Math Circles

Jeff Hicks
# Contents

Introduction \hspace{1cm} v

Chapter 1. Modular Arithmetic \hspace{1cm} 3

**Background**
1. A divisibility relation \hspace{1cm} 3
2. Clock Arithmetic \hspace{1cm} 7

**Handouts**
1. 9 and Math Magic \hspace{1cm} 11
2. Circles and Tables and Sleeping \hspace{1cm} 15
3. Warm Up: A quick review of modular arithmetic \hspace{1cm} 23
4. Division \emph{mod} $n$ \hspace{1cm} 24
5. The Sleepwalking Bishop \hspace{1cm} 27
6. Primes Numbers and Zero Divisors \hspace{1cm} 31

**Solutions**
Solutions \hspace{1cm} 39

Appendix A. Abstract Algebra \hspace{1cm} 45
Introduction

This is an attempt to put together a large number of handouts that I wrote for the Los Angeles Math Circle in 2012 and 2013, along with notes on how to teach the handouts. Hopefully you find the examples and explanations below entertaining. This collection is laid out as follows:

1. A Chapter covers a concept, and the topics in the chapters are meant to be taught in succession. The chapters are largely independent of each other.
2. Each Chapter is broken into two parts: Background and Handouts. The instructor should be familiar with both sections. The handouts are meant to be printed and distributed during the class to students to work on.
3. Additionally, the chapters are further broken down into sections. The sections were designed to fit within a single 2 hour class period—sometimes they did, and sometimes they did not.
4. Finally, every section is broken down into smaller subsections. Frequently, I would hand out the packets to my students by subsection. This kept them on task. If I gave them the whole packet at once, they would invariably skip around the packet, doing the problems they liked, or just kind of gazing at all of the problems at once. A smaller number of problems allowed them to focus better, and kept the classroom more manageable.

Beyond the Introduction, chapters and sections, I’ve also thrown a few appendixes for those who are interested in a more formal treatment of the material. These are designed for those who want to understand the material and how it relates to other sections of mathematics in more detail, and are recommended for the undergraduate who has already seen the material presented in the text. These sections are dense, skip lots of material, and are generally harder to read.
CHAPTER 1

Modular Arithmetic

Modular arithmetic is one of the very basic tools of discrete math. It allows us to analyze patterns that involve divisibility and repetition very easily. It’s use in number theory and algebra means that it is essential to have a good grasp on modular arithmetic before moving on to more advance topics in either of these fields.

I think that modular arithmetic is one of the easiest of concepts for kids to grasp, as it can be associated with long division (a concept that they have to master in school) and clocks. There are several different approaches to developing modular arithmetic, and these handouts try to expose each one of these intuitions. The three methods we look at can be summed up as

1. A divisibility relation
2. “Clock Arithmetic”
3. Remainders

When we ran these lessons, we started with a fun little magic trick that shows some of the power of modular arithmetic. However, to explain why the trick works requires a bit of work. For those with some existing math background, a formal approach to modular arithmetic allows one to prove results about multiplication and division without seemingly having to do any work at all. This is the approach to modular arithmetic that we’ll expose first, although if you prefer a more geometric intuition, I suggest that you skip ahead to the section on “Clock Arithmetic”. The final section, Remainders, allows you to quickly do computations, and may be easier to use. However, I feel that using remainders as a method to explain modular arithmetic sacrifices a lot of understanding in order to build an efficient machinery.

1. A divisibility relation

Modular arithmetic looks at how numbers are related to each other up to\(^1\) some fixed difference \(n\). The idea behind \(\text{mod } 5\) arithmetic is that the numbers 1, 6, 11, 16, … should be treated the same, and that the numbers 2, 7, 13, 18, … should be treated the same, and so on. This is like degrees on a circle: we think of 23° being the same angle as 383° and so on; a mathematician might say that degrees on a circle is like doing arithmetic \(\text{mod } 360\). In order to get a better formal understanding of this relation, let’s return to the case of looking at integers \(\text{mod } 5\), and write down a formal definition for our relation.

\(^1\)As I write this, I realize that much of the terminology used by mathematicians can be confusing. For instance, the phrase “up to \(X\)”. This is a very common phrase in mathematics, and it means roughly that you ignore differences of \(X\). This is one of the universal constructions of mathematics, and is formalized by the notion of quotienting.
Definition 1. We say that two numbers \(a\) and \(b\) are congruent mod 5 and write
\[
a \equiv b \mod 5
\]
if the difference \(a - b\) is divisible by 5.

Does this definition line up with the intuition that we had before? Certainly, as we know have that
\[
1 \equiv 6 \equiv 11 \equiv \ldots \mod 5
\]

Why do we use this notation? For one, it’s a lot quicker to write down than “11 and 6 are related by the fact that their difference is divisible by 5.” But more importantly, the notation suggests a lot of things should be true. The congruence sign looks a lot like an equal sign, and enjoys many of the same properties that the equal sign enjoys. In particular, congruence has the properties of symmetry, reflexivity, and transitivity\(^2\). Finally, the \(\mod 5\) at the end tells us that we are looking at numbers related by differences of 5, but we could easily extend this to be \(\mod n\) for any whole number \(n\). Naturally, the next thing we should do is write down the general definition of a congruence relation \(\mod n\).

Definition 2 (General Case). We say that two numbers \(a\) and \(b\) are congruent mod \(n\) and write
\[
a \equiv b \mod n
\]
if the difference \(a - b\) is divisible by \(n\).

Exercise 1. Let \(n\) be a number written in base 10. Show that it is congruent to its last digit \(\mod 10\).

Exercise 2. What numbers are congruent to 0 \(\mod 2\)? What about numbers congruent to 1 \(\mod 2\)?

Exercise 3. (*) Suppose that I know what a number \(n\) is congruent to \(a\) \(\mod 5\), and congruent to \(b\) \(\mod 3\). Find what \(n\) is congruent to \(\mod 15\).

1.1. Modular Arithmetic. Up until this point, we have only explained modular congruence. This section of the book is called modular arithmetic, so we’ll need to see how the congruence relation plays with addition and multiplication. The equal sign behaves very well with these operations. For instance, we have the “addition law of equality” which tells us whenever \(a = x\) and \(b = y\), then
\[
a + b = x + y.
\]

Relatedly, there is an “multiplication law of equality” which tells us that \(ab = xy\). What we really want to do is use these identities for equality, and see if they extended to congruence \(\mod n\). Just for a test, let’s run a sample computation and see if it works.

\[
3 \equiv 8 \mod 5 \\
4 \equiv 14 \mod 5
\]

\(^2\)For those of you that want to get ahead, these properties make \(\equiv\) what is suggestively called an “equivalence relation.”
CHAPTER 1. MODULAR ARITHMETIC

1. A DIVISIBILITY RELATION

We can now proceed by using the simple rules of addition that we know.

\[
\begin{align*}
4 + 3 & \equiv 7 \mod 5 \\
& \equiv 22 \mod 5 \\
& \equiv 8 + 14 \mod 5
\end{align*}
\]

The first identity isn’t that hard to prove, so I will include a proof of it here, as our first theorem of modular arithmetic (Indeed, the first theorem of this book!) Let’s give it a fancy sounding name.

Theorem 1 (Additive Property of Modular Equivalence). Suppose that \(a \equiv b \mod n\) and \(x \equiv y \mod n\). Then it follows that \(a + x \equiv b + y \mod n\).

**Proof.** This is going to be based on unwinding our definitions for two numbers to be congruent. If \(a \equiv x \mod n\), then this means that \(a - x\) is divisible by \(n\). This means that \(n\) goes into \(a - x\) a whole number of times. Let’s say that \(n\) fits into \(a - x\) a total of \(p\) times so that

\[
a - x = pn
\]

Likewise, \(b \equiv y \mod n\), so we know that there exists a whole number \(q\) so that

\[
b - y = qn
\]

If we sum these two equations together, then we have

\[
(a - x) + (b - y) = pm + qn
\]

Redistributing the terms so that the negative terms are grouped together on the left, and pulling out an \(n\) on the right

\[
(a + b) - (x + y) = n(p + g)
\]

This means that the difference between \((a + b)\) and \((x + y)\) is divisible by \(n\), which is exactly what we need to know that \(a + x \equiv b + y \mod n\). \(\square\)

This is a wonderful \(^3\) It means that we can treat addition of numbers with the congruence sign exactly the same way that we would treat the addition of numbers with the equal sign. Let’s prove the same type of identity, but this time, we’ll use multiplication instead of addition.

