Lesson 2.3 Divisibility

(Computer Science Engineering Degree)
Departamento de Matemática Aplicada
ETS Ingeniería Informática
Universidad Politécnica de Valencia

Contents

Divisibilty

Definition (Divisibility)

We say that an integer number $a \in \mathbb{Z}$ is **divisible by** an integer $b \in \mathbb{Z}$ different from 0, if there exists another integer $k \in \mathbb{Z}$ such that $a = bk$. It is also said b is a **divisor** of a, or b **divides** a, or a is a **multiple** of b. This is denoted as $b \mid a$.

Example: 3 divides 6 (or 6 is a multiple of 3), but 3 does not divide 5.

Definition (Prime numbers)

We say that a natural number $p > 1$ is **prime** if their two unique divisors (natural numbers) are 1 and p itself. If a natural number greater than 1 is not prime, then we say that it is **composed**.

The smallest prime numbers are $2, 3, 5, 7, 11, 13 \ldots$

GCD & LCM

Definition (GCD and LCM)

The **Greatest Common Divisor** of the integer numbers $a_1, a_2, \ldots, a_n \neq 0$ is the greatest positive number that divides all of them.

It is denoted as $\gcd(a_1, \ldots, a_n)$.

The **Least Common Multiple** of the integer numbers $a_1, a_2, \ldots, a_n \neq 0$ is the smallest positive integer that is a multiple of all of them.

It is denoted as $\text{lcm}(a_1, a_2, \ldots, a_n)$.

We say that $a, b \in \mathbb{Z}$ are **prime respect to the oher** if $\gcd(a, b) = 1$.

The Fundamental Theorem of Arithmetics

Theorem (The Fundamental Theorem of Arithmetics)

Every natrual number $n > 1$ can be written in a unique way (except by the order) as a product of prime numbers.

Example: $24 = 2^3 \cdot 3$ and $126 = 2 \cdot 3^2 \cdot 7$.

Consequences

Let a and b two nonnull integers. Consider the decompositions of $|a|$ and $|b|$ as a product of prime factors. Then

1. $\gcd(a, b)$ is the product of all the prime factors which are **common to both decompositions powered to the smallest exponent**.
2. $\operatorname{lcm}(a, b)$ is the product of all the prime factors that **appear in any of the decompositions (common and not common) powered to the greatest exponent**.
3. $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = |a \cdot b|$.

Example: $\gcd(24, 126) = 2 \cdot 3 = 6$. $\operatorname{lcm}(24, 126) = 2^3 \cdot 3^2 \cdot 7 = 504$.

Euclidean division

Theorem

Let $a, b \in \mathbb{Z}$, with $b > 0$. Then there are two unique integer numbers q, r such that $a = q \cdot b + r$ and $0 \leq r < b$.

The numbers a, b, q, and r are called **dividend, divisor, quotient**, and **remainder**, respectively.

Example

- If $a = 7$ and $b = 5$, then $7 = 1 \cdot 5 + 2$.
- If $a = 5$ and $b = 7$, then $5 = 0 \cdot 7 + 5$.
- If $a = -7$ and $b = 5$, then $-7 = -2 \cdot 5 + 3$.
- If $a = -5$ and $b = 7$, then $-5 = -1 \cdot 7 + 2$.

Euclides algorithm

The Euclides algorithm let us compute the greatest common divisor of two integer numbers without needing to find all the decompositions as a product of prime numbers. This is based on the following property:

Lemma

If a, $b \in \mathbb{Z}$, and $b \neq 0$, then $\gcd(a,b) = \gcd(b,r)$, where r is the remainder of the Eucllidean division of a by b.

This can be proved testing that the common divisors of a and b are the same common divisors of b and r.

Euclides algortihm

The Euclides algorithm consists on applying several times this property, reducing the size of the numbers without changing the gcd.

Example

Example (Let us compute the gcd(689, 234) using the Euclides algorithm.)

1. Divide $a = 689$ by $b = 234$:

$$\begin{array}{rl} 689 & |\underline{234} \\ 221 & 2 \end{array}$$

2. Divide the divisor by the remainder:

$$\begin{array}{rl} 234 & |\underline{221} \\ 13 & 1 \end{array}$$

3. Divide the new divisor by the new remainder:

$$\begin{array}{rl} 221 & |\underline{13} \\ 0 & 17 \end{array}$$

The last nonnull remainder is 13. So that, $\gcd(689, 234) = 13$.

