Lecture 04

Jose Capco (jcapco@risc.jku.at)

Proposition 1. Let X be an indeterminate, $n \in 2\mathbb{N}+1$ and $a \in \mathbb{N}$ be such that $(a,n) = 1$ then n is a prime number iff $(X+a)^n = X^n + a \bmod n$ (so we are looking at an equality in $(\mathbb{Z}/n\mathbb{Z})[X]$).

Proof. "$\Rightarrow$" This follows from Fermat's little theorem and taking the binomial expansion

$$(X+a)^n = X^n + a^n = X^n + a \bmod n$$

"$\Leftarrow$" Suppose n is an odd composite and $n = p^l m$ for some $p \in \mathbb{P}$ such that $p \nmid m$ and $m \in \mathbb{N}$. The binomial expansion is explicitly written as follows

$$(X+a)^n = \sum_{i=0}^{n} \binom{n-i}{i} a^i X^{n-i}$$

So we need to show that there is a monomial other than the constant and the highest degree term X^n. Since $a \bmod n \in (\mathbb{Z}/n)^*$, it suffices to show that $\binom{n}{p} \neq 0 \bmod n$ We compute

$$\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} = p^{l-1}m\binom{n-1}{p-1}$$

So it suffices to show that $p \nmid \binom{n-1}{p-1}$. We have

$$\binom{n-1}{p-1} = \frac{(n-1)(n-2)\cdots(n-p+1)}{(p-1)!} \bmod p$$

and the above involve multiplication and divisions in $\mathbb{F}_p^*$, so this is not 0 mod p. In fact, by Wilson's Theorem, the above is just a power of $-1 \mod p$. □

As we have noted, the above cannot be used directly to efficiently test for primes. One reason is because, for large n, the number of terms in the above (expanded) polynomial is rather large as well. But we can improve on the above result, i.e. we can take the polynomial above and 'trim' it. And this is exactly what the AKS theorem is all about.

AKS Theorem. Let $n \in 2\mathbb{N}+1$ with the following properties

[1.] n is not a square or a higher power of an integer

[2.] There is an $r \in \mathbb{N}$ satisfying

(a) $(r,n) = 1$

(b) if $p \in \mathbb{P}$ is in the interval $[2, \sqrt{\phi(r)}\log_2 n]$ then $p \nmid n$

(c) the order of n in $(\mathbb{Z}/r)^*$ is greater than $\log_2^2 n$

then n is a prime number iff

$$(X+a)^n = X^n + a \bmod \langle n, X^r - 1\rangle \qquad \forall a \in [1, \sqrt{\phi(r)}\log_2 n] \cap \mathbb{N} \tag{*}$$

Now, one is able to create an algorithm for prime testing from the above theorem. One could worry whether an r with the given condition exists for a natural number $n \in \mathbb{N}$. This we will leave as an exercise

Exercise 1. Prove that for any $n \in 2\mathbb{N}+1$ we can find an $r \in \mathbb{N}$ such that $(r,n) = 1$ and the order of n in $(\mathbb{Z}/r)^*$ is greater than $\log_2^2 n$. In fact, r can be search in the interval $[1, \log_2^5 n]$

Before proving the AKS Theorem, let us first discuss how easy one could check the conditions given in the Theorem. In the beginning, one would want to know if a positive integer is a square or a higher power of another integer. There is an easy algorithm to do this. One first checks if the number, say n, is a perfect square (take the square root, round off to an integer and square to check if it yields the same number). One then finds the upper bound k for which the number could be a k-th power of an integer. This bound is $\lceil \log_2 n \rceil$. So one repeats the same procedure as for the square-root but for all i-th root for $i = 3, \ldots, k$. In fact, if prime checking is fast, we need only check for all primes i, here is a pseudocode

Algorithm 1: Check if a positive integer is a power of another integer

Input: A number $n \in \mathbb{N}$
Output: `True` if n is a square or higher power, else `False`

```
Let k := ⌈log_2 n⌉
for all prime numbers in p in [2, k] do
    Set a = Round(ᵖ√n)
    if a^p = n then
        return True
    end
end
return False
```

The above algorithm is implemented in `fast_root.py` found in the file-server of the lecture notes.

We could also ask, how easy it is to find the order of a certain number modulo n in $(\mathbb{Z}/n)^*$. Here is an algorithm (that can also be extended to check the order any element of any finite group) we provide without much explanation[1]:

Algorithm 2: Find the the order of a number mod n

Input: Two numbers $a, n \in \mathbb{N}$ such that $(a, n) = 1$ and $n > 1$
Output: A number $o \in \mathbb{N}$ such that $\mathrm{ord}(a) = o$ in $(\mathbb{Z}/n)^*$

```
Let m = φ(n) (i.e. the cardinality of (Z/n)* and set o = m
Find the factorization m = ∏_{i=1}^{k} p_i^{e_i} for distinct primes p_i and e_i ∈ N
for i = 1, ..., k do
    Set o = o/p_i^{e_i}
    Compute b = a^o
    while b ≠ 1 do
        Set b = b^{p_i} and o = o p_i
    end
end
return o
```

In `Pari` the command for finding the order of a mod n is `znorder(Mod(`a, n`))`

Let us remind ourselves of an easy result in field theory that we may use in the proof of the AKS Theorem...

