1. Given universe $\mathcal{U} = \{3,4,5,7,9,10,11,23\}$; $A = \{5,7,9,10,11,23\}$; and $B = \{5,3,7\}$. Find the following:

- $\overline{\overline{(B-A)} \cap B}$ $= (B-A) \cup \bar{B}$
  $= \{3\} \cup \{4,9,10,11,23\} = \boxed{\{3,4,9,10,11,23\}}$

- $\overline{A \cup \overline{B}}$ $= \bar{A} \cap B = B - A = \boxed{\{3\}}$

- $|B \times \mathcal{P}(A \times B)|$ $= 3(2^{3\cdot 6}) = \boxed{3(2^{18})}$

- $|A \cup B|$ $= 3 + 6 - 2 = \boxed{7}$

2. Find the number of PINs using $\{0, ..., 9\}$, with 7 digits, no repeated numbers, where the first digit cannot be 3 and the fourth digit cannot be 5.

$\boxed{{}_{10}P_7 - {}_9P_6 - {}_9P_6 + {}_8P_5}$

$\left(= 490{,}560 \right.$
$\left. = 73 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \right)$

3. Find the number of DNA sequences using $\{A, G, T, C\}$, of length 5, where the first and second location cannot repeat, and the first location cannot be A.

$\boxed{3(4^4) - 3(4^3)}$

$(= 3^2 4^3)$ $(= 576)$

$(= 4^5 - 4^4 - 4^4 + 4^3)$

A _ _ _ _ $\quad$ x x _ _ _

$= 4^5 - 4^3(4 + 4 - 1)$

$= 4^5 - 7(4^3)$

4. Use contradiction to prove: $\forall z \in \mathbb{Z}$, $z^2 \equiv 7 (\text{mod } 6) \Rightarrow z$ is odd.

a) Negate the statement.

$\boxed{\exists z \in \mathbb{Z} \text{ s.t. } z^2 \equiv 7 (\text{mod } 6) \wedge z \text{ is even}}$

b) Write the assumptions, translated to algebraic equations.

$\boxed{z^2 - 7 = 6k \quad \text{and} \quad z = 2m}$

c) We will use the assumptions to show the falsehood $2|7$, which is translated $7 = 2w$ for some integer w. Show the proof steps, from assumptions to $2|7$.

$$z^2 - 7 = 6k$$

$$\Rightarrow (2m)^2 - 7 = 6k$$

$$\Rightarrow 4m^2 - 6k = 7$$

$$\Rightarrow \boxed{2(2m^2 - 3k) = 7} \quad \square$$

5. Use a direct proof to prove: $\forall z \in \mathbb{Z}$, $z \mod 3 = 2 \Rightarrow 9|(3z^2 + 6)$.

a) Write the assumption, translated to an algebraic equation.

$\boxed{z = 3k + 2}$

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

$\boxed{3z^2 + 6 = 9m}$

c) Proof steps:

$$3z^2 + 6 = 3(3k+2)^2 + 6$$
$$= 3(9k^2 + 12k + 4) + 6$$
$$= 27k^2 + 36k + 12 + 6$$
$$= \boxed{9(3k^2 + 4k + 2)} \quad \square$$

6. Use induction to prove: $\forall n \in \mathbb{Z}$, if $n \geq 4$ then $3|(2^{2n-5} + 1)$.

a) Show the base case.

$2^{2(4)-5} + 1 = 2^3 + 1 = 9 = \boxed{3(3)}$

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

$\boxed{2^{2k-5} + 1 = 3m}$

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

$\boxed{2^{2(k+1)-5} + 1 = 3p}$

d) Do the proof steps.

$$2^{2(k+1)-5} + 1 = 2^{2k+2-5} + 1$$
$$= 2^{2k-5} 2^2 + 1$$
$$= 2^{2k-5}(3+1) + 1$$
$$= 3(2^{2k-5}) + 2^{2k-5} + 1$$
$$= 3(2^{2k-5}) + 3m$$
$$= \boxed{3(2^{2k-5} + m)} = 3(4m-1) \quad \square$$

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

7. Consider the sequence $a_n = (n^2 + 10) \mod 12$; starting at $n = 1$. Use it to encrypt the word SAT. Your answer will be the new word.

n	*letter*	std. num.	find a_n		encrypt	letter
1	S	19	11 mod 12 =	11	19+11 = 30 mod 26 = 4	D
2	A	1	14 mod 12 =	2	(1+2) mod 26 = 3	C
3	T	20	19 mod 12 =	7	(20+7) mod 26 = 1	A

8. Consider the one-time-pad sequence $a_n = (2, 8, 11)$; starting at $n = 1$. It has been used to encrypt a message, and the encrypted message is DDF. Use the same sequence to decrypt and find the original word.

n	*letter*	std. num.	a_n	decrypt	letter
1	D	4	2	(4-2) mod 26 = 2	B
2	D	4	8	(4-8) mod 26 = 22	V
3	F	6	11	(6-11) mod 26 = 21	U

9. Consider the BBS (Blum Blum Shub) sequence $a_n = (a_{n-1})^2 \mod pq$; with $a_0 = 2$ and with $p = 5, q = 5$. Starting at $n = 1$, use this sequence to encrypt the binary number 1010. Your answer will be the new binary number. You may use either method from class.

n	*bit*	find a_n		encrypt	bit
1	1	4 mod 25 =	4	1+4 = 5 mod 2	1
2	0	16 mod 25 =	16	0+16 = 16 mod 2	0
3	1	256 mod 25 =	6	1+6 = 7 mod 2	1
4	0	36 mod 25 =	11	0+11 = 11 mod 2	1

