Math 406, Test I, Spring 2014

Dr. Holmes

February 18, 2018

You are allowed your paper, your writing instrument, and your nongraphing scientific calculator. Good luck!

There are five computational questions (more or less), 1-5, and three proof questions (more or less), 6-8. You may drop one computational question and one proof question. If you do more work, your best work will count, and good work over and above that will benefit you.

1. Find the greatest common denominator of 321 and 123 and find integers x and y such that 321x+123y=`gcd`(321,123). Use the algorithm demonstrated in class and show all work.

   The parts of your answer should be clearly identified as such (the gcd, x and y). This is most conveniently done by writing out the equation with numbers substituted in.

   Find another pair of integers x, y for which this is true.

2. I give you the information that $85 = 6^2 + 7^2 = 2^2 + 9^2$. From this data, compute and exhibit two different Pythagorean triples (a, b, c such that $a^2 + b^2 = c^2$) with $c = 85$, and verify that they are indeed Pythagorean triples.

3. Find all solutions to the congruence $24x \equiv 36 \bmod 60$. Your work should be informed by knowledge of the proof of the Linear Congruence Theorem.

4. Compute $2^{110} \,\texttt{mod}\, 111$ by the method of repeated squaring. Show calculations in detail.

   Explain why your result verifies that 111 is not a prime number (if you had any doubts about this), by reference to an appropriate theorem (this depends in no way on factoring 111).

   Now compute $\phi(111)$ (from the prime factorization of 111 which you should be able to determine) and use Euler's Theorem to compute $2^{110} \,\texttt{mod}\, 111$.

5. Solve the system of equations

   $x \equiv 12 \texttt{mod} 111$

   $x \equiv 121 \texttt{mod} 137$

   State the smallest solution and give a general description of all the solutions.

6. Prove that if $\texttt{gcd}(a, b) = 1$ and $a|bc$, then $a|c$. Your proof should not use any facts about factorizations into primes.

7. Demonstrate that if $\mathtt{gcd}(s,t) = 1$ that $\mathtt{gcd}(\frac{s^2+t^2}{2}, \frac{s^2-t^2}{2}) = 1$ (assuming also that $s > t$ and s, t are both odd.) You may use facts about factorization into primes if you wish.

8. Prove that if $r = a \,\texttt{mod}\, b$ abd $r_2 = b \,\texttt{mod}\, r$, that $r_2 < \frac{b}{2}$. This is not a question about congruences (those are real equations and the `mod`'s are remainder operations). It is a question about the division algorithm and it tells us something about the Euclidean algorithm.

   Tell me briefly what we learn from this about the Euclidean algorithm (no proof required).