Modular Arithmetic I

bissue

August 6, 2021

Contents

1 What's Left Behind

1.1 Two-Dimensional

As we saw in the first handout, recognizing divisibility can be essential to cracking all sorts of problems. Whether it be counting the number of divisors, or determining whether a number is a perfect square, the key concept of divisibility can be found in every single number theory problem you encounter.

However, divisibility, alone, is often not enough to fully describe the relationship between numbers. This handout discusses how we can use a much more powerful tool to learn more about the relationships between numbers: **remainders.**

First, observe that understanding the remainder when a is divided by b gives **more** information than understanding whether a is divisible by b. Consider how we can separate the integers into individual boxes, so that each box is reserved only for integers with a **specific remainder when divided by 7:**

$$\begin{aligned}
&\{\ldots, -14, -7, 0, 7, 14, 21, \ldots\} \quad \text{(Remainder = 0)},\\
&\{\ldots, -13, -6, 1, 8, 15, 22, \ldots\} \quad \text{(Remainder = 1)},\\
&\qquad\qquad\vdots\\
&\{\ldots, -8, -1, 6, 13, 20, 27, \ldots\} \quad \text{(Remainder = 6)},
\end{aligned}$$

If we instead classify the integers based on **divisibility by 7,** our ability to distinguish between numbers is decreased from 7 groupings to just 2:

$$\begin{aligned}
&\{-14, -7, 0, 7, 14, 21, \ldots\}\\
&\{-13, -12, -11, -10, -9, -8, -6, -5, \ldots\}
\end{aligned}$$

As you might notice, when we consider remainders instead of pure divisibility, the "not-divisible-by-seven" grouping is divided into six, more precise groupings, allowing us to extract much more information than before.

> **Exercise 1.1.** The remainder when N is divided by 30 equals 20. Then N is necessarily divisible by which of the following number(s)?
>
> $$2,\ 3,\ 5,\ 7$$

Notice that, in the exercise above, if we instead just said, "N is not divisible by 30", we would not have nearly as much information!

1.2 A Cylinder of Numbers

To introduce modular arithmetic, we take another look at our 7 groups of integers, this time giving the name S_i to each set if it contains all numbers whose remainder when divided by 7 equals i.

$$\begin{aligned}
S_0 &= \{-14, -7, 0, 7, 14, 21\}\\
S_1 &= \{-13, -6, 1, 8, 15, 22\}\\
&\vdots\\
S_6 &= \{-8, -1, 6, 13, 20, 27\},
\end{aligned}$$

Suppose we knew that an integer a exists in set S_1, and an integer b exists in set S_3. Where would the integer $a+b$ be? Intuitively, it would make sense for $a+b$ to be categorized in set S_{1+3}, or S_4. Similarly, if a exists instead in S_3 and b also exists in S_3, then $a+b$ would exist in S_6.

And if a exists in S_4 and b exists in S_6? Their sum would exist in S_{10}, which is the set of all integers equal to 10 more than a multiple of 7, shown below:

$$\{-4,\ 3,\ 10,\ 17,\ 24,\ \ldots\}$$

Observe that this is the same as the set of numbers whose remainder when divided by 7 equals 3, or S_3. Thus, we can say that $S_4 + S_6 = S_3$, and $S_3 = S_{10} = S_{17} = \cdots$.

Remark 1.2. Negative numbers can be a little tricky. Try the exercise below:

Exercise 1.3. What is the remainder when -4 is divided by 10? In other words, which set S_i does -4 belong to?

To solve this, we may simply observe that, in general, if a is in some set S_i, then $a+10$ must be in the same set. Hence, it follows that $-4+10=6$ is in the same set as -4 itself, implying that -4 is in S_6.

Exercise 1.4. Convince yourself that remainder addition works this way. If we instead worked with remainders when dividing by 11, what would $S_{16} + S_6$ equal?

Exercise 1.5. Identify a similarity between remainder addition and clocks.

Exercise 1.6. The remainder when k is divided by 11 equals 3. What is the remainder when $-k$ is divided by 11?

Thinking about this observation more closely, we recognize that, in order to compute the remainder of $a+b$, we do not need the exact values of a and b; instead, only the remainders of a and b are relevant! In other words,

Fact 1.7. If a and b have the same remainder when divided by p, then they are ***interchangeable*** under addition.

In other words, if we wish to compute the remainder when $a+b$ is divided by p, we can replace a and b with their respective remainders r_1 and r_2 to simplify the problem down to computing the remainder when $r_1 + r_2$ is divided by p.

