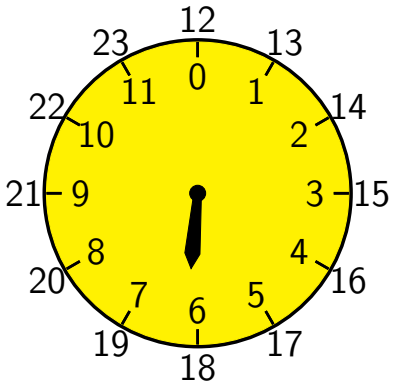
MODULAR ARITHMETIC

1 Societal usage of clock face arithmetic

In math class, everyone is used to counting, adding, and multiplying integers on the straight number line. However, there is a second, secret number system hiding in plain sight that all people are familiar with. This secret system is how we tell time! We can call it *clock face arithmetic*. We turn a circle into a number line by dividing it into twelve equal parts. In this case, one step is usually called one hour.



The hour hand moves from 0 to 1, from 1 to 2, ..., from 11 to 12 just as it would have on the straight number line. However, 12 "equals" 0 on this circle, so there it goes again, from 1 to 2, and so on. We write down the fact that 12 "equals" 0, 13 'equals" 1, 14 'equals" 2, and so on as

$$12 \equiv 0 \pmod{12}, \quad 13 \equiv 1 \pmod{12}, \quad 14 \equiv 2 \pmod{12}, \ldots$$

We formally read the above notation as *12 is congruent to 0 modulo 12*, *13 is congruent to 1 modulo 12*, and *14 is congruent*

to 2 modulo 12. While the usual = sign is reserved for equality on the straight number line; we use $\equiv$ for equality (which we call congruence) on the circle instead. Note that the symbol (mod 12) tells us that the circle is divided into 12 equal parts.

Problem 1 *Write down the smallest integers between* 0 *and* 11 *such that the following congruences are true.*

$$21 \equiv \qquad\qquad (\text{mod } 12)$$

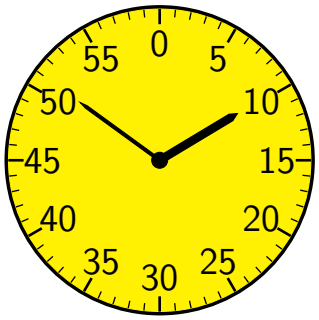
$$80 \equiv \qquad\qquad (\text{mod } 12)$$

$$9 + 4 \equiv \qquad\qquad (\text{mod } 12)$$

$$24 - 2 \equiv \qquad\qquad (\text{mod } 12)$$

Problem 2 *An experiment in a biological lab starts at 7:00 AM and runs for 80 hours. What time will it end?*

Another standard (societal) way to turn a circle into a number line is to divide it into 60 equal parts. Depending on the situation, the unit step is called either a minute or a second.



All the numbers living on this number line are considered modulo 60. We can define the congruence of integers modulo 60 just as we did modulo 12. In particular, we have $60 \equiv 0 \pmod{60}$, $61 \equiv 1 \pmod{60}$, $62 \equiv 2 \pmod{60}$ and so on.

Problem 3 *Write down the smallest integers between 0 and 59 such that the following congruences are true.*

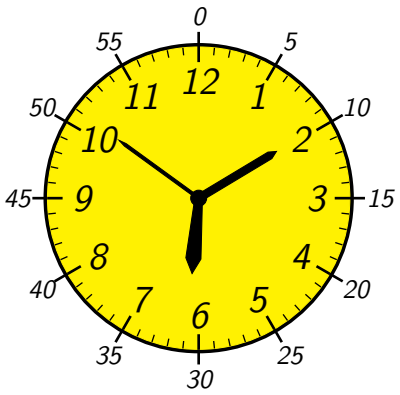
$$72 \equiv \qquad\qquad (\text{mod } 60)$$

$$-15 \equiv \qquad\qquad (\text{mod } 60)$$

$$55 + 55 \equiv \qquad\qquad (\text{mod } 60)$$

$$240 - 59 \equiv \qquad\qquad (\text{mod } 60)$$

Problem 4 *What is the time, in hours, minutes, and seconds, on the clock below?*



