Lecture 12

Lecturer: Madhu Sudan *Scribe: Zeyuan Allen Zhu*

1 Today's Problem: Primality Testing

Given an n-bit integer N, output YES if n is prime and NO otherwise.

This is one of the most basic questions about numbers, with the following history.

- By definition $\textsc{Prime} \in \mathsf{coNP}$, because the prime decomposition is a short certificate for a number that is not prime.
- [Pratt'75] showed that $\textsc{Prime} \in \mathsf{NP}$. The Pratt certificate of a number N being prime, is by looking at all prime factor q of $N-1$ (which will be proved recursively), and giving some a such that $a^{(N-1)/q} \not\equiv 1 \pmod N$ for all such q's. This proof is of length $\mathsf{polylog} N$.
- The subsequent discoveries by [Solovay-Strassen'70s] [Miller-Rabin'70s] put $\textsc{Prime}$ in coRP. This algorithm uses the fact that if there exists some a, k such that $a^{2k} \equiv 1 \pmod n$ but $a^k \not\equiv \pm 1 \pmod n$ then N is composite. Moreover, the probabilistic algorithm picks a at random, and with $> 1/2$ probability there will be some k satisfying such compositeness criterion if N is composite.
- [Goldwassar-Killian'86] [Adleman-Huang'87] used algebraic (elliptic curve) techniques and proved that $\textsc{Prime} \in \mathsf{RP}$.
- In 2002, Agarwal, Kayal, and Saxena finally put $\textsc{Prime}$ in P, and this will be the main topic of today.

2 Prelude: Agarwal-Biswas Probabilistic Testing

Lemma 1 *For all a such that $(a, N) \neq 1$,*

$$N \text{ is a prime} \implies (x+a)^N \equiv x^N + a \pmod N \implies N \text{ is a prime power.}$$

Proof The first "$\implies$" is easy. For the second one, if $N = B \cdot C$ and $(B, C) = 1$, then after some careful calculation one can verify that $\binom{N}{B} \equiv C \not\equiv 0 \pmod N$. This means, the coefficient for the x^B term does not equal to zero in the expansion of $(x+a)^N = \sum_{i=0}^{N} x^i a^{N-i} \binom{N}{i}$. ∎

The lemma reduces our number theoretical question to an algebraic question of checking whether $(x+a)^N \equiv x^N + a \pmod N$. However, we cannot write down this big expansion explicitly, because we want an algorithm that runs in time $O(\mathsf{poly}(n)) = O(\mathsf{polylog} N)$. [Agarwal-Biswas'99] then proposed the following test:

- pick a monic polynomial $Q \in \mathbb{Z}_N[x]$ of degree $\mathsf{polylog} N$ at random; then
- verify if $(x+a)^N \equiv x^N + a \pmod Q$.

This is an efficient algorithm because the degree of Q is small and we can use power method to compute $(x+a)^N \bmod Q$ in $\mathsf{polylog} N$ time. The correctness can be verified using the following two properties:

- With probability at least $\frac{1}{\deg Q}$, Q is irreducible over mod N. This is because letting $d = \deg Q$,

$$x^{q^d} - x = \prod(\text{all irred. polys. of degree dividing } d) \ ,$$

and thus counting the degree on both sides we have at least $\frac{q^d}{d}$ irreducible polynomials of degree dividing d, and since there are a total of q^d choices for monic polynomials of Q over $\mathbb{F}_p$, at least with probability $\frac{1}{d}$ we will get a polynomial Q that is irreducible over $\mathbb{F}_p$, and then of course Q is also irreducible module N.

- Conditioning on Q being irreducible, the probability that $(x+a)^N \equiv x^N + a \pmod{Q}$ if N is composite is very very small due to the Chinese Reminder Theorem. This is because, if $(x+a)^N \equiv x^N + a \pmod{Q}$ holds for many polynomials $Q_1, Q_2, \dots, Q_t$'s, then the congruence also holds module $\text{lcm}(Q_1, Q_2, \dots, Q_t)$ due to Chinese Reminder Theorem, but when $\deg(\text{lcm}(Q_1, Q_2, \dots, Q_t))$ exceeds N we will have $(x+a)^N \equiv x^N + a \pmod{N}$ as well because the degree on both sides are only N, contradicting the fact that N is composite.