Since $\gcd(689, 234) \cdot \operatorname{lcm}(689, 234) = 689 \cdot 234$, we can have the least common multiple of 689 and 234:

$$\operatorname{lcm}(689, 234) = 689 \cdot 234/13 = 12402.$$

Another example

Example (Compute gcd(54321,50) using the Euclides algorithm)

$$\begin{array}{rr|l} 54321 & 50 & \\ 21 & 1056 & \end{array} \qquad \begin{array}{rr|l} 50 & 21 & \\ 8 & 2 & \end{array} \qquad \begin{array}{rr|l} 21 & 8 & \\ 5 & 2 & \end{array}$$

$$\begin{array}{rr|l} 8 & 5 & \\ 3 & 1 & \end{array} \qquad \begin{array}{rr|l} 5 & 3 & \\ 2 & 1 & \end{array} \qquad \begin{array}{rr|l} 3 & 2 & \\ 1 & 1 & \end{array} \qquad \begin{array}{rr|l} 2 & 1 & \\ 0 & 2 & \end{array}$$

Since the remainder is nonnull, then 1 is the $\gcd(54321,50) = 1$, therefore 54321 and 50 are primes respect to the other.

In addition, the least common multiple is:

$$\operatorname{lcm}(54321,50) = 54321 \cdot 50 / \gcd(54321,50) = 2716050.$$

Consequences of the Euclides algorithm

The Euclidean algorithm let us prove an important theorem on Number Theory, the **Bézout Identity**, that states that the greatest common divisor of two numbers can be written as a linear combination of both of them:

Theorem (Bezout Identity)

For every pair of numbers $a, b \in \mathbb{Z}$, there exists two numbers $x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = x \cdot a + y \cdot b.$$

In addition, all the multiples of $\gcd(a, b)$, and only them, can be written as a linear combination of a and b.

Corollary

If $a, b, c \in \mathbb{Z}$, then there exists $x, y \in \mathbb{Z}$ such that $c = x \cdot a + y \cdot b$ if and only if $\gcd(a, b) \mid c$.

Example of the Bézout Identity

Example (Compute $x, y \in \mathbb{Z}$ such that $\mathrm{mcd}(250, 111) = x \cdot 250 + y \cdot 111$.)

We apply the Euclides algorithm to compute $\gcd(250, 111)$. Besides we will express the remainder of each one of the divisions as a sum of multiples of 250 and 111:

$$\begin{array}{r|l} 250 & 111 \\ \hline 28 & 2 \end{array} \qquad 250 = 2 \cdot 111 + 28 \;\Rightarrow\; 28 = 250 - 2 \cdot 111$$

$$\begin{array}{r|l} 111 & 28 \\ \hline 27 & 3 \end{array} \qquad \begin{aligned} 111 = 3 \cdot 28 + 27 \;\Rightarrow\; 27 &= 111 - 3 \cdot 28 \\ &= 111 - 3 \cdot (250 - 2 \cdot 111) \\ &= -3 \cdot 250 + 7 \cdot 111 \end{aligned}$$

$$\begin{array}{r|l} 28 & 27 \\ \hline 1 & 1 \end{array} \qquad \begin{aligned} 28 = 1 \cdot 27 + 1 \;\Rightarrow\; 1 &= 28 - 1 \cdot 27 \\ &= (250 - 2 \cdot 111) - 1 \cdot (-3 \cdot 250 + 7 \cdot 111) \\ &= 4 \cdot 250 - 9 \cdot 111 \end{aligned}$$

$$\begin{array}{r|l} 27 & 1 \\ \hline \mathbf{0} & 27 \end{array} \qquad \textbf{null remainder} \;\Rightarrow\; \boxed{\mathrm{mcd}(250, 111) = 1}$$

$x = 4$ and $y = -9$ satisfy the Bézout identity: $1 = 4 \cdot 250 + (-9) \cdot 111$

Congruence relations

We will study **the congruence relation modulo** m with more details.

