# 1 $\mathbb{Z}_{11}$ and ISBN numbers

As explained earlier, $\mathbb{Z}_{11}$ is a set consisting of 11 members, namely, the integers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ and 10.

The members of $\mathbb{Z}_{10}$ are called ***digits***. The members of $\mathbb{Z}_2$ are called ***bits***. By analogy with these two widely used names, we are going to call the members of $\mathbb{Z}_{11}$ ***elvits***. So an ***elvit*** is one of the numbers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. Notice that ***there are eleven elvits***.

## 1.1 ISBN numbers

**ISBN** numbers are used to catalog and identify books. Each book has an ISBN number.

**An ISBN number is a sequence**

$$(m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9, m_{10})$$

**of ten elvits.** When we work with ISBN numbers, the name of the elvit "10" is "$X$", so

$$\mathbb{Z}_{11} = \Big\{\, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X \,\Big\}\,.$$

The first nine of these ten elvits are required to belong to the set $\Big\{\, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \Big\}$, so $m_{10}$ is the only elvit in an ISBN number that is permitted to have the value $X$.

Furthermore, $m_{10}$ is a **redundant symbol**, included for error-correcting purposes. It is always given by the formula

$$m_{10} = \sum_{j=1}^{9} j m_j\,, \tag{1.1.1}$$

that is,

$$m_{10} = m_1 + 2m_2 + 3m_3 + 4m_4 + 5m_5 + 6m_6 + 7m_7 + 8m_8 + 9m_9\,.$$

Why do we use $\mathbb{Z}_{11}$ rather than $\mathbb{Z}_{10}$? And why do we use Equation (1.1.1)? I will explain this eventually. But before we do that, let us verify the formula for some books.

EXAMPLE 1. Our textbook has the ISBN number 0534399002. Let us verify (1.1.1), making sure we remember that we are working in $\mathbb{Z}_{11}$, so all

the operations are performed modulo 11.

$$\begin{aligned}
&m_1 + 2m_2 + 3m_3 + 4m_4 + 5m_5 + 6m_6 + 7m_7 + 8m_8 + 9m_9 \\
&\quad = \quad 0 + 2 \times 5 + 3 \times 3 + 4 \times 4 + 5 \times 3 + 6 \times 9 + 7 \times 9 + 8 \times 0 + 9 \times 0 \\
&\quad = \quad 0 + X + 9 + 5 + 4 + X + 8 + 0 + 0 \\
&\quad = \quad 0 + 10 + 9 + 5 + 4 + 10 + 8 + 0 + 0 \qquad \text{reduced modulo 11} \\
&\quad = \quad 46 \qquad \text{reduced modulo 11} \\
&\quad = \quad 2\,.
\end{aligned}$$

So it works!

EXAMPLE 2. The book "An Introduction to Analysis," by William R. Wade, has the ISBN number 0-13-093089-X. Let us verify (1.1.1).

$$\begin{aligned}
&m_1 + 2m_2 + 3m_3 + 4m_4 + 5m_5 + 6m_6 + 7m_7 + 8m_8 + 9m_9 \\
&\quad = \quad 0 + 2 \times 1 + 3 \times 3 + 4 \times 0 + 5 \times 9 + 6 \times 3 + 7 \times 0 + 8 \times 8 + 9 \times 9 \\
&\quad = \quad 0 + 2 + 9 + 0 + 45 + 18 + 0 + 64 + 81 \\
&\quad = \quad 11 + 1 + 7 + 9 + 4 \\
&\quad = \quad 1 + 7 + 9 + 4 \\
&\quad = \quad 21 \\
&\quad = \quad 10 \\
&\quad = \quad X\,.
\end{aligned}$$

Once again, it works!

I suggest you look at a few books that you can find at home or in the library, look at heir ISBN numbers, and check that in all cases Formula (1.1.1) is true.

