0368-4159: First Course in Derandomization 19,26/11/18 – Lecture 6,7

The AKS Algorithm

Lecturer: Amnon Ta-Shma

Scribe: Or Karni, Ori Sberlo

1 Primality Testing

The problem of determining whether a given number is prime is ancient. The input is a number n, represented in binary, and the goal is to decide if it is prime. Notice that the input length is the number of bits needed to represent n, i.e., $\log n$. Clearly the problem is in coNP, but it was also shown to be in NP [**?**]. There are several algorithms putting it in BPP. We are now going to see a deterministic polynomial time algorithm for it, putting it in P [1].

1.1 Random Algorithms

There are several probabilistic algorithms for the problem that rely on the following property of primes numbers.

Claim 1. *[Fermat's little theorem] Let n be a prime number then for any integer a it holds that $a^n \equiv a \pmod{n}$.*

Unfortunately, this is not a characterization of prime numbers since there are non-prime numbers that have this property. Consider the following randomized algorithm for primality Testing:

Algorithm 1 Algorithm for PT

1. Sample $a \in \mathbb{Z}_n^*$ uniformly.
2. If $gcd(a, n) \neq 1$, return "Composite".
3. If $a^n = a \pmod{n}$ return "Prime", else return "Composite".

According to Claim 1, if n is prime, we will always return "Prime". However, there are non-prime integers n that will always pass the test and so the algorithm fails for these numbers. It is true that there are very few inputs for which the above algorithm fails, but we want a *worst-case* algorithm, namely an algorithm which works for every input with small error probability over the random coins of the algorithm (and not for most inputs).

1.2 Characterization of primes with a polynomial identity

The identity $a^n = a \pmod{n}$ over $\mathbb{Z}$ is true for primes n, but does not characterize primes. Now, instead of working over $\mathbb{Z}$, we will work over the polynomial ring $\mathbb{Z}_n[X]$, the ring of all polynomials with degree at most n over $\mathbb{Z}$, and in return we will get a characterization. Working with polynomials

might look more complicated than working over the integers, but this is often not the case. In fact, quite the contrary is true. For example, polynomials (as integers) have unique factorization to irreducible polynomials. The problem of polynomial factorization can be done in polynomial time (sometimes, probabilistic polynomial time and sometimes deterministic polynomial time, depending on the field over which we work). In contrast, integer factorization is believed to be hard, and many cryptographic algorithms rely on the assumption that (at the very least) factorization is not in BPP. We claim:

Lemma 2. *Suppose $a, n \in \mathbb{Z}$ and $gcd(a, n) = 1$. Then, n is prime iff $(X + a)^n = X^n + a$, where the equality is over $\mathbb{Z}_n[X]$.*

Proof. We always have the binomial identity $(x + a)^n = \sum_{i=0}^{n} \binom{n}{i} x^i a^{n-i}$ where $\binom{n}{0} = \binom{n}{n} = 1$. If n is prime then for all $i > 1$,

$$\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i!}$$

The prime n divides the numerator once, and does not divide the denominator, hence $\binom{n}{i} \bmod n = 0$ and we are done (and for this part a can be any integer, not necessarily co-prime with n).

Suppose n is not prime and $a \in \mathbb{Z}$ s.t. $gcd(a, n) = 1$. Then n has a prime factor p and an integer k such that p^k divides n but p^{k+1} does not. Consider the monomial with coefficient

$$\binom{n}{p} = \frac{n(n-1)\dots(n-p+1)}{p!}.$$

p^k divides n but p doesn't divide $(n-1), \dots, (n-p+1)$, meaning $p^k | n(n-1)\dots(n-p+1)$ but p^{k+1} does not. Also, p divides p but not $1, \dots, p-1$, meaning $p | p!$ but p^2 does not. Therefore, $p^{k-1} | \binom{n}{p}$, but $p^k \nmid \binom{n}{p}$. This means that $n \nmid \binom{n}{p}$, so the monomial x^p does not vanish. □

2 The AKS algorithm

2.1 Outline and Complexity

The AKS algorithm [1] is a deterministic polynomial time algorithm for primality testing based on the characterization in Lemma 2. However, there is a problem in turning this characterization to a primality testing algorithm. To understand this, consider the following naive pseudo-algorithm:

Algorithm 2 Naive AKS

1. Check if $(X + a)^n = X^n + a^n$ for some arbitrary $a \in \mathbb{Z}_n$ (say $a = 2$).
2. If there equality return "Prime" otherwise return "Composite".

First, Lemma 2 implies that this algorithm is indeed a deterministic algorithm for primality testing. The problem is that the equality in step 2 is not an equality of integers, but rather an equality of polynomials, namely the PIT problem, and we do not know how to test this equality efficiently in general. Computing the polynomial would clearly require $\Omega(n)$ time as potentially this polynomial may have $\Omega(n)$ nonzero coefficients which is exponentially more time than we are allowed to

use. In fact, our problem now reduces to a special case of the famous PIT problem - testing the equality of two polynomials. The AKS algorithm finds a way around this and manages to solve deterministically this special case of PIT.

The approach is based (among other things) on an idea we already saw in the one-sided error algorithm for PIT. In the PIT algorithm we needed to evaluate a given polynomial $f(x)$ at a point $p \in \mathbb{R}^N$, but the value of $f(p)$ might be extremely large. Roughly, this is because polynomials might have degree exponentially large in their size of representation. To overcome this problem we computed this value modulus some prime, allowing us to use the fast exponentiation algorithm while controlling the magnitude of the values. Analogously, we will check the equality $(X+a)^n = X^n + a$ modulus some polynomial, namely check whether $(X+a)^n = X^n + a \pmod{\psi(x)}$.

Algorithm 3 AKS

1. Check whether n is a perfect power. If so, return "Composite".
2. Set $\bar{r} = 2000 \log^6 n$
3. Check for all $2 \leq i \leq \bar{r}$ that $(i, n) = 1$. If not, return "Composite".
4. Find $2 \leq r \leq \bar{r}$ s.t. $ord_r(n) > t_0 = 9 \log^2 n$ [1]. The order of an element $ord_r(n)$ is defined in the next section.
5. For all $1 \leq a \leq r$, check whether $(X+a)^n = X^n + a$ over the ring $\mathbb{Z}_n[X] \pmod{X^r - 1}$.
6. If one of the tests failed - return "Composite". Else, return "Prime".

