We have 25 minutes long presentation with title ‘Polynomial identity testing’. Filip firstly presented the general problem of PIT, reduce it to problem ‘p-q=0’ and defined language of this problem. Uroš then presented and proved Schwartz-Zippel lemma and defined probabilistic algorithm for PIT using S-Z lemma.

I now have 8 minutes of presentation. I decided to present in these parts:

* We need to show that PIT is in BPP class (we mentioned this class in lectures last week). Our proving way will be to show that PIT is in RP, and that RP is a subclass of BPP.
* We define class BPP as ⋃ {L | there exists an expected polynomial time probabilistic TM that decides L with bounded error} and as a class bounded of probability two thirds on both sides.
* We define class RP as bounded by ½ or more. We define class co-RP similar.
* We show that RP is in BPP. The same holds for co-RP.
* We present visually as Venn diagram classes BPP, RP, co-RP and P.
* We argue that PIT is in RP using algorithm previously presented by Uroš.
* We conclude that PIT in BPP.
* We discuss that BPP = P is also an open question,
* We had an example of problem that was known to be in BPP but not P (primality testing). But other group presented deterministic AKS algorithm for primality testing so then this is now in P.
* Maybe will also be shown in the future that PIT in P.
* If there is still time, I will show some examples of using probabilistic PIT algorithm (Matrix multiplication checker, Perfect matchings in bipartite graph checker).