1. Find multiplicative modular inverse

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

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,

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

It is also possible to find multiplicative inverses by using the Euler theorem, which states that if integers n and a are co-prime, then

$$a^{\varphi(n)} \equiv 1 \pmod n \ .$$

We can use this formula to obtain the multiplicative inverse of a as

$$a^{-1} \equiv a^{\varphi(n)-1} \pmod n \ ,$$

so that $a \cdot a^{-1} = a \cdot a^{\varphi(n)-1} = a^{\varphi(n)} \equiv 1 \pmod n$.

$\varphi(7) = 6$, and therefore $2^{-1} = 2^5 \equiv 4 \pmod 7$. $\varphi(11) = 10$, and so $4^{-1} = 4^9 \equiv 3 \pmod{11}$. $\varphi(26) = \varphi(2) \cdot \varphi 13 = 12$, and so $9^{-1} = 9^1 1 \equiv 3$. Finally, 2 is not invertible in $\mathbb{Z}_6$, no matter which formula or algorithm we use to calculate it.

2. Find additive inverse

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

Solution.

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

3. How many invertible elements?

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

Solution. There are 6 invertible elements in $\mathbb{Z}_6$, there are $\{0, 1, 2, 3, 4, 5\}$. There are

$$\varphi(6) = \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = (2-1)(3-1) = 2$$

invertible elements in $\mathbb{Z}_6^\times$, namely, $\{1, 5\}$. There are $\varphi(11) = 11 - 1 = 10$ invertible elements in $\mathbb{Z}_{11}^\times$.

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

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

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

   Solution. The Cayley tables for $\mathbb{Z}_5$ can be seen in Table 1, and the Cayley tables for $\mathbb{Z}_8$ can be seen in Table 2.

Table 1: Cayley tables for $\mathbb{Z}_5$.

+	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

Table 2: Cayley tables for $\mathbb{Z}_8$.

+	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

6. 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. Since $5^{-1} = 3$ in $\mathbb{Z}_7$, this is our answer. 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. $4^{-1} = 5$ in $\mathbb{Z}_{19}$, so 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 $4x \equiv 2 \pmod{13}$. $4^{-1} = -3 \equiv 10$ in $\mathbb{Z}_13$. 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) $2x+1 \equiv 9x - 4 \pmod{23}$.

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

$16^{-1} = 13$ in $\mathbb{Z}_{23}$, multiplying both sides of the equation by 13, we have $16 \cdot 13 \cdot x \equiv 18 \cdot 13 \pmod{23} \implies x \equiv 4 \pmod{23}$. 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, $5 \cdot 1 - 1 \equiv 3 \cdot 1 + 1 \pmod{23}$.

7. 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 $23a \equiv 16 \pmod{26}$. Since $23^{-1} = 17$ 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 $15a \equiv 11 \pmod{26}$. Since $15^{-1} = 7$ in $\mathbb{Z}_{26}$, multiplying both sides of the equation by 7, we get $a \equiv 7 \cdot 11 \equiv 25 \pmod{26}$. 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 $5 \cdot 7 + 4 = 39 \equiv 13 \pmod{26}$.

8. Solve for x

(a) $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{4} \end{cases}$ (b) $\begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 3 \pmod{7} \end{cases}$

(c) $\begin{cases} x \equiv 10 \pmod{12} \\ x \equiv 3 \pmod{5} \end{cases}$ (d) $\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{6} \end{cases}$

Solution. (a) The Bézout identity for $(3, 4)$ is $-1 \cdot 3 + 1 \cdot 4 = 1$. Hence the solution is

$$x = 1 \cdot 1 \cdot 4 + 2 \cdot (-1) \cdot 3 = 4 - 6 = -2 \equiv 10 \pmod{12} .$$

One can observe that $10 \bmod 3 = 1$ and $10 \bmod 4 = 2$.

