MAT 311

Number Theory

Instructor Sorin Popescu (office: Math 4-119, tel. 632-8358, e-mail sorin@math.sunysb.edu)

Time and Place TuTh 02:20pm-03:40pm, SBU 226

Prerequisites

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

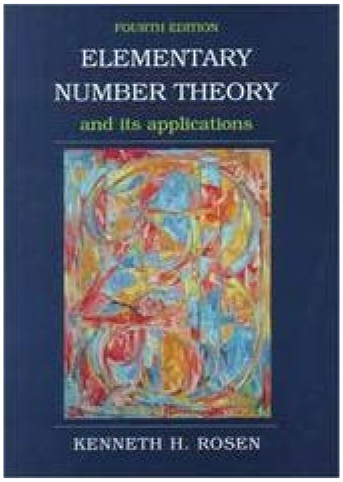
Textbook(s)

Elementary Number Theory and Its Applications , by Kenneth Rosen, (fourth edition) Addison-Wesley 2002.

This is a very nice textbook that integrates classical (elementary) topics in number theory with lots and lots of applications to cryptology, computer science, etc. It also features a number of computer (programming) projects, mainly for Mathematica and Maple.

There are many other excellent undergraduate books on the subject. Here is a sample (all of them available in our library):

- *A Friendly Introduction to Number Theory*, J.H. Silverman
- *An Introduction to the Number Theory*, H.M. Stark
- *Number Theory*, G.E. Andrews
- *Introduction to Analytic Number Theory*, T.M. Apostol
- *Lectures on Number Theory*, P.G.L. Dirichlet with supplements by R. Dedekind
- *The higher arithmetic*, H. Davenport
- *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, Silverman, Kumanduri and Romero) and more advanced (for example, Ireland and Rosen), algebraic (for example, Andrews) or analytic approaches (for example, Apostol). This course will concentrate only on elementary algebraic number theory, and applications.

Course description & Homework assignments

We will cover only part of the textbook and the following schedule may/will be adjusted based on students' preparation and progress. Problems marked with an asterisk (*) are for extra credit.

	Date	Topic	Homework	Notes
Wk 1				
	1/23	1.1 Numbers, sequences, and sums	p14/2,4,26,27; p22/5,10,16,30; p28/4,8,22; due 02/04; solutions	
Wk 2	1/28	1.2 Mathematical induction; 1.3 Fibonacci numbers		Fibonacci links
	1/30	1.4 Divisibility; 3.1 Prime numbers	p34/4,16,28; p76/2,6,10; p84/6,7,13,31; due 02/11; solutions	Half hour pretest
Wk 3	2/4	3.2 Greatest common divisor		Primes links
	2/6	3.3-3.4 Euclidean algorithm, Fundamental theorem of arithmetic	p94/5,7,19*; p123/2, 3, 6 p104/4, 10, 16*, 32, 35, 46; due 02/18; solutions	
Wk 4	2/11	3.6 Linear Diophantine equations		
	2/13	4.1-4.5: Congruences	p123/4, 21; p135/5, 22, 26, 28, 38*; p141/2, 6, 8; due 02/25; solutions	
Wk 5	2/18		p149/4a)-b), 12, 22, 24; p159/1, 10; p167/2, 4, 8b, 14* due 03/04; solutions	
	2/20		p177/12,19,22; p195/8,12,13,16,17 due 03/11; solutions	
Wk 6	2/25			
	2/27	5.1 Divisibility tests		
Wk 7	3/4	6.1-6.2 Wilson's theorem, Fermat's little theorem, pseudoprimes	p202/3, 12, 15, 20, 22, 23;	First project due
	3/6			

			p213/2, 7 due 03/27; solutions	
Wk 8	3/11	Midterm [exam] [solutions]		
	3/13	6.3 Euler's theorem		
Recess				
Wk 9	3/25	7. Multiplicative functions	p218/1, 6, 8, 12; p227/1, 2(c,e), 3, 5, 14, 35 due 04/3; solutions	
	3/27			
Wk 10	4/1		p235/2(a-c), 21, 22, 23, 24, 34*, 37* p257/1(a,b), 15,17,18,23; due 04/10; solutions	
	4/3	8. Cryptography		
Wk 11	4/8		p267/3, 14, 15 p278/1, 3, 4*, 13, 18, 19 p290/1, 3, 4*, 6, 7, 11*; due 04/22; solutions	
	4/10			
Wk 12	4/15		p304/1, 6, 10; p313/1, 6, 10, 18*; due 04/29; solutions	04/16-04/18 no classes Passover
		9. Primitive roots		
Wk 13	4/22		p319/3, 8, 12, 16; p337/2, 4, 9 due 05/06	Second project due
	4/24			
Wk 14	4/29	11. Quadratic residues		
	5/1			
Wk 15	5/6			
	5/8	Review		
	5/20	Final exam 2:00-4:30pm (SBU 226)		
	5/20	**Review** 05/16, 4:00pm-5:30pm (Math Towers P-131)		

Projects, Homework & Grading

Homework (see above) and projects (TBA) are an integral part of the course. Problems marked with an asterisk (*) are for extra credit. In addition you will be required to hand in 2 research/scholarship/computing projects. Projects with a nontrivial writing component may be used to satisfy the Mathematics Upper Division Writing Requirement.

- Project 1
- Project 2

Your grade will be based on the weekly homeworks (20%), two projects (15% each), midterm

(20%), and the final exam (30%). The two lowest homework grades will be dropped before calculating the average.

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.

Software

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.

Here are a number of interesting local links:

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

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.

Sorin Popescu

2002-12-21

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] [ƒ], *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] [ƒ],
  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

SKETCH OF SOLUTIONS (HOMEWORK I)

2.- Define the set $S \subset \mathbb{N}$ by $S = \{n \in \mathbb{N} \mid n = a - bk,\ k \in \mathbb{Z}\}$. S is not empty since the hypotheses on a imply $a \in S$ (taking $k = 0$) therefore S must have a minimum element by the well ordering principle.