Definition (Congruence relation)

If $m \in \mathbb{Z}$, $m > 1$, we say that two integer numbers a and b are **congruents modulo** m if $a - b$ is a multiple of m. We write it as $a \equiv b \pmod{m}$.

We can easily prove:

Proposition

$a \equiv b \pmod{m}$ if and only if the remainders of the Euclidean division of a and b by m coincide.

Example (Example)

$17 \equiv 53 \pmod{6}$ because $17 - 53 = -36$, which is a multiple of 6.
On the other hand, we can use the previous proposition: The remainder of the divisions of 17 and 53 by 6 coincide since

$$\begin{array}{r|l} 17 & 6 \\ \hline 5 & 2 \end{array} \qquad \begin{array}{r|l} 53 & 6 \\ \hline 5 & 8 \end{array}$$

Integers modulo m

Proposition

A congruences modulo m is an equivalence relation (it is reflexive, symmetric, and transitive).

Therefore, we can construct the correspondence quotient set:

Notation

Consider a positive integer number $m > 1$.

- We denote by $\mathbb{Z}_m$ the quotient set of $\mathbb{Z}$ respect to the congruence relation modulo m.
- The elements in $\mathbb{Z}_m$ are the equivalence classes of this relation. They are called **residual classes modulo** m (or simply the **integers modulo** m) and we denote them by $\overline{a}$, with $a \in \mathbb{Z}$.

For all $a \in \mathbb{Z}$ we have that $\overline{a} = \overline{r}$ in $\mathbb{Z}_m$, where r is the remainder of the Euclidean division of a by m. Therefore, $\mathbb{Z}_m$ has excatly m elements:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$$

The integers modulo m

- If $m = 2$, then $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, where

  $\overline{0} = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 2\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \{2n \mid n \in \mathbb{Z}\}$

  $\overline{1} = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 2\} = \{\ldots, -3, -1, 1, 3, 5, \ldots\} = \{1 + 2n \mid n \in \mathbb{Z}\}$

- If $m = 3$, then $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, where

  $\overline{0} = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = \{3n \mid n \in \mathbb{Z}\}$

  $\overline{1} = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\} = \{1 + 3n \mid n \in \mathbb{Z}\}$

  $\overline{2} = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\} = \{2 + 3n \mid n \in \mathbb{Z}\}$

- In general, $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$, where

  $\overline{0} = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod m\} = \{m \cdot n \mid n \in \mathbb{Z}\}$

  $\overline{1} = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod m\} = \{1 + m \cdot n \mid n \in \mathbb{Z}\}$

  $\overline{2} = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod m\} = \{2 + m \cdot n \mid n \in \mathbb{Z}\}$

  $\vdots$

  $\overline{m-1} = \{a \in \mathbb{Z} \mid a \equiv m-1 \pmod m\} = \{(m-1) + m \cdot n \mid n \in \mathbb{Z}\}$

Operations in $\mathbb{Z}_m$

Definition (Sum and product in $\mathbb{Z}_m$)

If $\overline{a}$ and $\overline{b}$ are two elements of $\mathbb{Z}_m$, then the **sum** and **product** of $\overline{a}$ and $\overline{b}$ is defined as follows:

$$\overline{a}+\overline{b}=\overline{a+b}, \quad \overline{a}\cdot\overline{b}=\overline{a\cdot b}$$

The definition of these operations does not depend of the representants choosen for every residual class:

Examples: In $\mathbb{Z}_4$, $\overline{2}+\overline{3}=\overline{5}=\overline{1}$, and in $\mathbb{Z}_7$, $\overline{3}\cdot\overline{6}=\overline{18}=\overline{4}$.

Showing the results

If m is small, we can construct a table with double input with all the possible results of the sum in $\mathbb{Z}_m$ (and also for the product). This kind of tables are known as the **Cayley table** of the operation.

Example: Let us to construct the Cayley tables of the sum and the product in $\mathbb{Z}_6$.

