Елементарна теорија бројева 2024./2025.

Све референце су из уџбеника

- Владимир Мићић, Зоран Каделбург, Душан Ђукић: Увод у теорију бројева, Материјали за младе математичаре, Свеска 15, Друштво математичара Србије, Београд, 2004.

и све референце се односе на теорију из поменутих глава. Поред тога, књига садржи и доста урађених примера, наравно не очекујем да их знате напамет, али је свакако препоручљиво погледати их ради бољег разумевања теорије.

Док траје блокада прочитати:

- Први двочас (18.-21.2.): **Глава 1 - Дељивост целих бројева**

  Ова глава је обнављање основних средњошколских појмова као што су дељивост, НЗД и НЗС, дељење са остатком и Еуклидов алгоритам.

- Други двочас (24.-28.2.): **Глава 2 - Прости бројеви** до Примера 3

  Посебно обратити пажњу на Теореме 1 и 4. Урадити Задатак 5 (детаљније решење се може наћи у Башићевим матријалима **tb03.pdf, Теорема 3.7**)

- Трећи двочас (3.-7.3.): део **Главе 3 - Конгруенције**, поднаслови **Релација конгруенције** и **Системи остатака**

  Треба разумети разлику између потпуног и сведеног система остатака. Посебно обратити пажњу на Ојлерову функцију φ и Ојлерову теорему. Поред тога, научити и идентитет $\sum_{d|n} \varphi(d) = n$ са линка

  https://proofwiki.org/wiki/Sum_of_Euler_Phi_Function_over_Divisors

  Напомена: 3. и 4. двочас су мало обимнији, али је зато 5. двочас кратак и елементаран. Ово је више подела по тематским целинама, а ви можете сами неки део оставити за наредну седмицу.

- Четврти двочас (10.-14.3.): део **Главе 3 - Конгруенције**, поднаслови **Поредак броја по модулу**, **Вилсонова теорема** и **Доказ егзистенције примитивног корена по простом модулу**

  За оне који су слушали курс алгебре: поредак броја по модулу = ред елемента у мутипликатвиној групи остатака, примитивни корен = генератор групе.

- Пети двочас (17.-21.3.): део **Главе 4 - Диофантове једначине**, поднаслови **Линеарне Диофантове једначине** и **Систем линеарних конгруенција**

- Шести и седми двочас (24.3.-4.4.): део **Главе 5 - Квадратне конгруенције**, поднаслови **Квадратне конгруенције по простом модулу** и **Квадратне конгруенције по сложеном модулу**

Циљ ове главе је да се установи брз критеријум за испитивање да ли квадратна конгруенцијска једначина има решења или не (без решавања те једначине). Најважнији резултат је Гаусов закон квадратног реципроцитета (Гаусова златна теорема) која даје везу између решивости једначина $x^2 \equiv p \pmod{q}$ и $x^2 \equiv q \pmod{p}$, за непарне просте бројеве p и q.

- Осми и девети двочас (7.-17.4.): **Глава 7 - Раширења прстена целих бројева**

  Раширења поља сте имали на алгебри, ово је један специјални случај: раширења поља рационалних бројева степена 2, позната као квадратна бројна поља. У оквиру ових поља се посматрају алгебарски цели бројеви, који су аналог целих бројева у $\mathbb{Q}$.

  Теорему 10 можете прескочити.

  На почетку последњег поднаслова **Аритметика у другим квадратним раширењима** је наведено тврђење без доказа. Погледати доказ на линку

  https://planetmath.org/integralbasisofquadraticfield

- Десети двочас (23.-25.4.): Из материјала професора Башића последње предавање **tb13.pdf**, само поднаслов **Представљање збиром два квадрата**

  Кључно је Тврђење 13.2 (Фермаова теорема), све остало је припрема за то тврђење. (Кога занима можете информативно погледати и остатак документа са представљањем збиром три или четири квадрата. Слично имате и на крају Главе 5 у књизи.)

- Једанаести и дванаести двочас (две радне суботе): Обнављање