Practice with Equivalence Relations
The Algebraic Systems $\mathbb{Z}_m$

Definition Suppose $m \in \mathbb{N}$. For integers $x, y \in \mathbb{Z}$, we say that

"x is congruent to y modulo m" iff $m|(y-x)$
iff (equivalently) $y - x$ is a multiple of m in $\mathbb{Z}$

We usually write this relation as $x \equiv_m y$ (although notations like $x = y \,(\text{mod}\, m)$,
$x \equiv y \,(\text{mod } m)$, and $x =_m y$ are also used).

We proved in class that $\equiv_m$ is an equivalence relation on $\mathbb{Z}$. Any two different equivalence classes are disjoint, and the union of the distinct equivalence classes is $\mathbb{Z}$ $-$ therefore we say that the collection of equivalence classes is a partition of $\mathbb{Z}$.

We also proved in class that x and y are in the same equivalence class iff they have the same remainder ($r = 0, 1, ...,$ or $m - 1$) when divided by m. This means that the relation $\equiv_m$ has m different equivalence classes: $[0]$, $[1]$, ..., $[m-1]$.

Example ($m = 4$) $x \equiv_4 y$ iff $y - x$ is a multiple of 4. Since "division by 4" has 4 possible remainders, every $x \in Z$ is congruent mod 4 to either $0, 1, 2$ or 3.

$$[0] = \{\ ...\ ,\ -12,\ -8,\ -4,\ 0, 4,\ 8,\ 12,\ ...\ \}$$
$$[1] = \{\ ...\ ,\ -11,\ -7,\ -3,\ 1, 5,\ 9,\ 13,\ ...\ \}$$
$$[2] = \{\ ...\ ,\ -10,\ -6,\ -2,\ 2, 6, 10,\ 14,\ ...\}$$
$$[3] = \{\ ...\ ,\ \ -9,\ -5,\ -1,\ 3, 7, 11, 15,\ ...\}$$

Recall that there are also other notations for equivalence classes: for example $[1]$, $\overline{1}$, *and* $1/\equiv_4$ *all refer to the same equivalence class.*

Of course $[-11] = [-7] = [-3] = [1] = [5] = [9] = ...$ are all names for the same equivalence class. The equivalence relation $\equiv_4$ "lumps together" all these equivalent numbers $...,\ -11,\ -7,\ -3,\ 1,\ 5,\ 9,\ ...$ and treats them as a single new object $-$ an equivalence class (that has many different names). Each integer $...,\ -11,\ -7,\ -3,\ 1,\ 5,\ 9, ...$ is called a representative of that equivalence class.

The collection of all equivalence classes of $\equiv_m$ is denoted $\mathbb{Z}_m$. So $\mathbb{Z}_m$ is a collection of sets: $\mathbb{Z}_m = \{\ [0],\ [1],\ ...,\ [m-1]\ \}$. For example, $\mathbb{Z}_4 = \{[0], [1],\ [2],\ [3]\ \}$.

It's useful to spend a little time thinking about these collections $\mathbb{Z}_m$ to get some practice working with equivalence relations and equivalence classes. But it turns out that the $\mathbb{Z}_m$'s also are interesting algebraic systems.

To create some "algebra" in $\mathbb{Z}_m$, we will define two operations called "addition modulo m" and "multiplication modulo m." For now, we will denote these operations by $\oplus$ and $\odot$ to avoid confusing them with the usual addition and multiplication in $\mathbb{Z}$.

Definition Suppose $m \in \mathbb{N}$. In the set $\mathbb{Z}_m$, define

i) $[x] \oplus [y] = [x + y]$ (Addition modulo m)
ii) $[x] \odot [y] = [x \cdot y]$ (Multiplication modulo m)

$($*the operations* $+$ *and* $\cdot$ *on the right are the usual addition and multiplication in* $\mathbb{Z}$.$)$

For example, in $\mathbb{Z}_4 = \{[0],\ [1],\ [2], [\,3]\}$

$$(*) \qquad \begin{cases} [2] \oplus [3] = [5] \ = [1] & \text{and} \\ [2] \odot [3] = [6] \ = [2] \end{cases}$$

In other words, we add ($\oplus$) equivalence classes by picking a representative of each class $(2,\ 3$ above), adding ($+$) the representatives in $\mathbb{Z}$ (to get 5), and then taking the equivalence class of the sum (to get $[5]$). We also multiply equivalence classes by choosing a representative from each equivalence class.

This raises an important issue: how do we know that the answer for a sum $\oplus$ or product $\odot$ doesn't depend on which representatives are chosen? For example, if “addition” $\oplus$ is to make any sense, $[2] \oplus [3]$ should always give the same answer, even if somebody does the calculation in a different way. For example, suppose Joe reasons in $\mathbb{Z}_4$:

$(**)$ $[2] = [14]$ and
$[3] = [7]$
so Joe computes: $2] \oplus [3] = [14] \oplus [7] = [21]$ and
$[2] \odot [3] = [14] \odot [7] = [98] = [2]$

Fortunately, $[21] = [1]$ and $[98] = [2]$ so the answers in $(*)$ and $(**)$ <u>are</u> the same.

But will it always work out this way? Are the results of addition ($\oplus$) or multiplication ($\odot$) always the same, whatever representatives from the equivalence classes are actually used in the calculations? The next theorem tells us the answer is “yes.”

