The Polynomial Time Algorithm for Testing Primality

George T. Gilbert

An algorithm is *polynomial time* if the number of “simple” steps (e.g. additions, multiplications, comparisons, …) required is bounded by polynomial in the size of the inputs.

This is equivalent to the existence of constants C and D such that the number of steps is bounded by $C\,|\mathrm{Input}|^D$.

This reflects an asymptotically fast algorithm because for any $r>0$, $b>1$, x^r / b^x goes to 0 as x goes to ∞.

When an integer n is the input, its size is the number of digits $\log_{10} n$ or the number of bits $\lg n = \log_2 n$. Because

$$\log_a n = \log_b n / \log_b a$$

the only effect of changing the base is to change the constant C.
Note that $n=2^{\lg n}$ and $\sqrt{n}= \sqrt{2}^{\lg n}$ are exponential.

Some Easy but Vital Preliminaries

We write a≡b (mod n) for a-b divisible by n. In particular,

a≡0 (mod n) if and only if a is divisible by n.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Clearly, if n is prime, then $\binom{n}{k}$ is divisible by n for k=1, 2, …, n-1.

The converse is also true. If q is a prime factor of n, then

$$\binom{n}{q} = \frac{n(n-1)...(n-q+1)}{q(q-1)...1}$$

is divisible only by n/q, but not n.

Thus, for p prime, $(x \pm a)^p \equiv x^p \pm a^p \pmod{p}$.

Fermat's Little Theorem For p prime and k relatively prime to p, $k^{p-1} \equiv 1 \pmod{p}$.

Pf. Setting $x=k$ and $a=1$, we get $(k \pm 1)^p \equiv k^p \pm 1 \pmod{p}$. Induction starting at 0 gives $k^p \equiv k \pmod{p}$ for all integers k, from which the theorem follows.

We can now conclude that the following are equivalent:

(i) n is prime

(ii) as polynomials in x, $(x+a)^n \equiv x^n + a \pmod{n}$ for some integer a relatively prime to n

(iii) as polynomials in x, $(x+a)^n \equiv x^n + a \pmod{n}$ for all integers a

The idea that Agarwal, Kayal, and Saxena, PRIMES is in P, preprint, August 2002, use is to combine coefficients whose powers of x are the same mod r, where r is on the order of $\ln^6 x$, a polynomial time computation (with D=12). Specifically, we consider whether

$$(x+a)^n \equiv x^n+a \mod(n, x^r-1) \text{ for all } a$$

If n is prime, the congruence must hold for all r and a, but the trick is to find a good r for which the above shows n is prime.

I will follow the exposition of Daniel Bernstein, Proving Primality after Agrawal-Kayal-Saxena, draft, January 2003. It incorporates a theorem of Hendrik Lenstra that avoids the deep sieving result from analytic number theory in AKS as well as a simplifying observation of Kiran Kedlaya.

How to Exponentiate

$53=2^5+2^4+2^2+2+1=(((1\cdot 2+1)2^2+1)2^2+1$

$x \rightarrow x^2 \rightarrow x^3 \rightarrow x^6 \rightarrow x^{12} \rightarrow x^{13} \rightarrow x^{26} \rightarrow x^{52} \rightarrow x^{53}$

Compute $(x+5)^{13}$ mod$(13, x^3-1)$.

$(x+5)^2=x^2+10x+25\equiv x^2-3x-1$

$(x+5)^3 \equiv(x^2-3x-1)(x+5)=x^3+2x^2-16x-5 \equiv 2x^2-16x+(1-5) \equiv 2x^2-3x-4$

$(x+5)^6 \equiv (2x^2-3x-4)^2=4x^4-12x^3-7x^2+24x+16$

$\quad\equiv -7x^2+(4+24)x+(-12+16) \equiv 6x^2+2x+4$

$(x+5)^{12} \equiv(6x^2+2x+4)^2 \equiv\ldots \equiv 1$

$(x+5)^{13} \equiv 1 \cdot(x+5) \equiv x+5$

$x^{13}+5 \equiv x^{4\cdot 3+1}+5 \equiv x+5$

On the other hand

$(x+2)^{65} \equiv 2x^6+2x^5+53x^4+49x^3+14x^2+52x+6 \mod(65,\ x^7-1)$,

not $x^{65}+2 \equiv x^2+2$, so 65 is not prime.

