BONUS HOMEWORK

WRITE CODE THAT CALCULATES MODULAR MULTIPLICATIVE INVERSE.

1.) To find the modular inverse we can use the extended encleidian algorithm. This will result with Bezut coefficients s and T where T will be the inverse. The algorithm will find the quotient, remainder and coefficients all together step by step.

2.) I will use 4 equations

1. $q_i = a \div b$
2. $r_{i+1} = r_{i-1} - q_i \cdot r_i$
3. $s_{i+1} = s_{i-1} - q_i \cdot s_i$
4. $t_{i+1} = t_{i-1} - q_i \cdot t_i$

$r_0 = a$, $r_1 = b$, $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, $t_1 = 1$

3) Example calculation

$n = 8 \quad a = 3$

INDEX	Quotient	Remainder	Si	Ti
0		8	1	0
1		3	0	1
2	$8 \div 3 = 2$	$8 - 2 \cdot 3 = 2$	$1 - 2 \cdot 0 = 1$	$0 - 2 \cdot 1 = -2$
3	$3 \div 2 = 1$	$3 - 1 \cdot 2 = 1$	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-2) = 3$
4	$2 \div 1 = 2$	$2 - 2 \cdot 1 = 0$	$1 - 2 \cdot (-1) = 3$	$-2 - 2 \cdot 3 = -8$

The coefficients are on the row just above where the remainder is equal to 0.

$$n \cdot s + a \cdot t = 1$$

$$8 \cdot (-1) + 3 \cdot 3 = 1$$

s t

4) When the integer is 3 with modulo 8 then the multiplicative inverse is 3. Because from the above calculation $t_3 = 3$.