Theorem Suppose $m \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$. If $a \equiv_{\,m} b$ and $c \equiv_{\,m} d$, then

i) $a + c \equiv_{\,m} b + d$
ii) $ac \equiv_{\,m} bd$

Phrased in terms of equivalence classes for $\equiv_{\,m}$ *, the theorem says that if* $[a] = [b]$ *and* $[c] = [d]$, *then*

i) $[a + c] = [b + d]$
ii) $[ac] = [bd]$

In other words if you calculate $[a] \oplus [c]$ *using* b *and* d *as the representatives for the equivalence classes, you get the same answer as when you use* a *and* c*:* $[a + c] = [b + d]$. *And similarly for multiplication.*

Proof By hypothesis, $b - a = km$ and $d - c = lm$ for some integers k, l.

Then i) $(b - a) + (d - c) = (b + d) - (a + c) = km + lm = (k + l)m$, so

$a + c \equiv_m b + d.$

And ii) $bd - ac = bd - bc + bc - ac = b(d - c) + c(b - a)$
$= b(lm) + c(km) = m(bl + ck)$, so

$ac \equiv_m bd.$ •

Mathematicians say that this theorem shows that $\oplus$ and $\odot$ are well-defined – meaning "independent of the representatives used from the equivalence classes." A theorem like this one needs to be proved every time a definition is given in terms of representatives chosen from various equivalence classes.

Example Suppose, in $\mathbb{Z}_4$, we "define" $[x] < [y]$ iff $x < y$.

Then John might say: $[2] < [3]$ is true, because $2 < 3$
And Mary might say: $[6] < [3]$ is false, because $6 \not< 3$.

But this is a real problem, because $[2] = [6]$!

This "definition" for a relation $<$ between equivalence classes in $\mathbb{Z}_m$ is not an acceptable definition because it depends on which representatives are chosen for the equivalence classes: in other words, $<$ is not well-defined in $\mathbb{Z}$. (*Sometimes "ill-defined" is used for "not well-defined*).

Corollary Suppose $m, n \in \mathbb{N}$. If $a \equiv_m b$, then $a^n \equiv_m b^n$.

Proof A complete proof would be done by induction. You can see the idea of how it works here.

We know that $\begin{cases} a \equiv_m b \\ a \equiv_m b \end{cases}$ If we multiply, the theorem gives $a^2 \equiv_m b^2$.

From $\begin{cases} a^2 \equiv_m b^2 \\ a \equiv_m b \end{cases}$ If we multiply, the theorem gives $a^3 \equiv_m b^3$.

Etc. (= "complete the argument by induction") •

Example Find the remainder when 2^{74} is divided by 63. Phrased another way: which equivalence class in $\mathbb{Z}_{63} = \{[0], [1], \ldots, [63]\}$ contains the integer 2^{74} ?

We know that $2^6 = 64 \equiv_{63} 1$. Therefore

$$\begin{aligned} &2^{72} = (2^6)^{12} \equiv_{63} (1)^{12} \equiv_{63} 1, \text{ so} \\ &2^{74} = 2^2(2^6)^{12} \equiv_{63} 2^2(1) \equiv_{63} 4. \end{aligned}$$

So 2^{74} has remainder 4 when divided by 63; equivalently, $2^{74} \in [4] \in \mathbb{Z}_{63}$.

(*Note: in writing down such a calculation, be sure to distinguish when you mean " $=$ " and when you mean $\equiv_m$; in particular, don't write "$a = b$" when the truth is "$a \equiv_m b$".*

Example What is the remainder r when 2^{30} is divided by 17?

Of course, $0 \leq r < 17$. Trying to simplify, we "reduce modulo 17" as much as we can $-$ replacing numbers with smaller, more manageable numbers (mod 17).

Noting that $2^4 \equiv_{17} (-1)$, we write $2^{30} = 2^2 2^{28} = 2^2(2^4)^7 \equiv_{17} 2^2(-1)^7 = -4$.

But $-4 \equiv_{17} 13$, so $2^{30} \equiv_{17} 13$. So 2^{30} has a remainder of 13 when divided by 17.

Example With the operations $\oplus$ and $\odot$, we can do "arithmetic" in $\mathbb{Z}_m$. We can easily write out the complete addition and multiplication tables in $\mathbb{Z}_4$ for example :

$\oplus$		**[0]**	**[1]**	**[2]**	**[3]**
[0]		$[0]$	$[1]$	$[2]$	$[3]$
[1]		$[1]$	$[2]$	$[3]$	[0]
[2]		$[2]$	[3]	[0]	$[1]$
[3]		$[3]$	$[0]$	$[1]$	$[2]$

$\odot$		**[0]**	**[1]**	**[2]**	**[3]**
[0]		$[0]$	$[0]$	$[0]$	$[0]$
[1]		$[0]$	$[1]$	$[2]$	$[3]$
[2]		$[0]$	$[2]$	$[0]$	$[2]$
[3]		$[0]$	$[3]$	$[2]$	$[1]$

Example Arithmetic in $\mathbb{Z}_{12} = \{[0], [1], \ldots, [11]\}$ is often referred to as "clock arithmetic." Why?

"Algebraic system" is a loose, general term for a set that has with one or more operations (called addition or multiplication) that work inside the set. Familiar examples of algebraic systems are $\mathbb{N}$, ω, $\mathbb{Q}, \mathbb{R},$ and $\mathbb{C}$ (the complex numbers). But now we also have examples of infinitely many other algebraic systems $\mathbb{Z}_m$ $-$ one for each $m \in \mathbb{N}$.

Why is $\mathbb{P}$, the set of irrationals, not an algebraic system with addition and multiplication?

We want to spend a little more time examining the algebraic structures $\mathbb{Z}_m$, but first we are going to digress to look, more generally, at two sets axioms that apply to a lot of "nice" algebraic systems. (*Actually, the second set of axioms is the same as the first with just one more axiom added.* From these axioms, we can prove theorems about "how to do algebra" in these systems. The beauty of this approach is that the theorems we are true in <u>every</u> algebraic system for which the axioms are true. So efficiency is one reason for the digression.

