ELIPTIČKE KRIVULJE - SEMINARSKE TEME

1. Od opće kubike do Weierstrassove forme ([2, Section 1.4])
2. Eliptičke krivulje nad poljem kompleksnih brojeva ([5, Chapter III])
3. Torzijska grupa ([6, Chapter II])
4. Mordellov teorem ([6, Chapter, III])
5. Weilovo i Tate-Lichtenbaumovo sparivanje ([7, Chapter 3])
6. Kompleksno množenje ([7, Chapter 10])
7. Cjelobrojne točke na eliptičkim krivuljama ([6, Chapter V])
8. Konačna polja ([4, Section II.1])
9. Aritmetika binarnih polja ([3, Section 2.3])
10. Zbrajanje točaka u projektivnim koordinatama ([3, Section 3.2])
11. Frobeniusov razvoj ([1, Section IV.3])
12. Koblitzove krivulje ([3, Section 3.4])
13. MOV napad ([1, Section V.2]
14. Napad na anomalne krivulje ([1, Section V.3])
15. Pollardova ρ metoda za problem diskretnog logaritma ([1, Section V.5])
16. Generiranje krivulja pomoću kompleksnog množenja ([1, Chapter VIII[)
17. Hipereliptički kriptosustavi ([1, Chapter X])

LITERATURA

[1] I. Blake, G. Seroussi, N. Smart: *Elliptic Curves in Cryptography*, Cambridge University Press, Cambridge, 1999.

[2] I. Connell: *Elliptic Curve Handbook*, McGill University, 1999.
`http://www.math.mcgill.ca/connell/public/ECH1/`

[3] D. Hankerson, A. Menezes, S. Vanstone: *Guide to Elliptic Curve Cryptography*, Springer-Verlag, New York, 2004.

[4] N. Koblitz: A Course in Number Theory and Cryptography, Springer-Verlag, Berlin, 1994.

[5] J. S. Milne: Elliptic Curves, BookSurge Publishers, 2006.
`http://www.jmilne.org/math/Books/ectext.html`

[6] J. H. Silverman, J. Tate: *Rational Points on Elliptic Curves*, Springer-Verlag, Berlin, 1992.

[7] L. C. Washington: *Elliptic Curves: Number Theory and Cryptography*, CRC Press, Boca Raton, 2003.