There are 24 hours in a day, so one further standard way to turn a cricle into a number line is to divide it into 24 equal parts. The US military uses the 24-hour clock. On the following page is a photograph of the 24-hour clock from the USS (United States Ship) *Mullinnix*, the last "all gun" US Navy destroyer in the Pacific, decommissioned in 1982.[1]

[1]See its homepage at `http://www.ussmullinnix.org/`

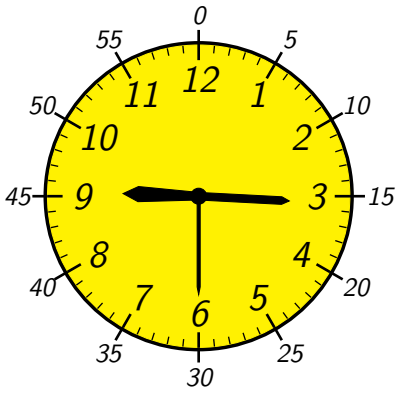
USS *Mullinnix* 24-hour clock.[2]

Since $60 \div 24$ is not a whole number, we can't use the same marks on the face of a 24-hour clock for minutes and hours (to better see this, please find the minute and hour marks on the face of the USS *Mullinnix* clock). $60 \div 12 = 5$, so this inconvenience doesn't exist for the clocks and watches we are used to. On the other hand, to disambiguate between, say, 1 o'clock night time and 1 o'clock afternoon, we have to use the A.M./P.M. notation not needed in the military. In their language, 1 o'clock P.M. is 13:00, plain and simple.

Problem 5 *What time does the USS Mullinnix clock show?*

[2]Downloaded from `http://www.ussmullinnix.org/MuxMemorabilia.html`

Problem 6 *What is the time on the clock below?*

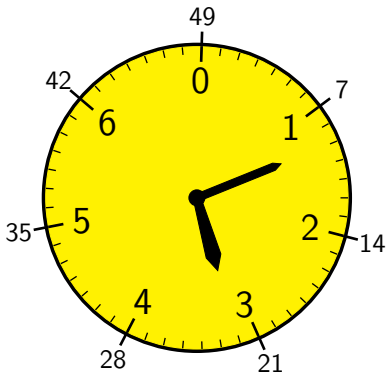


Suppose that this is the time P.M. How would the military call it?

Problem 7 *On the left, draw the civilian clock showing 1:45 P.M. On the right, draw the military clock showing 1:45 P.M.*

2 Generalizing clock face arithmetic

The planet of Heptadium in a galaxy far, far away makes one full rotation around its axis in 7 heptahours. The folks inhabiting Heptadium use heptahour clocks, pictured below.



They further divide a heptahour into 49 heptaminutes and a heptaminute into 49 heptaseconds. The heptahours are marked on the inside of the dial, the heptaminutes – on the outside.

Problem 8 *What time does the above heptahour clock show (in heptahour and heptaminutes)?*

Problem 9 *One Heptadian tells another, "The next day will begin in one minute." What time is his watch showing (in heptahour and heptaminutes)?*

Problem 10 *An experiment in a Heptadium nuclear lab starts at 4:00 and runs for 2000 hours. What time will it end?*

Problem 11 *They run four experiments in a Heptadium biological lab. The first three take an equal amount of time, the last experiment is as long as the first three together. The experiments are run one after another without time gaps. The first begins at 1:00. The last ends at 2:00. The first experiment takes more than a day, but less than two days and lasts a whole number of hours. How long does the last experiment take?*

As the example of the Heptadians shows, there is nothing stopping us from doing "clock face arithmetic" modulo any integer greater than 1. While humans typically do clock face arithmetic using 12, 24, or 60 as the *modulus*, the heptadians use 7 and 49 as the modulus instead. Indeed, mathematicians have thoroughly developed clock face arithmetic into the subject called *modular arithmetic*, which finds many usages throughout both pure and applied mathematics. We will try to develop the foundations of modular arithmetic ourselves!

