3.7 Non-linear Diophantine Equations

As an example of the use of congruences we can use them to show when some Diophantine equations do *not* have integer solutions. This is quite a negative application - we do **not** prove that the equations have solutions.

Idea 1) Given a Diophantine Equation first *assume* it has integer solutions.

2) Then look at the equation modulo an appropriate modulus.

3) Find a contradiction.

Example 3.7.1 ***Not given*** *Show there are* ***no*** *integer solutions to* $166361x + 4043y = 25$.

Solution Assume the equation *has* integer solution. Look at the equation modulo 13. Both 166361 and 4043 are divisible by 13 (as seen in previous Chapter) and so the left hand side of the equation is $\equiv 0 \bmod 13$. But the right hand side is $25 \equiv 12 \bmod 13$. Thus the equation becomes $0 \equiv 12 \bmod 13$, a contradiction. ■

We actually proved this result in the previous Chapter. The hardest past of this method in general is choosing the appropriate modulus.

Example 3.7.2 *(c.f. PJE problem 19.2.6, p.236) Prove that there are* ***no*** *integral solutions to*

$$15x^2 - 7y^2 = 1.$$

Solution Assume there **is** a solution $(x_0, y_0) \in \mathbb{Z}^2$, so $15x_0^2 - 7y_0^2 = 1$.

Look at the equation modulo 7, to get

$$15x_0^2 \equiv 1 \bmod 7 \quad \text{or} \quad x_0^2 \equiv 1 \bmod 7.$$

Unfortunately there is a solution to this, namely $x_0 = 1$. Thus we have **not** found a contradiction. This does not mean that there is anything wrong with the method, just that this modulus has not led to a contradiction. We must look at another modulus.

Alternatively, look at the equation modulo 5 to get

$$-7y_0^2 \equiv 1 \bmod 5 \quad \text{or} \quad 3y_0^2 \equiv 1 \bmod 5.$$

Multiplying both sides by 2 we get

$$6y_0^2 \equiv 2 \bmod 5 \quad \text{i.e.} \quad y_0^2 \equiv 2 \bmod 5.$$

We see if this is possible or not by testing each possible value for y.

$y \bmod 5$	$y^2 \bmod 5$
0	0
1	1
2	4
3	4
4	1

In **no** case do we get $y^2 \equiv 2 \bmod 5$, there being no 2 in the right hand column. So our assumption that $15x^2 - 7y^2 = 1$ has a solution has led to a *contradiction modulo 5*. Hence the original equation has no integer solutions. ■

Alternative Solution We could have looked at the equation modulo 3, to get $-7y_0^2 \equiv 1 \bmod 3$ or $2y_0^2 \equiv 1 \bmod 3$. multiply both sides by 2 to get $4y_0^2 \equiv 2 \bmod 3$, i.e. $y_0^2 \equiv 2 \bmod 3$. We see if this is possible or not by testing each possible value for y.

$y \bmod 3$	$y^2 \bmod 3$
0	0
1	1
2	1

In **no** case do we get $y^2 \equiv 2 \bmod 3$. So our assumption that $15x^2 - 7y^2 = 1$ has a solution has led to a *contradiction modulo 3*. Hence the original equation has no integer solutions. ■

The lesson from this is that the smaller you take the modulus the smaller the table, i.e. the less work you have to do.

Example 3.7.3 *(MATH10101 Exam 2009) Show that for any $n \equiv 1 \bmod 7$ no integers a, b can be found satisfying*

$$n = 2a^3 - 5b^3.$$

Solution The information concerning n is given modulo 7 so we look at the Diophantine equation modulo 7, and try to find integer solutions of

$$2a^3 - 5b^3 \equiv 1 \bmod 7.$$

This we do by searching all possible values of $(a^3, b^3) \bmod 7$.

$a \bmod 7$	$a^3 \bmod 7$
0	0
1	1
2	1
3	6
4	1
5	6
6	6

Hence a^3 takes only 3 different values, modulo 7, i.e.

$$a^3 \equiv 0, 1 \text{ or } 6 \bmod 7.$$

Thus there are only 9 different possibilities for the pair $(a^3, b^3) \bmod 7$.

$a^3 \bmod 7$	$b^3 \bmod 7$	$2a^3 - 5b^3 \bmod 7$
0	0	0
0	1	$-5 \equiv 2$
0	6	$-30 \equiv 5$
1	0	2
1	1	$-3 \equiv 4$
1	6	$-28 \equiv 0$
6	0	$12 \equiv 5$
6	1	$7 \equiv 0$
6	6	$-18 \equiv 3$.

