Agrawal–Kayal–Saxena Algorithm for

Testing Primality in Polynomial Time

slides by

Mitsunori Ogihara
Department of Computer Science
University of Rochester
ogihara@cs.rochester.edu

and

Stanisław Radziszowski
Department of Computer Science
Rochester Institute of Technology
spr@cs.rit.edu

Brief History

- Eratosthenes, 276 BC – 194 BC: the Eratosthenes Sieve
- Pratt '75: in NP
- Miller '76: $O(\log^4 n)$-time solvable if the Extended Riemann Hypothesis is true
- Solovay & Strassen '77; Rabin '80: in coRP, still the choice in applications
- Adleman, Pomerance, & Rumely '83: deterministic $O((\log n)^{\log\log\log n})$-time
- Goldwasser & Kilian, '86: "Almost all" primes can be proven to be prime in $O(\log^{12} n)$ time
- Adleman & Huang '87: in RP
- Fellows & Koblitz '92: in UP
- This paper: in P, $O((\log^{12} n)\mathrm{poly}(\log\log n))$-time

Preliminaries

$n \geq 3$: odd integer
Z_n : the integer ring modulo n
Z_n is a field if n is prime
Z_n^* : the multiplicative group modulo n
Z_n^* is a cyclic group if n is prime.

$\lg n = \log_2 n$: binary logarithm
$\ln n = \log_e n$: natural logarithm

a : integer, $\mathrm{GCD}(n, a) = 1$
$o_n(a)$: the order of a modulo n,
i.e., the smallest positive integer m such that
$a^m \equiv 1 \pmod{n}$

Preliminaries

Fermat's (Little) Theorem Let p be prime. Then, for all a relatively prime to p, $o_p(a)|p-1$, that is, $a^{p-1} \equiv 1 \pmod{p}$.

Basic Congruence (AKS) Let a and n be relatively prime. Then, n is prime iff

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

Proof of the AKS congruence

If n is prime, then by Fermat's Theorem, for all a relatively prime to n, $a^n \equiv a \pmod{n}$ For all i, $1 \leq i \leq n-1$, the coeff. of x^i in $(x-a)^n$ is $(-a)^{n-i}\binom{n}{i}$, a multiple of n. Thus

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

If n is composite, let q be a prime such that $n = q^k s$ and $q \not| s$. Since $\binom{n}{q} = \frac{q^k s \cdot \ldots \cdot (q^k s - q + 1)}{1 \cdot \ldots \cdot q}$, then

$$q^k \not| \binom{n}{q}, \quad \text{GCD}(q, a^{n-q}) = 1$$

so the coeff. of x^q is nonzero modulo n.

Congruence follows.

∎

Some Results on Polynomials

Proposition 1 *p, r : distinct primes*

1. *For all polynomials $f(x) \in F_p[x]$,*
   $f(x)^p \equiv f(x^p) \pmod{p}$.
2. *Let $h(x)$ be a factor of $x^r - 1$.*
   For all integers m and m' such that
   $m \equiv m' \pmod{r}$,
   $x^m \equiv x^{m'} \pmod{h(x)}$.
3. *Over F_p, the polynomial $\frac{x^r-1}{x-1}$ is the product of degree-$o_r(p)$ irreducible polynomials.*

Proof of Proposition 1

[1] Let $f(x) = a_0 + a_1 x + \cdots + a_d x^d$
$0 \le j \le dp$
The coeff. of x^j in $f(x)^p$ is

$$\sum a_0^{i_0} \cdots a_d^{i_d} \frac{p!}{i_0! \cdots i_d!},$$

where the summation is over $\{(i_0, \ldots, i_d) \mid i_0 \ge 0, \ldots, i_d \ge 0 \wedge i_0 + \cdots + i_d = p \wedge 1 \cdot i_1 + 2 \cdot i_2 + \cdots + d \cdot i_d = j\}$. Note that

$$\frac{p!}{i_0! \cdots i_d!} \equiv \begin{cases} 1 \pmod{p} & (\exists u)[i_u = p] \\ 0 \pmod{p} & \text{otherwise.} \end{cases}$$