(b) The Bézout identity for $(4,7)$ is $2 \cdot 4 - 1 \cdot 7 = 1$. Hence the solution is

$$x = 3 \cdot 2 \cdot 4 + 0 = 24 \pmod{28} \ .$$

One can observe that $24 \bmod 4 = 0$ and $24 \bmod 7 = 3$.

(c) The Bézout identity for $(12,5)$ is $-2 \cdot 12 + 5 \cdot 5 = 1$. Hence the solution is

$$x = 3 \cdot -2 \cdot 12 + 10 \cdot 5 \cdot 5 = -72 + 250 = 178 \equiv 58 \pmod{60} \ .$$

One can observe that $58 \mod 12 = 10$ and $58 \mod 5 = 3$.

(d) The Bézout identity for $(5,6)$ is $1 \cdot 6 - 1 \cdot 5 = 1$. Hence the solution is

$$x = 5 \cdot 5 \cdot (-1) + 3 \cdot 6 \cdot 1 = -25 + 18 = -7 \equiv 23 \pmod{30} \ .$$

One can observe that $23 \bmod 5 = 3$ and $23 \bmod 6 = 5$.

9. Solve for x

$$(a) \quad \begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases} \qquad\qquad (b) \quad \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$$

Solution. (a) We've got 3 moduli, hence $N = 2 \cdot 3 \cdot 5 = 30$ and

$$N_1 = \frac{30}{2} = 15 \ , \qquad N_2 = \frac{30}{3} = 10 \ , \qquad N_3 = \frac{30}{5} = 6 \ .$$

The Bézout identities for $\gcd(N_i, n_i)$ are

$$\begin{aligned} \gcd(15,2) &= 1 \cdot 15 + (-7) \cdot 2 = 1 \ , \\ \gcd(10,3) &= 1 \cdot 10 + (-3) \cdot 3 = 1 \ , \\ \gcd(6,5) &= 1 \cdot 5 + (-1) \cdot 5 = 1 \ . \end{aligned}$$

Hence, $M_1 = M_2 = M_3 = 1$. We will use the formula

$$x \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{N} \ . \tag{1}$$

Therefore,

$$x = 0 + 2 \cdot 1 \cdot 10 + 3 \cdot 1 \cdot 6 = 38 \equiv 8 \pmod{30} \ .$$

To verify that 8 is indeed the solution, observe that

$$8 \bmod 2 = 0 \ , \qquad 8 \bmod 3 = 2 \ , \qquad 8 \bmod 5 = 3 \ .$$

(b) We've got 4 moduli, hence $N = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ and

$$N_1 = \frac{210}{2} = 105 \ , \qquad N_2 = \frac{210}{3} = 70 \ , \qquad N_3 = \frac{210}{5} = 42 \ , \qquad N_4 = \frac{210}{7} = 30 \ .$$

The Bézout identities for $\gcd(N_i, n_i)$ are

$$\begin{aligned}
\gcd(105, 2) &= 1 \cdot 105 + (-52) \cdot 2 = 1 \ , \\
\gcd(70, 3) &= 1 \cdot 70 + (-23) \cdot 3 = 1 \ , \\
\gcd(42, 5) &= (-2) \cdot 42 + 17 \cdot 5 = 1 \ , \\
\gcd(30, 7) &= (-3) \cdot 30 + 13 \cdot 7 = 1 \ .
\end{aligned}$$

Hence, $M_1 = M_2 = 1, M_3 = -2, M_4 = -3$. By (1), the solution is

$$x = 1 \cdot 1 \cdot 105 + 2 \cdot 1 \cdot 70 + 3 \cdot (-2) \cdot 42 + 5 \cdot (-3) \cdot 30 = -457 \equiv 173 \pmod{210} \ .$$

To verify that 173 is indeed the solution, observe that

$$173 \bmod 2 = 1 \ , \qquad 173 \bmod 3 = 2 \ , \qquad 173 \bmod 5 = 3 \ , \qquad 173 \bmod 7 = 5 \ .$$