Lemma 2. Let $n \in \mathbb{N}$ and K be a field of characteristic $p \in \mathbb{P} \cup \{0\}$ such that $p \nmid n$. Then $X^n - 1$ has distinct roots in a (possibly) finite extension $L \geq K$ and the roots form a cyclic group in L^* and the generator of this group (the primitive n-th root of 1) will generate L i.e. $L = K[\zeta]$ for a root ζ of $X^n - 1$.

Proof. The theorem says that a splitting field of $X^n - 1$ in K is L, this exists because the algebraic closure of K exists. In L, $X^n - 1$ is a product of linear factors. The factors cannot have a multiplicity greater than 1 because after taking the derivative the only zero of nX^{n-1} is $X = 0$,

[1] We iteratively divide $\phi(n)$ by its factors and check if the order of the number divides this

which is not a zero of $X^n - 1$, here we used the fact that the characteristic of K is coprime to n (why?). Thus there are n distinct roots for $X^n - 1$. The roots of $X^n - 1$ form a finite subgroups of L^* so we know it is cyclic (by our first lecture) and the generator of this group, say ζ, will generate all other roots. Therefore $L = K[\zeta]$. □

The ζ in the proof above is called a primitive n-th root of unity.

Proof of the AKS Theorem. We prove this theorem in five steps. For almost each step, we will define sets and give some of their properties.

For simplicity we write log for logarithm to the base 2 and denote

$$N := \lfloor \sqrt{\phi(r)} \log n \rfloor$$

One direction is clear, i.e. if n is prime then it satisfies [1.], [2.] and (*). Suppose now that n is a composite number satisfying [2.] and (*) and suppose that $p \in \mathbb{P}$ divides n outside the given interval in [2.], i.e. $p \notin [2, N]$.

Step 1.) Define

$$G := \{f \in \mathbb{F}_p[X] \,:\, f(X)^n = f(X^n) \bmod \langle X^r - 1\rangle\}$$

- G is multiplicative (or multiplicatively closed), i.e. if $f, g \in G$ then $fg \in G$. This is rather trivial. But this also tells us that any $f \in \mathbb{F}_p[X]$ is in G if it can be completely factored into linear factors of the form $X + a$ for some integer $a \in [0, N]$.
- We will prove if $f \in G$ then $f + \langle X^r - 1\rangle \subset G$: Let $g \in G$ and $f - g \in \langle X^r - 1\rangle$, then
$$f(X^n) - g(X^n) \in \langle X^{nr} - 1\rangle \Rightarrow f(X^n) - g(X^n) \in \langle X^r - 1\rangle$$
because $(X^r - 1) \mid (X^{nr} - 1)$. Thus
$$g(X)^n - g(X^n) = f(X)^n - f(X^n) \bmod \langle X^r - 1\rangle$$
In particular if $f(X) \in G$ then $f(X^n) \in G$.

Step 2.) Define

$$I := \{i \in \mathbb{N} \,:\, f(X)^i = f(X^i) \bmod \langle X^r - 1\rangle \quad \forall g \in G\}$$

then

- one easily checks that $n, p, 1 \in I$
- We will prove that I is also multiplicative: Let $i, j \in I$ and suppose $f \in G$ then
$$f^{ij}(X) = f(X^i)^j = f(X^{ij}) \bmod \langle X^r - 1\rangle$$
The first equality is because G is multiplicative, and the second is because all the polynomials in the equivalence class $f(X)^i + \langle X^r - 1\rangle$ are in G (so $f(X^i)$ is in G). Thus, $ij \in I$. Specifically $n^a p^b \in I$ for any integer $a, b \in \mathbb{N}_0$.

Step 3.) Let K be the splitting field of $X^r - 1$ extending $\mathbb{F}_p$, so we can write $K = \mathbb{F}_p[\zeta]$ for a primitive r-th root of 1. Let $H \leq (\mathbb{Z}/r)^*$ be the subgroup generated by $n \bmod r$ and $p \bmod r$ (recall $(n, r) = 1$ and $p \mid n$) and define $d := \#H$.

We now define (note for us, the 0 polynomial is also in G_d)

$$G(\zeta) := \{f(\zeta) \in K \,:\, f \in G\}$$
$$G_d := \{f \in G : \deg(f) < d\}$$

There is a natural map

$$G_d \to G(\zeta) \qquad f \mapsto f(\zeta)$$

In the next lecture we will prove that this map is injective and that $n^{\sqrt{d}} < \#G(\zeta)$

□