CS681	Computational Number Theory

Lecture 25 : The AKS Primality Test

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

We shall do the AKS primality test this class.

1 The Deterministic Primality Test

The algorithm is going to be the following:

1. Find two numbers r and l based on some requirements
2. Check if n is a perfect power. If it is, output COMPOSITE.
3. Check if any of the numbers less than l have a non-trivial gcd with n. If they do, output COMPOSITE.
4. For all $1 \leq a \leq l$, check if the following identity holds

   $$(X + a)^n = X^n + a \pmod{n, X^r - 1}$$

   Use repeated squaring to evaluate the LHS and RHS and check.

   If any of the test failed, output COMPOSITE.
5. If all the above tests succeeded, output PRIME

We shall figure out what the requirement of r,l as we go along. That would give a better picture of why we want those properties.

The algorithm will be in a way that if n was indeed a prime then the algorithm would answer correctly. We only need to make sure that the algorithm doesn't make a mistake on composite n. We shall ensure that if a composite n passes all the tests, then n has to be a power of a prime. And since we saw that testing of a number was a perfect power is easy, that is one of our preprocessing steps and hence such n will be eliminated. We shall now choose parameters in a way that no composite n can pass all the test.

Let us assume that n is composite, has p as a proper divisor and is not a power of p. And let us assume that n passes all the tests. Note that p has to

be larger than l since we have already made sure that n does not have any small factor in step 3.

The test is basically checking the identity $(X+a)^n = X^n+a \pmod{n, X^r-1}$, which is just checking if two terms in the ring $R = \mathbb{Z}[X]/(n, X^r - 1) = \frac{\mathbb{Z}/n\mathbb{Z}[X]}{(}X^r - 1)$. Rings are a little hard to handle; would be easier to go to a field.

1.1 Moving to a Field

Instead of looking at $R = \frac{\mathbb{Z}/n\mathbb{Z}[X]}{(X^r-1)}$, we shall look at the field $\mathbb{F}_p[X]/(h(X))$ where $h(X)$ the minimal polynomial of the primitive r-th root of unity. Note that this just starting with R, going modulo the ideal generated by p, then going modulo the ideal generated by $h(X)$. The ideal generated by p is a prime ideal in R and therefore $R/(p)$ became an integral domain. Then $h(X)$ generates a maximal ideal being irreducible, and therefore we get the field $\mathbb{F} = \mathbb{F}_p[X]/(h(X))$.

The important thing to note here is that, if equations were satisfied in R, they have to be satisfied in $\mathbb{F}$ as well as we are just going modulo some ideals. This is like saying, if $a = b$ in Z, then of course they are equal $\mathrm{mod} p$ as well. Thus let us work with this field. Now the next thing to note that in $\mathbb{F}_p[X]/(h(X))$, it is just $\mathbb{F}_p(\zeta)$ and X plays the role of ζ. Thus, if some n survived all the tests, then for each $1 \leq a \leq l$

$$(X + a)^n = X^n + a \bmod p, h(X)$$

Let us characterize this property of n by the following definition.

Definition 1. *A number m is called introspective for a polynomial f if*

$$f(X)^m = f(X^m) \quad \textit{in } \mathbb{F}$$

As the name suggests, it says that m is curious with respect to X; such powering can be pulled inside the brackets. The tests basically mean that n is introspective for $f(X) = (X + a)$. The following two observations are trivial.

Observation 1. *If m_1 and m_2 are introspective for f, then so is $m_1 m_2$.*

Observation 2. *If m is introspective for f and g, then m is introspective for fg.*

Since n passed the tests, we know that n is introspective for $(X + a)$ for all $1 \leq a \leq l$. And also note that, by the binomial theorem in $\mathbb{F}_p[X]$,

$$(X + a)^p = X^p + a$$

for any a. Therefore, p is introspective for $(X + a)$ as well. Therefore, by the two observations, and $n^i p^j$ is introspective for $\prod_{1 \leq a_i \leq l}(X + a_i)$. Let us create two groups to capture this property.

1.2 The two groups

Let G be the group generated by n and p modulo r. Or in other words, G is the set of numbers of the form $n^i p^j$ modulo r.

Similarly, let $\mathcal{G}$ be the group generated by $\{(X + a) \ : \ 1 \leq a \leq l\}$ in $\mathbb{F}$. And by the two observations, any element of G is introspective to any element of $\mathcal{G}$.

$$\begin{aligned} G &= \langle n, p \rangle \subseteq (\mathbb{Z}/r\mathbb{Z})^\star \\ \mathcal{G} &= \langle \{(X + a) \ : \ 1 \leq a \leq l\} \rangle \subseteq \mathbb{F} \end{aligned}$$

Let $|G| = t$. Since G is a subgroup of $(\mathbb{Z}/r\mathbb{Z})^\star$, $t \leq r$. Now note that the group generated by n is a subgroup of G and its cardinality is $ord_r(n)$. Therefore $t > ord_r(n)$.

We shall now get two bounds on the size of $\mathcal{G}$.

