MAT 302 Finals Checklist

- You will have 3 hours to solve about six problems.
- Make sure to go over all the materials – problem sets, your personal class notes, practice midterm and finals.
- You can bring an two-sided A4 sheet as the exam aid. No electronic equipment is permitted.
- Before the midterm:

  1. **[Groups]:** Groups $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$, and how to compute the Euler Totient Function $\phi(N)$, given the factorization of N?
  2. **[Algorithms]:**
     - Euclid and Extended Euclid, application to computing inverses in $\mathbb{Z}_N*$.
     - Exponentiation: how to compute $b^a \pmod N$ given b, a and N? The "square and multiply" algorithm for exponentiation.
     - Finding Roots: how to find b such that $b^a = c \pmod N$ given a, c and N? How to find roots for prime and composite N.
     - Discrete Log: how to find a such that $b^a = c \pmod N$ given b, c and N? The baby step giant step algorithm and its complexity.
     - Primality Testing: The Fermat test, Carmichael Numbers and the Miller-Rabin test. The notions of Fermat witnesses and liars, and the proof that there aren't too many Fermat liars mod N where N is composite and not Carmichael.
     - Finding generators for $\mathbb{Z}_p^*$.
  3. **[Number Theory]:** Fermat's Little theorem, Euler's theorem, Lagrange's theorem, Chinese Remainder theorem, $\mathbb{Z}_p^*$ is a cyclic group, the number of elements of order d in $\mathbb{Z}_p^*$.
  4. **[Cryptography]:**
     - Caesar cipher and the One-time pad.
     - Diffie-Hellman key exchange and El Gamal encryption.
     - RSA public-key encryption.

- After the midterm:

  1. **[How to Solve Equations modulo Composites]:** Remember, the Chinese Remainder Theorem is your friend! To solve an equation like $x^2 = 1 \pmod{55}$, first solve the equation modulo 5 and 11. In this case, you will get two solutions each.

     $$x = 1 \text{ or } 4 \pmod 5, x = 1 \text{ or } 10 \pmod{11}$$

     Any combination of these solutions (there are four) forms a solution to the equation modulo 55.

2. **[How to Factor Numbers]:** Pollard's $p-1$ factoring algorithm, Factoring by the difference of squares (see the textbook for each of these.)
3. **[Identification Schemes and Digital Signatures]**
4. **[Secret Sharing]:** How does Shamir's t-out-of-n secret sharing scheme work? Make sure you can describe the process for general t and n precisely. Other, more complex, examples of secret sharing from the problem set and the practice final.
5. **[Elliptic Curves]:** over the reals, and over finite fields. How to add points in each case (add two different points, add the same point to itself), and how to find inverses (just negate the y-coordinate).