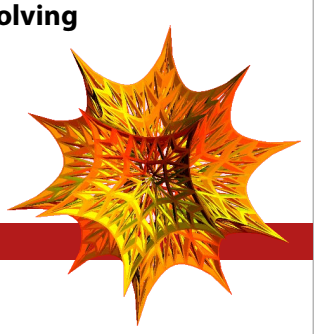
MAT 331: Computer Assisted Mathematical Problem Solving
Spring 2017
Raluca Tanase



Course Information

Course Description

Exploration of the use of the computer as a tool to gain insight into complex mathematical problems through a project-oriented approach. Students learn both the relevant mathematical concepts and ways that the computer can be used (and sometimes misused) to understand them. Interesting applications of mathematics to computer science are also discussed. Some of the specific topics that we will try to study this semester include linear algebra, graph theory and Markov chains, number theory and cryptography, dynamical systems and fractals, differential equations and computer graphics.

Click here to download a copy of the course syllabus. Please visit the **course website on Blackboard**.

Lectures & Office Hours

Instructor: Raluca Tanase
Lectures: Tuesdays & Thursdays 11:30-12:50pm in Mathematics S235;
Office hours: Tuesdays 1-2pm in MLC (next to the computer lab)
Thursdays 1-3pm in Math Tower 4-120, or by appointment.

Teaching Assistant: Nancy Hong
Office hours: Wednesdays 12-1pm in Mathematics S235 (computer lab).

Software

We will use *Mathematica*, which is a computational software program developed by Wolfram Research and used in many scientific, engineering, mathematical and computing fields, based on symbolic mathematics. *Mathematica* has a **comprehensive documentation** that we will make use of. *Mathematica* 10.3 is available for most operating systems (Windows, Macintosh, Linux, etc.).

Stony Brook students can download the Windows/Mac/Linux version of *Mathematica* from **Softweb**. You need your Stony Brook netID and netID password to log in to Softweb. To obtain an Activation Key for *Mathematica* you must visit the **Wolfram User Portal**. If it's your first time visiting the Wolfram User Portal, you must create a Wolfram ID and follow the steps in there to request an **Activation Key**.

In addition, you can use any of the campus SINC sites, or you can access the **Virtual SINC site**.

Grading Policy

There will be no exams. Grades will be computed using the following scheme:

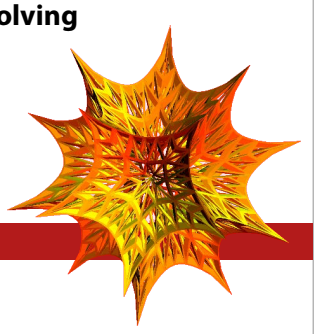
- Homework – 20%
- Lab Activity – 15%
- Projects – 65%

Students are expected to attend class regularly and to keep up with the material presented in the lecture and the assigned reading. There will be roughly five homework assignments (containing short exercises involving mathematical proofs and *Mathematica* code) as well as three or four projects. You may work together on your homework assignments and projects, and

you are encouraged to do so. However, all solutions must be written up independently.
A project is more like a term paper and you will be expected to devote a significant amount of time to doing it, as well as taking care with its presentation. The project should contain a detailed description of the problem or topic, what means were used to solve it, the mathematical solution and proofs, and the computer program (interactive model in Mathematica). The last project of the class may include also a short oral presentation at the end of the semester.

MAT 331: Computer Assisted Mathematical Problem Solving
Spring 2017
Raluca Tanase

Lectures, Homework & Projects



Schedule

A set of lecture notes for each class will be available in .pdf format and .nb (*Mathematica* notebook). Please log in to Blackboard with your netID and password to download the solutions to the homework assignments.