Now that you are convinced that ISBN numbers do indeed obey Formula (1.1.1), the three questions that you ought to be asking yourself are:

1. *Why do we use* $\mathbb{Z}_{11}$*?,*
2. *Why do we include* $m_{10}$*, which contains absolutely no new information, since it is completely determined by the first* 9 *elvits?,*
3. *Why do we use Formula (1.1.1)?*

*You will get the answers to these questions a little bit further in this handout.* But it would be a good idea if you started thinking about them right now. Here is a hint:

The crucial distinction is that $\mathbb{Z}_{11}$ ***is a field, but*** $\mathbb{Z}_{10}$ ***is not.***

## 1.2 What is a field?

A ***field*** is a system $\mathbb{F}$ of objects on which are specified (1) members 0 and 1 of $\mathbb{F}$, and (2) binary operations of addition (sending $x, y$ to $x+y$), subtraction (sending $x, y$ to $x-y$), multiplication (sending $x, y$ to $x \times y$, or $x \cdot y$), and division (sending $x, y$ to $\frac{x}{y}$), in such a way that the 13 axioms of "The axioms of arithmetic, Part I" (that is, the axioms of arithmetic that deal with 0, 1, addition, subtraction, multiplication, and division) are satisfied, if you put $\mathbb{F}$ instead of $\mathbb{R}$.

## 1.3 Why is $\mathbb{Z}_{10}$ not a field?

The number system $\mathbb{Z}_{10}$ is not a field because in it is not true that "every number which is not equal to zero has a multiplicative inverse." Or, in symbols, if you prefer, the statement

$$(\forall x)(x \neq 0 \Rightarrow (\exists y)x \cdot y = 1)$$

is not true in $\mathbb{Z}_{10}$.

How do we know that this is not true? Let us find a counterexample. I will show that $x = 2$ is a counterexample. I have to show that

$$2 \neq 0 \Rightarrow (\exists y)2 \cdot y = 1$$

isn't true. Notice that "$2 \neq 0$" *is* true, fortunately for us. (Why "fortunately for us"? Because if "$2 \neq 0$" wasn't true, then the implication that we are trying to prove, which says that "$2 \neq 0 \Rightarrow (\exists y)2 \cdot y = 1$," would be true!)

Since "$2 \neq 0$" is true, what we need is to prove that "$(\exists y)2 \cdot y = 1$" isn't true. Let us do it *by contradiction.* Suppose that there exists such a $y$. Pick one and call it $\bar{y}$. Then $2 \cdot \bar{y} = 1$ in $\mathbb{Z}_{10}$. This means that in $\mathbb{Z}$ the number $2 \cdot \bar{y}$ is equal to a multiple of 10 plus 1. But a multiple of 10 plus 1 must be odd, and $\bar{y}$ is even. So we have reached a contradiction, $y$ doesn't exist, and we are done. **END OF PROOF**

**ANOTHER PROOF:** In a field, it must be true that

$$(\forall x)(\forall y)(x \cdot y = 0 \Rightarrow (x = 0 \vee y = 0))\,. \tag{1.3.2}$$

(*Proof:* Let $a, b$ be arbitrary members of our field. Suppose that $a \cdot b = 0$. We want to show that $a = 0 \vee b = 0$

Clearly, either $a = 0$ or $a \neq 0$. We consider the two cases separately. If $a = 0$ then of course $a = 0 \vee b = 0$, so the conclusion we want holds. If

$a \neq 0$, then $\frac{1}{a}$ exists, and satisfies $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$. So

$$b = 1 \cdot b = \Big(\frac{1}{a} \cdot a\Big) \cdot b = \frac{1}{a} \cdot \Big(a \cdot b) = \frac{1}{a} \cdot 0 = 0\,.$$

(In the above calculation, we have used, in the last step, the fact that $\forall x) x \cdot 0 = 0$. This was proved in full detail in the "Homework No. 8" handout. Notice that the proof gien there only uses the field axioms, so it is valid in every field.) Therefore $a = 0 \vee b = 0$ in this case as well.

So we have seen that the conclusion that $a = 0 \vee b = 0$ holds in both cases, when $a = 0$ and when $a \neq 0$. Hence the Proof by Cases Rule tells us that

$$a = 0 \vee b = 0\,.$$

Since this was true for arbitrary members of our field, we have established (1.3.2).

