MAT 311
Number Theory

HOME | COURSE DESCRIPTION | HOMEWORK | PROJECTS | GRADE | LINKS

Instructor:

Sorin Popescu (office: Math 3-109, tel. 632-8255, e-mail sorin at math.sunysb.edu)

Grader:

Caner Koca (office: Math 3-118, e-mail caner at math.sunysb.edu)

Schedule:

TuTh 02:20pm-03:40pm, Lgt Engr Lab 154

Prerequisites:

Either **MAT 312** (Applied algebra), or **MAT 313** (Abstract Algebra) or **MAT 318** (Classical Algebra) are mandatory prerequisites for this class. In general some basic algebra exposure is required and assumed, but I will try to keep prerequisites to a minimum.

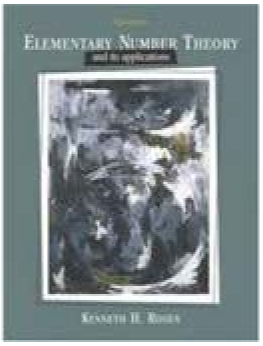
Textbook(s):

We will be covering a number of elementary topics in number theory and some applications. Some theoretical aspects will be trated in detail while others will provide brief but insightful and motivating excursions into topics like Mersenne Primes, number sieves, RSA cryptography, elliptic curves, etc if time will permit.

There are many excellent undergraduate books on the subject. Here is a sample list (all of them available in our library), however we will mainly use this semester only the first two of them:

- *The higher arithmetic*, by H. Davenport (7th edition)
- *Elementary Number Theory and Its Applications* , by K. Rosen, (5th edition)
- *An Introduction to the Number Theory*, H.M. Stark

- *Number Theory*, G.E. Andrews
- *Introduction to Analytic Number Theory*, T.M. Apostol
- *An Introduction to the Theory of Numbers*, I. Niven and H.S. Zuckerman
- *A Classical Introduction to Modern Number Theory*, K. Ireland and M. Rosen
- *Fundamentals of Number Theory*, W.J. LeVeque
- *Number theory with computer applications*, R. Kumanduri and C. Romero



These are a mixture of classical texts (for example Dirichlet), modern efforts, more elementary (for example Kumanduri and Romero) and more advanced (for example Rosen, or Ireland and Rosen), algebraic (for example Andrews or Davernport) or analytic approaches (for example, Apostol). This course will concentrate only on elementary algebraic number theory, and applications.

Course description:

We will cover only parts of the textbook(s) (Davenport and Rosen) and the schedule may/will be adjusted based on students' preparation and progress.

Topic	Sections in textbook	Week	Notes
Numbers, sequences, and sums. Induction. Fibonacci numbers. Divisibility	Davenport Chap. 1	1/23-1/28	
Greatest Common Divisor, Euclidean algorithm, Fundamental theorem of arithmetic		1/30-2/4	
Linear Diophantine equations / Congruences		2/6-2/11	
Fermat's little theorem / Euler's Formula	Davenport Chap. 2	2/13-2/18	

Projects, Homework & Grading:

Homework and project (TBA) are an integral part of the course. Problems marked with an asterisk (*) are for extra credit. In addition to homework you will be required to hand in a research/scholarship/computing project. Projects with a nontrivial writing component may be used to satisfy the Mathematics Upper Division Writing Requirement.

Your grade will be based on the weekly homeworks (20%), project (25%), midterm (25%), and the final exam (30%). The two lowest homework grades will be dropped before calculating the average.

- Homework assignments
- Projects (updated)

The midterm will be held in class on **03/23**.

A **review session** will be held on **04/28** in Math P-131, 3:00-4:00pm. The final exam will be comprehensive.

Grades are now posted on the Solar system. Have a nice summer!