Date	Topic	Reading	Assignments
Jan 24	Introduction & **Syllabus**	Notes (**nb**)	**HW1.nb** **HW1-Files.zip** Due February 11
Jan 26	Functions and Plotting Commands	Notes (**nb**)	
Jan 31	Conditional Statements and Loop Structures	Notes (**nb**)	
Feb 2	Linear Algebra in *Mathematica*	Notes (**nb**)	
Feb 7	Linear Algebra and Graph Theory	Notes (**nb**)	**HW2.nb** Due February 23
Feb 14	Making Interactive Models in *Mathematica*	Notes (**nb**)	
Feb 16	Using Dynamic[..] and Manipulate[..]	Notes (**nb**), **Map**	
Feb 21	Lab Exercises	Notes (**nb**)	**Project 1** Due March 12
Feb 23	Mathematics of Web Search	Notes (**nb**)	
Feb 28	Project Discussion	Notes (**nb**)	
March 2	Eigenvalues, Eigenspaces, multiplicity of an eigenvalue	**Lectures 1** & **2**	
March 7	Perron-Frobenius Theorem & Page Rank	**Lectures 3** & **4**	
March 9	Dynamical Systems, Fractals, Julia sets	Notes (**nb**)	**HW3.nb** Due March 31
March 14-16	*no classes this week, Spring Break!*		

March 21	Solvers	Notes (**nb**)	
March 23	Solving Differential Equations with Mathematica	Notes (**nb**)	
March 28	Linear Systems of Differential Equations	Notes (**nb**)	**Project 2** Due April 20
March 30	Nonlinear Systems of Differential Equations	Notes (**nb**)	
April 4	Nonlinear Systems (II)	Notes (**nb**)	
April 6	Solutions to the Lab Exercises	Notes (**nb**)	
April 11	Limit Cycles and Chaotic Behavior	Notes (**nb**)	
April 13	Interactive models with Phase Portraits and Locator	Notes (**nb**)	
April 18	An Introduction to Cryptography	Notes (**nb**)	**HW4.nb** Due April 27
April 20	Modular Arithmethic & Affine Ciphers	Notes (**nb**)	
April 25	Cryptanalysis of (mono/poly)alphabetic Ciphers	Notes (**nb**) Vigenere (**nb**)	**Project 3** Due May 13
April 27	Fermat's Little Theorem & Euler's Theorem	Lecture (**pdf**)	
May 2	The RSA Cryptosystem	Notes (**nb**)	
May 4	Digital Signatures	Notes (**nb**)	
May 10	Project Presentation - Wednesday, May 10, 5:30-8pm		

MAT 331: COMPUTER-ASSISTED MATHEMATICAL PROBLEM SOLVING
SPRING 2017
GENERAL INFORMATION

Instructor. Raluca Tanase
Email: raluca.tanase@stonybrook.edu
Office: Math Tower 4-120; Phone: (631) 632-4005
Office hours: Tuesdays and Thursdays 1:00-2:30pm in Math Tower 4-120.
TA. Nancy Hong
Email: nancy.hong@stonybrook.edu
Office hours: Wednesdays 12:00-1:00pm in MLC.

Lectures. Tuesdays & Thursdays 11:30–12:50pm in Mathematics S-235.

Blackboard. Grades and some course administration will take place on Blackboard. You will also use Blackboard to submit the projects and homework. Please log in using your NetID at http://blackboard.stonybrook.edu.

Courses Description. Exploration of the use of the computer as a tool to gain insight into complex mathematical problems through a project-oriented approach. Students learn both the relevant mathematical concepts and ways that the computer can be used (and sometimes misused) to understand them. Interesting applications of mathematics to computer science are also discussed. Some of the specific topics that we will try to study this semester include linear algebra, graph theory and Markov chains, number theory and cryptography, dynamical systems, fractals, differential equations and computer graphics.

Prerequisites. C or higher in MAT 203 or 205 or 307 or AMS 261.

TECH Objective. MAT 331 fulfills the "Understand Technology (TECH)" objective:

1. Demonstrate an ability to apply technical tools and knowledge to practical systems and problem solving.
2. Design, understand, build, or analyze selected aspects of the human-made world. The human-made world is defined for this purpose as artifacts of our surroundings that are conceived, designed, and/or constructed using technological tools and methods.

WRTD Objective. Students may use two of their MAT 331 projects to satisfy part of the Upper Division Writing Requirement for the major, or the "Write Effectively within One's Discipline (WRTD)" objective for the Stony Brook Curriculum (SBC):

1. Collect the most pertinent evidence, draw appropriate disciplinary inferences, organize effectively for one's intended audience, and write in a confident voice using correct grammar and punctuation.