Now that we know that (1.3.2) is true in any field, let us apply it to $\mathbb{Z}_{10}$. Supppose $\mathbb{Z}_{10}$ was a field. Then (1.3.2) would be true. In particular, we could apply it with $x = 2$, $y = 5$ and conclude that

$$2 \cdot 5 = 0 \Rightarrow (2 = 0 \vee 5 = 0))\,.$$

But, in $\mathbb{Z}_{10}$, $2 \cdot 5$ is equal to 0. So $2 = 0 \vee 5 = 0$. But "$2 = 0 \vee 5 = 0$" is false, because neither 2 nor 5 is equal to zero. (Here it is important that we are working in $\mathbb{Z}_{10}$. If we were working in $\mathbb{Z}_5$, for example, it would still be true that $2 \cdot 5 = 0$, but this woulkd cause no problem, since in $\mathbb{Z}_5$ 5 is equal to 0.) So we have reached a contradiction, showing that $\mathbb{Z}_{10}$ is not a field.

## 1.4 Why is $\mathbb{Z}_{11}$ a field?

Let us show that, at least, it is true that "every nonzero member of $\mathbb{Z}_{11}$ has a multiplicative inverse." Here is the proof:

$$\begin{aligned}
1 \times 1 &= 1\\
2 \times 6 &= 1\\
3 \times 4 &= 1\\
4 \times 3 &= 1\\
5 \times 9 &= 1\\
6 \times 2 &= 1\\
7 \times 8 &= 1
\end{aligned}$$

$$\begin{aligned} 8 \times 7 &= 1 \\ 9 \times 5 &= 1 \\ 10 \times 10 &= 1\,. \end{aligned}$$

Now, to prove that $\mathbb{Z}_{11}$ is a field we also have to prove all the other field axioms, such as, for example, the commutative law of addition (i.e., $(\forall x \in \mathbb{Z}_{11})(\forall y \in \mathbb{Z}_{11})x + y = y + x$), and many other things.

I leave that up to you, if you feel like doing it. But the main part is the existence of multiplicative inverses, because this is what makes $\mathbb{Z}_{11}$ different from, say $\mathbb{Z}_{10}$ or $\mathbb{Z}_{12}$.

## 1.5 Why do we use elvits for ISBN numbers?

In principle, we would like an ISBN number to consist of nine digits. (This would allow us to have a total of $10^9$—i.e. one billion—ISBN numbers, which presumably is more than the number of books ever published or to be published up to, say, the year 2100. For example, as this is being written, the U.S. Library of Congress has 14 million books, and a total of 88 million items including manuscripts, maps, music, art prints, photographs, motion pictures, videotapes, newspapers, pamphlets, recordings and other materials.)

Now, as you well know, ISBN numbers are transmitted, copied, rewritten, etc. Each of these operations can introduce ***transmission errors***. So it is customary to introduce some ***redundancy*** into a signal to use it to ***check for errors***. (For example, when you change your password for a computer system you use, you are asked to type in the new password and then to type it in again. In principle, if you type it in correctly the first time, there is no need to type it in again, because this would convey no new information. However, if you made a mistake the first time you typed it in, you will almost certainly type in a different string of symbols the second time, because it is extremely unlikely that you will make exactly the same mistake the second time. And then the computer will know that you made a mistake somewhere, and ask you start all over again.)

For ISBN numbers, we introduce redundancy by adding an extra symbol that carries no new information but will enable us to detect the most frequent types of errors. A simple example of how this could be done, if we were using $\mathbb{Z}_{10}$, would be to take $m_{10}$ to be the sum of the other 9 digits, i.e., to take

$$m_{10} = m_1 + m_2 + m_3 + m_4 + m_5 + m_6 + m_7 + m_8 + m_9\,. \tag{1.5.3}$$

***This would detect errors consisting of getting one digit wrong.***

(Indeed, if you make a mistake in one of your first nine digits, that will change the sum, so the tramsitted $m_{10}$ will no longer satisfy (1.5.3). For example, if the correct $m_5$ is 2, and you send a 7 instead, then the sum $m_{10}$ will be increased by 5 in $\mathbb{Z}_{10}$.)

Naturally, ***this method will not detect more complicated errors such as, for example, if you send two wrong symbols.*** (For example, if the correct string is 0636274165, and you send is 0686774165 instead, getting two digits wrong, then (1.5.3) will still hold, because the errors in $m_3$ and $m_5$ are both 5, so their sum in $\mathbb{Z}_{10}$ is 0.) But two mistakes are a lot less likely than one mistake, so this imperfect method will enable us to detect most errors, even though some errors will still go undetected.