In order to better understand modular arithmetic, we first need to know a little bit about sets. In math, a *set* is simply a collection of objects that we want to work with. For our purposes, we will only work with sets that contain integers. Sets are important as they allow us to easily talk about which integers we are interested in. You can think of sets as being organizational boxes that allow us to group together the integers in whatever ways we want. Because of this, we do not care about the order of the integers in sets. We also don't allow repeats in sets. Again, this is all because we simply use sets as ways to group the integers together. Let's consider the following example:

$$A = \{1, 2, 3\}.$$

A is the name we gave to our set that contains the integers $1, 2, 3$. Notice that when writing sets, we write the integers between curly brackets $\{\cdots\}$. As the order of the integers in the set A doesn't matter, we could have also defined A as

$$A = \{2, 3, 1\} \quad \text{or} \quad A = \{3, 1, 2\} \quad \text{or} \quad A = \{3, 2, 1\} \ldots$$

Of course, A is not the only set we can define. Consider the following examples.

$$B = \{-4, 0\}, \quad C = \{-1, -2, -3, \ldots\}, \quad D = \{\text{even integers}\}.$$

The set B shows that our sets can contain 0 or negative integers too. The set C shows that there is nothing stopping us from defining sets that contain infinitely many integers! In this case, C is the set of all negative integers. Notice how we used the ellipses $\ldots$ so that we can avoid writing down all of the negative integers forever. You should only use ellipses when the definition of your set is clear. Finally, the set D also contains infinitely

many integers, and shows that we can define sets using words as well. We could have also written D as

$$D = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}.$$

The equivalent ways of defining the sets A and D in our above examples brings up the natural notion for when two sets are equal. We say two sets are equal when they contain exactly the same objects. Determining when two sets are equal may not be as easy as it sounds.

Problem 12 *True or false: the following pairs of sets are equal.*

$\{0, 1\} = \{1, 0\}$ _____

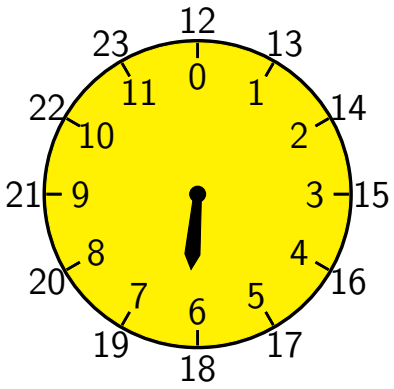
$\{-1, 0, 1\} = \{1, 0\}$ _____

$\{0, 1, 2, 3, \ldots\} = \{\text{positive integers}\}$ _____

$\{5, 6, 7, \ldots\} = \{\text{integers} \geq 5\}$ _____

$\{1+12, 1+24\} = \{25, 25-12\}$ _____

We can use the mathematical tool of sets to better understand clock face arithmetic modulo 12. Remember, we turn the circle into a number line by dividing it into 12 parts as below.



This circular number line tells us which integers we want to be "the same". So, for an integer a, we can use the circular number line to find all of the integers that a is congruent to modulo 12. Starting at a, we can move around the circle clockwise n times to get to $a + n \cdot 12$. We can also move around the circle counterclockwise n times to get to $a + n \cdot (-12)$. So, the set of all integers that a is congruent to modulo 12 is

$$[a]_{12} = \{a, a \pm 12, a \pm 2 \cdot 12, a \pm 3 \cdot 12, \ldots\},$$

which we call the *congruence class of* a *modulo* 12. For example, the congruence classes of 0, 1, and 2 modulo 12 are