In the former case $p|j$. Thus,

$$f(x)^p \equiv \sum_{0 \le i \le d} a_i^p x^{ip} \pmod{p}.$$

Since p is prime, for all i, $0 \le i \le d$, $a_i^p \equiv a_i \pmod{p}$. So,

$$f(x^p) = \sum_{0 \le i \le d} a_i x^{ip} \equiv f(x)^p \pmod{p}.$$

[2] Suppose $m \equiv m' \pmod{r}$.
Let s be such that $m = sr + m'$.
Since $h(x) | x^r - 1$, $x^r \equiv 1 \pmod{h(x)}$.
So, $x^{sr} \equiv 1 \pmod{h(x)}$.
Thus, $x^m = x^{sr} x^{m'} \equiv x^{m'} \pmod{h(x)}$.

[3] p and r: distinct primes
$h(x)$: irreducible factor of $\frac{x^r-1}{x-1}$ in $F_p[x]$.
Let $k = \deg(h)$ and $d = o_r(p)$.
We'll show $d|k$ and $k|d$, which imply $d = k$.

Since h is irreducible and p is prime,
$F_p[x]/h(x)$ is a field.
The size of the field is p^k.
Furthermore, $(F_p[x]/h(x))^*$ is cyclic
Let $g(x)$ be a generator of $(F_p[x]/h(x))^*$.

d divides k

$h(x)|x^r - 1$, thus $x^r \equiv 1 \pmod{h(x)}$, it implies that order of x in $F_p[x]/h(x)$ divides r.
Since r is prime, the order is actually r.

Since g is a generator, the order of x should divide the order of g, so we have $r|p^k - 1$.
Thus, $p^k \equiv 1 \pmod{r}$.
Since $d = o_r(p)$, we have $d|k$.

k *divides* d

By (1), we have

$$g(x)^p \equiv g(x^p) \pmod{p},$$
$$g(x)^{p^2} \equiv g(x^p)^p \equiv g(x^{p^2}) \pmod{p},$$
$$\ldots$$
$$g(x)^{p^d} \equiv g(x^{p^{d-1}})^p \equiv g(x^{p^d}) \pmod{p}.$$

Since $d = o_r(p)$, $p^d \equiv 1 \pmod{r}$.
Then, by (2), $x^{p^d} \equiv x \pmod{h(x)}$,
so $g(x)^{p^d} \equiv g(x) \pmod{h(x)}$.
This implies that $g(x)^{p^d-1} \equiv 1 \pmod{h(x)}$.
The order of $g(x)$ is $p^k - 1$, so $p^k - 1 | p^d - 1$.
Let $d = ks + z, 0 \leq z < k$. We have

$$(p^d - 1) = (p^k - 1)(p^{d-k} + p^{d-2k} + \cdots + p^z) + p^z - 1$$

so $z = 0$ and $k|d$. ∎

“Useful” Primes

(This terminology is not used in AKS)

$n \geq 3$: odd
r : odd prime, GCD$(n, r) = 1$
r is **useful** (in testing n's primality),
if $r - 1$ has a prime factor q such that

1. $q \geq 4\sqrt{r} \ln n$ and
2. $n^{(r-1)/q} \not\equiv 1 \pmod{r}$.

If r is useful, there is only one prime q witnessing that r is useful;
also, $q | o_r(n)$ and $o_r(n) | r - 1$.

A prime r is **semi-useful** in testing n's primality if $r - 1$ has a prime factor q such that $q \geq 4\sqrt{r} \ln n$.

The Algorithm

n_1 is a constant given later.

