AKS Algorithm

Peter Kagey

Friday, September 27, 2019

The idea for this document is to write a high level overview of the AKS algorithm, which provides a convincing *heuristic* for why PRIME is in P in the number of bits of n.

1 Primes and binomial coefficients

The idea uses the fact that when $n \geq 2$ and $\gcd(a, n) = 1$, then n is prime if and only if

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

since all binomial coefficients are divisible by n if and only if n is prime. However $(x + a)^n$ has a linear number of terms, so it takes exponential time (with respect to $\log(n)$) to compute this power.

An improvement is to instead calculate these polynomials over $\mathbb{Z}[x]/(x^r - 1)$ for some r which is polynomial in $\log(n)$, because this computation is quick in general.

1.1 Power of a binomial over a quotient ring.

For example, if we want to compute

$$(x + 6)^{13} \pmod{x^3 - 1, 13}$$

we instead compute

$$\begin{aligned}
(x + 6) &\equiv (x + 6) \pmod{x^3 - 1, 13} \\
(x + 6)^2 &\equiv x^2 + 12x + 10 \pmod{x^3 - 1, 13} \\
(x + 6)^4 &\equiv (x^2 + 12x + 10)^2 \equiv 8x^2 + 7x + 7 \pmod{x^3 - 1, 13} \\
(x + 6)^8 &\equiv (8x^2 + 7x + 7)^2 \equiv 5x^2 + 6x + 5 \pmod{x^3 - 1, 13}
\end{aligned}$$

Since $13 = 1 + 4 + 8$, we can write

$$\begin{aligned}
(x + 6)^5 &\equiv (x + 6)(8x^2 + 7x + 7) \equiv 3x^2 + 10x + 11 \pmod{x^3 - 1, 13} \\
(x + 6)^{13} &\equiv (5x^2 + 6x + 5)(3x^2 + 10x + 11) \equiv x + 6 \equiv x^{13} + 6 \pmod{x^3 - 1, 13},
\end{aligned}$$

as expected. And the number of steps this requires is polynomial in r, which is itself polynomial in $\log(n)$. Simple enough. But testing just one value of a and r can result in false positives. In order to get rid of false positives, it's necessary to choose a list of $\{a_1, a_2, \ldots, a_m\}$. Moreover, if this algorithm is to be polynomial time, where m must be polynomial with respect to $\log(n)$.

1.2 Choosing r.

Let given some r and a, with $\gcd(a, r) = 1$, define

$$o_r(n) = \min \left\{ k \in \mathbb{N} : n^k \equiv 1 \pmod{r} \right\},$$

the order of a modulo r.
By Lemma 4.3, for large n we can find an $r \leq \log^5(n)$ (that is, polynomial in $\log(n)$) such that $o_r(n) > \log^2 n$.

1.3 Two things to check.

Now, for $n > 5690034$, we just need to

(i) trial divide a set of primes that is polynomial in $\log(n)$, namely check that $a \nmid n$ for all $1 < a \leq r$, and

(ii) check that $(x+a)^n \equiv x^n + a \pmod{x^r - 1, n}$ for all $a \leq \lfloor \log(n)\sqrt{\phi(r)} \rfloor$.

Of course, if (i) fails, then n has a nontrivial divisor, so n is composite. If (i) fails then n is composite by the properties of binomial coefficients discussed above. If (ii) succeeds, it is less obvious that n is prime.