Links:

The following is a short list of web sites devoted to number theory or number theoretic related topics relevant for our class:

- An On-Line Encyclopedia of Integer Sequences.
- Fibonacci Numbers and Nature. Or Tony Phillips' "The most irrational number". Also "Who was Fibonacci?": a brief biography of Fibonacci.
- Primes: Lots of interesting facts about prime numbers.
- Mersenne Primes: interesting facts about Mersenne primes, perfect numbers, and related topics.
- Primes is P: about a recent polynomial time deterministic algorithm to test if an input number is prime or not.
- RSA: The RSA company's web page containing lots of interesting information about the RSA public key cryptosystem and cryptography in general, from both a technological and a socio-political viewpoint.
- The RSA factoring challenge.
- The Wikipedia entry for RSA cryptography.
- The Enigma machine.
- Handbook of Applied Cryptography, by Alfred J. Menezes, Paul C.

van Oorschot and Scott A. Vanstone. It is a handbook for both novices and experts, introducing practical aspects of both conventional and public-key cryptography.
- The GCHQ Challenge (as of July 2005).
- Ron Rivest's Cryptography and Security links page.
- MIT Lecture Notes on Cryptography, by S. Goldwasser and M. Bellare.
- A brief history/introduction to error-correcting codes Digital Revolution - Error Correction Codes, Joseph Malkevitch, in What's New in Mathematics Feature Column of the AMS.
- Anatomy of Credit Card Numbers: a discussion of how to determine if a given credit card number might be valid or not.
- The Wikipedia entry for ISBN (that is International Standard Book Numbers). However, starting January 1, 2007, the book industry will begin using 13 digit ISBNs to identify all books in supply chain.
- A summary describing how information is encoded on Compact Discs. CDs use a modified form of the Reed-Solomon code called the Cross Interleave Reed-Solomon Coding (CIRC). Here is a short description of how Reed-Solomon codes are used for error-correction on a audio CD (Red Book Standard).
- FactorWorld is a web site dedicated to integer factorization results and algorithms. It also includes a list of recent factoring records.
- The list of the 221 currently known proofs of the Quadratic Reciprocity Law (from Legendre (1788) and Gauß (1801) to Szyjewski (2005))

A number of interesting local links that you are warmly encouraged to explore:

- Problem of the Month sponsored by the Stony Brook mathematics deptartment. The first two winners each month get $25!
- Math Club

Math Learning Center

The **Math Learning Center** (MLC), located in Room S-240A of the Math Tower, is an important resource. It is staffed most days and some evenings by mathematics tutors (professors and advanced students). For more information and a schedule, consult the MLC web site.

Special needs

If you have a physical, psychiatric, medical or learning disability that may impact on your ability to carry out assigned course work, you may contact the Disabled Student Services (DSS) office (Humanities 133, 632-6748/TDD). DSS will review your concerns and determine, with you, what accommodations may be necessary and appropriate. I will take their findings into account in deciding what alterations in course work you require. All information on and documentation of a disability condition should be supplied to me in writing at the earliest possible time AND is strictly confidential. Please act early, since I will not be able to make any retroactive course changes.

Last modified 2006-2-25

MAT 311
Number Theory

HOME | COURSE DESCRIPTION | HOMEWORK | PROJECTS | GRADE | LINKS

Homework:

Problems marked with an asterisk (*) are for extra credit.

- **HW 1** (due 02/02 in class) [solutions]
    - Davenport p.215/216: Ex 1.01, 1.02, 1.03
    - Use mathematical induction to show that $n<2^n$.
    - Use mathematical induction to show that $1^2-2^2+3^2-\dots+(-1)^{n-1}n^2 = (-1)^{n-1}n(n+1)/2$, for all positive n.
    - Find and prove a simple formula for the sum of the first n Fibonacci numbers with odd indices when n is a positive integer. That is find a simple formula for $f_1+f_3+f_5+\dots+f_{2n-1}$.
- **HW 2** (due 02/08 in class) [solutions]
    - Davenport p.215/216: Ex 1.04, 1.05, 1.11, 1.12
    - Find a simple function of x that approximates the counting function sq(x) := number of square numbers less than x. Use this estimate to explain why the statement "most numbers are not perfect square" makes sense.
    - Show that there are no prime triplets, that is primes p, $p+2$, $p+4$, other than 3,5, and 7.
    - Show that every integer greater than 11 is the sum of two composite integers.
    - Show that there are no primes of the form N^3+1 other than 2 $(=1^3+1)$
    - Find the smallest five consecutive composite integers.
- **HW 3** (due 02/15 in class) [solutions]
    - Davenport p.217 Ex 1.20, 1.23*, 1.24, 2.01
    - Find the greatest common divisor of 34709 and 100313 and express it as a linear combination of these integers.
    - Find the greatest common divisor of 15, 35 and 90 and

express it as a linear combination of these integers.