Theorem 2 (Multiplicative Property of Modular Equivalence). If \(a \equiv x \mod n\) and \(b \equiv y \mod n\), then \(ab \equiv pq \mod n\).

**Proof.** We know (similar to the other proof) that \(a - x = pn\) for some choice of \(p\), and similarly \(b - y = qn\) for some other whole number \(q\). Rearranging the terms gives us \(a = pn + x\) and \(b = qn + y\). Then we will make a series of computations to show that \(ab - pq\) is divisible by \(n\).

\(^3\)You should treat this as a fact around kids, at least initially. When working at the Los Angeles Math Circle, I found that it was extremely helpful to introduce a theorem to the kids first as a “fact”, and allow them to use it a lot with exercises until they were familiar with it. Once they were familiar with the theorem, we went and proved it.
Unfortunately, there is no pretty way to see this identity, but it is just a series of substitutions and algebraic manipulations.

\[ ab - pq = (nk + p)(nl + q) - pq = nknl + nkq + pnl + pq - pq = n(knl - kq + pl) \]

This shows that \( n \) divides \( ab - pq \). Thus, \( ab \equiv pq \mod n \). \( \square \)

1.2. Division Tricks. While the divisibility definition of congruence doesn’t give much intuition to modular arithmetic, it makes the proving things a lot easier. In order to show two things are congruent, we just have to find a way to show that their difference is divisible by \( n \). Now, we can go the other direction, and use congruence to prove things about divisibility. For instance, we have the following cute fact about the sums of digits of numbers \( \mod 3 \) and \( \mod 9 \).

Suppose we have a number \( k \). Then define \( \star k \) to be the digit sum of \( k \) to be the number which is made of the sums of the digits of \( k \) when it is written out in base ten. \(^5\) For instance, if \( k = 123 \), then \( \star k = 1 + 2 + 3 = 6 \). More abstractly, if \( k = a_0 + a_110^1 + a_210^2 + a_310^3 + \ldots a_d10^d \) is the base 10 expansion of \( k \), then \( \star k = a_0 + a_1 + \ldots + a_d \).

**Theorem 3.** Let \( k \) be a number. Then \( \star k \equiv k \mod 9 \) and \( \star k \equiv k \mod 3 \)

**Proof.** I will include a proof for the first statement, the second statement follows in a similar fashion. The key observation to make here is that \( 10^2 \equiv 1 \mod 9 \). By Theorem 2 we know that

\[
10^2 \equiv 10 \times 10 \mod 9 \\
\equiv 1 \times 1 \mod 9 \\
\equiv 1 \mod 9
\]

By repeating this process over and over, we see that \( 10^n \equiv 1 \mod 9 \) no matter what \( n \) is. With this idea in mind, let us express \( k \) in its base 10 expansion.

\[
k \equiv a_0 + a_110^1 + a_210^2 + \ldots + a_d10^d \mod 9 \\
\equiv a_0 + a_1(1) + a_2(1) + \ldots a_d(1) \mod 9 \quad \text{by observation that } 10^0 \equiv 1 \mod 9 \\
\equiv a_0 + a_1 + a_2 + \ldots + a_d \mod 9 \\
\equiv \star k \mod 9
\]

\( \square \)

From this theorem, we get a commonly known fact:

**Corollary 1.** \(^6\) A number \( k \) is divisible by 9 if and only if \( \star k \) is divisible by 9. A number \( k \) is divisible by 3 if and only if \( \star 3 \) is divisible by 3

\(^4\)I would not show this proof to kids, as handling 2 or 3 variables is more than enough. Handling the 9 that are required to make this proof work would probably be terrible.

\(^5\)I will frequently use a \( \star \) to mean some kind of operation, which is only useful for this lesson only. The next time you see a \( \star \), it won’t mean the same thing that it does here...

\(^6\)A corollary is a very small result, that is usually immediate from the result before.
CHAPTER 1. MODULAR ARITHMETIC

2. CLOCK ARITHMETIC

Proof. Again, I will only show the case with 9, the case with 3 is very similar. Suppose that a number \( k \) is divisible by 9. Then \( k \equiv 0 \mod 9 \), and by the above theorem, this means that \( \star k \equiv 0 \mod 9 \), which implies that \( \star k \) is divisible by 9.

Conversely, suppose that \( \star k \) is divisible by 9. Then \( \star k \equiv 0 \mod 9 \), and by the above theorem, \( k \equiv 0 \mod 9 \).

Somehow, once we have the language of congruences, and a few facts about modular arithmetic, proving this divisibility rule becomes incredibly easy and intuitive. In fact, we get a much stronger result than the divisibility rule, and this “cute fact” about \( k \) and \( \star k \) is what is exploited by the magic trick in the first handout.

Exercise 4. Prove that a number is only divisible by 3 if the sum of its digits is divisible by 3.

2. Clock Arithmetic

Let’s return to some of the intuition that clocks give us with regards to modular arithmetic. In the previous section we described modular arithmetic as a relation that was between numbers. In this section, we will describe it in terms of clocks.

Sometime in elementary school, we are required to learn “clock math”, the strange form of arithmetic that involves intervals of 60, 12, and 24 to describe our times. Clock arithmetic is fairly straightforward: if someone were to say that it was 9 on the clock right now, and asked what time it would be 5 hours from now, you would naturally say that it would be 2, without giving a second thought to it.

We see clock arithmetic in other contexts that involve time. Say we associate Sunday with the number 0, and Monday with the number 1, and so on and so forth until Saturday is the 6th day of the week. If I then told you that today was Wednesday (the 3rd day) and that 5 days would pass, with a bit of thinking you would say that it was now the 2nd day of the week. We might visualize this as a clock that had the days printed at 7 equally spaced positions along the circumference of the clock, where the “day hand” took exactly one weeks worth of time to rotate 360 degrees. With that in mind, we come up with a new definition for modular arithmetic.

**Definition 3 (Clock Math).** Let \( a, b \) be numbers between 0 and \( n-1 \), and \( x \) be any natural number. Suppose we have a clock with \( n \) different positions, and the hand on the clock is pointing at \( a \). If when you advance the hand \( x \) positions clockwise you end up at the number \( b \), then we say that \( a + x \equiv b \mod n \).

This is the intuitive way that we talk about clocks, if we let \( n \) be 12 and instead of saying “midnight” or “noon” we say 0 instead, (I think this would clear a lot of things up.) Modular arithmetic allows us to extend this definition further, to numbers other than 12. Here is a summary of things that are easily seen to have a circular, clock-like nature.

For clock arithmetic, the idea of adding numbers is particularly easy. However, the idea of multiplying two numbers doesn’t seem to make as much sense. After all, who would ever say “What is 3 o’clock times 5 o’clock”. How do we interpret “3 \times 5” on a clock? Maybe the best way would be “if I advance the hour hand 3 places 5 times, where would it end up?” I think for multiplication, the

---

7Incidentally, the Sumerians chose 60, 12 and 24 as the discretization of time due to the large number of different divisors that they have. The ancients didn’t believe in fractions, so they worked with numbers that had lots of divisors.
clock analogy does not work as well as the divisibility relation method for understanding modular arithmetic; however, for addition, it is nice to think of modular arithmetic as a clock.

- Clocks are mod 12.
- Military time is done mod 24
- When you measure angles, you do arithmetic mod 360
- The days of a week for math mod 7.
- Musical tones are done mod 12, when considered in solfège

With clocks, it makes sense to ask how things repeat over and over. For example, imagine that because of some unfortunate circumstance that you live by the following schedule:

- You wake up, and work for 7 hours
- You come back home, and sleep for two hours, before you are forced to wake up again to go to work.

So you live on this miserable 9 hour day. One question you might ask (besides when to find a better job) is how your sleep schedule relates to the rest of the world. So, if for instance, on the first of the month you wake up at 8AM, when will be the next time that you wake up at 8AM. Is it possible that you will never enjoy the opportunity to wake up at 8 again? For this problem, viewing clocks as equivalent to modular arithmetic becomes a handy way of analyzing patterns.

