**Prijedlog tema diplomskih radova:**

**Prosti brojevi**

Literatura:

1. G. A. Jones, J. M. Jones, Elementary Number Theory, Springer-Verlag, London, 2004.
2. Pete L. Clark, *Number Theory: A Contemporary Introduction*, [http://math.uga.edu/~pete/4400FULL.pdf 3](http://math.uga.edu/~pete/4400FULL.pdf%203)
3. S. P. Glasby, *Six proofs of the infinity of primes,*

<http://www.cwu.edu/~glasbys/INFINITY.PDF>

1. Gérard P. Michon*, The Set of Primes*, <http://www.numericana.com/answer/primes.htm>
2. *The Prime pages*, <http://primes.utm.edu/index.html>

**Pseudoprosti brojevi**

Literatura:

1. [A. Dujella, *Teorija brojeva u kriptografiji*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta)](http://www.mathos.unios.hr/uutb/Materijali/utblink.pdf).
2. A. Jurasić, M. Rukavina, *Pseudoprosti brojevi*, Matematičko fizički list **62** (2011), 20**-**25.
3. G. A. Jones, J. M. Jones, Elementary Number Theory, Springer-Verlag, London, 2004.
4. M. Križek, F. Luca, L. Somer, *17 Lectures on Fermat Numbers*, CMS, Springer-Verlag, New York, 2001.

***Lucasovi i Fibonaccijevi brojevi***

Literatura:

1. V. E. Hoggatt, Jr., *Fibonacci and Lucas Numbers,* Houghton Mifflin Company, 1969. (<http://www.fq.math.ca/fibonacci-lucas.html>)
2. M. Gardner*, Mathematical Circus,* MAA, Washington, 1992.
3. W. L. McDaniel, Pronic Lucas Numbers, Fib. Quart. **36(**1998), 56-59.
4. W. L. McDaniel, Pronic Lucas Numbers, Fib. Quart. **36(**1998), 60-62.

**Brojevne i polinomijalne kongruencije**

Literatura:

1. [A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta)](http://www.mathos.unios.hr/uutb/Materijali/utblink.pdf).
2. R. A. [Mollin*,*](http://math.ucalgary.ca/profiles/101-152961)  [*Fundamental Number Theory with Applications*](http://math.ucalgary.ca/research/publications/view/101-154064)*,* CRC Press, New York, 2008.
3. G. A. Jones, J. M. Jones, Elementary Number Theory, Springer-Verlag, London, 2004.

**Primitivni korijeni i kvadratni ostaci**

Literatura:

1. [A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta)](http://www.mathos.unios.hr/uutb/Materijali/utblink.pdf).
2. G. A. Jones, J. M. Jones, Elementary Number Theory, Springer-Verlag, London, 2004.
3. R. A. [Mollin*,*](http://math.ucalgary.ca/profiles/101-152961)  [*Fundamental Number Theory with Applications*](http://math.ucalgary.ca/research/publications/view/101-154064)*,* CRC Press, New York, 2008.

**Verižni razlomci i primjene**

Literatura:

1. [A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta)](http://www.mathos.unios.hr/uutb/Materijali/utblink.pdf).
2. A. Dujella, M. Maretić, Kriptografija, Element, Zagreb, 2007 .
3. A. Dujella, *Verižni razlomci i problem kalendara*, Matematika i škola **I** (1999), 74-77.
4. T. Andrescu, T. Andrica, *An Introduction to Diophantine Equations,* GIL Publishing House*,* Zalau, 2002.
5. C. D. Olds, Continued Fractions, Random House, New York, 1963.

**Eliptičke krivulje nad poljem racionalnih brojeva**

Literatura:

1. [A. Dujella, *Algoritmi za eliptičke krivulje*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta)](http://www.mathos.unios.hr/uutb/Materijali/utblink.pdf).
2. J. H. Silverman*, Rational Points on Elliptic Curves*, Springer, New York, 1992.
3. S. Schmitt, H. G. Zimmer, *Elliptic Curves – A Computational Approach*, Walter de Gruyter, Berlin – New York, 2003.