10. From 7 library books, how many subsets of exactly 3 books are there? Answer as a whole number.

$$\boxed{\binom{7}{3}} = \frac{7\cdot 6\cdot 5}{3\cdot 2\cdot 1} = \boxed{35}$$

11. For 4 books and 9 shelves of a bookcase, find the number of ways to distribute the books on the shelves (just in piles, not in order.)

$$\boxed{9^4} = 6561$$

12. For 9 books on 4 shelves of a bookcase, find the number of ways to place the books on the shelves in ordered rows.

$$\binom{9+4-1}{4-1}9! = \boxed{\binom{12}{3}9!} = 79{,}833{,}600$$

13. For 8 books and 6 shelves of a bookcase, find the number of plans for shelving, where at least 3 books are planned for the top shelf (a plan only tells how many books on each shelf.)

OR $\boxed{\binom{13}{5} - \binom{12}{4} - \binom{11}{4} - \binom{10}{4}}$

$$\binom{(8-3)+6-1}{6-1} = \boxed{\binom{10}{5}} = 252$$

14. For 4 books and 9 shelves of a bookcase, find the number of ways to distribute the books on the shelves, where the bottom shelf has at most one book (just in piles, not in order.)

OR $\boxed{9^4 - \binom{4}{2}8^2 - \binom{4}{3}8^1 - 1}$

$$\boxed{8^4 + 4(8^3)} = 6144$$

15. For 7 books and 9 shelves of a bookcase, find the number of ways to place the books on the shelves in ordered rows, where the bottom shelf has no more than 2 books.

$$7!\left(\binom{7+9-1}{9-1} - \binom{(7-3)+9-1}{9-1}\right) = \boxed{\left(\binom{15}{8} - \binom{12}{8}\right)7!}$$

OR

$$= 5940(7!)$$
$$= 29{,}937{,}600$$

$$7!\left(\binom{7+8-1}{8-1} + \binom{(7-1)+8-1}{8-1} + \binom{(7-2)+8-1}{8-1}\right)$$
$$= \boxed{\left(\binom{14}{7} + \binom{13}{7} + \binom{12}{7}\right)7!}$$

1. Given the original statement of implication: $((x < 2y) \wedge (x \geq 5)) \Rightarrow ((y > 8) \vee (3x \text{ is even}))$.

- Find the contrapositive of the original; write it without "not" and without "∼."

(2) $(y \leq 8 \wedge 3x \text{ odd}) \Rightarrow (x \geq 2y \vee x < 5)$

- Find the negation of the original; write it without "not" and without "∼."

(3) $(x < 2y \wedge x \geq 5) \wedge (y \leq 8 \wedge 3x \text{ odd})$

2. Given the statement:

(3) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{N}$ s.t. $(yx \geq y + 7) \Rightarrow ((x \text{ is even }) \wedge (y + x \text{ is odd }))$.

- Find its negation; write it without "not" and without "∼."

$\exists x \in \mathbb{Z}$ s.t. $\forall y \in \mathbb{N}, (yx \geq y + 7) \wedge (x \text{ is odd} \vee y + x \text{ is even})$

3. Given the original statement "If you have salt then you have sodium." Answer the following without "not" and without "∼.'

- Write the original statement using the word sufficient.

(1) Having salt is sufficient for having sodium.

- Write the converse of the original using the words "only if".

(1) You have sodium only if you have salt.

- Write the contrapositive of the original using the word necessary.

(1) Not having salt is necessary for not having sodium.

(OR) Having zero salt is necesrary for having zero sodium.

4 . Translate the following numbers.

- binary: 1101011 (6) (11) hexidecimal: 6B ... —
- binary: 1111010 7 10 hexidecimal: 7A
- hexidecimal: FA3 binary: 1111 1010 0011
- binary: 1010 decimal: 10

5. Suppose that $P = F$ (false) and $Q = T$ (true). Find whether each of these statements is true (T) or false (F). Put a box around each final answer of T or F.

- $Q \wedge \sim (P \Rightarrow Q)$. $\boxed{F}$

  T F T

  T

  F

  F

- $((\sim P) \wedge Q) \Longleftrightarrow ((\sim P) \vee \sim Q)$. $\boxed{T}$

  T T T

  T T

  T

- $(\sim (P \vee Q)) \Rightarrow P$. $\boxed{T}$

  T F

  T

  F

  T

- $(P \Longleftrightarrow (\sim Q)) \Rightarrow ((\sim P) \Rightarrow P)$. $\boxed{F}$

  F F T F

  T F

  F

6. For $S = \{1, -3, -4, -12\}$, find an example making the following true:

$$\exists x \in S \ s.t.\ ((x \mid 7) \vee (|x| > 3)) \Rightarrow ((x \text{ is odd }) \wedge (x \leq -1))$$

$1|7 \vee 1>3 \Rightarrow 1 \text{ odd} \wedge 1 \leq -1$ F

T F T F

T F

$\boxed{x = -3}$

$-3|7 \vee 3>3 \Rightarrow -3 \text{ odd} \wedge -3 \leq -1$ T

F F T T

F T

$-4|7 \vee 4>3 \Rightarrow -4 \text{ odd} \wedge -4 \leq -1$ F

F T F T

T F

$-12|7 \vee 12>3 \Rightarrow -12 \text{ odd} \wedge -12 \leq -1$ F

T F

7. Given the inputs of each circuit, fill in the outputs.