Introduction to Modular Arithmetic, the rings $\mathbb{Z}_6$ and $\mathbb{Z}_7$

The main objective of this discussion is to learn modular arithmetic. We do this by building two systems using modular arithmetic and then by solving linear and quadratic equations in those systems. The reader is no doubt familiar with techniques for solving these equations over the real numbers. However, in much the same way as learning Latin, French, or Spanish gives the language learner a better appreciation of English, so the careful examination of solution techniques in finite number systems adds depth to the mathematics students' understanding of equation solving. But why $\mathbb{Z}_6$ and $\mathbb{Z}_7$?

The answer is that $\mathbb{Z}_7$ behaves very much like the real numbers: every non-zero element has an inverse. In fact $\mathbb{Z}_7$ is a *field*. But $\mathbb{Z}_6$ has pairs of so-called *zero divisors*, that is, non-zero numbers whose product is zero. For example, in $\mathbb{Z}_6$, the product $2 \cdot 3 = 0$ because $2 \cdot 3$ is a multiple of 6. We begin by examining linear equations.

1 Solving Linear Equations

Before reading on, flip over to page 7 where the addition and multiplication tables for $\mathbb{Z}_6$ and $\mathbb{Z}_7$ are given. How did we build these tables? It's really easy: $x \oplus y$ is the remainder you get after dividing $x + y$ by 6 (or 7), and similarly, $x \odot y$ is the remainder you get after dividing $x \cdot y$ by 6 (or 7). For example, to find $3 \odot 4$ in $\mathbb{Z}_7$, divide 12 by 7 to get a remainder of 5, so $3 \odot 4 = 5$ in $\mathbb{Z}_7$.

Our aim is to learn a method for solving equations of the form

$$ax + b = c$$

in both $\mathbb{Z}_6$ and $\mathbb{Z}_7$. We do this by looking very carefully at how we would solve this in the real number system. We start with $\mathbb{Z}_7$. To be specific, consider

$$2x + 3 = 4.$$

In the real number system, we would subtract 3 from both sides. In other words, we'd add the negative (ie, additive inverse) of 3 to both sides. Look at the addition table for $\mathbb{Z}_7$ to see that 4 is the negative of 3 ($3+4=0$, right?). So we have $(2x+3)+4=4+4$ or $(2x+3)+4=1$. Now since addition is associative, we have $2x+(3+4)=1$, but since $3+4=0$, our equation reduces to $2x+0=1$.

Since $a+0=a$ for all a (0 is the additive identity), we can write $2x=1$. Now what. In the real system we would multiply by the multiplicative inverse of 2, sometimes written $\frac{1}{2}$. Look at the multiplication table of $\mathbb{Z}_7$ to find the multiplicative inverse of 2. Recall that a number e in a mathematical system is a multiplicative identity if $e \cdot x = x \cdot e = x$ for all number x. So 1 is a multiplicative identity for $\mathbb{Z}_7$. The multiplicative inverse of a number u is a number v such that $uv=1$. So what is the multiplicative inverse of 2? Check out the row of 2 in the table and notice that $2{\cdot}4=1$. So 4 is the inverse of 2. Now multiply on the left by 4 to get

$$4 \cdot 2x = 4 \cdot 1.$$

Use the associativity of $\cdot$ to get $(4 \cdot 2)\,x = 4$. That is $1 \cdot x = 4$. Finally, $1 \cdot x = x$, so we have our solution $x=4$. Of course, since $\mathbb{Z}_7$ is finite we could simply list the values of $2x+3$ as a function of x to see if and when the value 4 pops up.

x	$2x+3$
0	3
1	5
2	0
3	2
4	4
5	6
6	1

You can see from this that the range of the linear function $f(x)=2x+3$ is the entire set of $\mathbb{Z}_7$. This is the case for the real number system when the slope m of the line $f(x)=mx+b$ is not zero.

Moving on to $\mathbb{Z}_6$, we will try to solve

$$2x+3=4$$

in the same way we did in $\mathbb{Z}_7$.