In no row do we see a final result of 1, hence $2a^3 - 5b^3$ is never $\equiv 1 \bmod 7$, hence no $n \equiv 1 \bmod 7$ can be written as $2a^3 - 5b^3$ for integers a and b. ■

Question how do we find the appropriate modulus?

Answer There is no method for finding the right modulus, we have to look at the original equation with different moduli, trying to find a case that has no solutions. If, for all moduli we choose, the resulting congruence has a solution there is a chance that the original equation has solutions, but if so these have to be found by other means.

Other examples Students may wish to try:

Example (MATH10111 exam 2007)

Show that $7x^4 + 2y^3 = 3$ has no integer solutions.

Show that 5 does not divide $a^3 + a^2 + 1$ for any $a \in \mathbb{Z}$.

Example (MATH10111 exam 2008).

Show that $2x^3 + 27y^4 = 21$ has no integer solutions.

Example (MATH10111 exam 2009)

Show that $7x^5 + 3y^4 = 2$ has no integer solutions.

4 Congruence Classes

4.1 Definition

Definition 4.1.1 *(p.251) The* ***congruence class*** $\bmod m$ *of* $a \in \mathbb{Z}$ *is the set of integers congruent to* $a \bmod m$,

$$[a]_m = \{b \in \mathbb{Z} : b \equiv a \bmod m\}.$$

Example 4.1.2 *With* $m = 3$ *we have*

$$\begin{aligned} [0]_3 &= \{.., -6, -3, 0, 3, 6, ...\}, \\ [1]_3 &= \{.., -5, -2, 1, 4, 7, ...\}, \\ [2]_3 &= \{.., -4, -1, 2, 5, 8, ...\}. \end{aligned}$$

Recall that congruences are "reflexive", so $a \equiv a \bmod m$ and thus $a \in [a]_m$ for all $a \in \mathbb{Z}$.

Note that in the example above all the integers appear in these classes, and these classes are disjoint. We could go on, for instance

$$[-5]_3 = \{... - 11, -8, -5, -3, 1, ...\}.$$

But this is not disjoint with $[1]_3$, and in fact it equals $[1]_3$. In general we have the **fundamental result**

Theorem 4.1.3 *For integers* a, b,

i) If $a \equiv b \pmod m$ *then* $[a]_m = [b]_m$,

ii) If $a \not\equiv b \pmod m$ *then* $[a]_m \cap [b]_m = \varnothing$.

Since we have exactly one of $a \equiv b \pmod m$ *or* $a \not\equiv b \pmod m$ *we deduce that either two classes are identical or disjoint.*

Proof i) Assume $a \equiv b \pmod m$. To show that $[a]_m = [b]_m$ we need show that $[a]_m \subseteq [b]_m$ and $[b]_m \subseteq [a]_m$.

To show $[a]_m \subseteq [b]_m$ let $k \in [a]_m$. By definition this means that $k \equiv a \bmod m$. Combine this with $a \equiv b \pmod m$ using *transitivity* to deduce $k \equiv b \bmod m$. By definition this means $k \in [b]_m$. Since this is true **for all** $k \in [a]_m$ it means that $[a]_m \subseteq [b]_m$.

To show $[b]_m \subseteq [a]_m$ let $\ell \in [b]_m$. By definition this means that $\ell \equiv b \bmod m$. Use *symmetry* on the present assumption of $a \equiv b \pmod m$ to get

$b \equiv a \,(\mathrm{mod}\, m)$. Use *transitivity* to get $\ell \equiv a \bmod m$, which means $\ell \in [a]_m$. Since this is true **for all** $\ell \in [b]_m$ it means that $[b]_m \subseteq [a]_m$.

Combine the two set inclusions to get $[a]_m = [b]_m$.

ii) Assume $a \not\equiv b \,(\mathrm{mod}\, m)$. Assume for a contradiction that $[a]_m \cap [b]_m \neq \varnothing$.

Thus we can choose $c \in [a]_m \cap [b]_m$. From this we have $c \in [a]_m$ and $c \in [b]_m$, i.e. $c \equiv a \bmod m$ and $c \equiv b \bmod m$. *Symmetry* on $c \equiv a \bmod m$ gives $a \equiv c \bmod m$ which combines by *transitivity* with $c \equiv b \bmod m$ to get $a \equiv b \bmod m$. This contradicts the assumption $a \not\equiv b \,(\mathrm{mod}\, m)$ so the last assumption above is false and thus $[a]_m \cap [b]_m = \varnothing$. ■

Part (i) of this result shows that a class can be labeled with *any* element from within it. So in the example above with $m = 3$, we have

$$[0]_3 = [3]_3 = [6]_3 = ... = [-9]_3 = ...$$

In general, by the Division Theorem, every $n \in \mathbb{Z}$ can be written as $n = qm + r$ for some $0 \leq r \leq m-1$, the *reduced residue* mod m. We often use the reduced residue to label the class, i.e. $[r]_m$, in place of $[n]_m$.