We start by going over the algorithm and verify that each step can be done in polynomial time:

- Step 1: We need to verify if there exists integers a, k such that $n = a^k$ and $k > 1$. First we rule out $n = 1$. If $n > 1$ then clearly $a \geqslant 2$ and so $n = a^k \Rightarrow \log n = k \log a \geqslant k$ and so $k \leqslant \log n$. Therefore, it suffices to verify if for $k = 2, 3, 4, \ldots, \log n$ there exists $n = a^k$. For every fix $k \leqslant \log n$ this can be verified in polynomial time (i.e, polylog(n) time). To see this consider the trivial algorithm which preforms binary search to find such a which takes $O(\log n)$ time. We conclude that this step takes $O(\log^2 n)$ time.
- Step 3: We can compute (i, n) using Euclid's algorithm in $O(\log n)$ for any $i = 2, \ldots, \bar{r} = O(\log^5 n)$ and therefore this step takes $O(\log^7 n)$ time.
- Step 4: This step seems a bit dubious as it is unclear whether there exists an integer r satisfying $ord_r(n) > \log^2 n$ and $r \leqslant \bar{r}$. Nonetheless, this step can be done efficiently using brute force approach. There are $O(\log^2 n)$ many integers to check $r = 1, 2, \ldots, \bar{r} = O(\log^5 n)$ and all we need to check is that we can verify if $ord_r(n) \geqslant t_0$ or not efficiently. To do this one can simply compute $r^2, r^3, \ldots, r^{t_0}$ (which can be done efficiently using fast exponentiation). If $r^2, r^3, \ldots, r^{t_0} \neq 1 \pmod{r}$ then $ord_r(n) > t_0$ and otherwise $ord_r(n) \leqslant t_0$. In total, this step takes $O(\bar{r} \log^3 n) = O(\log^9 n)$.
- Step 5: This step can be done using fast exponentiation algorithm. That is, compute $(X+a)^{2^i} \pmod{X^r - 1}$ for $i = 1, 2, \ldots, r$ sequentially. In each iteration we can main-

[1] $ord_r(n)$ is the order of the element n within the group $\mathbb{Z}_r^*$. This is formally defined in Section 3.

tain our polynomial to have degree at most r. A naive computation of the square of degree r polynomials takes $O(r^2)$ time which is $O(\log^{12} n)$ time (this can be reduced to roughly $O(r \log r \log n)$ times using FFT). After that we have to multiply $\log n$ such polynomials. There are r such computations then this step takes $O(r^3 \log n) = O(\log^{19} n)$ time in total.

2.2 Simple Lemma

Step 4 of the AKS algorithm seems a bit suspicious as it is not clear that there exists an integer $r \leqslant \bar{r}$ such that $ord_r(n) > t_0$. The next lemma shows that such r always exists.

Lemma 3. *For every $n \in \mathbb{N}$ there exists $2 \leqslant r \leqslant \bar{r} = 2000 \log^5 n$ such that $ord_r(n) > t_0 = 9 \log^2 n$.*

Proof of Lemma 3. We will show that such r exists using a simple counting argument. Suppose r is such that $ord_r(n) = i \leqslant t_0$. Note that,

- $ord_r(n) = 1 \Rightarrow n^1 = 1 \pmod r \Rightarrow r \mid n - 1$
- $ord_r(n) = 2 \Rightarrow n^2 = 1 \pmod r \Rightarrow r \mid n^2 - 1$

  $\vdots$
- $ord_r(n) = t_0 \Rightarrow n^t = 1 \pmod r \Rightarrow r \mid n^{t_0} - 1$

Therefore, such r must divide the product $\prod_{i=1}^{t_0}(n^i - 1)$. Denote $A = \prod_{i=1}^{t_0}(n^i - 1)$ then A is some positive integer bounded by

$$\prod_{i=1}^{t_0} n^i = n^{\sum_{i=1}^{t_0} i} \leqslant n^{t_0^2}.$$

Also, A has at most $\log A \leqslant t_0^2 \log n$ distinct prime factors. On the other hand we have the following lower bound on the prime counting funciton.

Claim 4 (Chebyshev's Bound)**.** *For any natural number $k \in \mathbb{N}^+$ we have,*

$$\pi(2k) \geqslant \frac{k}{\log(2k)},$$

where $\pi(k)$ denotes the number of prime numbers smaller or equal to k.

It follows that there are at least $\frac{\bar{r}}{2\log(\bar{r})} = \frac{1000 \log^5 n}{\log(2000) + \log^5 n)}$ primes which are small or equal to $\bar{r}$. It straightforward to verify that $\frac{1000 \log^5 n}{\log(2000) + \log^5 n)} > 81 \log^5 n = t_0^2 \log n$ for every $n \in \mathbb{N}^+$. Hence there must be some prime which does not divide A. Denote this prime by r then as r does not divide A we have $ord_r(n) > t_0$. We remark that in the paper the argument is done in a more concise way and $\bar{r} = \log^5 n$ suffices. □

3 Some mathematical preliminaries

3.1 Multiplicative Order

For an integer r, $\mathbb{Z}_r^* = \{1 \leq a \leq r \mid (a, r) = 1\}$. $\mathbb{Z}_r^*$ is a multiplicative group. $\varphi(r) = |\mathbb{Z}_r^*|$ is *Euler's totient function.* For example, If p, q are prime, $\varphi(p) = p - 1$ and $\varphi(pq) = pq - p - q + 1$. In our case, $(n, r) = 1$ (because $r \leq \bar{r}$) and so $n \in \mathbb{Z}_r^*$ and $n^{\varphi(r)} = 1$.

Definition 5. *$ord_r(n)$ is the smallest number $k \geq 1$ s.t. $n^k = 1 \pmod r$.*

3.2 Cyclotomic Polynomials

How does $x^6 - 1$ factor over $\mathbb{C}$? It has exactly 6 roots - we define $\omega = e^{\frac{2\pi i}{6}}$ and get

$$X^6 - 1 = \prod_{k=0}^{5}(X - \omega^k)$$

How does $X^6 - 1$ factor over $\mathbb{Z}$? An easy claim (to be given as homework) shows that $X^a - 1 \mid X^b - 1$ iff $a \mid b$. Therefore, $X - 1, X^2 - 1, X^3 - 1$ divide $X^6 - 1$. It is not true that $X^6 - 1 = (X - 1)(X^2 - 1)(X^3 - 1)$ because $X - 1, X^2 - 1, X^3 - 1$ have common factors.