The axioms in the first set are numbered F1, F1$'$, ..., F5, F5$'$, F6. They are all true when interpreted as statements about any of the algebraic systems $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}_m$ (for <u>every</u> $m \in \mathbb{N}$). Any definitions we make or theorems we prove from these axioms apply equally well in every one of these algebraic systems. So, for example, we don't have to waste time proving results about "how algebra works" separately for each of the systems $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, ..., $\mathbb{Z}_{666}$, ...

To state the axioms, suppose that we have an algebraic system that consists of a set F and two operations called addition and multiplication defined inside F. In stating the axioms these operations are written as $+$ and $\cdot$, but in a specific example other symbols (such as $\oplus$ and $\odot$ in $\mathbb{Z}_m$) might be used instead. Notice that several of the axioms come in "pairs" – one part for addition, the other for multiplication.

F1) There are elements $0 \in F$ and $1 \in F$ (and $0 \neq 1$)
(*so the system has at least two elements*)

F2) $\forall x \forall y \forall z \ \ (x + y) + z = x + (y + z)$ F2$'$) $\forall x \forall y \ \forall z \ \ (x \cdot y) \cdot z = x \cdot (y \cdot z)$
(*addition and multiplication are associative*)

F3) $\forall x \forall y \ \ x + y = y + x$ F3$'$) $\forall x \forall y \ \ x \cdot y = y \cdot x$
(*addition and multiplication are commutative*)

F4) $\forall x \forall y \forall z \ \ x \cdot (y + z) = x \cdot y + x \cdot z$
(*the distributive law connects addition and multiplication*)

F5) $\forall x \ \ x + 0 = x$ F5$'$) $\forall x \ \ x \cdot 1 = x$
(*0 and 1 are "neutral" elements for addition and multiplication.* 0 *is called the* <u>*additive identity element*</u> *and* 1 *is called the* <u>*multiplicative identity element*</u> *in* F)

<u>Notice</u> that all of the axioms, so far, are satisfied in the system of whole numbers $\omega = \{0, 1, 2, ... \}$. This is because of how we defined $+$ and $\cdot$ in ω , and because of theorems we proved in ω (such as commutativity and associativity for addition and multiplication). This means that any theorem we prove using just the Axioms F1-F5$'$ would be valid theorems about ω or any other algebraic system satisfying these axioms. (*However, some of the axioms F1-F5$'$ are* <u>*not*</u> *true in* $\mathbb{N}$ *– which ones are not true in* $\mathbb{N}$*?*)

F6) $\forall x \, \exists y \ \ x + y = 0$ (*such a* y *is called an* <u>*additive inverse*</u> *of* x)

ω does <u>not</u> satisfy Axiom 6, but each of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ satisfies <u>all</u> these axioms, and we will see that the same is true for every $\mathbb{Z}_m$, (*At this point, we have not given a rigorous construction of the sets* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$*; so the preceding statement refers to the "informal" systems of integers, rationals, reals, and complex numbers. For the moment, you should consider the axioms (as far as* $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are concerned) as a small number of statements that you believe are true, and consider the definitions and theorems below as showing how the rest of the "rules of algebra" for these systems follow from this small set of assumptions.*)

When the number system $\mathbb{Z}$ *is constructed carefully as a formal system (we will do this very soon) then in that system we can prove that each of Z1-Z5*$'$*and Z6 is true. The rest of the algebraic rules that work in* $\mathbb{Z}$ *can then be proved from these. The same applies to* $\mathbb{Q}$,$\mathbb{R}$*, and* $\mathbb{C}$*.*

Example For every $m \in \mathbb{N}$, the algebraic system $\mathbb{Z}_m$ satisfies all of the Axioms F1-F5$'$ & F6. (*For now, we continue to refer to the operations in* $\mathbb{Z}_m$ *by* $\oplus$ *and* $\odot$). We will not actually check every axiom here, but illustrate how they are verified through a few examples. Roughly, each axiom is true in $\mathbb{Z}_m$ because we already know it is true in $\mathbb{Z}$.

Proof of F2$'$ in $\mathbb{Z}_m$ Suppose $[x],\ [y],\ [z]\ \in \mathbb{Z}_m$. Then $([x] \odot [y]) \odot [z] =\ [xy] \odot [z]$

$$= [(xy)z] \underset{\uparrow}{=} [x(yz)] = [x] \odot [yz] = [x] \odot ([y] \odot [z]). \quad \bullet$$

because multiplication <u>*in* $\mathbb{Z}$</u> *is associative*: *this is the key to getting associativity for multiplication in* $\mathbb{Z}_m$

Proof of F4 in $\mathbb{Z}_m$ Suppose $[x],\ [y],\ [z]\ \in \mathbb{Z}_m$. Then $[x] \odot ([y] \oplus [z]) = [x] \odot [y + z]$

$$= [x(y+z)] \underset{\uparrow}{=} [xy + xz] = [xy] \oplus [xz] = [x] \odot [y] \ \oplus\ [x] \odot [z]. \quad \bullet$$

because the distributive law holds in $\mathbb{Z}$*: this is the key to getting the distributive law to work in* $\mathbb{Z}_m$

Proof of F6 in $\mathbb{Z}_m$ Suppose $[x] \in \mathbb{Z}_m$ Let y be the integer $m - x$. Then $[y] \in Z_m$ and

$$[x] \oplus [y] = [x + y] = [x + (m - x)] = [m] = [0]. \quad \bullet$$

As an exercise, you should verify that the remaining F1-F5$'$ & F6 hold in every $\mathbb{Z}_m$.

We now look at a few definitions and theorems that we can prove from Axioms F1-F5$'$ & F6. All of them apply equally well in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C},$ and also in all the systems $\mathbb{Z}_m$.

