Math 406 Test I, Spring 2016

M. Randall Holmes

February 25, 2016

The exam starts at 10:30 and officially ends at 11:45. I will probably really give a five minute warning at 11:45 if people are still working.

You are allowed your writing instrument, your test paper, and a non-graphing calculator.

1. Find integers x and y such that $512x + 101y = \gcd(512,101)$, using the tabular method that was taught and demonstrated in class.

   Do tell me explicitly what x is, what y is, and what the gcd is. I have had students show me the correct table who clearly had no idea where the information was – not that I suspect any of you have this problem.

2. Chinese Remainder Theorem: Find a solution to the system of modular equations

   $x \equiv 47 \texttt{mod} 512$

   $x \equiv 51 \texttt{mod} 101$

   Of course you can recycle information from the previous problem if you are clever (and you are all clever!)

   Be sure to find the smallest solution, and to give a general description of all solutions.

3. Compute $3^{1083} \texttt{mod} 1147$ by the method of repeated squaring.

   Then consider the fact that 1147 can be factored as (31)(37).

   Compute $\phi(1147)$. Once you have done this, explain how to use Euler's theorem to compute $3^{1083} \bmod 1147$ with hardly any effort at all.

4. Compute all solutions to the congruence

$$52x \equiv 44 \texttt{ mod } 100$$

5. Prove Euclid's lemma: if p is a prime, and p goes evenly into ab, then either p goes into a or p goes into b.

6. Prove that if s and t are relatively prime odd numbers, then $\frac{s^2+t^2}{2}$ and $\frac{s^2-t^2}{2}$ are relatively prime. Hint: suppose they are not relatively prime. Then they have a common prime factor p. What goes wrong? If you are clever, you might notice why it is important that we consider a prime common factor.

7. Prove that in any primitive Pythagorean triple $a^2 + b^2 = c^2$, one of a and b must be divisible by 3.