Math 320 - Dr. Miller - Topics List for Final Exam, Fall 2017 - THURSDAY, Dec. 14, 1:00-3:00 pm

Non-Proof Tasks: Bring a calculator! *Pythagorean Triples are assessed on the separate HW, not this exam.*

1. Precisely, FULLY state the following (including hypotheses, even for definitions):
   (a) Defns (all versions): divides, GCD, LCM, prime, relatively prime, congruent mod n
   (b) Defns: arithmetic, multiplicative functions, Pythagorean Triple, primitive PT, Diophantine equation
   (c) Thms: Well-Ordering Principle (WOP), Division Algorithm, Fundamental Thm of Arithmetic (FTA)
   (d) Thms: Chinese Remainder Theorem (CRT), Wilson's, Fermat's Little (FLiT), converse to Wilson
2. Find the values of q and r promised by the Division Algorithm for given dividend and divisor.
3. Understand, use, give examples of synonyms for "divides": factor, divisor, multiple, divisible.
4. Classify as true or false statements about divisibility, GCD, LCM, congruence.
5. Find GCD, LCM of 2 or more numbers by your choice of inspection, listing, algorithm.
6. You can also use $gcd(ka, kb) = k \cdot gcd(a, b)$ and $gcd(a, b, c) = gcd(gcd(a, b), c)$ in computations.
7. Express the GCD of two positive integers as a linear combination of them.
8. Find sets of numbers that are/aren't mutually/pairwise relatively prime.
9. Memorize p.22 Corollary (linear combinations equal gcd's multiples) to use in computations/proofs.
10. Prime factor a given number; use prime factorization to find:
    (a) GCD, LCM, numbers with given GCD and LCM, τ, σ, ϕ, list of factors in a given range
11. Demonstrate the Prime Number Test; use it to explain when a given sized Sieve is "done."
12. Create a Diophantine equation or a congruence that has/lacks solutions. Explain without actually solving.
13. Solve a given Diophantine equation: find some/all solutions, or solutions with certain limitations.
14. Identify/create numbers that have/lack multiplicative inverses mod my choice of n; explain.
15. Use congruence arithmetic, FLiT, Wilson to find a given number's multiplicative inverse mod n.
16. Solve/simplify congruences, showing work as we've established. Use congruence arithmetic, FLiT, Wilson.
17. Solve a SHORT system via nested substitution; formally state CRT formula and justify why it works.
18. Demonstrate divisibility tests for 2 through 12; find missing digits/examples that are/are not divisible.
19. Informally tell what $\tau(n)$, $\sigma(n)$, $\phi(n)$ represent; compute them for given n; find n with specified τ, σ, ϕ.

Proof Tasks: *Proofs about basic concepts will state whether previous results may be used, or ONLY definitions.*

1. The following are always allowed as lemmas/previous results throughout the ENTIRE exam:
   (a) Well-Ordering Principle (WOP), both types of induction, Linear Combination Theorem (LCT)
   (b) Alternative definitions of prime (including Cor. 2 p.40), relatively prime, GCD
   (c) Division Algorithm, equivalence of the three definitions of congruent mod n
   (d) Fundamental Theorem of Arithmetic (except in its own proof!), Wilson's Thm, Fermat's Little Thm
2. The following are allowed as lemmas unless instructions say "definitions only":
   (a) All parts of Theorem 2.2 (properties of the divides relationship)
   (b) Euclid's Lemma and Corollary 2 p.23 about relatively prime numbers, products, and "divides"
   (c) Trivial qualities about GCDs given in #10, 11, and 12b p.25
   (d) Basic properties of congruence given in Theorems 4.2 and 4.3
3. Prove my choice of all or part of the Fundamental Theorem of Arithmetic (existence, uniqueness).
4. Use the Division Algorithm to launch proofs by cases, as in HW #2. It's not always obvious!
5. Most proofs will be new or in-class/text results on: $a|b$, GCD, LCM, relatively prime, prime, congruence.
   (a) Practice lots of text, class, and HW results, but prepare for new claims.
   (b) Some proofs may be short/simple, but others may require attention to detail. Think carefully!
   (c) Good non-trivial GCD results to practice are Non-Proof Item #6, $gcd(a, b) \cdot lcm(a, b) = ab$, etc.
   (d) Euclid's Lemma and the previous-page Corollary are also good practice.
   (e) Prove the circumstances under which congruences/equations have/lack solutions.
   (f) Prove the circumstances under which elements have/lack inverses mod n.
   (g) Prove small results about forms of primes similar to those in p.43 HW.
   (h) Prove basic results about congruence, such as Theorem 4.2 and p.68 #8, #17.
   (i) Prove (and state!) divisibility tests, including ones similar to the 7-test.
   (j) Prove congruences using Wilson's Theorem, FLiT, as in HW, p.89 Lemma, #6-7 p.96.
6. State appropriate hypotheses for the lemma that n divides n-choose-k; prove it.
7. Prove the converse to Wilson's Theorem. Prove statements about τ, σ, ϕ when n is/isn't prime.