The day works on a 24 hour schedule, and you start awake at 8AM. Then you sleep/work for periods of 9 hours, and you are interested in how many 9-hour periods it will be before you wake at 8AM again. This is equivalent to asking which $n$ satisfy the equation

$$8 + 9n \equiv 8 \mod 24$$

We can simplify this by subtracting 8 from both sides,

$$9n \equiv 0 \mod 24$$

It turns out that this equivalence only holds when $n = 0, 24, 48, \ldots$. But is this always the case, or was that a special property of the fact that we were working 9 hour periods over 24 hour long days? It turns out that we are in the latter case. For example, if you were to work 10 hour days, you would have to solve the equivalence

$$10n \equiv 0 \mod 24$$

which holds whenever $n = 0, 12, 24, 36, \ldots$. So what governs what numbers show up in this pattern? As long as we are at it, we may as well generalize to the fullest extent that we can, and ask:

**Question:** Let us fix some numbers $a, m$. What are the numbers $n$ so that $an \equiv 0 \mod m$?

It may not be too hard to guess the answer to this question: it turns out that it is related to greatest common factors of the numbers. But, let’s go an use this as an excuse to build some theory\footnote{Frequently, we will use a fairly simple problem like this to motivate doing something much more difficult, and usually far more interesting} to solve the problem.
2.1. Multiplication and Addition tables. Hopefully, everybody reading this book has seen multiplication and addition tables before. They look something like this:

\[
\begin{array}{cccccccc}
+ & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
0 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
1 & 2 & 3 & 4 & 5 & 6 & 7 & 1 \\
2 & 3 & 4 & 5 & 6 & 7 & 8 & 2 \\
3 & 4 & 5 & 6 & 7 & 8 & 9 & 3 \\
4 & 5 & 6 & 7 & 8 & 9 & 10 & 4 \\
5 & 6 & 7 & 8 & 9 & 10 & 11 & 5 \\
6 & 7 & 8 & 9 & 10 & 11 & 12 & 6 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
\times & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
2 & 0 & 2 & 4 & 6 & 8 & 10 & 12 \\
3 & 0 & 3 & 6 & 9 & 12 & 15 & 18 \\
4 & 0 & 4 & 8 & 12 & 16 & 20 & 24 \\
5 & 0 & 5 & 10 & 15 & 20 & 25 & 30 \\
6 & 0 & 6 & 12 & 18 & 24 & 30 & 36 \\
\end{array}
\]

This should seem pretty familiar to most students that are just beginning to learn mathematics, and is something familiar that they have a very good grasp of. One way to approach modular arithmetic is to expand the idea of the multiplication table so that it fits in with the ideas of modular arithmetic. Let us put forward a definition for what an operation table should be. We should be able to apply our idea of an operation table to different operations (such as \(\times\) or \(+\)) and the table should tell us how to compute things with that operation. Before we go and define what an operation table is, we should define what an operation is.

**Definition 4.** Let \(M\) be a set of objects. Then an **operation**\(^{10}\) \(\ast\) takes two things in \(R\) and creates a new thing out of it. If \(a\) is in \(M\), and \(b\) is in \(M\), we usually write this operation as \(a \ast b\). We additionally want our operation to satisfy some additional properties:

- **Closure:** If \(a\) and \(b\) are in \(M\), then \(a \ast b\) is also in \(M\).
- **Associativity:** If \(a\), \(b\), and \(c\) are in \(M\), then \((a \ast b) \ast c = a \ast (b \ast c)\)
- **Identity Element:** There is a special element \(e\), called the **identity** so that \(e \ast a = a\)

**Exercise 5.** Convince yourself that addition is an operation on the whole numbers. Also, convince that multiplication on the whole numbers is an operation. What is the identity element for addition? What about the identity element for multiplication?

Now that we know that an operation is, we can ask what talk about operation tables.

**Definition 5.** Let \(A\) be a set of things, with an operation \(\ast\) on them. Then an **operation table** is a grid where the columns and rows are labeled with elements of \(A\). If one row is labeled with \(a\), and another column labeled with \(b\), then the element in the \(a\) column and \(b\) row is \(a \ast b\). An operation table for the operation \(\ast\) will be referred to as \((T, \ast)\)

So, the standard multiplication table and addition table are the operator tables for the operations of \(+\) and \(\times\) respectively. But we can do so much more with more interesting operations out there. In particular, we can look at what these operation tables look like for clock arithmetic. We can define the operations on the clock \(+\) and \(\times\) like have done in the previous section, and build two new operation tables. For example, we could build an addition and multiplication table for addition mod 5— which we should think of addition and multiplication on a clock that has numbers 0, 1, 2, 3, 4.

---

\(^{9}\)This thing is not usually called an operation table in the mathematical literature. It is usually called a **Cayley Table**, which is a fantastic mathematical device in group theory. I guess “operation table” has a more medical sound to it, but it is easy to understand.

\(^{10}\)Something with this structure in math is usually called a **monoid**.
Notice that these addition and multiplication tables encapsulate all of the data that is required for us to do quick multiplication and adding mod 5. To make sure that your students now how to use a multiplication table, have them use these tables to quickly compute what the sum and product are mod 5 are quickly. Also, having students construct multiplication and addition tables for various sums mod n for various values of n. Now that we have constructed multiplication and addition tables, it makes sense to ask what properties these multiplication and addition tables have. For instance, you might notice on the addition table that every number between 0 and 5 shows up in every single row and column. While this property doesn’t hold for the second table, it almost does. Let us come up with a name for tables that have this property.

**Definition 6.** Let \((T, +_n)\) be an addition table for addition \(\mod n\). We say that \(T\) is **additive sudoku** if every number between 0 and \(n - 1\) shows up in every single row and column.

Let \((T, \times_n)\) be a multiplication table for multiplication \(\mod n\). We say that \(T\) is **multiplicative sudoku** if the numbers 0 to \(n - 1\) show up in every row and column besides the 0 row and column.

Frequently, I will drop the “multiplicative” and “additive” before sudoku, and just call a table “sudoku”. I hope that this is not too confusing. For example, the addition table and multiplication tables drawn above are both sudoku tables.

**Exercise 6.** Show that the multiplication for multiplication \(\mod 6\) is not sudoku. (Hint: there are faster ways to doing this than drawing out the whole entire table)

**Exercise 7.** (⋆) Show that every addition table is sudoku.

So, probably the most natural question to ask is the following:

**Question:** For what \(n\) is the multiplication table \(\mod n\) a Sudoku table?

To answer this question, we have to move over to a new topic, which is invertibility and multiplying to 0.

**2.2. Invertibility and Zero Divisors.** In mathematics, one of the most interesting properties that an operation can have is **inverses**. If you have an element, an inverse to that element is one whose product with it is the identity. Let’s make this more precise.

**Definition 7.** Suppose that \(M\) is a set of objects with \(*\) as an operation on it. Let \(x\) and \(y\) be two things in \(M\). Then \(x\) and \(y\) are **inverse to each other** if \(x * y = e\) (where \(e\) is the identity element that we identified earlier).
1. 9 and Math Magic

1.1. Introduction: A Magic Trick. Let’s start by looking at a simple magic trick.

Problem 1. Pick a number between 1 and 10. Then perform the following steps (show your work on the side!)

1. Take your number, and multiply it by 2
2. Take that number, and subtract 1 from it
3. Take that number, and multiply it by 9
4. Then take the digits of the number, and add them together. For instance, if you 34, you would now have $3 + 4 = 7$
5. Look at the phrase below. Pick the letter in the phrase corresponding to the number you now have.

   Like a pony he ran away
   For instance, if you had 7 at this point, you would pick the letter o.
6. Think of a color that begins with that letter.

When both you and your neighbors have gotten their colors, compare your answer with your neighbor. Did you have the same color? How did the magic trick work?

In this class, we will look at how this magic trick works.
1.2. Modular Arithmetic. In this section, we look at a way that numbers can be related via long-division. For example, what do the following numbers all have in common?

32, 11, 18, 4

The difference between any two of these numbers is divisible by 7! If the difference of two numbers, \(a - b\) is divisible by 7, then we say that they are congruent \(\mod 7\), and write

\[ a \equiv b \mod 7.\]

Here are a few examples of number that are congruent to each other.

- \(1 \equiv 3 \mod 2\). In fact, all odd numbers are congruent \(1 \mod 2\).
- \(3 \equiv 13 \mod 10\).
- If \(a\) divides \(b\) evenly, then \(b \equiv 0 \mod a\). Why?

Now you check some!

**Problem 2.** For each number \(a\), find the number between 0 and 4 that it is congruent to

(a) \(29 \equiv \mod 5\)

(b) \(16 \equiv \mod 5\)

(c) \(19 \equiv \mod 5\)

(d) \(501 \equiv \mod 5\)

**Problem 3 (Working \mod 2).** For each number below, find the number between 0 or 1 that it is congruent to \(\mod 2\).