$$[0]_{12} = \{\ldots, -36, -24, -12, 0, 12, 24, 36, \ldots\},$$

$$[1]_{12} = \{\ldots, -35, -23, -11, 1, 13, 25, 37, \ldots\},$$

$$[2]_{12} = \{\ldots, -34, -22, -10, 2, 14, 26, 38, \ldots\}.$$

Problem 13 *Write down all of the congruence classes modulo 12. How many are there in total? We will include for you the ones already listed above.*

$$[0]_{12} = \{\ldots, -24, -12, 0, 12, 24, \ldots\}$$

$$[1]_{12} = \{\ldots, -23, -11, 1, 13, 25, \ldots\}$$

$$[2]_{12} = \{\ldots, -22, -10, 2, 14, 26, \ldots\}$$

Problem 14 *Fill in the set definition for the following congruence classes.*

$$[21]_{12} = \{ \qquad \}$$

$$[9 \cdot 2]_{12} = \{ \qquad \}$$

$$[2-24]_{12} = \{ \qquad \}$$

The main takeaway is that, for integers a, b, we can determine if a is congruent to b modulo 12 by checking to see if b is in the set $[a]_{12}$ or not. Actually, we have the following two results which characterize congruency via equality of sets.

Problem 15 *Let a, b be integers. Prove that if a is congruent to b modulo 12, meaning b is in the set $[a]_{12}$, then $[b]_{12} = [a]_{12}$.*

Problem 16 *Let a, b be integers. Prove that if $[b]_{12} = [a]_{12}$, then a is congruent to b modulo 12 meaning that b is in the set $[a]_{12}$. Hint: this should be very, very simple.*

Together, Problem 15 and Problem 16 say that two integers are congruent modulo 12 if and only if their congruence classes are equal! This set equality definition of congruency will let us easily generalize clock face arithmetic to any modulus $M \geq 2$.

Problem 17 *Let $M \geq 2$ and a both be integers. Can you define the congruence class of a modulo M?*

$$[a]_M = \{ \qquad \}$$

Problem 18 *Let $M \geq 2$ and a, b all be integers. Recall we say that a is congruent to b modulo 12 if $[a]_{12} = [b]_{12}$ as sets. Also, when a is congruent to b modulo 12, we write $a \equiv b \pmod{12}$. Can you define when a is congruent to b modulo M using your answer from Problem 17? When a is congruent to b modulo M, we will write $a \equiv b \pmod{M}$.*

And we've done it! Problem 17 and Problem 18 define modular arithmetic for us using any modulus $M \geq 2$! Of course, these definitions on their own do not mean much. We should actually develop a few rules about how congruence, modular addition, and modular multiplication work!

3 Modular congruence, addition, and multiplication

As we already know, we can think of congruency modulo M as two numbers being "equal" on the circular number line divided into M parts. So, we would want congruency to actually satisfy the properties that equality on the number line satisfies. These properties are called reflexivity, symmetry, and transitivity. Although you can take them for granted with equality on the straight number line, let's prove them for modular arithmetic! The following proofs should be quite simple given your answers to Problem 17 and Problem 18.

Problem 19 *Let $M \geq 2$ and a both be integers. Can you prove $a \equiv a \pmod{M}$? This is called the reflexivity of congruency.*

Problem 20 *Let $M \geq 2$ and a, b all be integers. Prove that if $a \equiv b \pmod{M}$, then $b \equiv a \pmod{M}$. This is called the symmetry of congruency.*

Problem 21 *Let $M \geq 2$ and a, b, c all be integers. Prove that if $a \equiv b \pmod{M}$ and $b \equiv c \pmod{M}$, then $a \equiv c \pmod{M}$. This is called the transitivity of congruency.*

Now that we know congruence works as expected, we can study how modular addition and multiplication work. We can do so easily by proving the following two results first.

