Review sheet for Math 406 Test II, Spring 2016

Dr Holmes

April 13, 2016

Going through the notes and listing topics... You will be allowed a TI-89 or equivalent on this exam, and you will need one.

As usual, there will be four or five computation questions, one of which will be dropped, and three or four proof questions, one of which will be dropped.

section 9: You should be able to compute the Euler ϕ function for numbers you can factor. You should be reminded that the board example of finding several n such that $\phi(n) = 160$ is a kind of question I might ask.

The proof of Fermat's Little Theorem or Euler's theorem is something I might ask. The FLT is simpler so more likely.

section 10: A baby RSA example is fair game as a computational question. Since you will have your TI-89 it won't be nearly as laborious. Merely finding a kth root in a prime modulus p where k is relatively prime to $p - 1$ is also fair game.

section 11: You should know Korselt's Criterion and be able to determine whether numbers I give you are Carmichael numbers. Again, having a TI-89 makes this straightforward.

You should be able to carry out the Rabin-Miller test for compositeness of an odd number (computation)

You should be able to present the proof of the Rabin-Miller theorem (p. 38 of the notes).

section 14: You should know the basic theorem about even perfect numbers. If I give you an even number, you should be able to tell if it is perfect or not. Were I to ask about the proof of this theorem, I would only be asking about the direction proved by Euclid (a number of the given form is perfect), not the proof that all even perfect numbers are of this form, which is harder.

You should be able to compute the σ function (sum of the divisors) for a number you can factor.

You should be able to prove (for example) that a number of the form 3^k is not perfect, by computing $\sigma(3^k)$ and showing that it cannot be $2 \cdot 3^k$. This is algebra! Don't lose points by saying anything about the form of even perfect numbers – this number is odd!

The theorem in section 14.3 that every even perfect number ends in 6 or 8 is fun.

section 15: You should be able to find a primitive root in a small prime modulus.

You should be able to determine the order of an element of a small prime modulus.

You should know that the order of a residue mod p has to be a divisor of $p - 1$, but you don't have to be able to prove it.

section 16: You should know Euler's Criterion for whether a residue mod p is a quadratic residue: be able to use it (computation) and to prove that it works (p. 48).

The results about how many QRs there are and about products of QRs and NRs might also make proof questions.

Be able to compute a Legendre symbol (or Jacobi symbol) using the Generalized Quadratic Reciprocity Theorem (or the basic one: you will be working with numbers small enough to factor).

The only part of the Quadratic Reciprocity theorem which I might ask you to prove is the first part (whether -1 is a QR mod p) because this is simple (p. 48).

Famiiarize yourself with the proof that there are infinitely many primes of the form $4n + 1$ (p 51).