Definition 6. *ω is a primitive d-root of unity if $\omega^d = 1$ and $\omega^i \neq 1$ for all $i < d$.*

Definition 7. *The d-th cyclotomic polynomial is*

$$\Phi_d(X) = \prod_{\substack{\omega \text{ is a primitive} \\ d\text{-root of unity}}} (X - \omega).$$

Lemma 8. *For all r,*

$$X^r - 1 = \prod_{d|r} \Phi_d$$

Proof. We compare the r roots of $x^r - 1$ with the roots of $\Pi_{d|r}\Phi_d$.

There are r different roots of unity of order r. In particular all the roots of $x^r - 1$ are different, i.e., $x^r - 1$ is *separable*. (A polynomial $p \in K[x]$ is separable, if p has distinct roots in the algebraic closure of K). Every r-root of unity is a primitive d-root of unity for some $d \mid r$. Thus, we can define a mapping from the roots of $x^r - 1$ to the roots of $\prod_{d|r} \Phi_d$. This map is one-to-one (because $x^r - 1$ is separable) and onto (because each primitive root of order $d|r$ is a root of order r). Hence the two polynomials have the same roots in the algebraic closure and are equal. □

We therefore get the following sequence of polynomials:

$$\begin{aligned}
\Phi_1 &= x - 1 \\
\Phi_2 &= \frac{x^2 - 1}{\Phi_1} = x + 1 \\
\Phi_3 &= \frac{x^3 - 1}{\Phi_1} = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 \\
\Phi_4 &= \frac{x^4 - 1}{\Phi_1\Phi_2} = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1 \\
\Phi_5 &= \frac{x^5 - 1}{\Phi_1} = 1 + x + x^2 + x^3 + x^4 \\
\Phi_6 &= \frac{x^6 - 1}{\Phi_1\Phi_2\Phi_3} = (x - \omega)(x - \omega^5).
\end{aligned}$$

The representation of Φ_6 as $(x-\omega)(x-\omega^5)$ does not immediately reveal that Φ_6 is a polynomial over $\mathbb{Z}$ (even though it is relatively easy to see that because $w^5 = \bar{\omega}$). A better way to see that Φ_6 is a polynomial over $\mathbb{Z}$ is:

Fact 9. *If $f \cdot g \in \mathbb{Q}[X]$ and $f \in \mathbb{Q}[X]$, then $g \in \mathbb{Q}[X]$. If $f \cdot g$ and f are monic and in $\mathbb{Z}[X]$ then $g \in \mathbb{Z}[X]$.*

With that we claim:

Claim 10. $\Phi_d \in \mathbb{Z}[x]$.

Proof. By induction on d. For $d = 1$, $\Phi_1 = x - 1$. Assume for $d < n$. Then, $\Phi_n = \frac{x^n-1}{\Pi_{d|n, d<n}\Phi_d}$ and the claim follows by induction and the Fact 9 □

Finally:

Fact 11. *The polynomial $\Phi_d(X)$ is irreducible over $\mathbb{Z}[X]$ for any d.*

3.3 Finite fields

For every prime power p^k there exists a finite field with p^k elements. We describe one representation of such a field. Take an irreducible polynomial $E \in \mathbb{Z}_p[X]$ of degree k (A fact: for every finite field F and integer k there exists an irreducible polynomial of degree k over F). The elements of our new field, $\mathbb{F}_{p^k}$, are $\mathbb{Z}_p[X] \pmod{E(X)}$, i.e., the polynomials over $\mathbb{F}_p[X]$ with degree smaller than k. The addition and multiplication operations are:

- Addition: regular polynomial addition,
- Multiplication: $f \cdot g \pmod{E}$.

Definition 12. *Suppose $F \subset K$ are finite fields. Let $z \in K$. We say z is* algebraic *over F if there exists a polynomial $p \in F[x]$ such that $p(z) = 0$.*

Definition 13. *Suppose $F \subset K$ are finite fields and $z \in K$ algebraic over F. The minimal polynomial of z is the least degree monic polynomial among all polynomials in $F[X]$ that has z as its root.*

Remark 14. *The minimal polynomial is unique.*

Claim 15. *Suppose $F \subset K$ are finite fields, $z \in K$ algebraic over F and $p(X) \in F[X]$ is the minimal polynomial of z. Then, if $q(z) = 0$ for some $q \in F[X]$ then $p|q$.*

For example, consider $\mathbb{R} \subseteq \mathbb{C}$. The minimal polynomial of i over $\mathbb{R}$ is x^2+1. In general, the minimal polynomial of $z \in \mathbb{C}$ is $(x-z)(x-\bar{z}) = x^2 - (z+\bar{z})x + z\bar{z}$, which always a real polynomial.

Claim 16. *If $\mathbb{F}$ is a finite field then $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is a multiplicative group.*

The above claim implies that for any $z \in \mathbb{F}_q$ it holds that $z^{q-1} = 1$ and so for any $z \in \mathbb{F}_q$ it holds that $z^q = z$. Therefore,

$$X^{q-1} - 1 = \prod_{z \in \mathbb{F}_q^*} (X - z)$$

and all elements in $\mathbb{F}_q$ are algebraic over $\mathbb{F}_p$ (where p is the characteristic of $\mathbb{F}_q$).

3.3.1 Finding the minimal polynomial

Let us first consider the familiar field extension $\mathbb{R} \subset \mathbb{C}$. If $z = a + bi \in \mathbb{C} \setminus \mathbb{R}$ with $a, b \in \mathbb{R}$, then the minimal polynomial of z is the polynomial $p(x) = (x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z} = x^2 - 2ax + |z|^2 \in \mathbb{R}[x]$. $\bar{z}$ is the conjugate of z. In fact, there is one automorphism of K that keeps $\mathbb{R}$ in place, which is the mapping $\psi : (a + bi) \to (a - bi)$ and the conjugate of z is $\psi(z)$.

The situation when $F \subset K$ are finite fields is similar. Suppose $\mathbb{F} = \mathbb{F}_p[X] \pmod{E}$ is an extension field of $\mathbb{F}_p$ with p^k elements. The mapping $\psi : z \to z^p$ is an automorphism of $\mathbb{F}$ leaving the base field $\mathbb{F}_p$ unchanged, and so are the mappings $z \to z^{p^i}$. The conjugates of $z \in \mathbb{F}$, are z^{p^i} for $i \in \mathbb{N}$. The conjugates repeat themselves and go in cycles of length k, and sometimes with shorter cycles whose length divides k.

