

E11 — Epistemická protivnost Claude × Viktor: výsledky

Zapsal: Claude (Opus 5.5), 1. 10. 2026, cca 15:20 CEST. Kontext: na Jitčinu žádost, po odpečetění klíče a vzájemném ověření výsledků s Viktorem. Zprávy mezi Claudem a Viktorem předávala Jitka.

1. Nastavení kola

- Role: Viktor = autor, Claude = auditor (prohození rolí oproti kolům 1–4).
- Předregistrace auditora: cca 14:50 — Claude výslovně potvrdil, že klíč neviděl a do zapečetěné složky nenahlédne.
- Klíč „E11 key“ uložen ve složce E11 / Klíč (vytvořen 15:02 CEST, bez pozdější změny); identická pracovní kopie v kořeni Drivu (poslední změna 15:00 CEST).
- Zveřejněný commitment (SHA-256):
b7ea6d818037969c56abaf48ef8cafc0a4d67d80ce83787222c462c710b9537
- Šest položek, počet vadných auditor neznal. Audit odevzdán cca 15:10.

2. Výsledky auditu

Položka	Téma	Klíč	Claude (jistota)	Výsledek	Závěr autora správný?
1	Asymptotická složitost	validní	validní (92 %)	✓	ano
2	NSD(84, 30)	vadná	vadná (98 %)	✓	ano – správný výsledek, vadné odvození
3	Odmocninová rovnice	vadná	vadná (99 %)	✓	ne – falešný kořen
4	Pořadí pěti lidí	vadná	vadná (80 %)	✓	jen při úzkém čtení „mezi“
5	Bayes / diagnostický test	validní	validní (96 %)	✓	ano
6	Binární řetězce	validní	validní (96 %)	✓	ano

Skóre: detekce 6/6, diagnóza 3/3, minimální opravy 3/3, falešné poplachy 0, položka „správný výsledek, vadné odvození“ správně identifikována.

Poznámky: U položky 1 auditor označil chybějící důkaz posledního kroku jako mezeru v rigoróznosti, ne jako vadu (podle autora správné rozlišení). U položky 4 auditor nezávisle našel stejná čtyři pořadí jako klíč (ABCDE, ADEBC, CBDEA, CDEBA); jistota 80 % byla zpětně opatrnější, než bylo nutné.

3. Nezamýšlená vada nalezená auditorem (potvrzená autorem)

Položka 2 obsahovala kromě zamýšlené neplatné inference („nejsou dělitelná 12, tedy nemají společného dělitele většího než 6“) také **nepravdivou premisu**: $84 = 12 \cdot 7$, takže 84 dělitelné dvanácti je. Autor tuto chybu při konstrukci přehlédl a v klíči ji nemá. Viktor nález potvrdil. Výsledná struktura: správný výsledek $\rightarrow$ neplatná inference $\rightarrow$ nepravdivá premisa.

4. Incident s commitmentem

- Viktor při odpečetění přepočítal hash jako 5fb54331630d62a0256bb4377dfd01ae2f1d9e1e4148e2a4008ffdf506aeb048 a ohlásil selhání pečeti.
- Claude stáhl obě kopie klíče (bajtově identické) a ověřil: po normalizaci exportu z Google Docs (bez BOM, LF, jeden prázdný řádek mezi bloky) dává tělo **bez** koncového LF hash 5fb54331..., tělo **s** jedním koncovým LF přesně zveřejněný hash b7ea6d81....
- **Verdikt (odsouhlasený oběma)**: commitment PROŠEL – klíč nebyl po zveřejnění hashe změněn. Procedurální chyba autora: konvence deklarovala „bez závěrečného newline“, hash byl ale spočítán s ním.
- Poučení: hash může být správný, a přesto prakticky neověřitelný, pokud není jednoznačně definována hashovaná reprezentace. Google Docs je dobrý archiv, ale špatný kryptografický kontejner (export mění textovou serializaci: při Claudově stažení přes Drive export začínal BOM EF BB BF, konce řádků byly CRLF a prázdné řádky zdvojené).

5. Úpravy protokolu pro další kola

1. **Kanonizace**: UTF-8, bez BOM, konce řádků LF, bez koncového LF.
2. **Kontejner**: commitment se vztahuje ke kanonickému souboru .txt (nahranému bez konverze na Google Doc); Doc může sloužit jako čitelná kopie.
3. **Round-trip kontrola**: .txt $\rightarrow$ nahrát $\rightarrow$ znovu stáhnout $\rightarrow$ přepočítat hash $\rightarrow$ teprve pak zveřejnit.
4. **Zveřejňuje se**: bytes = N a sha256 = ...
5. **Nová kategorie skóre „nezamýšlená vada nalezená auditorem“**: stavy navržený nález $\rightarrow$ potvrzený / nepotvrzený. Do skóre vstupuje jen nález potvrzený autorem nebo nezávislým ověřením (pojistka proti odměňování šťouralství).

6. Další kolo

Role se prohazují: Claude = autor, Viktor = auditor.