

Math 3330 Syllabus
Number Theory and Cryptography
Fall 2015 Sul Ross State University

Sec. 001:	Mon, Wed, Fri: 10:00-10:50a in ACR 206
Instructor:	Dr. Kris Jorgenson
Office:	ACR 109D
Phone:	Office: (432) 837-8398; cell: (210) 422-3672
E-mail:	kjorgenson@sulross.edu
Office Hours:	M, W, F: 11a-12p; M, W: 3:30-5p; Tue: 2-5p; Thu: 4-5p; Fri: 3-5p
	also available by appointment

Course Description: This is an introductory course in basic number theory via with applications in modern cryptography. Topics include divisibility and the Euclidean algorithm, congruences, prime numbers, finite fields, bar codes, and public-key cryptography, among other topics. The prerequisite course is Linear Algebra (Math 2318) or permission of the instructor.

Student Learning Objectives Successful students will demonstrate correct understanding and knowledge of the topics including but not limited to those of the preceding paragraph. Students will demonstrate knowledge of the computational tools of number theory as well as proficiency in using complete sentences to write mathematical proofs.

This course is supportive of the

Program Learning Outcomes for the Bachelor of Science degree in Mathematics:

The graduating student will demonstrate that he/she is able to:

- Apply knowledge of basic mathematics principles;
- Identify and provide valid proofs or solutions for theorems and problems;
- Recognize and dispute invalid mathematical statements using counter-examples.

Required Materials: Textbook: Number Theory Through Inquiry, by David C. Marshall, Edward Odell, Michael Starbird, 2007 Mathematical Association of America ISBN-10: 978-0-88385-751-9.

Class Materials: Students are expected to be prepared in every class with pencils and paper to take notes and get involved in in-class assignments. Students should have a notebook for the purpose of containing the completed solutions of the assignments, and proofs given in class by a student or instructor. A few homework solutions will be due each week.

Technology: Students may find it convenient to have a scientific calculator (one with buttons labeled y^x , a^b , $\ln x$, or something similar to these denotations) handy during the semester. Use of an Excel spreadsheet application may also be helpful, but not required. You must also have access to Blackboard and have an e-mail address that you check

regularly be the e-address you have registered in Blackboard.

Grading and Assignments: The assignments discussed below will help students achieve all of the Learning Objectives mentioned previously through active learning and assessment. Your total grade will break down as follows:

Grading: Exercises will be assigned most classes to be handed in the following week. The **Homework Assessment (HWA) grade is worth 15%**. Time will be made for in-class presentations in order to give help on homework assignments. The **presentation grade will be worth 10%**. There will be **3 in-class test grades worth a total of 55%**. All students will present a **final project problem (worth 10%)** at the end of the semester during the final exam time and perhaps the last class of the semester. This will be a problem (or sequence of problems) that a student chooses with instructor approval concerning a number theory topic of interest. The **Project Attendance Grade (worth 5%)** will be calculated based on the percentage of final project problem presentations (other than their own) for which a student is present. **Class attendance (worth 5%)** will be based on the percentage of classes attended.

Test 1	Wed, Fri Sep. 23, 25
Test 2	Wed, Fri Oct. 21, 23
Test 3	Mon, Nov 23, 30

Late Work, Rescheduled Quizzes/Tests No late homework will be accepted, but I will accept homework (which might arise if we have a take-home quiz) as long as it is handed in by 5 pm on the due date. To take an in-class quiz or test at a time other than the scheduled time, you must notify me of this absence ON OR BEFORE THE DAY MISSED, and satisfy one of two requirements: either (1) supply a written medical excuse signed by a medical professional for the day of the absence, or (2) your excuse is for a university activity, in which case you must notify me of this authorized absence in writing with your name, the name of your organization and the date(s) of your absence, and your name must appear on a published explained absence list that I am provided (or this is verified by a faculty sponsor). Also, you and I must set up a time for you to make up the quiz or test within a reasonable time period (not more than 1-3 days) before or after the time of the missed grade. Usually I will let you make up a grade according to the above conditions if it is due to another one-time occurrence, such as the care of someone else in your family or a friend, or for a work-related excuse as long as you can document your absence and you let me know BY THE DAY OF THE ABSENCE AT THE LATEST. A CSG may also be made up with me in my office if you follow the above policy.

Attendance I will be taking attendance as university policy precludes you from missing more than 5 classes for anything other than authorized university activities since you cannot miss 3 weeks of classes (six classes). To excuse an absence for a university activity, in addition to letting me know of the absence by the day of the absence (as explained previously) you must also spend at least 60 minutes outside of class on this course with me

or with a tutor, but they will need to sign a note that documents this made-up time. Also I will allow you to excuse a test day for a documented medical absence as long as you also make up the test with me. If you have 6 or more unexcused absences, I reserve the right to drop you from this class with a grade of 'F', which is university policy.

Good Advice Concentrate on learning the material of the course rather than worrying about your grade. Your time is best spent concentrating on the material to be learned in the impending assignments, asking questions, and devoting yourself to activities that will help you learn the material and do better in the course. I will worry about the details of your grade since you doing so does not help you earn a higher grade. But learning the material and doing well on the tests *will* help your grade. **Remember that math is not a spectator sport**, so the more problems you work yourself and the more practice you get, the more confident you will be, and the better you will do in this course. Working on the problems helps you to figure out what your specific questions are.

More Good Advice Keep absences to a minimum. You never know when you might miss something you will find important either from the lecture or class discussion such as questions other students ask. Remember: YOU ARE RESPONSIBLE FOR EVERYTHING THAT IS DISCUSSED DURING CLASS WHETHER YOU ARE PRESENT OR NOT.

