

# Theory of Numbers

Spring Semester 2018

---

**Course** MATH 416 Section 1, MWF 9:00–9:50am, RB 107

**Instructor** Dr. Hanspeter Fischer

**Contact** Office: RB 426

Phone: 285-8680

E-mail: [hfischer@bsu.edu](mailto:hfischer@bsu.edu) (please use MATH 416 as subject line)

<http://www.cs.bsu.edu/~fischer/math416>

**Office Hours** Mon 11:00–11:50am, Tue 9:00–9:50am, Wed 10:00–10:50am, Thu 9:00–9:50am, Fri 11:00–11:50am, and by appointment.

**Prerequisites** MATH 215

**Text** *Elementary Number Theory and Its Applications* (6th Edition), by K.H. Rosen

**Contents** This course is an introduction to elementary number theory, that is, number theory which does not require tools from analysis. The textbook combines the classical results of this area beautifully with the most modern applications, such as cryptography—the common themes being how to determine if a given large number is prime and how to factor it if it is not.

We will begin with a review of prime numbers and greatest common divisors (Chapter 3). We then study the important arithmetic by remainder, upon which all of this material builds (Chapter 4). (Some of the material in Chapter 4 will be review, but some of it will be covered in more detail than you might have seen before.) In Chapters 6 and 9, we will learn some basic group theory as it relates to number theory. Among other things, we will learn how to conduct probabilistic primality tests based on this group theory. Functions  $f$  whose domain are the positive integers and whose values  $f(n)$  can be calculated from the prime-power factorization of  $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$  by the formula  $f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_m^{a_m})$ , deserve special attention in number theory—we will study them in Chapter 7. In Chapter 11, we will discuss the intriguing theory of “square roots” in modular arithmetic, again with an eye on secure communication. We then switch gears somewhat and look at how best to approximate irrational numbers with rational numbers (Chapter 12). Although this may seem a bit out of context, we will see how this knowledge, too, can be used to factor large numbers and to launch various clever attacks on modern encryption systems. Time permitting, we might select some topics from Chapter 13 on popular equations involving whole numbers.

**Homework** Homework assignments will be made as we work through the material. Some problems will be assigned for practice only while other designated problems will be collected and graded. As a rule, homework will be due the Friday of the following week; the exception being the week before an exam, during which other due dates might be announced. Late homework will not be accepted. The assignments (with due dates) will be available online at above web site.

When submitting exercises make sure to have your name and course number on it to earn credit. Please staple your solutions.

---

One of the goals of this course is to master the craft of proof-writing. Your homework assignments are therefore an important part of your engagement with the material. *Never submit the first draft of your homework.* Instead, neatly rewrite your ideas into logically complete proofs, which could be easily read and understood by a classmate.

---

**Technology** Some of the assignments will ask you to use the software package *Mathematica*. The relevant number theoretic *Mathematica* commands are listed in Appendix C.2 on pages 619–623 of the textbook. Some templates will be provided.

**Examinations** There will be three midterm examinations. The comprehensive final exam will be on Friday, May 4, 7:30–9:30am. All exams must be taken at their scheduled time (see attached time table); the only exception being a verifiable illness or family emergency, of which you must inform your instructor *before* the test.

The exams will have an in-class and a take-home component to them.

**Evaluation** All three midterm exams combined make up 50% of your grade and the final exam represents 25%. Homework accounts for the remaining 25%.

The approximate grading scale (in percent) is:

A: 90 – 100, B: 80 – 90, C: 70 – 80, D: 60 – 70, F: below 60.

**Timetable** A tentative schedule is attached. See above website for changes and updates.

**Deadlines** The last day to change a course is Sunday, January 14. The course withdrawal period is Monday, January 15, through Monday, March 19. During this period students can elect to receive a “W” for the course by completing and submitting the proper form to the Registrar’s Office. The instructor’s permission is not required. For details, see the section *Withdrawal* under *Degree Requirements and Time Limits* in the current Undergraduate Catalog.

- Remarks**
- (1) Students are expected to come prepared to all meetings, having read upcoming sections of the textbook. Be always up to date!
  - (2) It takes time to digest and master new concepts. Expect to be studying for a minimum of two hours outside of class for each hour in class. Missing class is a major setback.
  - (3) Everybody is strongly encouraged to engage with classmates in frequent general discussions of the material. However, on assignments, credit should be claimed only for one’s own work. Moreover, collaboration on take-home exams is not permitted.
  - (4) If you need course adaptations or accommodations because of a disability, please contact me as soon as possible. Ball States Disability Services office coordinates services for students with disabilities; documentation of a disability needs to be on file in that office before any accommodations can be provided. Disability Services can be contacted at 765-285-5293 or [dsd@bsu.edu](mailto:dsd@bsu.edu).
  - (5) Ball State University aspires to be a university that attracts and retains a diverse faculty, staff and student body. We are committed to ensuring that all members of the campus community are welcome through our practice of valuing the various experiences and world views of those we serve. We promote a culture of respect and civil discourse as evident in our Beneficence Pledge. For Bias Incident Response service information, go to [bsu.edu/multiculturalcenter/bias](http://bsu.edu/multiculturalcenter/bias) or e-mail [mc2@bsu.edu](mailto:mc2@bsu.edu).
  - (6) Please turn cell phones off during class. Thank you.