1 Introduction

The AKS-algorithm delivers us a primality test that can be computed in polynomial time cd^A for some positive constants c and A. d stands for the number of digits of the number n on which the AKS-primality test ist applied. The improvement of bit operations (steps) in comparision to older algorithms were brought down from $d^{c\log\log d}$ for some constant $c > 0$ to $d^{7.5}$ steps and a modification by Lenstra and Pomerance in about d^6 steps. This was also called Gauss's dream which describes an algorithm that can find prime numbers in polynomial time and puts that Problem in the **P** complexity class.

Our objective is to prove the following elegant characterization of prime numbers by Agrawal, Kayal and Saxena.

Theorem (Agrawal, Kayal and Saxena). *For given integer $n \geq 2$, let r be a positive integer $r < n$, for which n has order $> (\log n)^2 \mod r$. Then n is prime if and only if*

- *n is not a perfect power,*
- *n does not have any factor $\leq r$,*
- *$(x+a)^n \equiv x^n + a \mod (n, x^r - 1)$ for each $a \in \mathbb{Z}, 1 \leq a \leq A := \sqrt{r}\log n$*

2 Proof Steps

We start by assuming that a given number $n > 1$ is odd, not a perfect power, with no prime factor $\leq r$ and has order $d > (\log n)^2 \mod r$ such that

$$(x+a)^n \equiv x^n + a \mod (n, x^r - 1) \tag{1}$$

We know it holds for n is a prime, so we must show that they cannot hold if n is composite. We start by letting p be a prime dividing n and $h(x)$ be an irreducible factor of $x^r - 1$ to get $(x+a)^n \equiv x^n + a \mod (p, h(x))$. The congruence classes $\mod (p, h(x))$ can be viewed as elements of the ring $\mathbb{F} :\equiv \mathbb{Z}/(p, h(x))$ which is isomorphic to a field of p^m elements. This makes working with the fields much easier.
We define the following sets

$$H := \langle x + b : 1 \leq b \leq [A] \rangle \tag{2}$$

$$G := H \mod (p, h(x)) \tag{3}$$

$$S := \{k \in \mathbb{N} : g(x^k) \equiv g(x)^k \mod (p, x^r - 1), \forall g \in H\} \tag{4}$$

Now our goal is to give an upper and lower bound on the size of G to establish a contradiction, therefore showing that eq. (1) doesn't work for n composite.

2.1 Upper Bound on $|G|$

We start by proving the following lemmas

Lemma 2.1.1. If $a, b \in S$, then $ab \in S$

Lemma 2.1.2. if $a, b \in S$ and $a \equiv b \mod r$, then $a \equiv b \mod |G|$

We define R as follows. $R \leq (\mathbb{Z}/r\mathbb{Z})^\times$ and $R = \langle n, p \rangle$. Since n is not a power of p, the integers $n^i p^j$ with $i, j \geq 0$ are distinct. There are $> |R|$ such integers with $0 \leq i, j \leq \sqrt{|R|}$ and so two must be congruent $\pmod r$

$$n^i p^j \equiv n^I p^J \pmod r \tag{5}$$

By lemma 2.1.1 these integers are both in S. By lemma 2.1.2 their difference is divisble by $|G|$ and therefore

$$|G| \leq |n^i p^j - n^I p^J| \leq (np)^{\sqrt{|R|}} - 1 < n^{2\sqrt{|R|}} - 1 \tag{6}$$

We can improve this by showing that $n/p \in S$ and then replace n by $n/p \in S$ eq. (6) to get

$$|G| \leq n^{\sqrt{|R|}} - 1 \tag{7}$$

2.2 Lower bounds on $|G|$

The inital idea was to show that there are many distinct elements of G. If $f(x), g(x) \in \mathbb{Z}[x]$ with $f(x) \equiv g(x) \mod (p, h(x))$, then we can write $f(x) - g(x) \equiv h(x)k(x) \mod p$ for $k(x) \in \mathbb{Z}[x]$. If both $\deg(f)$ and $\deg(g) < \deg(h)$, then $k(x) \equiv 0 \mod p$ which implies $f(x) \equiv g(x) \mod p$. For all polynomials of the form $\prod_{1 \leq a \leq A}(x+a)^{e_a}$ of degree $< \deg(h) = m$ are distinct elements of G. Therefore if $p^m \equiv 1 \pmod r$ is large, then we can get a good lower bound on $|G|$. However proving that such r exists proves challenging and needing non-trivial tools of analytical number theory. Inspired by Lenstra and Pomerance we can replace m by $|R|$

Lemma 2.2.1. Suppose that $f(x), g(x) \in \mathbb{Z}[x]$ with $f(x) \equiv g(x) \mod (p, h(x))$ and the reductions of f and g in $\mathbb{F}$ both belong to G. If $\deg(f)$ and $\deg(g) < |R|$, then $f(x) \equiv g(x) \mod p$

We define R as follows

$$R := \langle n : n \pmod r \rangle \tag{8}$$

so $|R| \geq d$, with d being the order of $n \mod r$, which is $> (\log n)^2$ by the assumption of AKS. That gives us $|R| > (\log n)^2$. Therefore $|R| > B$, where $B := [\sqrt{|R|} \log n]$. lemma 2.2.1 implies that the products $\prod_{a \in T}(x + a)$ give distinct elements of G for every subset T of the set $\{0, 1, 2, \ldots, B\}$. This gives us

$$|G| \geq 2^{B+1} - 1 > n^{\sqrt{|R|}} - 1 \tag{9}$$

which contradicts eq. (7). That completes the proof of the theorem of AKS. So we proved by contradiction that eq. (1) doesn't work for n being composite.

3 Improvements by Lenstra and Pomerance

The core idea behind this improvement of Lenstra-Pomerance is to replace the polynomial $\Phi_r(x)$ in AKS by a certain polynomial $f(x)$ with integer coefficients of degree d and positive integer n. We say that $\mathbb{Z}[x]/(n, f(x))$ is a *pseudofield* if

a) $f(x^n) \equiv 0 \mod (n, f(x))$

b) $x^{n^d} - x \equiv 0 \mod (n, f(x))$, and

c) $x^{n^{d/q}} - x$ is a unit in $\mathbb{Z}[x]/(n, f(x))$ for all primes q dividing d

When n is prime and $f(x)$ is irreducible $\mod n$, then these criteria are all true and $\mathbb{Z}[x]/(n, f(x))$ is a field.

Theorem (Lenstra and Pomerance). *For a given $n, r \in \mathbb{Z}$, $n \geq 2$ let $d \in \mathbb{Z}$ be in $((\log n)^2, n)$ for which there exists a polynomial $f(x)$ of degree d with integer coefficients such that $\mathbb{Z}[x]/(n, f(x))$ is a pseudofield. Then n is prime if and only if*

- *n is not a perfect power,*
- *n does not have any prime factor $\leq d$,*
- *$(x + a)^n \equiv x^n + a \mod (n, f(x))$ for each $a \in \mathbb{Z}, 1 \leq a \leq A := \sqrt{d} \log n$.*

One can quickly determine if for a given f one gets a pseudofield, and if so check the criteria of the theorem. This fact gives this version of the primality test its speed.