Lecture 05

Jose Capco (jcapco@risc.jku.at)

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

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

We continue the proof started from the last lecture ...

Continuation of Proof. In the last lecture, we assumed n is an odd composite satisfying [2.] and (*). Then we fixed a $p \in \mathbb{P}$ dividing n (so it should be outside the given interval in [2.]).

Step 1.) In the last lecture, we defined

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

and proved that

- G is multiplicative
- $f \in G \Rightarrow f + \langle X^r-1\rangle \subset G$

Step 2.) In the last lecture we defined

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

and showed that I is multiplicative. Specifically $n^a p^b \in I$ for any integer $a, b \in \mathbb{N}_0$.

Step 3.) Now 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 $p \bmod r$ and define $d := \#H$.

We define

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

Then there is a natural map

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

- We first prove that the map is one-to-one. Suppose $f, g \in G(d)$ such that $f(\zeta) = g(\zeta)$. Consider an element $k \bmod r \in H$, then k can be regarded to be of the form $n^a p^b$ (H is generated by p and n) for some $a, b \in \mathbb{N}_0$. So $k \in I$ and we have

  $$f(\zeta)^k = f(\zeta^k) = g(\zeta^k) = g(\zeta)^k$$

  Also ζ^k is distinct for any distinct k modulo r. So $f-g$ is a polynomial in $\mathbb{F}_p[X]$ of degree at most $d-1$ ($f, g, \in G(d)$) with at least d distinct zeros in

  $$\{\zeta^k \,:\, k \bmod r \in H\}$$

  This can only happen if $f = g$ (see first lecture on polynomial over fields and number of zeros).

- Now we will show that
$$n^{\sqrt{d}} < \#G(d) \leq \#G(\zeta)$$
The right inequality is clear because of the previous result. We shall argue that the following elements are in $G(d)$ and are distinct
$$f(X) = 0 \tag{i}$$
$$f(X) = \prod_{a \in [0, \sqrt{d}\log n] \cap \mathbb{N}_0} (X+a)^{i_a} \qquad i_a \in \{0,1\}, \sum i_a \leq \lfloor \sqrt{d}\log n \rfloor \tag{ii}$$
Note that (by [2.])
$$\langle n \bmod r \rangle \leq H \Rightarrow \log^2 n \leq \mathrm{ord}_r(n) \leq d$$
Thus $\sqrt{d}\log n < d$, which implies that $f(X)$ in (ii) has degree less than d. Furthermore
$$H \leq (\mathbb{Z}/r)^* \Rightarrow d \leq \phi(r)$$
guarantees that the $f(X)$'s in (ii) are in G. Notice also that the sequences (i_a) uniquely determine $f(X)$ in (ii), this is because a cannot exceed p (p is outside the interval in [2.], because it divides n) and these $f(X)$'s are uniquely determined by their zeros in $\mathbb{F}_p$. So the count for $f(X) \neq 0$ above is the same as the number of choices of sequences (i_a)'s such that not all i_a are 1. Thus, there are at least
$$1 + (2^{\lfloor \sqrt{d}\log n \rfloor + 1} - 1) > 2^{\sqrt{d}\log n} = n^{\sqrt{d}}$$
elements in $G(d)$.

Step 4.) Let $k \in \mathbb{N}$ be the degree of the field extension $K/\mathbb{F}_p$ (i.e. $[K : \mathbb{F}_p] = k$. If we know a little field theory, we also know that this is the same as the degree of the minimal polynomial of ζ)[1]. K is again a finite field and its multiplicative group has cardinality $p^k - 1$. Now, define a new set
$$J = \{j \in \mathbb{N} : \exists i \in I \twoheadrightarrow j = i \bmod (p^k - 1)\}$$
We discuss some of the properties of J

- J is (clearly) multiplicative because I is multiplicative
- One immediately also sees that, for all $j \in J$ and $f \in G$ we have $f(\zeta)^j = f(\zeta^j)$: There is an $i \in I$ such that $j = i + m$, where m is a multiple of $p^k - 1$. So
$$\zeta^j = \zeta^{i+m} = \zeta^i \zeta^m = \zeta^i$$
$$f(\zeta)^j = f(\zeta)^{i+m} = f(\zeta)^i f(\zeta)^m = f(\zeta^i) = f(\zeta^j)$$
Note that the above also holds even if $f(\zeta)$ is 0.
- We will prove that n/p is in J: n and p are in I , which is multiplicative. Thus, $np^{k-1} \in I$ and because
$$np^{k-1} - \frac{n}{p} = \frac{n}{p}(p^k - 1) \in \mathbb{Z}(p^k - 1)$$
we have proven that $\frac{n}{p} \in J$.