Students who want to use two of the MAT 331 projects for this purpose should sign up for MAT 459: *Write Effectively in Mathematics* as a zero-credit course, with me as instructor.

Software. Most lectures will be held in the Math computer lab (Math Tower S-235). No previous experience with computers is needed.

We will use *Mathematica*, which is a computational software program developed by Wolfram Research and used in many scientific, engineering, mathematical and computing fields, based on symbolic mathematics. *Mathematica* has a comprehensive documentation, also available online at http://reference.wolfram.com/language/.

Mathematica 10 is available for most operating systems (Windows, Macintosh, Linux, etc.). Stony Brook students can download the Windows/Mac/Linux version of *Mathematica* from

Softweb: http://softweb.cc.stonybrook.edu/. You need your Stony Brook netID and netID password to log in to Softweb. To obtain an Activation Key for *Mathematica* you must visit the Wolfram User Portal https://user.wolfram.com/portal/login.html. If it's your first time visiting the Wolfram User Portal, you must create a Wolfram ID and follow the steps in there to request an Activation Key.

In addition, you can use any of the campus SINC sites, or you can access the Virtual SINC site at http://it.stonybrook.edu/services/virtual-sinc-site.

Reading resources. We will try to follow several sources, depending on the topic which we are covering. A set of notes written by Scott Sutherland and Santiago Simanca is available online at http://www.math.stonybrook.edu/~scott/Book331/331book.pdf. For the first part of the course we will use a set of lecture notes written by Raluca Tanase and Remus Radu about *The Mathematics of Web Search*, available at http://www.math.cornell.edu/~mec/Winter2009/RalucaRemus/. Other useful materials and lecture notes will be posted on the course website on Blackboard as we advance in the semester.

Grading policy. There will be no exams. Grades will be computed using the following scheme:

- Lab 15%
- Homework 20%
- Projects 65%

Students are expected to attend class regularly and to keep up with the material presented in the lecture and the assigned reading. There will be roughly five homework assignments (containing short exercises involving mathematical proofs and *Mathematica* code) as well as three or four projects. You may work together on your homework assignments and projects, and you are encouraged to do so. **However, all solutions must be written up independently**. A project is more like a term paper and you will be expected to devote a significant amount of time to doing it, as well as taking care with the presentation. The project should contain a detailed description of the problem or topic, what means were used to solve it, the mathematical solution and the computer program (interactive model in Mathematica). The last project of the class may include also a short oral presentation at the end of the semester.

Extra Help. You are welcome to attend my office hours and the TA's office hours and ask questions about the lectures and about the homework. In addition, math tutors are available at the Math Learning Center (MLC): http://www.math.stonybrook.edu/MLC.

Information for students with disabilities. If you have a physical, psychological, medical or learning disability that may impact your course work, please contact Disability Support Services, ECC (Educational Communications Center) Building, Room 128, (631) 632-6748, or at the following website http://studentaffairs.stonybrook.edu/dss/index.shtml. They will determine with you what accommodations, if any, are necessary and appropriate. All information and documentation is confidential.

Academic integrity. Each student must pursue his or her academic goals honestly and be personally accountable for all submitted work. Representing another person's work as your own is always wrong. Faculty is required to report any suspected instances of academic dishonesty to the Academic Judiciary. Faculty in the Health Sciences Center (School of Health Technology & Management, Nursing, Social Welfare, Dental Medicine) and School of Medicine are required to follow their school-specific procedures. For more comprehensive information on academic integrity, including categories of academic dishonesty please refer to the academic judiciary website at http://www.stonybrook.edu/uaa/academicjudiciary.

Critical Incident Management. Stony Brook University expects students to respect the rights, privileges, and property of other people. Faculty are required to report to the Office of University Community Standards any disruptive behavior that interrupts their ability to teach, compromises the safety of the learning environment, or inhibits students' ability to learn.

Prime numbers

A natural number $p \neq 1$ is prime if and only if it has no factors (divisors) other than 1 and itself.

Fundamental Theorem of Arithmetics.

Any positive integer n can be expressed as the product of powers of primes in a way that is unique up to a possible reordering of factors.