Input an odd integer $n \geq n_1$
▷ Search for a Useful Prime
$r \leftarrow 3$
while $(r < n)$ **do** {
    if GCD$(n, r) \neq 1$ **then** output("composite")
    if r is prime **then** {
        $q \leftarrow$ the largest prime factor of $r - 1$
        if $(q \geq \lceil 4\sqrt{r} \ln n \rceil)$ **and**
            $(n^{(r-1)/q} \not\equiv 1 \pmod{r})$ **then** break }
    $r \leftarrow r + 2$ }
▷ Binomial Power Test
for $a \leftarrow 1$ **to** $\lceil 2\sqrt{r} \lg n \rceil$ **do**
    if $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$
        then output("composite")
▷ Prime Power Test
for $k \leftarrow 2$ **to** $\lfloor \ln n / \ln 3 \rfloor$ **do**
    if $(\lfloor n^{1/k} \rfloor)^k = n$ **then** output("composite")
output("prime")

Theorem 1 *The above algorithm works correctly and runs in time polynomial in* $\log n$.

The Proof Strategy

GOAL I **The smallest useful prime number is $O(\log^6 n)$.**

GOAL II **For all $n \geq n_1$, given a useful prime r, the two tests correctly decide whether n is a prime.**

GOAL III **The algorithm has a polynomial running time.**

Achieving Goal I

Theorem 2 $(\exists c_1, c_2, n_1)(\forall n \geq n_1)$
The interval $[c_1 \ln^6 n, c_2 \ln^6 n]$ *contains a prime that is useful in testing* n*'s primality.*

Two useful lemmas.

Lemma 1 *[Fouvry '85]* $(\exists c_0, n_0)(\forall x \geq n_0)$
$|\{p \mid p \leq x \wedge p$ *is a prime* $\wedge\, p-1$ *has a prime factor* $\geq x^{\frac{2}{3}}\}| \geq c_0 x / \ln x$

Lemma 2 *[Apostol '97]* *For all* $n \geq 1$,

$$\frac{n}{6 \ln n} \leq \pi(n) \leq \frac{8n}{\ln n},$$

where $\pi(n)$ *is the number of primes* $\leq n$.

(Apostol '76 gave a better upper bound $\frac{6n}{\ln n}$)

Proof of Theorem 2

Let c_1 be any constant $\geq 4^6 = 4096$.
Let c_2 be any constant such that c_3 defined by $c_3 = \frac{c_0 c_2}{7} - \frac{4c_1}{3}$ is positive.
Let $c_4 = \frac{c_2}{4\sqrt{c_1}}$.

Let n_1 be the smallest integer m such that

(i) $c_2 \ln^6 m \geq n_0$,

(ii) $\ln m \geq c_2$, and

(iii) $(c_4)^2 < \frac{c_3 \ln m}{\ln \ln m}$.

Then, for all $n \geq n_1$, (i)–(iii) hold with $m = n$.
Let $I = [c_1 \ln^6 n, c_2 \ln^6 n]$.

The Proof Strategy:

- Bound from below the # of semi-useful primes in I.
- By counting argument show that one of the semi-useful primes is actually useful.

of Semi-Useful Primes in $I \geq$?

Since (i) holds, Lemma 1 can be applied.
# of primes $r \leq c_2 \ln^6 n (= x)$ such that $r - 1$ has a prime factor $\geq r^{\frac{2}{3}}$ is at least

$$\geq c_0 \frac{c_2 \ln^6 n}{\ln(c_2 \ln^6 n)}$$

$$= \frac{c_0 c_2 \ln^6 n}{\ln c_2 + 6 \ln \ln n}$$

By (ii), $\ln \ln n \geq \ln c_2$. So, this is at least

$$\geq \frac{c_0 c_2 \ln^6 n}{7 \ln \ln n}.$$

OTOH
the # of primes r such that $r \leq c_1 \ln^6 n$
is equal to $\pi(c_1 \ln^6 n)$.