3 Derandomization: Agarwal-Kayal-Saxena Primality Testing

[Agarwal-Kayal-Saxena'02] considered the nice form $Q(x) = x^r - 1$ for some nice prime $r = \Theta(\mathsf{polylog} N)$, and their primality testing is as follows:

- Pick some prime $r = \Theta(\mathsf{polylog} N)$.
- Pick $A = \{1, 2, \dots, \mathsf{polylog} N\}$.
- Verify if $N = m^t$ for integer t, and output NO if this happens.

  (By enumerating all possible choices of t and computing m using binary search for each t.)
- Verify if $\exists a \in A$ divides N, and output NO if this happens.
- Verify if for all $a \in A$, we have $(x+a)^N \equiv x^N + a \pmod{N, x^r - 1}$. Output YES if this is true, and NO if there exists some $a \in A$ that fails the test.

(The proof of AKS (to be shown below) is quite a novel one. Prof. Madhu Sudan claims no such proof was seen before in either the CS or number theory literature.)

Notice that $R := \mathbb{Z}[x]/(N, x^r - 1)$ is not a field, because it is module N which is not a prime, and module $x^r - 1$ which might not be irreducible. In fact, if we define p to be any prime divisor of N, we can let $L := \mathbb{Z}[x]/(p, x^r - 1)$, while identities in R imply these in L. We can go another step further, by letting $h(x)$ to be any irreducible factor of $\frac{x^r - 1}{x - 1}$ in $\mathbb{F}_p[x]$, and define $K := \mathbb{Z}[x]/(p, h(x))$. Now, K is finally a field, and although R is the ring we are performing the primality testing, K is where we are going to work on the proof. Notice that identities in R also hold in K.

Proof overview: The main idea of the proof is to find a large collection of polynomials $\mathcal{F} \subseteq \mathbb{Z}[x]$ that, when viewed as elements of L satisfy several "semi"-nice "near"-algebraic conditions (called introversion below), assuming N passes the AKS test. The key idea in AKS is to convert this "semi"-nice "near"-algebraic conditions into a "pure" algebraic one, i.e., in the form of a non-zero polynomial $\mathcal{P} \in K[z]$ such that every element of $\mathcal{F}$, when viewed as an element of K, is a zero of $\mathcal{P}$. This conversion is neat in that $\mathcal{P}$ has low-degree if (and potentially only if) N is not a prime power. This leads to a contradiction because $\mathcal{P}$ now has many distinct zeroes (namely appropriately chosen elements of $\mathcal{F}$) while its degree is small! (Note that if N had been a prime, the degree of $\mathcal{P}$ would have been much larger and so the presence of so many zeroes would be perfectly OK.)

Definition 2 (Introversion) *We say that $f(x) \in L$ is* introverted *for m if $f(x^m) \equiv f(x)^m$ in L.*

Proposition 3

1. *For any* $a \in A$, $f(x) = x + a$ *is introverted for* $m = N$ *(if* N *passes the test);*
2. *for all* $f(x) \in L$, f *is introverted for* $m = p$*;*
3. *if* $f(x), g(x) \in L$ *are both introverted for* m*, then* $f(x) \cdot g(x)$ *is introverted for* m*; and*
4. *if* $f(x) \in L$ *is introverted for both* a *and* b*, then* $f(x)$ *is also introverted for* $a \cdot b$*.*

Proof The first three propositions are trivial, so we only prove the last one. Starting from:

