

|   |   |                 |                     |   |       |       |
|---|---|-----------------|---------------------|---|-------|-------|
| Studijski program   | Vrste studija ( ciklus)   |                 |                     | III ciklus                              |       |       |
|   | Naziv studijskog programa   |                 |                     | Matematičke nauke u jugoistočnoj Evropi |       |       |
| <b>PREDMET</b>  |   |                 |                     |   |       |       |
| Naziv predmeta  | <b>Konačna polja i primjene</b>   |                 |                     |   |       |       |
| Šifra predmeta  | Semestar  | Status predmeta | ECTS                | Kontakt sati                            |       |       |
| PMAT 615  | I   | <b>izborni</b>  | 10                  | 30                                      |       |       |
| Cilj predmeta   | Cilj je upoznati student sa teroijom konačnih polja i njihovim primjenama u teoriji kodiranja, kriptologiji i sl., tako da student budu sposobni da primjenjuju ovu oblast u praksi i da budu sposobni da vrše dalja istraživanja iz ove oblasti. |                 |                     |   |       |       |
| <b>SADRŽAJ PREDMETA</b>   |   |                 |                     |   |       |       |
| <ul style="list-style-type: none"> <li>• Struktura konačnih polja</li> <li>• Polinomi nad konačnim poljima</li> <li>• Jednačine nad konačnim poljima</li> <li>• Faktorizacija polinoma</li> <li>• Eksponencijalne sume</li> <li>• Permutacioni polinomi</li> <li>• Linearni rekurentni nizovi</li> <li>• Primijene u kombinatorici, teoriji kodiranja i pseudoslučajnim brojevima.</li> </ul> |   |                 |                     |   |       |       |
| <b>LITERATURA</b>   |   |                 | <b>OCJENJIVANJE</b> |   |       |       |
| [1.] Lidl, Niederreiter, Finite Fields and Their Applications, Encyclopedia of mathematics, Vol 20<br>[2.] Finite Fields, D. Jungnickel, Wissenschaftsverlag, 1993<br>[3.] Handbook of Finite Fields, Gary L. Mullen, Daniel Panario, Chapman and Hall/CRC, 2013.   |   |                 | Kriterij            |   | Poeni | Uslov |
|   |   |                 | 1.                  | Zadaće                                  | 30    | 17    |
|   |   |                 | 2.                  | Projekt                                 | 20    | 13    |
|   |   |                 | 3.                  | Završni ispit                           | 50    | 25    |
|   |   |                 | Ukupno              |   | 100   | 55    |