Operations in $\mathbb{Z}_m$

Remarks

- The sum and the product in $\mathbb{Z}_m$ are commutative and associative.
- The product is distributive respect to the sum.
- $\overline{0}$ are $\overline{1}$ indentity elements respect to sum and the product, respectively.
- Every element of $\mathbb{Z}_m$ has a symmetric element respect to the sum (also known as **opposed**). In particular, the opposed number of $\overline{a}$ is $\overline{-a}$, since $\overline{a}+\overline{-a}=\overline{0}$.

However, not all the elements in $\mathbb{Z}_m$ have a an invers element for the product.

- $\overline{0}$ has no inverse element in $\mathbb{Z}_m$ because $\overline{0}\cdot\overline{a}=\overline{0}\neq\overline{1}$, $\forall\ \overline{a}\in\mathbb{Z}_m$.
- $\overline{3}$ has no inverse element in $\mathbb{Z}_6$ since there is no element $\overline{a}$ of $\mathbb{Z}_6$ that satisfies $\overline{3}\cdot\overline{a}=\overline{1}$.

Let us see how to know if an integer modulo m has an inverse element, and if it exists, let us see how to compute it.

Inverse elements in $\mathbb{Z}_m$

$$\begin{aligned}\overline{a} \in \mathbb{Z}_m \text{ The inverse } &\iff \text{There exists } \overline{x} \in \mathbb{Z}_m \text{ such that } \overline{a}\cdot\overline{x} = \overline{1} \text{ in } \mathbb{Z}_m \\ &\iff \text{There exists } x \in \mathbb{Z} \text{ such that } (a\cdot x) - 1 \text{ is a multiple of } m \\ &\iff \text{There exists } x, y \in \mathbb{Z} \text{ such that } 1 = a\cdot x + y\cdot m.\end{aligned}$$

From the previous equivalence we can easily define the following result as a consequence of Bézout equality:

Theorem

$\overline{a} \neq \overline{0}$ has an inverse (respect to the product) in $\mathbb{Z}_m$ if, and only if, $\gcd(a, m) = 1$.

How to find the inverse element?

If $\gcd(a, m) = 1$, in order to find the inverse element of $\overline{a}$ in $\mathbb{Z}_m$ it is enough to find two integer numbers $x, y \in \mathbb{Z}$ such that $1 = x\cdot a + y\cdot m$, that is, the coefficients of a Bézout equality for a and m.

In that case, $\overline{x}$ will be the inverse of $\overline{a}$ in $\mathbb{Z}_m$ (that we denote as $\overline{a}^{-1}$).

Example

Example (Prove that $\overline{11}$ has an invers in $\mathbb{Z}_{27}$ and find it.)

It can be proved that $\gcd(27,11)=1$. Therefore, by the previous theorem, $\overline{11}$ has an invers in $\mathbb{Z}_{27}$.
In addition, we can obtain the invers of $\overline{11}$ in $\mathbb{Z}_{27}$ if we compute the Bézout identity for 11 and 27:

$$\begin{array}{cc} 27 & |\underline{11} \\ 5 & 2 \end{array} \qquad 27 = 2\cdot 11 + 5 \;\Rightarrow\; 5 = -2\cdot 11 + 27$$

$$\begin{array}{cc} 11 & |\underline{5} \\ 1 & 2 \end{array} \qquad 11 = 2\cdot 5 + 1 \;\Rightarrow\; 1 = -2\cdot 5 + 11 = -2\cdot(-2\cdot 11 + 27) + 11 = 5\cdot 11 + 1\cdot 27$$

$$\begin{array}{cc} 5 & |\underline{1} \\ \mathbf{0} & 5 \end{array} \qquad \textbf{null remainder} \;\Rightarrow\; \gcd(250,111) = 1 = \mathbf{5}\cdot 11 - 2\cdot 27$$

The inverse of $\overline{11}$ in $\mathbb{Z}_{27}$ is the class of the coefficient of 11 in the previous Bézout identity (since from that equality it can be deduced that $\overline{1} = \overline{5}\cdot\overline{11}$ in $\mathbb{Z}_{27}$). Therefore,

$$\overline{11}^{\,-1} = \overline{5}, \quad \text{in} \quad \mathbb{Z}_{27}.$$

Remarks

If we compute the inverse of an integer number $\overline{a}$ modulo m using the previous process, we have to express the residual class using the corresponding class in $\{0,1,\ldots,m-1\}$ (since in the process it is assumed that $a<m$).