Now let $z \in \mathbb{F}$. Clearly $p(X) = X^{|\mathbb{F}|} - x$ is a polynomial in $\mathbb{F}_p[X]$ and z vanishes on $p(X)$, so z is algebraic over $\mathbb{F}_p$. Suppose $Q(x)$ is the minimal polynomial of z over $\mathbb{F}_p$. Denote $Q(x) = \sum \alpha_i x^i$ where $\alpha_i \in \mathbb{F}_p$ then $Q(z) = 0 \Rightarrow Q(z^p) = 0$. To see this,

$$Q(z^p) = \sum \alpha_i z^{pi} = \Big(\sum \alpha_i z^i \Big)^p = \big(Q(z)\big)^p = 0$$

Applying this repeatedly we get that $Q(z) = 0$ implies $Q(z^{p^i}) = 0$ for every $i \in \mathbb{N}$. This suggests that all the conjugates of z are roots of $Q(X)$ (i.e, roots of the minimal polynomial of z). In fact, these are the only roots of the minimal polynomial of z.

Claim 17. *Suppose $\mathbb{F}_p \subset \mathbb{F}_q$ where p is prime (hence $q = p^k$ for some k), $z \in \mathbb{F}_q$ algebraic over $\mathbb{F}_p$ and $p(X) \in \mathbb{F}_p[X]$ is the minimal polynomial of z. Then,*

$$p(X) = \prod_{\substack{\alpha \text{ is a} \\ \text{conjugate of } z}} (X - \alpha).$$

3.3.2 An Example

Let us construct a field with 7^3 elements. Let $E(x) = X^3 + 2, \mathbb{F}' = \mathbb{F}_7[X] \pmod{E}$. To see that E is irreducible over $\mathbb{F}_7$, notice that otherwise E must have a linear factor (because E is degree 3) but it does not have a linear factor because it does not vanish on $\mathbb{F}_7$.

Now, let us find the minimal polynomial of $z = X^2 \in \mathbb{F}'$. We first compute the conjugates of z (remember that in $\mathbb{F}$, $X^3 = -2$):

$$\begin{aligned} z &= X^2 \\ z^7 &= x^{14} = X^{3 \cdot 4 + 2} = (-2)^4 X^2 = 16X^2 = 2X^2 \\ z^{7^2} &= (2X^2)^7 = 2 \cdot (2X^2) = 2^2 X^2 \\ z^{7^3} &= (2^2 X^2)^7 = 2 \cdot (2^2 X^2) = 2^3 X^2 = x^2. \end{aligned}$$

Therefore, the minimal polynomial of $z = X^2$ is $Q(Y) = (Y - X^2)(Y - 2X^2)(Y - 4X^2)$. In this representation it looks as if Q does not have coefficients from $\mathbb{F}_7$. However, the coefficients are symmetric functions in the conjugates and do belong to $\mathbb{F}_7$. For example, the free coefficient is $-X^2 \cdot 2X^2 \cdot 4X^2 = -8X^6 = -32 = 3 \in \mathbb{F}_7$.

3.4 The factorization of Φ_r over $\mathbb{F}_p$

Suppose $(n,p)=1$. How does X^n-1 and $\Phi_n(x)$ factorize over $\mathbb{F}_p$? To answer this we try to analogously define cyclotomic polynomials over $\mathbb{F}_p$, or more accurately, over the algebraic closure of $\mathbb{F}_p$, namely $\overline{\mathbb{F}_p}=\cup_k \mathbb{F}_{p^k}$.[2]

Definition 18. *We say that $\alpha \in \overline{\mathbb{F}_p}$ is a primitive d'th root of unity if $\alpha^d=1$ (this equality is in the field $\overline{\mathbb{F}_p}$) and d is the least such positive integer with that property.*

Definition 19. *Define $\Phi_{d(p)}(X)$ to be the monic polynomial whose roots are all the primitive d'th roots of unity in $\overline{\mathbb{F}_p}=\cup_k \mathbb{F}_{p^k}$. That is,*

$$\Phi_{d(p)}(X)=\prod_{\substack{\alpha \text{ is a } d\text{'th} \\ \text{primitive root of unity}}}(X-\alpha)$$

Note that the definition of $\Phi_{d(p)}(X)$ over $\overline{\mathbb{F}_p}$ is completely analogous to the definition of $\Phi_d(X)$ over $\mathbb{C}$. Using the cyclotomic polynomials $\Phi_d(X)$ we were able to factorize the polynomial X^n-1 over $\mathbb{C}$ $X^n-1=\prod_{d|n}\Phi_d(X)$. We now prove an analogous claim over $\mathbb{F}_p$.

Claim 20. *Let $f(X)\in\mathbb{F}_p[X]$. f is separable iff $gcd(f,f')=1$ (f' is the formal derivative of the the polynomial p).*

Using that $(n,p)=1$ we conclude that X^n-1 is separable (i.e, all roots have multiplicity 1) and so we conclude that

$$X^n-1=\prod_{d|n}\Phi_{d(p)}(X)$$

over $\overline{\mathbb{F}_p}$ (the proof is the same as over $\mathbb{C}$). Using again the same induction we see that $\Phi_{d(p)}(X)\in\mathbb{F}_p[X]$. In fact,

Claim 21. *Suppose d is relatively prime to p. Then $\Phi_{d(p)}(X)=\Phi_d(X) \pmod p$.*

Proof. $\Phi_{1(p)}=x-1=\Phi_1$. By induction, $\Phi_{n(p)}=_{\text{mod } p}\frac{x^n-1}{\Pi_{d|n,d<n}\Phi_{d(p)}}=\frac{x^n-1}{\Pi_{d|n,d<n}\Phi_d}=\Phi_n$. □

Henceforth we will write $\Phi_d(X)$ for the d'th cyclotomic polynomial, whether we are over $\mathbb{C}$ or $\overline{\mathbb{F}_p}$).

Recall that $\Phi_d(X)$ is irreducible over $\mathbb{C}$ which brings us to the next question - is $\Phi_d(X)$ irreducible over $\mathbb{F}_p$? The answer is "no", in general.