By Lemma 2, this is

$$\leq \frac{8c_1 \ln^6 n}{\ln(c_1 \ln^6 n)}$$

$$= \frac{8c_1 \ln^6 n}{\ln c_1 + 6 \ln \ln n}$$

$$\leq \frac{8c_1 \ln^6 n}{6 \ln \ln n} = \frac{4c_1 \ln^6 n}{3 \ln \ln n}.$$

By combining the two bounds,
the # of primes $r \in I$ such that $r-1$ has a prime factor $\geq r^{\frac{2}{3}}$ is

$$\geq \frac{c_0 c_2 \ln^6 n}{7 \ln \ln n} - \frac{4 c_1 \ln^6 n}{3 \ln \ln n}$$

$$= \left(\frac{c_0 c_2}{7} - \frac{4 c_1}{3} \right) \frac{\ln^6 n}{\ln \ln n}$$

$$= \frac{c_3 \ln^6 n}{\ln \ln n}.$$

All $t \in I$ satisfy $t \geq c_1 \ln^6 n$.
Since $c_1 \geq 4^6$, we have $t^{\frac{1}{6}} \geq 4 \ln n$.
For all $x \geq 0$, $x^{\frac{2}{3}} = x^{\frac{1}{6}}\sqrt{x}$.

We counted primes $r \in I$, for which the largest prime factor q of $r-1$ satisfies

$$q \geq r^{\frac{2}{3}} = r^{\frac{1}{6}}\sqrt{r} \geq 4\sqrt{r}\ln n.$$

This implies that

the # of semi-useful primes in I is

$$\geq \frac{c_3 \ln^6 n}{\ln \ln n}.$$

of "Useless" Primes $\leq$?

Let $M = \lfloor c_4 \ln^2 n \rfloor$. Define

$$\Psi = \prod_{1 \leq i \leq M} (n^i - 1).$$

Then # of odd prime factors of Ψ is less than

$$\ln \Psi = \sum_{1 \leq i \leq M} \ln(n^i - 1).$$

$(\forall i \geq 1)[\ln(n^i - 1) < i \ln n]$
$(\forall d \geq 1)[\sum_{(1 \leq i \leq d)} i = d(d+1)/2 \leq d^2]$
So, the # of odd prime factors of Ψ is

$$< M^2 \ln n \leq (c_4)^2 \ln^5 n$$

and by (iii)

$$< \frac{c_3 \ln^6 n}{\ln \ln n}.$$

Thus, **there is a semi-useful prime $r \in I$ such that $r \not| \Psi$.**

We now claim that such
semi-useful primes are actually useful.

r : semi-useful prime in I, $r \not| \Psi$
q : the largest prime factor of $r-1$
$q \geq 4\sqrt{r}\ln n$.

Assume r is not useful, i.e. $q \not| o_r(n)$.
Since r is prime, $o_r(n) | r-1$.
Since q is prime and $q \not| o_r(n)$, $o_r(n) | \frac{r-1}{q}$.

Since $c_1 \ln^6 n \leq r \leq c_2 \ln^6 n$ and
$q \geq 4\sqrt{r}\ln n$, we have

$$\frac{r-1}{q} \leq$$

$$\left\lfloor \frac{c_2 \ln^6 n}{4\sqrt{(c_1 \ln^6 n)\ln n}} \right\rfloor =$$

$$\left\lfloor \frac{c_2}{4\sqrt{c_1}} \ln^2 n \right\rfloor = \left\lfloor c_4 \ln^2 n \right\rfloor = M.$$

Now

$$o_r(n)|\tfrac{r-1}{q} \text{ and } \tfrac{r-1}{q} \leq M$$

imply that r divides at least one of

$$n-1, n^2-1, \ldots, n^M-1,$$

and thus $r|\Psi$, which is a contradiction.

Hence, $q|o_r(n)$ and so r is useful.
This proves Theorem 2.

