6.S897 Algebra and Computation	March 16th
Lecture 12	
Lecturer: Madhu Sudan	*Scribe: Chiheon Kim*

1 Introduction

Today we are going to talk about primality testing algorithm by Agarwal, Kayal, and Saxena.

The problem is following.

Given an integer N, determine if N is a prime.

There is a sequence of results dealing with this problem.

- By definition, Primality is in coNP. Any nontrivial factorization of N is a short proof that the N is not a prime.
- [Pratt '75][1] Primality is in NP. Note that N is prime if and only if there is $a \in (\mathbb{Z}_N)^\times$ such that $\text{ord}_N(a) = N-1$, i.e., $a^{N-1} = 1 \pmod N$ but $a^{(N-1)/q} \neq 1 \pmod N$ for all prime q dividing $N-1$. We recursively give certificates that each of q is prime, so the total length of proof is $\mathsf{polylog}(N)$.
- [Solovay-Strassen '77][2][Miller-Rubin '80][3] Primality is in coRP. This result observes that if N is not a prime, then there is a and k such that $a^{2k} = 1 \pmod N$ but $a^k \neq \pm 1 \pmod N$. Moreover, if we pick a at random, then with probability at least half there is k such that the test holds. Under Generalized Riemann Hypothesis, the test can be made deterministic by checking $\mathsf{polylog}(N)$ many a's.
- [Goldwasser-Kilian '86][4][Adleman-Huang '87][5] Primality is in RP. They used elliptic curves to prove the result.
- In 2003, Agarwal, Kayal, and Saxena proved that Primality is in P.

2 Another proof of Primality $\in$ coRP

In 2000, Agrawal and Biswas proved that Primality is in coRP using different identity[6]. Observe that if N is a prime, that $(x+a)^N = x^N + a^N = x^N + a \pmod N$ for any a. We think it as a polynomial identity. We claim that converse is also true.

Lemma 1 *If N is a composite* (here we mean that N has two distinct prime factors) then $(x+a)^N \neq x^N + a \pmod N$ for any a which is coprime to N.*

Proof Let $N = P^i Q$ where P is a prime and P^i doesn't divide Q. Then, the coefficient of x^{N-P^i} in $(x+a)^N$ is $a^{P^i}\binom{N}{P^i}$. But $a^{P^i} = a \pmod P$ and $\binom{N}{P^i} \neq 0 \pmod P$, so the coefficient cannot be zero. ■

Now we want to check the polynomial identity $(x+a)^N = x^N + a \pmod N$. It is inefficient to write down all the coefficients of $(x+a)^N$, so Agrawal and Biswas proposed a probabilistic way to reduce the degree of polynomial.

[1] Pratt, V. (1975), "Every Prime Has a Succinct Certificate." SIAM J. Comput. 4, 214-220.
[2] Solovay, Robert M.; Strassen, Volker (1977). "A fast Monte-Carlo test for primality". SIAM J. Comput. 6 (1): 8485.
[3] Rabin, Michael O. (1980), "Probabilistic algorithm for testing primality", J. Number Theory 12 (1): 128138.
[4] S. Goldwasser, J. Kilian (1986), Almost all primes can be quickly certified, STOC 1986, 316-329
[5] Leonard M. Adleman, Ming-Deh A. Huang (1987), Recognizing Primes in Random Polynomial Time. STOC 1987: 462-469
[6] M. Agrawal, S. Biswas (2003), Primality and Identity Testing via Chinese Remaindering. J. ACM, 50(4):429443.

- Pick irreducible $Q(x) \in \mathbb{Z}_N[x]$ with $\mathsf{polylog}(N)$ degree at random.
- Accept if $(x+a)^N = x^N + a \pmod{N, Q(x)}$.

We can compute $(x+a)^N \pmod{N, Q(x)}$ in $\mathsf{polylog}(N)$ time using repeated squaring.

If N is a prime, the test will always accept. If N is composite*, then we have $(x+a)^N \neq x^N + a \pmod{N}$. We claim that the number of (monic) irreducible polynomial Q of degree at most $\mathsf{polylog}(N)$ such that $(x+a)^N = x^N + a \pmod{N, Q(x)}$ is at most N. This is because if we have $Q_1, \cdots, Q_{N+1}$ satisfying the identity, then the identity holds for $Q = Q_1 \cdots Q_{N+1}$ due to Chinese Remainder Theorem. We have $\deg(Q) > N$, so $(x+a)^N = x^N + a \pmod{N}$. There are roughly $\approx 2^{\mathsf{polylog}(N)}$ irreducible Q, so with high probability the test fails.

3 Agrawal-Kayal-Saxena Primality Testing

In 2003, Agrawal, Kayal, and Saxena proved that Primality is in P[7]. Instead of picking Q at random, they used $Q(x) = x^r - 1$ for some nice prime r along with $\mathsf{polylog}(N)$ many choices of a's. The algorithm is as follows.

1. Choose a prime r such that $\mathrm{ord}_r(N) \geq \mathsf{polylog}(N)$.
2. For $a = 1, \cdots, A$, test if $(x+a)^N = x^N + a \pmod{N, x^r - 1}$.
3. Accept if all tests accepts.

