1. Apply the Euclidean algorithm and calculate

$$\gcd(26, 9) \qquad\qquad \gcd(81, 18)$$

Solution.

$$\gcd(26, 9) = \gcd(9, 8) = \gcd(8, 1) = \gcd(1, 0) = 1$$
$$\gcd(81, 18) = \gcd(18, 9) = \gcd(9, 0) = 9$$

2. Express the following pairs of numbers in the form of Bezout identity

$$\alpha a + \beta b = \gcd(a, b) \ .$$

$$(60, 12) \qquad\qquad (12, 18) \qquad\qquad (26, 9)$$

Solution.

60	12	a	b
0	12	a-5b	b

12	18	a	b
12	6	a	b-a
0	6	a-2(b-a)=3a-2b	b-a

26	9	a	b
6	9	a-2b	b
6	3	a-2b	b-(a-2b)=3b-a
0	3	a-2b-2(3b-a) = 3a-8b	3b-a

The Bezout identities are:

$$0 \cdot 60 + 1 \cdot 12 = \gcd(60, 12) \ ,$$
$$-1 \cdot 12 + 1 \cdot 18 = \gcd(12, 18) \ ,$$
$$-1 \cdot 26 + 3 \cdot 9 = \gcd(26, 9) \ .$$

3. Find multiplicative modular inverse

$$2^{-1} \text{ in } \mathbb{Z}_7 \qquad\qquad 4^{-1} \text{ in } \mathbb{Z}_{11}$$
$$9^{-1} \text{ in } \mathbb{Z}_{26} \qquad\qquad 2^{-1} \text{ in } \mathbb{Z}_6$$

Solution.

2	7	a	b
2	1	a	b-3a
0	1	a-2(b-3a)=7a-2b	b-3a

4	11	a	b
4	3	a	b-2a
1	3	a-(b-2a)=3a-b	b-2a
1	0	3a-b	b-2a-3(3a-b) = -11a+4b

9	26	a	b
9	8	a	b-2a
1	8	a-(b-2a)=3a-b	b-2a
1	0	3a-b	b-2a-8(3a-b)=-26a+9b

2	6	a	b
2	0	a	b-3a

So,

$$2^{-1} \equiv 4 \pmod 7 \qquad 4^{-1} \equiv 3 \pmod{11} \qquad 9^{-1} \equiv 3 \pmod{26} \qquad 2^{-1} \notin \mathbb{Z}_6 \ .$$

4. Find additive inverse

$$-3 \text{ in } \mathbb{Z}_5 \qquad\qquad -4 \text{ in } \mathbb{Z}_{10}$$

Solution.

$$-3 \equiv 2 \pmod 5 \qquad\qquad -4 \equiv 6 \pmod{10}$$

5. How many invertible elements?

$$\mathbb{Z}_6 \qquad\qquad \mathbb{Z}_6^\times \qquad\qquad \mathbb{Z}_{11}^\times$$

Solution. There are 6 invertible elements in $\mathbb{Z}_6$, there are

$$\phi(6) = \phi(2 \cdot 3) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 6 \cdot \frac{1}{2} \cdot \frac{2}{3} = 2 \ .$$

invertible elements in $\mathbb{Z}_6^\times$. Also, if $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, where p_i are primes, then $\phi(n) = \phi(p_1) \cdot \phi(p_2) \cdot \ldots \cdot \phi(p_k)$, then

$$\phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3) = (2-1)(3-1) = 2 \ .$$

There are $\phi(11) = 11 - 1 = 10$ invertible elements in $\mathbb{Z}_{11}^\times$.

6. Which elements have multiplicative inverses in $\mathbb{Z}_8$ and $\mathbb{Z}_{20}$?

Solution. In $\mathbb{Z}_8 : 1, 3, 5, 7$. In $\mathbb{Z}_{20} : 1, 3, 7, 9, 11, 13, 17, 19$.

7. Write out addition and multiplication tables in $\mathbb{Z}_5$ and $\mathbb{Z}_8$.

Solution. The Cayley tables for $\mathbb{Z}_5$ are the following.

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

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

The Cayley tables for $\mathbb{Z}_8$ are the following.

