1.16. Write out the following tables for $\mathbb{Z}/m\mathbb{Z}$ and $(\mathbb{Z}/m\mathbb{Z})^*$, as we did in Figs. 1.4 and 1.5.

(a) Make addition and multiplication tables for $\mathbb{Z}/3\mathbb{Z}$.
(b) Make addition and multiplication tables for $\mathbb{Z}/6\mathbb{Z}$.

(a) $\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \ldots, m-1\}$

For $\mathbb{Z}/3\mathbb{Z}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(b) For $\mathbb{Z}/6\mathbb{Z}$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

•	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

1.17. Do the following modular computations. In each case, fill in the box with an integer between 0 and $m-1$, where m is the modulus.

(a) $347+513 \equiv \boxed{} \pmod{763}$.

(b) $3274+1238+7231+6437 \equiv \boxed{} \pmod{9254}$.

(c) $153 \cdot 287 \equiv \boxed{} \pmod{353}$.

(d) $357 \cdot 862 \cdot 193 \equiv \boxed{} \pmod{943}$.

(e) $5327 \cdot 6135 \cdot 7139 \cdot 2187 \cdot 5219 \cdot 1873 \equiv \boxed{} \pmod{8157}$.
(*Hint.* After each multiplication, reduce modulo 8157 before doing the next multiplication.)

(f) $137^2 \equiv \boxed{} \pmod{327}$.

(a) $347+513 = 860 \equiv 97 \pmod{763}$

(b) $3274+1238+7231+6437 = 18180$

$18180 \div 9254 = 1 \text{ r } 8926$

$18180 - 9254 = 8926$

$\equiv 8926 \pmod{9254}$

(c) $153 \cdot 287 = 43911$

$43911 \div 353 = 124 \text{ r } 139$

$43911 - 43772 = 139$

$\equiv 139 \pmod{353}$

(d) $357 \cdot 862 \cdot 193 = 59392662$

$59392662 \div 943 = 62982 \text{ r } 636$

$59392662 - 59392026 = 636$

$\equiv 636 \pmod{943}$

(e) $5327 \cdot 6135 = 32681145 \div 8157 = 4006 \cdot 8157$

$= 32676942$

$4203 \pmod{8157}$

$7139 \cdot 2187 = 15612993 \div 8157 = 1914 = 15612498$

$\equiv 495 \pmod{8157}$

$5219 \cdot 1873 = 9775187 / 8157 = 1198 = 9772086$

$\equiv 3101 \pmod{8157}$

$\rightarrow 4203 \cdot 495 = 2080485 \div 8157 = 255 = 2080035$

$\equiv 450 \pmod{8157}$

$\rightarrow 450 \cdot 3101 = 1395450 \div 8157 = 171 = 1394847$

$\equiv 603 \pmod{603}$

(f) $137^2 \pmod{327}$

$= 18769 \div 327 = 57 \rightarrow 18769 - 18639$

$\equiv 130 \pmod{327}$

1.18. Find all values of x between 0 and $m-1$ that are solutions of the following congruences. (*Hint.* If you can't figure out a clever way to find the solution(s), you can just substitute each value $x = 1$, $x = 2, \ldots$, $x = m-1$ and see which ones work.)

(a) $x + 17 \equiv 23 \pmod{37}$.

(b) $x + 42 \equiv 19 \pmod{51}$.

(c) $x^2 \equiv 3 \pmod{11}$.

(d) $x^2 \equiv 2 \pmod{13}$.

(a) $x + 17 \equiv 23 \pmod{37}$

$23 - 17 \equiv x$

$x \equiv 6 \pmod{37}$

(b) $x + 42 \equiv 19 \pmod{51}$

$x \equiv 19 - 42$

$\rightarrow x \equiv -23$ Since negative, mod $51 - 23 = 28$

$x \equiv 28 \pmod{51}$ $28 + 42 = \frac{70}{51} = 1$ $\begin{array}{r} 70 \\ -51 \\ \hline 19 \end{array}$ ✓

(c) $x^2 = 3 \pmod{11}$

$2^2 \equiv 4\ x$

$3^2 = 9\ x$

$4^2 = 16 = 5\ x$

$5^2 = 25 \equiv 3$ ✓

$x \equiv 5 \pmod{11}$

(d) $x^2 = 2 \pmod{13}$

None from above work,

$6^2 = 36 \mid 13 = 10\ x$, $7^2 = 10\ x$, $8^2 = 64 = 12\ x$

$9^2 = 3\ x$, $10^2 = 100 = 9\ x$, $11^2 = 4\ x$, $12^2 = 1\ x$,

$13^2 = 0\ x$,

No Solution Found

4. FIND INVERSE $100 \pmod{433}$. $\gcd(100, 433) = 1$

Theorem 13. Let $a \in \mathbb{Z}/m\mathbb{Z}$. If $u, v \in \mathbb{Z}$ such that

$$au + mv = 1, \text{ then } a^{-1} \equiv u \pmod{m}$$

$\gcd(100, 433) = 1$?

$433 = 4 \times 100 + 33$
$100 = 3 \times 33 + 1$ ← $\gcd(100, 433)$ ✓
$33 = 3 \times 1 + 0$

Extended Euc. ALG.

$33 = a - 4b$ $\quad 100 = 3(a - 4b) + (a - 3b)$
$1 = a - 3b$ $\quad 100 = 3a - 12b + a - 3b$
$100 = 4a - 15b$

$1 = 100 - 3(a - 4b)$
$1 = 100 - 3a + 12b$
$1 = 100 - 3(433) + 12(100)$
↳ $1 = 100(13) - (433)3$

$1 = au + mv$ then $a^{-1} \equiv u \pmod{m}$

$100^{-1} = 13 \pmod{433}$

5. Find $(\mathbb{Z}/16\mathbb{Z})^*$, the set of units modulo 16

Need $a \in \{0,1,2,3,\ldots,15\}$ such that $\gcd(a,16)=1$

$\gcd(1,16)=1$ ✓

$\gcd(2,16) \rightarrow 16 = 2\times 8 + 0 = 2$ ✗

$\gcd(3,16) \rightarrow 16 = 3\times 5 + 1 = 1$ ✓

$\gcd(4,16) \rightarrow 16 = 4\times 4 + 0 = 4$ ✗

$\gcd(5,16) \rightarrow 16 = 5\times 3 + 1 = 1$ ✓

$\gcd(6,16) \rightarrow 16 = 6\times 2 + 4 = 4$ ✗

$\gcd(7,16) \rightarrow 7 = 2\times 3 + 1 =$ ✓

$\gcd(8,16) = 16 = 8\times 2 = 8$ ✗

$\gcd(9,16) = 16 = 1\times 9 + 7 = 1$ ✓

$\gcd(10,16) = 16 = 10\times 1 + 6 = 10 = 6\times 1 + 4 = 2$ ✗

$\gcd(11,16) = 16 = 1\times 11 + 5 = 1$ ✓

$\gcd(12,16) = 16 = 1\times 12 + 4 = 12 = 4\times 3 + 0 = 4$ ✗

$\gcd(13,16) = 16 = 13\times 1 + 3 = 13 = 3\times 4 + 1$ ✓

$\gcd(14,16) = 16 = 14\times 1 + 2 = 14 = 2\times 7 + 0 = 2$ ✗

$\gcd(15,16) = 16 = 15\times 1 + 1$ ✓

$$(\mathbb{Z}/16\mathbb{Z})^* = \{1,3,5,7,9,11,13,15\}$$