Discrete Test 2 Review: first study quizzes!

(1) Prove $\forall a, b \in \mathbb{Z}$, if ($a \mod 6 = 5$ and $b \mod 4 = 3$) then $4a + 6b \mod 8 = 6$.
Use a Direct proof.

a) Write the assumption, translated to algebraic equations.

b) Write what we want to show, translated to algebraic equations.

c) Write the proof steps.

(2) Suppose we were to prove the statement "$\forall y \in \mathbb{Z}$, y is even $\Rightarrow$ $(y^3 - 1)$ is odd." (Answer using alegebraic equations, without using the word "not" or the symbol "$\sim$.")

a)For a direct proof we assume ______________________ and show ______________________.

b) For proof using the contrapositive we assume ___________________ and show ______________________.

c) For proof by contradiction we assume ______________________________________ and show that we reach a false conclusion.

(3) Use contradiction to prove: $\forall a, b \in \mathbb{Z}$, if ($a$ is even and b is odd) then 4 does not divide $(a^2 + 2b^2)$.
a) Negate the statement.

b) What do we assume? Translate to algebraic equations.

c) Use the assumptions to prove that $4|2$, as an algebraic equation.

(4) Prove by induction that: $\forall n \in \mathbb{N}$, if $n \geq 2$ then $3|(2^{(4n-4)} + 2^{(2n-3)})$.
a) Show the base case.

b) State the induction assumption, translate to algebraic equations.

c) State what we need to show, translate to algebraic equations.

d) Do the proof steps.

(5) Use a Direct proof to prove: $\forall z \in \mathbb{Z}, 3|(z + 1) \Rightarrow z^2 \mod 3 = 1$.

a) Write the assumption, translated to algebraic equations.

b) Write what to show, translated to algebraic equations.

c) Do the proof steps.

For your use:

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

(6) Given the one-time-pad sequence $(2, 6, 13, 1)$ encrypt the word COOL. Your output will be letters.

(7) Use the BBS sequence $a_n = (a_{n-1})^2 \mod pq$ to encrypt the word ZAP. Use the seed $a_0 = 11$ and the constant $pq = 7 * 13 = 91$. Start the encryption with $n = 1$.

(8) Use the same BBS sequence to decrypt the word LLJ. Use the seed $a_0 = 11$ and the constant $pq = 7*13 = 91$.

(9) Use the sequence $a_n = 5 + 3(a_{n-1} \mod n)$; $a_0 = 7$ to encrypt the digits 1101. Start with $n = 1$.

(10) Use the sequence $a_n = n^2 - 1$ to decrypt the digits 1110. Start with $n = 1$.

(11) Given universe $\mathcal{U} = \{1, 2, 3, 4, 5, 7, 9, 10, 21, 25\}$; $A = \{7, 9, 10, 21, 25\}$; and $B = \{5, 4, 7, 10, 21\}$. Find the following:

- $\overline{A \cup \overline{B}}$
- $(A - B) \cup (B - A)$
- $\overline{\overline{(B - A)} \cap A}$
- $|\mathcal{P}(A)|$
- $|\mathcal{P}(A \times B) \times A|$
- $|\mathcal{P}(A \cup B)|$
- $|\overline{A \cup B}|$

(12) How many PIN's are there with 7 digits, no repeated digits?

(13) How many PIN's are there with 3 digits, repeated digits allowed, and such that the first digit is not 0 and the second digit is not 9?

(14) How many ways can 7 students fill in the first row of 4 seats? (seated in order, leaving 3 students still standing.)

(15) How many DNA sequences are there, using $\{A, G, T, C\}$, of length 5 where the sequence cannot start with G in 1st location, and cannot repeat two letters in the 4th and 5th location?

(16) Also study the quizzes!