MATH 601 Midterm 2 Conceptual Review

Exam details.

Date: Thursday, April 16
Location: Snow 256
Topics: Everything covered in lecture and group explorations.
Length: 6-7 problems.
Aids: Both sides of a 3 in. $\times$ 5 in. notecard. No calculators!

Suggested problems appear in blue and Group Explorations in green.

Square roots and computations.

(1) How many square roots of an integer can there be modulo a non-prime? Can you apply the CRT to produce square roots modulo pq if you know square roots modulo p, and modulo q, where p and q are distinct primes? GE 2
(2) What can you say about square roots of an integer modulo a prime p with $p \equiv 3 \bmod 4$? GE 2
(3) Our remote coin-flipping strategy used the fact that knowing enough square roots of an integer modulo $n = pq$ can be used to recover the factors p and q. Can you prove this? GE 2

Primitive roots, Diffie-Hellman, ElGamal.

(1) What is the basic setup of the Diffie-Hellman key exchange? What is the purpose of this? Is it a cryptosystem? HPS: 2.6
(2) What is the basic setup of ElGamal? How does it differ from Diffie-Hellman? HPS: 2.8(a), replacing the k there with the one furnished by Diffie-Hellman, as we did in lecture.

RSA and Digital Signatures.

(1) What is the basic setup of RSA? What is the public/private key? How does one send/receive messages?
(2) Why is RSA considered secure? HPS: 3.7, 3.8
(3) How would Alice use her public RSA key to create a digital signature? What is the purpose of a digital signature? HPS: 4.1, 4.2

Factoring algorithms.

(1) What is Pollard's $p-1$ method for factoring an integer? If you are trying to factor n using the sequence a_k described in our notes derived from an integer $1 < a < n$, then when will your computations stop? HPS: 3.22
(2) What is the Quadratic Sieve factoring algorithm? HPS Examples 3.37, 3.38 in the text. HPS: 3.26.
(3) It may be impractical to do long calculations on Midterm 2 without the use of a calculator. Still, can you run through the $p-1$ method, or Quadratic Sieve, in some very small examples, to factor some small numbers? Apply these factoring algorithms for smallish numbers, whose factorizations you already know.

Elliptic curves and the group law: The basics.

(1) What is the definition of an elliptic curve (EC)?
(2) What does the graph of an EC look like?
(3) What is a singular point of an EC?
(4) Can you write the formula for the line connecting distinct points of an EC, or for the tangent line to an EC at a point? Even when the field is of the form $\mathbb{Z}/p\mathbb{Z}$ for some prime p?
(5) What is the group structure on an EC? Why does non-singularity matter? What is the identity? What is the inverse of a point?
(6) Can you explicitly compute the sum of points of an EC under the group law? HPS: 6.1, 6.2, 6.3, 6.6ab, 601 Digest Week 12