6. Use the EXTENDED EUCLIDEAN ALGORITHM to compute the following multiplicative inverses:

(USE PEN AND PAPER)

- $17^{-1} \mod 101$
- $357^{-1} \mod 1234$
- $3125^{-1} \mod 9987$

[def. $ax + by = \gcd(a, b)$] Extended Euclidean Alg.

1) $17^{-1} \mod 101$

$\gcd(101, 17)$ $a = 101$, $b = 17$

$101 \mid 17$ $\quad 16 \mid 5$ $\Rightarrow 101 \bmod 17 = 16$

$b = a \bmod b = 101 \bmod 17$

$b = 16$, $a = 17$

$17 \mid 16$ $\quad 1 \mid 1$ $\Rightarrow 17 \bmod 16 = 1$

$b = 1$, $a = 16$

$16 \mid 1$ $\quad 0 \mid 16$ $\Rightarrow$ $16 \bmod 1 = 0$ $\Rightarrow b = 0$, $a = 1$

* Como gcd es 1 $\Rightarrow$ Existe mutiplicative inverse.

$101 \mid 17$ $\quad 16 \mid 5$

$a = 5b + 16$

$16 = a - 5b$

$a_1 = 17$, $b_1 = 16$

$17 \mid 16$ $\quad 1 \mid 1$

$a_1 = b_1 + 1$

$1 = a_1 - b_1 \rightarrow 1 = b - (a - 5b)$

$1 = -a + 6b$

$a_2 = 16$, $b_2 = 1$

$16 \mid 1$ $\quad 0 \mid 16$

$16 = 16 b_2 + 0$

$16 = 16(-a + 6b)$

$16 = -16a + 96b$

$1 = -a + 6b$

$17^{-1} \equiv 6 \pmod{101}$

2) $357^{-1} \bmod 1234$

$a = 1234 \quad b = 357$

1234	357
163	3

$a = 3b + 163$

$163 = a - 3b$

$a_1 = 357 \quad b_1 = 163$

357	163
31	2

$a_1 = 2b_1 + 31$

$31 = a_1 - 2b_1$

$31 = b - 2(a - 3b)$

$31 = -2a + 7b$

$a_2 = 163, \; b_2 = 31$

163	31
8	5

$a_2 = 5b_2 + 8$

$8 = a_2 - 5b_2$

$8 = (a - 3b) - 5(-2a + 7b)$

$8 = 11a - 38b$

$a_3 = 31, \; b_3 = 8$

31	8
7	3

$a_3 = 3b_3 + 7$

$7 = a_3 - 3b_3$

$7 = -2a + 7b - 3(11a - 38b)$

$7 = -35a + 121b$

$a_4 = 8, \; b_4 = 7$

8	7
1	1

$a_4 = b_4 + 1$

$1 = a_4 - b_4$

$1 = 11a - 38b - (-35a + 121b)$

$1 = 46a - 159b$

$a_5 = 7, \; b_5 = 1$

7	1
0	7

$a_5 = 7b_5 + 0$

$7 = 7(46a - 159b)$

$1 = 46a - 159b$

$357^{-1} \equiv -159 \pmod{1234}$

$-159 + 1234 = 1075$

$\Rightarrow 357^{-1} \equiv 1075 \pmod{1234}$

3) $3125^{-1} \bmod 9987$

$9987 \mid 3125$

$613 \quad 3$

$a = 3b + 613$

$613 = a - 3b$

$a_1 = 3125, \; b_1 = 613$

$3125 \mid 613$

$470 \quad 5$

$a_1 = 5b_1 + 470$

$470 = a_1 - 5b_1$

$470 = b - 5(a - 3b) = -5a + 16b$

$a_2 = 613 \quad b_2 = 470$

$613 \mid 470$

$143 \quad 1$

$143 = a_2 - b_2$

$143 = a - 3b - (-5a + 16b)$

$143 = 6a - 19b$

$a_3 = 470, \; b_3 = 143$

$470 \mid 143$

$41 \quad 3$

$41 = a_3 - 3b_3$

$41 = -5a + 16b - 3(6a - 19b)$

$41 = -23a + 73b$

$a_4 = 143, \; b_4 = 41$

$143 \mid 41$

$20 \quad 3$

$20 = a_4 - 3b_4$

$20 = 6a - 19b - 3(-23a + 73b)$

$20 = 75a - 238b$

$a_5 = 41, \; b_5 = 20$

$41 \mid 20$

$1 \quad 2$

$1 = a_5 - 2b_5$

$1 = -23a + 73b - 2(75a - 238b)$

$1 = -173a + 549b$

$a_6 = 20, \; b_6 = 1$

$20 \mid 1$

$0 \quad 20$

$a_6 = 20b_6 + 0$

$1 = -173a + 549b$

$3125^{-1} \equiv 549 \pmod{9987}$