The following theorems and definitions all refer to an algebraic system
***S that satisfies Axioms* F1 $-$ F5$'$ & F6**
This hypothesis is not repeated in each theorem below but it is assumed.

Theorem 1 $(\forall x)(\exists!\, y)\ x + y = 0$

Proof (*Axiom F6 guarantees that y exists; the new information in the theorem is that y is unique. Theorem 1 says that each x has a unique additive inverse.*) The proof will be a homework exercise.

Definition 2 If $x \in S$, then the unique y for which $x + y = 0$ is denoted by $-x$.

Definition 3 We define subtraction in S as follows:

for $u, v \in S,\ u - v$ means $u + (-v)$.

So, by definition: $x - x = x + (-x) = 0.$

Theorem 4 If $x \in S$, then $x \cdot 0 = 0$

Proof $x \cdot 0 = x(0 + 0)$ (Axiom F5)
$= x \cdot 0 + x \cdot 0$ (Axiom F4 $-$ distributive axiom)

so

$$x \cdot 0 + (-(x \cdot 0)) = (x \cdot 0 + x \cdot 0) + (-(x \cdot 0))$$

so $0 = x \cdot 0 + 0$ (using def. of $-(x \cdot 0)$ and Axiom F2 $-$ associativity)

so $0 = x \cdot 0$ (Axiom F5)

Theorem 5 **(**Various "sign rules") For all x, y, z :

i) $-(x+y) = -x-y$
ii) $-(-x) = x$
iii) $(-x)y = -(xy)$
Notice that, for $x=1,$ *iii) says that* $(-1)\cdot y = -(1\cdot y) = -y$
iv) $x(-y) = -(xy)$
v) $(-x)(-y) = xy$
vi) $x(y-z) = xy - xz$

Proof i) The proof will be a homework exercise.

ii) By definition, $-(-x)$ is the unique z that satisfies the equation:

$$(-x) + z = 0.$$

Check that x satisfies the equation: $(-x)+x=0$ (*by definition of* $-x$)
so $-(-x) = x.$

iii) By definition, $-(xy)$ is the unique z that satisfies the equation

$$xy + z = 0.$$

Notice that $z = (-x)(y)$ satisfies the equation:

$$xy + (-x)y = yx + y(-x) \qquad \text{(Axiom F3}' - \text{commutativity for multiplication)}$$
$$= y(x + (-x)) \qquad \text{(Axiom F4} - \text{distributive axiom)}$$
$$= y \cdot 0 \qquad \text{(definition of } -x)$$
$$= 0 \qquad \text{Theorem 4}$$

so $-xy = (-x)y.$

iv) Exercise: similar to iii)

$$\text{v)}\quad \begin{aligned}(-x)(-y) &= -(x(-y) && \text{(by part iii)}\\ &= -(-xy) && \text{(by part iv)}\\ &= xy && \text{(by part ii)}\end{aligned}$$

$$\text{vi)}\quad \begin{aligned}x(y-z) &= x(y+(-z) && \text{(def. of subtraction)}\\ &= xy+x(-z) && \text{(distributive axiom)}\\ &= xy+(-xz) && \text{(by part iv)}\\ &= xy-xz && \text{(def. of subtraction)}\end{aligned}$$

Theorem 6 (Cancellation for addition) For all x, y, z: if $x+y=x+z$, then $y=z$.

Proof If $x+y=x+z$, then $(-x)+(x+y)=(-x)+(x+z)$. Using associativity, we get that $0+y=0+z$, so $y=z$. ●

Example: Algebra in $\mathbb{Z}_6$

As we said earlier, all the preceding definitions and Theorems 1-6 apply in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}_m$ (for every $m \in \mathbb{N}$).

Here are some illustrations in $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$.

<u>To simplify notation</u>: *we have had enough practice by now to realize that addition and multiplication in $\mathbb{Z}_m$ are different operations from addition and multiplication in $\mathbb{Z}$. Therefore it should be safe to refer to them as $+$ and $\cdot$ rather than using the clumsy $\oplus$ and . These symbols which were introduced at the beginning to avoid confusion with the addition and multiplication operation in $\mathbb{Z}$. Hereafter, the context determines which operations “ $+$ " and “ $\cdot$ ” refer to.*

There is a unique z in $\mathbb{Z}_6$ such that $[2]+z=[0]$, namely, $z=[4]$. We say that $[2]$ and $[4]$ are additive inverses (for each other) in $\mathbb{Z}_6$; therefore we write $-[2]=[4]$ and $-[4]=[2]$.

Similarly, $-[0]=[0]$, $-[1]=[5]$, and $-[3]=[3]$.

Therefore we have the following subtraction examples:

$$[2]-[4]=[2]+(-[4])=[2]+[2]=[4]$$

$$[5]-[3]=[5]+(-[3])=[5]+[3]=[2]$$

$$[3]-[5]=[3]+(-[5])=[3]+[1]=[4]$$

$$-([1]+[5]) = \begin{cases} -[1]-[5] = -[1]+(-[5]) = -[1]+[1]=[0], & \text{OR}\\ -[6] = -[0]=[0] \end{cases}$$

$$(-[2])(-[4]) = \begin{cases} [4][2]=[8]=[2] \quad (\textit{using that } -[2]=[4], \textit{etc}) & \text{OR}\\ [2][4]=[8]=[2] \quad (\textit{using that } (-x)(-y)=xy) \end{cases}$$

$$\begin{aligned}(-[2])[3]\ +\ [5]([1]-[2]) = \quad & -[6]+[5][1]-[5][2] = [0]+[5]-[10] \\ = & [5]+[2] = [1]\end{aligned}$$

The equation $z+[5]=[2]$ can be solved by subtracting $[5]$ from both sides:

$$z=[2]-[5]=[2]+(-[5]) \quad = [2]+[1]=[3]$$

However, there are also some peculiarities in the algebra of $\mathbb{Z}_6$:

$[2][3]=[0]$ even though neither factor is $[0]$.

