Rámcové okruhy ke zkoušce z Elementární teorie čísel (M6520)

1. Dělitelnost a její základní vlastnosti, gcd, základní věta aritmetiky
2. Prvočísla, jejich vlastnosti a rozložení v $\mathbb{N}$, prvočíselná věta
3. Základní vlastnosti kongruencí
4. Aritmetické funkce – Eulerova funkce, Möbiova funkce, σ, τ
5. Eulerova funkce, Eulerova věta, úplná a redukovaná soustava zbytků, RSA
6. Řád čísla a jeho vlastnosti, primitivní kořeny a jejich existence, Diffie-Hellman
7. Lineární kongruence a jejich soustavy, Čínská zbytková věta
8. Polynomiální kongruence, Henselovo lemma, kongruence modulo prvočíslo, Wilsonova věta
9. Binomické kongruence a primitivní kořeny – věta o řešitelnosti binomických kongruencí, existence primitivních kořenů
10. Kvadratické kongruence a Legendreův symbol – Legendreův a Jacobiho symbol a jejich vlastnosti, Gaussovo lemma, zákon kvadratické reciprocity, Rabinův kryptosystém
11. Výpočetní aspekty teorie čísel – složitost elementárních operací, binární umocňování, složitost rozkladu na prvočísla
12. Testování složenosti (příp. prvočíselnosti)
13. Základy asymetrické kryptografie, šifrování a podepisování, výměna klíče, kryptosystémy RSA, ElGamal, Diffie-Hellman
14. Diofantické rovnice – lineární a příbuzné, využití nerovností
15. Diofantické rovnice – metoda rozkladu, Pythagorova rovnice, zmenšování *ad absurdum*

Důkazy vět, které budou požadovány pouze po těch, kdo aspirují na „A“

1. Věta 12 (Euler) – Řada převrácených hodnot prvočísel diverguje
2. Věta 24 – Henselovo lemma
3. Věta 29 a pomocná lemmata a tvrzení – existence primitivních kořenů
4. Věta 32 – Zákon kvadratické reciprocity

Znalost ostatních důkazů se očekává od všech studentů!