**Question 1.** Determine whether each of these integers is prime.

a) 21 , not prime
b) 29 , prime
c) 71 , prime
d) 97 , prime
e) 111 , not prime
f) 143 , not prime

**Question 2.** What are the greatest common divisors and the least common multiple of these pairs of integers?

a) GCD $= 3^5 \times 5^3$ , GCM $= 2^{11} \times 3^7 \times 5^9 \times 7^3$
b) GCD $= 1$, GCM $= 2^9 \times 3^7 5^5 \times 7^3 \times 11 \times 13 \times 17$
c) GCD $= 23^{17}$ , GCM $= 23^{31}$
d) GCD $= 41 \times 43 \times 53$, GCM $= 41 \times 43 \times 53$
e) GCD $= 1$ , GCM $= 2^{12} \times 3^{13} \times 5^{17} \times 7^{21}$
f) GCD $= 1111$ , GCM is undefined

**Question 3.** Use the extended Euclidean algorithm to express $\gcd(26, 91)$ as a linear combination of 26 and 91.

*Solution.*

$$91 = 3 \times 26 + 13$$
$$26 = 13 \times 2$$
$$13 = 91 - 3 \times 26$$

The linear combination: $(-3) \times 26 + 1 \times 91 = 13$ ∎

**Question 4.** Show that 15 is an inverse of 7 modulo 26.

*Solution.*
$a$, and $b$ are inverse of each others mod $m$ if $ab = 1 \mod m$
$a = 15,\ b = 7$ and $m = 26$

$a \times b = 15 \times 7 = 105 = 26 \times 4 + 1 = 1 \mod 26$
$105 \equiv 1 \mod 26$

**Question 5.** Show that if $a$ and $m$ are relatively prime positive integers, then the inverse of $a$ modulo $m$ is unique modulo $m$. [Hint: Assume that there are two solutions $b$ and $c$ of the congruence $ax \equiv 1 \mod m$. Use Theorem 7 of Section 4.3 to show that $b \equiv c \mod m$.]

*Solution.*
Suppose that $b$ and $c$ are both inverses of $a$ modulo $m$.
Then $ba \equiv 1 \mod m$ and $ca \equiv 1 \mod m$.
Hence, $ba \equiv ca \mod m$. Because $\gcd(a, m) = 1$ it follows by Theorem 7 in Section 4.3 that $b \equiv c \mod m$. ■

**Question 6.** Find an inverse of $a$ modulo $m$ for this pair of relatively prime integers:
$a = 4, m = 9$
Then solve the congruence $4x \equiv 5 \mod 9$ using the inverse of 4 modulo 9 .

*Solution.*
The inverse of $a$ modulo $m$ is an integer $b$ for which $ab \equiv 1 \mod m$
First, perform Euclidean algorithm

$$\begin{aligned} 9 &= 2 \times 4 + 1 \\ 4 &= 4 \times 1 \end{aligned}$$

The greatest common divisor is then the last non-zero reminder, $\gcd(a, m) = \gcd(9, 4) = 1$
Next, write the greatest common divisor as multiple of $a$ and $m$:

$$\begin{aligned} \gcd(a, m) &= 1 \\ &= 9 - 2 \times 4 \\ &= 1 \times 9 - 2 \times 4 \end{aligned}$$

The inverse is the coefficient of $a$, which is -2.
Since $-2 \mod 9 = 7 \mod 9$, then 7 is also the inverse of $a$ modulo $m$.

Then, we can solve congruence $4x \equiv 5 \mod 9$ by multiplying each side by the inverse 7.

$$\begin{aligned} 4x &\equiv 5 \mod 9 \\ 7 \times 4x &\equiv 7 \times 5 \mod 9 \\ 28x &\equiv 35 \mod 9 \\ x &\equiv 35 \mod 9 .................(28 \mod 9 = 1) \\ x &\equiv 8 \mod 9 .................(35 \mod 9 = 8) \end{aligned}$$

Thus, the solution of the congruence is $x \equiv 8 \mod 9$

**Question 7.** Use Fermats little theorem to find $7^{121} \mod 13$.

*Solution.*
Fermats little theorem states $a^{p-1} \equiv 1 \mod p$, if $p$ is prime and $a$ is not divisible by $p$.
When $a = 7$, and $p = 13$, Fermats little theorem them implies $7^{12} = 7^{13-1} \equiv 1 \mod 13$
Since $121 = 120 + 1 = 12 \times 10 + 1$ then

$$\begin{aligned} 7^{121} \mod 13 &= 7^{12 \times 10 + 1} \mod 13 \\ &= (7^{12 \times 10} \times 7) \mod 13 \\ &= ((7^{12 \times 10} \mod 13) \times (7 \mod 13)) \mod 13 \\ &= (((7^{12})^{10} \mod 13) \times (7 \mod 13)) \mod 13 \\ &= (((7^{12} \mod 13))^{10} \mod 13 \times (7 \mod 13)) \mod 13 \\ &= ((1)^{10} \mod 13 \times (7)) \mod 13 \\ &= ((1) \mod 13 \times (7)) \mod 13 \\ &= (1 \times 7) \mod 13 \\ &= 7 \end{aligned}$$