CS681	Computational Number Theory

Lecture 22 : Towards the AKS Primality Test

Instructor: Piyush P Kurur *Scribe: Ramprasad Saptharishi*

Overview

Our next goal is to do the deterministic polynomial time primality test that was found by Manindra Agrawal, Neeraj Kayal and Nitin Saxena in 2002. It was a remarkable achievement and it also gave an example of how certain problems that are open for a long time can have such beautiful, elegant solutions.

1 Derandomization Approaches and the Riemann Hypothesis

We had very good randomized algorithms like the Solovay-Strassen test which we discussed last time, or the Rabin-Miller test.[1] But people wanted a deterministic algorithm for primality testing that runs in polynomial time.

However, it was known that under some strong assumptions, the above algorithms can be derandomized and made into a deterministic algorithm. If the *Extended Riemann Hypothesis* (ERH) is true, then we can completely remove randomness from the Solovay-Strassen test (or the Miller-Rabin test) and make it a deterministic polynomial time algorithm.

This conjecture is widely believe to be true and has been a very important long-standing open problem for a long time. Infact, Clay Mathematical Institute has a prize of a million dollars for anyone who solves it. Of course, if someone proves the riemann hypothesis, we already have a deterministic primality test. But trying to prove the ERH for a primality test is like trying to uproot a whole tree to get a fruit on top of it; completely avoiding the tree and instead using some stick would be better.

Let us have a small discussion on what the ERH, or the Riemann Hypothesis is.

[1] another randomized algorithm for primality testing. We will see this as an assignment.

1.1 The Zeta Function

Riemann introduced a function called the *Riemann Zeta Function.* The Riemann Hypothesis is to do with the roots of this function. Some of you might have seen the equalities like

$$\begin{aligned} 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} \cdots &= \frac{\pi^2}{6} \\ 1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} \cdots &= \frac{\pi^4}{90} \end{aligned}$$

One question is what happens when we vary the exponent of the summation. What can we say about

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Note that there are diverging series like $\zeta(s)$ since

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \approx \log n$$

and therefore if n goes to infinity, the sum goes to infinity as well; the infinite some diverges. Infact, the series $\zeta(s)$ converges for all real s if and only if $|s| > 1$.

Now why not s when it is complex? Why do we restrict ourselves to just real exponents? Then we can define $\zeta(s)$ to be the function when s is any complex number. There again, the infinite sum issues props up. It can be shown that $\sum \frac{1}{n^s}$ converges for all s such that the real part of s, denoted by $\Re(s)$ is greater than 1.

And hence $\zeta(s)$ is well defined for all numbers s such that $\Re(s) > 1$. A pictorial way to look at it is if you consider the complex plane, it is well-defined for all point to the right of the line $x = 1$.

Suppose we consider functions over real values, we have this notion of continuity. A function being continuous at a point x_0 essentially means that irrespective of whether we approach x_0 from the left (also denoted by left hand limit) or the right (right hand limit), the value should coincide with the functional value at x_0. This is sometimes also written as

$$\lim_{x \to x_0^-} f(x) = \lim_{x \to x_0^+} f(x) = f(x_0)$$

In the case of complex functions, we have a function over a plane. So it is not just a line and hence just left or right approaches. In the complex case, it is said to be continuous if no matter what part you take to approach x_0, the limits should match $f(x_0)$.

Similarly for derivatives in the real case, we want the derivative on the left hand side to match the derivative on the right hand side. In the complex case, the derivative must be the same on all directions.

A complex function that satisfies these conditions is called an *analytic function.* We say function is analytic over a region D if the above properties hold for every point in D.

Analytic functions have very strong properties like not just the first derivative but all higher order derivatives exist, a whole bunch of properties. It imposes a lot of restriction on the function.

Riemann showed that the zeta function is analytic in the region $\Re(s) > 1$.

Suppose we have a function f that we define over a small domain D over the compex plane. And over this domain, suppose the function f is analytic. We haven't defined the function outside this domain at all. A process known as *analytic continuation* can be used to extend the domain of this function.

Formally speaking, g (whose domain is D_g) is an analytic continuation of f (whose domain is D_f) if the following properties hold:

- g is analytic over D_g.
- $D_f \subseteq D_g$.
- For all $z \in D_f$, $f(z) = g(z)$.

In simple words, g extends f to a larger domain keeping in mind that if f was already defined at a point z, then g shouldn't change that value; g should coincide with f wherever it is defined already.

There is a remarkable results that if g_1 and g_2 both analytically extend f independently, then essentially $g_1 = g_2$. Therefore, the analytic continuation of a function f is uniquely determined; we can hence talk of *the* analytic continuation of f.

The zeta function is actually the analytic continuation of the function

$\sum \frac{1}{n^s}$. It is however written as just

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

The analytic continuation now extends the domain to the entire complex plane except the point $z = 1$. Thus our $\zeta(s)$ is a function defined over the entire complex plane except 1; there is a simple pole at the point $z = 1$.

1.2 Why is this important?

Now what is the importance of this function? What does it give us? The answer is that it essentially captures the factorization of integers in it.

Every n can be factorized as a product of primes $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and hence

$$\frac{1}{n^s} = \frac{1}{(p_1^{\alpha_1})^s (p_2^{\alpha_2})^s \cdots (p_k^{\alpha_k})^s}$$

And therefore, every term in the zeta function can be written as such a term on the RHS. And therefore,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \text{Primes}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_{p \in \text{Primes}} \left(\frac{1}{1 - \frac{1}{p^s}}\right)$$

This is not a rigerous proof; mathematicians will stand on their head and complain that such infinite sum/product manipulation is an unforgivable sin. However, the final equality is true; can be made rigerous.