However, $(x+5)^{1729} \equiv x^{1729}+5 \mod(1729,\ x^3-1)$,

and even $(x+a)^{1729} \equiv x^{1729}+a \mod(1729,\ x^3-1)$ for all a,

yet $1729 = 7\cdot 13\cdot 19$.

Note that

$(x+5)^{1729} \equiv 1254x^4+799x^3+556x^2+1064x+1520 \mod(1729,$
$x^5-1)$,

not $x^{1729}+5 \equiv x^4+5$

This was obtained by the Maple command

Powmod(x+5,1729,x^5-1,x) mod 1729;

The Modified AKS Algorithm

1. Check that n is not a perfect power.

2. Find a special prime $r \leq (16+\square)\lg^5 n$ for which $\mathrm{ord}_r n$ is at least $4 \lg^2 n$, checking that n is not divisible by primes up through r.

3. Verify that $(x+a)^n \equiv x^n+a \bmod (n, x^r-1)$ for a from 1 to r.

We must construct r. Once done, if n fails to clear any step, it is clearly composite. The heart of the rest of the proof is to show that an n that gets through the algorithm must be prime.

Step 1. N is not a perfect power

For a fixed k, we can check whether n is a perfect kth power in polynomial time. One can perform (essentially) lg n iterations of either the bisection method or Newton's method on x^k-n to estimate $n^{1/k}$ to within .5 and then check whether the kth power of the nearest integer is n

Since $2^{\lg n}$=n, the largest power k to consider is lg n.

Step 2. Finding a special r

We want a prime r for which $\mathrm{ord}_r n$ is fairly large.

$\mathrm{ord}_r n \geq x$ (we'll be able to take any $x > 4 \lg^2 n$)

iff

r does not divide

$$(n-1)(n^2-1)\cdots(n^{x-1}-1) < n^{1+2+\cdots+(x-1)}$$

$$= n^{(x-1)x/2} < n^{\frac{1}{2}x^2} < 2^{\frac{1}{2}x^2 \lg n}$$

Lemma (Chebyshev). $\prod_{p \le 2m} p \ge 2^m$

Pf. One checks that this is true for m<32.

$$\binom{2m}{m} = \frac{(2m)!}{(m)!\ m!} = \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2m-1)}{2 \cdot 4 \cdot 6 \cdot \cdots \cdot 2m} 2^{2m}$$

$$= \frac{1}{\sqrt{2}} \cdot \frac{3}{\sqrt{2} \cdot \sqrt{4}} \cdot \frac{5}{\sqrt{4} \cdot \sqrt{6}} \cdot \cdots \cdot \frac{2m-1}{\sqrt{2m-2} \cdot \sqrt{2m}} \cdot \frac{1}{\sqrt{2m}} 2^{2m}$$

$$> \frac{2^{2m}}{\sqrt{4m}} = 2^{2m - \frac{1}{2}\lg(4m)}$$

Now the power of a prime p dividing m! is

$$\lfloor m/p \rfloor + \lfloor m/p^2 \rfloor + \cdots + \left\lfloor m/p^{\lfloor \log_p m \rfloor} \right\rfloor$$

Thus,

$$\lg \binom{2m}{m} = \sum_{p \le 2m} \lg p \sum_{k=1}^{\log_p 2m} \left(\lfloor 2m/p^k \rfloor - 2 \lfloor m/p^k \rfloor \right)$$

$$\le \sum_{p \le 2m} \lg p + \sum_{p \le \sqrt{2m}} \lg p \sum_{k=2}^{\log_p 2m} \left(\lfloor 2m/p^k \rfloor - 2 \lfloor m/p^k \rfloor \right)$$

$$\le \sum_{p \le 2m} \lg p + \sum_{p \le \sqrt{2m}} \lg p \left(\frac{\lg 2m}{\lg p} - 1 \right)$$

$$\le \sum_{p \le 2m} \lg p + \sum_{p \le \sqrt{2m}} \left(\lg 2m - 1 \right)$$

$$\le \sum_{p \le 2m} \lg p + \tfrac{1}{2}\sqrt{2m}\left(\lg 2m - 1 \right) \qquad \text{(for } \sqrt{2m} \ge 8, \text{ i.e. m} \ge 32)$$