(a) What is \(3 \equiv \mod 2\).

(b) What about \(5 \equiv \mod 2\).

(c) Why are all odd number congruent to \(1 \mod 2\)?

**Problem 4 (Working \mod 10).** For each number \(a\), find the number between 0 and 9 that it is congruent to.

(a) What is \(38 \equiv \mod 10\)?

(b) What about \(22 \equiv \mod 10\)?
(c) What is an easy way of telling what something is congruent to mod 10?

Congruence works well with multiplication and addition, that is if \( a \equiv p \mod n \) and \( c \equiv q \mod n \), then \( a + b \equiv p + q \mod n \), and \( a \times b \equiv c \times d \mod n \). We will prove this in a later problem, but in the meantime, you can use this fact to make the next few problems easier.

**Problem 5 (Use mod 7).** Isaac is going to have a barbecue next weekend. He buys hot dogs and he has hotdog buns at home. Hot dogs come in packages of 7. Isaac has a rule at his house, and the rule is you cannot eat a hot dog without a bun (or vice versa).

(a) Suppose that Isaac has 34 hot dog buns. How many packages of hot dogs should he buy if he doesn’t want to have left over hot dogs? How many hot dog buns will he be left over with?

(b) The very same week, Jonathan decides to have a Bratwurst party. Coincidentally, Bratwurst also is packaged in groups of 7. He has the same rule about eating bratwurst and using buns. If he starts with 22 buns, how many packages of bratwurst should he buy? How many buns will he be left over with?

(c) That weekend, Jonathan and Isaac have discovered that they are holding the barbecue in the same the same park. Why is this a good thing?

**Problem 6.** In full sentence, explain why if \( n \) divides \( a \) evenly, then there exists a whole number \( p \) so that \( a = np \)

**Problem 7.** Suppose that \( n \) divides \( a \) evenly, and also \( n \) divides \( b \) evenly. Then why does \( n \) divide \( a + b \)?

**Problem 8.** Suppose that \( a \equiv x \mod n \) and \( b \equiv y \mod n \).

1. How does the previous section show us that \( n \) divides \( (a + b) - (x + y) \)? (Hint: \( n \) divides \( a - x \), and \( n \) divides \( a - y \). Why?) Write your solution out in full sentences.

2. Why does this show that \( a + b \equiv x + y \mod n \)? Explain in full sentences.
1.3. **The Trick Explained.** How did the trick work? The trick lies in the step where you add the digits together. When we write a number between 0 and 99, we can write it as a a sum of it’s tens place and ones place. For example,

\[
25 = 20 + 5 \\
= 2 \times 10 + 5
\]

What happens when we look at a number \( n \pmod{9} \)?

\[
25 \equiv 2 \times 10 \pmod{9} \\
\equiv 2 \times 1 + 5 \pmod{9} \\
\equiv 2 + 5 \pmod{9}
\]

The sum of the digits of a number is congruent to the number \( n \pmod{9} \). Let us look closely at the magic trick. Let us say that we started with the number \( n \), and keep track of what we get.

(1) Take your number, and multiply it by 2 \( n \mapsto 2n \)
(2) Take that number, and subtract 1 from it \( 2n \mapsto 2n - 1 \)
(3) Take that number, and multiply it by 9 \( 2n - 1 \mapsto 9(2n - 1) \)
(4) Then take the digits of the number, and add them together.

This is the important step. As \( 9(2n - 1) \) is divisible by 9, we know that it is congruent to 0 \( \pmod{9} \). We also know that the sum of digits is also congruent to \( 9(2n - 1) \pmod{9} \). So we have that

\[
9(2n - 1) \equiv 0 \equiv \text{sum of the digits of } 9(2n - 1) \pmod{9}
\]

(5) Look at the phrase below. Pick the letter in the phrase corresponding to the number you now have. (which is either 9 or 18)

Like a pony he ran away

Which letters have a position that is congruent to 0 \( \pmod{9} \)? They are both \( y \). So at this point, everybody has chosen the letter \( y \).

Finally, the last step is to pick of a color that starts with the letter \( y \). Anybody think of something other than yellow?
2. Circles and Tables and Sleeping

2.1. Warm Up: The problem with sleeping Mathematicians. When we think about addition, we think about it occurring on a straight number line. However, we can think about addition on a circle instead. One easy example of this is on a clock. On an old clock, there are twelve numbers arranged in a circle.

**Problem 9.** Consider the clock with numbers $1, 2, \ldots, 12$ on it.

(a) Derek goes to bed at 8, and sleeps for 5 hours. What time will he wake up at? (Ignore AM/PM)

(b) Johnathan has a sleeping problem. He too goes to bed at 8, goes to sleep for 5 hours, but then immediately goes back to sleep again for another 5 hours. He does this three times in total. What time will he wake up at?

(c) Jeff has an even larger sleeping problem. Jeff goes to sleep at 8 as well, but he goes to sleep for 5 hours and wakes up again a total of 85 times. What time will he wake up at?

(d) Morgan, while a perfectly good sleeper, has an obsession with his favorite number. Morgan also sleep for 5 hours a night, and goes to sleep at 8. When Morgan wakes up, he looks at his clock, and if the hour hand is pointing at his favorite number, he decides to get out of bed. Will Morgan ever be able to wake up?

(e) Isaac is just like Morgan, except he only sleeps for 4 hours at a time. He too goes to bed at 8, and will only get out of bed if he sees that the clock is showing his favorite number. Why should Jeff wake him up right now and tell him that this is a bad idea?
2.2. Addition and Multiplication Tables. Remember we also had that sums and multiplication worked with \( \mod n \). If we had

\[
a \equiv c \mod n
\]

and

\[
b \equiv d \mod n
\]

then we have the congruences

\[
a + b \equiv c + d \mod n
\]

\[
ab \equiv cd \mod n
\]

This is just like regular multiplication and addition of whole numbers. However, there are a few differences: this kind of addition and multiplication is very interesting. For instance you can have two non-zero numbers multiply to 0. You can have even have a number which is its own square!

How do we capture the structure of addition and multiplication? One way is to use addition and multiplication tables. We are all familiar with the usual addition and multiplication table:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
<td>24</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
<td>30</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>18</td>
<td>24</td>
<td>30</td>
<td>36</td>
</tr>
</tbody>
</table>

However, one might consider looking at multiplication tables for modular arithmetic! This is a addition and multiplication table for adding and multiplying numbers \( \mod 5 \)

<table>
<thead>
<tr>
<th>+5</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>×5</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Problem 10 (Even and Odds). Using \( \mod 2 \), we can check if numbers are even or odd.

<table>
<thead>
<tr>
<th>×2</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

+2

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

(a) How do you use \( \mod 2 \) to check if a number is even or odd?

(b) Use an addition table for \( \mod 2 \) to show the sum of two even numbers is even. What about odd and even? Odd and odd?

(c) Use a multiplication table for \( \mod 2 \) to show that if \( a \times b \) is odd, then \( a \) and \( b \) are both odd.
Problem 11 (Unusual square numbers). Recall that we write \( x^2 \) for \( x \times x \).

(a) Can you find all numbers \( x \) so that 
\[
x^2 \equiv x \pmod{10}
\] , where \( x \) is between 1 and 10?

(b) What about all numbers so that 
\[
x^2 = x
\]  
(Note! There is no mod here!)

(c) Can you find all numbers \( x \) other than 1 so that 
\[
x^2 \equiv 1 \pmod{10}
\]

(d) What about all numbers \( x \) other than 1 so that 
\[
x^2 = 1
\]  
(Again, no mod here!)
Problem 12 (Multiplying to 0). (a) Are there any two non-zero numbers that multiply to 0? Give a proof of why or why not

(b) Can you find two numbers $a$ and $b$ so that

$$a \times b \equiv 0 \mod 10$$

(c) Find all solutions (where $0 \leq a < 10$ and $0 \leq b < 10$) to

$$ab \equiv 0 \mod 10$$

Problem 13. Construct a multiplication table and addition table for multiplying $\mod 3$

<table>
<thead>
<tr>
<th>$\times_3$</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$+$</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Problem 14. Construct a multiplication table and addition table for multiplying $\mod 4$

<table>
<thead>
<tr>
<th>$\times_3$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$+$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Problem 15. We say that a multiplication table is called **Sudoku** if no number occurs twice in any row or column, besides the 0 row or column.

