6.S897 Algebra and Computation Mar 18, 2015

Lecture 13

Lecturer: Madhu Sudan *Scribe: Daniel Grier*

1 Overview - Deterministic Primality Testing

Last time we saw the major components of the AKS deterministic test for primality. Today we will finish the analysis. We first present the approach given in the original paper which relies on a rather strong number theoretic statement. We then give a more sophisticated analysis which will allow us to use a weaker number theoretic statement, which follows straightforwardly from the prime number theorem. In fact, we will even show an elementary proof of the prime number theorem, allowing us to prove that primality testing is achievable in polynomial time without any number-theoretic assumptions.

2 Review of AKS Algorithm

Let N be the number that we are testing for primality. Let $A = \{1, 2, \ldots, \mathsf{polylog}(N)\}$. Choose prime $r = O(\mathsf{polylog} N)$. The method by which we choose our prime r will depend on our number-theoretic assumption. Assume for now that it is given. The test for primality is as follows:

- Verify that N has no divisors in A.
- Verify that N is not a prime power. This can be accomplished in $\mathsf{polylog}$ time by checking that for each $t \in \{2, 3, \ldots, \log N\}$ that $N \neq m^t$ by binary searching on the value of m.
- For all $a \in A$ verify

$$x^N + a \equiv (x + a)^N \pmod{N, x^r - 1}$$

- If all tests pass, then output that N is prime.

3 Analysis

It is clear that the test passes if N is a prime. Assume, by contradiction, that N passes the test but is composite. In particular, let p be some prime divisor of N. Although the algorithm is really working in the ring $R := \mathbb{Z}[x]/(N, x^r - 1)$, it will be convenient in the analysis to work with the rings $L := \mathbb{Z}[x]/(p, x^r - 1)$ and $K := \mathbb{Z}[x]/(p, h(x))$ where $h(x)$ is an irreducible factor of the polynomial

$\frac{x^r-1}{x-1} \in \mathbb{Z}_p[x]$. Notice that identities in R, imply identities in L and K, and that identities in L imply identities in K. The magic of the proof is finding nice properties of certain polynomials in L, which will therefore hold in K; however, the fact that K is actually a field, will allow us to draw a contradiction.

Definition 1 *A polynomial $f \in \mathbb{Z}[x]$ is* introverted *with respect to m if*

$$f(x^m) \equiv f(x)^m \pmod{p, x^r - 1}$$

Because we assumed N passed the test, we have that the polynomial $x + a$ is introverted with respect to N and p for all $a \in A$. Furthermore, by the properties of introversion that we saw last time, we have that all polynomials in the family

$$\mathcal{F} := \left\{ \prod_{a \in A} (x + a)^{d_a} \mid d_a \geq 0 \right\}$$

are introverted with respect to any element of $\{N^i p^j \mid i, j \geq 0\}$.

Lemma 2 *If f is introverted with respect to distinct m_1, m_2 but $m_1 \equiv m_2 \pmod{r}$, then $f(x)$ is a root of $z^{m_1} - z^{m_2} \in K[z]$.*

Proof

$$f(x)^{m_1} \equiv f(x^{m_1}) \equiv f(x^{m_2}) \equiv f(m)^{m_2}$$

where the first and last equalities use introversion, and the second equality leverages the fact that we are working mod $x^r - 1$ in K. ■

The reason that we want to work in the field K now becomes clear. Because K is a field, the polynomial $z^{m_1} - z^{m_2}$ has at most $\max(m_1, m_2)$ roots. If we can find m_1 and m_2 that are relatively small compared to the number of polynomials that are roots of $z^{m_1} - z^{m_2}$, we will have arrived at a contradiction.

If we choose m_1 and m_2 from the set $\{N^i p^j \mid i, j \geq 0\}$, then $\mathcal{F}$ is a natural large class of functions where we can look for a contradiction. This is exactly what we will do.

Lemma 3 *$\exists$ distinct $m_1, m_2 \in \{N^i p^j \mid i, j \geq 0\}$ such that $m_1 \equiv m_2 \pmod{r}$ and $\max(m_1, m_2) \leq N^{2\sqrt{r}}$.*

Proof First notice that all elements of $\{N^i p^j \mid i, j \geq 0\}$ are distinct because N is composite and not a prime power. Therefore, there if we consider i and j in the range from 0 to $\sqrt{r}$, we have $(\lfloor \sqrt{r} \rfloor + 1)^2 > r$ distinct numbers of the form $N^i p^j$ which are less than $N^{2\sqrt{r}}$. By the pigeonhole principle we must have two settings of i and j such that $N^i p^j$ are equivalent mod r. ■

There are two things one might now worry about. First, for $a, b \in A$ perhaps $x + a$ is equivalent to $x + b$ in K so that these two polynomials are actually identical (i.e. ruining our argument that the polynomial has too many roots). This would imply however that either $a \geq p$ or $b \geq p$, which shows that p is an element of A. Recall now that we explicitly checked for this condition in the test, so this is impossible.

Secondly, one might worry that many different elements in $\mathcal{F}$ would be equivalent mod $h(x)$. This is where we will invoke the strong number theoretic statement that we can in fact find an $h(x)$ such that $\deg h(x) \geq r^{1/2}\mathsf{polylog}(N)$. If

we only consider polynomials in $\mathcal{F}$ of degree less than the degree of $h(x)$, then they will all be distinct in K. This motivates the following definition.

