Math 406 Test II, Spring 2014

Dr. Holmes

March 20, 2014

The exam will begin at 1030 am and end at 1145 pm (officially: I will actually give a five minute warning at that point). You may use your non-graphing scientific calculator.

You should do five of the computational problems 1-6 and two of the proofs 7-10. You are welcome to do more; your best work will count and good work on more problems may give extra credit.

1. Euclidean algorithm and an application. Part c is optional and can improve your score on the CRT problem on Test I.

   (a) Find integers x and y such that $111x + 26y = \texttt{gcd}(111, 26)$. Use an organized format (I suggest my tabular format) and be sure to identify x, y and $\texttt{gcd}(111, 26)$

   (b) Compute the multiplicative inverse of 26 in mod 111 arithmetic.

(c) (optional, can improve mark on the Test I CRT question) Hint: if you set this up right you have already done much of the work.

Solve

$$x \equiv 8 \bmod 111$$

$$x \equiv 2 \bmod 137$$

Be sure to state the smallest positive solution and the general form of all solutions.

2. Let $N = 35$ and $r = 3$ make up your RSA key.

   Determine s, your decryption exponent (of course you know how to factor 35).

   Decrypt the message 49.

3. Use Korselt's Criterion to determine whether each of the following numbers is or is not a Carmichael number.

   (a) 715 = 5*11*13

   (b) 605= 5*11*11

   (c) 1105 = 5*13*17

4. Compute the numbers of interest in the Rabin-Miller test (where $m = 2^k q$, q being odd, compute $a^{2^i q} \texttt{ mod } m$ for each i from 0 to $k-1$) where $a = 2$ and $m = 1729$. What do the results tell you about 1729?

5. Compute the sum of the divisors of $792 = 2^3 * 3^2 * 11$, using the fact that the sum of divisors function is multiplicative.

6. Determine whether 851 is a quadratic residue mod 1103, by computing the Legendre symbol $\left(\frac{851}{1103}\right)$ using the Quadratic Reciprocity Theorem.

   The fact that 851=23*37 will be useful. You should comment on the reasons for plus signs or minus signs having to do with remainders mod 4 and 8.

   The answer here is 1 0r -1 and it is very easy to make a mistake: I will be more interested in the documentation of steps using the theorem, so explain them carefully.

7. Prove that if $\texttt{gcd}(b, m) = 1$ and $\texttt{gcd}(k, \phi(m)) = 1$ then the congruence $x^k \equiv b \bmod m$ has one and only one solution (up to congruence mod m).

8. Prove Euclid's theorem, that $2^{p-1}(2^p - 1)$ is perfect if $2^p - 1$ is a prime. You do need to make it clear that you know what "perfect" means.

9. Use Fermat's Little Theorem to prove the validity of the theorem behind the Rabin-Miller test: if p is an odd prime and $p-1 = 2^k q$, q odd, and $1 \leq a < p$ then either $a^q \equiv 1 \bmod p$ or some $a^{2^i q}$ with $0 \leq i < k$ is congruent to -1.

10. Prove that the product of a quadratic residue (QR) and a non-quadratic residue (NR) is a non-quadratic residue (NR) in mod p arithmetic for a fixed odd prime p.