Exercise 1.8. Convince yourself that two integers a and b have the same remainder when divided by p if and only if $a-b$ is divisible by p.

Exercise 1.9. It is given that a and b have the same remainder when divided by 3. Why is $a+2b$ necessarily a multiple of 3? [a]

[a] Recall that being a multiple of 3 is equivalent to having a remainder of zero when divided by 3.

Example 1.10
The Fibonacci Sequence has its first two terms equal to 1 and 1. It has the property that any term (after the first two) is equal to the sum of the two terms before it. What is the remainder when the 100th term is divided by 3?

Proof. First, we can try to list out the first few terms of the sequence:

$$1, 1, 2, 3, 5, 8, 13, \cdots$$

However, the question only asks for the remainder when the 100th term is divided by 3. This means that we do not need the actual values of the Fibonacci Sequence; rather, we only need their remainders when divided by 3. [1] Listing the first few remainders, we find:

$$1, 1, 2, 0, 2, 2, 1, \cdots$$

Then, to construct the next term of the sequence, we add the previous two terms and find the remainder when the sum is divided by 3. Note that, by considering remainders only, our computational workload is lessened significantly. The next few remainders of the sequence are not nearly as difficult to find as the next few terms of the sequence:

$$1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0, 2, 2, 1, 0, 1 \cdots$$

At this point, you might recognize that the sequence actually repeats!

$$\boxed{1, 1}, 2, 0, 2, 2, 1, 0, \ \boxed{1, 1}, 2, 0, 2, 2, 1, 2, \ 1, \cdots$$

The reason why the sequence repeats is because, as soon as we reach the boxed pair of consecutive terms $(1, 1)$ for the second time, the computations are exactly the same, resulting in the sequence repeating itself. This means that we actually know what the sequence looks like without having to write all 100 terms.

Every 8 terms, the sequence repeats itself. Thus, terms F_1, F_9, F_{17}, and so on are all the same. Similarly, terms F_2, F_{10}, F_{18}, and so on are all the same. (Is this familiar?) Therefore, we can work backwards to find that

$$F_{100} = F_{92} = F_{84} = \cdots = F_4$$

and $F_4 = 0$, implying that the remainder when the 100th term is divided by 3 is $\boxed{0.}$ □

Remark 1.11. A common theme in number theory is that sequences often repeat. Look out for this when dealing with sequences "remaindered" by some number!

Exercise 1.12. Why is it that, for any positive integer n, the remainders of the terms of the Fibonacci Sequence when divided by n must be periodic? Additionally, why is it that all rational numbers (numbers of the form $\frac{a}{b}$) have either a periodic or terminating decimal representation?

[1] Recall that each term of the Fibonacci Sequence is ***interchangeable*** with its remainder, since all that is being done is addition.

Exercise 1.13. What is the last digit of 197×286? [a]

[a] Consider the sequence $197, 197+197, 197+197+197, \ldots$)

Exercise 1.14. Compute the remainder when

$$72 + 79 + 86 + 93 + \ldots + 765 + 772$$

is divided by 14.

2 Abstraction

2.1 Terminology

Right now, our definition of "remainder" is a bit contrived. It makes less sense when considering negative numbers, and it unnecessarily restricts us to integers between 1 and n. What matters more is the set S_i each number belongs to, not the exact remainder.

In fact, defining numbers to be contained within sets is more complicated than necessary. We might as well develop a form of notation that describes whether two numbers are in the same set, since numbers in the same set are generally identical when purely considering remainders. This is where modular arithmetic comes in.

Fact 2.1. We write the **modular congruence**:

$$a \equiv b \pmod{q}$$

if and only if a and b have the same remainder when divided by q. (In other words, when q divides $a - b$.)

That $\equiv$ sign looks strangely similar to an $=$ sign; this is no coincidence! If

$$a \equiv b \pmod{q},$$

then it is not necessarily true that $a = b$, but it is true that they are identical under addition, which means they might as well be the same. For this reason, we read the $\equiv$ sign as "congruent to".

Exercise 2.2. Convince yourself that the following modular congruences are true.

$$-18 \equiv 6 \pmod{12}.$$
$$m \equiv n \pmod{m-n}.$$
$$3491 + 9818 \equiv 91 + 18 \pmod{100}.$$

Remark 2.3. To read the equation

$$a \equiv b \pmod{p}$$

formally, one might say:

"a is congruent to b modulo q."