First 'subtract' 3 (note that in Z_6, $3=-3$) from both sides:

$$(2x+3)+3=4+3$$

and use associativity to get

$$2x + 0 = 1$$

and finally

$$2x = 1.$$

Notice that 3 is its own additive inverse. Why?

Now look for the inverse of the number 2 (we use the word inverse here and elsewhere to mean *multiplicative inverse* because we have the word negative to use for the additive inverse of a number). In other words, look for a number we can multiply by 2 to get the multiplicative identity 1. Whoops, there isn't one. The reason is that the row of 2 in the times table of $\mathbb{Z}_6$ does not have a 1. So 2 has no inverse. The equation $2x = 1$ has no solutions. Since $2x = 1$ is equivalent to our original equation, it follows that

$$2x + 3 = 4$$

has no solutions.

What is the range of $f(x) = 2x + 3$ in $\mathbb{Z}_6$? Look at the tables to see that $2x + 3$ can be any of the number in the set $\{1, 3, 5\}$.

Now we turn to solving quadratic equations.

2 Solving Quadratic Equations

As we did for linear equations, we will look carefully at the solution techniques we use in equations defined over real numbers to see the extent to which they can be used in $\mathbb{Z}_7$ and $\mathbb{Z}_6$. The general quadratic equation in one variable is

$$ax^2 + bx + c = 0.$$

There are two common techniques, factoring and using the quadratic formula. But we don't even know if the quadratic formula holds in $\mathbb{Z}_7$ so we will have to think deeply about why it is true in the system $\mathbb{R}$.

Factoring

Consider $x^2 - 4x + 3 = 0$. In $\mathbb{R}$ we write $x^2 - 4x + 3 = (x - 3)(x - 1)$ without much thinking. Can we do this in $\mathbb{Z}_7$? Let's see. Try to find the reason for each step below:

$$\begin{aligned}(x-3)(x-1) &= (x-3)x+(x-3)(-1)\\ &= x^2-3x+x(-1)+(-3)(-1)\\ &= x^2+4x+6x+4\cdot 6(-1=6 \text{ in } \mathbb{Z}_7)\\ &= x^2-3x+6x+3(-1=6 \text{ in } \mathbb{Z}_7)\\ &= x^2+3x+3\\ &= x^2-4x+3.\end{aligned}$$

So it seems the factoring technique might work. Now given a factorable quadratic, how do we solve the corresponding equation? Of course, you know that we set each of the factors $x-3$ and $x-1$ equal to zero. We can do this because $\mathbb{R}$ satisfies the zero product property.

That is to say, if the product of two numbers is zero, then one of the two numbers must actually be zero. Put another way, the product of two non-zero numbers is non-zero. Thus, $x^2-4x+3=0$ has two solutions in $\mathbb{Z}_7, x=3$ and $x=1$.

Completing the square in $\mathbb{R}$

Often we resort to using the quadratic formula to solve quadratic equations when factoring isn't possible. To understand why the quadratic formula works, we must think about how to derive it. Recall that we derived the quadratic formula using a technique called *completing the square*. We will use this on $x^2-4x+3=0$ in $\mathbb{R}$ to illustrate. First, note that

$$x^2-4x+4=(x-2)^2.$$

We can add 1 to both sides of $x^2-4x+3=0$ to get $x^2-4x+4=1$ and then write $(x-2)^2=1$. Take the square root of both sides to get $x-2=\pm 1$ and solve the two equations $x-2=1$ and $x-2=-1$ to get $x=3$ and $x=1$.