(a) Can you find an example of a multiplication table \( \text{mod } n \) that is Sudoku for modular arithmetic? (Hint! Look through the tables that we have done)

(b) Can you find an example of a multiplication table that is not Sudoku?

(c) Suppose that \( b \) shows up twice in the same row \( a \) of a multiplication table. Show that \( b \) can be written as a product of \( a \) in two different ways.

(d) Can you show that if a table is not Sudoku, then there is a row with two zero’s in it?

Problem 16. We say that an addition table is **Sudoku** if no number occurs twice in any row or column.
(a) Suppose that $b$ shows up twice in the same row $a$ of an addition table. Show that $b$ can be written as a sum of $a$ in two different ways.

(b) Can you find an addition table for modular arithmetic which is *not* Sudoku? Why or why not can you find one?
Problem 17. We have so far constructed multiplication tables for multiplication \( \mod 2, \mod 3, \mod 4 \) and \( \mod 5 \).

(a) Construct a multiplication table for \( \mod 6 \)

\[
\begin{array}{c|ccccc}
\times_6 & 0 & 1 & 2 & 3 & 4 & 5 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 \\
2 & 0 & 2 & 4 & 0 & 2 & 4 \\
3 & 0 & 3 & 0 & 3 & 0 & 3 \\
4 & 0 & 4 & 0 & 4 & 0 & 4 \\
5 & 0 & 5 & 0 & 5 & 0 & 5 \\
\end{array}
\]

(b) Which rows exhibit the numbers 0 through 5?

(c) Which rows do not?

Problem 18. Which numbers have multiplication tables that are Sudoku? Do you have a conjecture on which numbers have multiplication tables that are Sudoku?
Problem 19 (A return to the sleeping Mathematicians). Jonathan, Isaac, Derek, Jeff and Morgan have gone to vacation in outer space!

(a) Derek plans on visiting the planet Mars. On Mars, they use clocks that have 7 hours on them. Derek decides on the following macabre sleep pattern: When he wakes up, he will look at his clock. He will then take whatever number he sees, and sleep for that many hours. If he wakes up at 7 o’clock, he will get out of bed. Why is this a terrible idea if he doesn’t go to bed at midnight?

(b) Isaac is on the planet Venus. On Venus, the clocks are only 6 hours long. Every time Isaac wakes up, he looks at his clock. If he has not seen that number before, he goes back to sleep. If Isaac wants to see every number on his clock, how long should each one of his naps be? (note: a proper nap is longer than 1 hour)

(c) Morgan is on the planet Jupiter. As it is quite a bit bigger than Pluto, it’s day is 11 hours long. Morgan is like Derek, and is a bit rocket-lagged from his travels. When he wakes up, he looks at his clock, and sleeps for 3 times the amount that appears on his clock. Assuming Morgan starts at 2 o’clock, Does Morgan ever look at his clock and see 11 o’clock? What about 1 o’clock?

(d) Jonathan is back to his old tricks. After traveling to Saturn, Jonathan has decided to add a bit of randomness to his life. Saturn has a clock that is 17 hours long. When he goes to sleep, he constantly dreams of numbers. When he wakes up, he has a number $x$ which is between 1 and 10 in his head. He looks at his clock, and sees the hour hand pointing to the number $y$. Jonathan then falls asleep for $x \times y$ hours. Jonathan plans on waking up at 17o’clock. Why should Morgan wake him up instead?
Dividing Zero with the Sleepwalking Bishop

3. Warm Up: A quick review of modular arithmetic

Problem 20. Fill in the blank space!

(a) \(3 + 9 \equiv \mod 10\)

(b) \(5 \times 2 \equiv \mod 7\)

(c) \(11 + 11 \equiv \mod 2\)

Problem 21 (Take mods, then Compute!). I would suggest you follow the hint—again, fill in the blank.

(1) \(13684735 \times 163873882794 \mod 2\)

(2) \(26487739 + 3687287304 \mod 10\)

(3) \(247980 \times 19378469280 \mod 10\)
4. Division mod $n$

What does it mean for a whole number $a$ to divide another number $b$? It means that there is a third number $x$, such that

$$a \times x = b$$

For example, 3 divides 12 because there exists 4 so that

$$3 \times 4 = 12$$

Finding the answer to the problem $12 \div 3$ is equivalent to solving the equation

$$3 \times x = 12$$

We have a good definition for divisibility of whole numbers. We want to use this definition for division in mod $n$ arithmetic. The way to change our old definition for divisibility of whole numbers into one for mod $n$ is to replace the equal sign with a congruence sign and stick on a mod $n$ at the end. We will say that a number $a$ divides a number $b$ mod $n$ if there exists a number $x$ that makes the following equation true

$$a \times x \equiv b \mod n$$

Here are a few examples of divisibility mod 10.

- We have that 2 divides 6 mod 10, as $2 \times 3 \equiv 6 \mod 10$
- We have that 3 divides 7 mod 10, as $3 \times 9 \equiv 27 \equiv 7 \mod 10$
- We have that 3 divides 5 mod 10, as $3 \times 5 \equiv 15 \equiv 5 \mod 10$
- We have that 5 divides 0 mod 10, as $2 \times 5 \equiv 10 \equiv 0 \mod 10$
Problem 22. Rewrite the following equations using a division sign and solve.

(1) \(5 \times x = 25\)

(2) \(7 \times x = 63\)

Problem 23. First construct a multiplication table for \(\mod 5\), then do the following divisions \(\mod 5\).

\[
\begin{array}{c|cccc}
\times 5 & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 1 & 2 & 3 & 4 \\
2 & 2 & 4 & 1 & 3 \\
3 & 3 & 1 & 4 & 2 \\
4 & 4 & 3 & 2 & 1 \\
\end{array}
\]

Rewrite each division problem as an equation, and then solve the equation. For example, if the division was \(3 \div 2\) we first write

\[2 \times x \equiv 3 \mod 5\]

and then solve for \(x\).

(a) \(4 \div 1 \equiv \mod 5\)

(b) \(4 \div 3 \equiv \mod 5\)
(c) $3 \div 4 \equiv \mod 5$

(d) $3 \div 2 \equiv \mod 5$
5. The Sleepwalking Bishop

The Bishop is a piece from the game of chess that can move diagonally. We draw the bishop with the symbol \( \text{bishop} \).

The Bishop of Bounce lives in courtyard that is covered in little squares. His yard measures 5 by 6 squares. The bishop is a sleepless fellow, and sometimes in the middle of the night he wakes up and begins to stumble around his yard. As he sleepwalks, he walks in a straight line and when he reaches a wall, he bounces off the wall and keeps on walking. For instance, one possible route the bishop may start on a particular night is

\[ \text{bishop} \]

The bishop goes back to sleep when he walks into a corner. So, the full walk that the bishop would take on the night above would be

\[ \text{bishop} \]

Problem 24. Can the Bishop ever visit every square of the courtyard? Why or why not?

Problem 25. Where should the bishop start if he wants to visit as many squares as possible when sleepwalking?

Problem 26. Is there a place that the bishop can start so never runs into a corner and falls asleep? (hint! Use the previous problem)
The Bishop of Bounce has a good friend, the Bishop of Tic-Tac-Toe. The Bishop of Tic-Tac-Toe has a courtyard that is 3 squares long by 3 squares wide.

Problem 27. Why does the Bishop of Tic-Tac-Toe sleepwalk considerably more than the Bishop of Bounce on some nights?

Problem 28. What is the shortest sleepwalk that the Bishop of Tic-Tac-Toe take?
Last year, the Bishop of Bounce and Bishop and the Bishop of Tic-Tac-Toe had a friend that passed away, the late Bishop Walkthroughwalls. His ghost now haunts the Bishop of Bounce and his neighbor’s yard! If left unstopped, he will wander the world forever. His world is like one infinitely large grid.

In order to help their friend, the Bishop of Bounce and Bishop of Tic-Tac-Toe place markers for their dead friend to rest peacefully as shown on the picture.

Problem 29. Is there a starting place on this grid which will allow the Bishop Walkthroughwalls to float on forever? How is this similar to the situation that Bishop Tic-Tac-Toe faced in his garden?

Problem 30. The Bishop of Bounce realizes there is a problem with the layout of x’s. As the Bishop of Bounce is cheap, he doesn’t want to place to crosses next to each other. How can he place marks across the infinite grid so that the late Bishop Walkthroughwalls will find a resting place no matter where he starts?
6. Primes Numbers and Zero Divisors

You may have heard of prime numbers before. What is a prime number? We will use this definition:

**Definition 1.** We call a whole number \( p \) prime if the only numbers that divide \( p \) are 1 and \( p \).

What are a few examples of prime numbers? Well, 2, 3, 5, 7, 11… are a few examples of prime numbers that you may have heard of.