4.- a) True: (Proof by contradiction) Let t be irrational and $\frac{a}{b}$ be a rational number ($a, b \in \mathbb{Z}$, $b \neq 0$). Suppose $t + \frac{a}{b}$ is rational, that is, $\frac{t}{1} + \frac{a}{b} = \frac{bt+a}{b} = \frac{p}{q}$ with $p, q \in \mathbb{Z}$, $q \neq 0$. Then we get that

$$t = \frac{bp - qa}{qb}$$

but this means that t is rational! (a contradiction). Therefore $t + \frac{a}{b}$ is irrational.

b) False: $\sqrt{2} - \sqrt{2} = 0 \in \mathbb{Q}$

c) False: $0 \cdot \sqrt{2} = 0 \in \mathbb{Q}$

d) False: $\sqrt{2} \cdot \sqrt{2} = 2 \in \mathbb{Q}$

26.- $\sum_{k=2}^{n} \frac{1}{k^2} = \frac{1}{2} \sum_{k=2}^{n} \left(\frac{1}{k-1} - \frac{1}{k+1} \right)$ notice that in this last sum all terms cancel each other out, except the first two terms. Therefore we get:

$$\sum_{k=2}^{n} \frac{1}{k^2} = \frac{1}{2} \left[1 + \frac{1}{2} - \frac{1}{n} - \frac{1}{n+1} \right] = \frac{1}{2} \left[\frac{3}{2} - \frac{2n+1}{n(n+1)} \right]$$

27.- Notice $(k+1)^3 - k^3 = 3k^2 + 3k + 1$ thus $k^2 = \frac{1}{3}[(k+1)^3 - k^3 - 3k - 1]$. Adding over k we get:

$$\sum_{k=1}^{n} k^2 = \frac{1}{3} \left[\sum_{k=1}^{n} \left((k+1)^3 - k^3 \right) - 3 \sum_{k=1}^{n} k + \sum_{k=1}^{n} 1 \right] = \frac{1}{3} \left[(n+1)^3 - 1 - 3\frac{n(n+1)}{2} + n \right]$$

(Simplifying the expression we get: $\frac{n(n+1)(2n+1)}{6}$)

Section 1.2

5.-

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

Proof by induction:

Base: When $n = 1$ this is just the definition of A

Inductive step: Suppose $A^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ We must show then that $A^{k+1} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}$. But $A^{k+1} = A \cdot A^k = A \cdot \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ (By the induction hypothesis) Multiplying we get:

$$A^{k+1} = A \cdot A^k = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}$$

10.- **Base:** $\sum_{j=1}^{1}(-1)^{j-1}j^2 = 1 = (-1)^0\frac{1(1+1)}{2}$
Inductive step: Suppose $\sum_{j=1}^{k}(-1)^{j-1}j^2 = (-1)^{k-1}\frac{k(k+1)}{2}$ Then $\sum_{j=1}^{k+1}(-1)^{j-1}j^2 = \sum_{j=1}^{k}(-1)^{j-1}j^2 + (-1)^k(k+1)^2 = (-1)^{k-1}\frac{k(k+1)}{2} + (-1)^k(k+1)^2 = (-1)^k\frac{(k+1)(k+2)}{2}$

16.- **Base:** $H_{2^1} = \sum_{j=1}^{2}\frac{1}{j} = 1 + \frac{1}{2} \leq 1 + 1$
Inductive step: Suppose $H_{2^k} = \sum_{j=1}^{2^k}\frac{1}{j} \leq 1 + k$. Then $H_{2^{k+1}} = \sum_{j=1}^{2^{k+1}}\frac{1}{j} = \sum_{j=1}^{2^k}\frac{1}{j} + \sum_{j=2^k+1}^{2^{k+1}}\frac{1}{j} \leq 1 + k + \sum_{j=2^k+1}^{2^{k+1}}\frac{1}{j}$ so we only need to make sure the last sum is less than 1. But for this last sum we have $\frac{1}{j} \leq \frac{1}{2^k}$ (by the range of the indices) therefore

$$\sum_{j=2^k+1}^{2^{k+1}}\frac{1}{j} \leq \sum_{j=2^k+1}^{2^{k+1}}\frac{1}{2^k} = \frac{1}{2^k}\sum_{j=2^k+1}^{2^{k+1}} 1 = \frac{1}{2^k}(2^{k+1} - (2^k + 1) + 1) = 1$$

30.- **Base:** $2^5 = 32 > 25 = 5^2$
Inductive step: Suppose $2^k > k^2$ Then $2^{k+1} = 2 * 2^k > 2k^2 = k^2 + k^2 > k^2 + 2k + 1 = (k+1)^2$ The last inequality is a consequence of the following inequality: $k^2 > 2k+1$ for $k > 3$ The proof of this inequality goes as follows $k > 3 \Rightarrow k^2 > 3k = 2k + k > 2k + 1$

Section 1.3

4.- $f_2 + f_4 + \ldots + f_{2n} = f_{2n+1} - 1$ The proof is by induction over n
Base: $f_2 = f_3 - f_1 = f_3 - 1$
Inductive step: Suppose $f_2 + f_4 + \ldots + f_{2k} = f_{2k+1} - 1$ then $f_2 + f_4 + \ldots + f_{2k} + f_{2(k+1)} = f_{2k+1} - 1 + f_{2k+2} = f_{2k+3} - 1 = f_{2(k+1)+1} - 1$

8.- By induction on k
Base: $f_1 f_2 = 1 * 1 = f_2^2$
Inductive step: Suppose $f_1 f_2 + \ldots f_{2k-1}f_{2k} = f_{2k}^2$ then $f_1 f_2 + \ldots f_{2k-1}f_{2k} + f_{2k}f_{2k+1} + f_{2(k+1)-1}f_{2(k+1)} = f_{2k}^2 + f_{2k}f_{2k+1} + f_{2k+1}f_{2k+2} = f_{2k}(f_{2k} + f_{2k+1}) + f_{2k+1}f_{2k+2} = f_{2k}f_{2k+2} + f_{2k+2}f_{2k+1} = f_{2k+2}(f_{2k} + f_{2k+1}) = f_{2k+2}f_{2k+2} = f_{2(k+1)}^2$

22.- **Note: There is a mistake on the book. The last term of the sum should be**

$$\binom{\lceil \frac{n}{2} \rceil}{\lfloor \frac{n}{2} \rfloor}$$

Base: $\binom{1}{0} = 1 = f_2$
Inductive step: Suppose $\binom{n}{0} + \binom{n-1}{1} + \ldots + \binom{\lceil \frac{n}{2} \rceil}{\lfloor \frac{n}{2} \rfloor} = f_{n+1}$ for all $n \leq k$ then let $x := \binom{n}{0} + \binom{n-1}{1} + \ldots + \binom{\lceil \frac{n+1}{2} \rceil}{\lfloor \frac{n+1}{2} \rfloor}$ (that is, x is the sum corresponding to $k = n+1$) Then, using **Pascal's Identity** (Theorem B.2. of the book) we get that

$$x - f_{n+1} = \left[\binom{n+1}{0} - \binom{n}{0}\right] + \left[\binom{n}{1} - \binom{n-1}{1}\right] + \ldots + = 0 + \binom{n-1}{0} + \binom{n-2}{1} + \ldots +$$

which by the inductive hypothesis equals f_n therefore we get

$$x - f_{n+1} = f_n$$

But by the definition of the Fibonacci numbers this means $x = f_{n+2}$

SKETCH OF SOLUTIONS (HOMEWORK II)