There is no solution for the equation $[2]w+[1]=[4]$.

We can simplify by subtracting $[1]$ from both sides to get

$$[2]w=[3] \qquad (*)$$

But there is no value of w that works (try all possible values : $w=[0],...,[5]$!)

In general, if $a,b,c\in\mathbb{Z}_6,$ a linear equation like $aw+b=c$ might not have a solution for w. (*It depends on the choice of* a,b,c : *can you create an equation of this form that does have a solution in* $\mathbb{Z}_6$*?*)

We would be able to solve the equation (*) if there were an element $s\in\mathbb{Z}_6$ for which $s\cdot[2]=[1]$ – for then we could write :

$$\begin{aligned}&[2]w=[3]\\&(s\cdot[2])\,w=s\cdot[3]\\&1\cdot w=s\cdot[3]\\&\ \ w=s\cdot[3]\end{aligned}$$

.

Similarly, if there were such an element $s\in\mathbb{Z}_6$ the equation $[2][3]=[0]$ would be impossible – because that would mean $(s\cdot[2])\cdot[3]=s\cdot[0]$, so that

$$\begin{aligned}&\qquad\quad ||\\ [3]=\ &[1]\cdot[3]=[0].\end{aligned}$$

The peculiarities of these particular examples arise because there is no s in $\mathbb{Z}_6$ for which $s\cdot[2]=[1]$ – that is, $[2]$ does not have a “multiplicative inverse” in $\mathbb{Z}_6$. *Which elements in* $\mathbb{Z}_6$ *do have a “multiplicative inverse?”*

The strange behaviors observed in the algebra of $\mathbb{Z}_6$ can occur in $\mathbb{Z}_m$ for many values of m – but not all, as we will see below.

Fields

"Abstract Algebra" (such as Math 430) is devoted to the study of various algebraic systems. These systems have names like groups, rings, and fields. A system S satisfying the Axioms $\text{F1} - \text{F5}'$ & F6 is called a commutative ring with a unit (1) $-$ but you don't need to remember that name.

Fields are especially important algebraic systems. A field satisfies all the axioms $\text{F1} - \text{F5}', \text{F6}$ plus one additional axiom $\text{F6}'$ $-$ and when $\text{F6}'$ is also true in an algebraic system, it rules out the strange algebraic behaviors we saw in a system like $\mathbb{Z}_6$.

Axiom F6′ $(\forall x)\ x \neq 0 \Rightarrow (\exists y)\ y \cdot x = 1$ (*such a y is called a multiplicative inverse for x).*

Definition An algebraic system F satisfying all the axioms $\text{F1} - \text{F6}'$ is called a field.

It was because of this definition that we used the letter "F" in labeling the axioms: F1 $-$ F6$'$ are "the field axioms."

Example i) Each of the (informal) algebraic systems $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ is a field. However, $\mathbb{Z}$ is not a field because Axiom $6'$ is not true in $\mathbb{Z}$. (*In fact, only a very few elements of $\mathbb{Z}$ have a multiplicative inverse: which ones?*)

ii) $\mathbb{Z}_6$ is not a field. It satisfies all of the field axioms except $\text{F6}'$: for example, $[2]$ has no multiplicative inverse in $\mathbb{Z}_{6.}$

iii) $\mathbb{Z}_3$ is a field. Like every $\mathbb{Z}_m$, it satisfies Axioms F1-F5$'$ & F6. Also, $\mathbb{Z}_3$ has only two nonzero elements, $[1]$ and $[2]$ and each has a multiplicative inverse in $\mathbb{Z}_3$: $[1] \cdot [1] = [1]$ and $[2] \cdot [2] = [1]$. Therefore $\mathbb{Z}_3$ also satisfies Axiom F6$'$.

Because every field F satisfies Axioms F1-F5$'$ & F6, all of preceding definitions and theorems in this section are true in every field. But because fields satisfy, in addition, the Axiom F6$'$, we can prove some additional theorems about algebra in a field.

Theorem 7 Suppose F is a field. Then $(\forall x)\,(x \neq 0 \Rightarrow (\exists! y)\, y \cdot x = 1)$

Proof (*Axiom F6′ guarantees that y exists; the new information in the theorem is that y is unique. So Theorem 7 says that each x has a unique multiplicative inverse.*)

Suppose $x \neq 0$ and that	$y \cdot x = 1$ and $z \cdot x = 1$	
Then	$z \cdot (y \cdot x) = z \cdot 1 = z$	(Axiom F5′)
so	$(z \cdot x) \cdot y = z$	Commutative and associative axioms for multiplication
so	$1 \cdot y = z$	
so	$y = z$	(Axiom F5′) ●

Definition 8 If x is a nonzero element in a field F, then the unique y for which $y \cdot x = 1$ is denoted by x^{-1} .

Definition 9 We define <u>division</u> in a field F as follows:

$$\text{for } x, y \in F \text{ and } x \neq 0,\ \tfrac{y}{x} \text{ means } y \cdot x^{-1}.$$

Here are a couple of the most important theorems related to "doing algebra" in a field (such as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_3$).

Theorem 10 (Cancellation Rule for Multiplication in a Field) Suppose F is a field and that $x, y, z \in F$. If $x \neq 0$ and $xy = xz$, then $y = z$.