Example 22. *The cyclotomic polynomial $\Phi_7(X)=X^6+X^5+X^4+X^3+X^2+X+1$ is irreducible over $\mathbb{C}$ though reducible over $\mathbb{F}_2$ $\Phi_7(X)=(X^3+X^2+1)(X^3+X+1) \pmod 2$.*

Now, suppose $\Phi_d(X)$ factorizes over $\mathbb{F}_p[X]$. What do the factors over $\mathbb{F}_p$ look like? To answer that, suppose θ is a root of Φ_d in the algebraic closure of $\mathbb{F}_p$. According to Claim 17 the minimal polynomial of θ (over $\mathbb{F}_p$) is given by

$$m(X)=\prod_{i=1}^{k}(X-\theta^{p^i}),$$

[2] This is the minimal field extension of $\mathbb{F}_p$ satisfying that every polynomial $f(X)\in\mathbb{F}_p[X]$ completely factorizes in it, i.e all the roots of $f(X)$ are in $\overline{\mathbb{F}_p}$

where k is the minimal positive integer such that $\theta^{p^k} = 1$, i.e., $\theta^{p^k \bmod d} = 1$ (because θ is a primitive d root of unity), or equivalently $k = ord_d(p)$ (note that this quantity only depends on d, p and independent on the choice of θ). Also recall that the minimal polynomial $m(X)$ must divide any polynomial that has θ as its root. Thus $m(X)$ is an irreducible (over $\mathbb{F}_p$) dividing $\Phi_d(X)$. This can be done to any root (in the aslgebraic closure) of Φ_d, implying that $\Phi_d(X)$ factorizes to minimal polynomials each of degree exactly $ord_d(p)$. That is, $\Phi_d(X)$ factors into $\frac{\deg(\Phi_d)}{ord_d(p)} = \frac{\varphi(d)}{ord_d(p)}$ irreducible polynomials over $\mathbb{F}_p$ each of degree $ord_d(p)$ (as a sanity check verify that $ord_d(p)$ divides $\varphi(d)$).

Example Consider $d = 10$ and take prime p such that $ord_{10}(p) = 2$. Consider $\Phi_{10}(x) = X^4 - X^3 + X^2 - X + 1$ then $\Phi_{10}(X)$ factors into 2 irreducible polynomials over $\mathbb{F}_p$ of degree 2 each.

$$\Phi_{10}(X) = (X^2 + aX + b)(X^2 + cX + d)$$

There exist θ, ζ in the algebraic closure of $\mathbb{F}_p$ s.t.

$$\begin{aligned} X^2 + aX + b &= (X - \theta)(X - \theta^p) \\ X^2 + cX + d &= (X - \zeta)(X - \zeta^p) \end{aligned}$$

Indeed, take $p = 19$ then $ord_{10}(p) = 2$ and $\Phi_{10}(X) = (X^2 + 4X + 1)(X^2 + 14X + 1) \pmod{19}$.

4 Correctness of The AKS Algorithm

4.1 Proof Overview

To prove that the AKS algorithm works we need to show that an integer n is prime if and only if the AKS algorithm outputs "Prime". The easy direction is that if n is prime then the algorithm is correct, i.e outputs "Prime" and indeed this is straightforward to see. The hard direction is proving that if n is not prime then the algorithm outputs "Composite".

Theorem 23. *If n is compositite then the AKS algorithm outputs "Composite".*

We are going to prove the contra-positive of this statement, namely that if the AKS outputs "Prime" then n is necessarily prime. Therefore, our starting point is an integer n that passes all the tests (i.e, the AKS algorithm outputs "Prime"). The proof is by contradiction - we shall assume that n is composite and reach a contradiction. To simplify things lets write down all the properties of n:

- n has at least two distinct large prime factors. That is, there exists primes $p \neq q$ such that $p, q | n$ and $p, q = \Omega(\log^5 n)$.
- For every $i = 1, 2, \ldots, \bar{r}$ it holds that $(i, n) = 1$. In particular $(n, r) = 1$.
- There exists an integer $r \leqslant \bar{r}$ such that for every $a = 1, \ldots, r$ it holds that,

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

It follows that n has two distinct prime factors since n n is composite and not a perfect power. Also, due to the fact that n passed step 2 of the algorithm, for every $i = 1, 2, \ldots, \bar{r}$ it holds that

$(i, n) = 1$. This shows that the above first two properties hold. The last property is since n passed step 5 of the algorithm. Our objective is to show if n satisfy all the above properties then this leads to a contradiction.

Henceforth n denotes a composite integer which satisfy all of the above properties and p is some (large) prime factor of n. Also, denote

$$R = \mathbb{Z}_p[X] \pmod{X^r - 1}$$

and every equality of polynomials is by default equality in the polynomial ring R (unless stated explicitly otherwise). That is, the equality $f = g$ means that there exists a polynomial $A(X) \in \mathbb{Z}[X]$ such that $f(X) = g(X) + A(X) \cdot (X^r - 1)$.

Lets start by giving an overview of the proof highlighting the key ideas. The main idea is to consider the set P of all polynomials $f \in R$ satisfying

$$f(X^n) = f(X)^n \pmod{X^r - 1, n}. \tag{1}$$

Let us explain why this is a natural thing to do. If n is prime then P is simply the set of all polynomials (as $X \to X^q$ is an automorphism of $\mathbb{Z}_q$ if q is prime). However, in our case n is not prime though it behaves like a prime in the sense that it passes all the tests, specifically that equation (1) holds for all $a = 1, 2, \ldots, r$. This immediately implies that all the polynomials $(X + a)$ for $a = 1, 2, \ldots, r$ are in the set P and possibly suggests that P is large. Indeed, we will show that this holds by showing that P satisfy some closure properties. On the other hand, we shall show that the fact that n has two distinct large prime factors implies that P cannot be too large which leads to a contradiction (as P must be large). To make this argument work we will need algebraic tools that we can apply. Unfortunately, we are not working over a field but rather over the polynomial ring $\mathbb{Z}_n[X] \pmod{X^r - 1}$ which makes life a bit harder for us. To amend this our analysis will be done in $\mathbb{Z}_p[X] \pmod{\psi(X)}$ where $\psi(x)$ is some irreducible factor of $X^r - 1$ and hence $\mathbb{Z}_p[X] \pmod{\psi(X)}$ is a field.

4.2 The Set P and Its Properties

We shall now define the set P and a more general class of sets.