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

we have:

$$f(z^b)^a \equiv f(z^{ba}) \pmod{z^{br} - 1} \ .$$

Now, since $z^r - 1 | z^{br} - 1$, we also have:

$$f(z^b)^a \equiv f(z^{ba}) \pmod{z^r - 1} \ ,$$

and this is one place (and we will see another place shortly) that we have specific reason to use polynomials of the form $x^r - 1$; in general, it may not be the case that $h(z)|h(z^b)$. We have not used any property of r yet. At last, we have:

$$f(z)^{ba} = f(z^b)^a \equiv f(z^{ba}) \pmod{z^r - 1} \ .$$

■

Proposition 4 *If* $f(x) \in L$ *is introverted for* m_1 *and* m_2 *while* $m_1 = m_2 \pmod r$*, then* $f(x)^{m_1} = f(x)^{m_2}$*.*

Proof $f(x)^{m_1} = f(x^{m_1}) = f(x^{m_2}) = f(x)^{m_2}$ and the second equality is because $m_1 \equiv m_2 \pmod r$ and we are in the ring module $x^r - 1$. ■

3.1 High Level Ideas for the Analysis

Now using above propositions, we want to find

- a large set $\mathcal{F}$ of polynomials, even when viewed module $h(x)$, and
- two small integers m_1 and m_2 satisfying $m_1 = m_2 \pmod r$, such that for any $f(x) \in \mathcal{F}$, f is introverted for both m_1 and m_2.

If we found such m_1, m_2, then all $f \in \mathcal{F}$ are roots to polynomial $\mathcal{P}(z) := z^{m_1} - z^{m_2}$, and although $f \in L$ and L is not a field, but it is contained in K which is a field, so $\mathcal{P}(z) \in K[z]$. Now notice that $\mathcal{F}$ is a large set of zeros of $\mathcal{P}(z)$, so if we had $|\mathcal{F}| > \max\{m_1, m_2\}$ we would have a contradiction.

3.2 Details

A very natural set $\mathcal{F}$ to consider is, for some fixed t, let

$$\mathcal{F}_t := \Big\{ \prod_{a \in A} (x + a)^{d_a} \Big| \sum_{a \in A} d_a \le t \Big\} \ .$$

Then, $|\mathcal{F}_t| = \binom{t+|A|}{|A|}$. If we choose $t = |A|$ we always have $|\mathcal{F}_t| \geq 2^t$ being a large set. Notice that we still need to make sure that all polynomials in $\mathcal{F}_t$ are distinct module $h(x)$, but we will worry about this later.

Now, how to make m_1 and m_2 small? Recall from Proposition 3 that all polynomials in $\mathcal{F}_t$ are introverted for all numbers in $\{N^i P^j | 0 \leq i \leq \sqrt{r}, 0 \leq j \leq \sqrt{r}\}$. In fact, since this set has more than r elements we can find two distinct $m_1, m_2 \leq N^{2\sqrt{r}}$ such that all polynomials in $\mathcal{F}_t$ are introverted for m_1 and m_2 and $m_1 \equiv m_2 \pmod r$.[1]

At last, we use the following powerful lemma

Lemma 5 (Fourry'80s) *$\exists$ prime $r = O(\mathsf{polylog} N)$ s.t. for sufficiently large p, $\deg h(x) > r^{2/3}$.*

Using the above lemma, if we pick $t = \deg h - 1$ for $\mathcal{F}_t$, then $|\mathcal{F}_t| \geq 2^{r^{2/3}}$ and it contains only distinct polynomials module $h(x)$. Recall that $m_1, m_2 \leq 2^{\sqrt{r} \log N}$, so this is sufficient to give the contradiction and is indeed the original proof. We emphasize here that one needs to check all small r's because the Fourry lemma does not give an explicit construction for such prime r.

3.3 Improved Analysis

We will now potentially choose $t > \deg h$, but still try to argue that elements in $\mathcal{F}_t$ are distinct module $h(x)$. Let us define

$$T = \left\{ N^i p^j \pmod r \;\middle|\; i, j \in \mathbb{Z}^{\geq 0} \right\} ,$$

and define $l = |T| \leq r$. We know that all polynomials in $\mathcal{F}_\infty$ are introverted for any $m \in T$. Now, let us consider a specific one $\mathcal{F}_{l-1}$, and will show that

- elements of $\mathcal{F}_{l-1}$ are all distinct module $h(x)$ (which will be proved in Lemma 6).
- $m_1, m_2 \leq N^{2\sqrt{l}}$ (using similar proof as before), such that $m_1 \equiv m_2 \pmod r$ and all polynomials in $\mathcal{F}_{l-1}$ are introverted for m_1 and m_2.