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

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

8. Solve the following linear equations

$$\begin{array}{lll} x+3 \equiv 2 \pmod 5 & 5+6 \equiv x \pmod{11} & 5x+2 \equiv 3 \pmod 7 \\ 4x+3 \equiv 11 \pmod{12} & x-4 \equiv 7 \pmod{12} & 4x \equiv 2 \pmod{19} \\ 4x+3 \equiv 5 \pmod{13} & 2x+1 \equiv 9x-4 \pmod{23} & 5x-1 \equiv 3x+1 \pmod{26} \end{array}$$

Solution. (a) $x+3 \equiv 2 \pmod 5$. Since $-3 \equiv 2$ in $\mathbb{Z}_5$,

$$x+3+2 \equiv 2+2 \pmod 5 \implies x \equiv 4 \pmod 5 .$$

(b) $5+6 \equiv x \pmod{11}$. It is easy to see that $5+6 = 11 \equiv 0 \pmod{11}$.

(c) $5x+2 \equiv 3 \pmod 7$. Since $-2 \equiv 5$ in $\mathbb{Z}_7$, $5x \equiv 1 \pmod 7$. Next, we need to find 5^{-1} in $\mathbb{Z}_7$ to solve the equation.

5	7	a	b
5	2	a	b-a
1	2	a-2(b-a)=3a-2b	b-a
1	0	3a-2b	b-a-2(3a-2b) = -7a + 5b

Therefore, $5^{-1} = 3$. Indeed, $5 \cdot 3 + 2 = 17 \equiv 3 \pmod 7$.

(d) $4x+3 \equiv 11 \pmod{12}$. Since $-3 \equiv 9$ in $\mathbb{Z}_{12}$, $4x \equiv 8 \pmod{12}$. There is no element 4^{-1} in $\mathbb{Z}_{12}$, since $\gcd(4,12) = 4 \neq 1$. Let us divide this equation by 4 to get $x \equiv 2 \pmod 3$. This is the solution to the original equation as well. To verify, observe that $4 \cdot 2 + 3 = 11 \equiv 11 \pmod{12}$.

(e) $x-4 \equiv 7 \pmod{12}$. Adding 4 to both sides of the equation we get $x \equiv 11 \pmod{12}$.

(f) $4x \equiv 2 \pmod{19}$. To solve the equation we need to find 4^{-1} in $\mathbb{Z}_{19}$ and multiply both sides of the equation by it.

4	19	a	b
4	3	a	b-4a
1	3	a-(b-4a) = 5a-b	b-4a
1	0	5a-b	b-4a-3(5a-b) = -19a+4b

So $4^{-1} = 5$ in $\mathbb{Z}_{19}$. Multiplying both sides of the equation by 5, we get

$$5 \cdot 4x \equiv 5 \cdot 2 \pmod{19} \implies x \equiv 10 \pmod{19} .$$

Indeed, $4 \cdot 10 = 40 \equiv 2 \pmod{19}$.

(g) $4x+3 \equiv 5 \pmod{13}$. Adding $-3 \equiv 10 \in \mathbb{Z}_{19}$ to both sides of the equation, we get $4x \equiv 2 \pmod{13}$.

4	13	a	b
4	1	a	b-3a
0	1	a-4(b-3a) = 13a-4b	b-3a

So, $4^{-1} = -3 \equiv 10 \pmod{13}$. Multiplying both sides of the equation by 10, we get

$$10 \cdot 4x \equiv 10 \cdot 2 \pmod{13} \implies x \equiv 7 \pmod{13} .$$

Indeed, $4 \cdot 7 + 3 = 31 \equiv 5 \pmod{13}$.

(h) $2x + 1 \equiv 9x - 4 \pmod{23}$.

$$2x + 1 \equiv 9x - 4 \pmod{23} \implies 16x + 1 \equiv -4 \pmod{23} \implies 16x \equiv 18 \pmod{23} .$$

16	23	a	b
16	7	a	b-a
2	7	a-2(b-a)=3a-2b	b-a
2	1	3a-2b	b-a-3(3a-2b) = -10a+7b
0	1	3a-2b-2(-10a+7b) = 23a-16b	-10a+7b

Therefore, $16 \cdot 13 \cdot x \equiv 18 \cdot 13 \pmod{23} \implies x \equiv 4 \pmod{23}$. Indeed, $2 \cdot 4 + 1 \equiv 9 \cdot 4 - 4 \pmod{23} \implies 9 \equiv 32 \pmod{23}$.

(i) $5x - 1 \equiv 3x + 1 \pmod{26}$.

$$\begin{aligned} 5x - 1 \equiv 3x + 1 \pmod{26} &\implies 5x \equiv 3x + 2 \pmod{26} \\ &\implies 2x \equiv 2 \pmod{26} \implies x \equiv 1 \pmod{26} . \end{aligned}$$

Indeed, $5 \cdot 1 - 1 \equiv 3 \cdot 1 + 1 \pmod{23}$.

