MATH 601 Midterm 1 Conceptual Review

Exam details.

Date: Thursday, March 05
Location: Snow 256
Topics: Everything covered in lecture and group explorations.
Length: 6-7 problems.
Aids: *Both sides* of a 3×5 notecard. No calculators!

Suggested problems appear in **blue**.

Basic properties of $\mathbb{N}$ and $\mathbb{Z}$.

(1) What is the well-ordering principle for the natural numbers?
(2) What does the notation $a|b$ mean? **HPS 1.6**
(3) What is the division algorithm?
(4) What is the Euclidean Algorithm (EA)? What does the EA have to do with greatest common divisors? **HPS 1.9**
(5) What does the phrase "$\mathbb{Z}$-linear combination of integers a and b" refer to? What does the notation $\text{span}_{\mathbb{Z}}(a, b)$ stand for? What does this have to do with greatest common divisors?
(6) What is the Extended Euclidean Algorithm (EEA) and Bezout's Identity (BI)? **HPS 1.10**
(7) Can you apply BI to prove things? **HPS 1.19, 1.29**
(8) What is a prime number? The *property of primes*?
(9) What is the Fundamental Theorem of Arithmetic (FTA)?

Basics of modular arithmetic.

(1) Can you translate the congruence $x \equiv y \bmod m$ into a statement about integers?
(2) How are integers added, subtracted, and multiplied in modular arithmetic? **HPS 1.15, 1.16, 1.17**
(3) What does it mean for an integer to be a unit modulo m? How can you tell whether an integer is a unit modulo m? What does the notion of a unit have to do with "division"?
(4) What does it mean for integers to be inverses of each other modulo m? In addition, if you know that a has an inverse modulo m, then how do you find $a^{-1} \bmod m$? More to the point, what does this have to do with EEA and Bezout's Identity? How do inverses make solving congruences easier?

Chinese Remainder Theorem (CRT).

(1) What is the statement of the CRT that we proved in class?
(2) What is the "splicing" method to solve the two simple systems of congruences modulo relatively prime moduli? What does this have to do with EEA and Bezout's Identity? **HPS 1.24b**
(3) Can you iteratively apply the CRT to solve simple systems of congruences with 3 or more equations? **HPS 1.24c**

Euler's Phi, Euler's Theorem, and Fermat's Little Theorem.

(1) What is Euler's totient function? In other words, if n is a positive integer, then what is the definition of $\varphi(n)$? Can you calculate $\varphi(n)$ using the definition for small-ish values of n?
(2) Is there a formula for $\varphi(n)$? If so, in terms of what data? Can you use it to simplify your computations in small cases? **Group Exploration 1**
(3) What is the precise statement of Euler's Theorem? What role does φ play in this theorem? How does it help you simplify the task of raising units to large powers mod n?
(4) What is Fermat's Little Theorem? How is it related to Euler's Theorem?

Basics of square roots.

(1) How many square roots of an integer can there be modulo a prime? Can you prove this fact, using the property of primes?
(2) Can you identify which integers have square roots modulo m from a table, like we did in class?

Primitive roots, Diffie-Hellman, ElGamal.

(1) What is a primitive root? Can you compute them? **HPS 1.36abc**
(2) What is the basic setup of the Diffie-Hellman key exchange? What is the purpose of this? Is it a cryptosystem? **HPS 2.6**
(3) What is the basic setup of ElGamal? How does it differ from Diffie-Hellman? **HPS 2.8a, replacing the k there with the one furnished by Diffie-Hellman, as in lecture.**