    - * If f_n denotes the *n*-th Fibonacci number show that $(f_n, f_m) = f_{(n,m)}$.
    - Let *n* be a positive integer and let *p* be a prime. Show that the power of *p* appearing in the prime-power factorization of *n!* is $[n/p]+[n/p^2]+[n/p^3]+...$, where [..] denotes the integral part of a number.
    - How many zeroes are at the end of 1000! in decimal notation?
    - Find the prime factorization of 2^{36}-1. Do not use a calculator and do not compute the decimal representation of 2^{36}-1...
    - A shopper spends a total of $5.49 for oranges which cost 18c each and grapefruit which cost 33c each. What is the minimum number of fruit that the shopper could have bought?
    - Which combinations of pennies, dimes and quarters have a total value of 99c?
    - NoFrills Airlines offers three types of tickets on the route Boston-NYC. Business class tickets are $140, economy tickets are $110 and standby tickets are $78. If 69 passengers pay a total of $6548 for their tickets on a particular flight, how many of each type of ticket were sold?
- **HW 4** (due 02/23 in class) [solutions]
    - Davenport p.217 Ex 2.03, 2.04
    - Using the Chinese remainder theorem, explain (only) how to add and how to multiply 784 and 813 on a computer with word size 100.
- **HW 5** (due 03/02 in class) [solutions]
    - Davenport p.218 Ex 2.05, 2.07, 2.12
    - * Show that if *p* is an odd prime then the remainder of *2(p-3)!* when divided by *p* is -1.
    - What is the remainder of 5^{100} when divided by 7?
    - What is the remainder of 18! when divided by 437?
    - Use Euler's theorem to find the last digit of the decimal expansion of 7^{1000}.
    - Find the last digit of the base 7 expansion of 3^{100}.
    - Show that 42 | (n^7-n) for all positive integers *n*.

  - Show that *$\varphi(n)\varphi(m)=\varphi((n,m))\varphi([n,m])$*.
  - *Find the smallest positive integer n with $\tau(n)=3$. Find also the smallest positive integer n with $\tau(n)=13*31$.
  - *Which positive integers have exactly four positive divisors?
- **HW 6** (due 03/09 in class) [solutions]
  - Davenport p.219 Ex 2.21, 2.22.
  - Show that $\tau(n)$ is odd if and only if n is a perfect square. Also show that $\sigma(n)$ is odd if and only if n is a perfect square or twice a perfect square.
  - A number n is called "abundant" if $\sigma(n)>2n$.
    1. Find the six smallest abundant postive integers.
    2. Show that a multiple of an abundant or a perfect number (other than the perfect number itself) is abundant.
    3. Show that if $n= 2^{m-1}(2^m-1)$, where m is a postive integer and 2^m-1 is composite (i.e. not a prime), then n is abundant.
  - Let $\Lambda(n)$ be the Von Magoldt function: $\Lambda(n)=0$ if n is not a prime power, and $\Lambda(p^m)=\log p$ for any prime power p^m.
    1. Is $\Lambda(n)$ a multiplicative function ?
    2. Show that

       $$\Sigma_{d|n} \Lambda(d) = \log n$$

       for all natural numbers $n >0$.
  - Let $\lambda(n)$ be the Liouville function: $\lambda(1)=1$ and $\lambda(n)=(-1)^r$ if n is a product of r (not necessarily distinct) prime numbers.
    1. Show that $\lambda(n)$ is a multiplicative function.
    2. * Show that the Dirichlet (or convolution) inverse of $\lambda(n)$ is the characteristic function of the squarefree numbers (that is it is the function μ^2, where &mu denotes the Moebius function).
  - Find a closed form expression for the following sums:
    1. $\Sigma_{d|n} \mu(d)/d$
    2. $\Sigma_{d|n} \mu(d)\varphi(d)$
    3. $\Sigma_{d|n} \mu^2(d)/\varphi(d)$

