiv (1-x)x - x(1-x) = 0.$

The Frobenius Test, in this case, asks whether $x^n \equiv 1-x \bmod (n, x^2-x-1)$. From that, it follows that n passes the Fibonacci test.

Not vice versa. 323 is the first Fibonacci pseudoprime. 5777 is the first Frobenius pseudoprime with respect to $x^2 - x - 1$.

Why Should You Buy a Definition from Me?

Gurak and Szekeres have given generalizations of the Perrin test. I should have to convince you why you should adopt mine.

First of all, it contains their definitions. This is good, but not sufficient.

Looking at polynomials over finite fields exposes the underlying structure.

I discovered that two types of pseudoprimes – Lehmer pseudoprimes and Lucas pseudoprimes – are essentially equivalent.

Both notions are over 25 years old.

OK, but what else does it come with?

Competitors to Monier-Rabin

Arnault showed that a composite n is a strong Lucas pseudoprime to at most $\frac{4}{15}$ of the bases. (Except for some easy to detect cases.)

Jones and Mo showed that a composite is an extra strong Lucas pseudoprime to at most $\frac{1}{8}$ of the bases. The test takes 2 times as long as the strong pseudoprime test.

A version of my test, the Quadratic Frobenius Test, takes asymptotically 3 times as long to run as the strong pseudoprime test. Any composite passes for less than $\frac{1}{7710}$ of the bases.

A Version of the Quadratic Frobenius Test

Here is one formulation of the Quadratic Frobenius Test for numbers $n \equiv 1 \bmod 4$.

1) Verify that n is not a perfect square.

2) Verify that n is not divisible by a prime less than 50000.

3) Choose (b, c) at random until you find a pair with $\left(\frac{b^2+4c}{n}\right) = -1$.

4) Let $y = x^{\frac{n+1}{2}} \bmod (n, x^2 - bx - c)$. Verify that $y \in \mathbf{Z}$ and $y^2 \equiv -c$.

5) Perform a strong pseudoprime test to the base y.

How Many Are There?

Let $f(x) \in \mathbf{Z}[x]$ be a monic, squarefree polynomial with splitting field K. There are infinitely many Frobenius pseudoprimes with respect to $f(x)$. In fact, there are $\gg N^c$ Frobenius pseudoprimes with respect to $f(x)$ which are less than N, for some $c = c(K) > 0$. These numbers are Frobenius pseudoprimes for any polynomial with splitting field K.

This theorem answers the 1982 conjecture of Adams and Shanks, as well as proving there are infinitely many pseudoprimes in the senses of Gurak and Szekeres, **or any other definition that uses the same basic concepts.**