9. Solve the systems of linear equations

$$\begin{cases} a + b \equiv 17 \pmod{26} \\ 2a + b \equiv 0 \pmod{26} \end{cases} \qquad \begin{cases} a + b \equiv 17 \pmod{26} \\ 4a + b \equiv 1 \pmod{26} \end{cases}$$

$$\begin{cases} a + b \equiv 17 \pmod{26} \\ 3a + b \equiv 0 \pmod{26} \end{cases} \qquad \begin{cases} 5a + b \equiv 21 \pmod{26} \\ 16a + b \equiv 10 \pmod{26} \end{cases}$$

$$\begin{cases} 8a + b \equiv 8 \pmod{26} \\ 5a + b \equiv 13 \pmod{26} \end{cases}$$

Solution. (a) $\begin{cases} a + b \equiv 17 \pmod{26} \\ 2a + b \equiv 0 \pmod{26} \end{cases}$.

Subtracting the first equation from the second, we get $a \equiv 9 \pmod{26}$. Substituting this value of a into the first equation, we have $b + 9 \equiv 17 \implies b \equiv 8 \pmod{26}$. To verify, observe that $9 + 8 \equiv 17 \pmod{26}$ and $2 \cdot 9 + 8 \equiv 0 \pmod{26}$.

(b) $\begin{cases} a + b \equiv 17 \pmod{26} \\ 4a + b \equiv 1 \pmod{26} \end{cases}$.

Subtracting the second equation from the first one, we get $23a \equiv 16 \pmod{26}$. Next, we find 23^{-1} in $\mathbb{Z}_{26}$.

23	26	a	b
23	3	a	b-a
2	3	a-7(b-a)=8a-7b	b-a
2	1	8a-7b	b-a-(8a-7b) = -9a+8b
0	1	8a-7b-2(-9a+8b) = 26a-23b	-9a+8b

Therefore, $23^{-1} = 17$ in $\mathbb{Z}_{26}$. Multiplying both sides of the equation by 17, we have

$$17 \cdot 23a \equiv 17 \cdot 16 \implies a \equiv 12 \pmod{26} .$$

Substituting a into the first equation, we have $b + 12 \equiv 17 \implies b \equiv 5 \pmod{26}$. To verify, observe that $12 + 5 = 17 \pmod{26}$ and $4 \cdot 12 + 5 = 53 \equiv 1 \pmod{26}$.

(c) $\begin{cases} a + b \equiv 17 \pmod{26} \\ 3a + b \equiv 0 \pmod{26} \end{cases}.$

Subtracting the second equation from the first one, we get $24a \equiv 17 \pmod{26}$. This equation is not solvable, since there is no element 24^{-1} in $\mathbb{Z}_{26}$ and $2 \nmid 17$.

(d) $\begin{cases} 5a + b \equiv 21 \pmod{26} \\ 16a + b \equiv 10 \pmod{26} \end{cases}.$

Subtracting the second equation from the first one, we get $15a \equiv 11 \pmod{26}$. Next we look for 15^{-1} in $\mathbb{Z}_{26}$.

15	26	a	b
15	11	a	b-a
4	11	a-(b-a) = 2a-b	b-a
4	3	2a-b	b-a-2(2a-b)=-5a+3b
1	3	2a-b-(-5a+3b)=7a-4b	-5a+3b
1	0	7a-4b	-5a+3b-3(7a-4b) = -26a + 15b

Therefore, $15^{-1} = 7$ in $\mathbb{Z}_{26}$. We have $a \equiv 7 \cdot 11 \equiv 25 \pmod{26}$. Substituting the value of a into the first equation, we get $b = 21 - 5 \cdot 25 \equiv 0 \pmod{26}$.

(e) $\begin{cases} 8a + b \equiv 8 \pmod{26} \\ 5a + b \equiv 13 \pmod{26} \end{cases}.$

Subtracting the second equation from the first one, we get

$$3a \equiv 21 \pmod{26} \implies a \equiv 7 \pmod{26} .$$

Substituting the value of a into the first equation, we get

$$7 \cdot 8 + b \equiv 8 \pmod{26} \implies 4 + b \equiv 8 \pmod{26} \implies b \equiv 4 \pmod{26} .$$

To verify that the solution is indeed correct, observe that $8 \cdot 7 + 4 = 60 \equiv 8 \pmod{26}$ and $5 \cdot 7 + 4 = 39 \equiv 13 \pmod{26}$.