        4. * $\sum_{d|n} \mu(n/d) \log d$

- **HW 7** (due 03/16 in class) [solutions]
    - Davenport p.225 Ex 8.06 and 8.07.
    - Find the period length of the sequence of pseudorandom numbers generated by the linear congruential method with $x_0=0$ and x_{n+1} $4x_n+7$ (mod 25).
    - Would the numbers generated by the linear congruential method x_{n+1} x_n+c (mod n) for given (fixed) n, c and x_0 be a good choice for a sequence of pseudorandom numbers? Explain!
    - Use the Pollard ρ-method with $x_0=2$ and $x_{n+1}= x_n^2+1$ to factor the number 133.
    - * Explain why the choice of a linear function $x_{n+1}= ax_n+b$ to generate the x_n is a poor choice for Pollard ρ-method.
    - Show that every composite Fermat number $F_n=2^{2^n}+1$ is a pseudoprime to the base 2.
    - Show that 1387 is a pseudoprime, but not a strong pseudoprime, to the base 2. Is 1387 a Carmichael number?
    - Show that 1373653 is a strong pseudoprime to both bases 2 and 3.
- **HW 8** (due 03/30 in class) [solutions]
    - Davenport p.219 Ex. 3.04, 3.05, 3.11, 3.12, 3.13*
    - Let p be a prime number. Use Lagrange's theorem to show that each coefficient of the polynomial $f(x)=(x-1)(x-2)...(x-p+1)-x^{p-1}+1$ is divisible by p. Use this fact to give another proof to Wilson's theorem.
    - *Show that if q is an odd prime and $p=2q+1$ is also a prime number, and if a is a positive integer with $1 < a < p-1$, then $p-a^2$ is a primitive root modulo p.
    - Use index arithmetic to find all the solutions of the congruences
        1. $3x^5$ 1 (mod 23)
        2. $3x^{14}$ 2 (mod 23)
        3. 3^x 2 (mod 23)

  - For which positive integers *a* is the congruence ax^4 2 (mod 13) solvable?
- **HW 9** (due 04/06 in class) [solutions]
  - Davenport p.219 Ex. 3.14, 3.15, 3.18, 3.19
  - Find a primitive root modulo 17^2.
  - Show that 101 is a prime number using Lucas' converse of Fermat's little theorem with $x=2$.
  - Show that if an integer *x* exists such that $x^{2^{2^n}}$ 1 (mod F_n) and $x^{2^{(2^n-1)}} \neq 1$ (mod F_n), then the Fermat number $F_n=2^{2^n}+1$ is prime.
  - * Let *n* be a positive integer possessing a primitive root of unity. Using this primitive root prove that the product of all positive integers less than *n* and relatively prime to *n* is congruent to -1 modulo *n*. (When *n* is a prime number this is just Wilson's theorem.)
  - Find the minimal universal exponent of 884, that is λ(884).
  - Find all positive integers *n* for which λ(*n*)=2.
- **HW 10** (due 04/20 in class)
  - Davenport p.220 Ex. 3.21, 3.22, 3.23, 3.25, 3.26
  - Find all solutions of the quadratic congruence x^2+x+1 0 (mod 7).
  - Does the congruence x^2-3x-1 0 (mod 31957) have any solutions?
  - * Show that if *p* is an odd prime with *p* > 5 then there are always two consecutive quadratic residues mod *p*.
  - * Show that there are infinitely many primes of each of the following types:
    - *8k+3*
    - *8k+5*
    - *8k+7*
  - Evaluate each of the following Legendre symbols: (111/991), (7/79), (31/641)
  - Verify if the following assertion is true: If *p* is congruent to 1 modulo 5, then 5 is a quadratic reside mod *p*

- **HW 11** (due 04/27 in class) [solutions]
  - Davenport p.220 Ex. 3.16, 3.17
  - Use Pepin's test to check that the Fermat numbers F_3=257 and F_4=65537 are primes.
  - * Use Pepin's test to conclude that 3 is a primitive root of every Fermat prime.
  - Find a congruence describing all primes for which 5 is a quadratic residue.
  - The integer p=1+8*3*5*7*11*13*17*19*23=829371481 is a prime (e.g this can be checked with the help of Maple or Pari). Show that all primes q with q < 24 are quadratic residues mod p. Conclude that there is no quadratic nonresidue of p less than 29 and that p has no primitive root less than 29.
  - Evaluate the following Jacobi symbol: (1009/2307).
  - For which positive integers n that are relatively prime to 15 does the Jacobi symbol (15/n) equal 1?
  - Use succesive squaring to compute 11^{864} (mod 1729) and use quadratic reciprocity to compute (11/1729). What can you conclude concerning the possible primality of 1729?
  - Show that if a prime number p > 5 can be written in the form $p = a^2 + 5b^2$ then p 1 or 9 (mod 20).
- **HW 12** (due 05/04 in class, for extra credit)
  - * Find the solutions of x^2 482 (mod 2773)
  - * Let p be an odd prime, and let C P^e (mod p) be a cyphertext obtained by modular exponentiation from the plaintext P, with exponent e and modulus p, where $0 < C < p$ and (e, p-1)=1. Show that C is a quadratic residue mod p if and only if P is a quadratic residue mod p.
  - * Let n=3149=47*67 and suppose that x^4 2070 (mod 3149). Find the least nonnegative residue of x^2 mod 3149.
  - * Run through the steps used to verify that a user has the secret information consisting of the factorization of 24617=103*239. (This is a toy example, since in reality primes with hundreds of digits would be used instead.)
  - * Davenport p.225 Ex 8.11 and 8.12.