We also want to talk about when a non-zero numbers divide 0! Here are some examples:

- 4 divides 0 \( \mod 10 \) because \( 4 \times 5 \equiv 20 \equiv 0 \mod 10 \)
- 2 divides 0 \( \mod 10 \) because \( 2 \times 5 \equiv 10 \equiv 0 \mod 10 \)
- 5 divides 0 \( \mod 10 \) because \( 5 \times 8 \equiv 40 \equiv 0 \mod 12 \)

We say that if \( a \times b \equiv 0 \mod n \), and neither \( a \) or \( b \) is congruent to 0 \( \mod n \), then we call \( a \) a **zero divisor**. So 2, 4 and 5 are all examples of zero divisors \( \mod 10 \).

**Problem 31.** Check if the following numbers divide 0 \( \mod 12 \)

(a) Does 4 divide 0 \( \mod 12 \)?

(b) Does 7 divide 0 \( \mod 12 \)?

(c) Does 2 divide 0 \( \mod 12 \)?

(d) Does 3 divide 0 \( \mod 12 \)?

**Problem 32.** Find all the zero divisors between 1 and 5 for multiplication \( \mod 6 \)
Problem 33 (Not-Unique Division and Zero Divisors). We show that if you have non-unique division, you can find a zero divisor.

(a) Find a number $x$ between 0 and 9 so that
$$2 \times x \equiv 4 \mod 10$$

(b) Find a different number $y$ between 0 and 11 so that
$$2 \times y \equiv 4 \mod 10$$

(c) Subtract the first congruence from the second one. Conclude that 2 is a zero divisor in $\mod 10$ arithmetic.

Problem 34 (Zero Divisors and Not-Unique Division). We show that if you have a zero divisor, then division is not unique.

(a) Find a number $z$ between 1 and 9 so
$$5 \times z \equiv 0 \mod 10$$

(b) Find a number $x$ between 1 and 9 so that
$$5 \times x \equiv 5 \mod 10$$

(c) Add the two congruences together to conclude that there is a number $y \neq x$ so that
$$5 \times y \equiv 5 \mod 10$$
and conclude that division is not unique $\mod 12$. 
Problem 35 (Division is unique mod 5). Construct a multiplication table for mod 5

<table>
<thead>
<tr>
<th>×5</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

If $a$ divides $c$ mod 5, then there is a number $b$ so that

$$a \times b \equiv c \pmod{5}$$

Show that if $a$ divides $c$ mod 5, then there is unique $b$ so that

$$a \times b \equiv c \pmod{5}$$

(Hint! Use the multiplication table above, as well as the method for finding division that you came up with in Problem 36)
Problem 36 (A method for Division using multiplication tables). Let’s find a faster way to do division using Multiplication tables.

(a) Let’s say that I wanted to find $30 \div 6$. Describe how I would find the solution using this multiplication table.

\[
\begin{array}{cccccccc}
\times & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
2 & 0 & 2 & 4 & 6 & 8 & 10 & 12 \\
3 & 0 & 3 & 6 & 9 & 12 & 15 & 18 \\
4 & 0 & 4 & 8 & 12 & 16 & 20 & 24 \\
5 & 0 & 5 & 10 & 15 & 20 & 25 & 30 \\
6 & 0 & 6 & 12 & 18 & 24 & 30 & 36 \\
\end{array}
\]

(b) Let’s say that I wanted to tell if $a$ was divisible by $b$. How could I use the multiplication table to quickly find this out? What if $a$ was divisible by $b$, how would I find $a \div b$?

Problem 37 (Division using whole numbers is unique). Can you find a different number greater than 0 so that

\[2 \times c = 3\]

Explain.

Problem 38 (Division is not unique mod 12). (a) Show that 2 divides 6 in mod 12 arithmetic by finding a number $b$ greater than 0 and less than 12 so that

\[2 \times b \equiv 6 \mod 12\]
(b) Can you find another number $c$, so that 
\[ 2 \times c \equiv 6 \pmod{12} \]

(c) With this in mind, does $6 \div 2$ make any sense \( \pmod{12} \)?

**Problem 39 (Finding a number with a zero divisor).** Here we will be using the definition of prime to help us. Recall that if $n$ is *not* prime, it can be written as $a \times b$ for some numbers $a$ and $b$, neither of which are 1.

(a) Show that $a$ is a zero divisor \( \pmod{n} \)

(b) Conclude that if a number is *not* prime, it has a zero divisor.
Problem 40. Recall from last week that we call a multiplication table Sudoku if it contains every number once in each row and column (besides the 0 row and column).

(a) Why is it if a $\mod p$ multiplication table is Sudoku, then there only one solution to $a \div b \mod n$? (Hint: Think about Problem 36)

(b) Why does it follow that if a $\mod p$ multiplication table is Sudoku, there are no zero divisors?
Problem 41 (A return to the sleeping Mathematicians). Jonathan, Isaac, Derek, Jeff and Morgan have gone to vacation in outer space!

(a) Derek plans on visiting the planet Mars. On Mars, they use clocks that have 7 hours on them. Derek decides on the following macabre sleep pattern: When he wakes up, he will look at his clock. He will then take whatever number he sees, and sleep for that many hours. If he wakes up at 7 o’clock, he will get out of bed. Why is this a terrible idea?

(b) Isaac is on the planet Venus. On Venus, the clocks are only 6 hours long. Every time Isaac wakes up, he looks at his clock. If he has not seen that number before, he goes back to sleep. If Isaac wants to see every number on his clock, how long should each one of his naps be? (note: a proper nap is longer than 1 hour)

(c) Morgan is on the planet Jupiter. As it is quite a bit bigger than Pluto, it’s day is 11 hours long. Morgan is like Derek, and is a bit rocket-lagged from his travels. When he wakes up, he looks at his clock, and sleeps for 3 times the amount that appears on his clock. Assuming Morgan starts at 2 o’clock, Does Morgan ever look at his clock and see 11 o’clock? What about 1 o’clock?
Solutions

(2, a) $29 \equiv 4 \mod 5$
(2, b) $16 \equiv 1 \mod 5$
(2, c) $19 \equiv 4 \mod 5$
(2, d) $501 \equiv 1 \mod 5$

(3, a) $3 \equiv 1 \mod 2$
(3, b) $5 \equiv 1 \mod 2$
(3, c) Because an odd number minus 1 is even, and all even numbers are divisible by 2.

(4, a) $38 \equiv 8 \mod 10$
(4, b) $22 \equiv 2 \mod 2$
(4, c) You can just take the last digit of the number when written out, and it will be congruent to the number $\mod 10$. This is because a number minus its last digit ends in 0, and all numbers that end in 0 are divisible by 10.

(5, a) Since hot dogs show up in packages of 7, the number of buns that will be left over at the end of the day will be a number between 0 and 6. Therefore, we are looking for a number between 0 and 6 that the 34 buns are congruent to, which is $6 \equiv 34 \mod 7$.
(5, b) Following the logic of the previous problem, we expect Jonathan to have a number congruent to $22 \mod 7$ which is between 0 and 6. This number is $22 \equiv 1 \mod 7$.
(5, c) It’s a good thing, because the number of buns they have together is divisible by 7. This is because

$$22 + 34 \equiv 1 + 6 \mod 7$$

$$\equiv 7 \mod 7$$

$$\equiv 0 \mod 7$$

(6, 3) If $n$ divides $a$ evenly, then $n$ fits into $a$ a whole number of times. Let’s say that this number is $p$. Then we know that $a = np$

(7, 3) $n$ divides $a$, so $a = pm$ for some multiplier $p$ (by the definition of divides). Furthermore, $b = qn$, for some multiplier $q$. Then

$$a + b = pm + qn$$

$$= (p + q)n$$

which shows that $n$ divides $a + b$.