However, just as $\sqrt{3}$ is sometimes read "root 3", congruences like these might just be said as "a is b mod q" for the sake of efficiency, or sometimes just "a equals b" when context is known.

Keep in mind that $\pmod{p}$ is **not** an operation. Formally, it would be incorrect to define a function $f(x) = x \pmod{8}$ to signify that $f(x)$ outputs the remainder when x is divided by 8. The symbol $\pmod{p}$ is only used to signify the sets S_i we are using.

Of course, when speaking aloud or writing down scratch work, it is perfectly fine to treat $\pmod{p}$ as its own operation.

Modular arithmetic notation is generally more concise, so the rest of this handout will be written in terms of modular arithmetic.

Remark 2.4. Often, contest problems will not spell out the modular congruences for you, so be sure to have a clear understanding of when to use them!

2.2 Addition, Subtraction, Multiplication, –

If you aren't careful, it may seem like the following theory is "obvious" and "intuitive". Whenever you think this may be the case, look back at this case of invalid logic as a reminder that things are not always as simple as they seem...

It is the case that $2 \equiv 5 \pmod{3}$, so it seems intuitive that they should be interchangeable under all contexts modulo 3. This is true in the case of addition; you should already be convinced that the following is true for all integers a:

$$a + 2 \equiv a + 5 \pmod{3}$$

However, it is not true for all operations! For example,

$$2^2 \equiv 4 \equiv 1 \pmod{3}$$

$$2^5 \equiv 32 \equiv 2 \pmod{3}$$

This shows that $2^2 \not\equiv 2^5 \pmod{3}$, even though $2 \equiv 5 \pmod{3}$. In other words, we cannot just substitute numbers with other numbers congruent to them wherever we choose! It just so happens that we are allowed to do so for the majority of arithmetic operations.

Now, let's go on to explore multiplication within modular arithmetic by proving the following claim:

Claim — If $a \equiv b \pmod{p}$, then it follows that a and b are interchangeable not just under addition, but also under multiplication!

This fact is relatively intuitive, but it requires a little more rigorous proof than the proof for addition. We'll walk you through the proof with a couple of exercises:

Exercise 2.5. We want to rewrite the concept that $m \equiv n \pmod{p}$ in some "algebraic" sense. If we knew that $x \equiv 2 \pmod{3}$, for example, we would say $x = 3k + 2$, for some integer k. How can we express the numerical value of m in terms of p, k, and n?

Exercise 2.6. Assuming $m \equiv n \pmod{p}$, the goal is to show that, for any positive integer a,

$$am \equiv an \pmod{p}.$$

To prove[a] this, substitute your expression for m into am and expand. Any terms which are a multiple of p are congruent to 0 modulo p. After removing the terms that effectively equal 0, what is the result?

[a](Look back at the "caution" example if you think this is obvious!)

Exercise 2.7. Why does the above exercise imply that, if $m \equiv n \pmod{p}$, then m and n are interchangeable under multiplication modulo p?

(Note that, if you solved Exercise 1.8, you could extend the same argument to achieve the exact same result. It just goes to show how fundamental this fact is!) To recap:

Fact 2.8. If $a \equiv b \pmod{p}$, then a and b are interchangeable under addition, subtraction, and multiplication.

However, it is *not* the case that a and b are interchangeable at the exponent of a number, meaning $n^a \equiv n^b \pmod{p}$ is not necessarily true.

A natural question to ask is, "What about division?"[2] The answer to this question will have to wait; for now, let's just practice applying these techniques to get a better understanding of modular arithmetic.

2.3 Applications

Using this new theory, make an attempt at these problems on your own!

Example 2.9

1. What is the remainder when 9^{9999} is divided by 10?
2. What is the remainder when 777×889 is divided by 11?
3. What is the sum of the digits of 124×421?
4. What is the remainder when 1024×729 is divided by 6^6?

Now for the solutions!

[2]Hint: It's not as straightforward as you might think!

Proof. For the first question, we note that $9 \equiv -1 \pmod{10}$, so

$$\begin{aligned} 9^{9999} &\equiv 9 \times 9 \times \ldots \times 9 \\ &\equiv (-1) \times (-1) \times \ldots \times (-1) \\ &\equiv (-1)^{9999} \equiv -1 \equiv 9 \pmod{10} \end{aligned}$$

so the answer is $\boxed{9}$. □

Remark 2.10. This problem demonstrates two key ideas:

1. If $a \equiv b \pmod{p}$, then a and b are interchangeable at the **base** of the exponent. In other words, for any positive integer k, given that $a \equiv b \pmod{p}$, it follows that
$$a^k \equiv b^k \pmod{p}.$$
It is **not** the case that $k^a \equiv k^b \pmod{p}$, however, as we saw from the "caution" example.
2. Both positive and negative numbers are important under modular arithmetic! When dealing with multiplication, it is better to work with numbers whose ***absolute values*** are small.