Another limitation of the method is that it will detect errors but ***it will not tell you how to correct them,*** because you will not know which digit is wrong. (For example, if you receive the string 0636774165, then you know for sure that it has to be wrong, because $0+6+3+6+7+7+4+1+6 = 0$—in $\mathbb{Z}_{10}$—whereas $m_{10} = 5$, so (1.5.3) is not true. But you do not know which digit was wrong.) Again, this is a limitation of the method that we are willing to accept, because once we know that there is a mistake we can ask the sender to send us the number again.

The real problem is that there is another very common type of error that this method will not detect, namely, ***transposition errors***, in which two symbols get exchanged. (For example, if the correct 9-digit string is 0636274165, and you send instead 0616274365, so that $m_3$ and $m_7$ are interchanged, the sum of (1.5.3) will be the same.)

If we want to detect transposition errors as well as the simpler ones consisting of getting one symbol wrong, then we need a formula

$$m_{10} = a_1m_1 + a_2m_2 + a_3m_3 + a_4m_4 + a_5m_5 + a_6m_6 + a_7m_7 + a_8m_8 + a_9m_9\,, \tag{1.5.4}$$

where the coefficients $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ are all different. But then, if we insist on working in $\mathbb{Z}_{10}$, and we use (1.5.4) taking the coefficients $a_j$ to be all different, we run into another difficulty: at least one of the $a_j$ will have to be even (why?), and then $5a_j = 0$ in $\mathbb{Z}_{10}$, which means that if we make an error of 5 in the $j$-th digit, then we will not detect this error. In other words: ***if we work in*** $\mathbb{Z}_{10}$ ***there is no way to add an extra "error-detecting" digit*** $m_{10}$ ***given by a formula (1.5.4) so that we will detect both (a) errors in the transmission of a single digit, and (b) transposition errors.***

On the other hand, let me prove to you that ***in*** $\mathbb{Z}_{11}$ ***it is possible to add an extra "error-detecting" digit*** $m_{10}$ ***given by a formula***

***(1.5.4) so that we will detect both (a) errors in the transmission of a single digit, and (b) transposition errors.*** Indeed, we can use the formula that is actually used in real life, namely,

$$m_{10} = m_1 + 2m_2 + 3m_3 + 4m_4 + 5m_5 + 6m_6 + 7m_7 + 8m_8 + 9m_9\,. \quad (1.5.5)$$

Notice that this corresponds to taking $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 4$, $a_5 = 5$, $a_6 = 6$, $a_7 = 7$, $a_8 = 8$, $a_9 = 9$. These are 9 different elvits, and this is exactly as it should be, since we have already seen that in order to detect transposition errors you do need that $a_j$ to be all different.

I will now prove to you rigorously (with your help) that ***if the*** $m_j$ ***are elvits chosen so that (1.5.5) holds, then every error consisting of one wrong elvit or two transposed elvits will be detected.***

Here is the first half of the proof. Consider the first type of error, namely, one wrong elvit. Let $j$ be the place where this error is made, so $j$ is one of the numbers $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ and the correct elvit $m_j$ is replaced by the wrong elvit $\tilde{m}_j$, but all the other elvits $m_i$ (for $i \neq j$) are correct. Let us deal separately with the cases when $j < 10$ and $j = 10$. If $j < 10$, then the right-hand side $m_{10}^{computed}$ of (1.5.5) computed from the transmitted elvits will be $m_{10} + j(\tilde{m}_j - m_j)$, but the received 10-th elvit will be the correct $m_{10}$.

Since $j \neq 0$ and $\tilde{m}_j - m_j \neq 0$, the product $j(\tilde{m}_j - m_j)$ is also different from 0

so $m_{10}^{computed}$ will not be equal to $m_{10}$. This means that the received ten-elvit string will not satisfy (1.5.5), so the error will be detected.

Now let us look at the remaining case, when the wrong elvit is the tenth one. In that case, the transmitted $m_j$ (for $j = 1, 2, 3, 4, 5, 6, 7, 8, 9$) will be correct, but the transmitted value $\tilde{m}_{10}$ will be different from the true value $m_{10}$. The computed tenth elvit will be $m_{10}$, but the one received will be $\tilde{m}_{10}$, which is different. So once again the error will be detected.