MAT 311
Number Theory

Information about Project

In addition to homework you will be required to hand in a research/scholarship/computing projects. Projects with a nontrivial writing component may be used to satisfy the Mathematics Upper Division Writing Requirement. The project should be handed in final form by **04/17**. You need to make your selection and also inform me of it (in writing) by **02/28**. Here is a list of suggestions for your projects:

1. Discuss the existence, number, etc of non-negative solutions of a diophantine equation $ax+by=n$ where a,b,n are positive, $(a,b)=1$. For instance
   - Show that whenever $n\geq(a-1)(b-1)$ then there always are nonnegative solutions.
   - Show that if $n=(a-1)(b-1)-1$ then there are no nonnegative solutions.
   - For how many nonnegative integers $n<(a-1)(b-1)-1$ does there exist a non-negative solution to the above equation?
   - Write a program to find all n for which the above equation has nonnegative solutions.
2. Give estimates for the number of bit operations needed to compute each of the following:
   - n!
   - n choose k
   - Find the binary expansion of a number given its decimal expansion.

   (Hint: Read more in Rosen Section 2.3)
3. Write a program to explore the following statements. For those you believe true try to provide a proof!
   - If p_1, p_2, ... ,p_t are primes not exceeding n then $p_1p_2\ldots p_t\leq 4^n$.
   - The n-th prime number p_n is smaller than $2^{2^{n-1}}$.

n

The n-th prime number p_n is smaller or equal than 2 .

4. Fermat numbers are numbers of the form $F_n=2^{2^n}+1$, for positive integers n.
    - Find the last 2 digits of a Fermat number F_n in its decimal expansion.
    - Estimate the number of decimal digits in the Fermat number F_n.

      Show that $(F_n, F_m)=1$, for distinct positive integers n and m.
    - What is the the gcd of F_n and n?
5. Write a program that finds all twin primes less than 20,000. Hardy and Littlewood conjectured that the number of twin primes not exceeding n is asymptotic to $C\ n/(\ln n)^2$ for a constant C, approximately equal to 0.66016. Determine how accurate this asymptotic formula is for values of n as large as you can compute.
6. Prove that unique factorization holds in $\mathbf{Z}+\mathbf{Z}[i]$ (where i is the imaginary unit). Describe an analogue of the Euclidean algorithm in this context. What happens for numbers of type $\mathbf{Z}+\mathbf{Z}\sqrt{5}$?
7. Show that if p is a prime of the form $4k+3$ and $q=2p+1$ is prime, then q divides the Mersenne number $M_p=2^p-1$. (Hint: use Legendre symbols).
8. Derive an explicit formula that gives the day of the week of any day of any given year in the Julian or the Gregorian calendars. Use these formulas to find the day of the week of the following important dates (Hint: Use the Julian calendar before September 3, 1752 and the Gregorian calendar after that date):
    - October 12, 1492 (Columbus sights land in the Caribbean)
    - July 4, 1776 (US Declaration of Independence)
    - March 30, 1867 (US buys Alaska from Russia)
    - July 20, 1969 (First man on the moon)

   Which of your birthdays, until your one hundredth, fall on the same day of the week as the day you were born?
9. A Carmichael number is an absolute pseudoprime n, that is a number n such that a^{n-1} 1 (mod n) for all positive integers a such that $(a,n)=1$.
    - Show that if n is a Carmichael number then it is squarefree.

