Math 406 Test I Review, Spring 2015

Dr. Holmes

February 16, 2015

Chapter 1: This section contains general concepts which might enter into a test question, such as triangular numbers, prime pairs (or prime triplets as in question 1.3). A question based on this section is likely to be one which is easy to do – if you get the right idea.

Chapters 2,3: Be familiar with the formulas that generate Pythagorean triples. I might ask you questions which actually require you to compute some Pythagorean triples.

The entire Pythagorean Triples Theorem proof is rather much for a test question, but I might ask you a question based on a step in this proof.

Question 2.1 is examinable (talk about divisibility of a, b, c by 3 or 5 in a primitive Pythagorean triple; which ones are even or odd is also fair game).

It might be useful to know the relationship between Pythagorean triples and points with rational coordinates on the unit circle.

Chapters 5,6: You should be ready to compute $\texttt{gcd}(a, b)$ and express it in the form $ax + by$, both as an easy freestanding question and as a step in other questions.

Question 5.3 might be examinable (showing that $r_{i+2} < \frac{r_i}{2}$, not the logarithm stuff).

Chapter 7: Lemma 7.1, statement and proof,p. 46, is examinable. Problems 7.1 and 7.2 are related, and might be used as variations.

Problem 7.3 is examinable (it is related to issues in the proofs of the results about Pythagorean triples).

Chapter 8: Theorem 8.1 p. 59 is examinable in the sense that I may ask you to solve equations of this form and find all solutions (or tell me how many solutions there are). You should be able to use this theorem (I wont ask you to prove it).

You should be able to compute multiplicative inverses in modular arithmetic.

I won't ask you directly about the Polynomial Roots mod p theorem, but I might ask you to cook an example of an m such that mod m arithmetic contains more than two square roots of some remainder (and tell me what the remainders are). Think about how you could do this for a different polynomial than $x^2 - a$: that might be the basis of a challenge problem. 8.10, in a similar vein, might be examinable.

Chapters 9.10: You should be able to prove Fermat's Little Theorem and use it to compute powers in mod p arithmetic. You should similarly be able to prove Euler's Theorem, though I am less likely to ask you for this proof, and you should be able to use it to compute powers in mod m arithmetic.

Chapter 11: You should be able to compute the Euler ϕ function for numbers that you can factor (and use it to compute powers in modular arithmetic). You should be able to solve equations of the sort described in the Chinese Remainder Theorem (you might even have a word problem).

Chapter 12: The proof that there are infinitely many primes is examinable. Theorem 12.2 might make a challenge problem.

Chapter 16: You should be able to compute powers in modular arithmetic by repeated squaring (either the way I do it or the way the book does it): you might be asked to use this technique and compare results with answers using the methods of chapters 9-11.

General Remark: I am not going to examine you on axioms of arithmetic or formal definitions of number systems, but I might examine you on induction or the use of the Well-Ordering Theorem. Think of problem 7.4 or the proof that numbers have prime factorizations (simpler than the proof that they have *just one* prime factorization).