4.- a) yes. b)no, c) yes, d) yes, e) yes, f) no

16.- Suppose the division algorithm yields $a = qb + r$, $q = ct + s$ with $r < b$, $s < c$. Then substituting we get:

$$a = (cb)t + (sb + r)$$

If we show that $sb + r < cb$ we are done (*why?*). Notice $s < c \Rightarrow s + 1 \leq c$ Thus $(s + 1)b \leq cb$ but since $r < b$ we get $sb + r < sb + b \leq cb$

28.- We must require $m, n > 0$

$$\left[\frac{x+n}{m}\right] = \left[\frac{[x+n]}{m}\right] = \left[\frac{[x]+n}{m}\right]$$

The first equality comes from example 1.34 and the second from example 1.31

Section 3.1

2.- a) not prime, b) not prime, c) not pime, d) prime, e) not prime, f) not prime

6.- Notice $n^3+1 = (n+1)(n^2-n+1)$ Therefore n^3+1 is prime iff $n+1 = n^3+1$ (and $n + 1 > 1$) iff $n = 1$

10.- Let p_i be a prime in the list. Without loss of generality we can say p_i divides Q and p_i does not divide R. But then p_i cannot divide $Q + R$. Since $Q + R > p_n$ there must be more than n primes.

Section 3.2

6.- If $b|a$ and $b|a + 2$ then $b|a + 2 - a$ therefore $\gcd(a, a + 2)$ is either 1 or 2. If a is even then $\gcd(a, a + 2) = 2$

7.- By theorem 3.8 we kno (ca, cb) is the least positive integer of the form $cma + cmb = |c||ma + nb|$ therefore $|ma + nb|$ is minimum i.e. $|ma + nb| = (ma, nb)$

31.- Suppose $\frac{ad+bc}{bd} = k$ then $kbd = ad + bc$ therefore $d|bc$. But $d \nmid c$, therefore we must have $d \mid b$. Analogously $b \mid d$

SKETCH OF SOLUTIONS (HOMEWORK III)

5.- a) $\gcd(6,10,15)=1$ b) $\gcd(70,98,105)=7$ c) $\gcd(280,330,405,490)=5$

7.- a) $1(10)+1(6)-1(15)=1$ b) $0(70)-1(98)+1(105)=7$ c) $8(490)-17(405)+9(330)=5$

19.- Notice that if r is the residue of dividing u by v then a^r-1 is the residue of dividing a^u-1 by a^v-1:

$$a^u-1=a^{vq+r}-1=(a^v-1)(a^{v(q-1)}+r+\ldots+a^r)+(a^r-1)$$

((a^r-1) is indeed the residue since $r<v\Rightarrow a^r<a^v$)
Therefore we can perform simultaneously the algorithm for finding $\gcd(m,n)$ and $\gcd(a^m-1,a^n-1)$ and the result follows.

Section 3.4

4.- a) $2,5,$ b) $2,3,5,$ c) $2,3,5,7,$ d) $3,5,7,11,13,23,29$

10.- Suppose p is a prime in the factorization of a such that $p^t\mid a$ but $p^{t+1}\nmid a$. Let $b=q_1^{s_1}\cdots q_n^{s_n}$ be the prime factorization of b. We know $p^{3t}\mid b^2$ therefore there exists q_i such that $q_i=p$ and $3t+\alpha=2s_i$ with $\alpha\geq 0$ therefore $2s_i\geq 3t$ i.e. $s_i\geq\frac{3}{2}t>t$ but this implies $p^t\mid b$

16.- We are looking for the exponent of the maximum power of 10 that we can factor out in the product 1000!. Since $10=2\cdot 5$ we are looking for the exponent of the maximum power of 5 that we can factor out from 1000! (this is less than the exponent of the maximum power of 2 that we can factor out since every other number is even). This equals

$$\sum_{j=1}^{4}\left[\frac{1000}{5^j}\right]=249$$

For finding the number 0's in base 8 we have to find the maximum exponent of a power of 8 that factors out of the product 1000! since $8=2^3$ this equals the number of 2's that we can factor out divided by three:

$$\frac{\sum_{j=1}^{9}\left[\frac{100}{2^j}\right]}{3}=331$$

Section 3.6

2.- a) $x=1+4t$ $y=1-3t$ b) $\gcd(12,18)=6\nmid 50$ therefore there are no solutions c) $x=-121-47t$ $y=77+30t$ d) $x=776-19t$ $y=194+5t$ e) $x=442-1001t$ $y=143t+102t$

3.- The equation we must solve is

$$122x+112y=15286$$

(with the restriction of having positive x and y) this equation has two possible solutions $x=39$, $y=94$ and $x=95$ $y=33$

6.- The equation we must solve is $18x + 33y = 549$ (in order to solve the number x of oranges and y of grapefruit) with the conditions of x and y being positive and y maximum.The solution is $x = 3$ and $y = 15$ which gives a total of 18 pieces of fruit

SKETCH OF SOLUTIONS (HOMEWORK IV)

4.- The equation we must solve is $19x + 59y = 1706$ with the restriction of x, y being positive. The solution is $x = 37$, $y = 17$

21.- Let x be the number of cocks, y the number of hens and z the number of chickens We have to solve the equations

$$\begin{array}{lcl} x + y + z & = & 100 \\ 5x + 3y + \frac{z}{3} & = & 100 \end{array}$$

with the condition of x, y, z being non-negative. The solutions are

$$(x, y, z) = \begin{cases} (0, 25, 75) \\ (4, 18, 78) \\ (8, 11, 81) \\ (12, 4, 84) \end{cases}$$

Section 4.1

5.- Suppose $a = 2n+1$ then $a^2 = 4n(n+1)+1$, since either n or $n+1$ is even, we have that $8 \mid 4n(n+1)$ therefore $a^2 \equiv 1 \mod 8$

22.- **Base:** $4 \equiv 1 + 3 \mod 9$
Inductive step: Suppose $4^n \equiv 1 + 3n \mod 9$ then $4^{n+1} \equiv 4 + 12n \equiv 1 + 3 + 12n \equiv 1 + 3(1 + 4n) \mod 9$ therefore we only need to show that $3(1 + 4n) \equiv 3(n + 1) \mod 9$ but $3 + 12n \equiv 3n + 3 \mod 9 \Leftrightarrow 12n - 3n \equiv 0 \mod 9 \Leftrightarrow 9n \equiv 0 \mod 9$