Achieving Goal II

We need to show the following:

Theorem 3 *Let $n \geq n_1$ be a prime. Then n passes the Binomial Power Test and the Prime Power Test.*

Theorem 4 *Let $n \geq n_1$ be an odd composite number. If n passes through the Binomial Power Test (passes lines 1-14, enters line 15), then n is a prime power.*

Proof of Theorem 3

n : a prime number $\geq n_1$
r : the useful prime selected by the algorithm
q : the witness of r's usefulness

$4\sqrt{r}\ln n \leq q < r < n$
So, by line (5) of the algorithm, for all a,
$1 \leq a \leq \lceil 2\sqrt{r}\lg n \rceil$, $\mathrm{GCD}(n, a) = 1$.

Thus, by the Basic Congruence

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

The equivalence still holds if the polynomials are reduced by taking modulo $x^r - 1$.

So, n passes the Binomial Power Test.

Prime n must pass the Prime Power Test.

∎

Proof of Theorem 4

n : odd composite number $\geq n_1$
r : the useful prime selected by the algorithm
q : the prime witnessing that r is useful
$p_1, \ldots, p_t$: all distinct prime divisors of n

For each i, $1 \leq i \leq t$, since GCD$(r, p_i) = 1$,
we can let $\lambda_i = o_r(p_i)$.

Define $\lambda_0 =$ LCM$(\lambda_1, \ldots, \lambda_t)$.
For all i, $1 \leq i \leq t$, $p_i^{\lambda_0} \equiv 1 \pmod{r}$.
So, $n^{\lambda_0} \equiv 1 \pmod{r}$, and thus, $o_r(n) | \lambda_0$.

Since q is prime and $q | o_r(n)$,
$(\exists i : 1 \leq i \leq t)[\ q \mid \lambda_i\ ]$.
Choose any such i and let $p = p_i$.

After Line 14

Let $h(x)$ be an irreducible polynomial in $F_p[x]$, such that $h(x)|\frac{x^r-1}{x-1}$.
Set $d = \text{deg}(h)$ and $\ell = \lceil 2\sqrt{r}\,\text{lg}\, n\rceil$.
By (3) of Proposition 1, $d = o_r(p)$.

Suppose n passes the Binomial Power Test. Then

- $(\forall a : 1 \leq a \leq \ell)$
  $(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$.

Since $h(x)|x^r - 1$ and $p|n$, we have

- $(\forall a : 1 \leq a \leq \ell)$
  $(x-a)^n \equiv x^n - a \pmod{h(x), p}$.

$\text{GCD}(n, \prod_{1\leq i\leq r} i) = 1$ and $r > \ell$ imply that $p > \ell$, and thus $1, \ldots, \ell$ are pairwise distinct modulo p.

A Cyclic Group of Polynomials

Define G to be the set of all polynomials in $(F_p[x]/h(x))^*$ of the form

$$(x-1)^{\alpha_1}\cdots(x-\ell)^{\alpha_\ell}$$

such that $\alpha_1,\ldots,\alpha_\ell$ are nonnegative integers.

Proposition 2

G is a cyclic multiplicative group of order Ω, and

$$\Omega > \left(\frac{\ell+d-1}{\ell}\right)^{\ell}$$

Proof of Proposition 2

It is known fact that every multiplicative subgroup of a field is cyclic.
G is a subset of the field $F_p[x]/h(x)$ and is a group (closed under multiplication).
So, G is a cyclic group.
Let $g(x)$ be a generator of G.
$g(x)$ has order Ω.

We need to show that $\Omega > \left(\frac{\ell+d-1}{\ell}\right)^{\ell}$.

Define $S \subset G$ to be the set of all polynomials in $(F_p[x]/h(x))^*$ of the form

$$(x-1)^{\alpha_1} \cdots (x-\ell)^{\alpha_\ell}$$

such that $\alpha_1, \ldots, \alpha_\ell$ are nonnegative and $\alpha_1 + \cdots + \alpha_\ell \le d-1$.