Definition 24. *For every integer m define $P_m = \{f \in R \mid f(X^m) = f(X)^m \pmod{X^r - 1, p}\}$. Moreover, define $P = P_n$.*

Remark 25. *The polynomial $f(X^m)$ is obtained by substituting X^m to $f(X)$. For instance, if $f(X) = X^3 + X + 6$ and $m = 2$ then $f(X^2)$ stands for the polynomial $X^6 + X^2 + 6$.*

Claim 26. *The set P_m is well defined.*

Proof. It is not trivial that P_m is well-defined as the operation $f(X) \to f(X^m)$ may not respect the equivalence classes of R. To see that this is non-trivial we give a non-example first. Consider $f(X) = X + 1$, $g(X) = 0$ in the ring $\mathbb{Z}_n[X] \pmod{X + 1}$ then clearly $g(X), f(X)$ are both equivalent to the zero polynomial and so are $f(X)^2, g(X)^2$. On the other hand, while $g(X^2) = 0$ is also equivalent to the zero polynomial, the polynomial $f(X^2) = X^2 + 1$ is not equivalent to the zero polynomial in the ring $\mathbb{Z}_n[X] \pmod{X + 1}$. Fortunately for us, P is well defined in the polynomial

ring R. To see this, let $f = g$ in the polynomial ring R then $f(X) = g(X)+A(X)\cdot(X^r-1)+p\cdot B(X)$ for some polynomials $A(X), B(X) \in \mathbb{Z}[X]$. Thus,

$$\begin{aligned} f(X^m) &= g(X^m) + A(X^m)(X^{mr}-1) + pB(X^m) \\ &= g(X^m) + A(X^m)(X^{r(m-1)} + X^{r(m-2)} + \ldots + X^r + 1)\cdot(X^r-1) + p\cdot B(X^m) \end{aligned}$$

and so $f(X^m) = g(X^m)$ in the polynomial ring R. □

One immediate observation is:

Observation 27. *$P_p = R$.*

Another simple claim is:

Claim 28. *For every $j = 1, 2, \ldots, r$ we have $(X + j) \in P_n$.*

Proof. Let $1 \leqslant j \leqslant r$. Since n passed step 5 of the algorithm we have $(X+j)^n = X^n + j \pmod{X^r - 1, n}$. Thus,

$$\begin{aligned} (X+j)^n &= X^n + j \pmod{X^r - 1, n} \\ &= A(x)(X^r-1) + X^n + j + nB(X) \\ &= X^n + j \pmod{X^r - 1, p} \end{aligned}$$

because $p|n$. □

We now show P has a closure property:

Claim 29. *$f, g \in P_m \Rightarrow f \cdot g \in P_m$.*

Proof. Let $f, g \in P_m$ then $f(X^m) = f(X)^m \pmod{X^r - 1, p}$, $g(X^m) = g(X)^m \pmod{X^r - 1, p}$. Thus,

$$\begin{aligned} f\cdot g(X^m) \pmod{X^r-1,p} &= f(X^m)\cdot g(X^m) \pmod{X^r-1,p} \\ &= \big(f(X)\big)^m \cdot \big(g(X)\big)^m \pmod{X^r-1,p} \\ &= \big(f(X)\cdot g(X)\big)^m \pmod{X^r-1,p} \\ &= \big(f\cdot g(X)\big)\big)^m \pmod{X^r-1,p}. \end{aligned}$$

□

Corollary 30. *For any $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ we have $\prod_{j=1}^{r}(X+j)^{\alpha_j} \in P$.*

Next, we show a closure property of a different kind:

Claim 31. *$f \in P_m, f \in P_k \Rightarrow f \in P_{m\cdot k}$*

Proof. Set $Y = X^m$. Then $X^r - 1 \mid Y^r - 1 = X^{rm} - 1$

$$\begin{aligned} f(X^{m\cdot k}) \pmod{X^r - 1, p} &= f(Y^k) \pmod{Y^r - 1, p} \\ &= \big(f(Y)\big)^k \pmod{Y^r - 1, p} \\ &= \big(f(Y)\big)^k \pmod{X^r - 1, p} \\ &= \big(f(X^m)\big)^k \pmod{X^r - 1, p} \\ &= \big(f(X)\big)^{m\cdot k} \pmod{X^r - 1, p}. \end{aligned}$$

□

4.3 Projecting P To a Field

The next step in the proof is to embed $P = P_n$ in a field. To achieve this, let $\psi(X)$ be an irreducible factor of $\Phi_r(X)$ (which is a factor of $X^r - 1$). According to section 3.4 the degree of ψ equals $ord_r(p)$. Consider $\mathbb{F} = \mathbb{Z}_p[X]/\psi(X)$ which is a field extension of $\mathbb{Z}_p$ of degree $\deg(\psi) = ord_r(p)$. Note that $r \neq p$ as $(n, r) = 1$, but a-priori it is possible that $p = 1 \pmod r$ and $ord_r(p) = 1$, i.e the extension might be trivial or not. The elements of $\mathbb{F}$ can be though of as polynomials in $\mathbb{Z}_p[X]$ of degree at most $\deg(\psi) - 1$.

Next, we project the elements of $P = P_n$ to $\mathbb{F}$.

Definition 32. *Define* $P_\psi = \{f \pmod{\psi(X), p} \mid f \in P\}$.

What can one expect from this projection? Is it one-to-one? The answer is NO. The set P is infinite but the set P_ψ is finite.However, we shall soon see that it is one-to-one on a large subset of P.

Our lower and upper bounds on P_ψ will not be absolute, but rather related to a different quantity which is the size of the following set.

Definition 33. *Define* $G = \big\{i \mid i \in \mathbb{N} \wedge (i, r) = 1 \wedge \forall f \in P. f(X^i) = f(X)^i \pmod{X^r - 1, p}\big\}$.

The set G is naturally a subset of $\mathbb{N}$. However, we are more interested in working over the multiplicative group $\mathbb{Z}_r^*$, which is more natural to us as we work with polynomials modulus $X^r - 1$, and so we will project G to $\mathbb{Z}_r$ by taking all its elements modulus r.

Definition 34. *Define* $G_r = \{i \pmod r \mid i \in G\}$.