Further, if $0 \leq r_1 < r_2 \leq m-1$ then $1 \leq r_2 - r_1 \leq m-1$ and so $m \nmid (r_2 - r_1)$, i.e. $r_2 \not\equiv r_1 \,(\mathrm{mod}\, m)$. By part ii of the Theorem above this means that $[r_2]_m$ and $[r_1]_m$ are disjoint.

Hence in the set $\{[r]_m : 0 \leq r \leq m-1\}$ we see each congruence class *once*, and *only* once.

Definition 4.1.4 *We write* $\mathbb{Z}_m$ *for the set of congruence classes* mod m.

Example 4.1.5

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}.$$

But we could equally have written

$$\mathbb{Z}_3 = \{[3]_3, [7]_3, [11]_3\}$$

since $[3]_3 = [0]_3$, $[7]_3 = [1]_3$ *and* $[11]_3 = [2]_3$.

To be consistent we label each class with the least non-negative remainder, so

$$\mathbb{Z}_m = \{[r]_m : 0 \leq r \leq m-1\}.$$

Example 4.1.6 $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$.

Since we can add and multiply elements of $\mathbb{Z}$ we can define addition and multiplication on $\mathbb{Z}_m$.

Definition 4.1.7 *For $a, b \in \mathbb{Z}$ define*

$$[a]_m + [b]_m = [a+b]_m\,, \tag{1}$$

and

$$[a]_m \times [b]_m = [a \times b]_m\,. \tag{2}$$

Example 4.1.8

$$[7]_{10} + [8]_{10} = [15]_{10} = [5]_{10}$$

and

$$[7]_{10} \times [8]_{10} = [56]_{10} = [6]_{10}\,.$$

This definition of addition and multiplication on $\mathbb{Z}_m$ might seem to depend on the choice of labels for the classes. The next result shows this is not the case. The following result is, in fact, simply a reinterpretation of the earlier Theorem on Modular Arithmetic.

Theorem 4.1.9 *Addition and multiplication on $\mathbb{Z}_m$ are "well-defined".*
If $[a]_m = [a']_m$ and $[b]_m = [b']_m$ then

$$\begin{aligned} [a]_m + [b]_m &= [a']_m + [b']_m \\ \textit{and } [a]_m \times [b]_m &= [a']_m \times [b']_m\,. \end{aligned}$$

Thus it does not matter what label we choose for a class.

Proof p.256. Since different labels for the same congruence class $\bmod m$ are congruent $\bmod m$ we have

$$\begin{aligned} [a]_m &= [a']_m \Rightarrow a \equiv a' \bmod m \\ [b]_m &= [b']_m \Rightarrow b \equiv b' \bmod m. \end{aligned}$$

The earlier Theorem on Modular Arithmetic implies $a+b \equiv a'+b' \bmod m$ which in turn implies $[a+b]_m = [a'+b']_m$. Then

$$\begin{aligned} [a]_m + [b]_m &= [a+b]_m \quad \text{by (1)} \\ &= [a'+b']_m \\ &= [a']_m + [b']_m \quad \text{again by (1)}\,. \end{aligned}$$

Similarly, Modular Arithmetic implies $a \times b \equiv a' \times b' \bmod m$ which in turn implies $[a \times b]_m = [a' \times b']_m$. Then

$$\begin{aligned} [a]_m \times [b]_m &= [a \times b]_m \quad \text{by (2)} \\ &= [a' \times b']_m \\ &= [a']_m \times [b']_m \quad \text{again by (2)}. \end{aligned}$$

■

If we express the result of addition or multiplication as a class $[r]_m$ with label $0 \leq r \leq m-1$ we can write all results in a ***multiplication table*** (even if the operation is addition!).

Examples $(\mathbb{Z}_4, +)$

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$(\mathbb{Z}_4, \times)$

$\times$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

Aside In this table we see something never seen in $(\mathbb{Z}, \times)$, namely that we can multiply two non-zero objects and get zero! For example $[2]_4 \times [2]_4 = [0]_4$. Here, $[2]_4$ is an example of ***divisors of zero***.