Also do not allow yourself to develop bad habits such as missing classes. It's human nature to be controlled by our habits, so once you develop a daily habit for the semester, it can be hard to break this habit. So be sure that you allow the necessary time for this course, ESPECIALLY if you consider mathematics not to be your best subject. If you have trouble in math, then you should attend EVERY class of a college mathematics course. Not showing up to class or not doing the required work will not cause this class to "go away". If you do have to miss, let me know before class, and plan to come and see me and make an appointment to discuss what was missed and pick up assignments you did not get back. However meeting in my office is not a substitute for attending class.

Ask questions no matter how easy or trivial they may seem. There is no such thing as a bad or silly question. Questions result when you are interested and have been thinking about areas, such as mathematics, in which you have some limitations in your educational background. Being in a college mathematics course means you will have questions both obvious and more subtle. Asking questions is a very important part of learning.

Study and work problems regularly—every day. Work on assignments discussed in class as soon as you can after class while the methods discussed are still fresh in mind. You can't expect to succeed in a math course by waiting till the last minute to only study and cram prior to a test. If you promise yourself you will study for ½-hour, get into the work, forget the clock, then the next thing you know, you've studied and worked for one to two hours.

Classroom Conduct It is important to conduct yourself in a college classroom so that everyone can benefit from good communication between instructor and students. My goal is to create an environment in which everyone can do their best work, learn, and make the best grades possible.

I think you will find that I am a very friendly, sympathetic, and generous instructor as long as you are sincerely working to succeed in this course and certain guidelines for

classroom behavior are followed during class to allow a sanctity of study for your fellow students. Classroom habits such as holding conversations during lecture, or being engaged in activities not related to this course such as working on a different course or reading a newspaper will work against the goal of this course and cause you to be counted absent and you will lose Daily Grade credit. Also engaging with electronic communication devices of any kind during class or coming into class more than 5 minutes late or leaving early before class is dismissed circumvent the goals of this course and cause you to lose credit. My sympathy and generosity will quickly evaporate if I find that you are working against the goals of the course or that you are simply trying to get a good grade without learning or without honestly doing the required work. I want you to have every opportunity to succeed in this course.

Please be aware of the rules for Academic Honesty that you will find in the Sul Ross Student Handbook and building codes prohibiting food, beverages, tobacco (smokeless or otherwise) in the classroom. Use commonsense to think of anything else that will allow you to learn and do the best work that you can in this class, and for me to better help you do your best work. Remember that being registered for this course does not allow you to behave in any manner you wish during class. You must keep other people in mind. It is within university policy for me to send a student out of this class on a temporary or permanent basis if disruptions or interruptions like the types listed above persist.

Equal Access The university is committed to equal access in compliance with the Americans with Disabilities Act of 1990 (ADA) and section 504 of the Rehabilitation Act of 1973. If you have questions regarding accessibility, please consult with the ADA coordinator, Mary Schwartze, Counselor in the Counseling and Accessibility Services Office in Ferguson Hall Rm. 112, and feel free to discuss this with me in private. The mailing address is Accessibility Services, Box C-122, Sul Ross State University, Alpine, Texas 79832. The telephone number is (432) 837-8203; FAX: (432) 837-8363.

E-mail: mschwartz@sulross.edu.

Important Dates

Mon, August 24	First day of classes; late registration, schedule changes begin
Thur, August 27	Last day for late registration and schedule changes
Mon, September 7	Labor Day holiday, no classes
Wed, September 9	12th class day: last day to drop without creating record
Fri, November 13	Last day to drop a course with grade of "W" by 4 pm in Registrar's Office
Wed-Fri Nov. 25-27	Thanksgiving holiday, no classes
Wed, Dec 2	Last Class Day before finals
Thu, Fri Dec 3, 4	Dead Days, no classes
M-Th, Dec. 7-10	Final Exams

Tentative Math 3330 Course Schedule

X = no class

Fall 2015	Mon	Wed	Fri
Aug. 24, 26, 28	First Class Day Logic and Induction	Induction Presentations	Presentations
Aug. 31 Sep. 2, 4	Divisibility, Euclidean Algorithm	Divisibility, Euclidean Algorithm Presentations	Presentations
Sep. 9, 11	X - Labor Day	Diophantine Equations	Presentations
Sep. 14, 16, 18	Presentations	Prime Numbers	Presentations
Sep. 21, 23, 25	Presentations	Presentations Test 1	Test 1
Sep. 28, 30, Oct. 2	Relations and Partitions	Relations and Partitions Arithmetic in Z_n	Arithmetic in Z_n
Oct. 5, 7, 9	Presentations	Equations in Z_n	Presentations
Oct. 12, 14, 16	Bar Codes	Bar Codes	Presentations
Oct. 19, 21, 23	Presentations	Presentations Test 2	Test 2
Oct. 26, 28, 30	Chinese Remainder Theorem	Chinese Remainder Theorem Euler Phi Function	Euler Phi Function
Nov. 2, 4, 6	Theorems of Euler and Fermat	Theorems of Euler and Fermat Presentations	Presentations
Nov. 9, 11, 13	Public-Key Cryptography	Presentations	Radical Irrationals
Nov. 16, 18, 20	Presentations	Rational Points on Elliptic Curves	Presentations Deadline choosing Final Project Problem
Mon, Nov. 23	Test 3, Part 1	X - Thanksgiving Holidays -----> Nov. 25-27	
Nov. 30, Dec. 2	Test 3, Part 2	Final Project Work	X - Dead Day
Mon, Dec. 7	Final Projects: 10:15-12:15		