(8, 1) $n$ divides $(a - x)$, and $n$ divides $(b - y)$ so by the problem 7, we have that $n$ divides their sum $(a - x) + (b - y)$. Rearranging the signs yields the $n$ divides $(a + b) - (x + y)$.
(8, 2) \( n \) divides the difference of \((a + b)\) and \((x + y)\), so the two must be congruent \( \mod n \) by the definition of congruence,

(9, a) He will sleep until \( 8 + 5 = 13 \) o’clock, which is congruent to \( 1 \mod 12 \)

(9, b) He sleeps for 15 additional hours, so a total of
\[
8 + 15 = 23 \text{ hours}
\]
which is equal to 11 on the clock

(9, c) We use modular arithmetic here to make the problem a bit simpler. We note that
\[
5 \times 85 \equiv 5 \times 1 \mod 12
\equiv 5 \mod 12
\]
Therefore Jeff sleeps for 5 hours; meaning that he will wake up at 1

Look at the sequence of numbers that Morgan sees when he wakes up:
\[
8 \rightarrow 1 \rightarrow 6 \rightarrow 11 \rightarrow 4 \rightarrow 9 \rightarrow 2 \rightarrow 12 \rightarrow 5 \rightarrow 10 \rightarrow 3 \rightarrow 8
\]
As you can see, every number between 1 and 12 shows up in this sequence, so Morgan will be able to wake up.

(9, e) Let us look at the sequence of number that Isaac sees when he wakes up:
\[
8 \rightarrow 12 \rightarrow 4 \rightarrow 8 \rightarrow 12
\]
This repeats as a pattern, so Isaac may not be able to wake up, if his number is, for instance, 1

If a number is even, it is divisible by 2, so it is congruent to \( 0 \mod 2 \). If a number is odd, then it must be congruent to \( 1 \mod 2 \) (Why?)

(11, a) 0, 1, 5, 6 all are their own squares \( \mod 10 \)

(11, b) The only number that is its own square is 1

(11, c) 1, 9 square to 1.

(11, d) 1 and \(-1\) (Why are there no others?)

(12, a) For natural numbers, certainly not, because \( a \times b \geq a \) and we assumed that \( a > 0 \) and \( b > 0 \)

Certainly,
\[
2 \times 5 \equiv 0
\]

(15, a) Any prime will work

(15, b) Any non-prime will work

(15, c) If \( b \) shows up in a row twice, then \( b = ac \) and \( b = ad \), where \( c \) and \( d \) are the columns that \( b \) appears in
If a table is not Sudoku, then $b = ac$ and $b = ad$. Subtracting, we have
\[ b - b = ac - ad = a(c - d) \]
Since $c \neq d$, this means that $c - d \neq 0$, so 0 appears twice in the $a$ row. $a \times 0 = a \times (c - d) = 0$

(16, a) If $b$ shows up in a row twice, then $b = a + c$ and $b = a + d$, where $c$ and $d$ are the columns that $b$ appears in

(16, b) You cannot, because if you could, let $b$ be in the $a$ row and $c$ and $d$ column. $a + c = b = a + d$ which tells us that $b = d$.

(19, a) We know that using a 7 hour clock is like taking a number \mod 7, so let us first examine the problem without taking the \mod. Suppose Derek goes to sleep at 1. Then Derek’s sleep pattern is:
\[ 1 \rightarrow 2 \rightarrow 4 \rightarrow 8 \rightarrow 16 \rightarrow 32 \rightarrow 64 \ldots \]
So Derek sleeps at hours that appear like $2^n$. However, there is no number that is not a multiple of 7 that you can multiply to get a multiple of 7. Therefore, $2^n \neq 0 \mod 7$ for any $n$, so Derek will never wake up.

(19, b) If Isaac sleeps for 5 hours a night, it will work, as his sleep pattern will be
\[ 6 \rightarrow 5 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 1 \rightarrow 6 \]

(19, c) Using the trick that was developed in Derek’s sleeping problem, we see that Morgan will sleep according to powers of 4.
\[ 3 \rightarrow 3 \times 4 \rightarrow 3 \times 4^2 \rightarrow 3 \times 4^4 \]
By checking these numbers, you can see that Morgan will see 2, but never 11

(19, d) Every time Jonathan sleeps, he sleeps til the time $(x + 1) \times y$ hours. However, $(x + 1) \neq 0 \mod 17$, so $(x + 1) \times y \neq 0 \mod 17$. So Jonathan never sees 17.

\[ 3 + 9 \equiv 2 \mod 10 \]
\[ 2 \times 5 \equiv 3 \mod 7 \]
\[ 11 + 11 \equiv 0 \mod 2 \]
We take mods first, so this is the same as
\[ 1 + 0 \equiv 1 \mod 2 \]
We take mods first, so this is the same as
\[ 9 + 4 \equiv 3 \mod 10 \]
We take mods first, so this is the same as
\[ 0 \times 0 \equiv 0 \mod 10 \]
\[ 25 \div 5 = 5 \]
\[ 63 \div 7 = 9 \]
\[ 1 \times x \equiv 14 \mod 5 \]
\[ x \equiv 4 \mod 5 \]
\[ 41 \]
3 \times x \equiv 4 \mod 5
\quad x \equiv 3 \mod 5
4 \times x \equiv 3 = 1 \mod 5
\quad x \equiv 2 \mod 5
2 \times x \equiv 3 = 1 \mod 5
\quad x \equiv 4 \mod 5

Checkerboard the chess board. The bishop can only visit the color of square he starts on, so he cannot visit all of the squares.

Imagine we take the bishop and we run him in the opposite direction. He can continue going in the opposite direction that he starts in as long as he doesn’t run into a corner. From here, it makes sense that the bishop must start from a corner.

No, because he visits every other square.

On some nights, he goes on a path that doesn’t ever stop; if he doesn’t start on the center square or in a corner, he will continue to walk forever.

1 square: he could start in a corner, facing toward the corner.

If he starts in between two 2, he will walk on forever.

If he lays out the x like his own courtyard, it will work.

Yes, as \(4 \times 3 \equiv 0 \mod 12\)

No

Yes, as \(2 \times 6 \equiv 0 \mod 12\)

Yes, as \(4 \times 3 \equiv 0 \mod 12\)

2, 3, 4

\(2 \times 2 \equiv 4 \mod 10\)

\(2 \times 7 \equiv 4 \mod 10\)

\begin{align*}
0 & \equiv 4 - 4 \mod 10 \\
& \equiv 2 \times 7 - 2 \times 2 \mod 10 \\
& \equiv 2 \times (7 - 2) \mod 10 \\
& \equiv 2 \times 5 \mod 10
\end{align*}

Find first 30 in the 6 row, and see what column it is in.
Look for $a$ in the $b$ column, and then the row it appears in would be $a \div b$

$2 \times 3 \equiv 6 \mod 12$

$2 \times 9 \equiv 18 \equiv 6 \mod 12$

No it does not because $9 \not\equiv 3 \mod 12$

$a \times b \equiv n \equiv 0 \mod n$

If a number $c$ is not prime, then it can be written as $a \times b = c$ where $a \neq c$. 
APPENDIX A

Abstract Algebra

0.1. Basics about Rings. We need to talk about rings. They are super-important, and you’ve known about them your whole entire life. Rings are the objects that we work with the most: objects that have a notion of addition and one of multiplication. We require the addition operation to be abelian, and we require that the multiplication operation distributes over the addition operation as well.

Definition 8. A Ring is a set of elements \( R \) with two operations, \(+ : R \times R \to R\) and \( \cdot : R \times R \to R\) satisfying the following properties:

1. \((R, +)\) form an abelian group, with identity written as \(0\).
2. \((R, \cdot)\) forms a monoid— that is:
   a. There exists an identity \(1\) such that for all \(r \in R\) we have that \(1 \cdot r = r \cdot 1 = r\).
   b. The operation \(\cdot\) is associative, that is for all \(a, b, c \in R\) we have that \((a \cdot b) \cdot c = a \cdot (b \cdot c)\).
3. The multiplication operation distributes across the addition operation, that is for all \(a, b, c \in R\) we have that
   \[a \cdot (b + c) = a \cdot b + a \cdot c\]
   \[(b + c) \cdot a = b \cdot a + c \cdot a\]

So a ring is an abelian group with a multiplication structure. The important thing about this multiplication structure is that it plays well with the additive group structure, and by “play well”, I mean that we have the distributive rule. Notice that the multiplication need not be commutative, nor have inverses. While this may seem like too little structure for multiplication, most of the interesting rings out there are the ones that are either non-commutative, or do not have a good idea of multiplicative inverses. The fact that the multiplication must distribute over the addition gives us enough additional structure that we can make do without the idea of commutivity or inverse. For notation, we will frequently drop the multiplication sign and write \(a \cdot b = ab\).