Let $\mathcal{F}_t := \{f \in \mathcal{F} \mid \deg(f) \leq t\}$. A simple counting argument shows that $|\mathcal{F}_t| = \binom{t+|A|}{t}$. If we let $|A| = t = \deg h - 1$, we get that $|\mathcal{F}_t| \geq 2^{r^{1/2}\mathsf{polylog}N} \gg N^{2\sqrt{r}}$, which completes the argument that primality testing can be done in polynomial time.

4 Analysis that Relies on Less Number Theory

We now give up the assumption that we can find an $h(x)$ with large degree. We instead rely on a relatively weak number-weak theoretic fact that we can find a prime r with large order. First define $\mathrm{ord}_r(N) := |\{N \mod r, N^2 \mod r, \ldots, N^r \mod r\}|$.

Claim 4 *There exists prime r such that* $\mathrm{ord}_r(N) \geq \mathsf{polylog}N$.

Let $l := |\{N^i p^j \pmod r \mid i, j \geq 0\}|$. It is clear that $\mathrm{ord}_r(N) \leq l \leq r$. Using the same pigeonhole argument of Lemma 2, we can show that there exist distinct $m_1, m_2 \leq N^{2\sqrt{l}}$ such that $m_1 \equiv m_2 \pmod r$. Notice then that if we let $|A| = l$ we get

$$|\mathcal{F}_{l-1}| \geq 2^l \gg N^{2\sqrt{l}}$$

if $l > \log^2 N$, which we get from our number-theoretic assumption. If we can show that all polynomials in $\mathcal{F}_{l-1}$ are distinct when viewed in the field K, then we would be done. This is what we will show.

Lemma 5 *If $f, g \in \mathcal{F}_{l-1}$, then $f \neq g \pmod{h(x)}$.*

Proof First view f, g as polynomials in $\mathbb{Z}_p[z]$. Since $\mathbb{Z}_p$ is a subfield of K, we can consider $f(z) - g(z)$ as a polynomial in $K[z]$. Assume now that $f \equiv g \pmod{h(x)}$, which implies that $h(x)|f(x)-g(x)$, so x is a root of the polynomial $f(z) - g(z)$.

We now give l possible roots of $f(z) - g(z)$ of the form x^m. This follows from the fact that for every $m \in \{N^i p^j \pmod r\}$ we have

$$\begin{aligned} f(x^m) - g(x^m) &\equiv f(x)^m - g(x)^m \\ &= (f(x) - g(x))(f(x)^{m-1} + f(x)^{m-2}g(x) + \ldots + g(x)^{m-1}) \\ &\equiv 0 \pmod{h(x)} \end{aligned}$$

Since the degree of $f(z) - g(z)$ is less than l we must have that $x^a \equiv x^b \pmod{p, h(x)}$ for $a < b$, so $h(x)|x^a(x^{b-a} - 1)$. Recall that $h(x)|x^r - 1$ and is irreducible, so there must be some $i < r$ such that $h(x)|x^i - 1$. This implies that $h(x)|x^{\gcd(i,r)} - 1$. We know r is prime, so $h(x)|x - 1$; however, we explicitly forbid $h(x)$ dividing $x - 1$ in our choice of $h(x)$ leading to the contradiction. ■

We now show that the number theoretic fact follows easily from a weak form of the prime number theorem. Let $\#(m)$ be defined as the number of distinct primes less than m.

Theorem 6 (Prime Number Theorem)

$$\#m \geq c\frac{m}{\log m}$$

for some constant c.

Proof Consider the integral $\int_0^1 x^m(1-x)^m \mathrm{d}x$. If we just expand out $x^m(1-x)^m$ and use the power rule, then we get that this integral is equal to some positive integer z divided by the $\mathrm{lcm}(m+1, m+2, \ldots, 2m+1) = \mathrm{lcm}(1, 2, \ldots, 2m+1)$. Also, in the interval [0,1], we have that $x(1-x) \leq 1/4$. Stringing this together we have

$$\frac{z}{\mathrm{lcm}(1, 2, \ldots, 2m+1)} = \int_0^1 x^m(1-x)^m \mathrm{d}x \leq \frac{1}{4^m}$$

Noticing that $\mathrm{lcm}(1, 2, \ldots m) \leq m^{\#(m)}$ we get

$$z4^m \leq \mathrm{lcm}(1, 2, \ldots, 2m+1) \leq (2m+1)^{\#(2m+1)}$$

Changing variables we get

$$\#m \geq \log_m z2^{m-1} = \frac{\log(z2^{m-1})}{\log m} \geq \frac{m-1}{\log m} \geq c\frac{m}{\log m}$$

for some appropriately chosen c. ■

Using the prime number theorem, we can now derive our weak number theoretic claim.

Claim 7 *There exists prime r such that* $\mathrm{ord}_r(N) \geq \mathsf{polylog}N$.

Proof Suppose that for all prime $r \leq \mathsf{polylog}N$, we have that $\mathrm{ord}_r(N) \leq k$. For each r there is some i in the range 1 to k such that $r|N^i - 1$. For every prime $r \leq \mathsf{polylog}N$ we have

$$r \left| \prod_{i=1}^{k} (N^i - 1) \right.$$

but that $\prod_{i=1}^{k}(N^i - 1)$ is at most N^{k^2}. Assuming that $k \leq \mathsf{polylog}N$ and using the prime number theorem, we know there exists an $m \leq k^2 \log^2 N \leq \mathsf{polylog}N$ such that $\#(m) > k^2 \log N$. If all primes of size at most m divide N^{k^2}, then so must their products. However, the product of all the primes is at least $2^{\#(m)}$, which is greater than N^{k^2} by construction. ■

Relating this back to the original AKS algorithm, we can now find r deterministically by simply brute forcing all possible primes less than some $\mathsf{polylog}N$.