We will claim that distinct sequences $\alpha_1, \cdots, \alpha_\ell$ in the definition lead to different elements of S. Once the claim is proved, using

$\frac{x+1}{y+1} < \frac{x}{y}$ for $0 < y < x$,

we can observe that for $d > 1$

$$|S| = \binom{\ell + d - 1}{\ell} =$$

$$\frac{\ell + d - 1}{\ell} \cdot \frac{\ell + d - 2}{\ell - 1} \cdot \frac{\ell + d - 3}{\ell - 2} \cdot \ldots \cdot \frac{d}{1} >$$

$$\left(\frac{\ell + d - 1}{\ell}\right)^\ell,$$

which will finish the proof of Proposition 2.

Proving the Claim. Let
$v(x) = (x-1)^{\alpha_1} \cdots (x-\ell)^{\alpha_\ell}$ and
$w(x) = (x-1)^{\beta_1} \cdots (x-\ell)^{\beta_\ell}$

be two polynomials in S such that

(*) $\quad v(x) \equiv w(x) \pmod{h(x), p}$.

For each a, $1 \le a \le \ell$, let

- $\gamma_a = \min\{\alpha_a, \beta_a\}$,
- $\alpha'_a = \alpha_a - \gamma_a$, and
- $\beta'_a = \beta_a - \gamma_a$.

Note that

- $\alpha_a = \beta_a$ implies $\alpha'_a = \beta'_a = 0$
- $\alpha_a < \beta_a$ implies $\alpha'_a = 0$
- $\alpha_a > \beta_a$ implies $\beta'_a = 0$

Since $F_p[x]/h(x)$ is a field, we can divide (*) by $\prod_{1 \le a \le \ell} (x-a)^{\gamma_a}$.

Proving the Claim (cont'd)

Then we have

$$\prod_{1\le a\le \ell}(x-a)^{\alpha'_a} \equiv \prod_{1\le a\le \ell}(x-a)^{\beta'_a} \pmod{h(x), p},$$

or,

$$\prod_{1\le a\le \ell}(x-a)^{\alpha'_a} - \prod_{1\le a\le \ell}(x-a)^{\beta'_a} \equiv 0 \pmod{h(x), p}.$$

The roots of LHS : the a's such that $\alpha'_a > 0$.
The roots of RHS : the a's such that $\beta'_a > 0$.
The intersection of the two sets is empty.

If one of them is nonempty, we have a nonzero polynomial of degree $\le d-1$ that is congruent to 0 modulo $h(x)$.

That's a contradiction since h is irreducible.

So, both are empty, i.e.
$\alpha'_1, \ldots, \alpha'_\ell, \beta'_1, \ldots, \beta'_\ell = 0$.

Reminder

$q|d = deg(h) = o_r(p)$, and $o_r(p)|r-1$

$x^r - 1 \pmod p$ factorizes into $(x-1)$ and $(r-1)/d$ degree-d irreducible polynomials $h_s(x)$, $1 \leq s \leq (r-1)/d$, where $h(x)$ is one of them:

$$x^r - 1 \equiv (x-1) \prod_{1 \leq s \leq (r-1)/d} h_s(x) \pmod p$$

Note also that
$d \geq q \geq \lceil 4\sqrt{r} \ln n \rceil > \ell = \lceil 2\sqrt{r} \lg n \rceil$

Order of G

Observe that since $d \geq l + 1$ we have $(\ell + d - 1)/\ell \geq 2$, and use $\lg e < 2$ (when changing the base of logarithms).

Thus, by Proposition 2,

$$\Omega = |G| > \left(\frac{\ell + d - 1}{\ell}\right)^{\ell} \geq$$

$$2^{\ell} \geq (2^{\lg n})^{2\sqrt{r}} \geq n^{2\sqrt{r}}.$$

So, the order of $g(x)$ in $(F_p[x]/h(x))^*$ is greater than $n^{2\sqrt{r}}$.

