AN EXPOSITION OF THE AKS POLYNOMIAL-TIME PRIMALITY TEST

Michael J. Jacobson, Jr.
University of Calgary

November 29, 2002

History

Miller 1976 — deterministic polynomial time (Extended Riemann Hypothesis)

Rabin 1980 — randomized polynomial time (no ERH)

Adleman, Pomerance, Rumely 1983 — deterministic $O((\log n)^{O(\log\log\log n)})$

Goldwasser Kilian 1986 — expected polynomial time

Adleman, Huang 1992 — randomized polynomial time

* Agrawal, Kayal, Saxena 2002 — $\tilde{O}(\log^{12} n)$

Notation and Assumptions

$\tilde{O}(\log^c n) = O(\log^c n \text{ poly}(\log\log n)) = O(\log^{c+\epsilon} n)$

Multiply two integers $\leq n$:

- $O(\log^2(n))$ or $O(\log n \log\log n)$ using FFT

Multiply two degree r polynomials:

- $O(r^2)$ coefficient mults or $O(r \log r)$ using FFT

Computing a^x — $O(\log x)$ multiplications

$o_r(n)$ — smallest $k \in \mathbb{Z}^+$ such that $n^k \equiv 1 \pmod{r}$

- if $q \mid r - 1$ and $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ then $q < o_r(n)$

$\mathbb{F}_p[x]$ — ring of polynomials with coeffs modulo p

$\mathbb{F}_p[x]/h(x)$ — equivalence classes modulo $h(x)$

Observation

Let $\gcd(a, n) = 1$. Then n is prime if and only if

$$(x - a)^n \equiv x^n - a \pmod{n}$$

(follows from the binomial theorem)

Example:

$$\begin{aligned}(x-3)^7 &= x^7 - 21x^6 + 189x^5 - \cdots + 5103x - 2187 \\ &\equiv x^7 - 3 \pmod{7}\end{aligned}$$

$$\begin{aligned}(x-5)^6 &= x^6 - 30x^5 + 375x^4 - \cdots - 18750x + 15625 \\ &\equiv x^6 + 3x^4 + 2x^3 + 3x^2 + 1 \pmod{6}\end{aligned}$$

This idea unconditionally proves primality:

- Takes time $\Omega(n)$ (polys of degree n)
- Can this be reduced?

Main Idea

Compute $(x-a)^n$ and $x^n - a \bmod x^r - 1, n$ (small r)

- only work with polynomials of degree $< r$
- $O(r^2 \log^3 n)$ or $\tilde{O}(r \log^2 n)$ (using FFT)

If n is prime, $(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$

If n is composite, $\exists a, r$ such that $(x-a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$

Example:

$$(x-5)^6 \equiv 3x^4 + 2x^3 + 3x^2 + x + 1 \pmod{x^5 - 1, 6}$$
$$x^6 - 5 \equiv x + 1 \pmod{x^5 - 1, 6}$$

- Can such a, r be found in polynomial time?
- Can we verify that none exist in polynomial time?

The Algorithm (AKS 2002)

1. If n is a perfect power, output COMPOSITE

2. Find prime r (sequentially) such that:

- $\gcd(n, r) = 1$,
- $q \geq 4\sqrt{r} \log n$ (largest prime factor of $r - 1$)
- $n^{(r-1)/q} \not\equiv 1 \pmod{r}$

3. For all $a \in \{1, \ldots, \lfloor 2\sqrt{r} \log n \rfloor\}$:

- if $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$
  output COMPOSITE

4. Output PRIME

Need to address runtime and correctness

Polynomial Time?

