Topics for Exam 1, MATH433-Summer 2013

The exam will consist mainly of the problem from the suggested homework posted for the preparation to the quizzes 1-7 and the problems similar to those solved during the class. It does not mean it will consist only of the problems similar to the problems from these quizzes but such problems will form a substantial part of it. A substantial part of the test will be computational checking your ability to apply the Euclidean algorithm, to find the inverse of a congruence class, to solve a linear congruence and a system of linear congruences using the Chinese Remainder Theorem, to find the remainder of a big power of a number modulo another number using Fermat's and Euler's Theorem, to know how to make decoding in RSA public key system. However, a part of the test will consist of problems that will require to write a proof (again such problems will be similar to the suggested homework posted for the preparation to the quizzes 1-7, the problems from quizzes 1-7, and/or exercises solved in class).

Below are the topics for the exam. Please read carefully all items below. Then make the review topic by topic. Note that the exam will cover most of the topics below. If a specific Theorem/ Corollary/theoretical exercise is indicated in this list it means you should be able to prove it as well. Do not put yourself in the situation that you come to the test without reviewing some of the topics. If you struggle with a topic, do not hesitate to come to my office hours or send me an email with your concerns.

1. Greatest common divisor, Euclidean algorithm, properties of coprimes (Theorem 1.1.6, Exercise 6, page 15);
2. Mathematical induction;
3. Primes, the sieve of Eratosthenes, prime factorization, Unique Factorisation Theorem (Theorem 1.3.3, Corollary 1.3.4, pp. 28-29);
4. Congruence classes, modular arithmetic;
5. Inverse of a congruence class (to know the criterium for invertibility and the algorithm for finding inverse, Theorem 1.4.3, page 43)
6. Linear congruences (to know the condition for solvability of a linear congruence and the algorithm how to solve it, Theorem 1.5.1, page 50)
7. Chinese Remainder Theorem (Theorem 1.5.2, page 54)
8. The multiplicative order of a congruence class (to know properties of the order given in Theorems 1.6.1 and 1.6.2, page 60-63)
9. Fermats little theorem (Theorem 1.6.3, page 63-64), Eulers theorem (Theorem 1.6.7, pages 68-69)
10. Eulers φ-function (to know how to calculate it from the prime factorization of a number)
11. Public key encryption, the RSA system (to know how to decode the message)
12. Relations (to know how to manipulate with the notions of reflexivity, symmetricity, weak antisymmetricity, transitivity, of an equivalence relation, a partial order and a strict partial order)