Homework Assignment #5
Student: Shuo Yang

1. Create a subtraction table for Z_7, $(x-y) \mod 7$, similar to slide 6.

   Table is shown below, the row index represents x and the column index represents y.

$-$	0	1	2	3	4	5	6
0	0	6	5	4	3	2	1
1	1	0	6	5	4	3	2
2	2	1	0	6	5	4	3
3	3	2	1	0	6	5	4
4	4	3	2	1	0	6	5
5	5	4	3	2	1	0	6
6	6	5	4	3	2	1	0

2. Compute $GCD(500, 793)$ using method given in slide 10. Show your work.

   Let $a = 793$ and $b = 500$, with Euler's GCD algorithm, we have the following recursive steps:

   iter-1: $a = 793$, $b = 500$, $q = \lfloor 793/500 \rfloor = 1$
   iter-2: $a = 500$, $b = 793 \mod 500 = 293$, $q = \lfloor 500/293 \rfloor = 1$
   iter-3: $a = 293$, $b = 500 \mod 293 = 207$, $q = \lfloor 293/207 \rfloor = 1$
   iter-4: $a = 207$, $b = 293 \mod 207 = 86$, $q = \lfloor 207/86 \rfloor = 2$
   iter-5: $a = 86$, $b = 207 \mod 86 = 35$, $q = \lfloor 86/35 \rfloor = 2$
   iter-6: $a = 35$, $b = 86 \mod 35 = 16$, $q = \lfloor 35/16 \rfloor = 2$
   iter-7: $a = 16$, $b = 35 \mod 16 = 3$, $q = \lfloor 16/3 \rfloor = 5$
   iter-8: $a = 3$, $b = 16 \mod 3 = 1$, $q = \lfloor 3/1 \rfloor = 3$
   iter-9: $a = 1$, $b = 3 \mod 1 = 0$, return $(1, 1, 0)$

   Now work backwards to reach to the final answer:

   iter-9: $a = 1$, $b = 3 \mod 1 = 0$, return $(1, 1, 0)$
   iter-8: $a = 3$, $b = 16 \mod 3 = 1$, $q = \lfloor 3/1 \rfloor = 3$,
   $(d, k, l) = (1, 1, 0)$, $d = 1, l = 0, k - lq = 1$, return (1,0,1)
   iter-7: $a = 16$, $b = 35 \mod 16 = 3$, $q = \lfloor 16/3 \rfloor = 5$,
   $(d, k, l) = (1, 0, 1)$, $d = 1, l = 1, k - lq = 0 - 1 * 5 = -5$, return (1,1,-5)
   iter-6: $a = 35$, $b = 86 \mod 35 = 16$, $q = \lfloor 35/16 \rfloor = 2$,
   $(d, k, l) = (1, 1, -5)$, $d = 1, l = -5, k - lq = 1 - (-5) * 2 = 11$, return (1,-5, 11)
   iter-5: $a = 86$, $b = 207 \mod 86 = 35$, $q = \lfloor 86/35 \rfloor = 2$,
   $(d, k, l) = (1, -5, 11)$, $d = 1, l = 11, k - lq = (-5) - 11 * 2 = -27$, return (1,11,-27)
   iter-4: $a = 207$, $b = 293 \mod 207 = 86$, $q = \lfloor 207/86 \rfloor = 2$,
   $(d, k, l) = (1, 11, -27)$, $d = 1, l = -27, k - lq = 11 - (-27) * 2 = 65$, return (1,-27,65)
   iter-3: $a = 293$, $b = 500 \mod 293 = 207$, $q = \lfloor 293/207 \rfloor = 1$,
   $(d, k, l) = (1, -27, 65)$, $d = 1, l = 65, k - lq = -27 - 65 * 1 = -92$, return (1,65,-92)
   iter-2: $a = 500$, $b = 793 \mod 500 = 293$,$q = \lfloor 500/293 \rfloor = 1$,
   $(d, k, l) = (1, 65, -92)$, $d = 1, l = -92, k - lq = 65 - (-92) * 1 = 157$, return (1,-92,157)
   iter-1: $a = 793$, $b = 500$, $q = \lfloor 793/500 \rfloor = 1$
   $(d, k, l) = (1, -92, 157)$, $d = 1, l = 157, k - lq = -92 - 157 * 1 = -249$, return (1,157,-249)

   Therefore $GCD(500, 793) = (1, -249, 157)$.