26.- We are looking for solutions of $x(x-1) \equiv 0 \mod p$. Since p is prime, either $p \mid x$ or $p \mid x - 1$ i.e. $x \equiv 0 \mod p$ or $x \equiv 1 \mod p$

28.- a) 42 b) 2 c) $2^{200} = 2^{4*47+12} = (2^{12})(2^4)^{47} \equiv (2^{12})(2^4) \equiv 2^{16} \equiv 18(\mod 47)$

38.- 15621

Section 4.2

2.- a) $x \equiv 3(\mod 7)$ b) $x \equiv 2, 5, 8(\mod 9)$ c) $x \equiv 7(\mod 21)$ d) No solutions e) $x \equiv 812(\mod 1001)$ f) $x \equiv 1596(\mod 1597)$

6.- There are solutions iff $\gcd(12, 30) = 6 \mid c$ therefore iff $c \equiv 0, 6, 12, 18, 24 \mod 30$ in every case there are 6 incongruent solutions $\mod 30$ (By theorem 4.10)

8.- a) 7, b) 9, c) 8, d) 6

SKETCH OF SOLUTIONS (HOMEWORK V)

4.- a) $37 \mod 187$, b) $23 \mod 30$

12.- We have to solve the system:

$$\begin{aligned} x &\equiv 1 \mod 2 \quad (1)\\ x &\equiv 2 \mod 3 \quad (2)\\ x &\equiv 3 \mod 4 \quad (3)\\ x &\equiv 4 \mod 5 \quad (4)\\ x &\equiv 5 \mod 6 \quad (5)\\ x &\equiv 0 \mod 7 \quad (6)\end{aligned}$$

We *can not* use the Chinese remainder theorem directly since the moduli are not relatively prime. If we solve the system involving equations (2), (3), (4) and (6) the answer is $119 \mod 420$. Notice that this also solves the first and fifth congruences.

22.- The system we must solve is:

$$\begin{aligned} x &\equiv 3 \mod 17 \quad (7)\\ x &\equiv 10 \mod 16 \quad (8)\\ x &\equiv 0 \mod 15 \quad (9)\end{aligned}$$

Using the Chinese remainder theorem we get $x = 3930$

24.- Take a set of numbers (each < 100) whose product is greater than the product of 784 and 813 and such that they are pairwise relatively prime. And use the Chinese remainder theorem. Example: Take $97, 98, 99$, and let $x = 784$, $y = 813$ then:

$$\begin{array}{lllllll} x & \equiv & 8 \mod 97 & \quad & y & \equiv & 37 \mod 97\\ x & \equiv & 0 \mod 98 & & y & \equiv & 29 \mod 98\\ x & \equiv & 91 \mod 99 & & y & \equiv & 21 \mod 99\end{array}$$

Using the Chinese remainder theorem we solve the equations

$$\begin{array}{llllllllll} x+y & \equiv & 8+37 & \equiv & 45 \mod 97 & \quad xy & \equiv & 8*37 & \equiv & 5 \mod 97\\ x+y & \equiv & 0+29 & \equiv & 29 \mod 98 & \quad xy & \equiv & 0*29 & \equiv & 0 \mod 98\\ x+y & \equiv & 91+21 & \equiv & 13 \mod 99 & \quad xy & \equiv & 91*21 & \equiv & 30 \mod 99\end{array}$$

Therefore $x + y = 1597$ and $xy = 637392$

Section 4.4

1.- a) $x = 1, 2$ b) $x = 8, 37$ c) $x = 132, 211$ (assuming the equation is $x^2 + 4x + 2 = 0$ the solution is $106, 233$)

10.- Three, namely: $6, 51$ and 123

Section 4.5

2.- a) $y = n, x = 6 + 2n$ b) no solutions

4.-

$$\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$$

8.- b)

$$\begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$$

14.- Let k and l be integers between 0 and $n^2 - 1$. Suppose that they fall into the same entry (i, j) of the matrix. Then we have:

$$\begin{aligned} a + ck + e[k/n] &\equiv a + cl + e[l/n] \mod n \\ b + dk + f[k/n] &\equiv b + dl + f[l/n] \mod n \end{aligned} \tag{10}$$

This system is equivalent to:

$$\begin{aligned} c(k - l) + e([k/n] - [l/n]) &\equiv 0 \mod n \\ c(k - l) + e([k/n] - [l/n]) &\equiv 0 \mod n \end{aligned}$$

Since the matrix

$$\begin{pmatrix} c & e \\ d & f \end{pmatrix}$$

has determinant $cf - de$ which by hypothesis is relatively prime to n there is exactly one solution to the system, namely $(0, 0)$. Therefore $k \equiv l \mod n$ and $[k/n] \equiv [l/n] \mod n$ Since $0 \leq k, l \leq n^2 - 1$ we must have $0 \leq k/n, l/n \leq n - 1/n$ Thus $|k - l| < n$. Then, since $k \equiv l \mod n$ we have that $k = l$

SKETCH OF SOLUTIONS (HOMEWORK VI)

12.- The repunits with an even number of digits.

19.- Let $a = (a_n a_{n-1} \dots a_0)_1 0$ then $a = \sum_{i=0}^{n} a_i 10^i \equiv a_0 + a_1 10 + a_2 100 + 1000(a_3 + a_4 10 + a_5 100) + \dots \equiv (a_0 a_1 a_2) + (a_3 a_4 a_5) + \dots \mod 37$ Therefore a is divisible by 37 iff $(a_0 a_1 a_2) + (a_3 a_4 a_5) + \dots$ is divisible by 37. Using this test we get that $443,692 \equiv 443+692 \equiv 1135 \not\equiv 0 \mod 37$ and $11,092,785 \equiv 11 + 92 + 785 \equiv 88 \equiv 0 \mod 37$

22.- Since $88 = 11 \cdot 8$ we must have $8 \mid x42y$ therefore $8 \mid 42y$ therefore $y = 4$ since $11 \mid x424$ we must have $11 \mid 4-2+4-x$ i.e. $11 \mid 6-x$. Therefore $x = 6$

Section 5.5

8.- a) $5 \mod 10$

b) Let $(x_i)_{10}$ be the correct id and $(y_i)_{10}$ be the id with a single error. Then $(x_i)_{10} - (y_i)_{10} \equiv a(x_k - y_k) \mod 10$ with a being either $3, 7$ or 9. Since $3, 7$ and 9 are units modulo 10 a single error can always be detected.

c) A transposition which are not detected are the transpositions of digits x_i and x_j such that $i \mid j \mod 3$ or $x_i \equiv x_j \mod 5$

12.- a) 7 b) 9 c) 7

13.- $0 - 07 - 289905 - 0$

16.- a) 2 b) 4 c) 3 d) 7

17.- Let $(x_i)_{10}$ be the correct UPC code and $(y_i)_{10}$ be the UPC code with a single transposition. Then $(x_i)_{10} - (y_i)_{10} \equiv a(x_k - y_k) \mod 10$ where a is either 3 or 1. Since 1 and 3 are units modulo 10 a single transposition can always be detected.

