Math 458, Final Review Sheet

The final exam is cumulative. Most questions on the final exam will be similar to previous questions on homeworks and midterms. Midterm questions where many people made mistakes have a tendency to show up again on my final exams, so there is a benefit to understanding your past errors.

The topics since the last midterm have been:

• Elliptic curves over \( \mathbb{F}_p \), and the groups \( E(\mathbb{F}_p) \).
• The classification of finite abelian groups, how orders of elements behave, and applications to understanding the groups \( E(\mathbb{F}_p) \)
• Integer factorization by computing orders in \( \mathbb{Z}/N \), and also by Lenstra’s algorithm using elliptic curves (see HW#8)
• The very basics of quantum systems, and applications to quantum cryptography.

Here are a few more practice questions:

1. Let \( N = 17688431 \). A computer tells you that the order of 5 in \( (\mathbb{Z}/N)^* \) is 4419966. Explain how you could use this information to find a factor of \( N \). (You don’t have to do the computations, just explain how you would do them given enough time).

2. Let \( E \) be the elliptic curve \( y^2 = x^3 + Ax + B \) over \( \mathbb{F}_p \), which we assume to be nonsingular.
   (a) If \( P = (x, y) \) is a point on the curve, write down the formula for computing \( 2P \).
   (b) For what values of \( x \) and \( y \) does the above formula not make sense? These correspond to points \( P \) where \( 2P = \mathcal{O} \).
   (c) Explain the following: The elliptic curve \( E \) can have at most three points of order 2.
   (d) Can the group \( E(\mathbb{F}_p) \) ever be isomorphic to \( \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/11 \)? Explain.

3. (a) How many elements in the group \( (\mathbb{Z}/8, +) \) are generators? List them all.
   (b) How many elements in the group \( (\mathbb{Z}/5, +) \) are generators? List them.
   (c) If \( (a, b) \in \mathbb{Z}/8 \times \mathbb{Z}/5 \), what is the formula for the order of \( (a, b) \)?
   (d) How many elements of \( \mathbb{Z}/8 \times \mathbb{Z}/5 \) are generators (i.e., have order 40)? Explain how you know.
   (e) Using that \( \mathbb{F}^*_313 \) is isomorphic to \( \mathbb{Z}/312 \), determine how many elements of this group are generators. (Hint: First write \( \mathbb{Z}/312 \) as a product of \( \mathbb{Z}/n \)'s where the \( n \)'s are as small as possible).

4. For the prime \( p = 7321 \), the group \( \mathbb{F}^*_p \) has 1920 generators.
(a) If an element of $\mathbb{F}_p^*$ is chosen randomly, what is the probability that it is NOT a generator?

(b) Someone writes a computer program to find a generator, which chooses an element randomly, tests if it is a generator, and if not it chooses another random element and repeats. If the program does not find a generator after a certain number of repetitions, it “fails”.

For the field $\mathbb{F}_{7321}$, what is the smallest number of repetitions that would make the probability of failure smaller than 0.1?

5. When $N > 2$ there are always at least two solutions to $x^2 = 1$ in $\mathbb{Z}/N$: namely $x = 1$ and $x = -1$. When $N$ is prime, these are the only solutions. Find a third solution when $N = 70$. (Hint: Chinese Remainder Theorem).