  - Show that if $n=p_1p_2...p_n$ is a product of distinct primes such that $p_i-1|n-1$ for all i, then n is a Carmichael number. Use this to show that 564651361 is a Carmichael number. Can you write a program to find other Carmichael numbers?
  - Find as many Charmichael numbers of the form $(6m+1)(12m+1)(18m+1)$ as you can.

10. An integer n is called highly composite if $\tau(n)= \tau(m)$ for all integers $m<n$. Find all highly composite numbers not exceeding 10,000.
11. Suppose that a new Stony Brook ID will be implemented where each student gets assigned a 10 digit code word x_1 $x_2...x_{10}$. Each digit is a decimal digit, and the valid codes are those satisfying the congruences $\sum x_i \quad \sum ix_i \quad \sum i^2x_i \quad \sum i^3x_i \quad 0$ (mod 11).
    - How many valid 10 digit code words there are? Will there be enough many such IDs for all the SB students?
    - Show how any two errors in such a code word can be corrected.
    - For instance suppose we have typed 0204906710 as a code word but we have made two mistakes. What should have been the correct code word?
12. Discuss the cryptanalysis of Vigenere ciphers and write a program to decrypt messages which have been encrypted using such ciphers.

For any of the programming projects, please email me at sorin at math.sunysb.edu both the program source code (in readable form -- indented and commented) and the project, and please hand in the program outline and a reasonable amount of program output. You can use any programming language you like (within reasonable limits - i.e., a language for which there exist easily available compilers). Preferred ones are *Maple*, *Mathematica* (yes, they are programming languages), *C*, *OCAML* and *Java*, but you can also use *C++*, *Pascal*, *Python*, *Fortran*, *Lisp*, *Turing machine*...

Sorin Popescu
2006-2-10

Sorin Popescu

Department of Mathematics
Stony Brook University
Stony Brook, NY 11794-3651

email: sorin@math.sunysb.edu
Office: Math 3-109
Phone: (631)-632-8255
Fax: (631)-632-7631

Research Interests: Algebraic Geometry, Commutative Algebra, Combinatorics and Computational methods

Teaching:

Spring 2006	MAT 311 Number Theory	MAT 614 Topics in Algebraic Geometry
Previous years	Teaching Archive	

Algebra, Geometry and Physics seminar: Spring 2006

Publications & E-Prints: Unless otherwise indicated, the files below are DVI files (DVI), PostScript files (PS), PDF files (PDF), or tar gziped DVI and PostScript files (). Files marked as (PDF) or (ƒ) are hyperlinked PDF or Macromedia Flash files formated for screen viewing. Other formats (source, PS using Type I fonts) can be obtained via the UC Davis Front to the Mathematics ArXiv. Click on () or () for related *Macaulay2*, or *Macaulay* code.

Syzygies:

- *Gale Duality and Free Resolutions of Ideals of Points* [DVI], [PS] [PDF] [] [], *Invent math* **136** (1999) 2, 419-449
  David Eisenbud and Sorin Popescu
- *The Projective Geometry of the Gale Transform* [DVI], [PS] [PDF] [], *J. Algebra* **230** (2000), no. 1, 127-173

  David Eisenbud and Sorin Popescu
  (in the D. Buchsbaum anniversary volume of *J. Algebra*)
- *Syzygy Ideals for Determinantal Ideals and the Syzygetic Castelnuovo Lemma* [PS] [PDF], [MathSci],

