

**Seminarske teme za predmet Seminar 2**  
**Pedagoška matematika, 4. letnik**  
**Študijsko leto 2010/11**

Vir: Judith D. Sally, Paul J. Sally, Jr., *Roots to Research, A vertical development of mathematical problems*, poglavje 2, AMS, 2007.

1. tema: **Pravokotni trikotniki in pitagorejske trojice**

Nekaj različnih dokazov Pitagorovega izreka, obrat Pitagorovega izreka, posplošitve, nepravokotni trikotniki, Pappusov izrek, pitagorejska enačba, primitivne pitagorejske trojice in njihove lastnosti, osnovni izrek, naloge.

2. tema: **Vsote dveh kvadratov**

Wilsonov izrek, mali Fermatov izrek in Dirichletovo načelo, potrebni pogoji, da je liho število vsota dveh kvadratov, zadostni pogoji za vsoto dveh kvadratov, izrek za praštevila, splošni izrek o vsoti dveh kvadratov, hipotenuze pravokotnih trikotnikov, racionalni pravokotni trikotniki, Lagrangev izrek o vsoti štirih kvadratov, naloge.

3. tema: **Število reprezentacij v obliki vsote dveh kvadratov**

Praštevila imajo eno reprezentacijo, konstrukcija netrivialnega delitelja pri številu z dvema reprezentacijama, Gaussova cela števila, izrek o številu reprezentacij, celoštevilске točke na krožnici s polmerom  $\sqrt{n}$ , Leibnizova vrsta za  $\pi$ , naloge.

4. tema: **Kongruentna števila**

Definicija in osnovne ugotovitve, karakterizacija kongruentnih števil s primitivnimi pitagorejskimi trojicami, tabela, karakterizacija kongruentnih števil z aritmetičnim zaporedjem.

5. tema: **Nekatera nekongruentna števila**

Ploščina racionalnega pravokotnega trikotnika ni nikoli kvadrat ali dvojni kvadrat, števili 1 in 2 nista kongruentni, rešitev nekaterih diofantskih enačb, kolobar  $\mathbb{Z}[\sqrt{2}]$ , število 3 ni kongruentno število, naloge.

6. tema: **Eliptične krivulje**

Projektivna ravnina, homogene koordinate in homogeni polinomi, ničelne množice, sekante in tangente na kubično krivuljo, presek krivulje s premico, Bezoutov izrek.

**7. tema: Racionalne točke na eliptični krivulji**

Nova karakterizacija kongruentnih števil, definicija grupne strukture na eliptični krivulji, abelova grupa racionalnih točk na eliptični krivulji.

**8. tema: Eliptične krivulje nad  $\mathbb{Q}$  in nad končnimi obsegi**

Struktura abelove grupe, Mordellov izrek o končni generiranosti grupe  $E_n(\mathbb{Q})$ , število  $\mathbb{F}_q$ -točk na  $E_n(\mathbb{F}_q)$ , injektivnost naravne preslikave, Dirichletov izrek o praštevilih v aritmetičnem zaporedju.

**9. tema: Eliptična krivulja in kongruentna števila**

Torzijska podgrupa v  $E_n(\mathbb{Q})$  ima red 4, karakterizacija kongruentni števil, izrek Tunnella, domneva Bircha in Swinnerton-Dyerja.