Math 401 Fall 2019
Cryptology HW 5
Due Thursday, October 3

1. Is 2 a primitive root mod 31? Prove or disprove your answer.
2. Is 17 a primitive root mod 31? Prove or disprove your answer.
3. Compute $\log_5(17) \mod 23$ and $\log 10(22) \mod 47$.
4. Suppose you are doing a Diffie-Hellman key exchange with Alice. You have agreed to use $p = 1373, g = 2$.
   (a) You choose the secret value $b = 871$. What number should you send to Alice?
   (b) Alice sends you $A = 974$. What is the secret shared key?
   (I recommend using Wolfram Alpha or Mathematica or something similar for this one, to avoid long and tedious hand arithmetic).
5. Suppose you are doing another Diffie-Hellman key exchange, this time with Bob. You have chosen $p = 29$ and $g = 12$.
   (a) You choose the secret value $a = 11$. What number should you send to Bob?
   (b) It turns out that Bob has chosen $b = 15$. What number does he send you?
   (c) What is your shared secret?
   (d) How hard would it be for Eve to break your secret? What's unusual about this choice of g?
6. From the definition of big-O notation, prove that $x^2 + \sqrt{x} = O(x^2)$.
7. Prove (using the definition or the limit property) that:
   (a) $k^{300} = O(2^k)$
   (b) $(\log_2(k))^{100} = O(k)$.
8. Use the efficient modular exponentiation algorithm (showing your steps) to compute $3^{51} \mod 71$.
9. Use Shanks's algorithm (showing your steps) to solve $11^x \equiv 21 \mod 71$.