

**Non-Proof Tasks:**

1. Precisely, FULLY state the following (including hypotheses, even for definitions):
  - (a) Fundamental Theorem of Arithmetic, definition of prime
  - (b) Any/all definitions of congruence mod  $n$
2. Prime factor a given number; use prime factorization to find:
  - (a) GCD, LCM, numbers with given GCD and LCM
  - (b) Number of factors, list of factors in a given range
3. Demonstrate the Prime Number Test; use it to explain when a given sized Sieve is “done.”
4. Create a Diophantine equation in two variables or a congruence in one variable that has/lacks solutions. Be able to explain why informally, without actually solving.
5. Solve a given Diophantine equation in two variables: I may ask for a specific number of solutions, all solutions, or solutions with certain limitations (such as positive).
6. Use congruence arithmetic to simplify numeric expressions mod my choice of  $n$ .
7. Identify/create numbers that have/lack multiplicative inverses mod my choice of  $n$ ; explain.
8. Find a given number’s multiplicative inverse mod my choice of  $n$ .
9. Solve congruences, showing work as we’ve established; beware extraneous solutions!

**Take-home task:** Solve a given system using my choice of nested substitution and/or CRT formula.  
(It will be due Monday, Nov. 6.)

**Proof Tasks:**

1. Master proofs of Thm 3.1, Cor. 1-2 on p.40, FTA existence, FTA uniqueness.
2. Prove small results about primes similar to those in p.43 HW.
3. Proofs of Theorems 3.4 and 3.5 will NOT be asked.
4. Prove one direction within TFAE proof for congruence mod  $n$  definitions.
5. Prove basic results about congruence, such as Theorem 4.2, 4.3, and p. 67-68 HW.
  - (a) When instructed, use ONLY the definitions of congruence in such proofs.
  - (b) Use previous congruence results when allowed.
  - (c) Previous DIVISIBILITY results (Exam #1 material) are always allowed in congruence proofs.

Divisibility TESTS will NOT be asked about on the exam, but you are welcome to use them if you like.

**Bring a calculator.**