This relation between the zeta function and the prime product is one of the many things that make it important.

1.3 The Riemann Hypothesis

The analytically continued function has a lot of roots in $\mathbb{C}$. Infact, it has a root at every negative integer. These are considered as trivial roots since they provide us with no consequence. It has been shown that all the non-trivial zeroes lie in the critical strip of $\{s \,:\, 0 < \Re(s) < 1\}$, the strip between the y-axis and the line $x = 1$.

The *Riemann Hypothesis* is the conjecture that all the non-trivial zeroes of the zeta function lie on the line $x = \frac{1}{2}$. That is, any non-trivial root s must

satisfy $\Re(s) = \frac{1}{2}$.

As of now, all the roots that have been discovered lie on this line. But we do not have a way of proving, or disproving, that all the non-trivial roots lie on this line.

1.4 The Extended Riemann Hypothesis

This is a slight generalization of the zeta function. A character χ is a periodic[2] function is multiplicative. That is, $\chi(mn) = \chi(m)\chi(n)$.

For example, $\chi = \left(\frac{a}{n}\right)$ for a fixed a is a character.

The generalized zeta function is the analytic continuation of

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

Clearly, when $\chi(n) = 1$ for all n, this is just the zeta function.

The Extended Riemann Hypothesis is the conjecture that for any character χ, all the non-trivial zeroes of the L function lie on the line $\Re(s) = \frac{1}{2}$.

1.5 Derandomizing using ERH

One of the major consequences of ERH, that is used in a lot of places is that, for any prime p, the first quadratic non-residue is less than $O(\log^2 p)$.

So, in essence, the witness for the Solovay-Strassen test can be found without going too far. One just need to go till up to polylog(n) to get a witness. This thus derandomizes the Solovay-Strassen test.

As remarked earlier, the RH or the ERH is a really strong conjecture. One doesn't need to go as far as the ERH to get a primality test. Agrawal-Kayal-Saxena show that primality can be solved in deterministic polynomial time without using any high-end mathematical machinery. The give a very elegant and simple algorithm.

2 The AKS Primality Test: The Idea

All primality tests have the same form:

[2] there exists a number k such that $\chi(n + k) = \chi(n)$ for all n

1. Find a property such that it is satisfied only by primes.

2. Try to verify that property

In the Solovay-Strassen test, it was the properties of the Legendre symbol that we checked. The following proposition is the property used in the AKS test.

Proposition 1. *The equation "$(X + a)^n = X^n + a \pmod n$" is true for all a if and only if n is prime.*

Proof. When n is a prime, then the above equation is just the binomial theorem for prime numbers. Therefore the equation is indeed true for all a when n is a prime.

Suppose n is not a prime, then we must show that the two polynomials $(X + a)^n$ and $X^n + a$ are not the same. Suppose $n = pq$ where p is a prime and $q \neq 1$, then look at the following binomial term:

$$\binom{n}{p} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-(p-1))}{p \cdot (p-1) \cdot (p-2) \cdots 1}$$

Let p^m be the largest power of m that divided n. The only term in the numerator that is divisible by p is the first term since it is a product of p consecutive integers and therefore only one of the can be divisible by p. Therefore the largest power or p that divides the numerator is p^m since it divides n and none of the other terms are divisible by p. The denominator has a factor of p and therefore will cancel off one factor of p from the numerator. Therefore the largest power of p that divides $\binom{n}{p}$ is p^{m-1}. And since $p^m \nmid \binom{n}{p}$, clearly $n \nmid \binom{n}{p}$ and therefore this terms survives.

Since $p \neq n$, this isn't the last term in the binomial series. Therefore, the two polynomials are different. □

There is one major problem here - how do we check if the two polynomials are the same? We can compute them by repeated squaring. But note that the polynomial $(X + a)^n$ has n terms. Checking if every term other than the first and the last is zero would take atleast $O(n)$ time adn therefore will be exponential in the input size which is $\log n$. We are looking for an algorithm that runs in $(\log n)^{O(1)}$ time.

The natural fix to this is computing the equation modulo a polynomial of small degree. Instead of computing $(X + a)^n \bmod n$, we compute $(X + a)^n \bmod (X^r - 1), n$ where $r \leq \log^c n$.

If n was a prime, then $(X+a)^n = X^n+a \bmod n$ and therefore $(X+a)^n = X^n + a \bmod (X^r - 1, n)$. The tricky part is the converse. It is very well possible that some composite number could satisfy this equation since we are going modulo a very small degree polynomial. What AKS does here is try this for different a's; they check if $(X + a)^n = X^n + a \bmod (X^r - 1, n)$ for a fixed r and $a \in (1, 2, \cdots, l)$ where $l \leq \log^{c'} n$. They then argue that if all these tests go through, n has to be a prime or a power of a prime.

Checking if n is a power of a prime is easy and that would conclude the algorithm.

2.1 Checking if $n = p^k$ for $k \geq 2$

Now $p \geq 2$ and therefore k can be at most $\log n$. Suppose we fix a k and want to find if $n = p^k$ for some p, how do we do that? Just a binary search.

Try $(n/2)^k$. If this is equal to n, you already got it. If it is less than n, then you know that if an a exists, it must be greater than $n/2$. Recurse on that half.

Thus, the number of steps is $\log^2 n$, which is polynomial in the input size.

We need to understand some properties of *cyclotomic extensions* over finite fields. We shall do those next time and that should fix the choice of l, r and other constants that come in the process.