$n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$

Stirling's Formula

MA-410
Theory of Numbers
Spring 2019
SAS Hall 2106, TueThur 8:30am-9:45am

Syllabus People Homeworks Web resources

Current Announcements

- **NEW** The course web sites for Spring 2018, Spring 2017, Spring 2016, Spring 2015, Spring 2012, Spring 2011, Spring 2010, Spring 2009, Spring 2008, Spring 2007 and Spring 2005 may contain old homeworks, mid-semester exams, and anonymous grade lists.
- My office hours are listed on my schedule.

Peoples' home pages: Erich Kaltofen.

Homeworks

- Homework 1, due Tuesday, Feb. 5 at 16:59pm, in my mailbox in SAS 3151.
- Homework 2, due Thursday, Feb. 28, at 16:59pm, in my mailbox in SAS 3151.
- Homework 3, due Thursday, Apr. 11, 16:59pm, in my mailbox in SAS 3151.
- Homework 4, due Thursday, Apr. 25, 16:59pm, in my mailbox in SAS 3151.

Web resources for the course

- Maple basic lesson from MA 141
- Victor Shoup's downloadable book A Computational Introduction to Number Theory and Algebra

Old Announcements

Outline	People	Reading	Grading	Academics	Homepage

MA 410 2019 Syllabus

Course Outline*

Lecture	Topic(s)	Notes	Book(s)
1. Jan 8	Introduction; Fibonacci		ENT/CINTA
2. Jan 10	Mathematical induction; the binomial theorem		ENT §1
3. Jan 15	Inductive definition of addition, multiplication, exponentiation; divisibility and division with remainder	Maple Worksheet	Class notes; ENT §2
4. Jan 17	Euclid's algorithm		ENT §2
Mon, Jan 21	**M. L. King Holiday**		
5. Jan 22	Extended Euclidean algorithm; diophantine linear equations		ENT §2; class notes
6. Jan 24	Continued fractions; Euclid's lemma		ENT §2
7. Jan 29	Fundamental theorem of arithmetic		ENT §3
8. Jan 31	Theorems on primes: Euclid, Chebyshev, Dirichlet, Hadamard/de la Vallee Poussin, Green-Tao Conjectures on primes: Goldbach, twin, Mersenne, Fermat	sequences of equidistant primes; Barkley Rosser, Lowell Schoenfeld. Approximate formulas of some functions of prime numbers. *Illinois J. Math.* vol. 6, pp. 64--94 (1962). list of Mersenne primes, factors of Fermat numbers	ENT §3
9. Feb 5	Catch-up; review for first exam		
10. Feb 7	Thursday, **First Exam**	Counts 20%	
11. Feb 12	Equivalence relations, congruence relations, congruences		Class notes; ENT §4
12. Feb 14 ❤	Return of first exam; congruences continued		
13. Feb 19	Congruences continued		
14. Feb 21	The Chinese remainder theorem	Maple Worksheet	ENT §4.4
15. Feb 26	The little Fermat theorem; pseudoprimes; Fermat primality test;	Carmichael numbers	ENT §5.3
16. Feb 28	Carmichael numbers; Miller-Rabin test	Maple Worksheet	ENT §5.2
Mon, Mar 4, 11:59pm **Last day to drop the course**			
17. Mar 5	Euler's phi function; sums of divisors		ENT §7
18. Mar 7	Public key cryptography; the RSA		ENT §7.5
Mar 11-15, 2019	**Spring Break, no class**		
19. Mar 19	Catch-up; review for exam		

20. Mar 21	Thursday, **Second exam**	Counts 20%	
21. Mar 26	Index calculus: order of an integer modulo *n* and existence of primitive roots modulo *p*		ENT §8
22. Mar 28	Return of second exam; primitive roots continued		ENT §8
23. Apr 2	Diffie-Hellman-Merkle key exchange; el-Gamal public key crypto system; digital signatures	Class notes	
24. Apr 4	Quadratic and cubic residuosity	Maple Worksheet	ENT §9.1
25. Apr 9	Legendre symbol, the quadratic reciprocity law		ENT §9.2, §9.3
26. Apr 11	Jacobi symbol		ENT §9.3, Problems 16-19
27. Apr 16	Computing squareroots modulo p	Maple worksheet	Tonelli-Shanks Algorithm
28. Apr 18	Pythagorean triples, Fermat's last theorem for n=4		ENT §12.1, §12.2
Friday, Apr 19	**Spring Holiday, no class**		
29. Apr 23	Final exam review		
30. Apr 25	Snow day slack lecture		
Tuesday, April 30, 9am-11am, Final exam (counts 30%)			
Thursday, May 9, 11:59pm, Grades due			

* This is a *projected* list and subject to amendment.

Instruction Personnel

For instructor, office hours, telephone numbers, email and physical address see the homepages of Erich Kaltofen.

Textbook and Online Notes

We will use the books:

"Elementary Theory of Numbers" (abbr. ENT)
David M. Burton
McGraw Hill

I will cover some topics that are not in the book, and will use

A Computational Introduction to Number Theory and Algebra (abbr. CINTA)
Victor Shoup
Cambridge University Press

Shoup's book can be downloaded in pdf format for free. I had considered only using Shoup's book and am interested what you think about that idea. In any case, the syllabus above refers to chapters in these books. For topics in neither book, handouts will be provided.

On-line information: All information on courses that I teach (except individual grades) is now accessible via html browsers, which includes this syllabus. My web page listing all my courses' is at

http://www.math.ncsu.edu/~kaltofen/courses/courses/courses.html

You can also find information on courses that I have taught in the past, and examinations that I have given.

Grading and General Information

Grading will be done **with plus/minus refinement**.

There will be four homework assignments of approximately equal weight, two mid-semester examinations during the semester, and final examination. Depending on time constraints, I may only grade a selection of homework problems.

I will check who attends class. You will forfeit 5% of your grade if you **miss 3 or more classes** without a valid justification. I you miss a class because you are sick, etc., please let me know. I may require you to document your reason.

Grade split up	
Accumulated homework grade	25%
Final examination	30%
First mid-semester exam	20%
Second mid-semester exam	20%
Class attendance	5%
Course grade	100%

Grade distribution of Spring 2018.

If you need assistance in any way, please let me know (see also the University's policy).

Academic Standards

*Examinations:*The three examinations will be **closed book and closed class notes**. However, you will be able to bring **note sheets** of paper with pertinent information to the examinations (1 for first exam and 2 for second exam and 3 for the final exam).

Collaboration on homeworks: I expect every student to be his/her own writer. Therefore the only thing you can discuss with anyone is how you might go about solving a particular problem. You may use freely information that you retrieve from public (electronic) libraries or texts, but you must properly reference your source.

Late submissions: All programs must be submitted on time. The following penalties are given for (unexcused) late submissions:

- up to 1 day late: 20% reduction
- up to 2 days late: 50% reduction

- after 2 days: no credit (= 100% reduction)

Alleged cheating incidents: I will not decide any penalty myself, but refer all such cases to the proper judiciary_procedures.