Thm (Euclid 300 BC) There are infinitely many prime numbers.

proof: Assume that there are exactly N primes, $p_1 = 2, p_2 = 3, \ldots p_N$

Then $m = (p_1 \cdot p_2 \cdots p_N) + 1$ is an integer bigger than $p_1, p_2, \ldots p_N$ which is not divisible by any of the primes $p_1, p_2, \ldots p_N$, contradiction.

Thm (Prime Number Theorem) Let $\pi(x)$ be the number of primes less than or equal to x. Then $\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$

Fermat's little Theorem

Let p be a prime number.

a) if a is relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.

b) $a^p \equiv a \pmod{p}$ for any integer a

proof a) Let $a \in \{1, 2, \ldots p-1\}$. Consider the numbers

$$a \cdot 1 \bmod p \quad a \cdot 2 \bmod p \quad \ldots \quad a \cdot (p-1) \bmod p$$

These are all distinct, and in the range $1, 2, \ldots p-1$. Otherwise, suppose by contradiction, that $a \cdot i \bmod p = a \cdot j \bmod p$ for some $1 \leq i < j \leq p-1$

Then $a(i-j) \equiv 0 \pmod{p} \Rightarrow a(i-j)$ is divisible by p. However this is impossible because p is prime, and $p \nmid a$ and $p \nmid i-j$.

In conclusion, multiplying by a has rearranged the numbers $1, 2, \ldots p-1$.

$$(a\cdot 1)\cdot(a\cdot 2)\cdots(a\cdot(p-1)) \equiv 1\cdot 2\cdots p-1 \pmod p.$$

$$a^{p-1}\cdot(1\cdot 2\cdots(p-1)) \equiv (1\cdot 2\cdots(p-1)) \pmod p.$$

$\Rightarrow$ $a^{p-1}\equiv 1 \pmod p$ because $1\cdot 2\cdots(p-1)$ is relatively prime to p. hence invertible mod p.

Theorem (Euler) Let p and q be distinct primes.

a) if a is relatively prime to p and to q, then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

b) if a is any integer, and k is any positive integer, then

$$a^{k(p-1)(q-1)+1} \equiv a \pmod{pq}.$$

proof: a)

a is relatively prime to p and p is prime, so by Fermat's theorem we have

$$a^{p-1} \equiv 1 \pmod p.$$

a is relatively prime to q (which is prime) so by Fermat's Thm we know that

$$a^{q-1} \equiv 1 \pmod q.$$

Then we have:

$$\left(a^{p-1}\right)^{q-1} \equiv 1 \pmod p \Rightarrow \left(a^{p-1}\right)^{q-1} - 1 \equiv 0 \pmod p.$$

$$\left(a^{q-1}\right)^{p-1} \equiv 1 \pmod q \Rightarrow \left(a^{q-1}\right)^{p-1} - 1 \equiv 0 \pmod q$$

$\Rightarrow$

$p \mid \left(a^{p-1}\right)^{q-1} - 1$

$q \mid \left(a^{q-1}\right)^{p-1} - 1$

Since p and q are distinct primes

$\Rightarrow$ $pq \mid a^{(p-1)(q-1)} - 1$

$\Leftrightarrow$ $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

Example: Compute $3^{12} \pmod{26}$

$$3^{(13-1)(2-1)} \equiv 1 \pmod{26}.$$

Thm. Fermat Let p be a prime number.

1. If a is relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.
2. If a is any integer, then $a^p \equiv a \pmod{p}$

Thm Euler Let p and q be distinct prime numbers

1. If a is relatively prime to p, then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$
2. If a is any integer, and k is any positive integer, then
$$a^{k(p-1)(q-1)+1} \equiv a \pmod{pq}$$