SKETCH OF SOLUTIONS (HOMEWORK VII)

3.- By Wilson's theorem $18 \equiv 18! \equiv 16!(17)(18) \mod 19$ Therefore $1 \equiv 16!(-2) \mod 19$ i.e. $-10 \equiv 16! \mod 19$ so $9 \equiv 16! \mod 19$

12.- $2^{1000000} \equiv (2^{16})^{62500} \equiv 1^{62500} \equiv 1 \mod 17$

15.- a) $7^{15} \equiv (7^3)^5 \equiv 3^5 \equiv 5 \mod 17$ Therefore $x \equiv 7^{15} \cdot 12 \equiv 5 \cdot 12 \equiv 9 \mod 17$

b) Analogously $4^{17} \equiv 5 \mod 19$ Therefore $x \equiv 5 \cdot 11 \equiv 17 \mod 19$

20.- Notice $168 = 2^3 \cdot 3 \cdot 7$ Since $(42, a) = 1$ we know a is odd, therefore $a^6 \equiv (a^2)^3 \equiv 1 \mod 8$ (since every unit modulo 8 has order 2).Also, by FLT we get $a^6 \equiv (a^2)^3 \equiv 1 \mod 3$ and $a^6 \equiv 1 \mod 7$. These three congruences imply $a^6 \equiv 1 \mod 168$

22.- Since $30 = 2 \cdot 3 \cdot 5$. We only need to solve $n^9 - n \equiv 0 \mod 2, 3, 5$ notice that if $n \equiv 0 \mod 2, 3, 5$ the congruences are satisfied. Otherwise n is a unit $\mod 2, 3, 5$ and we obtain the equivalent set of congruences $n^8 \equiv 1 \mod 2, 3, 5$. These sete of congruences can be simultaneously solved by FLT

23.- Apply FLT to every term of the sum. Adding all the terms we get $p-1 \equiv -1 \mod p$

Section 6.3

2.-

$$17^{45} \equiv 17^{4 \cdot 11} 17 \equiv 1^{11} 17 \equiv 17 \mod 45$$
$$19^{45} \equiv 19^{2 \cdot 22} 19 \equiv 1^{22} 19 \equiv 19 \mod 45$$

7.- We know

$$2^{2^n} \equiv -1 \mod F_n$$

raising each side of the congruence to the power $2^{2^n - n}$ we get

$$\left(2^{2^n}\right)^{2^{2^n - n}} \equiv 2^{2^n (2^{2^n - n})} \equiv 2^{2^{2^n}} \equiv 1 \mod F_n$$

MAT 311 **Midterm 1** **Mar 11, 2003**

Name: ____________________ **Id:** ____________________

You may use a calculator. You may **NOT** use any books or notes. Please write full solutions, not just answers. **Show your work**, **explain your reasoning**, and cross out anything I should ignore when grading. This midterm has 6 questions, for a total of 100 points. Good luck!

	1 15 pts	2 15 pts	3 15 pts	4 20 pts	5 15 pts	6 20 pts	**Total** 100 pts
Score							

1. (15 points) For each of the congruences below, find all solutions (if any).
   (a) $927x \equiv 4 \bmod 102$
   (b) $928x \equiv 4 \bmod 102$

2. (15 points) An Japanese tourist returning home from a trip to Europe and U.S. exchanges his Euro and Dollar bills for yens. If he receives $15,286$ yen, and received 112 yen for each Euro and 122 for each U.S. Dollar, and he had more Dollars than Euros, how many of each type of currency did he exchange ?

3. (15 points) What is the smallest natural number n such that

$$n \equiv 1 \bmod 3$$
$$n \equiv 3 \bmod 8$$
$$n \equiv 2 \bmod 5$$

4. (a) (10 points) What is the last digit in the decimal representation of 7^{19522}?
   (b) (10 points) Find all the solutions to the congruence

$$x^2 + x \equiv 0 \bmod 437 \qquad (437 = 23 * 19)$$

5. (15 points) Find at least one solution to the following congruence:

$$x^2 - 3x - 7 \equiv 0 \bmod 27$$

6. (a) (10 points) Determine if the following ISBN number is valid:

$$0 - 404 - 50874 - 9$$

   (b) (10 points) While copying the ISBN for a book, a clerk accidentally transposed two digits. If the clerk copied the ISBN as 0-07-289095-0 and did not make any other mistakes, what is the correct ISBN for the book ?

SKETCH OF SOLUTIONS (MIDTERM EXAM)

1.- For each of the congruences below, find all solutions (if any).

(a) $927x \equiv 4 \mod 102$

Notice that $927 \equiv 9 \mod 102$ *and* $(9, 102) = 3$*. Since* 4 *is not a multiple of* $3 \mod 102$ *there are no solutions.*

(b) $928x \equiv 4 \mod 102$

Now we must solve $10x \equiv 4 \mod 102$*. Since* $(10, 102) = 2$ *and* $x \equiv 31 \mod 51$ *the solutions are* $x \equiv 31 \mod 102$ *and* $x \equiv 31 + 51 \equiv 82 \mod 102$

2.- A Japanese tourist returning home from a trip to Europe and U.S. exchanges his Euro and Dollar bills for yens. If he receives 15,286 yen, and received 112 yen for each Euro and 122 for each U.S. Dollar, and he had more Dollars than Euros, how many of each type of currency did he exchange?