The inequalities $\sqrt{2m} > \lg 4m > \lg 2$ for m ≥32 imply

$$\prod_{p \le 2m} p \geq 2^{2m - \frac{1}{2}\lg 4m - \frac{1}{2}\sqrt{2m}(\lg 2m - 1)}$$

$$> 2^{2m - \frac{1}{2}\sqrt{2m}\lg 2m} > 2^{m} \qquad \text{QED}$$

Find the least prime r that does not divide the earlier product and check that r and smaller primes don't divide n.
We conclude that, unless we have found a prime factor of n that is ≤r, we can find a prime r≤2m with $\mathrm{ord}_r n \geq x$ if $2m \geq x^2 \lg n$.
(With $x \approx 4 \lg^2 n$, we'll have $2m \sim 16 \lg^5 n$.)

Step 3. Verify that $(x+a)^n \equiv x^n + a \bmod (n, x^r-1)$ for a=1 to r

We now show that if n passes all these steps, that n is prime.
Let p be a prime factor of n. Note p>r.

Let $h(x) \in F_p[x]$ be an irreducible factor of $\dfrac{x^r - 1}{x - 1}$

of degree d. We examine the implications of Step 3 on the finite field $F = F_p[x] / \langle h(x) \rangle$, which has p^d elements. Recall that the multiplicative group F^* is cyclic of order $p^d - 1$.

Note that $f(x) \equiv g(x) \bmod (n, x^r-1)$ implies $f(x) \equiv g(x) \bmod (p, h(x))$, i.e. $f(x)=g(x)$ in F.

Lemma. $d=\mathrm{ord}_r\, p$

Proof. Since $x^r=1$ in F, $x\neq 1$ in F, and r is prime, the order of x is r.

By Lagrange's theorem r divides p^d-1. Thus $\mathrm{ord}_r\, p$ divides d.

To show d divides $\mathrm{ord}_r\, p$, let g(x) generate F^*. We have
$g(x)^p = g(x^p)$ and, iterating

$$g(x)^{p^{\mathrm{ord}_r p}} = g(x^{p^{\mathrm{ord}_r p}}) = g(x)$$

Thus, the order of g(x), p^d-1, divides $p^{\mathrm{ord}_r p} - 1$
hence d divides $\mathrm{ord}_r\, p$.

Remark. Every choice of h(x) has the same degree.

We have $(x+a)^n \equiv x^n+a \mod(n, x^r-1)$,
hence $(x+a)^n \equiv x^n+a \mod(p, x^r-1)$, for a=0 to r.
We also have $(x+a)^p \equiv x^p+a \mod(p, x^r-1)$ for a= 0 to r.

The idea is that these two sets of congruences impose too much structure, allowing us to find u, v for which $g^u=g^v$ has too many solutions in F. Such an equation has at most $|u-v|$ nonzero solutions unless u=v.

Let $w=|F_r^*/\langle n,p\rangle|$. Let K denote a set of w coset representatives, denoting a typical representative by k. Observe that

$$w = \frac{r-1}{|\langle n, p \rangle|} \,\Bigg|\, \frac{r-1}{\mathrm{ord}_r n} \;\square\; \frac{r-1}{x}$$

Now consider $$\left\{ n^i p^j : i, j \in \left[0, \left\lfloor \sqrt{\frac{r-1}{w}} \right\rfloor \right] \right\}$$

The order of this set is $$\left(1 + \left\lfloor \sqrt{\frac{r-1}{w}} \right\rfloor \right)^2 > \frac{r-1}{w}$$

Thus $n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \mod r$ for some $(i_1, j_1) \neq (i_2, j_2)$

The equation $$g^{n^{i_1} p^{j_1}} = g^{n^{i_2} p^{j_2}} \qquad \text{(EQ)}$$

has at most $\left| n^{i_1} p^{j_1} - n^{i_2} p^{j_2} \right| \le n^{2\sqrt{\frac{r-1}{w}}} = 2^{2\sqrt{\frac{r-1}{w}} \lg n}$

nonzero solutions in F unless $n^{i_1} p^{j_1} = n^{i_2} p^{j_2}$.