Set I_g

Define
$I_g = \{m \mid g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$.

Fact 1 *I_g is closed under multiplication.*

Proof of the Fact

Assume $m_1, m_2 \in I_g$. Then

(a) $g(x)^{m_1} \equiv g(x^{m_1}) \pmod{x^r - 1, p}$

(b) $g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$

In (b), put x^{m_1} in place of x. Then
$g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^{m_1 r} - 1, p}$.
Now, since $x^r - 1 | x^{m_1 r} - 1$
$g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p}$.
OTOH, by (a),
$g(x)^{m_1 m_2} \equiv g(x^{m_1})^{m_2} \pmod{x^r - 1, p}$.
So, $g(x)^{m_1 m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p}$. ∎

Hint:

r is very small, $< c_2 \ln^6 n$

Ω is very large, $> n^{2\sqrt{r}}$

Lemma 3 *For all $m_1, m_2 \in I_g$, if $m_1 \equiv m_2 \pmod{r}$, then $m_1 \equiv m_2 \pmod{\Omega}$.*

Proof of Lemma 3

Let $m_1, m_2 \in I_g$.

Suppose that $m_1 \equiv m_2 \pmod{r}$.

Let $m_2 = m_1 + kr$ for some integer $k \geq 0$.

Since $m_2 \in I_g$,

$g(x)^{m_1+kr} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$,

and thus, $g(x)^{m_1+kr} \equiv g(x^{m_2}) \pmod{h(x), p}$.

By (2) of Proposition 1,

$g(x^{m_1+kr}) \equiv g(x^{m_1}) \pmod{h(x)}$, so

$g(x^{m_2}) \equiv g(x^{m_1}) \pmod{h(x), p}$.

Proof of Lemma 3 (cont'd)

Thus, by the latter and since $m_1, m_2 \in I_g$,

$$g(x^{m_1}) \equiv g(x^{m_2}) \equiv$$

$$g(x)^{m_2} \equiv g(x)^{m_1+kr} \equiv$$

$$g(x)^{m_1} g(x)^{kr} \equiv$$

$$g(x^{m_1}) g(x)^{kr} \pmod{h(x), p}$$

This implies $g(x)^{kr} \equiv 1 \pmod{h(x), p}$.
Thus, $\Omega | kr$.
Hence, $m_1 \equiv m_2 \pmod{\Omega}$. ∎

n and p are members of I_g

Our assumption is that $(\forall a : 1 \leq a \leq \ell)$
$[(x-a)^n \equiv x^n - a \pmod{x^r - 1, p}]$.

$g(x)$ can be represented as a product of factors (with multiplicities) chosen from $x-1, x-2, \ldots, x-\ell$.

Each term $(x-a)$ of g satisfies
$[(x-a)^n \equiv x^n - a \pmod{x^r - 1, p}]$.

Hence, any product of terms $(x-a)$ also does, and thus,

$$g(x)^n \equiv g(x^n) \pmod{x^r - 1, p}.$$

This implies that $n \in I_g$.

OTOH, by (1) of Proposition 1,
$g(x)^p \equiv g(x^p) \pmod{x^r - 1, p}$,
and thus, $p \in I_g$.

n must be a prime power

Define $E = \{n^i p^j \mid 0 \leq i, j \leq \lfloor\sqrt{r}\rfloor\}$.

By Fact 1, I_g is closed under multiplication. So, $E \subseteq I_g$.

Consider exponents i_1, j_1, i_2, j_2 with the range as in E. Since

$$|E| = (1 + \lfloor\sqrt{r}\rfloor)^2 > r,$$

by the pigeon-hole principle we have

$(\exists (i_1, j_1), (i_2, j_2))$
$[\ ((i_1 \neq i_2) \vee (j_1 \neq j_2)) \wedge (i_1 \geq i_2)$
$\wedge\, n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \pmod{r}]$.