Observation important for Cryptography

whenever two positive integers d and e satisfy $d \cdot e = 1 + k(p-1)(q-1)$
or equivalently $d \cdot e \equiv 1 \mod ((p-1)(q-1))$

then the functions

$E(x) = x^e$ MOD pq $\quad 1 \le x \le pq-1$ and

$D(y) = y^d$ MOD pq $\quad 1 \le y \le pq-1$ are inverses

$$E(D(y)) = E(y^d) = (y^d)^e = y^{de} = y^{1+k(p-1)(q-1)} = y \pmod{pq}$$
$$D(E(x)) = D(x^e) = (x^e)^d = x^{de} = x^{1+k(p-1)(q-1)} = x \pmod{pq}.$$

$$x \xrightarrow{E} y = x^e \text{ MOD } pq \xrightarrow{D}$$

RSA public key cryptosystem

100-200 decimal digits

Alice – selects two distinct primes p and q.
– computes $m = pq$, $n = (p-1)(q-1)$.
– selects a number e which is relatively prime to n
– and uses the Extended Euclidean Algorithm to find the multiplicative inverse of e mod n, that is an integer d such that $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$

Alice broadcasts e and m.
m is called the modulus
e is the public key or encryption key

Alice keeps d and p and q a secret
d is the private key or decryption key

Bob – has a message to send to Alice

message = number x in range $0, m-1$.

– uses Alice's pubic key e and modulus m to encrypt the message:

$$y = x^e \text{ MOD } m$$

– sends y to Alice.

Alice – receives y from Bob

– uses her private key d to decode the message:

$$x = y^d \text{ MOD } m$$

$$y^d \equiv (x^e)^d \equiv x^{ed} \pmod m \equiv x \pmod m$$ because

$ed \equiv 1 \bmod ((p-1)(q-1)) \Rightarrow ed = 1 + k(p-1)(q-1)$

By Euler's theorem $x^{1+k(p-1)(q-1)} \equiv x \pmod m$

Bob – performs the same setup as Alice

choose two distinct primes p and q, etc ...

Cryptanalysis – essentially equivalent to factoring m

– the factors are large ~ 200 digits.

– the security of the RSA resides in the hardness/time consuming problem of factoring

Example :

+ select primes $p = 11$ and $q = 3$

- compute $m = pq = 33$ and $n = (p-1)(q-1) = (11-1)(3-1) = 20$

- choose e relatively prime with $n = 20$

$e = 3$

- find d such that $e \cdot d \equiv 1 \pmod{20}$

$d = 7$

Euclidean Alg: find s, t such that $3s + 20t = 1$.

$20 = 6 \cdot 3 + 2 \Rightarrow 0 = -2 - 3 \cdot 6 + 20$ $\mapsto$ $1 = 7 \cdot 3 - 20$

$3 = 2 + 1 \Rightarrow 1 = -2 + 3$ $\Rightarrow$ $3^{-1} \equiv 7 \pmod{20}$

$GCD(20, 3) = GCD(3, 2) = GCD(2, 1) = 1$

- public key $(e, m) = (3, 33)$

- private key $(d, m) = (7, 33)$

Bob wants to encrypt the message $x = 14$, using Alice's public key

$y = x^e \pmod{m}$

$y = 14^3 \pmod{33} = 2744 \pmod{33} = 83 \cdot 33 + 5 \pmod{33}$

$2744 = 83 \cdot 33 + 5$

Hence the ciphertext is $y = \boxed{5}$

Alice - receives the ciphertext $y = 5$ from Bob.

- uses her private key to decrypt it.

$x = y^d \pmod{m}$

$x = 5^7 \pmod{33} = \boxed{14} \pmod{33}$

$5^7 = (5^3)^2 \cdot 5 = 125 \cdot 125 \cdot 5 = 15625 \cdot 5 = 78125$

$(-7)^2 \cdot 5 = 7 \cdot 2 = 14 \pmod{33}$

$5^7 = 5^2 \cdot 5^2 \cdot 5^2 \cdot 5 = 25 \cdot 25 \cdot 25 \cdot 5$

$25 \equiv -8 \pmod{33}$

$5^7 \pmod{33} \equiv (-8)(-8)(-8) \cdot 5 \equiv 64 \cdot (-25) \equiv 13 \cdot (-2) \equiv -26 \equiv 7$

$-64 \cdot 40 = 2 \cdot 7 = 14 \pmod{33}$

- receives the ciphertext $y = 17$

$D(17) = 17^7 \pmod{33} \equiv (-16)^7 \equiv -2^{28} \equiv -2^{20} \cdot 2^8 \equiv -2^8 \equiv -2^5 \cdot 2^3 \equiv (-32) \cdot 8 \equiv 8 \pmod{33}$