Uvod u aritmetiku eliptičkih krivulja - seminarske teme.

1. Singularne kubične krivulje.
Osnovna literatura: [S-T], str. 99-102, zad. 3.10 i 3.11.
Dodatna literatura: [W], str. 55-59, [Kn], str. 77-79.

2. $\mathbf{Q}(E[3])$ za $E : y^2 = x^3 + x$.
Osnovna literatura: [S-T], str. 191.
Dodatna literatura: Po volji.

3. Torzijske grupe za specijalne krivulje.
Osnovna literatura: [Kn], str. 148-150. i 130-134.
Dodatna literatura: [S-T], str. 49-57, 121-125.

4. Endomorfizmi eliptičkih krivulja.
Osnovna literatura: [W], str. 46-54.
Dodatna literatura: Po volji.

5. Torzijske točke i djelitbeni polinomi.
Osnovna literatura: [W], str. 76-82 i 73-76.
Dodatna literatura: [S-T], zad. 6.4 i 6.5.

6. Opća Weiestrassova jednadžba.
Osnovna literatura: [Kn], str. 56-67.
Dodatna literatura: [Si], str. 46-52.

7. Minimalna jednadžba.
Osnovna literatura: [Kn], str. 290-294.
Dodatna literatura: [Si], str. 223-227.

8. Eliptičke krivulje u karakteristici 2 i 3.
Osnovna literatura: [W], str. 44-45 i [Si], str. 324-327.
Dodatna literatura: Po volji.

Napomene. (i) Teme 1., 2. i 3. nezavisne su medjusobno i nezavisne su od ostalih tema i mogu se držati bilo kada. Temu 2. treba prezentirati do najsitnijih detalja.
(ii) Teme 4. i 5. čine cjelinu i bilo bi dobro da se drže jedna za drugom. Dio koji se odnosi na karakteristiku 2 (a i 3) može se izostaviti ili samo spomenuti. U 5. ne treba dokazivati Teorem 3.6. (dokaz je na str. 288-289), već samo komentirati.
(iii) Teme 6., 7. i 8. su cjelina i najprije treba držati temu 6., a za 7. i 8. nije bitan redoslijed.
(iv) Za obradu pojedinih tema, katkad će trebati dijelovi teksta iz literature koji su izvan navedenih stranica, na primjer zadatci ili su tvrdnje koje se dokazuju formulirane ranije.
(v) Sva literatura postoji u matematičkoj knjižnici (ili kod prof. Dujelle).
(vi) Teme treba pripremiti za izlaganje u trajanju do 90 minuta; ako je gradivo preopsežno za to vrijeme, treba voditi računa da se jasno formuliraju definicije i tvrdnje, i da se dade skica i logička struktura dokaza, s probranim detaljima.
(vii) Sastavni dio seminara je seminarska radnja koju mi prije izlaganja treba poslati na uvid.

Literatura:

[Kn] A.W. Knapp, Elliptic Curves, Princeton University Press.

[Si] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag.

[S-T] J.H. Silverman, J. Tate, Rational Points on Elliptic Curves, Springer.

[W] L.C.Washington, Elliptic Curves, number theory and criptography, Chapman and Hall.

Ivica Gusić
igusic@fkit.hr