This completes the first half of the proof, having to do with detecting errors in the transmission of a single elvit. Now we have to do the second part, namely, prove that the formula used in real life also detects transposition errors. *I am leaving this part of the proof for you to do!*

Let me give you an example. Suppose the correct ISBN number for a book is 0534399002, but a transmission error is made and the number actually sent is 0539349002. (This is a *transposition error*. The 4 and the first 9 are transposed.) Now the transmitted $m_{10}$ is 2, but the $m_{10}$ computed using Formula (1.5.5) is

$$1 \times 0 + 2 \times 5 + 3 \times 3 + 4 \times 9 + 5 \times 3 + 6 \times 4 + 7 \times 9 + 8 \times 0 + 9 \times 0\,,$$

that is,

$$0 + 10 + 9 + 36 + 15 + 24 + 63 + 0 + 0 \qquad \text{reduced modulo } 11\,,$$

which is equal to

$$19 + 3 + 4 + 2 + 8 \qquad \text{reduced modulo } 11\,,$$

i.e., to 3. So our transposition error resulted in a computed $m_{10}$ equal to 3, which is different from the transmitted $m_{10}$, whose value was 2. So we have detected the error.

Why did this work? Because, in the sum

$$1 \times 0 + 2 \times 5 + 3 \times 3 + 4 \times 4 + 5 \times 3 + 6 \times 9 + 7 \times 9 + 8 \times 0 + 9 \times 0\,,$$

which we would have used for the correct ISBN number, the terms $4 \times 4$ and $6 \times 9$ got replaced by $4 \times 9$ and $6 \times 4$, so that the contribution of these two terms to the total sum has been incremented by

$$(4 \times 9 + 6 \times 4) - (4 \times 4 + 6 \times 9)\,,$$

that is, by

$$(6 - 4) \times 4 + (4 - 6) \times 9)\,,$$

which is equal to $(6-4)\times(4-9)$. In other words, *the effect of the transposition is to change $m_{10}$ by the product $\mu \times \nu$, where $\mu$ is the difference between the indices of the elvits that were transposed (for example, if you transpose $m_i$ and $m_j$, and $i < j$, then $\mu = j - i$), and $\nu$ is the difference between the actual values of the elvits that were transposed (for example, if you transpose $m_i$ and $m_j$, and $i < j$, then $\mu = m_i - m_j$).* The crucial point is that $\mu$ is always $\neq 0$ (in $\mathbb{Z}_{11}$), and $\nu$ is always $\neq 0$ (because if $m_i = m_j$ and you transpose $m_i$ and $m_j$ then there is no error). So ***the important thing is that the inequalities*** $\mu \neq 0$ ***and*** $\nu \neq 0$ ***imply*** $\mu \times \nu \neq 0$***, which is true in*** $\mathbb{Z}_{11}$ ***because*** $\mathbb{Z}_{11}$ ***is a field.***

PROBLEM 1 (ON $\mathbb{Z}_{11}$): Write a detailed proof that Formula (1.5.5) for ISBN numbers detects transposition errors, along the lines of the previous paragraph. That is, prove the following: if a sequence $\mathbf{m} = (m_1, m_2, \cdots, m_{10})$ of ten elvits satisfies (1.5.5) then any sequence of $\tilde{\mathbf{m}}$ obtained from $\mathbf{m}$ by exchanging two different elvits (that is, any $\tilde{m} = (\tilde{m}_1, \tilde{m}_2, \cdots, \tilde{m}_{10})$ such that, for some $i, j$ for which $i \neq j$ and $m_i \neq m_j$, we have $\tilde{m}_k = m_k$ if $j \neq k \neq i$, $\tilde{m}_i = m_j$ and $\tilde{m}_j = m_i$) will fail to satisfy (1.5.5). (WARNING: you will have to be careful and consider separately two types of interchanges, namely, those that do not involve $m_{10}$ and those that do. Alternatively, there is a cute trick that will enable you to deal with both cases in one swoop. See if you can figure it out. *Hint: In* $\mathbb{Z}_{11}$, $-a = X \cdot a$ *for all* $a$, *where, as we explained before,* $X$ *is the name of the number* 10 *in* $\mathbb{Z}_{11}$. *Apply this to* $m_{10}$.)

