A1. Calculate the following:

(a) $55 \bmod 13$

(b) $81 \bmod 13$

(c) $(55 \times 81) \bmod 13$

(d) $-4 \bmod 15$

Solution:

(a) $55 \bmod 13 = 3$

(b) $81 \bmod 13 = 3$

(c) We can reduce the factors individually and get

$$\begin{aligned} 55 \times 81 \bmod 13 &= ((55 \bmod 13) \times (81 \bmod 13)) \bmod 13 \\ &= 3 \times 3 \bmod 13 \\ &= 9. \end{aligned}$$

(d) The number $-4 \bmod 15$ is the same as the number $-4 + 15 \bmod 15$, which is 11.

A2. (a) Find three numbers x satisfying $x \equiv 19 \pmod{32}$

Solution: We can choose 19 plus any multiple of 32. Some of these numbers are

$$\ldots, -45, -13, 19, 51, 83, \ldots$$

(b) Find three numbers x satisfying both $x \equiv 0 \pmod{2}$ and $x \equiv 1 \pmod{13}$.

Solution: The condition $x \equiv 0 \pmod{2}$ just says that x is an even number. The condition $x \equiv 1 \pmod{13}$ says that x is one more than a multiple of 13. Some even numbers that are one more than multiples of 13 are

$$\begin{aligned} 13 + 1 &= 14 \\ 39 + 1 &= 40 \\ 65 + 1 &= 66. \end{aligned}$$

(c) Find three numbers x satisfying both $x \equiv 1 \pmod 3$ and $x \equiv 1 \pmod{10}$.
Solution: Some numbers that satisfy $x \equiv 1 \pmod 3$ are

$$-5, -2, 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, \ldots$$

Among these we spot two that satisfy $x \equiv 1 \pmod{10}$; they are 1 and 31. A third such number is 61.

A3. (a) Write down a complete multiplication table modulo 8. Index the rows and columns with the numbers 0 through 7, and in the cell at row x and column y, fill in $(x \times y) \bmod 8$.
Here's the table

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Solve the congruence $3x \equiv 7 \pmod 8$. Find a solution in the set $\{0, 1, 2, \ldots, 8\}$.
Solution: We multiply by the multiplicative inverse of 3. We get

$$\begin{aligned} 3 \times 3x &\equiv 3 \times 7 \pmod 8 \\ x &\equiv 21 \pmod 8 \end{aligned}$$

so that $x = 21 \bmod 8 = 5$.

(c) (Trickier) Are there any solutions (again in the set $\{0, 1, 2, \ldots, 7\}$) to the congruence $6x \equiv 20 \pmod 8$? How about $6x \equiv 21 \pmod 8$?
Solution: The congruence $6x \equiv 20 \pmod 8$ is equivalent to the congruence $6x \equiv 4 \pmod 8$, so we need only look along the 6 row in the table above. We find two solutions: $x = 2$ and $x = 6$.

The congruence $6x \equiv 21 \pmod 8$ is equivalent to the congruence $6x \equiv 5 \pmod 8$. From the table above, we see that there are no solutions to this congruence.

B1. (a) Which of the numbers in the set $\{0, 1, 2, \ldots, 21\}$ have multiplicative inverses modulo 22?

The numbers that have multiplicative inverses modulo 22 are those that are relatively prime to 22. They are 1, 3, 5, 7, 9, 13, 15, 17, 19, and 21.

(b) Find the multiplicative inverse of each number you identified in part B1a.

We find these more or less by trial and error. We observe that

$$\begin{aligned} 3 \times 15 &\equiv 1 \pmod{22} \\ 5 \times 9 &\equiv 1 \pmod{22} \\ 7 \times 19 &\equiv 1 \pmod{22} \\ 13 \times 17 &\equiv 1 \pmod{22} \\ 21 \times 21 &\equiv 1 \pmod{22} \end{aligned}$$

The multiplicative inverses are

x	1	3	5	7	9	13	15	17	19	21
x^{-1}	1	15	9	19	5	17	3	13	7	21

(c) Solve the congruences

i. $17x + 14 \equiv 2 \pmod{22}$

ii. $6x - 4 \equiv x + 10 \pmod{22}$

Solution:

i. We subtract 14 from each side to get

$$\begin{aligned} 17x &\equiv -12 \pmod{22} \\ &\equiv 10 \pmod{22}. \end{aligned}$$

We then multiply by the multiplicative inverse of 17 to get

$$\begin{aligned} 13 \times 17x &\equiv 13 \times 10 \pmod{22} \\ x &\equiv 130 \pmod{22} \\ x &\equiv 20 \pmod{22}. \end{aligned}$$

ii. We subtract x from each side and add 4 to each side to get

$$5x \equiv 14 \pmod{22}.$$

We then multiply by the multiplicative inverse of 5 to get

$$\begin{aligned} 9 \times 5x &\equiv 9 \times 14 \pmod{22} \\ x &\equiv 126 \pmod{22} \\ &\equiv 16 \pmod{22}. \end{aligned}$$

(d) Given that

$$\begin{aligned} 3a + b &\equiv 15 \pmod{22} \\ 8a + b &\equiv 6 \pmod{22} \end{aligned}$$

find a and b.

We subtract the top congruence from the bottom one to get

$$\begin{aligned} 5a &\equiv -9 \pmod{22} \\ &\equiv 13 \pmod{22}. \end{aligned}$$

We then multiply by the multiplicative inverse of 5 to get

$$\begin{aligned} 9 \times 5a &\equiv 9 \times 13 \pmod{22} \\ a &\equiv 117 \pmod{22} \\ &\equiv 7 \pmod{22}. \end{aligned}$$

To find b, we plug this value for a into the top congruence. We get

$$\begin{aligned} 3 \times 7 + b &\equiv 15 \pmod{22} \\ 21 + b &\equiv 15 \pmod{22} \\ b &\equiv -6 \pmod{22} \\ &\equiv 16 \pmod{22}. \end{aligned}$$

The solution is $a = 7$, $b = 16$.

B2. Decrypt the following, using the affine decryption key $a = 5$, $b = 7$.

```
JMCRZ CJXSV WJSRC XDRCL VXWPI PCURW P
```

Here's the decryption alphabet

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$f_{5,7}(x)$	H	M	R	W	B	G	L	Q	V	A	F	K	P
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$f_{5,7}(x)$	U	Z	E	J	O	T	Y	D	I	N	S	X	C

The text decrypts as "A procrastinator's work is never done."