Let e *denote the number of euros and* d *the number of dollars, then we must solve the following equation:*

$$112e + 122d = 15286$$

with the restrictions $e, d \geq 0$ *and* $d > e$

Since $122/2 = 61$ *which is prime we have* $(122, 112) = 2$ *Using the euclidean algorithm we find*

$$112(12) - 122(11) = 2$$

Therefore

$$112(12)(7643) - 122(11)(7643) = 2 * 7643 = 15286$$

So all solutions are of the form

$$d = -84073 + 56t, \ \ e = 91716 - 61t$$

Now, e *is positive if* $t > 1501$ *and* d *is positive if* $t < 1504$ *therefore the only possible solutions are* $d = 39$, $e = 94$ *and* $d = 95$, $e = 33$*. But we know* $d > e$ *therefore the solution is* $d = 95$, $e = 33$

3.- What is the smallest natural number n such that

$$\begin{aligned} n &\equiv 1 \mod 3 \\ n &\equiv 3 \mod 8 \\ n &\equiv 2 \mod 5 \end{aligned}$$

Using the Chinese remainder theorem we find the solution:

$$x = (1)(8 * 5)(1) + (3)(3 * 5)(7) + (2)(8 * 3)(4) \equiv 67 \mod 120$$

4.-

(a) What is the last digit in the decimal representation of 7^{19522}?
We are asked to find the smallest natural number which represents the class of $7^{19522} \mod 10$. *Notice that*

$$7^2 \equiv 9 \mod 10$$

$$7^3 \equiv 7 * 7^2 \equiv 7 * 9 \equiv 3 \mod 10$$

and finally

$$7^4 \equiv 7 * 7^3 \equiv 7 * 3 \equiv 1 \mod 10$$

Therefore the remainder we are looking for only depends on the equivalence class of $19522 \mod 4$. *But* 19522 *can only be divided once by* 2, *therefore* $19522 \equiv 2 \mod 4$. *Therefore* $7^{19522} \equiv 7^2 \equiv 9 \mod 10$

(b) Find all the solutions to the congruence

$$x^2 + x \equiv 0 \mod 437$$

$x^2 + x \equiv x(x+1) \mod 437$. *Also, using the fact that* $437 = 23 * 19$ *we find first all the solutions modulo* 23 *and modulo* 19 *which are* $0, 18, 22$ *Now we solve the systems of congruences*

$$\begin{aligned} x &\equiv 18 \mod 19 \\ x &\equiv 22 \mod 23 \end{aligned}$$

$$\begin{aligned} x &\equiv 0 \mod 19 \\ x &\equiv 22 \mod 23 \end{aligned}$$

$$\begin{aligned} x &\equiv 18 \mod 19 \\ x &\equiv 0 \mod 23 \end{aligned}$$

$$\begin{aligned} x &\equiv 0 \mod 19 \\ x &\equiv 0 \mod 23 \end{aligned}$$

and we get all possible solutions, namely $x \equiv 436, 114, 322, 0 \mod 437$

5.- Find at least one solution to the following congruence:

$$x^2 - 3x - 7 \equiv 0 \mod 27$$

We start by looking for solutions $\mod 3$. *Let* $f(x) = x^2 - 3x - 7$ *Then* $f(x) \equiv (x+1)(x-1) \mod 3$ *therefore* $f(1) \equiv 0 \mod 3$ *Using the fact that* $f'(1) \neq 0 \mod 3$, *by Hensel's lemma* $f(1+0) \equiv 0 \mod 3^2$. *Again,* $f(1) \neq 0 \mod 3^2$ *and* $f'(1) \neq 0 \mod 3$ *therefore* $f(1 + 2 * 9) = 0 \mod 3^3$ *i.e.* 19 *is a solution of the congruence. (the other possible solution is* 11*)*

6.- (a) Determine if th following ISBN number is valid:

$$0 - 404 - 50874 - 9$$

Not valid:

$$(1)(0)+(2)(4)+(3)(0)+(4)(4)+(5)(5)+(6)(0)+(7)(8)+(8)(7)+(9)(4)+(10)(9) \equiv 287 \equiv 1 \mod 11$$

(b) While copying the ISBN for a book, a clerk accidentally transposed two digits. If the clerk copied the ISBN as 0-07-289095-0 and did not make any other mistakes, what is the correct ISBN for the book?
Let $x_1 \ldots x_{10}$ *be the digits of the correct ISBN, and let* $y_1 \ldots y_{10}$ *be the digits of the given ISBN. Since* $\sum_{i=1}^{10} iy_i \equiv 9 \mod 11$ *and* $\sum_{i=1}^{10} ix_i \equiv 0 \mod 11$ *we must have* $\sum_{i=1}^{10} i(y_i - x_i) \equiv 9 \mod 11$ *but we know that* $x_i = y_i$ *for all* i *except for two values* j, k *which are transposed.*

Therefore all terms in the last sum are zero with the exceptions of the terms corresponding to j and k i.e.

$$j(y_j - x_j) + k(y_k - x_k) \equiv 9 \mod 11$$

We also know that $y_j = x_k$ and $y_k = x_j$ therefore we get the equation

$$j(y_j - y_k) + k(y_k - y_j) \equiv (y_j - y_k)(j - k) \equiv 9 \mod 11$$

By trial, we find that $j = 8$ and $k = 7$ work:

$$(y_8 - y_7)(8 - 7) \equiv (9)(1) \equiv 9 \mod 11$$

Therefore the correct ISBN is $0 - 07 - 289905 - 0$

SKETCH OF SOLUTIONS (HOMEWORK VIII)

1.- a) $\{1, 5\}$ b) $\{1, 2, 4, 5, 7, 8\}$ c) $\{1, 3, 7, 9\}$ d) $\{1, 3, 5, 9, 11, 13\}$ e) $\{1, 3, 5, 7, 9, 11, 13, 15, 17\}$ f) $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$

6.- Notice that $\Phi(10) = 4$ and $999,999 = 4(249,999)+3$. Using Euler's theorem we get that the last decimal digit is 3.

8.- Using Fermat's theorem we get $a^7 \equiv a \mod 7$. We only need to show that $a^9 \equiv a \mod 9$ (since $9 \cdot 7 = 63$). If $9 \mid a$ we have $0 \equiv 0 \mod 9$. If $3 \nmid a$ then $(a, 9) \equiv 1$. But since $\Phi(9) = 6$ we have $a^6 \equiv 1 \mod 9$ i.e. $a^7 \equiv a \mod 9$.

12.- Notice that x is a solution by Euler's theorem, and it is unique by the Chinese remainder theorem.