Problem 22 *Let $M \geq 2$ and a, b all be integers. Prove that if a is congruent to b modulo M, then M divides $a - b$ without any remainder. In other words, prove there is some integer k such that $M \cdot k = a - b$ (note that k does not have to be positive).*

Problem 23 *Let $M \geq 2$ and a, b all be integers. Suppose that M divides $a - b$ without any remainder, meaning there is some integer k such that $M \cdot k = a - b$. Prove that a is congruent to b modulo M. This problem is the converse to Problem 22.*

The following two results allow us to completely understand modular addition and multiplication.

Problem 24 *Let $M \geq 2$ and a, b, k all be integers. Prove that if $a \equiv b \pmod{M}$, then*

$$a + k \equiv b + k \pmod{M},$$

$$a \cdot k \equiv b \cdot k \pmod{M},$$

and

$$a \cdot k \equiv b \cdot k \pmod{M \cdot k}.$$

Problem 25 *Let $M \geq 1$ and a, b, c, d all be integers. Suppose*

$$a \equiv b \pmod{M} \qquad \textit{and} \qquad c \equiv d \pmod{M}.$$

Prove that

$$a + c \equiv b + d \pmod{M} \qquad \textit{and} \qquad a \cdot c \equiv b \cdot d \pmod{M}.$$

We will leave the analogue of "division" in modular arithmetic as an extra challenge at the end of this packet. For now, using the new rules of arithmetic you have learned, lets tackle a few problems!

Problem 26 *Fill in the set definition for the following congruence classes.*

$$[7]_5 = \{ \quad \}$$

$$[14]_5 = \{ \quad \}$$

$$[100]_5 = \{ \quad \}$$

$$[-1]_7 = \{ \quad \}$$

$$[6]_7 = \{ \quad \}$$

$$[8]_7 = \{ \quad \}$$

Problem 27 *Fill in the smallest integer between 0 and the modulus minus 1 (the number written after the notation* mod*) such that the following congruencies are true.*

$$1 + 7 \equiv \qquad \pmod 5$$

$$3 + 3 \equiv \qquad \pmod 5$$

$$2 \cdot 17 \equiv \qquad \pmod 8$$

$$32 \cdot 0 \equiv \qquad \pmod 2$$

$$1 + 3 - 6 \equiv \qquad \pmod 6$$

$$100^2 \equiv \qquad \pmod{99}$$

$$((16^2 - 4) \cdot 8) - 1 \equiv \qquad \pmod 4$$

$$25^{100000} - 1 \equiv \qquad \pmod 5$$

Problem 28 *Write whether each of the following congruencies are true or false.*

$1 + 9 \equiv 3 \pmod 6$ _____

$3 + 3 \equiv 0 \pmod 3$ _____

$17 + 2 \equiv 3 + 2 \pmod 7$ _____

$29384 \cdot 0 \equiv 2 \pmod 9$ _____

$1 + 5 - 7 \equiv 101 \pmod{10}$ _____

$100^2 \equiv 1 \pmod{25}$ _____

$30^2 - 30^{9120382} \equiv 0 \pmod{30}$ _____

$4 \cdot 25 + 1 \equiv -99 \pmod{100}$ _____

We conclude this section with a few more challenging, and interesting, examples!

Example 1 *Find the smallest integer between* 0 *and* 6 *that is congruent to* 3^{100} *modulo* 7*.*

There are two ways to solve this problem. The first is more obvious, but requires more work. Let us take a look at the consecutive powers of three.

$$3^1 = 3 \equiv 3 \pmod 7$$

$$3^2 = 3^1 \cdot 3 = 9 \equiv 2 \pmod 7$$

$$3^3 = 3^2 \cdot 3 \equiv 2 \cdot 3 = 6 \equiv 6 \pmod 7$$

$$3^4 = 3^3 \cdot 3 \equiv 6 \cdot 3 = 18 \equiv 4 \pmod 7$$

$$3^5 = 3^4 \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 5 \pmod 7$$

$$3^6 = 3^5 \cdot 3 \equiv 5 \cdot 3 = 15 \equiv 1 \pmod 7$$

$$3^7 = 3^6 \cdot 3 \equiv 1 \cdot 3 = 3 \equiv 3 \pmod 7$$

From this point on, the powers begin repeating one another in a cycle of length six.