Springer 1999
David Eisenbud and Sorin Popescu

- *Extremal Betti Numbers and Applications to Monomial Ideals* [PS] [PDF] [ ] [ ], *J. Algebra* **221** (1999), no. 2, 497-512
  Dave Bayer, Hara Charalambous and Sorin Popescu
- *Lagrangian Subbundles and Codimension 3 Subcanonical Subschemes* [DVI], [PS] [PDF] [ ], *Duke Math. J.* **107** (2001), no. 3, 427-467
  David Eisenbud, Sorin Popescu and Charles Walter
- *Enriques Surfaces and other Nonpfaffian Codimension 3 Subcanonical Subschemes* [PS] [PDF] [PDF] [ƒ], *Comm. Algebra* **28** (2000), 5629-5653
  David Eisenbud, Sorin Popescu and Charles Walter
  (in the Hartshorne anniversary volume of *Comm. Algebra*)
- *Syzygies of Unimodular Lawrence Ideals* [PS] [PDF] [ ] [ ], *J. Reine Angew. Math* **534** (2001), 169-186
  Dave Bayer, Sorin Popescu and Bernd Sturmfels
- *Hyperplane Arrangement Cohomology and Monomials in the Exterior Algebra* [DVI] [PS] [PDF] [ ] [ ], Trans. AMS. **355** (2003), 4365-4383
  David Eisenbud, Sorin Popescu and Sergey Yuzvinsky
- *Exterior algebra methods for the Minimal Resolution Conjecture* [DVI] [PS] [PDF] [ ], *Duke Math. J.* **112** (2002), no. 2, 379-395
  David Eisenbud, Frank-Olaf Schreyer, Sorin Popescu and Charles Walter
- *Symmetric resolutions of coherent sheaves* [DVI] [PS] [PDF]
  David Eisenbud, Sorin Popescu and Charles Walter
- *A note on the Intersection of Veronese Surfaces* [DVI] [PS] [PDF] [PDF] [ƒ]
  David Eisenbud, Klaus Hulek and Sorin Popescu
- *Restricting linear syzygies: algebra and geometry* [DVI] [PS] [PDF] [PDF] [ƒ], *Compositio Math.* **141** (2005), no.6, 1460-1478
  David Eisenbud, Mark Green, Klaus Hulek and Sorin Popescu
- *Small schemes and varieties of minimal degree* [DVI] [PS] [PDF] [PDF] [ƒ], *Amer. J of Math* (2005), to appear
  David Eisenbud, Mark Green, Klaus Hulek and Sorin Popescu

Abelian varieties, modular varieties and equations:

- *Equations of (1,d)-polarized abelian surfaces* [PS] [PDF] [ ], *Math. Ann.* **310** (1998), no. 2, 333-377
  Mark Gross and Sorin Popescu
- *The moduli space of (1,11)-polarized abelian surfaces is unirational* [PS] [PDF] [ ], *Compositio Math.* **126** (2001), no. 1, 1-24
  Mark Gross and Sorin Popescu
- *Calabi-Yau threefolds and moduli of abelian surfaces I* [PS] [ ] [PDF], *Compositio Math.* **127**, no. 2, (2001), 169-228
  Mark Gross and Sorin Popescu

PS PDF

Calabi-Yau threefolds and moduli of abelian surfaces II [ ] [ ] [ ]
Mark Gross and Sorin Popescu

- *Elliptic functions and equations of modular curves* [DVI] [PS] [PDF] [⚡], *Math. Ann.* **321** (2001), no. 3, 553-568
  Lev A. Borisov, Paul Gunnells, and Sorin Popescu

Surfaces in P^4 and threefolds in P^5:

- *The Geometry of Bielliptic Surfaces in P^4* [DVI], [PS] [PDF], *Internat. J. Math.* **4** (1993), no. 6, 873-902
  A. Aure, W. Decker, K. Hulek, S. Popescu and K. Ranestad
- *On Surfaces in P^4 and Threefolds in P^5* [DVI] [PS] [PDF], [MathSci], LMSLN **208**, 69--100
  W. Decker and S. Popescu
- *Surfaces of degree 10 in P^4 via linear systems and linkage* [DVI] [PS] [PDF] [▲] [▲], *J. Algebraic Geom.* **5** (1996), no. 1, 13-76
  S. Popescu and K. Ranestad
- *Syzygies of Abelian and Bielliptic Surfaces in P^4* [DVI] [PS] [PDF], *Internat. J. Math.* **8** (1997), no. 7, 849-919
  A. Aure, W. Decker, K. Hulek, S. Popescu and K. Ranestad
- *Examples of smooth non general type surfaces in P^4* [DVI] [PS] [PDF] [▲] [▲], *Proc. London Math. Soc.* (3) **76** (1998), no. 2, 257-275
  S. Popescu
- *Surfaces of degree >= 11 in the Projective Fourspace* [DVI] [PS] [PDF]+ *Appendix* [DVI] [PS] [PDF]
  S. Popescu

PRAGMATIC 1997: A summer school in Catania, Sicily

- *Research Problems for the summer school* [DVI], [PS] [PDF], [MathSci], *Matematiche* (Catania) **53** (1998), 1-14
  David Eisenbud and Sorin Popescu

Algorithmic Algebra and Geometry: Summer Graduate Program (1998) at MSRI:

- Poster [PS] [PDF], lecture slides and streaming video , CD ROM,
  Dave Bayer and Sorin Popescu