Proof $xy = xz \;\Rightarrow\; x^{-1}(xy) = x^{-1}(xz) \;\Rightarrow\; (x^{-1}x)y = (x^{-1}x)z$
$\Rightarrow 1 \cdot y = 1 \cdot z \;\Rightarrow\; y = z.$ ●

Theorem 11 In any field, if $xy = 0$, then either $x = 0$ or $y = 0$.

Proof A homework exercise.

Theorem 12 Suppose F is a field, that $a, b, c \in F$ and that $a \neq 0.$ Then the linear equation $ax + b = c$ has a unique solution in F.

Proof If $ax + b = c$, then adding $-b$ to both sides (= "subtracting b from both sides") gives $ax = c - b$. Then dividing both sides by a (= "multiplying both sides by a^{-1}") gives $x = a^{-1}(c - b) = \frac{c-b}{a}$. ●

Example: Algebra in the field $\mathbb{Z}_5$ The algebraic system $\mathbb{Z}_5$ is a field. To check Axiom F6$'$, simply note that

$$[2]^{-1} = [3] \text{ (since } [3] \cdot [2] = [1]\,) \qquad [1]^{-1} = [1]$$
$$[3]^{-1} = [2] \qquad [4]^{-1} = [4]$$

Any algebraic manipulation that we could do in $\mathbb{Z}_6$ (above) is also legitimate $\mathbb{Z}_5$ (or any other $\mathbb{Z}_m$). But we can also do new things:

$$[2] \text{ divided by } [3] = \tfrac{[2]}{[3]} = [2] \cdot [3]^{-1} = [2] \cdot [2[= [4]$$

$$[3] \text{ divided by } [2] = \tfrac{[3]}{[2]} = [3] \cdot [2]^{-1} = [3] \cdot [3] = [4]$$

In $\mathbb{Z}_5$ solve the linear equation $[3]z + [4] = [1]$:

$$[3]z = [1] - [4] = [1] + [1] = [2]$$

so $z = [3]^{-1} \cdot [2] = \tfrac{[2]}{[3]} = [4].$

(*Check by substituting:* $[3][4] + [4] = [2] + [4] = [1].$)

<u>Certain quadratic equations can be solved in</u> $\mathbb{Z}_5$:

$x^2 + [2]x + [2] = [0]$

$\Leftrightarrow$ $(x + [3]) \cdot (x + [4]) = [0]$ (*check the factoring by using the distributive, commutative and associative properties as needed*)

$\Leftrightarrow$ $(x + [3]) = [0]$ or $(x + [4]) = [0]$ (by Theorem 11)

$\Leftrightarrow$ $x = -[3]$ or $x = -[4]$

$\Leftrightarrow$ $x = [2]$ or $x = [1]$ (*Check by substituting!*)

<u>Not all quadratics can be solved</u> in $\mathbb{Z}_5$: Check that $z^2 = [3]$ has no solution in $\mathbb{Z}_5$.

The last example shows that elements in a field do not necessarily have square roots. The element $[3]$ has no square root in $\mathbb{Z}_5$; and we learned long ago that 2 has no square root in the field $\mathbb{Q}$.

When is $\mathbb{Z}_m$ a field?

We have seen that $\mathbb{Z}_4$ and $\mathbb{Z}_6$ are not fields. A quick check shows that $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, and $\mathbb{Z}_{11}$ are all fields. We are going to prove that $\mathbb{Z}_m$ is a field iff m is a prime number. This depends on looking an important little theorem about integers, primes and modular arithmetic – a theorem important enough to have a name attached to it.

Fermat's Little Theorem Suppose $a \in \mathbb{Z}$. If p is a prime number and p does not divide a, then $a^{p-1} \equiv_p 1$ (*that is,* $a^{p-1} - 1$ *is divisible by* p.))

Note: 1) In terms of $\mathbb{Z}_p$, the theorem says that if p is a prime number and p does not divide a, then $[a^{p-1}] = [1]$ in $\mathbb{Z}_p$. If $p|a$, the conclusion of the theorem may be false – for example, if $p = 3$ and $a = 6$, then $6^{3-1} \not\equiv_3 1$.

2) A little bit of history:

> *The most significant of Pierre de Fermat's correspondents in number theory was Bernhard Frenicle de Bessy (1605-1675), an official at the French mint who was renowned for his gift of manipulating large numbers. (Frenicle's facility in numerical calculation is revealed by the following incident: on hearing that Fermat had proposed the problem of finding cubes which when increased by their proper divisors become squares, as is the case with* $7^3 + (1 + 7 + 7^2) = 20^2$, *he immediately gave four different solutions; and supplied six more the next day.) Though in no way Fermat's equal as a mathematician, Frenicle alone among his contemporaries could challenge him in number theory and his challenges had the distinction of coaxing out of Fermat some of his carefully guarded secrets. One of the most striking is* (...the Little Theorem, stated above...). *Fermat communicated this result in a letter to Frenicle dated October 18, 1640, along with the comment "I would send you the demonstration, if I did not fear its being too long."*
>
> (D.M. Burton, Elementary Number Theory, Allyn and Bacon, 1980, p. 97)

Fermat is better known for a different result which might be called "Fermat's Big Theorem" – although people usually call it "Fermat's Last Theorem." He wrote it down in 1647 in the margin of a book (a translation of the Arithmetica of Diophantus). It states that there are no positive integers x, y, z satisfying the equation $x^n + y^n = z^n$ when n is a natural number larger than 2. (For $n = 2$, it's easy to find positive integers x, y, z that work: for example, $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$.) In the margin, Fermat also wrote that he had a "truly marvelous" proof but that the margin was too small to contain it.