$(\mathbb{Z}_8, \times)$ *Not given in the lectures because of size*

$\times$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$
$[1]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[2]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$
$[3]_8$	$[0]_8$	$[3]_8$	$[6]_8$	$[1]_8$	$[4]_8$	$[7]_8$	$[2]_8$	$[5]_8$
$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$
$[5]_8$	$[0]_8$	$[5]_8$	$[2]_8$	$[7]_8$	$[4]_8$	$[1]_8$	$[6]_8$	$[3]_8$
$[6]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$
$[7]_8$	$[0]_8$	$[7]_8$	$[6]_8$	$[5]_8$	$[4]_8$	$[3]_8$	$[2]_8$	$[1]_8$

Again we have divisors of zero, i.e. $[4]_8$ and $[6]_8$.

Notation If, in a problem, we are working throughout with one modulus m we often drop the $[..]_m$ and write simply r in place of $[r]_m$. See section 21.3 of PJE for a discussion of the map $[r]_m \longmapsto r$. If we want to be reminded of the modulus we often write $r_1 +_m r_2$ and $r_1 \times_m r_2$ in place of $[r_1]_m + [r_2]_m$ and $[r_1]_m \times [r_2]_m$ respectively.

Example 4.1.10 *We have not given the table for* $(\mathbb{Z}_8, \times)$ *because it is too large. But consider the subset* $\{[0]_8, [2]_8, [4]_8, [6]_8\} \subseteq \mathbb{Z}_8$. *The multiplication table modulo 8 for this subset is*

$\times$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$
$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$
$[2]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$
$[4]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$
$[6]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$

We can fill in this table using the elements from the set $\{[0]_8, [2]_8, [4]_8, [6]_8\}$ *because the product of two even integers is even.*

We say that the set $\{[0]_8, [2]_8, [4]_8, [6]_8\}$ *is* ***closed*** *under multiplication modulo 8.*

Example 4.1.11 *The set* $\{[2]_8, [4]_8, [6]_8\}$ *is* ***not*** *closed under multiplication modulo 8. For example,* $[2]_8 \times [4]_8 = [0]_8$ *which is not in the set. That is, we*

cannot complete the table

$\times$	$[2]_8$	$[4]_8$	$[6]_8$
$[2]_8$	$[4]_8$	?	$[4]_8$
$[4]_8$	?	?	?
$[6]_8$	$[4]_8$	?	$[4]_8$

Example 4.1.12 *The set* $\{[2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}$ *is a closed subset of* $(\mathbb{Z}_{10}, \times)$.

Verification

$\times$	$[2]_{10}$	$[4]_{10}$	$[6]_{10}$	$[8]_{10}$
$[2]_{10}$	$[4]_{10}$	$[8]_{10}$	$[2]_{10}$	$[6]_{10}$
$[4]_{10}$	$[8]_{10}$	$[6]_{10}$	$[4]_{10}$	$[2]_{10}$
$[6]_{10}$	$[2]_{10}$	$[4]_{10}$	$[6]_{10}$	$[8]_{10}$
$[8]_{10}$	$[6]_{10}$	$[2]_{10}$	$[8]_{10}$	$[4]_{10}$

As soon as we have operations such as addition and multiplication we have equations with unknowns.

Theorem 4.1.13 *The equation*

$$[a]_m \times [x]_m = [c]_m$$

has a solution in $\mathbb{Z}_m$ *if, and only if* $\gcd(a, m) | c$.

Proof Recall from the theory of linear Diophantine equations with two unknowns that

$$\begin{aligned}
\gcd(a, m) | c &\Leftrightarrow ax + my = c \quad \text{has solutions with } x, y \in \mathbb{Z} \\
&\Leftrightarrow ax \equiv c \bmod m \quad \text{has solutions with } x \in \mathbb{Z} \\
&\Leftrightarrow [ax]_m = [c]_m \quad \text{has solutions with } x \in \mathbb{Z} \\
&\Leftrightarrow [a]_m [x]_m = [c]_m \quad \text{has solutions with } [x]_m \in \mathbb{Z}_m.
\end{aligned}$$

■

Definition 4.1.14 • *An element* $[a]_m$ *of* $\mathbb{Z}_m$ *is an* ***invertible element*** *if there exists* $[a']_m$ *such that*

$$[a]_m [a']_m = [1]_m .$$

- *We say that* $[a']_m$ *is the* ***inverse*** *of* $[a]_m$ *and write* $[a']_m = [a]_m^{-1}$.
- *We write* $\mathbb{Z}_m^*$ *for the set of invertible elements in* $\mathbb{Z}_m$.

