

Math 364 (02) Q3 - Course Outline, 2010 Spring and Summer Session.

LECTURES: MTWRF, 1:00 p.m. – 3:20 p.m., ESB 243.

INSTRUCTOR: Pawel Gladki.

OFFICE: 208 McLean Hall.

E-MAIL: gladki@math.usask.ca WEBSITE: <http://math.usask.ca/~gladki>

OFFICE HOURS: If you want to see your instructor in his office, please make an appointment: see him before or after class, call his office or send him an e-mail.

TEXTBOOK: Charles Vanden Eynden, *Elementary number theory*, 2nd Edition, Waveland Press. Other editions of this book are suitable, but page and section references in this information sheet and homework problems are taken from the 2nd edition.

EVALUATION: 12 assignments, counting for a total of 10% of your mark, 2 midterm tests, each counting for 20% of your mark for a total of 40% and final examination counting for 50% of your mark.

EXAMINATIONS: Midterm exams will be held on **July 9th** and **July 16th**. Durations of each mid-term test will be 50 minutes. All examinations will be closed book: no calculators, notes or formula sheets will be permitted. **Please be advised that cheating on an examination is considered a serious offence and can be met with disciplinary actions, including suspension or repulsion.** All examinations will be “show all work” tests of up to 5 (midterms) or 10 (final) questions. There will be no make up exams. Students who miss either one of the midterm exams for legitimate reasons will have the value of that examination transferred to the final examination thereby increasing the value of the final examination accordingly.

HOMEWORK: Problems from each section of the text will be released at least 2 or 3 days prior to discussing the topics. There are two kinds of problems: **drill exercises** and **assignments**. Drill problems will not be handed in or graded, but it is strongly advised to solve all of them (or as many as your time permits) before you start working on assignments - in order to get familiar with new definitions, theorems and examples. Assignments are to be completed and handed in for grading - there are 12 short assignments consisting of 5-6 problems, approximately each for one lecture. They will be returned in the following lecture. It is suggested that you have a look to the textbook before each class and skim the material to be instructed (see course calendar).

MATH HELP CENTRE: There is a Math Help Centre in room 144 Murray. Its hours of operation will be posted on the web page: <http://www.usask.ca/ulc/math.php>.

COURSE CALENDAR:

Jul. 2: Mathematical Induction.

Jul. 5: Integers. Divisibility. Modular arithmetics.

Jul. 6: Prime numbers. Fundamental theorem of arithmetics.

Jul. 7: GCD and LCM. Euclidean algorithm. Linear diophantine equations and linear congruences. Chinese remainder theorem.

Jul. 8: Euler’s φ function and Euler’s theorem. Multiplicativity of Euler’s φ function.

Jul. 9: Midterm 1. Distribution of primes, prime tests and RSA coding.

Jul. 12: Basic algebraic structures: groups, rings, and fields. Homomorphisms and isomorphisms. Orders of groups, subgroups, and elements of groups.

Jul. 13: Arithmetic functions, Dirichlet’s convolution and Möbius formula.

Jul. 14: Structure of the group \mathbb{Z}_n . Primitive roots.

Jul. 15: Quadratic reciprocity law.

Jul. 16: Midterm 2. Two square theorem. Integers as sums of squares. Waring’s problem.

Jul. 19: Continuous fractions.

Jul. 20: Diophantine approximations.

Jul. 21: Diophantine equations of degree 2 and higher.

Jul. 22: Pell’s equation.