Let us look carefully at the derivation of the quadratic formula in $\mathbb{R}$. Divide by the non-zero coefficient a to get $x^2+\frac{b}{a}x+\frac{c}{a}=0$. Subtract $\frac{c}{a}$ and then add the square of $\frac{b}{2a}$ to both sides to get $x^2+\frac{b}{a}x+\frac{b^2}{4a^2}=-\frac{c}{a}+\frac{b^2}{4a^2}$. Since the left side is a perfect square, we can write

$$\left(x+\frac{b}{2a}\right)^2=-\frac{c}{a}+\frac{b^2}{4a^2}.$$

This leads to

$$x + \frac{b}{2a} = \pm\sqrt{\frac{b^2}{4a^2} - \frac{c}{a} \cdot \frac{4a}{4a}}$$

and finally

$$\begin{aligned} x &= -\frac{b}{2a} \pm \sqrt{\frac{b^2 - 4ac}{4a^2}} \\ &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \end{aligned}$$

The quadratic formula in $\mathbb{Z}_7$

Can we do this in $\mathbb{Z}_7$?

Start with $ax^2 + bx + c = 0$, where $a \neq 0$. Since each non-zero number in $\mathbb{Z}_7$ has an inverse, we can write

$$x^2 + a^{-1}bx + a^{-1}c = 0$$

and

$$x^2 + a^{-1}bx = -\left(a^{-1}c\right)$$

Can we add a number to $x^2 + a^{-1}bx$ to make it a perfect square as we did above? The number we added above to the left side is $(a^{-1}b/2)^2$. So we get for the left side $x^2 + a^{-1}bx + (a^{-1}b/2)^2$. Try squaring $x + a^{-1}b/2$ and you'll see that it works. So now the right side is

$$\begin{aligned} -\left(a^{-1}c\right) + \left(\frac{1}{2}a^{-1}b\right)^2 &= -a^{-1}c + \frac{1}{2}a^{-1}b\left(\frac{1}{2}a^{-1}b\right) \\ &= -a^{-1}c + 4a^{-1}b\left(4a^{-1}b\right) \\ &= -a^{-1}c + 2a^{-1}a^{-1}bb \\ &= -a^{-1}caa^{-1} + 2a^{-1}a^{-1}bb \\ &= -a^{-1}a^{-1}ac + 2a^{-1}a^{-1}bb \\ &= \left(2b^2 - ac\right)a^{-2} \\ &= \left(4 \cdot 2b^2 - 4 \cdot ac\right)4^{-1}a^{-2} \\ &= \left(1b^2 - 4ac\right)(2a)^{-2}. \end{aligned}$$

Notice that we have made use of several interesting properties in $\mathbb{Z}_7$; for example $2 \cdot 4 = 1$ and $4^{-1} = 2$. What we have is a situation with which we are quite familiar, namely that under some circumstances we can take the square root (and get a number in our number system). Thus

$$(x + a^{-1}b/2)^2 = \left(x + 4a^{-1}b\right)^2 = \left(b^2 - 4ac\right)(2a^{-1})^2$$

and

$$x + 4a^{-1}b = \pm\left[\left(b^2 - 4ac\right)(2a)^{-2}\right]^{\frac{1}{2}}.$$

Therefore, distributing the square root across the product,

$$\begin{aligned} x &= -4a^{-1}b \pm \frac{\sqrt{(b^2 - 4ac)}}{2a} \\ &= -(2^{-1}a^{-1}b) \pm \frac{\sqrt{(b^2 - 4ac)}}{2a} \\ &= \frac{-b}{2a} \pm \frac{\sqrt{(b^2 - 4ac)}}{2a} \\ &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

Ah ha! same formula.

Which of the quadratic equations $x^2+x+1 = 0, x^2+x+2 = 0, x^2+x+3 = 0, x^2 + x + 4 = 0, x^2 + x + 5 = 0$ and $x^2 + x + 6 = 0$ have solutions in $\mathbb{Z}_7$? Use the quadratic formula to solve them.The table below may help

x	$x^2 + x$
0	0
1	2
2	6
3	5
4	6
5	2
6	0

In order that $x^2 + x + k = 0$ we must have $x^2 + x = 7 - k$. For example, $x^2 + x + 4 = 0$ if $x^2 + x = 7 - 4 = 3$, but 3 does not belong to the range of $x^2 + x$.

Thus, $x^2 + x + 1 = 0$ has two solutions, $x = 2, x = 4$; $x^2 + x + 2 = 0$ has one solutions $x = 3$; $x^2 + x + 3 = 0$ has no solution; $x^2 + x + 4 = 0$ has no solution; $x^2 + x + 5 = 0$ has two solutions, $x = 1, x = 5$; and $x^2 + x + 6 = 0$ has no solution.

