Math 406 Spring 2021 Midterm

Dr Holmes

March 12, 2021

This is a takehome midterm. It will be distributed on Thursday March 11 and is due Tuesday March 16 at 1155 pm.

Please do not consult any other person than myself.

In all problems, you are welcome to use my programs and spreadsheets, but you **are** expected to show work. So the programs are better for checking results; though if one understands the spreadsheets one can extract the writeup of the work from them (which does not mean copy the spreadsheet: explanations are expected).

1. Compute the greatest common divisor of 6321 and 1236, and find integers x and y such that $6321x + 1236y = \mathtt{gcd}(6321, 1236)$.

   Show work. In each division that you carry out, state the quotient and remainder.

2. Prove that if s and t are relatively prime and both odd, $(st, \frac{s^2-t^2}{2}, \frac{s^2+t^2}{2})$ is a primitive Pythagorean triple.

   You will need to verify both that it is actually a Pythagorean triple and that the numbers in the triple have no nontrivial common factor (hint: suppose that $\frac{s^2-t^2}{2}, \frac{s^2+t^2}{2}$ have a nontrivial common factor d (which you may suppose is a prime, why?) and show that s and t would have a common factor, contrary to assumption).

3. Solve the following equations in modular arithmetic (two separate problems). Find all solutions which are nonnegative and less than the modulus. Show all work and explain any theorems you use.

   (a)
   $$111x \equiv 23\texttt{mod}137$$

   (b)
   $$161x \equiv 217\texttt{mod}259$$

4. Compute $17^{1939}\mathtt{mod}2047$ using repeated squaring (lengthy, and please explain each step: of course you can set it up on the spreadsheet but I want to see justifications of each number using a mod 2047 calculation).

   Compute $17^{1939}\mathtt{mod}2047$ again using Euler's theorem (which should be much faster).

5. Find all numbers n with $\phi(n) = 352$.

6. Chinese remainder theorem

   Find x such that

$$x \equiv 13\mathtt{mod}111$$

$$x \equiv 1\mathtt{mod}137$$

   Show all calculations. Give the smallest nonnegative solution and a description of all integer solutions.

7. My RSA key is $N = 1147; r = 7$.

   Encrypt the vitally important message 42 (the meaning of life, the universe and everything) to me.

   Of course, I'm not really very secure, since $1147 = (31)(37)$ is not really much of a secret.

   Determine my decryption exponent and check that the encrypted message really does decrypt to 42. Please show all calculations (of course you can easily check this with my spreadsheets).

8. Verify that $2^{10}(2^{11}-1)$ is not perfect by computing the sum of its proper divisors.

   Your calculations should include a computation of $\sigma(2^{10}(2^{11}-1))$ using the fact that the σ function is multiplicative.

9. I must admit that thsi question is really a take-home question, but it should not be hard to do with my modular exponentation spreadsheet.

   49 is of course a composite number. Find all of its Rabin-Miller misleaders (all the numbers *a* between 2 and 47 inclusive for which the Rabin-Miller test reports that 49 “might be prime”). Show the full calculations for at least two of the misleaders; you don’t have to show them for the non-misleaders.

   What this question is really testing is that you understand the Rabin-Miller test; your computations should clearly indicate understanding of the test.