Example In the last Chapter we found that 53 had inverse 5 modulo 93. Thus $[53]_{93} \in \mathbb{Z}_{93}$ is invertible with inverse $[5]_{93}$, i.e. $[53]_{93}^{-1} = [5]_{93}$. Hence $[53]_{93} \in \mathbb{Z}_{93}^*$. Similarly $[5]_{93} \in \mathbb{Z}_{93}^*$.

Question What does $\mathbb{Z}_m^*$ look like?

Theorem 4.1.15 $[a]_m$ *is invertible if, and only if,* $\gcd(a, m) = 1$.

Proof The class $[a]_m$ is invertible iff $[a]_m [x]_m = [1]_m$ is soluble which, by the Theorem above, is soluble iff $\gcd(a, m) | 1$ iff $\gcd(a, m) = 1$ iff a and m are coprime. ■

So we can write

$$\mathbb{Z}_m^* = \{[r]_m : 1 \leq r \leq m, \gcd(r, m) = 1\}.$$

Note The set $\mathbb{Z}_m^*$ is **not** discussed in PJE.

Example (i) $\mathbb{Z}_5^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ and the multiplication table for $(\mathbb{Z}_5^*, \times)$ is

$\times$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

It is easy to read off inverses from a table, so

$$[1]_5^{-1} = [1]_5, \quad [2]_5^{-1} = [3]_5, \quad [3]_5^{-1} = [2]_5 \quad \text{and} \quad [4]_5^{-1} = [4]_5.$$

(ii) $\mathbb{Z}_8^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ and the multiplication table for $(\mathbb{Z}_8^*, \times)$ is

$\times$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[1]_8$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[3]_8$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$[5]_8$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$[7]_8$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

This time we see that every element is a **self inverse**. So in some fundamental way the tables for $(\mathbb{Z}_8^*, \times)$ and $(\mathbb{Z}_5^*, \times)$ are different.

Aside What of the tables for $(\mathbb{Z}_5^*, \times)$ and $(\mathbb{Z}_4, +)$, written as

$\times$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

and

$+$	$[0]_4$	$[1]_4$	$[3]_4$	$[2]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[3]_4$	$[2]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[0]_4$	$[3]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[2]_4$	$[1]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[1]_4$	$[0]_4$

do they not have the same "form"? As an advert for future courses on Algebraic Structures, they look at different algebraic structures on sets, attempting to answer difficult questions such as how many are there on a given set and how to recognise if two given structures are the same or different.

Theorem 4.1.16 *For all $m \in \mathbb{N}$, $(\mathbb{Z}_m^*, \times)$ is a closed subset of $(\mathbb{Z}_m, \times)$.*

Proof Let $[a]_m$ and $[b]_m \in \mathbb{Z}_m^*$. This means they have inverses, i.e. there exist $[a]_m^{-1}$ and $[b]_m^{-1} \in \mathbb{Z}_m^*$ for which $[a]_m [a]_m^{-1} = [1]_m$ and $[b]_m [b]_m^{-1} = [1]_m$. Consider

$$\begin{aligned} \left([a]_m [b]_m\right)\left([b]_m^{-1} [a]_m^{-1}\right) &= [a]_m \left([b]_m [b]_m^{-1}\right) [a]_m^{-1} \\ &= [a]_m [1]_m [a]_m^{-1} \\ &= [a]_m [a]_m^{-1} = [1]_m . \end{aligned}$$

Thus $[a]_m [b]_m$ has an inverse $[b]_m^{-1} [a]_m^{-1}$, and is therefore invertible. Hence $[a]_m [b]_m \in \mathbb{Z}_m^*$. ■

Aside As another observation we see that in $\{[2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}, \times\}$, $(\mathbb{Z}_8^*, \times)$ and $(\mathbb{Z}_5^*, \times)$ we have the nice property that in every row and every column every element occurs once and only once. This property was not seen in $(\mathbb{Z}_8, \times)$ nor $(\{[0]_8, [2]_8, [4]_8, [6]_8\}, \times_8)$.

Finally, from Chapter 4 we have as part of a Theorem: If $\gcd(a, m) = 1$ then

$$ab_1 \equiv ab_2 \bmod m \text{ if, and only if, } b_1 \equiv b_2 \bmod m.$$

In terms of congruence classes this becomes

Cancellation Law in $\mathbb{Z}_m^*$. For $[a]_m, [b_1]_m, [b_2]_m \in \mathbb{Z}_m^*$, if

$$[a]_m [b_1]_m = [a]_m [b_2]_m$$

then $[b_1]_m = [b_2]_m$.