

Instructor: Leo Goldmakher

Williams College
Department of Mathematics and Statistics

MATH 313 : NUMBER THEORY

Midterm Exam – to be taken Monday, November 5th—Thursday, November 8th

INSTRUCTIONS

The midterm exam will consist of three questions, to be discussed orally with the instructor. The duration of the exam will be no longer than 25 minutes. You will have access to a blackboard; *no other aids are permitted*.

The exam will begin with Question A, which will be asked of every student. The other two questions will be selected by coin flip from Lists B and C, one question from each. (See next page for questions.)

I would like you to understand each topic as deeply as possible. To this end, I reserve the right to follow up on anything you mention during your discussion. For example, if you refer to Fermat's Little Theorem, I may ask you to state it; I may then follow up by asking you to prove it. In short, as you study the material, I want you to continually ask yourself the question: *can I define / prove this without looking it up?*

Often, it is during an exam that you realize for the first time that you don't properly understand something. This is not only natural, it is totally OK; I will give you as many hints as you need to get back on track. Although part of the exam is to see how far you can go on your own, the more valuable aspect of an oral exam is that it's a chance for some individualized learning.

I strongly encourage you to practice for the exam with one another; find a study buddy or two and take turns acting the role of the examiner. Don't go easy on your partner! Any time anything is unclear, follow up on it; any time they use a theorem or a definition, press for more details.

Best of luck!

Leo

Problems on other page...

MATH 313 : NUMBER THEORY

Midterm Exam – to be taken Monday, November 5th—Thursday, November 8th

PROBLEMS

Question A (Big Theorem)

Prove that whenever $(m, n) = 1$, the map $\beta : \mathbb{Z}_{mn}^\times \rightarrow \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$ given by $\beta(x) := (x \pmod{m}, x \pmod{n})$ is a bijection. Deduce that φ is multiplicative.

List B (Theory)

- B.0** State and prove Euler's theorem concerning $a^{\varphi(n)} \pmod{n}$.
- B.1** State and prove the Fundamental Theorem of Arithmetic.
- B.2** State and prove the upper bound in Chebyshev's theorem.
- B.3** State and prove the lower bound in Chebyshev's theorem.

List C (Computation)

- C.0** I will give you a power congruence and ask you to solve it.
- C.1** I will give you a date and ask you to compute the day of the week it falls on.
- C.2** I will give you two integers a and b and ask you to find integers x and y such that $ax + by = \gcd(a, b)$.
- C.3** I will give you two integers a and n and ask you to find $\frac{1}{a} \pmod{n}$.