Discrete Test 2 Review: Answers!

(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.

$a = 6m + 5$ and $b = 4k + 3$

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

$4a + 6b = 8p + 6$

c) Write the proof steps.

$$\begin{aligned} 4a + 6b &= 4(6m+5) + 6(4k+3) \\ &= 24m + 20 + 24k + 18 \\ &= 24m + 24k + 32 + 6 \\ &= 8(3m + 3k + 4) + 6 \end{aligned}$$

(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 $y = 2k$ and show $y^3 - 1 = 2m + 1$.

b) For proof using the contrapositive we assume $y^3 - 1 = 2p$ and show $y = 2q + 1$.

c) For proof by contradiction we assume $y = 2k$ and $y^3 - 1 = 2m$ 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.

$\exists\, a, b \in \mathbb{Z}$ s.t. a is even and b is odd and $4 \mid (a^2 + 2b^2)$.

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

$a = 2k$ and $b = 2m + 1$ and $a^2 + 2b^2 = 4p$

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

$$\begin{aligned} & a^2 + 2b^2 = 4p \\ \Rightarrow\ & (2k)^2 + 2(2m+1)^2 = 4p \\ \Rightarrow\ & 4k^2 + 2(4m^2 + 4m + 1) = 4p \end{aligned}$$

$$\begin{aligned} & 4(k^2 + 2m^2 + 2m) + 2 = 4p \\ \Rightarrow\ & 4p - 4(k^2 + 2m^2 + 2m) = 2 \\ \Rightarrow\ & 4(p - k^2 - 2m^2 - 2m) = 2 \end{aligned}$$

□

(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.

Base case: $n = 2$: $2^4 + 2^1 = 18 = 3(6)$.

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

$2^{(4k-4)} + 2^{(2k-3)} = 3m$.

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

$2^{(4(k+1)-4)} + 2^{(2(k+1)-3)} = 3q$

d) Do the proof steps.

Proof.

$2^{(4(k+1)-4)} + 2^{(2(k+1)-3)} = 16(2^{(4k-4)}) + 4(2^{(2k-3)})$

$= 15(2^{(4k-4)}) + 3(2^{(2k-3)}) + 2^{(4k-4)} + 2^{(2k-3)}$

$= 15(2^{(4k-4)}) + 3(2^{(2k-3)}) + 3m$

$= 3(5(2^{(4k-4)}) + 2^{(2k-3)} + m)$.

□

(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.

$z+1 = 3k$

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

$z^2 = 3m + 1$

c) Do the proof steps.

$z^2 = (3k-1)^2$

$= 9k^2 - 6k + 1$

$= 3(3k^2 - 2k) + 1$

□

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.

C = 3 + 2 → 5 mod 26 = 5 → E
O = 15 + 6 → 21 mod 26 = 21 → U
O = 15 + 13 → 28 mod 26 = 2 → B
L = 12 + 1 → 13 mod 26 = 13 → M

(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 $n = 1$.

n		a_n	
1	Z = 26 + 30	56 mod 26 = 4	D
2	A = 1 + 81	82 mod 26 = 4	D
3	P = 16 + 9	25 mod 26 = 25	Y

$81^2 = 6561$

$91 \overline{)6561}$ 72 R 9
637
191
182
9

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

L = 12 − 30 → −18 mod 26 = 8 → H
L = 12 − 81 → −69 mod 26 = 9 → I
J = 10 − 9 → 1 mod 26 = 1 → A

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

n		a_n		
1	1 + 5	6 mod 2	=	0
2	1 + 8	9 mod 2	=	1
3	0 + 11	11 mod 2	=	1
4	1 + 14	15 mod 2	=	1

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

n		a_n		
1	1 + 0	1 mod 2	=	1
2	1 + 3	4 mod 2	=	0
3	1 + 8	9 mod 2	=	1
4	0 + 15	15 mod 2	=	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:

- $\overline{A \cup \overline{B}}$ $= \bar{A} \cap \bar{\bar{B}} = \bar{A} \cap B = B - A = \boxed{\{5, 4\}}$
- $(A - B) \cup (B - A)$ $= \{9, 25\} \cup \{5, 4\} = \boxed{\{9, 25, 5, 4\}}$
- $\overline{\overline{(B - A)} \cap A}$ $= (\overline{\overline{B - A}}) \cup \bar{A} = (B - A) \cup \bar{A}$
  $= \{5, 4\} \cup \{1, 2, 3, 4, 5\} = \boxed{\{5, 4, 1, 2, 3\}}$
- $|\mathcal{P}(A)|$ $= 2^5 = \boxed{32}$
- $|\mathcal{P}(A \times B) \times A|$ $= |\mathcal{P}(A \times B)| \cdot |A| = 2^{|A \times B|} \cdot 5 = 2^{5 \cdot 5} \cdot 5 = \boxed{5(2^{25})}$
- $|\mathcal{P}(A \cup B)|$ $= |\mathcal{P}(\{5, 4, 7, 9, 10, 21, 25\})| = \boxed{2^7}$
- $|\overline{A \cup B}|$ $= |\{1, 2, 3\}| = \boxed{3}$