$$3^8 = 3^7 \cdot 3 \equiv 3 \cdot 3 = 9 \equiv 2 \equiv 3^2 \pmod 7$$

We get the following pattern.

$$3^1 \equiv 3^7 \equiv 3^{13} \equiv 3^{19} \ldots \pmod 7$$

$$3^2 \equiv 3^8 \equiv 3^{14} \equiv 3^{20} \ldots \pmod 7$$

$$3^3 \equiv 3^9 \equiv 3^{15} \equiv 3^{21} \ldots \pmod 7$$

$$3^4 \equiv 3^{10} \equiv 3^{16} \equiv 3^{22} \ldots \pmod 7$$

$$3^5 \equiv 3^{11} \equiv 3^{17} \equiv 3^{23} \ldots \pmod 7$$
$$3^6 \equiv 3^{12} \equiv 3^{18} \equiv 3^{24} \ldots \pmod 7$$

The final step of the solution is to figure out which of the above six sequences contains 3^{100}*. Note that if we divide any power from the first sequence by six, the remainder will always be equal to* 1*. It will be equal to* 2 *for the second sequence, to* 3 *for the third, and so on. Now,* $100 = 96 + 4 = 16 \cdot 6 + 4$*. Therefore,* 3^{100} *will appear in the forth sequence.*

$$3^{100} \equiv 3^4 \equiv 4 \pmod 7$$

The following way to solve the above problem is more elegant. Let us make a table with powers of two not exceeding 100 in the left column and with the number three raised to the corresponding power of two in the right one.

1 $\quad 3^1 = 3 \equiv 3 \pmod 7$

2 $\quad 3^2 = 3^1 \cdot 3^1 = 9 \equiv 2 \pmod 7$

4 $\quad 3^4 = 3^2 \cdot 3^2 \equiv 2 \cdot 2 = 4 \equiv 4 \pmod 7$

8 $\quad 3^8 = 3^4 \cdot 3^4 \equiv 4 \cdot 4 = 16 \equiv 2 \pmod 7$

16 $\quad 3^{16} = 3^8 \cdot 3^8 \equiv 2 \cdot 2 = 4 \equiv 4 \pmod 7$

32 $\quad 3^{32} = 3^{16} \cdot 3^{16} \equiv 4 \cdot 4 = 16 \equiv 2 \pmod 7$

64 $\quad 3^{64} = 3^{32} \cdot 3^{32} \equiv 2 \cdot 2 = 4 \equiv 4 \pmod 7$

128 $3^{128} = 3^{64} \cdot 3^{64} \equiv 4 \cdot 4 = 16 \equiv 2 \pmod 7$

Since $100 < 128$*, we stop here. The last line is not needed for the subsequent computations. It is used as a stop sign.*

Next, let us represent 100 *as a sum of powers of two.*

$$100 = 64 + 32 + 4$$

Therefore,

$$3^{100} = 3^{64} \cdot 3^{32} \cdot 3^4 \equiv 4 \cdot 2 \cdot 4 = 32 \equiv 4 \pmod 7.$$

Problem 29 *Find the smallest integer between* 0 *and* 6 *that is congruent to* 5^{1234} *modulo* 7*.*

Problem 30 *Find the last two digits of* 7^{2012}*. Since we are only interested in the last two digits, we can reformulate the problem as follows: find the smallest integer between* 0 *and* 99 *that is congruent to* 7^{2012} *modulo* 100*.*

