Discrete Test 2, Spring '20. Version B.

My signature here is to pledge that I have answered each test question from my own knowledge and understanding, without giving or receiving any unauthorized help.

Sign:______________________________

Name:______________________________

Time:______________________________

Date:______________________________

Read directions carefully! Put a box around your final answer if there is any extra work shown.

1. Fill in the blanks. Suppose we are trying to prove the statement

   "$\forall x, y, z \in \mathbb{Z}$, $(x > 2 \text{ and } z|y^2) \implies (x + |y| \geq 7 \text{ and } xy \nmid 4.)$"

   (Answer the following without using the word "not" or the symbol "$\sim$.")

   a) For a proof via the contrapositive we assume:

   ____

   and show:

   ____.

   b) For proof by contradiction we assume:

   ____

   and show that we reach a false conclusion.

   c) For direct proof we assume:

   ____

   and show:

   ____.

   d) For disproof by counterexample we find:

   ____.

2. Prove: $\forall a, b \in \mathbb{Z}$, (a is even and $4|(b+7)$) $\implies$ $4 \nmid (a^2 + b^2 - 36)$, by precisely following these steps:

   Step 1: Write the negation of the implication.

   ____

   Step 2: Assume the negation of the implication and use it to prove that $4|13$, thus achieving a contradiction.

   Hint! Assuming the negation will mean three separate facts about divisibility, turned into equations. Use a different variable for each $(p, m, n.)$ You will substitute the first two facts into the third fact: but first, solve the second one a bit by subtracting 7 from both sides to get $b = 4m - 7$.

3. Prove: $\forall n \in \mathbb{N},\, n \geq 2 \Longrightarrow 3|(7^n - 3^n - 1)$.
   Label the base case, the inductive assumption, the statement to be shown, and then prove. Hint! In the proof, after you substitute, you can factor a 3 out of 3^k like this: $3^k = 3 \cdot 3^{k-1}$.

   Base case checked:

   Induction–Assume:

   Show:

   Proof:

4. Let $a_1 = 4, a_2 = 16$, and $a_n = 11a_{n-1} - 28a_{n-2}$. Prove: $\forall n \in \mathbb{N}, n \geq 1 \implies a_n = 4^n$.
   Label the base cases, the strong inductive assumption, the statement to be shown, and then prove.

   Base cases checked:

   Induction–Assume:

   Show:

   Proof:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26=0

5. Consider the sequence $a_n = (n^2 + 4) \mod 9$; starting at $n = 1$. Use it to encrypt the word FUZZY.

i	*letter*	std. number	a_i			
1	F					
2	U					
3	Z					
4	Z					
5	Y					

6. Consider the sequence $a_n = 2n + 1$; starting at $n = 1$. It has been used to encrypt a message, and the encrypted message is QNJN. Use the same sequence to decrypt and find the original word.

i	*letter*	std. number	a_i			
1	Q					
2	N					
3	J					
4	N					

7. Consider the BBS (Blum Blum Shub) sequence $a_n = (a_{n-1})^2 \mod pq$; with $a_0 = 7$ (that is, $k = 7$) and with $p = 5, q = 5$. Starting at $n = 1$, use this sequence to encrypt the binary number 1010.

i	*bit*	a_i		
1	1			
2	0			
3	1			
4	0			