1.3 An Upper Bound on $|\mathcal{G}|$

Not that every element of $\mathcal{G}$ is actually a product of $(\zeta + a)$'s since X is ζ in $\mathbb{F}$. In order to get a bound on the size of $\mathcal{G}$ let us restrict ourselves to just products of distinct $(\zeta + a)$'s. Set $l = t - 1$.

For every subset K of $1, 2, \cdots l$, we can construct a polynomial $f_K(X) = \prod_{i \in K}(X + i)$. And there are 2^t such polynomials. These polynomials are clearly distinct as each of them has a different set of roots. But what happens if we substitute ζ in them? Is it possible that for $K \neq K'$, $f_K(\zeta) = f_{K'}(\zeta)$?

Suppose they were equal, then note that $f_K(\zeta)^m = f_{K'}(\zeta)^m$ for any m, and in particular any $m \in G$. If m is in G, then $f_K(\zeta^m) = f_K(\zeta)^m = f_{K'}(\zeta)^m = f_{K'}(\zeta^m)$. Thus, if $g(X) = f_K(X) - f_{K'}(X)$, then ζ^m is a root of g for every $m \in G$. But since $|G| = t$, this means that $g(X)$ has t roots. But $g(X)$ is a polynomial of degree at most l which is less than t. Such a polynomial cannot have t roots unless it is the zero polynomial. Thus,

$f_K(\zeta)$s are distinct. Since there are 2^{t-1} possible $f_K(X)$s possible, each of this would give a distinct $f_K(\zeta)$ in $\mathcal{G}$. Therefore,

$$|\mathcal{G}| \geq 2^{t-1}$$

1.4 A Lower Bound for $|\mathcal{G}|$

Look at the set $S = \left\{n^i p^j \ : \ 0 \leq i, j \leq \sqrt{t}\right\}$. And if n wasn't a power of p, this set S has $(1+\sqrt{t})^2 > t$ elements. Now, considering them modulo r, they are a subset of $|G|$ and by pigeon hole principle, there must be some $m_1 \neq m_2 \in S$ such that $m_1 = m_2 \bmod r$ and therefore $m_1 = m_2 + kr$. Then, if $f(\zeta) \in \mathcal{G}$

$$f(\zeta)^{m_2} = f(\zeta)^{m_1+kr} = f(\zeta^{m_1+kr}) = f(\zeta^{m_1}) = f(\zeta)^{m_1}$$

Thus, if we were to consider $g(X) = X^{m_1} - X^{m_2}$, then every $f(\zeta) \in \mathcal{G}$ is a root of $g(X)$. Note that degree of $g(X)$ is at most the max of m_1, m_2. And $m_1 = n^i p^j \leq n^{\sqrt{t}} n^{\sqrt{t}} = n^{2\sqrt{t}}$. And since the degree of g is is at most $n^{2\sqrt{t}}$, the number of roots can also be only that much. Therefore

$$|\mathcal{G}| \leq n^{2\sqrt{t}}$$

1.5 Conflicting Bounds

Combining the two bounds, we have

$$2^{t-1} \leq |\mathcal{G}| \leq n^{2\sqrt{t}}$$

Now if we can ensure that the lower bound is larger than the upper bound, we would get the contradiction we are looking for; that would rule out the possiblity that a composite number passed all the tests.

Thus we want $2^{t-1} > n^{2\sqrt{t}}$. Taking logs, $t - 1 > 2\sqrt{t} \lg n$. And if $t > 4 \log^2 n$, that should be to make the bounds for $|\mathcal{G}|$ contradict.

Thus all we need to do now is find an r so that $ord_r(n) > 4 \log^2 n$.

1.6 Getting an r such that $ord_r(n) > 4 \log^2 n$

What we shall do to get an r is just try $1, 2, \cdots$ until it is satisfied. But how long would we have to go until we hit a good r?

Look at the following number

$$B = \prod_{i=1}^{4\log^2 n} (n^i - 1) < n^{\log^4 n}$$

If r was a prime number not dividing this B, then the order of n modulo r cannot be less than $4\log^2 n$. The number of prime factors of B is at most $\log^4 n \log n = \log^5 n$. And therefore, the $\log^5 n+1$-th prime would definitely not divide B. Therefore, we can just enumerate all primes starting from 2 and get the $\log^5 n + 1$-th prime. And this search is assured to be within $\log^6 n$ by the prime number theorem. Therefore, we are in good shape.

2 The Final Algorithm

Thus, putting all the pieces together.

Algorithm 1 AKS PRIMALITY TEST

1: Check if the input number n is a perfect power of some number. If so, **return** COMPOSITE.
2: Find the least prime r such that $ord_r(n) > 4\log^2 n$. Let $l = ord_r(n) - 1$. In the process, check if any of those r's have a non-trivial factor with n. If yes, **return** COMPOSITE.
3: **for** $1 \leq a \leq l$ **do**
4: **if** $(X + a)^n \neq X^n + a \bmod (n, X^r - 1)$ **then**
5: **return** COMPOSITE.
6: **end if**
7: **end for**
8: **return** PRIME.

The total time complexity is about $O(\log^{12} n)$. The current best is about $O(\log^6 n)$.