Math 406 Spring 2021 Second Exam

Dr Holmes

April 24, 2021

This is the second take home exam in Math 406, Spring 2021. It is being distributed on 4/24/2021 and will be due at 5 pm on Friday, May 7. You may not communicate about this exam with any person other than the instructor. There are no other restrictions on what resources you may use. Please show work when asked to do so.

If you think you have identified an error in the instructions or setup of a problem, please communicate with me promptly. These do happen (particularly since I am writing under the effect of COVID vaccine side-effects) and can be dealt with.

1. Korselt's criterion – use the criterion to determine whether some numbers are Carmichael numbers. Tell me exactly how you use the Criterion to answer the question (briefly explain why the Criterion tells you the number is or is not Carmichael).

   Then for each number m from the list above which is not a Carmichael number, find an actual a which is a counterexample to Carmichaelness: that is, for which $\texttt{gcd}(a, m) = 1$ and $a^{m-1} \not\equiv_m 1$. Show calculations (of course, these could be copied from spreadsheet or computer program output).

   Hint: you need to factor each number. None of these numbers has a smallest prime factor greater than 211: a TI89 will factor all of them, or a fairly simple loop in Python.

   You are very free to use my spreadsheets or programs in my Python file. I dont think the spreadsheet works correctly to compute powers in all of these moduli: some are too large and something like round off error sets in.

   (a) 294409

   (b) 320087

   (c) 56052361

   (d) 1928107

2. 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 $(p-1)(q-1)$.

3. Solve $x^{1153} \equiv 2 \bmod 28907$. Hint: there is a theorem in the notes about computing roots in modular arithmetic under special conditions.

4. Find a number in mod 28907 arithmetic which has four distinct square roots. State the number and at least four square roots mod 28907 which are incongruent mod 28907. Hint: look at the example in the last paragraph on p. 34 of the notes. We are approaching things here from a slightly different angle: you need to do a little bit of algebra.

5. Make a table of the orders of all positive integers less than 37 in mod 37 arithmetic. Make a list of all the generators in mod 37 arithmetic. Choose one of the generators a. List $a^n \texttt{mod} 37$ for n from 1 to 36. Circle the powers which are generators. What common characteristic do the exponents which give generators have?

6. One of the primes 11159 and 11161 can be expressed as a sum of two squares and one cannot. You should be able to determine which one can be expressed as a sum of two squares immediately: tell me which one and explain why (and explain why the other one cannot).

   For the one which is a sum of two squares, find two squares which add to it. Use the algorithm on page 187 of the book (the physical book, not the notes). To find the number M you start with, use the hint in the footnote on page 188.

   Show work following the algorithm on p. 187 and explain how you used the footnote on p. 188 to compute the starting value of M.

7. Determine whether 283 is a quadratic residue mod 11159 using the Quadratic Residue theorem. Carefully state the reasons for each step (since there are only two possible answers, I will really scoring on accurate justifications: this is a test of precise application of a procedure).

8. An Euler integer is a complex number of the form $a + bi\sqrt{3}$, where a, b are integers. Of course ordinary integers are also Euler integers.

   An Euler prime is an Euler integer n with the property that if $ab = n$ (a and b Euler integers) then $\{a, b\}$ must be $\{1, n\}$ or $\{-1, -n\}$.

   Find an integer prime which is not an Euler prime (hint: think about conjugates).

   Find an integer which can be expressed as a product of Euler primes in two fundamentally different ways (differing by more than order or multiplication by -1). Hint: there is a very small example.

   Please explain in detail, giving all relevant factorizations into Euler primes.