Note that $\mathrm{GCD}(n, r) = 1$, so $n^{-1} \pmod{r}$ exists, and thus

$$n^{i_1 - i_2} p^{j_1} \equiv p^{j_2} \pmod{r}.$$

By Lemma 3,

$$n^{i_1 - i_2} p^{j_1} \equiv p^{j_2} \pmod{\Omega}.$$

n must be a prime power

Since $\Omega > n^{2\sqrt{r}}$ and
$0 \leq (i_1 - i_2), |j_1 - j_2| \leq \lfloor\sqrt{r}\rfloor$, then

$n^{(i_1-i_2)}, p^{|j_2-j_1|} < n^{\sqrt{r}} < \sqrt{\Omega}$.

$\Omega | p^d - 1$, so $\mathrm{GCD}(\Omega, p) = 1$, and there exists $p^{-1} \pmod{\Omega}$. So, if $j_2 \geq j_1$,

$$n^{i_1-i_2} \equiv p^{j_2-j_1} \pmod{\Omega},$$

and the congruence is actually an equality

$$n^{i_1-i_2} = p^{j_2-j_1}.$$

Note that $i_1 - i_2 = 0$ iff $j_2 - j_1 = 0$,
so $i_1 \neq i_2$, and we have a prime power

$$n = p^{\frac{j_2-j_1}{i_1-i_2}}.$$

If $j_2 < j_1$, we obtain a contradiction

$$\Omega > n^{i_1-i_2} p^{j_1-j_2} \equiv 1 \pmod{\Omega}.$$

This implies that n is a prime power,
and completes the proof of Theorem 4. ∎

Achieving Goal III

Cost of the Search Phase

(lines 2-10)

$r = O(\log^6 n)$ bounds the number of rounds

If naive primality test for r and factorization of $r-1$ methods are used, each makes up to $\sqrt{r} = O(\log^3 n)$ rounds.

GCD (line 5) and exponentiation (line 9) are done only once at each round, and are faster than naive factoring of $r-1$.

All arithmetic is done on numbers up to r.

Altogether, one round of the search loop requires up to $O((\log^4 n)\text{poly}(\log r))$ steps, so the search phase requires $O((\log^{10} n)\text{poly}(\log \log n))$ steps.

Achieving Goal III, cont'd.

Cost of the Binomial Power Test
(lines 12-14)

In the Binomial Power Test the loop-body is executed $O(\sqrt{r} \log n)$ times, which is the same as $O(\log^4 n)$.

Using Fast Fourier Transform in Z_n, multiplication of two polynomials having degree $\leq r$ modulo a polynomial having degree r can be done in

$$O(r \log r \log n) = O((\log^7 n)\text{poly}(\log r))$$

steps.

If repeated squaring is used for powering, a single test requires $O((\log^8 n)\text{poly}(\log r))$ steps.

Thus, the Binomial Power Test requires $O((\log^{12} n)\text{poly}(\log \log n))$ steps.

Cost of the Prime Power Test
(lines 16-17)

Prime Power Test makes $O(\log n)$ rounds.

If the binary search is used for root finding, then one round of the Prime Power Test requires only $O(\log^3 n)$ steps.

Prime Power Test runs in time $O(\log^4 n)$.

Total Cost

Total running time is dominated by the Binomial Power Test, and thus is bounded by

$$O((\log^{12} n)\text{poly}(\log\log n)).$$

This completes the proof of Theorem 1.

Reference

This is a presentation based on the original paper "PRIMES in P" by Agrawal, Kayal and Saxena, posted on August 6, 2002 at

http://www.cse.iitk.ac.in/news/primality.html

Revisions

revision #1, October 28, 2002, presented by Mitsunori Ogihara at the University of Rochester.

revision #2, November 28, 2002, presented by Stanisław Radziszowski at the Technical University of Gdańsk.

revision #3, December 13, 2002.