In fact, "Fermat's Last Theorem" remained unproved, in spite of many attempts, for more than 350 years. Finally, in 1993, a British mathematician named Andrew Wiles announced that he had a proof. It turned out that Wiles' "proof" was flawed, but he and a collaborator worked to fix the error and finally produced a correct proof in 1995. The proof is a real tour-de-force of modern mathematics and indicates that Fermat's Last Theorem is actually "very, very deep" in spite of being very simple to state. No one today believes Fermat actually had the proof he referred to in the margin of Diophantus – although he might have believed that he did.

To prove the "Little Theorem" we need a result that we proved some time ago: if p is a prime and $p|ab$, then $p|a$ or $p|b$. (*Here's a quick recap of how that proof was done: if $p \not| \, a$, then gcd$(a, p) = 1$, so there must exist integers x, y such that $1 = ax + py$. Multiplying by b gives $b = abx + pby$. Since $p|abx$ and $p|pby$, it follows that $p|b$.*)

Proof of the "Little Theorem" (*This proof is handled in $\mathbb{Z}_p$. The heart of the proof consists of the two simple observations.*) Assume that p is a prime number and p does not divide a.

i) No two of the integers a, $2a$, $3a$, ... , $(p-1)a$ are equivalent modulo p.

Consider any two integers from the list, say ka and la where $1 \leq k < l \leq p-1$. We are assuming that p does not divide a, and p does not divide $l - k$ (since $0 < l - k < p$). Therefore (since p is prime), p does not divide the product $a(l-k) = al - ak$, and so al and ak are not equivalent modulo p.

Therefore no two equivalence classes from $\mathbb{Z}_p$ in the list $[a]$, $[2a]$, $[3a]$, ..., $[(p-1)a]$ are the same.

ii) None of the equivalence classes $[a]$, $[2a]$, $[3a]$, ..., $[(p-1)a]$ is $[0]$.

Suppose $1 \leq k \leq p-1$. Since p is a prime that does not divide a or k, p cannot divide the product ka. Therefore $[ka] \neq [0]$ in $\mathbb{Z}_p$.

So $[a]$, $[2a]$, $[3a]$, ... , $[(p-1)a]$ is a list containing a total of $(p-1)$ different nonzero equivalence classes from $\mathbb{Z}_p$; that means it is a list of all the nonzero equivalence classes in $\mathbb{Z}_p$ (*how many different nonzero equivalence classes does $\mathbb{Z}_p$ have?*).

Here's another list of the all different nonzero equivalence classes in $\mathbb{Z}_p$: $[1]$, $[2]$, ... , $[p-1]$. So the two lists must contain exactly the same equivalence classes (*although probably listed in different orders*).

Since multiplication in $\mathbb{Z}_p$ is commutative, the two lists have the same product in $\mathbb{Z}_p$:

$$[a] \cdot [2a] \cdot \ldots \cdot [(p-1)a] = [1] \cdot [2] \cdot \ldots \cdot [p-1]$$

Because of the definition of multiplication in $\mathbb{Z}_p$, this means that

$$[a \cdot 2a \cdot \ldots \cdot (p-1)a] = [1 \cdot 2 \cdot \ldots \cdot (p-1)]$$

so $\quad [\,(p-1)! \cdot a^{p-1}\,] = [\,(p-1)!\,]$

so $\quad (p-1)! \cdot a^{p-1} \equiv_p (p-1)!$

so $\quad (p-1)! \cdot a^{p-1} - (p-1)! = (p-1)!\,(a^{p-1} - 1)$ is divisible by p.

Since p is prime and p does not divide any of the factors $1, 2, ..., p-1$, we see that $p \not| \,(p-1)!$,. Therefore we conclude that $p \,|\, (a^{p-1} - 1)$, or, in other words, $a^{p-1} \equiv_p 1$. •

Here is a slight variation of the theorem which is true whether or not p divides a.

Corollary If p is a prime, then $a^p \equiv_p a$.

Proof If $p|a$, then $a^p \equiv_p 0 \equiv_p a$. If $p \nmid a$, then the theorem tells us that $a^{p-1} \equiv_p 1$, and multiplying both sides by a gives $a^p \equiv_p a$. ●

Example To illustrate, suppose $p = 5$. Whenever a is not a multiple of 5, then $a^4 \equiv_5 1$, that is, $5|(a^4 - 1)$. For example:

$a = 3$	$3^4 - 1 = \ 80$
$a = 4$	$4^4 - 1 = 255$
$a = 6$	$6^4 - 1 = 1295$
$a = 32$	$32^4 - 1 = 1048575$
$a = 179$	$179^4 - 1 = 1026625680$

In each example, $5|a^4 - 1$ (just as the theorem says should happen).

Example Fermat's Little Theorem can be used to find the smallest natural number congruent to a given number $(\text{mod } p)$. For example, $3^6 \equiv_7 1$, so $3^{1874} = (3^6)^{312} \cdot 3^2 \equiv_7 (1)^{312} \cdot 3^2 = 9 \equiv_7 2$. Therefore $[3^{1874}] = [2]$ in $\mathbb{Z}_7$.

Example Verify that $5^{38} \equiv_{11} 4$.

By Fermat's Little Theorem, $5^{10} \equiv_{11} 1$. Therefore $5^{38} = (5^{10})^3 \cdot 5^8 \equiv_{11} (1)^3 \cdot 5^8$
$= 5^8 = (5^2)^4 \equiv_{11} (3)^4 = 81 \equiv_{11} 4$.

Note: there is not necessarily a "best" way to do such a simplification. I used the method above just to illustrate Fermat's Little Theorem. Someone might notice a quicker calculation. For example

Since $5^5 = 3125 \equiv_{11} 1$, *then* $5^{38} = (5^5)^7 \cdot 5^3 \equiv_{11} (1)^7 5^3 = 125 \equiv_{11} 4$.