Example (To compute the inverse of $\overline{19}$ in $\mathbb{Z}_7$)

We apply the previous process to $\overline{5}$, since $\overline{19}=\overline{5}$ in $\mathbb{Z}_7$ and $5<7$.

If m is small, the inverse of an integer modulo m can be computed just making a brief search and testing all the possible choices.

Let us comute the inverse of $\overline{5}$ in $\mathbb{Z}_7$

We can obtain the inverses computing the sequence of products $\overline{5}\cdot\overline{x}$ where $x\in\mathbb{Z}_7=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}\}$ until we get 1 as a result $\overline{1}$:
Since $\overline{5}\cdot\overline{0}=\overline{0}\quad\overline{5}\cdot\overline{1}=\overline{5}\quad\overline{5}\cdot\overline{2}=\overline{10}=\overline{3}\quad\overline{5}\cdot\overline{3}=\overline{15}=\overline{1}$.Therefore, the inverse of $\overline{5}$ in $\mathbb{Z}_7$ is $\overline{3}$.

Linear congruence equations

In the previous section we have analyzed the problem of finding the invers (if there exists) of an element $\overline{a}$ of $\mathbb{Z}_m$, that is, the problem of solving the following equation in $\mathbb{Z}_m$ (if there exists a solution):

$$\overline{a} \cdot \overline{x} = \overline{1}.$$

We will deal with the more general problem of solving any linear equation of first order in $\mathbb{Z}_m$, that is, any equation in $\mathbb{Z}_m$ of the form:

$$\overline{a} \cdot \overline{x} = \overline{b},$$

where $\overline{a}, \overline{b} \in \mathbb{Z}_m \setminus \{\overline{0}\}$, and $\overline{x}$ is an unknown that represents a class of $\mathbb{Z}_m$. These equations can also be posed in the form:

$$a \cdot x \equiv b \ (mod \ \ m).$$

Solving congruence equations

We analyze in which cases we can solve the equation $\overline{a} \cdot \overline{x} = \overline{b}$ in $\mathbb{Z}_m$.

$$\begin{aligned} \exists\ \overline{x} \in \mathbb{Z}_m \text{ such that } \overline{a} \cdot \overline{x} = \overline{b} &\iff \exists\ x \in \mathbb{Z} \text{ such that } a \cdot x \equiv b\ (mod\ \ m) \\ &\iff \exists\ x \in \mathbb{Z} \text{ such that } (a \cdot x) - b \text{ is a multiple of } m \\ &\iff \exists\ x, y \in \mathbb{Z} \text{ such that } a \cdot x + m \cdot y = b. \end{aligned}$$

By the previous equivalence and the corollary of Bézout identity we have:

Theorem

The equation $\overline{a} \cdot \overline{x} = \overline{b}$ in $\mathbb{Z}_m$ has a solution if, and only if, $\gcd(a, m) \mid b$.

This theorem shows in which cases we have a solution for that equation, but we do not know how many solutions we have. This information is provided by the next result.

Theorem

If $d = \gcd(a, m)$ divides b, then the equation $\overline{a} \cdot \overline{x} = \overline{b}$ in $\mathbb{Z}_m$ exactly has d solutions.

Solution of congruence equations

The solution of a equation of the type $\overline{a}\cdot\overline{x}=\overline{b}$ in $\mathbb{Z}_m$ (with $\overline{a},\overline{b}\neq 0$) depends on the value of $\gcd(a,m)$:

- **Case 1**: $\gcd(a,m)=1$. The equation $\bar{a}\cdot\bar{x}=\bar{b}$ has only one solution that is obtained multiplying both members of the equation by the inverse of $\bar{a}$ in $\mathbb{Z}_m$: $\bar{x}=\bar{a}^{-1}\cdot\bar{b}$.
- **Case 2**: $\gcd(a,m)\neq 1$ but divides b. The equation has d solutions, where $d=\gcd(a,m)$. Since d divides a,m, and b we can construct the equation

$$\frac{\overline{a}}{d}\cdot\overline{x}=\frac{\overline{b}}{d},\quad \text{in}\quad \mathbb{Z}_{\frac{m}{d}}\quad \text{(equation of case 1)}.$$