Solving quadratic equations in $\mathbb{Z}_6$

Can we do all this in $\mathbb{Z}_6$? The answer here is no and the reason is similar to what we saw in the case of linear equations.

Again, we ask what members of our system have square roots. Since $1^2 = 1, 2^2 = 4, 3^2 = 3, 4^2 = 4, 5^2 = 1$, we see that 3 has a unique square root, 1 and 4 have two square roots and 2 and 5 do not have square roots.

Consider the quadratic $3x^2 + c = 0$ in $\mathbb{Z}_6$. The list below has each of the equations, where $c \in \mathbb{Z}_6$ and the solutions. For $c = 1$, $3x^2 + 1 = 0$ has no solution. For $c = 2$, $3x^2 + 2 = 0$ has no solution. For $c = 3$, $3x^2 + 3 = 0$ has three solutions $x = 5, x = 3, x = 1$. For $c = 4$, $3x^2 + 4 = 0$, has no solutions. For $c = 5$, $3x^2 + 5$ also has no solutions. Finally for $c = 0$, $3x^2 = 0$ has three solutions, $x = 0, x = 2$, and $x = 4$.

The main trouble here is that $\mathbb{Z}_6$ does not satisfy the Zero Product Property. To see this, look at the times table for $\mathbb{Z}_6$. Find a pair of nonzero numbers whose product is zero. There are two such pairs, $\{2, 3\}$ and $\{3, 4\}$. Now suppose we want to solve $(x - 2)(x - 3) = 0$. With the Zero Product property, we would just say $x - 2 = 0$ so $x = 2$ and $x - 3 = 0$ so $x = 3$. But notice that $x = 5$ also satisfies the equation: $(5 - 2)(5 - 3) = 3 \cdot 2 = 0$. Notice that also $x = 0$ satisfies the equation.

The digit tables for $\mathbb{Z}_6$ and $\mathbb{Z}_7$

Below you'll find the addition and multiplication tables for $\mathbb{Z}_6$ and $\mathbb{Z}_7$. Notice that in the tables for $\mathbb{Z}_7$ we have dropped the cell notation even though the objects are cells. Its that at this point there is no compelling reason to emphasize that notation.

Addition and multiplication in $\mathbb{Z}_6$

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Addition and multiplication in $\mathbb{Z}_7$

$\oplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\odot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Problems.

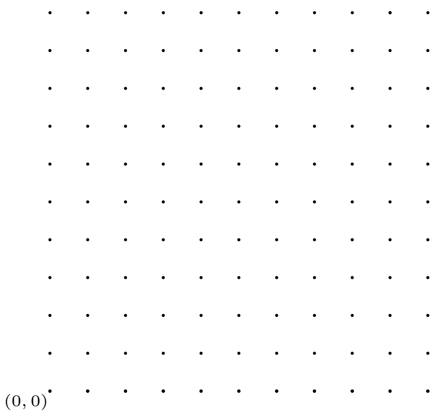
1. Construct the addition and multiplication tables for the digits of $\mathbb{Z}_{11}$ in the space provided.

$\oplus$	0	1	2	3	4	5	6	7	8	9	10
0											
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

$\odot$	0	1	2	3	4	5	6	7	8	9	10
0											
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

2. Use the tables above to solve the equation $3x - 4 = 9$ showing each step and stating how you get from each step to the next one.

3. Use the grid below to sketch the graph of $y = 3x - 4$. Notice that the origin has been labeled.



4. Which of the numbers in $\mathbb{Z}_{11}$ have square roots?

5. Which of the following quadratic equations are solvable over $\mathbb{Z}_{11}$? Find solutions to all that are solvable. Show your reasoning.

   (a) $2x^2 - 3x + 4 = 0$

   (b) $3x^2 - 4x + 2 = 0$

   (c) $4x^2 + 2x - 3 = 0$