Math 406 Test II, Spring 2015

Dr. Holmes

April 6, 2015

The exam lasts from 9 am to 10:15 am officially. What really happens at 10:15 am is that you get a five minute warning. You are allowed the use of your writing instrument, your test paper, and your non-graphing scientific calculator (no symbolic computation capability).

I am going to let the number of problems that I drop or reduce the weight of be determined by class performance. Make sure that you attempt both computational problems and proof problems. You should be able to tell which are which. You are probably all right if you skip one in each category.

1. Express the greatest common denominator of 4321 and 3456 in the form $4321x + 3456y$.

2. RSA calculations. Let $N = 91$ (of course no one will notice that $91 = (7)(13)$!). Let $r = 5$ (explain why I did not choose $r = 3$).

   Find the decryption exponent s.

   Decrypt the message 35 (you **know** what it decrypts to, but show the calculations).

   Why is 35 not really a very good message to be sending with this key?

3. How many generators are there in mod 29 arithmetic? Find one.

4. Determine whether 2435 is a quadratic residue mod 2801 by computing the appropriate Legendre symbol. The Generalized Law of Quadratic Reciprocity is supplied. Be careful to document all of your calculations.

5. Use the procedure on the attached page 189 to find integers a, b such that $a^2 + b^2 = 157$. We know that there must be such integers because 157 is a prime of the form $4n + 1$. I give you the information that $129^2 + 1^2 = (106)(157)$ to start with.

6. Prove that if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is a perfect number.

7. Show that if $\texttt{gcd}(b, m) = 1$ and $\texttt{gcd}(k, \phi(m)) = 1$, then b has one and only one kth root in mod m arithmetic (i.e, there is exactly one x with $0 < x < m$ such that $x^k \equiv b \,\texttt{mod}\, m$). Hint: this is an application of Euler's theorem and facts about existence of reciprocals in modular arithmetic.

8. Prove the Rabin-Miller theorem: if p is an odd prime and $p - 1 = 2^k q$ where q is odd, and $0 < a < p$, then either $a^q \equiv 1 \bmod p$ or some $a^{2^i q} \equiv -1 \bmod p$ where $0 \leq i < k$. You need Fermat's Little Theorem (stated elsewhere in your paper) and a fact about roots of polynomials in prime moduli.

9. Prove that there are no Carmichael numbers of the form pq, where p and q are distinct odd primes. You may assume Korselt's Criterion: an odd composite number n with no divisors which are squares of odd primes is a Carmichael number iff $p-1|n-1$ for each prime p which is a divisor of n.

   Hint (at the risk of making it absurdly easy): set $n = pq$ and think about the two numbers $pq-1$ and $(p-1)(q-1)$.