# Math 287, Spring 2022, Test II

Dr Holmes

April 6, 2022

This exam will be given from 1030-1145 on Thursday April 7.

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

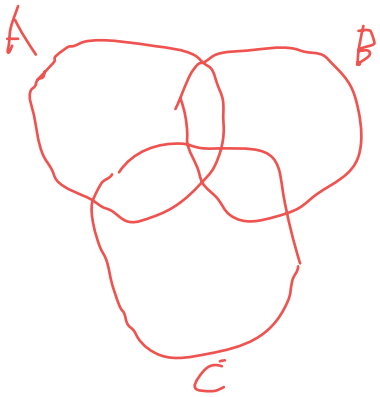
1. Define $a_1 = 6; a_2 = 20; a_{k+2} = 6a_{k+1} - 8a_k$.

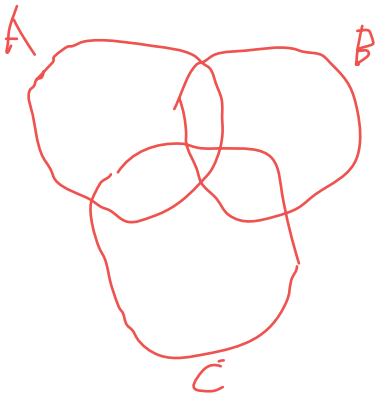
   Compute the terms of this sequence up to $a_6$.

   Prove by strong induction that $a_n = 2^n + 4^n$ for each natural number $n$.

2. Give a Venn diagram demonstration of the identity $A - (B \cap C) = A - B \cup A - C$.

   You should shade sets of interest informatively in each of the two pictures, provide a key to the shadings, and clearly outline the set which is the result of the computation.



3. Do one of the two proofs. If you do both, the best one will count; if you do well on both extra credit is possible.

   (a) Prove that the relation $x \equiv_n y$ is an equivalence relation

(b) Prove that if $a \equiv_n a'$ and $b \equiv_n b'$, then $ab \equiv_n a'b'$.

4. Construct addition and multiplication tables for mod 7 arithmetic, and make a table of multiplicative inverses.

5. Prove Euclid's Lemma: if $p$ is prime and $p|ab$ then either $p|a$ or $p|b$.

   The proof depends on the extended Euclidean algorithm theorem, which I remind you says that for any $a, b$ not both equal to zero there are integers $x, y$ such that $ax + by = \texttt{gcd}(a, b)$.

6. Each of the parts in this problem provides information for the next one.

   (a) Find integers $x, y$ such that $137x + 15y = 1$ using the extended Euclidean algorithm (my table format).

   (b) Compute $15^{-1} \texttt{mod} 137$.

   (c) Solve the equation $15x \equiv_{137} 16$ for $x$.

7. Compute $23^{72} \texttt{mod} 100$ using the method of repeated squaring. Show all work.

8. Simplification of modular exponentiation.

   (a) Use Fermat's Little Theorem to simplify the calculation of $2^{927} \texttt{mod} 23$

   (b) Use Euler's Theorem to simplify the computation of $5^{1282} \texttt{mod} 55$ (notice that 55 is of the form $pq$ with $p$ and $q$ prime).

9. My public key has $N = 55, r = 3$.

   Encrypt the message 42 to me.

   My secret, which you can't possibly guess, is that $N = (5)(11)$.

   Determine my decryption exponent $s$.

   Carry out the calculation I will do to decrypt your message.

   (The numbers here are wonderfully small; of course the cryptographic security is zip!)