Step 5.) We will now be able to finally prove the theorem. Recall that $H = \langle n, p \rangle$ in $(\mathbb{Z}/r)^*$ and $\#H = d$. Clearly $\frac{n}{p} \bmod r \in H$. Also note that there are more than d pairs in $\mathbb{N}_0^2 \cap [0, \sqrt{d}]^2$. So

[1] characteristic p is a bit tricky because cyclotomic polynomials are not necessarily irreducible. For instance $\Phi_3(X) = X^2 + X + 1 = X^2 - 2X + 1 = (X-1)^2 \bmod 3$

there are distinct integer pairs $(a_1, b_1), (a_2, b_2)$ in this set such that if we set $j_1 = p^{a_1}(n/p)^{b_1}$ and $j_2 = p^{a_2}(n/p)^{b_2}$ then $j_1 = j_2 \bmod r$. Thus $\zeta^{j_1} = \zeta^{j_2}$ and since $j_1, j_2 \in J$ we have

$$f(\zeta)^{j_1} = f(\zeta)^{j_2} \quad \forall f \in G$$

In particular, all the elements in $G(\zeta) \subset K$ are zeros of the polynomials $x^{j_1} - x^{j_2}$. However, we know that

$$j_1, j_2 \leq n^{\sqrt{d}}$$

and yet we have $\#G(\zeta) > n^{\sqrt{d}}$ zeros. This can only happen if $j_1 = j_2$ and we easily concludes that this implies that

$$n^{b_1 - b_2} = p^{b_1 - b_2 + a_2 - a_1}$$

which means that n has only p in its prime factorization. Since we assumed n is composite, we can conclude that n is p^2 or a higher power of p, i.e. [1.] is not satisfied.

□

Assume $n \in \mathbb{N}$ is an odd composite natural number. We want to factorize this integer. In the course we will discuss four methods. Two naive methods and two serious ones that are based on the naive methods.

Before describing these methods, we might want to look at some definitions that will be used to analyse them

Definition. Let $n \in \mathbb{N}$ and $B \in \mathbb{R}$ be a positive number then

- n is said to be *B-smooth* if for all $p \in \mathbb{P}$ such that $p \mid n$ one has $p \leq B$
- n is said to be *B-power-smooth* if for all $p \in \mathbb{P}$ if $p^e \mid\mid n$ then $p^e \leq B$
- If we say a number is *smooth* or a *power-smooth* we mean it for certain unspecified B. Also we use the following notation for $x \in \mathbb{N}$

$$\psi(x, B) := \#\{n \in \mathbb{N} : n \leq x, n \text{ is } B\text{-smooth}\}$$

One thing that one easily notices is that B-smooth numbers are not bounded, however B-power-smooth numbers are bounded. Namely, they are the numbers bounded by (and dividing) $\operatorname{lcm}(2, 3, \ldots, \lfloor B \rfloor)$. Whether we work with B-smooth or B-power-smooth numbers, we tend to choose B in such a way that prime factorization and prime recognitions for all numbers less than B are "cheap", i.e. we often assume that even trial division is not costly for these numbers. In practice, if B has $1/3$ or less digits than n then we say/hope we can recognize B-smooth numbers (this is the part of the lectures where there is more heuristics than actual proofs).

The most naive way of testing prime numbers and prime factorization is by the Eratosthenes sieve below are two tables that shown in the next page

		$\sqrt{n}$						n
2	3	4	5	6	7	8	9	10
1	1	0	1	0	1	0	1	0
	1	0	1	0	1	0	0	0

Table 1: Eratosthenes sieve of prime numbers up to $n = 10$

		$\sqrt{n}$	$\frac{n}{2}$					n
2	3	4	5	6	7	8	9	10
2	1	(2^2)	1	2	1	(2^3)	1	2
	3	(2^2)	1	$(2 \cdot 3)$	1	(2^3)	(3^2)	2
			5	$(2 \cdot 3)$	7	(2^3)	(3^2)	$(2 \cdot 5)$

Table 2: Eratosthenes sieve of factorization up to $n = 10$

Exercise 1. Write an algorithm that modifies Eratosthenes sieving algorithm to get B-smooth numbers up to n for given B and n.

Remark 1. There are some very non-trivial estimates for the ration $\frac{\psi(x,x^{1/u})}{x}$ for $x \in \mathbb{N}$ and positive $u \in \mathbb{R}$. For instance

- Dickmann and later de Bruijn have estimated

$$\frac{\psi(x, x^{1/u})}{x} \sim u^{-u}$$

  for sufficiently large x and with the assumption that $1 \leq u \leq (\log x)^{3/8-o(1)}$.

- In the book *Mathematics of Paul Erdős*, Pomerance and Konyagin showed that for a positive real number $u \in \mathbb{R}$ and a number $x \in \mathbb{N}$ such that $x \geq 4$ and $2 \leq x^{1/u} \leq x$ one has

$$\psi(x, x^{1/u}) \geq \frac{x}{\ln^u x}$$

- Using the inequality of Pomerance and Konyagin one can prove the exercise below and this eventually helps to prove that the Miller-Rabin test for $n \in 2\mathbb{N} + 9$ is deterministic if we look for all strong pseudo-primes bases below $2\ln^2(n)$ and if we assume that a generalized form of Riemann hypothesis is true.

Exercise 2. In the Miller-Rabin test, the set of (composite witnesses) for an odd composite n is

$$\{a \in \mathbb{N} : 1 \leq a < n \text{ and } a \text{ does not satisfy } (*)\}$$

where $(*)$ is the criterion for a in the Miller-Rabin test (see Lecture 02). The minimum number in this set is called the *least witness* for n and denoted $w(n)$. For most numbers $w(n) = 2$. Use the second item in the above remark (inequality of Pomerance and Konyagin) to prove a result of Granville:

If a composite odd number n is not square-free (so there is a prime $p \in \mathbb{P}$ such that $p^2 \mid n$) then $w(n) < \ln^2 n$.