3. Compute $GCD(720, 999)$ using method given in slide 12. Show your work.

   $999 = 720 * 1 + 279$
   $720 = 279 * 2 + 162$
   $279 = 162 * 1 + 117$
   $162 = 117 * 1 + 45$
   $117 = 45 * 2 + 27$
   $45 = 27 * 1 + 18$
   $27 = 18 * 1 + \mathbf{9}$
   $18 = 9 * 2 + 0$

   Therefore, $GCD(720, 999) = 9$.

4. Compute i and j such that $GCD(500, 793) = i * 500 + j * 793$. Show your work.

   1: 793 = 500 * 1 + 293
   2: 500 = 293 * 1 + 207
   3: 293 = 207 * 1 + 86
   4: 207 = 86 * 2 + 35
   5: 86 = 35 * 2 + 16
   6: 35 = 16 * 2 + 3
   7: 16 = 3 * 5 + $\underline{\mathbf{1}}$
   8: 3 = 1 * 3 + 0

   So $GCD(500, 793) = 1$.

   Transform the equtions 1 to 7 as:

   1: 793 - 500 * 1 = 293
   2: 500 - 293 * 1 = 207
   3: 293 - 207 * 1 = 86
   4: 207 - 86 * 2 = 35
   5: 86 - 35 * 2 = 16
   6: 35 - 16 * 2 = 3
   7: 16 - 3 * 5 = $\underline{\mathbf{1}}$

   Now work from 2 to 7:

   2: 500 - 293 * 1 = 207
   substitute 293 with (793 - 500 * 1):
   500 - (793 - 500 * 1) * 1 = 207
   793 * -1 + 500 * 2 = 207

   3: 293 - 207 * 1 = 86
   substitute 207 with (793 * -1 + 500 * 2), and 293 with (793 - 500 * 1):
   (793 - 500 * 1) - (793 * -1 + 500 * 2) * 1 = 86
   793 * 2 + 500 * (-3) = 86

   4: 207 - 86 * 2 = 35
   substitute 207 with (793 * -1 + 500 * 2), and 86 with (793 * 2 + 500 * (-3)):
   (793 * -1 + 500 * 2) - (793 * 2 + 500 * (-3)) * 2 = 35

793 ∗ -5 + 500 ∗ 8 = 35

5: 86 - 35 ∗ 2 = 16
substitute 86 with (793 ∗ 2 + 500 ∗ (-3)): and 35 with (793 ∗ -5 + 500 ∗ 8)
(793 ∗ 2 + 500 ∗ (-3)) - (793 ∗ -5 + 500 ∗ 8) ∗ 2 = 16
793 ∗ 12 + 500 ∗ -19 = 16

6: 35 - 16 ∗ 2 = 3
substitute 35 with (793 ∗ -5 + 500 ∗ 8) and 16 with (793 ∗ 12 + 500 ∗ -19):
(793 ∗ -5 + 500 ∗ 8) - (793 ∗ 12 + 500 ∗ -19) ∗ 2 = 3
793 ∗ -29 + 500 ∗ 46 = 3

7: 16 - 3 ∗ 5 = **1**
substitute 16 with (793 ∗ 12 + 500 ∗ -19) and 3 with (793 ∗ -29 + 500 ∗ 46):
(793 ∗ 12 + 500 ∗ -19) - (793 ∗ -29 + 500 ∗ 46) ∗ 5 = **1**
793 ∗ 157 + 500 ∗ (-249) = **1**

Therefore $GCD(500, 793) = 1 = 500 * (-249) + 793 * 157$, $i = -249, j = 157$.

5. Compute i and j such that $GCD(720, 999) = i * 720 + j * 999$. Show your work.

1. 999 = 720 ∗ 1 + 279
2. 720 = 279 ∗ 2 + 162
3. 279 = 162 ∗ 1 + 117
4. 162 = 117 ∗ 1 + 45
5. 117 = 45 ∗ 2 + 27
6. 45 = 27 ∗ 1 + 18
7. 27 = 18 ∗ 1 + **9**
8. 18 = 9 ∗ 2 + 0

So $GCD(720, 999) = 9$. Transform the equtions 1 to 7 as:

1. 999 - 720 ∗ 1 = 279
2. 720 - 279 ∗ 2 = 162
3. 279 - 162 ∗ 1 = 117
4. 162 - 117 ∗ 1 = 45
5. 117 - 45 ∗ 2 = 27
6. 45 - 27 ∗ 1 = 18
7. 27 - 18 ∗ 1 = **9**

Now work from 2 to 7:

2. 720 - 279 ∗ 2 = 162
Substitute 279 with (999 - 720 ∗ 1):
720 - (999 - 720 ∗ 1) ∗ 2 = 162
720 ∗ 3 - 999 ∗ 2 = 162

