MATH 180

Course Description Number theory is one of the oldest topics in mathematics, and was always considered one of the purest. Yet, recent decades have seen applications emerging in many fields, most notably communications and cryptography. The course will introduce basic mathematical notions and methods, covering properties of divisors, prime numbers, integer functions and equations in integers, as well as some of the above mentioned applications.

Provisional syllabus We will apply standard mathematical tools, such as induction and infinite descent, to derive some of the classical results of number theory. As this is a first course in mathematics for most students, the concept of 'proof' will be emphasized through examples and exercises.

The course will cover basic properties of the integers, greatest common divisor, primes, Fermat's little theorem and similar results, integer functions (σ, Euler's ϕ, Mobiüs function), applications to cryptography (such as RSA and Rabin encryption scheme), and Diophantine equations. If time permits, we will also discuss quadratic residues, primality testing, continued fractions and Pell's equation.

Textbook: Elementary Number Theory and its Applications (4th edition), by Kenneth H. Rosen.

Date: July 4, 2005.