I bet you are already familiar with a bunch of rings, so let's look at a few more:

1. \(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\) all form rings with the usual multiplication and addition structures. Note, however, that \(\mathbb{N}\) is not a ring, as it does not have additive inverses.
2. The set of cyclic rings, written \(\mathbb{Z}/n\mathbb{Z}\), have elements \(\{0, 1, 2, \ldots, n - 1\}\) and has addition given by addition \(\mod n\) and multiplication by multiplication \(\mod n\).
3. Let \(C(\mathbb{R})\) denote the set of all continuous functions on \(\mathbb{R}\). Then these form a ring with multiplication and addition of functions defined pointwise. You could additionally consider the set \(C^\infty(\mathbb{R})\), the set of all smooth continuous functions— you have to check that the product and sum of smooth functions is again smooth.
Let $R$ be a ring. $\mathbb{M}_n(R)$, the set of $n \times n$ matrices with entries in $R$, form a ring with the usual addition and matrix multiplication. You could also consider the rings $GL_n(R)$ the set of all invertible matrices, or $SL_n(R)$, the set of all invertible matrices over $R$.

The quaternion ring, $\mathbb{H}$ is given by $\mathbb{R}[1, i, j, k]$ forms a ring with $\mathbb{R}$ as a subring. The ring is constructed as follows: The elements of $\mathbb{R}[1, i, j, k]$ are those vector space with basis vectors $1, i, j, k$. We define the addition on this ring by the addition of vectors, and multiplication of the basis vectors by the multiplication table

\[
\begin{array}{c|cccc}
1 & i & j & k \\
\hline
1 & 1 & i & j & k \\
i & i & -1 & k & j \\
j & j & -k & -1 & i \\
k & k & -j & -i & -1 \\
\end{array}
\]

The quaternion ring is super important, and I would be come super familiar with them, because they show up everywhere.

The last two rings are examples of rings that do not have commutative multiplication.

**Exercise 8.** Check that some of the things I claimed were rings were actually rings. If you want a tricky one, try the quaternion ring.

Notice that every single ring has at least one element which has no multiplicative inverse-- the 0 element. You should prove this if you have some time. We have a bunch of nice properties that a ring can have. Before we continue, let us assign special names for 3 special types of rings.

**Definition 9.** Let $R$ be a ring. Then

- If $R$ has commutative multiplication, it is called a commutative ring.
- If every element of $R$ besides 0 has a multiplicative inverse, then it is called a division ring.
- If $R$ is both a commutative ring and a division ring, it is called a field.

**Exercise 9.** Can you classify which of the above rings from the example are fields? Commutative? Division rings?

### 0.2. Commutative Rings

In this section, we will assume that the rings that we talk about are commutative. Most of the results in this section can carry over in one form or another to noncommutative rings, but they are just a little more difficult to work with. So, unless I specify a specific ring in this section, whenever I say “ring” in this section I really mean “commutative ring.”

Let us back up to the integers as an example of a ring. If we look at the subset of all even numbers, we notice that this subset is “downward closed”- that is, the product of any even number with any other number is again another even number. This is also true of the “threenen” numbers (which is the set of all multiples of 3 in $\mathbb{Z}$) and so on. When we talk about ring, these downward closed subsets are going to capture a lot of the structure of the ring, and are therefore interesting to talk about.

---

1. I think it would be very interesting to develop a Math Circle centered around using the quaternions. This would definitely be too advanced for 5th and 6th graders, but I think would be just fine for a HS group. There is plenty of interesting history behind the quaternions, and their applications are numerous.
Definition 10. Let $R$ be a ring. We call a subset $I \subset R$ 

- **left ideal** if for all $s \in I$ and $r \in R$ we have that $rs \in I$.
- **right ideal** if for all $s \in I$ and $r \in R$ we have that $sr \in I$.
- **two-sided ideal** (or when unambiguous, **ideal**) if for all $s \in I$, $sr, rs \in I$.

Notice that being an ideal is stronger than being just multiplicatively closed. It means that multiplying things inside $I$ with things outside of $I$ winds up back inside $I$. Here a few examples of ideals various rings:

1. Let $\mathbb{Z}$ be the ring integers. Pick some specific integer $n$. Then $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ is an ideal of our ring.
2. Let $k$ be a field. Then the only ideals of $k$ are just $\{0\}$ and $k$.
3. Let $C(\mathbb{R})$ be the set of continuous functions on $\mathbb{R}$. Then the set of all functions that have a 0 at the origin is an ideal.
4. Let $\mathbb{R}[x]$ be the set of polynomials $f(x)$ with coefficients in $\mathbb{R}$. Then the set of all polynomials that are at least degree $n$ is an ideal.

Ideals can have some special properties, and you should become comfortable with these various special properties that an ideal can have.

Exercise 10. Show that in a commutative ring, all of the left and right ideals are two sided ideals.

Exercise 11. An ideal $P \subset R$ is called a **prime ideal** if for every pair of elements $r, s \in R$, whenever $rs \in P$ we know that either $r \in P$ or $s \in P$. Let $\mathbb{Z}$ be the ring of integers. Show that if $p$ is a prime, that the set $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

Exercise 12. An ideal $M \subset R$ is called a **maximal ideal** if $M \neq R$ and there are no ideals that contain $M$. Show that every maximal ideal is prime.

Exercise 13. ($\star$) Let $C(\mathbb{R})$ be the ring of continuous function on $\mathbb{R}$. Show that the set 

$$I_{1,2} = \{f(x) \mid f(1) = f(2) = 0\}$$

is a prime ideal of $C(\mathbb{R})$, but is not maximal. Find what maximal ideal it is contained in.

Exercise 14. Let $\mathbb{Z}$ be the ring of integers.

(a) Show that the only ideals of $\mathbb{Z}$ are the subsets $n\mathbb{Z}$ (defined above)
(b) Show that if $a|b$, then $b\mathbb{Z} \subset a\mathbb{Z}$.
(c) Find all of the prime ideals of $\mathbb{Z}$. (hint: the name should be revealing!)
(d) Show that the only maximal ideals of $\mathbb{Z}$ are the prime ideals.

Before we get much farther, we should define what “good” functions between rings are. The functions that we should be thinking about when we talk about rings are those that respect the ring operations.

Definition 11. Let $R$ and $S$ be two different rings. We say that $\phi : R \to S$ is a **ring homomorphism** if the following properties hold:

1. Let $a, b \in R$. Then $\phi(a + b) = \phi(a) + \phi(b)$
2. Let $a, b \in R$. Then $\phi(ab) = \phi(a)\phi(b)$
EXERCISE 15. Show that there is a ring homomorphism from $\mathbb{C}$ to $GL_2(R)$ by sending $a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

EXERCISE 16. Let $\phi : R \to S$ be a ring homomorphism. The kernel of $\phi$ is the set of all elements that are mapped to zero, that is $\ker(\phi) = \{ r \in R | \phi(r) = 0 \}$ Show that $\ker(\phi)$ is an ideal of $R$.

EXERCISE 17. (⋆) Construct a similar map $\phi : \mathbb{H} \to GL_2(\mathbb{C})$.

Finally, let’s provide a few constructions for new rings out of the old ones that we already have.

DEFINITION 2. Here is a variety of constructions for rings

(1) Let $R$ and $S$ be two different rings. Then the product of $R$ and $S$ is denoted $R \times S$ and
   • As a set, $R \times S = \{(r, s) | r \in R, s \in S\}$
   • As a ring, has product and addition defined component-wise so that
     $(r, s)(r', s') = (rr', ss')$
     $(r, s) + (r', s') = (r + r', s + s')$

(2) Let $R$ be a ring, and $I$ an ideal. Define an equivalence relation on $R$ by $r \sim_i s$ if $i - s \in I$.
   Then the quotient of $R$ by $S$ is denoted $R/S$ and
   • As a set, $R/S$ is the equivalence classes of $R$ under $\sim$.
   • Let $[r], [s]$ be two different equivalence classes. Then $[r][s] = [rs]$, and $[r + s] = [r] + [s]$

EXERCISE 18. (⋆) Check that these definitions actually produce rings.

EXERCISE 19. Show that $\mathbb{Z}/n\mathbb{Z}$ isomorphic to arithmetic to integers mod $n$.

EXERCISE 20. Suppose that $M$ is a maximal ideal of $R$. Show that $R/M$ is a field.

EXERCISE 21. Show that $\mathbb{Z}/p\mathbb{Z}$ is a field for every prime $p$. 

48