3. 279 - 162 ∗ 1 = 117
Substitute 279 with (999 - 720 ∗ 1) and 162 with (720 ∗ 3 - 999 ∗ 2):

(999 - 720 $*$ 1) - (720 $*$ 3 - 999$*$ 2) $*$ 1 = 117
720 $*$ -4 + 999 $*$ 3 = 117

4. 162 - 117 $*$ 1 = 45
Substitute 162 with (720 $*$ 3 - 999 $*$ 2) and 117 with (720 $*$ -4 + 999 $*$ 3):
(720 $*$ 3 - 999 $*$ 2) - (720 $*$ -4 + 999 $*$ 3) $*$ 1 = 45
720 $*$ 7 - 999 $*$ 5 = 45

5. 117 - 45 $*$ 2 = 27
Substitute 117 with (720 $*$ -4 + 999 $*$ 3) and 45 with (720 $*$ 7 - 999 $*$ 5):
(720 $*$ -4 + 999 $*$ 3) - (720 $*$ 7 - 999 $*$ 5) $*$ 2 = 27
720 $*$ -18 + 999 $*$ 13 = 27

6. 45 - 27 $*$ 1 = 18
Substitute 45 with (720 $*$ 7 - 999 $*$ 5) and 27 with (720 $*$ -18 + 999 $*$ 13):
(720 $*$ 7 - 999 $*$ 5) - (720 $*$ -18 + 999 $*$ 13) $*$ 1 = 18
720 $*$ 25 - 999 $*$ 18 = 18

7. 27 - 18 $*$ 1 = $\underline{\mathbf{9}}$
Substitute 27 with (720 $*$ -18 + 999 $*$ 13) and 18 with (720 $*$ 25 - 999 $*$ 18):
(720 $*$ -18 + 999 $*$ 13) - (720 $*$ 25 - 999 $*$ 18) $*$ 1 = $\underline{\mathbf{9}}$
720 $*$ (-43) + 999 $*$ 31 = $\underline{\mathbf{9}}$

Therefore $GCD(720, 999) = 9 = 720 * (-43) + 999 * 31$, $i = -43, j = 31$.

6. Create a modular multiplication table for Z_{13}, xy mod 13 and highlight inverses.

Inverses are highlighted as $\underline{\mathbf{1}}$.

$\times$	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$\underline{\mathbf{1}}$	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	$\underline{\mathbf{1}}$	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	$\underline{\mathbf{1}}$	4	7	10
4	0	4	8	12	3	7	11	2	6	10	$\underline{\mathbf{1}}$	5	9
5	0	5	10	2	7	12	4	9	$\underline{\mathbf{1}}$	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	$\underline{\mathbf{1}}$	7
7	0	7	$\underline{\mathbf{1}}$	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	$\underline{\mathbf{1}}$	9	4	12	7	2	10	5
9	0	9	5	$\underline{\mathbf{1}}$	10	6	2	11	7	3	12	8	4
10	0	10	7	4	$\underline{\mathbf{1}}$	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	$\underline{\mathbf{1}}$	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	$\underline{\mathbf{1}}$

7. Create a modular exponentiation table for Z_{11}, x^y mod 11.

	y	y	y	y	y	y	y	y	y	y
exp	1	2	3	4	5	6	7	8	9	10
1^y	1	1	1	1	1	1	1	1	1	1
2^y	2	4	8	5	10	9	7	3	6	1
3^y	3	9	5	4	1	3	9	5	4	1
4^y	4	5	9	3	1	4	5	9	3	1
5^y	5	3	4	9	1	5	3	4	9	1
6^y	6	3	7	9	10	5	8	4	2	1
7^y	7	5	2	3	10	4	6	9	8	1
8^y	8	9	6	4	10	3	2	5	7	1
9^y	9	4	3	5	1	9	4	3	5	1
10^y	10	1	10	1	10	1	10	1	10	1

8. How would you compute $x^{98} \bmod p$ using repeated squaring. Show your work.

   First, express x^{98} as:

   $x^{98} = x^{64+32+2} = x^{64} * x^{32} * x^2$

   Next, compute x^{64}, x^{32}, x^2 using repeated squaring:

   $x^2 = x * x$
   $x^4 = x^2 * x^2$
   $x^8 = x^4 * x^4$
   $x^{16} = x^8 * x^8$
   $x^{32} = x^{16} * x^{16}$
   $x^{64} = x^{32} * x^{32}$

   Therefore, $x^{98} \mod p = x^{64} * x^{32} * x^2 \mod p$