Section 7.1

1.- a) Yes: $f(mn) = 0 = 0 \cdot 0 = f(m)f(n)$, b) No: $f(2 \cdot 2) = 2 \neq 4 = f(2)f(2)$, c) No: $f(2 \cdot 3) = 3 \neq \frac{2}{2}\frac{3}{2} = f(2)f(3)$, d) No: $\log(4) > 1$ (since $4 > e$) but $\log(2)\log(2) < 1$, e) Yes: $f(mn) = (mn)^2 = m^2n^2 = f(m)f(n)$, f) No: $f(2 \cdot 2) = 4! \neq 4 = f(2)f(2)$, g) No: $f(1 \cdot 1) = 2 \neq 2 \cdot 2 = f(1)f(1)$, h) No: $f(4) = 4^4 = 256 \neq 16 = f(2)f(2)$, i) Yes: $f(mn) = \sqrt{mn} = \sqrt{m}\sqrt{n} = f(m)f(n)$

2.- c) $\Phi(1001) = \Phi(7 \cdot 11 \cdot 13) = 6 \cdot 10 \cdot 12 = 720$ e) Using theorem 7.5 we get $\Phi(10!) = 10!(1-1/2)(1-1/3)(1-1/5)(1-1/7)$ (All the prime factors must be all the primes less than or equal to 10). $= 829, 440$

3.- They all equal 2592

5.- We know $6 = \Phi(n) = \Pi_{j=1}^{k} p_j^{a_j-1}(p_j - 1)$. But since $\Phi(p) \geq 4$ for all primes greater than or equal to 5, we must have $k \leq 2$.(Otherwise three or more prime factors would give a value of $\Phi(n)$ greater than or equal to $4 \cdot 2$) If $k = 1$ then $p_1^{a_1-1}(p_1 - 1) = 6$ Notice that we only need to try values of p_1 between 2 and 7. The solutions for this case are $n = 7, 9$. If $k = 2$ then the solutions are $n = 14, 18$.

14.- Suppose $k\Phi(n) = kn(p_1 - 1)/p_1 \cdots (p_r - 1)/p_r = n$. Then $k = p_1/(p_1 - 1) \cdots p_r/(p_r - 1)$ is an integer. There can be at most one even number among the p_i (because 2 is the only even prime), so there can be at most one odd prime among the p_i (since k is an integer). The only possible values for n are $n = 1, 2^{a_1}, 2^{a_1}3^{a_2}$ with $a_1, a_2 \geq 1$

35.- a) If either $m > 1$ or $n > 1$ then $mn > 1$ and one of $i(m)$ or $i(n)$ is equal to zero. Then $i(mn) = 0 = i(m)i(n)$. Otherwise, $m = n = 1$ and we have $i(mn) = 1 = 1 \cdot 1 = i(m)i(n)$.

b) $(i * f)(n) = \sum_{d|n} i(d)f(n/d) = i(1)f(n) = f(n)$ by the definition of i. $f * i(n) = \sum_{d|n} f(d)i(n/d) = f(n)$ also by the definition of i

SKETCH OF SOLUTIONS (HOMEWORK IX)

2.- a) $\tau(36) = \tau(2^2 3^2) = (2+1)(2+1) = 9$, b) $\tau(99) = \tau(3^2 \cdot 11) = (2+1)(1+1) = 6$, c) $\tau(144) = \tau(2^4 \cdot 3^2) = (4+1)(2+1) = 15$

21.- $\sigma_k(p) = 1 + p^k$

22.- $\sigma_k(p^a) = \frac{p^{k(a+1)}-1}{p-1}$

23.- Let a, b be such that $(a, b) = 1$. Then $\sum_{d|ab} d^k = \sum_{d|a,d|b} (d_1 d_2)^k = \sum_{d|a} d_1^k \sum_{d_2^k} = \sigma_k(a)\sigma_k(b)$

34.- Both sides of the equality are multiplicative functions, therefore we only need to verify that they coincide for $n = p^k$ with p prime and k a positive integer. But in this case:

$$\left(\sigma_{d|p^k} \tau(d)\right)^2 = \left(\sum_{j=0}^{k} \tau(p^j)\right)^2 = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

(using the formula for the sum of the first $k+1$ positive integers). Also,

$$\sum_{d|p^k} \tau(d)^3 = \sum_{j=0}^{k} \tau(p^j)^3 = \left(\frac{(k+1)(k+2)}{2}\right)^2$$

(using the formula for the sum of the cubes of the first $k+1$ positive integers)

37.- Let M be the matrix with entries (i, j). Let D be the matrix with entries $\Phi(1), \Phi(2), \ldots, \Phi(n)$ on the diagonal and zeros elsewhere. Let A be the matrix defined by the rule: If i divides j then the (i, j)-th entry is 1 and it is zero otherwise. Notice that A has only zeros below the main diagonal, therefore $\det(A) = \det(A^t) = 1$. Also notice that $D = ADA^t$ (to prove this, use the identity $\sum_{k|(i,j)} \Phi(k) = (i, j)$ and the fact that if $k \mid i$ and $k \mid j$ then $k \mid (i, j)$). Since $\det(D) = \det(ADA^t) = 1 \cdot \det(D) \cdot 1 = \Phi(1)\Phi(2) \cdots \Phi(n)$ we are done.

Section 7.4

1.- a) 0, b) 1

15.- Using Moebius inversion formula with the identity $n = \sum_{d|n} \Phi(d)$ we get that $\Phi(n) = n \sum_{d|n} \mu(d)/d$

17.- Since f and μ are multiplicative, so is $f\mu$ and also $\sum_{d|n} \mu(d)f(d)$. Therefore it suffices to prove the theorem for prime powers. But

$$\sum_{d|p^a} \mu(d)f(d) = \mu(p^a)f(p^a) + \ldots \mu(p)f(p) + \mu(1)f(1) = -f(p) + 1$$

(Since $\mu(p^j) = 0$ for $j > 1$)

18.- Using $f(n) = n$ in exercise 17 we get $\sum_{d|n} d\mu(d) = \Pi_{i=1}^{k}(1 - p_i)$

23.- Using $f(n) = \mu(n)$ in exercise 17 we get $\sum_{d|n} \mu(d)\mu(d) = 2 \cdot 2 \cdots 2$ where the last product has $\omega(n)$ factors.

SKETCH OF SOLUTIONS (HOMEWORK X)

3.- DWWDF NDWGD ZQ

14.- E is mapped into J and E is mapped into O. $a = 9$ and $b = 25$ the message is: WE USE FREQUENCIES OF LETTERS TO DECRYPT SECRET MESSAGES

15.- $C \equiv 17(5P+13)+3 \equiv 85P+224 \equiv 7P+16 \mod 26$

Section 8.2

1.- VSPJXH HIPLKB KIPMIE GTG

3.- Look for repeated patterns of letters, the gcd of the lengths of the distances between patterns is likely to be the length of the cipher, or period (say it is k). Then perform the frequency-count analysis on characters which are at distance k from each other.