Now if we let $|A| = l - 1$, we can lower bound $|\mathcal{F}_{l-1}| = \binom{l-1+|A|}{|A|} \geq 2^{l-1}$, and we will have a similar contradiction as before if $2^{l-1} > N^{2\sqrt{l}}$. This latter inequality will always be true when $l = |T| = \Omega(\log^2 N)$, to be shown in Lemma 7.

3.4 Two Technical Lemmas

Lemma 6 *Suppose $f \neq g$ and $f, g \in \mathcal{F}_{l-1}$ are introverted with respect to $m_1, \ldots, m_l$ (all distinct $\bmod\ r$). Then $f \not\equiv g \pmod{h(x)}$.*

Proof We can view $f(z), g(z) \in \mathbb{F}_p[z]$ as $f(z), g(z) \in K[z]$ because $\mathbb{F}_p \subseteq K$. If $f(x) \equiv g(x) \pmod{h(x)}$, then $x \in K$ is a root of $f(z) - g(z)$ which is a non-zero polynomial with degree no more than $l - 1$.

Now using introversion, we also have $f(x^m) = f(x)^m = g(x)^m = g(x^m)$ for each $m \in T$ so there are at least l roots to $f(z) - g(z)$, so there must be true that $x^{m_i} \equiv x^{m_j} \pmod{h(x)}$ for some distinct $m_i, m_j \in T$. In such a case, we have both

$$\begin{aligned} x^{m_i - m_j} - 1 &\equiv 0 \pmod{h(x)} \\ x^r - 1 &\equiv 0 \pmod{h(x)} \end{aligned}$$

(This is another reason for our choice of polynomials like $x^r - 1$). We therefore have that $x^{\gcd(m_i - m_j, r)} - 1 \equiv 0 \pmod{h(x)}$, giving $x - 1 \equiv 0 \pmod{h(x)}$ but this is against our choice of $h(x)$. ■

[1] Notice that if we just look at all N^i we can get N^r naively, but using p we can benefit.

Lemma 7 *There exists prime* $r \le O(k^2 \log N)$ *such that*

$$\big|\{N^i \pmod r \mid i\}\big| \ge k \ .$$

Notice that by choosing choosing $k = \log^2 N$ *we have* $l = |T| \ge \big|\{N^i \pmod r \mid i\}\big| \ge \log^2 N$.

Proof [not provided in class but can be found in prenotes]

Suppose this is not true for some prime r, that is $\big|\{N^i \pmod r \mid i\}\big| < k$, then r must divide the difference between N^i and N^j for some $0 \le i, j \le k-2$, and therefore:

$$r \ \Big| \ M := \prod_{i=1}^{k-2} (N^i - 1) \ , \quad \text{and } M \le N^{k^2} \ .$$

However, if this is true for all prime r that is below m, then we have

$$\prod_{p_i \le m, \ p_i \text{ is prime}} p_i \le M \le N^{k^2} \ .$$

But this contradicts with Corollary 9 below, when $m = \Omega(k^2 \log N)$. ■

Theorem 8 (Weak Prime Number Theorem)

$$\Big|\big\{\textit{prime number} \le 2m+1\big\}\Big| \ge \frac{m}{\log_4(2m+1)} \ .$$

Proof Ommited, but it uses the fact that $\text{lcm}(1, 2, \ldots, 2m+1) \ge 4^m$. See the prenotes. ■

Corollary 9 *There exists some constant* $c > 1$ *such that*

$$\prod_{p_i \le m, \ p_i \ \textit{is prime}} p_i > c^m \ .$$