4 Optional challenge: Modular division

In the prior section, we studied how addition and multiplication work in modular arithmetic. However, when working on the straight number line, there are two more important operations: subtraction and division. Subtraction is the inverse of addition, meaning that

$$(a + b) - b = a = (a - b) + b$$

for any integers a, b. Similarly, division is the inverse of multiplication, meaning that

$$(a \cdot b) \div b = a = (a \div b) \cdot b$$

for any integers a, b as long as $b \neq 0$ (remember we cannot divide by 0). Although subtraction and division play analogous roles on the straight number line, there is a major difference between the operations. $a - b$ is always an integer whenever a, b are integers. However, $a \div b$ does NOT have to be an integer even when a, b are integers. Instead $a \div b = \frac{a}{b}$ is a rational number, which may or may not simplify to an integer. Because we can only work with integers in modular arithmetic, this difference between subtraction and division is the underlying reason for why subtraction in modular arithmetic is very simple to understand while division is much more complicated. For those brave enough, we will discover how modular division works and even understand the equivalent of "rational numbers" in modular arithmetic.

Problem 31 *Let $M \geq 2$ and a, b, c, d, k all be integers. Prove that if*

$$a \equiv b \pmod{M} \quad \textit{and} \quad c \equiv d \pmod{M},$$

then

$$a - k \equiv b - k \pmod{M} \quad \textit{and} \quad a - c \equiv b - d \pmod{M}.$$

Hint: the proof should be very easy if you use Problem 24 and/or Problem 25.

Problem 31 is truly all we need to understand modular subtraction! The following is the first baby step we can take towards understanding modular division. It allows us to cancel common factors as though we can "divide" both sides by k.

Problem 32 *Let $M \geq 2$, $k \neq 0$, and a, b all be integers. Prove that if $a \cdot k \equiv b \cdot k \pmod{M \cdot k}$, then $a \equiv b \pmod{M}$.*

While Problem 32 is useful, it requires that we change the modulus we are working with from $M \cdot k$ to M. This hints towards the issue at the heart of modular division: understanding the shared factors between k and the modulus. Let a, b be non-zero integers. The *greatest common divisor (gcd) of* a, b is the largest positive integer that divides a without remainder AND also divides b without remainder, which we denote as $\gcd(a, b)$. For example, $\gcd(4, 6) = 2$ since $2 \cdot 3 = 6$, $2 \cdot 2 = 4$, and one can check that any number larger than 2 does not divide 6 and 4.

Problem 33 *Let* a, b *be two non-zero integers. Then,* $\gcd(a, b)$ *is greater than or equal to* 1*. Also,* $\gcd(a, b)$ *is less than or equal to the minimum of* $|a|$ *and* $|b|$ *(the absolute values of* a, b*). Why are these two facts true?*

Problem 34 *Find the gcd of the following pairs of integers.*

$$\gcd(1, 9301293) =$$

$$\gcd(10, 15) =$$

$$\gcd(-6, 12) =$$

$$\gcd(7, 9) =$$

Now, we say that two non-zero integers a, b are *coprime* if $\gcd(a, b) = 1$. The notion of being coprime is important as it is the core of the following result.

Theorem 1 *Let a, b be two non-zero integers. Then, a, b are coprime if and only if there exists integers x, y such that*

$$ax + by = 1.$$

We skip the proof of Theorem 1 for now as it is a bit advanced. Those who are interested can ask their instructors for the proof after finishing this worksheet! Theorem 1 allows us prove a version of Problem 32 that leaves the modulus unchanged.

Problem 35 *Suppose a, b are coprime, non-zero integers. Let c be an integer such that a divides $b \cdot c$ without remainder. Prove that a must divide c without remainder. Hint: use Theorem 1 and then multiply by c.*

Problem 36 *Let $M \geq 2$, $k \neq 0$ be coprime integers. Also, let a, b both be integers. Prove that if $a \cdot k \equiv b \cdot k \pmod{M}$, then $a \equiv b \pmod{M}$. Hint: use Problem 35.*

Note that, as promised, Problem 36 is a version of Problem 32 that leaves the modulus unchanged. We now conclude with "rational numbers" in modular arithmetic.

