Answers 4

Problem 1

00 01 10 } $S = 1$
01 00
10 11
11

$n = 2,\ (2^n - 2)/n = (4 - 2)/2 = 2/2 = 1 = S$

Problem 2

000000	100000	000001 000010 000100 001000 010000 100000	} $S_6 = 9$
000001	100001	000011 000110 001100 011000 110000 100001	
000010	100010	000101 001010 010100 101000 010001 100010	
000011	100011	000111 001110 011100 111000 110001 100011	
000100	100100	001011 010110 101100 011001 110010 100101	
000101	100101	001101 011010 110100 101001 010011 100110	
000110	100110	001111 011110 111100 111001 110011 100111	
000111	100111	010111 101110 011101 111010 110101 101011	
001000	101000	011111 111110 111101 111011 110111 101111	
001001	101001	001001 010010 100100	} $S_3 = 2$
001010	101010	011011 110110 101101	
001011	101011	010101 101010	} $S_2 = 1$
001100	101100	000000	
001101	101101	111111	
001110	101110		
001111	101111		
010000	110000		
010001	110001		
010010	110010		
010011	110011		
010100	110100		
010101	110101		
010110	110110		
010111	110111		
011000	111000		
011001	111001		
011010	111010		
011011	111011		
011100	111100		
011101	111101		
011110	111110		
011111	111111		

$6 \times S_6 + 3 \times S_3 + 2 \times S_2 + 2 = 2^n = 2^6 = 64$
$S_6 = (2^n - 3 \times S_3 - 2 \times S_2 - 2)/6 = (64 - 3 \times 2 - 2 \times 1 - 2)/6 = (64 - 6 - 2 - 2)/6 = 54/6 = 9$
The total sets are $S = S_6 + S_3 + S_2 = 9 + 2 + 1 = 12$

If $n = p \times q$ where p and q are prime, then $S_n = (2^n - p \times S_p - q \times S_q - 2)/n$,
where $S_p = (2^p - 2)/p$ and $S_q = (2^q - 2)/q$,
and $S = S_n + S_p + S_q = (2^n - p \times S_p - q \times S_q - 2)/n + (2^p - 2)/p + (2^q - 2)/q$

Problem 3
For $a = 10$ and $p = 5$, $(a^p - a)/p = (100{,}000 - 10)/5 = 99{,}950/5 = 19{,}990$.
For $a = 15$ and $p = 5$, $(a^p - a)/p = (759{,}375 - 15)/5 = 759{,}360/5 = 151{,}872$.
For $a = 15$ and $p = 3$, $(a^p - a)/p = (759{,}375 - 15)/5 = 759{,}360/3 = 253{,}120$.
For $a = 21$ and $p = 7$, $(a^p - a)/p = (1{,}801{,}088{,}541 - 21)/7 = 1{,}801{,}088{,}520/7 = 257{,}298{,}360$.

Problem 4
Circular Code Theorem: $a^p - a$ is divisible by p. But $a^p - a = a(a^{p-1} - 1)$. Then if a is not divisible by p, then the other factor $a^{p-1} - 1$ must be divisible by p, which is Fermat's Little Theorem. So the two theorems are just two ways of saying the same thing. So we might as well say that Fermat's Little Theorem is that $a^p - a$ is divisible by p, or $(a^p - a) \bmod p = 0$.

Problem 5
Saying $(a^p - a)$ by p has a remainder of 0 is the same as saying $a^p - a = c \times p$, where c is some integer. Adding a to both sides, we have $a^p = c \times p + a$. Then p goes into a^p c times with a remainder of a.
For $a = 2$ and $p = 7$, $a^p = 128 = 18 \times 7 + 2$. So 7 goes into 128 18 times with a remainder of $2 = a$.
For $a = 3$ and $p = 5$, $a^p = 243 = 48 \times 5 + 3$. So 5 goes into 243 48 times with a remainder of $3 = a$.

Problem 6
$a = 3,\ p = 2,\ a^p = 9$

00	01 10	$S = 3$
01	02 20	
02	12 21	
10	00	$a = 3$
11	11	
12	22	
20		
21		
22		

$S = (a^p - a)/p = (9 - 3)/2 = 6/2 = 3$.