Observation 35. *Note that while G_r is naturally a subset of $\mathbb{Z}_r$ and in fact a subset of $\mathbb{Z}_r^*$ as all the elements of G are co-prime to r.*

Claim 36. *G_r is closed under multiplication.*

Proof. Let $i, j \in G_r$ then for all $f \in P$ it holds that $f(X^i) = f(X)^i \pmod{X^r - 1, p}$, $f(X^j) = f(X)^j \pmod{X^r - 1, p}$ and $(i, r) = (j, r) = 1$. We want to show that $ij \in G$ which is equivalent to showing that for any $f \in P$ it holds that $f(X^{ij}) = f(X)^{ij} \pmod{X^r - 1, p}$. Let $f \in \mathbb{Z}[X]$ then in particular $f \in P_i, P_j$. According to Claim 31 it holds that $f \in P_{ij}$. Also note that $(i, r) = (j, r) = 1$ implies $(ij, r = 1$ therefore $ij \in G_r$ as required. □

Corollary 37. *For any $i, j \in \mathbb{N}$ it holds that $n^i p^j \in G_r$.*

Proof. Using that G_r is closed under multiplication it suffices to prove that $n, p \in G$. For n this follows almost by definition as $(n, r) = 1$ and $f \in P \Rightarrow f(X^n) = f(X)^n \pmod{X^r - 1, p}$. To see that $p \in G$ first note that since $(n, r) = 1$ and $p|n$ then $(p, r) = 1$. Let $f \in \mathbb{Z}[X]$ be any polynomial then $f(X^p) = f(X)^p$ in $\mathbb{Z}_p[X]$ (Frobenius automorphism) and in particular this holds for every $f \in P$ and modulus $X^r - 1$. □

Corollary 38. $|G_r| \geqslant ord_r(n) \geqslant t_0$.

Proof. For any $1 \leqslant i \leqslant ord_r(n)$ the elements n^i are distinct in $\mathbb{Z}_r^*$ and are also in G_r due to the above corollary. □

The above corollary sheds a little on the choice of r (See step 2 of the algorithm). It is meant to ensure that $|G_r|$ is large.

Claim 39. *G_r is a subgroup of $\mathbb{Z}_r^*$.*

Proof. We showed that G_r is closed under multiplication. Clearly G_r is associative and $1 \in G_r$ unit element, thus it is left to show that G_r is closed under taking the inverse. This basically follows since $G_r \subseteq \mathbb{Z}_r^*$ is a subset of a finite group. To see this, let $g \in G$ then also $g^2, g^3, \ldots \in G_r$ since G_r is closed under multiplication. By the pigeonhole principle $g^i = g^j$ for some $i < j$ and so $g^{i-j} = 1$ (make sure you understand how the fact that G_r is a subset of a group is used). □

4.4 Proving $|P_\psi|$ Is Large

The lower bound will be proved as follows. We will first find a large set in P. Roughly speaking, this set will be the set of all polynomials of the form $\prod_{i=1}^{n}(X + i)^{j_i}$. However, recall that we are no longer interested in P but rather in P_ψ and the problem is that during the projection of P to $\mathbb{Z}_p[X] \pmod{X^r - 1}$ this set might shrink significantly. This is where G_r comes into play and it turns out that restricting our degree to be smaller than $|G_r|$ does the trick.

Definition 40. $A = \left\{(X + 1)^{j_1}(X + 2)^{j_2} \cdots (X + r)^{j_r} \in \mathbb{Z}_p[X] \mid \sum_{i=1}^{r} j_i < |G_r|\right\}$

Claim 41. $|A| = \binom{|G_r|+r-1}{|G_r|-1}$.

Proof. We first notice that the polynomials in A are indeed distinct in $\mathbb{Z}_p[x]$. This is because $\mathbb{Z}_p[x]$ is aUFD (unique factorization domain) and different polynomials in A have different factorization, because $r < p$.

Calculating the size of A is now equivalent to calculating the number of non-negative integer solutions to the inequality $\sum_{i=1}^{r} j_i \leqslant |G_r| - 1$. This is equivalent to the number of non-negative integer solutions to the equality $\sum_{i=1}^{r+1} x_i = |G_r| - 1$ (by introducing another dummy variable). Generally, an easy combinatorial argument reveals that the number of non-negative integers solutions to the equation $\sum_{i=1}^{N} x_i = K$ equals $\binom{N+K-1}{K}$ and so the claim follows by substituting $N = r + 1$ and $K = |G_r| - 1$. □

Lemma 42. *Let $f, g \in A$ such that $f \neq g$ as polynomials in R then $f \neq g$ in $\mathbb{F}$.*

Proof of Lemma 42. Let $f, g \in R$ such that $f \neq g$ and assume $f(X) = g(X)$ in $\mathbb{F}$ as field elements, f, g are equivalent as polynomials modulus $\psi(X)$ and p. Also, let $i \in G_r$ then,

$$(f-g)(X^i) = f(X^i) - g(X^i) = f(X)^i - g(X)^i = 0,$$

then X^i is a root of $(f-g)(X)$. That is, we treat f, g as polynomials in the polynomial ring $\mathbb{F}[X]$ and substitute the field elements $X^i \in \mathbb{F}$ where $i \in G_r$. Applying this to every element of G_r we obtain $|G_r|$ roots.

We now claim the roots X^i are *distinct* in $\mathbb{F}$. This is true because X is a root of ψ, and we saw before that the roots of $\psi(X)$ (or any irreducible factor of Φ_r over $\mathbb{F}_p$) are *primitive* roots of unity of order r over the algebraic closure of $\mathbb{F}_p$. Hence X^i are all distinct, as long as $i < r$, which holds because any $i \in G_r$ is an element of $\mathbb{Z}_r^*$.

Thus, we found $|G_r|$ distinct roots of $f-g$. However, $\deg(f), \deg(g) < |G| \Rightarrow \deg(f-g) < |G|$ and therefore, $f - g \in \mathbb{F}$ must be the zero polynomial in the sense that every coefficient of it is zero, or, equivalently, that $f = g$ in R. □

Lemma 43. $|P_\psi| \geqslant 2^{|G_r|-1}$.