Here is the main theorem about the $\mathbb{Z}_m$'s that was promised earlier.

Theorem $\mathbb{Z}_m$ is a field if any only if m is a prime number.

Proof i) Assume $m = p$, a prime number. is a prime number. The field axioms except for F6$'$) are true in every $\mathbb{Z}_m$, so all we need to prove is that Z6$'$ is also true in $\mathbb{Z}_p$ when p is prime. So suppose $[x] \in \mathbb{Z}_p$ and $[x] \neq 0$.

Then $p \not| \, x$, so Fermat's Little Theorem gives that $[x^{p-1}] = [1]$. Since x^{p-2} is an integer, we can let $[y] = [x^{p-2}] \in \mathbb{Z}_p$. Then $[y] \cdot [x] = [x^{p-2}] \cdot [x] = [x^{p-1}] = [1]$. So $[y]$ is an additive inverse for $[x]$ in $\mathbb{Z}_p$. Therefore $\mathbb{Z}_p$ is a field,

ii) Assume m is not a prime number. Then we can write $m = kn$ where $k, n \in \mathbb{N}$, $1 < k < m$ and $1 < n < m$. Then in $\mathbb{Z}_m$, $[k] \neq [0]$ and $[n] \neq [0]$, but $[k] \cdot [n] = [0]$. According to Theorem 11, this cannot happen in a field. So $\mathbb{Z}_m$ is not a field. ●

Some Concluding Thoughts

Earlier we agreed that the operations in $\mathbb{Z}_m$ will be referred to as $+$ and $\cdot$ rather than with the more clumsy notation $\oplus$ and $\odot$. By now, you should also be comfortable enough with the fact that the members of $\mathbb{Z}_m$ are sets (equivalence classes) that we can relax a bit and simplify notation further. We will henceforth just refer to the elements of $\mathbb{Z}_m$ as $0, 1, ..., m-1$ with the understanding that these are just shorthand for $[0]$, $[1]$, ..., $[m-1]$. You can carry in your head that when working in $\mathbb{Z}_m$, $0, 1, ..., m-1$ are really equivalence classes of integers modulo m.

The context of what we're talking or writing about determines whether "1" refers to "the integer 1" or "the equivalence class $[1]$ in $\mathbb{Z}_m$."

> *If you are working in a setting where sometimes "2" means "the integer 2" and sometimes "2" refers to an element of $\mathbb{Z}_m$, then it might be helpful to revert to different notations like 2 and $[2]$ to help keep things straight.*

With those understandings, the arithmetic tables for $\mathbb{Z}_4$ look much neater:

$+$		**0**	**1**	**2**	**3**
0		0	1	2	3
1		1	2	3	0
2		2	3	0	1
3		3	0	1	2

$\cdot$		**0**	**1**	**2**	**3**
0		0	0	0	0
1		0	1	2	3
2		0	2	0	2
3		0	3	2	1

We can think of $\mathbb{Z}_4$ (or $\mathbb{Z}_m$) as a "new number system" whose members "really" are equivalence classes of numbers we already had (integers).

What we did was to use an equivalence relation ($\equiv_m$) together with the (informal) number system $(\mathbb{Z})$ to create the new number systems $\mathbb{Z}_m$. In $\mathbb{Z}_m$, the "new numbers" are really equivalence classes, built using the old numbers and an equivalence relation. This idea is very important. For example, very soon we are going to use the "old" number system ω (which we have previously constructed in a very careful way from sets) together with ordered pairs and equivalence classes to very carefully construct a “new” number system that will be “act just like” the informal system of integers, $\mathbb{Z}$. This will then become the official, precise definition of the system of integers $\mathbb{Z}$. Is this formal system $\mathbb{Z}$, each integer will turn out to be a certain equivalence class.

Some final comments about fields (without proof)

1) The fields $\mathbb{Q}$ and $\mathbb{R}$ are infinite. Each field $\mathbb{Z}_p$ (p a prime) is an example of a finite field (with p elements).

There are examples of finite fields other than the fields $\mathbb{Z}_p$. A finite field always has p^n elements, where p is some prime number and $n \in \mathbb{N}$.

2) In the fields $\mathbb{Q}$ and $\mathbb{R}$, a sum of $1's$ can never be 0, that is

$$(\forall n \in \mathbb{N}) \qquad \sum_{i=1}^{n} 1 = 1 + 1 + ... + 1 \neq 0$$

A field with this property is called a field of characteristic 0.

By contrast, in $\mathbb{Z}_3$, $\sum_{i=1}^{3} 1 = 1 + 1 + 1 = 0$, and more generally, in $\mathbb{Z}_p$ the sum of p 1's is 0.

For any field F: if $\sum_{i=1}^{p} 1 = 0$ but $\sum_{i=1}^{n} 1 \neq 0$ for all $n < p$, then we say that F is a field of characteristic p. For example, $\mathbb{Z}_5$ is said to have characteristic 5 and for any prime p, $\mathbb{Z}_p$ has characteristic p.

There are fields of characteristic p other than the fields $\mathbb{Z}_p$. In fact, there exist infinite fields with characteristic $p \neq 0$.

It turns out that the characteristic of any field F is either 0 or a prime number p.

3) Every field F of characteristic p $(\neq 0)$ contains a “copy” of $\mathbb{Z}_p$ inside itself. In some sense, every such field F is a “extension” of $\mathbb{Z}_p$.

Take Math 430 to learn much more about fields! The theory of fields leads naturally into a subject called Galois Theory. Elementary applications of Galois Theory include proving that it's impossible to trisect an angle using just a compass and straightedge; and that there cannot be a general formula (analogous to the quadratic formula) that expresses all the roots $a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ (where $a_5 \neq 0)$ in terms of the coefficients.