4.- The period is 3. The cipher is BOX. The plaintext is: TOBEO RNOTT OBETH ATIST HEQUE STION WHETH ERTIS NOBLE RINTH EMIND TOSUF FERTH ESLIN GSAND ARROW SOFOU TRAGE OUSFO RTUNE

13.- $C = AP \mod 26$ where

$$A = \begin{pmatrix} 11 & 6 \\ 2 & 13 \end{pmatrix}$$

18.- DQ BC IG KT AC EX

19.-

$$P \equiv \begin{pmatrix} 17 & 4 \\ 1 & 7 \end{pmatrix} C + \begin{pmatrix} 22 \\ 15 \end{pmatrix} \mod 26$$

Section 8.4

3.- Since a block of ciphertext p is less than n, we must have $(p,n) = p$ or $(p,n) = q$. Therefore the cryptanalyst has a factor of n

4.- The probability that it is divisible by p is $1/p$ and the probability that it is divisible by q is $1/q$. Also, since 0 is the only integer between 0 and $n-1$ which is divisible by both p and q, the probability of being divisible by both of them is $1/pq$. Using the formula for the probability of the union we get $P(\gcd(P,n) > 1) = 1/p + 1/q - 1/pq$

6.- 101900141066218713492155

7.- GR EE TI NG SX

11.- Let P be the plaintext message and the two encrypting exponents e_1 and e_2. Let $a = (e_1, e_2)$. Then there exist integers x and y such that $e_1x + e_2y = a$. Let $C_1 \equiv P^{e_1} \mod n$ and $C_2 \equiv P^{e_2} \mod n$ be the two cipher texts. Since C_1, C_2, e_1 and e_2 are known, and since x and y can be computed, we can compute $C_1^x C_2^y \equiv P^{e_1x} P^{e_2y} \equiv P^{e_1x+e_2y} \equiv P^a \mod n$. Then computing the ath roots of P^a we recover P

SKETCH OF SOLUTIONS (HOMEWORK XI)

1.- $5^{27} \equiv 94 \mod 103$ and $94^{31} \equiv 90 \mod 103$

6.- a) $\Phi(19 \cdot 67) = 1188$ and $(713 \cdot 5) \equiv 1 \mod 1188$. The numerical equivalents of the message are:

$$0614, 1403, 0418, 2204, 0419, 1114, 2104$$

The decryption function is raising each block to the 713th power $\mod 19 \cdot 67$. We get:

$$1100, 0731, 0945, 0304, 0285, 0324, 1046, 1248$$

Since the other modulus is smaller we split each block in two before encrypting them with the other key. The encryption function is raising each block to the 3rd power and reducing modulo $11 \cdot 71$. We get.

$$550, 000, 343, 113, 729, 529, 027, 064, 008, 259, 027, 547, 219, 492, 166, 471$$

b) Same procedure as in a) (with the appropriate keys!!) The message is:

$$000, 266, 32, 1119, 225, 442, 900, 1127, 1119, 999, 1119, 1127$$

10.- $K_0 = K + tp = 5 + 14 \cdot 7 = 103$. The three shadows are given by $k_1 \equiv 103 \equiv 4 \mod 11$, $k_2 \equiv 103 \equiv 7 \mod 12$, $k_3 \equiv 103 \equiv 1 \mod 17$

Section 9.1

1.- a)4, b) 4, c) 6, d) 4

6.- Notice that the group of units $\mod 20$ is $\{1, 3, 9, 7\} \times \{1, 19\} =< 3 > \times < 19 >$ therefore the highest order is 4

10.- Suppose $\text{ord}_n a = r$ and $\text{ord}_n b = s$. Then

$$(ab)^{rs} = a^{rs} b^{rs} = (a^r)^s (b^s)^r = 1$$

Therefore $t := \text{ord}_n(ab) \mid rs$. Also, notice that

$$1 \equiv (ab)^t \equiv (ab)^{rt} \equiv (a^r)^t b^{rt} \equiv b^{rt} \mod n$$

But this implies that $s \mid rt$, thus $s \mid t$ (since $(r, s) = 1$) Similarly $r \mid t$. Therefore $rs \mid t$. i.e. $rs = t$

18.- Let $h = \text{ord}_p 2$ Then $h \mid \Phi(p) = p - 1$. Note that $2^{2^n} \equiv -1 \mod p$, so $(2^{2^n})^2 \equiv 2^{2^{n+1}} \equiv 1 \mod p$. Therefore, $h \mid 2^{n+1}$, say $h = 2^k$. But if $k < n + 1$ then $2^{2^n} \equiv 1 \mod p$ (a contradiction. Therefore $h = 2^{n+1}$

b) Since $2^{n+1} = \text{ord}_p 2 \mid \Phi(p) = p - 1$, we have $2^{n+1} k = p - 1$ or $p = 2^{n+1} k + 1$

MAT 311 -- Information about Project 1

Project 1 should be handed in by 03/06. Please select one of the topics listed below. You need to make your selection and also inform me of it by 2/20. All programming projects and Computing and Programming Exercises (CPE) are taken from the 4th edition of Rosen's textbook.

- A proof that the rational and algebraic numbers are countable and that the irrationals and transcendental numbers are not.
- A short (2 to 4 typed pages) biography of a prominent number theorist.
- A proof of unique factorization in **Z**+**Z**[i] (where i is the imaginary unit).
- Programming project 1.3.1
- CPE 3.1.16
- Programming project 3.3.5.
- CPE 3.4.2
- CPE 4.4.2
- Programming project 4.5.1.
- Programming project 4.6.1.
- Programming project 5.1.2.

For any of the programming projects, please email me at `sorin@math.sunysb.edu` the program source code (in readable form -- indented and commented), and 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*...

Back to MAT 311 home page

MAT 311 -- Information about Project 2

Project 2 should be handed in by 04/29. Please select one of the topics listed below. You need to make your selection and also inform me of it by 4/15. All programming projects and Computing and Programming Exercises (CPE) are taken from the 4th edition of Rosen's textbook.

- Programming project 6.1.2.
- Programming project 6.2.2.
- Computational and Programming Exercise 7.1.6
- Computational and Programming Exercise 7.2.4
- Programming project 7.4.1.
- Programming project 8.1.4.
- Programming project 8.2.1.
- Programming project 9.3.2.
- A short (2 to 4 typed pages) paper on the mathematical contributions of a number theorist. Note: This is not a biography - you will need to describe mathematical results, their proofs, etc.

For any of the programming projects, please email me at `sorin@math.sunysb.edu` the program source code (in readable form -- indented and commented), and 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*...

Back to MAT 311 home page