  If $\bar{s}$ is the solution of the previous equation modulo $\frac{m}{d}$, then the d solutions of the former equation $\bar{a}\cdot\bar{x}=\bar{b}$ in $\mathbb{Z}_m$ are:

$$\bar{s},\ \overline{s+\frac{m}{d}},\ \overline{s+2\cdot\frac{m}{d}},\ \ldots,\overline{s+(d-1)\cdot\frac{m}{d}}$$

- **Case 3**: $\gcd(a,m)$ does not divide b. The equation $\bar{a}\cdot\bar{x}=\bar{b}$ in $\mathbb{Z}_m$ has no solution.

Example (case 1)

Example (Solve the congruence equation $11 \cdot x \equiv 6 \pmod{27}$)

This is the same as solving is

$$\overline{11} \cdot \overline{x} = \overline{6}, \quad \text{in} \quad \mathbb{Z}_{27}$$

Since $\gcd(11,27) = 1$, this equation has **only one solution, (Case 1)**.
For computing this solution, we multiply both sides of the equation by the invers of 11 in $\mathbb{Z}_{27}$. So that, it is enough with computing that inverse. We did this before and we obtained

$$\overline{11}^{\,-1} = \overline{5}, \quad \text{in} \quad \mathbb{Z}_{27}.$$

Multiplying by $\overline{11}^{\,-1}$ both sides of the equation we obtain:

$$\overline{x} = \overline{11}^{\,-1} \cdot \overline{6} = \overline{5} \cdot \overline{6} = \overline{30} = \overline{3}, \quad \text{en} \quad \mathbb{Z}_{27}.$$

Therefore, the equation $\overline{11} \cdot \overline{x} = \overline{6}$ in $\mathbb{Z}_{27}$ has the solution $\overline{x} = \overline{3}$.

Example (case 2)

Example (Solve the congruence equation $18 \cdot x \equiv 6 \pmod{15}$)

This is the same as the equation $\overline{18} \cdot \overline{x} = \overline{6}$ in $\mathbb{Z}_{15}$.

Attention!!

We cannot simplify a 6 since 6 has no inverse in $\mathbb{Z}_{15}$. That is, the equation is not equivalent to the equation $\overline{3} \cdot \overline{x} = \overline{1}$, in $\mathbb{Z}_{15}$ (this last equation has no solution, it is an example of case 3).

Example

Firstly, we write $\overline{18}$ using its representant in $\{0, 1, \ldots, 14\}$. So that $\overline{18} = \overline{3}$ in $\mathbb{Z}_{15}$, and the initial equation is equivalent to:

$$\overline{3} \cdot \overline{x} = \overline{6}, \quad \text{in} \quad \mathbb{Z}_{15}.$$

We can directly see that $\overline{2}$ is a solution of this equation, but it is not the only one (since $\overline{3}$ has no inverse in $\mathbb{Z}_{15}$). As $\gcd(3, 15) = 3 \neq 1$ but it divides 6 (the other coefficient), the equation has 3 solutions (Case 2).

Example (case 2)

Example (Cont.)

Since the two coefficients and the modulo are divisible by 3, we can divide them and we obtain an equivalent equation to the first one, but with modulo 5:

$$\overline{1}\cdot\overline{x}=\overline{2},\quad \text{in}\quad \mathbb{Z}_5.\quad \text{(a Case 1 equation)}$$

This equation is already solved because the coefficient of $\overline{x}$ is $\overline{1}$ (in another case, we have to compute its inverse in order to solve it). It is $\overline{x}=\overline{2}$ in $\mathbb{Z}_5$. Now, in $\mathbb{Z}_5$, $\overline{2}=\overline{7}=\overline{12}=\ldots,$ but in $\mathbb{Z}_{15}$, these 3 classes are different. Therefore, the solution of the equation in $\mathbb{Z}_5$ gives 3 different solutions of the former equation in $\mathbb{Z}_{15}$:

$$\overline{x}=\overline{2}$$
$$\overline{x}=\overline{7}$$
$$\overline{x}=\overline{12}$$

where each one is obtained from the other just increasing 5.