1. Perfect power test — $O(\log^3 n)$

2. Finding r (test all $1, 2, \ldots, r$):

- $\gcd(n, r)$ —poly$(\log r)$
- r prime, finding q — $O(r^{1/2}\ \mathrm{poly}(\log r))$
- $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ — poly$(\log r)$
- Total: $\tilde{O}(r \cdot r^{1/2}\ \mathrm{poly}(\log r))$

3. Testing primality condition:

- $\lfloor 2\sqrt{r} \log n \rfloor$ tests
- each test costs $\tilde{O}(r \log^2 n)$ (using FFT)
- Total: $\tilde{O}(r^{3/2} \log^3 n)$

Need to know size of r — should be poly$(\log n)$

Size of r

Need r such that:

1. $r - 1$ has a prime factor $q \geq 4\sqrt{r}\log n$

2. $q \mid o_r(n)$ (order of n modulo r)

Property 1:

Let $P(n)$ denote the largest prime divisor of n

Fouvry 1985 — $O(x/\log x)$ primes $r \leq x$ have $P(r-1) > x^{2/3}$

If $x \in O(\log^6 n)$, then $\exists\, r \in O(\log^6 n)$ with

$$q = P(r-1) \geq r^{2/3} \geq 4\sqrt{r}\log n$$

Call such r "special primes"

Size of r — Property 2

Let $x = c\log^6 n$ and consider

$$\Pi = (n-1)(n^2-1)\dots(n^{\lfloor x^{1/3}\rfloor}-1)$$

- Π has at most $x^{2/3}\log n$ distinct prime factors
- $\exists$ at least $c_3\log^6 n/(\log\log n)$ "special primes"
- $\exists$ at least one special prime $r \nmid \Pi$

Does $q \mid o_r(n)$?

- $o_r(n) > x^{1/3}$ (since $n^k \equiv 1 \pmod{r} \Longrightarrow r \mid n^k - 1$)
- $(r-1)/q < r/(r^{2/3}) = r^{1/3} < x^{1/3} < o_r(n)$
- $o_r(n) \mid r-1$ but $o_r(n) \nmid (r-1)/q \Longrightarrow q \mid o_r(n)$

Thus, $r \in O(\log^6 n)$

Summary of Run Time

1. Perfect power test — $O(\log^3 n)$

2. Finding r :

- $r \in O(\log^6 n)$
- testing each $1, \ldots, r$ costs $O(r^{1/2} \operatorname{poly}(\log r))$
- Total — $\tilde{O}(\log^6 n \ (\log^6 n)^{1/2}) = \tilde{O}(\log^9 n)$

3. Testing primality condition — $\tilde{O}(r^{3/2} \log^3 n)$

- $\tilde{O}((\log^6 n)^{3/2} \log^3 n) = \tilde{O}(\log^{12} n)$

Overall runtime: $\tilde{O}(\log^{12} n)$

(Asymptotic) polynomial time!

Is the Algorithm Correct?

Need to show:

1. If n is prime, output is PRIME (easy)

2. If output is PRIME, then n is prime (not so easy)

To show 1 (assume n is prime):

- $(x-a)^n \equiv x^n - a \pmod{n}$ for all a with $\gcd(a,n)=1$.
- All a in Step 3 have $\gcd(a,n)=1$.
- $(x-a)^n \equiv x^n - a \pmod{x^r-1, n}$ for all a in Step 3

Outline of Proof

Assume $(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$

1. $\exists$ prime $p \mid n$ and $h(x) \mid x^r - 1$ s.t.

$$(x-a)^n = x^n - a \text{ in } \mathbb{F}_p[x]/h(x)$$

(i.e., coefficients mod p and polynomials mod $h(x)$)

2. $\exists$ a "large" cyclic subgroup G of $(\mathbb{F}_p[x]/h(x))^*$

3. $\exists$ $(i_1, j_1) \neq (i_2, j_2)$ such that

- $0 \leq i_1, i_2, j_1, j_2 \leq \lfloor \sqrt{r} \rfloor$
- $t \equiv u \pmod{r}$ where $t = n^{i_1} p^{j_1}$ and $u = n^{i_2} p^{j_2}$
- $g^t = g^u$ for all $g \in G$

4. If g generates G and $|G|$ is "large"

- $t = u$, and thus $n = p^k$

Underlying Structure

Let $\ell = \lfloor 2\sqrt{r}\log n \rfloor$

Assume the algorithm outputs PRIME. Then

- $(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$, $1 \le a \le \ell$

By construction $q \mid o_r(n)$

- $\exists$ prime $p \mid n$ such that $q \mid o_r(p)$
- $q \mid o_r(p) \Rightarrow q \le o_r(p)$
- $\exists\ h(x) \mid x^r - 1$, $\deg(h(x)) = o_r(p)$, irreducible
- $q \le d = \deg(h(x))$