Beginning with $(x+a)^n \equiv x^n+a \bmod (p, x^r-1)$, we have

$$\left(x^{n^i}+a\right)^n \equiv x^{n^{i+1}}+a \mod(n, x^{n^i r}-1)$$

$$\Rightarrow \left(x^{n^i}+a\right)^n \equiv x^{n^{i+1}}+a \mod(p, x^r-1)$$

$$\Rightarrow (x+a)^{n^i} \equiv x^{n^i}+a \mod(p, x^r-1) \quad \text{by induction}$$

Next, we see that

$$(x+a)^{n^i p^j} \equiv x^{n^i p^j}+a \mod(p, x^r-1) \quad \text{by induction}$$

and finally that

$$\left(x^k+a\right)^{n^i p^j} \equiv x^{kn^i p^j}+a \mod(p, x^{kr}-1)$$

$$\Rightarrow \left(x^k+a\right)^{n^i p^j} \equiv x^{kn^i p^j}+a \mod(p, x^r-1)$$

Any element of the subgroup G of F^* generated by x^k+a, k in K, $0 \le a \le r$ is a solution of (EQ).

AKS restricted to k=1 and showed the order of G is too big if n is not prime.

Lenstra's idea was to introduce the set K and to consider G^w instead of G. The argument is more complicated, but is self-contained instead of depending on a VERY hard theorem.

We will let $s:\{0,1,\ldots,r\}\to\mathbb{N}:\{0,1,\ldots\}$ describe the exponents for an element of G^w of the following form:

$$g(s) = \left(\prod_{0 \le a \le r} \left(x^k + a\right)^{s(a)} \right)_{k \in K}$$

$$= \left(\prod_{0 \le a \le r} \left(x^{k_1} + a\right)^{s(a)}, \ldots, \prod_{0 \le a \le r} \left(x^{k_w} + a\right)^{s(a)} \right) \in G^w$$

Claim: If $s_1 \neq s_2$ with $\sum s_1(a) \leq r-2$ and $\sum s_2(a) \leq r-2$, then $g(s_1) \neq g(s_2)$.

Proof of claim. Suppose $g(s_1) = g(s_2)$.

$$\left(\prod_{0 \leq a \leq r} \left(x^{kn^i p^j} + a \right)^{s_1(a)} \right)_{k \in K} = \left(\prod_{0 \leq a \leq r} \left(x^k + a \right)^{n^i p^j s_1(a)} \right)_{k \in K}$$

$$= g(s_1)^{n^i p^j} = g(s_2)^{n^i p^j} = \left(\prod_{0 \leq a \leq r} \left(x^{kn^i p^j} + a \right)^{s_2(a)} \right)_{k \in K}$$

Now, $kn^i p^j$ runs over a complete set of representatives for F_r^*
Therefore, the degree at most r-2 polynomial over F,

$$\prod_{0 \leq a \leq r} (X+a)^{s_1(a)} - \prod_{0 \leq a \leq r} (X+a)^{s_2(a)},$$

has roots $x, x^2, \ldots, x^{r-1}$, so is identically 0, i.e. $s_1 = s_2$.

The number of such s is the number of r+1-tuples of nonnegative integers whose sum is at most r-2. This equals the number of r+2-tuples of nonnegative integers whose sum equals r-2. This, in turn, is the number of arrangements of r+2 identical balls in r-2 boxes. Therefore,

$$|G|^{w} \geq \binom{2r-1}{r+1} > 2^{r-1}$$

for r≥3 by induction.

However, $2^{2\sqrt{\frac{r-1}{w}}\lg n} \geq 2^{\frac{r-1}{w}}$ iff $4 \lg^{2} n \geq \frac{r-1}{w} \geq x > 4 \lg^{2} n$

Finally, $n^{i_1} p^{j_1} = n^{i_2} p^{j_2}$,

so n is a power of p, which by Step 1 means n=p.