Proof. Lemma 42 implies that the mapping $f \to f \pmod{\psi(X), p}$ from the set A to the set P_ψ is one-to-one and hence $|P_\psi| \geqslant |A|$. Also, by Claim 41 $|A| = \binom{|G_r|+r-1}{|G_r|-1}$. Since $|G_r| \leqslant r$ as $G_r \subseteq \mathbb{Z}_r^*$ we have $|G_r| + r - 1 \geqslant 2(|G_r| - 1)$ and so,

$$\binom{|G_r|+r-1}{|G_r|-1} \geqslant \binom{2(|G_r|-1)}{|G_r|-1} = \frac{|G_r| \cdot (|G_r|+1) \cdot 3 \cdots 2(|G_r|-1)}{1 \cdot 2 \cdot 3 \cdots (|G_r|-1)} \geqslant 2^{|G_r|-1}.$$

□

4.5 Proving $|P_\psi|$ Is Small

We showed an upper bound on the size of P_ψ in terms of $|G_r|$ and now we give a lower bound in terms of $|G_r|$. While proving that P_ψ is large relied on the fact that n passed all the tests, proving the upper bound relies on the fact that n has two large distinct prime factors.

Lemma 44. $|P_\psi| \leqslant n^{2\sqrt{|G_r|}}$.

Proof. We start with the following sub-claim.

Claim 45. *There exists two distinct integers $m_1 \neq m_2$ satisfying:*

- $m_1 = n^{i_1} p^{j_1}$, $m_2 = n^{i_2} p^{j_2}$ *where* $0 \leqslant i_1, j_1, i_2, j_2 \leqslant \sqrt{|G_r|}$.
- $m_1 \equiv m_2 \pmod{r}$

Proof. The proof is simply by counting. For convenience let us denote $|G_r| = s$ and note that $s \geqslant r$. There are $(\sqrt{s}+1)^2 > s \geqslant r$ of pairs (i, j) such that $0 \leqslant i, j \leqslant \sqrt{s}$ though only r elements in $\mathbb{Z}_r$. By the pigeonhole principle there must exists $0 \leqslant i_1, j_1, i_2, j_2 \leqslant \sqrt{s}$ satisfying $n^{i_1} p^{j_1} = n^{i_2} p^{j_2} \pmod{r}$ where $(i_1, j_1) \neq (i_2, j_2)$ (i.e, either $i_1 \neq i_2$ or $j_1 \neq j_2$). Thus, to conclude that $n^{i_1} p^{j_1} \neq n^{i_2} p^{j_2}$ (as integers) it suffices to prove that $n^{i_1} p^{j_1} = n^{i_2} p^{j_2}$ necessarily implies that $i_1 = i_2$, $j_1 = j_2$. To see

this recall that as n has two distinct prime factors $p \neq q$ and so $n = pq^{\alpha} \cdot n'$ where n' is co-prime to q. Thus, $n^{i_1}p^{j_1} = n^{i_2}p^{j_2}$ implies $p^{i_1+j_1}q^{\alpha i_1}(n')^{i_1} = p^{i_2+j_2}q^{\alpha i_2}(n')^{i_2}$. Using the uniqueness of the prime factorization, we have $\alpha i_1 = \alpha i_2 \Rightarrow i_1 = i_2$ (α is clearly nonzero). Cancelling $p^{i_1}q^{\alpha i_1}(n')^{i_1}$ from both sides we get $p^{j_1} = p^{j_2}$ and so $j_1 = j_2$. □

We now proceed with the proof of Lemma 44. Let m_1, m_2 as given in the above claim and consider the following polynomial $Q(X) = X^{m_1} - X^{m_2} \in \mathbb{Z}_p[X] \pmod{\psi(X)}$. Without the loss of generality assume $m_1 \geqslant m_2$. First observe that as m_1, m_2 are of the form $n^i p^j$ then by Corollary 37 it follows that $m_1, m_2 \in G_r$. Next, recall that $\mathbb{Z}_p[X] \pmod{\psi(X)}$ is a field (in fact, field extension of $\mathbb{Z}_p$) and its elements are polynomials in $\mathbb{Z}_p[X]$ modulus $\psi(X)$. This relies on the fact that $\psi(X)$ is irreducible polynomial in the polynomial ring $\mathbb{Z}_p[X]$. Also, note that $Q(X)$ is clearly nonzero as $m_1 \neq m_2$. We claim that every element of P_ψ is a root of Q. To see this, let $f \in P_\psi$ then,

$$\begin{aligned} Q(f) &= f(X)^{m_1} - f(X)^{m_2} \pmod{\psi(X), p} \\ &= f(X^{m_1}) - f(X^{m_2}) \pmod{X^r - 1, p} \\ &= f(X^{m_1}) - f(X^{m_2}) \pmod{\psi(X), p} \\ &= f(X^{m_1 \bmod(r)}) - f(X^{m_2 \bmod(r)}) \pmod{\psi(X), p} \\ &= 0. \end{aligned}$$

Note that we used that $\psi(X)$ divides $X^r - 1$ and so congruence modulus $X^r - 1$ necessarily implies congruence modulus $\psi(X)$.

Note that we consider $f \in P_\psi$ as a field element of $\mathbb{F}$ and evaluate the polynomial $Q(X) \in \mathbb{F}[X]$ at the point f. We show this turned out to be always the zero element in the field $\mathbb{F}$. As $\deg(Q) = m_1$, Q may have at most m_1 distinct roots and as every element of P_ψ is a root of Q we have $|P_\psi| \leqslant m_1$. Recall that $m_1 = n^i p^j$ where $i, j \leqslant \sqrt{s}$ then $|P_\psi| \leqslant n^{\sqrt{s}} p^{\sqrt{s}} \leqslant n^{2\sqrt{s}}$. □

4.6 Proof of Theorem 23

We now prove theorem 23.

Proof of Theorem 23. Lets assume towards contradiction that n is composite and the algorithm outputs "Prime", i.e n passes all the tests. For convenience let us denote $|G| = s$. According to Lemma 44 we have $|P_\psi| \leqslant n^{2\sqrt{s}}$. Also, according to Lemma 43 $|P_\psi| \geqslant 2^{s-1}$. Putting the two together yields,

$$2^{s-1} \leqslant n^{2\sqrt{s}} \Rightarrow s - 1 \leqslant 2\sqrt{s}\log n \Rightarrow s \leqslant 2\sqrt{s}\log n + 1,$$

and so $s \leqslant (2\log n + 1)^2 < 9\log^2 n$. On the other hand, by Corollary 38 it we have $s > 9\log^2 n$ contradiction. We conclude that there is no composite n for which the algorithm outputs "Prime". □

References

[1] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Annals of mathematics*, pages 781–793, 2004.