$(x-a)^n = x^n - a$ in $\mathbb{F}_p[x]/h(x)$

(Intuition: $x \equiv y \pmod{pq} \Rightarrow x \equiv y \pmod{p}$)

The Group G

Consider set of products of $(x-a)$ in $\mathbb{F}_p[x]/h(x)$

$$G = \left\{ \prod_{1 \le a \le \ell} (x-a)^{\alpha_a} \mid \alpha_a \ge 0 \right\}$$

- G is a cyclic subgroup of $(\mathbb{F}_p[x]/h(x))^*$
- $\exists$ a generator g with order $|G|$

How large is G?

- The following products are distinct modulo $h(x)$:
  $$\prod_{1 \le a \le \ell} (x-a)^{e_a}, \quad \sum_{1 \le a \le \ell} e_a \le d-1$$
  (since all $a < n$ and $\gcd(a, n) = 1$)
- $|G| > \binom{\ell + d - 1}{\ell} = \frac{(d+l-1)(d+l-2)\dots(d)}{l!} > \left(\frac{d}{\ell}\right)^{\ell}$

$d \ge q \ge 2\,\ell$, so $|G| > 2^{\ell} = n^{2\lfloor\sqrt{r}\rfloor}/2$

More Properties of G

If $(x-a)^n \equiv x^n - a \pmod{p, x^r - 1}$ then

- $(x^{n^i} - a)^n = x^{n^{i+1}} - a$
- $(x-a)^{n^i} = x^{n^i} - a$, $i \geq 0$ (induction)
- $(x-a)^{n^i p^j} = (x^{n^i} - a)^{p^j} = x^{n^i p^j} - a$

Let $t = n^{i_1} p^{j_1}$ and $u = n^{i_2} p^{j_2}$ with

$$(i_1, j_1) \neq (i_2, j_2) \quad \text{and} \quad t \equiv u \pmod{r}$$

Then for all $1 \leq a \leq \ell$

$$(x-a)^t = (x-a)^u \text{ in } \mathbb{F}_p[x]/h(x)$$

For any $g \in G$, $g^t = g^u$ since

$$g = (x-1)^{\alpha_1}(x^2-1)^{\alpha_2} \dots (x-\ell)^{\alpha_\ell}$$

and

$$\begin{aligned} g^t &= ((x-1)^t)^{\alpha_1}((x^2-1)^t)^{\alpha_2} \dots ((x-\ell)^t)^{\alpha_\ell} \\ &= ((x-1)^u)^{\alpha_1}((x^2-1)^u)^{\alpha_2} \dots ((x-\ell)^u)^{\alpha_\ell} \\ &= g^u \end{aligned}$$

Putting it Together

Consider $n^i p^j$, $0 \leq i, j \leq \lfloor \sqrt{r} \rfloor$:

- total number of pairs is $(1 + \lfloor \sqrt{r} \rfloor)^2 > r$
- $\exists (i_1, j_1) \neq (i_2, j_2)$ such that $n^{i_1} p^{j_1} \equiv n^{i_2} p^{i_2} \pmod{r}$

Let $g \in G$

- $g^t = g^u$, where $t = n^{i_1} p^{j_1}$ and $u = n^{i_2} p^{i_2}$
- $g^{|t-u|} = 1$ in G
- $|t - u| < n^{\lfloor \sqrt{r} \rfloor} p^{\lfloor \sqrt{r} \rfloor} \leq n^{2 \lfloor \sqrt{r} \rfloor}/2 < |G|$

If g generates G, we must have $t = u$:

- $n^{i_1} p^{j_1} = n^{i_2} p^{j_2}$ with $(i_1, j_1) \neq (i_2, j_2)$
- $n = p^k$

Step 1 assures us that $k = 1$

Advertisement

What: Conference in Number Theory in Honour of Professor H.C. Williams

Where: The Banff Centre, Banff, Alberta, Canada

When: May 24–30, 2003

Who and Why:

Manindra Agrawal will give a special evening lecture at the Banff Center on Sunday May 25, 2003, with a reception to follow in his honour sponsored by RSA Security Inc.

More Info:

www.fields.utoronto.ca/programs/scientific