***Kvadratna polja***

Literatura:

1. [A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta)](http://www.mathos.unios.hr/uutb/Materijali/utblink.pdf).
2. I. Gusić, *Ideja jednoznačne faktorizacije I,* math.e**13,** prosinac 2008.
3. K. Conrad, *Factoring in quadratic fields*, <http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/quadraticundergrad.pdf>

**Prijedlog tema završnih radova:**

***Elementarne metode za rješavanje diofantskih jednadžbi***

Literatura:

1. T. Andrescu, T. Andrica, *An Introduction to Diophantine Equations,* GIL Publishing House*,* Zalau, 2002.
2. K. Burazin, [*Nelinearne diofantske jednadžbe*](http://www.mathos.unios.hr/~kburazin/papers/diofantske.pdf)*,* Osječki matematički list 7 (2007), 11-21.

***Zanimljivi brojevi***

Literatura:

1. [C. K. Caldwell](C.%20K.%20Caldwell), *The Prime Glossary*, <http://primes.utm.edu/glossary/>
2. J. H. Conway, R. K. Guy, *The book of numbers*, Springer-Verlag, New York, 1995.
3. M. Keith, *Keith Numbers,* [*http://www.cadaeic.net/keithnum.htm*](http://www.cadaeic.net/keithnum.htm)
4. E. Deza, M. M. Deza, Figurate Numbers, World Scientific Publishing, Singapore, 2012.

**Kongruentni brojevi**

Literatura:

1. K. Conrad, The Congruent Number Problem, <http://www.aimath.org/news/congruentnumbers/congruentnumbers.pdf>
2. K. E. Morrison, *Congruent Numbers,* [*http://aimath.org/news/congruentnumbers/congruentnumbers.pdf*](http://aimath.org/news/congruentnumbers/congruentnumbers.pdf)
3. A. Dujella, *Eliptičke krivulje i njihova primjena u kriptografiji*, <http://web.math.pmf.unizg.hr/~duje/ecc/kongruentni.html>

**Sume kvadrata**

Literatura:

1. G. A. Jones, J. M. Jones, Elementary Number Theory, Springer-Verlag, London, 2004.
2. R. A. [Mollin*,*](http://math.ucalgary.ca/profiles/101-152961)  [*Fundamental Number Theory with Applications*](http://math.ucalgary.ca/research/publications/view/101-154064)*,* CRC Press, New York, 2008.

**Primitivni korijeni i indeksi**

Literatura:

1. M. B. Nathanson, *Elementary Methods in Number Theory,* Springer – Verlag, NY,2000.
2. [A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta)](http://www.mathos.unios.hr/uutb/Materijali/utblink.pdf)
3. R. A. Mollin*, Fundamental Number Theory with Applications,* CRC Press, New York, 2008.

***Eulerova funkcija***

Literatura:

1. A. [Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta)](http://www.mathos.unios.hr/uutb/Materijali/utblink.pdf).
2. R. A. Mollin*, Fundamental Number Theory with Applications,* CRC Press, New York, 2008.
3. Pete L. Clark, *Number Theory: A Contemporary Introduction*, <http://math.uga.edu/~pete/4400FULL.pdf>

**Chebyshevljev teorem o prostim brojevima**

Literatura:

1. B. Nathanson, *Elementary Methods in Number Theory,* Springer – Verlag, NY,2000.
2. Franz Lemmermeyer*, The Prime Number Theorem*, <http://www.fen.bilkent.edu.tr/~franz/nt/cheb.pdf>

***Lagrangeov teorem***

Literatura:

1. H. Kraljević, *Algebra*, Odjel za matematiku, Svučilište J.J. Strossmayera u Osijeku, 2007 (skripta).
2. K. Conrad, [*Cosets and Lagrange's Theorem*](http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/coset.pdf), http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/coset.pdf