CSE107 Hw 4

#1

1. $\mathbb{Z}_{20}^* = \{1, 3, 5, 7, 9, 11, 13, 17, 19\}$

$|\mathbb{Z}_{20}^*| = 9$

2. $|\mathbb{Z}_{2039}^*| = 2038$

3. $3^{0x\text{E5E107}} \bmod 967 = 3^{12968199} \bmod 967$

$|\mathbb{Z}_{961}^*| = 966$

$3^{(12968199 \bmod 966)} = 3^{615} = ((3^3)^5)^{41}$

615

5 123

41 3

$= ((27)^5)^{41} = ((27 \cdot 27)^2 \cdot 27)^{41}$

$= (558 \cdot 27)^{41}$

$(561)^{41}$

$= (561 \cdot 561)^{20} \cdot 561$

(mod) $= (446)^{20} \cdot 561$

$= (446 \cdot 446)^{10} \cdot 561$

(mod) $= (681)^{10} \cdot 561$

$= (681 \cdot 681)^5 \cdot 561$

(mod) $= (568)^5 \cdot 561 = (568 \cdot 568)^2 \cdot 568 \cdot 561$

(mod) $= (613)^2 \cdot 505$

(mod) $= \boxed{232} \pmod{967}$

4.

Ext-GCD(428, 2022)

$(r_0, u_0, v_0) \leftarrow (2022, 0, 1)$

$(r_1, u_1, v_1) \leftarrow (428, 1, 0)$

while $r_1 \neq 0$ $\quad r_0 \quad r_1 \quad q, r_2$

INT_DIV(2022, 428) = (4, 310)

$u_2 = -4$; $v_2 = 1$

(428, 1, 0) # r_0, u_0, v_0

(310, -4, 1) # r_1, u_1, v_1 $\quad q \quad r_2$

INT_DIV(428, 310) = (1, 118)

$u_2 = 1 - (1)(-4) = 5$; $v_2 = 0 - 1(1) = -1$

(310, -4, 1) # r_0, u_0, v_0

(118, 5, -1) # r_1, u_1, v_1

INT_DIV(310, 118) = (2, 74)

$u_2 = -4 - 2(5) = -14$; $v_2 = 1 - (2)(-1) = 3$

(118, 5, -1) # r_0, u_0, v_0

(74, -14, 3)

INT_DIV(118, 74) = (1, 44)

$u_2 = 5 - (-14) = 19$, $v_2 = -1 - 3 = -4$

(74, -14, 3)

(44, 19, -4)

INT_DIV(74, 44) = (1, 30)

$u_2 = -14 - 19 = -33$; $v_2 = 3 - (-4) = 7$

(44, 19, -4); (30, -33, 7)

INT_DIV(44, 30) = (1, 14)

$u_2 = 19 + 33 = 52$; $v_2 = -4 - 7 = -11$

(30, -33, 7); (14, 52, -11)

INT_DIV(30, 14) = (2, 2)

$u_2 = -33 - 52(2) = -137$; $v_2 = 7 + 11(2) = 29$

(14, 52, -11); (2, -85, 18)

INT_DIV(14, 2) = (7, 0)

$\boxed{(2, -137, 29)} = -137(428) + 29(2022) = 2$

Ext_gcd(428, 2022) = (2, -137, 29)

2 is the gcd of 428 & 2022

5. $43^{2022} \bmod 2039 = \boxed{1757}$

11111001110	$y = 43$
11	$y = (43)^2 \cdot 43 = (43)^3$
111	$y = 43^7$
1111	$y = (43)^{15}$
11111	$y = (43)^{30}$
111111	$y = (43 \cdot 43 \cdot 43)^{21} \equiv (2025)^{21}$
1111110	$y = (2025 \cdot 2025)^{21} \equiv (196)^{21}$
11111100	$y = (196 \cdot 196)^{21} = (1714)^{21}$
11111001	$y = (1714 \cdot 1714)^{21} \cdot 43 = (1636)^{21} \cdot 43$
111111011	$y = ((1636)^{21} \cdot 43)^2 \cdot 43 = (1636 \cdot 1636)^{21} \cdot 43^3$
	$= (1328)^{21} \cdot 2025$
1111110010	$y = (1326 \cdot 1328)^{21} \cdot 2025^2 = (1888)^{21} \cdot 196$

$((1888)^3)^7 \cdot 196 = (920)^7 \cdot 196 = (920 \cdot 920)^3 \cdot 920 \cdot 196$

$= (215)^3 \cdot 888 = 299 \cdot 888 \bmod 2039 = \boxed{1757}$