Prime Number Theorem implies that for any integer $k \geq 1$, there is a prime $r = O(k^2 \log N)$ such that $\mathrm{ord}_r(N) \geq k$. So, for $k = \mathsf{polylog}(N)$ we can test all $r \leq \mathsf{polylog}(N)$ to find a good one. We defer the proof to next lecture.

It is always nice to work with a ring, so let $R = \mathbb{Z}[x]/(N, x^r - 1)$. This ring has a lot of zero divisors, hence is not a field. Fix a prime divisor p of N and let $L = \mathbb{Z}[x]/(p, x^r - 1)$. Moreover, fix an irreducible factor $h(x)$ of $x^r - 1$ in $\mathbb{Z}_p[x]$. Define $K = \mathbb{Z}[x]/(p, h(x))$. Then K is a field. It is immediate to see that if $f = 0$ in R, then $f = 0$ in L and K.

From now on, we fix N and r.

Definition 2 *$f(x) \in \mathbb{Z}[x]$ is introverted with respect to $m \in \mathbb{Z}^+$ if $f(x^m) = f(x)^m \pmod{p, x^r - 1}$.*

Note that $x + a$ is introverted with respect to N. From this fact, we can generate lots of introverted polynomials with respect to many numbers.

Proposition 3 *If f and g are introverted with respect to m, then fg is also introverted with respect to m. If f is introverted with respect to m_1 and m_2, then f is introverted with respect to $m_1 m_2$.*

Proof The first part is easy, as $f(x^m)g(x^m) = f(x)^m g(x)^m = (fg)(x)^m \pmod{p, x^r - 1}$. For the second part, note that $f(x^{m_1}) = f(x)^{m_1} \pmod{p, x^r - 1}$ implies that $f(x^{m_1 m_2}) = f(x^{m_2})^{m_1} \pmod{p, x^{r m_2} - 1}$. Since $x^r - 1$ divides $x^{r m_2} - 1$, we have $f(x^{m_1 m_2}) = f(x^{m_2})^{m_1} \pmod{p, x^r - 1}$. Hence, $f(x^{m_1 m_2}) = f(x)^{m_1 m_2} \pmod{p, x^r - 1}$ as desired. ■

Due to the proposition, we know that $\{\prod_{d_a \geq 0} (x+a)^{d_a} \mid d_a \geq 0\}$ are introverted with respect to $\{N^i p^j \mid i, j \geq 0\}$.

Proposition 4 *If $f(x) \in \mathbb{Z}[x]$ is introverted for distinct m_1 and m_2 such that $m_1 = m_2 \pmod{r}$. Then $f(x)$ as in K is a zero of $z^{m_1} - z^{m_2} \in K[z]$.*

[7] Agrawal, M., Kayal, N., Saxena, N. (2004), PRIMES is in P. Annals of Mathematics 160 (2): 781793

Proof In $L = \mathbb{Z}[x]/(p, x^r - 1)$, we have $f(x)^{m_1} - f(x)^{m_2} = f(x^{m_1}) - f(x^{m_2}) \pmod{p, x^r - 1}$. Since $x^{m_1} = x^{m_1 \pmod r}$ and $x^{m_2} = x^{m_2 \pmod r}$ in L, we have $f(x)^{m_1} - f(x)^{m_2} = 0 \pmod{p, x^r - 1}$. This identity holds in K, so $f(x) \in K$ is a root of $z^{m_1} - z^{m_2}$. ■

Suppose that there are distinct $m_1, m_2 \le B$ with $m_1 = m_2 \pmod r$. If there were distinct $f_1(x), \cdots, f_{B+1}(x)$ in K such that each f_i is introverted with respect to m_1 and m_2, then $z^{m_1} - z^{m_2}$ has $B + 1$ distinct roots. But this is impossible because K is a field.

The main idea of AKS primality testing is as follows. We know that any polynomial in

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

is introverted with respect to any number of the form $N^i p^j$. For $\{N^i p^j \mid 0 \le i, j \le \sqrt{r}\}$, by Pigeonhole there are distinct m_1 and m_2 in this set, satisfying $m_1 = m_2 \pmod r$. Moreover, m_1 and m_2 are at most $N^{2\sqrt{r}}$. On the other hand, the number of polynomials in $\mathcal{F}$ is more than 2^A. If they are distinct in K, by Proposition 4 there are 2^A roots for $z^{m_1} - z^{m_2}$, so $2^A \le N^{2\sqrt{r}}$. But if we take large enough $A = \Theta(\mathsf{polylog}(n))$, this cannot happen, contradicting that N is composite*.

Here we assumed that polynomials in $\mathcal{F}$ are distinct enough modulo p and $h(x)$. This is indeed true if we restrict polynomials having degree at most the degree of $h(x)$. But this degree could be very small, so we need to ensure that (1) p is large, and (2) every irreducible factor of $x^r - 1$ in $\mathbb{Z}_p[x]$ has degree $\approx \mathsf{polylog}(N)$. We will give a detailed analysis in next lecture.