MATH 601 Final Exam Conceptual Review

Exam details.

Date: Tuesday, May 12
Location: Snow 256
Topics: Everything covered in lecture and group explorations. The material appearing below will be over-emphasized.
Length: 6-9 problems.
Aids: Both sides of a 3 in. $\times$ 5 in. notecard. No calculators!

Suggested problems appear in blue and Group Explorations in green.

The basics of elliptic curves and the group law.

(1) What is the definition of an elliptic curve? What is the discriminant of an equation that defines an elliptic curve? Why do we require it to be nonzero?
(2) What is the group structure determined by an elliptic curve? What role does the point at infinity play?
(3) Given explicit points P and Q on an elliptic curve, can you explicitly compute $P + Q$, even when $P = Q$?
GE 3, HSP Problems 6.1, 6.2, 6.3, 6.6ab
Note: For each of these problems from HSP, try to compute the sum of points by hand, and check your answer using the computer program you wrote for GE 3.

Orders of points on elliptic curves modulo a prime.

(1) Let u be a unit modulo p. What is the order of u? Which integers k satisfy $u^k \equiv 1 \bmod p$? Can you prove it?
(2) Let P be a point of an elliptic curve $E(p)$. What is the order of P? Which integers k satisfy $kP = \mathcal{O}$? Can you prove it? What is the relationship between the order of a point and $|E(p)|$?
(3) Can you compute the order of a point using a program? GE 3.
(4) What is the *Hasse bound*? GE 3.
(5) For some elliptic curves, we have a nice formula for $|E(p)|$. What are those curves? What are those formulas?

Elliptic curves: Applications to cryptography and attacks.

(1) What is a psuedo elliptic curve modulo some integer n?
(2) What is the basic idea behind Lenstra's factoring algorithm? Can you describe some variations of this process? For example, given a point P of a pseduo elliptic curve $E(n)$, what are the common ways to generate other points from P to use in Lenstra's factoring algorithm? No matter which variation you use, what does the failure of the ability to add certain points on a pseudo elliptic curve $E(n)$ tell you about n? How can you exploit this to obtain a factor n?
GE 3
(3) What is the setup for the EC version of Diffie-Hellman?
(4) How does the EC version of ElGamal work?
HSP Problem 6.14abc
(5) What is the Elliptic Curve Discrete Logarithm problem? What does this have to do with the security of the EC versions of Diffie-Hellman and ElGamal? In other words, what is preventing Eve from breaking the ElGamal cryptosystem?
(6) What is a Mersenne number? How can we use pseudo elliptic curves to test whether a Mersenne number is prime?
This is from the last lecture.