Problem 37 *Let $M \geq 2$ and $a \neq 0$ both be integers. Prove that there exists an integer x such that $a \cdot x = 1 \pmod{M}$ if and only if M, a are coprime. Hint: use Theorem 1.*

For coprime integers $M \geq 2$ and $a \neq 0$, the integer x such that $a \cdot x = 1 \pmod{M}$ is called the *multiplicative inverse of a modulo M*. We typically denote it by $a^{-1} = x$. The multiplicative inverse a^{-1} of a modulo M is analogous to the rational number $\frac{1}{a}$ on the straight number line. Indeed, $a \cdot \frac{1}{a} = 1$ on the straight number line while $a \cdot a^{-1} \equiv 1 \pmod{M}$ on the circular number line. The whole reason we had to understand gcd's is because we only want to work with integers in modular arithmetic, while rational numbers on the straight number line do not have to be integers. This is the point of Problem 37.

A further interesting observation is that, since a^{-1} on the circular number line corresponds to $\frac{1}{a}$, we can think of the any rational number $\frac{b}{a}$ on the straight number line (where b is an integer) as corresponding to $b \cdot a^{-1}$ on the circular number line.

Problem 38 *Let $M \geq 2$ and $a, b \neq 0$ all be integers. Suppose $a \equiv b \pmod{M}$. Prove that if the multiplicative inverse a^{-1} of a modulo M exists, then the multiplicative b^{-1} of b modulo M exists and $a^{-1} \equiv b^{-1} \pmod{M}$.*

Example 2 *We find the analog of* $\frac{3}{4}$ *modulo* 7*. As explained above, this means that we are looking for the integer* x *such that* $x \cdot 4 \equiv 3 \pmod 7$ *since* $\frac{3}{4} \cdot 4 = 3$ *on the straight number line. Let us first find the analog of* $\frac{1}{4}$*, meaning the multiplicative inverse* 4^{-1} *of* 4 *modulo* 7*.*

First, we can quickly see that $\gcd(4, 7) = 1$ *since* 7 *is prime and* 4 *is not a multiple of* 7*. So, by Problem 37, we know that the multiplicative inverse* 4^{-1} *of* 4 *modulo* 7 *exists. Now, there are only seven congruence classes modulo* 7*, namely* $[0]_7$*,* $[1]_7$*,* $[2]_7$*,* $[3]_7$*,* $[4]_7$*,* $[5]_7$*, and* $[6]_7$*. One of them must contain the* 4^{-1}*. So, plugging the numbers* $0, 1, 2, 3, 4, 5, 6$ *into the expression*

$$\square \cdot 4 \equiv 1 \pmod 7$$

one by one, we find that

$$2 \cdot 4 = 8 \equiv 1 \pmod 7,$$

meaning 2 *is the multiplicative inverse of* 4 *modulo* 7*.*

To finish, we know that $\frac{3}{4} = 3 \cdot \frac{1}{4}$ *on the straight numberline. So, the analog of* $\frac{3}{4}$ *modulo* 7 *must be* 3 *times the multiplicative inverse of* 4 *modulo* 7*. This is* $3 \cdot 2 = 6$*, and indeed*

$$6 \cdot 4 = 3 \cdot (2 \cdot 4) \equiv 3 \cdot 1 = 3 \pmod 7.$$

So, 6 *corresponds to* $\frac{3}{4}$ *modulo* 7*!*

Problem 39 *Find the analog of* $\frac{1}{2}$ *modulo* 7*.*

Problem 40 *Find the analog of* $\frac{1}{4}$, $\frac{2}{4}$, *and* $\frac{3}{4}$ *all modulo* 7.

Problem 41 *Find the analog of* $\frac{1}{5}$, $\frac{2}{5}$, $\frac{3}{5}$, *and* $\frac{4}{5}$ *all modulo* 9.