PROBLEM 2 (ON $\mathbb{Z}_{11}$): Suppose we wanted to increase the number of ISBN numbers by using 11 elvits instead of 10. That is, we would define an ISBN number to be a sequence $(m_1, m_2, \cdots, m_{10}, m_{11})$ of *eleven* elvits, and we would use the error-detecting formula

$$m_{11} = m_1 + 2m_2 + 3m_3 + 4m_4 + 5m_5 + 6m_6 + 7m_7 + 8m_8 + 9m_9 + Xm_{10}\,. \quad (1.5.6)$$

(Recall that $X$ is the name of 10 in $\mathbb{Z}_{11}$.) Would this still work to detect both types of errors?

### 1.6 A remark on fields

The crucial step in the proof of the first half of our theorem or the error-detecting properties of $\mathbb{Z}_{11}$-based ISBN numbers was the assertion that

$$\boxed{\text{In } \mathbb{Z}_{11}, \text{ if } a \neq 0 \text{ and } b \neq 0 \text{ then } a \times b \neq 0.}$$

How do we know that this is true? Well, you could check it directly, by trying all possible pairs of values of $a$ and $b$ (there are only 100 such pairs!) such that $a \in \mathbb{Z}_{11}$, $b \in \mathbb{Z}_{11}$, $a \neq 0$, $b \neq 0$, and verifying that in each case $a \times b \neq 0$.

A much easier way to see it is to remember that we ***proved*** this (cf. Page 3), not just for $\mathbb{Z}_{11}$, but for any field. Since $\mathbb{Z}_{11}$ is a field, the general result can be applied to $\mathbb{Z}_{11}$.

## 1.7 When is $\mathbb{Z}_n$ a field?

In a previous section, we proved that $\mathbb{Z}_{11}$ is a field by directly checking that every nonzero member of $\mathbb{Z}_{11}$ has a multiplicative inverse, that is, that

$$(\forall x \in \mathbb{Z}_{11})(x \neq 0 \Rightarrow (\exists y \in \mathbb{Z}_n)(x \times y = 1)) \,.$$

We did by checking every nonzero member of $\mathbb{Z}_{11}$ and,in each case, finding the multiplicative inverse. But this is a horrible and boring method! Suppose we wanted to check that $\mathbb{Z}_{101}$ is a field. We would have to list all 100 nonzero members of $\mathbb{Z}_{101}$ and for each one find a multiplicative inverse. And that would be a lot of work. So it is better to have a general theorem:

**THEOREM.** Assume that $n \in \mathbb{N}$ and $n > 1$. Then $\mathbb{Z}_n$ is a field if and only if $n$ is prime.

*Proof.* Assume first that $n$ is not prime. Let us prove that $\mathbb{Z}_n$ is not a field. Since $n$ is not prime, we can pick integers $k, \ell$ such that $k \cdot \ell = n$, $1 < k < n$, and $1 < \ell < n$. But then $k$ and $\ell$ are nonzero as members of $\mathbb{Z}_n$, but their product $k \times \ell$ is $\mathbb{Z}_n$ is equal to zero, since $k \cdot \ell = n$. Hence (1.3.2) is not true in $\mathbb{Z}_n$. But (1.3.2) is true in any field. So $\mathbb{Z}_n$ is not a field.

Now assume that $n$ is prime, and let us prove that $\mathbb{Z}_n$ is a field. As we already explained before, the crucial point is to prove that every nonzero member of $\mathbb{Z}_n$ has a multiplicative inverse, that is, that

$$(\forall x \in \mathbb{Z}_n)(x \neq 0 \Rightarrow (\exists y \in \mathbb{Z}_n)(x \times y = 1)) \,.$$

Let $a$ be an arbitrary nonzero member of $\mathbb{Z}_n$. Then $a \in \mathbb{N}$, $a > 0$, and $a < n$. Let $c$ be the greatest common divisor of $a$ and $n$. Then $c = 1$, because $n$ is prime. On the other hand, we know that the greatest common divisor of two integers is an integer linear combination of these two integers. So we may pick integers $u, v$ such that $ua + vn = 1$. Using the Division Theorem, pick integers $q, r$ such that $u = nq + r$ and $0 \leq r < n$. Then $r \in \mathbb{Z}_n$. Furthermore,

$$ra = (u - nq)a = ua - nqa = 1 - vn - nqa = 1 + (-v - qa)n \,.$$

But this means that $ra$, reduced modulo $n$, equals 1. Hence the product $r \times_n a$ (that is, the product of $r$ and $a$ in $\mathbb{Z}_n$), is equal to 1, so $r$ is the desired multiplicative inverse of $a$. $\diamondsuit$