Linear algebra notes

- *On circulant matrices* [DVI], [PS] [PDF] [PDF] [⚡],
  Daryl Geller, Irwin Kra, Sorin Popescu and Santiago Simanca

---

Upcoming conferences:

- DARPA FunBio Mathematics-Biology Kick-off meeting, Princeton, September 21-23, 2005
- MAGIC 05: Midwest Algebra, Geometry and their Interactions Conference, University of Notre Dame, Notre Dame, October 7-11, 2005
- AMS Special Session on Resolutions, Eugene, OR, November 12-13, 2005
- Clay Workshop on Algebraic Statistics and Computational Biology, Clay Mathematics Institute, November 12-14, 2005
- CIMPA School on Commutative Algebra, December 26, 2005 - January 6, 2006, Hanoi, Vietnam
- AMS Special Session on Syzygies in Commutative Algebra and Geometry, San Antonio, TX, January 12-15, 2006
- KAIST Workshop on Projective Algebraic Geometry, January 23-25, 2006, Korean Advanced Institute of Science and Technology, Daejeon
- AMS Special Session on the Geometry of Groebner bases, San Francisco, CA, April 29-30, 2006
- Castenuovo-Mumford regularity and related topics, Workshop at CIRM, Luminy, France, May 9-13, 2006
- Commutative Algebra and its Interaction with Algebraic Geometry, Workshop at CIRM, Luminy, France, May 22-26, 2006
- Syzygies and Hilbert Functions, Banff International Research Meeting, Canada, October 14-19, 2006

Past conferences:

- A conference on alegbraic geometry to celebrate Robin Hartshorne's 60th birthday, Berkeley, August 28-30, 1998
- Western Algebraic Geometry Seminar, MSRI, Berkeley, December 5-6, 1998
- Conference on Groebner Bases, Guanajato, Mexico, February 8-12, 1999
- The Pacific Northwest Geometry Seminar
- Computational Commutative Algebra and Combinatorics, Osaka, July 21-30, 1999.
- Kommutative Algebra und Algebraische Geometrie, Oberwolfach, August 8-14, 1999.
- AMS Western Section Meeting Salt Lake City, UT, September 25-26, 1999.
- Algebra and Geometry of Points in Projective Space, Napoli, February 9-12, 2000.
- AMS Spring Eastern Sectional Meeting Lowell, MA, April 1-2, 2000.
- Algèbre commutative et ses interactions avec la géométrie algébrique, Centre International de Rencontres Mathématiques, June 5-9, 2000.
- Topics in Classical Algebraic Geometry, Oberwolfach, June 18-24, 2000
- AMS Fall Central Section Meeting Toronto, Ontario Canada, September 22-24, 2000
- AMS Fall Eastern Section Meeting, New York, Columbia U. in New York, November 4-5, 2000
- Exterior algebra methods and other new directions in Algebraic Geometry, Commutative Algebra and Combinatorics, 8-15 September 2001, Ettore Majorana Centre, Erice, Sicily, Italy. Photos from the conference.
- Classical Algebraic Geometry, Oberwolfach, May 26 - June 1, 2002
- Current trends in Commutative Algebra, Levico, Trento, June 17-21, 2002
- Birational and Projective Geometry of Algebraic Varieties, Ferrara, September 2-8, 2002
- Commutative Algebra, Singularities and Computer Algebra, Sinaia, September 17-22, 2002. Photos from the conference.
- James H. Simons Conference on Quantum and Reversible Computation , Stony Brook, May 25-31, 2003

- Conference on Commutative Algebra, Lisbon, June 23-27 2003. Photos from the conference. Also photos from Belém.
- Commutative Algebra and Interactions with Algebraic Geometry and Combinatorics, ICTP, Trieste, June 6-11
- III Iberoamerican Congress on Geometry, Salamanca, June 7-12
- Projective Varieties: A Conference in honour of the 150th anniversary of the birth of G. Veronese, Siena, June 8-12 , 2004. Photos from the conference.
- Algebraic Geometry: conference in honour of Joseph Le Potier & Christian Peskine, Paris, June 15-18, 2004
- Classical Algebraic Geometry, Oberwolfach, June 27-July 3, 2004
- Combinatorial Commutative Algebra, Oberwolfach, July 4-10th, 2004

Last updated on 10 Dec 2003