Exercise 2.11. What is the remainder when $(2k-1)^{2k-2}$ is divided by $2k$?

Proof. For the second question, we note that $777 \equiv 7 \pmod{11}$, and $889 \equiv 9 \pmod{11}$, so

$$777 \times 889 \equiv 7 \times 9 \equiv 63 \equiv \boxed{8} \pmod{11}.$$

□

Exercise 2.12. It is given that the remainder when 9! is divided by 11 equals 1. What is the remainder when

$$100 \times 101 \times \ldots \times 109$$

is divided by 11?

Proof. For the third question, instead of multiplying the number out, we note that the remainder when n is divided by 9 is congruent to the sum of its digits modulo 9. The remainder when 124×421 is divided by 9 can be found to equal

$$124 \times 421 \equiv 7 \times 7 \equiv 49 \equiv 4 \pmod{9}$$

Thus, the sum of the digits of 124×421 could equal 4, 13, 22, and so on. However, it is unreasonable for the sum of digits to be as small as 4 or as big as 22, so the answer is almost certainly $\boxed{13.}$ □

Remark 2.13. When taking a multiple choice contest such as the AMC, a good trick for eliminating answer choices is to take each answer choice modulo p and see if it lines up!

For example, if you knew that the correct answer had to be congruent to 4 modulo 5, then you could eliminate all answer choices that are **not** congruent to 4 modulo 5. If you're lucky, you might reduce the number of choices down to one!

Proof. This last question is just a check to see whether you remember the basics. Here, we can't reduce 1024 or 729 modulo 6^6, since 6^6 is greater than both of them. However, we simply observe that

$$1024 \times 729 = 2^{10} \times 3^6 = 6^6 \times 16,$$

and therefore, 1024×729 is a multiple of 6^6, implying that the answer is $\boxed{0.}$ □

Let's just take a moment to fully comprehend the power of what we have discovered. Consider the number 13^{13}; its decimal representation looks like this:

$$302875106592253$$

Just from looking at this number, there is no way to determine its remainder when divided by 7. However, with modular arithmetic, we simply note that

$$13^{13} \equiv (-1)^{13} \equiv -1 \equiv 6 \pmod 7,$$

giving the answer of 6 almost instantly! Keep this trick in mind whenever you are asked to find remainders.

Exercise 2.14. What is the remainder when 2^{100} is divided by $2^{10} - 2$?

Exercise 2.15. Allie claims that 2 more than the square of her favorite number is a multiple of 7. Is it possible that Allie's favorite number is a positive integer?

Exercise 2.16. (★) Prove that if $a \equiv b \pmod p$, and $f(x)$ is a polynomial with integer coefficients, then $f(a) \equiv f(b) \pmod p$. [a]

[a] Hint: Consider what happens when $f(x)$ is linear, first. And if $f(x) = x^2$, why is this true? How can we extend this to higher powers, and even further to sums of higher powers?

3 Rational Thinking

3.1 Prime Pattern-Finding

Consider the following addition table, where all sums are taken modulo 7:

+	0	1	2	3	4	5	6
0	0	**1**	2	3	4	5	6
1	1	2	3	4	5	**6**	0
2	2	3	**4**	5	6	0	1
3	3	4	5	6	0	1	**2**
4	4	5	6	**0**	1	2	3
5	**5**	6	0	1	2	3	4
6	6	0	1	2	**3**	4	5

We can observe a sort of cyclical pattern here. If you read numbers down a row or column, you'll find the numbers $\{0,1,2,3,4,5,6\}$, just rotated by some amount. And if you read along any diagonals, looping around the grid when you reach an edge, the resulting numbers will be some permutation of $\{0,1,2,3,4,5,6\}$.

In fact, if we consider some of the non-obvious diagonals (one of which is bolded), we see that even these diagonals contain all of the numbers from 0 through 6.

Exercise 3.1. These "diagonals" are actually just arithmetic progressions. Why do arithmetic progressions, with common difference not equal to 7, contain all remainders modulo 7 in a cyclical pattern? (Rigorous proof is not necessary; just convince yourself that this is the case.)

However, if we instead consider addition tables taken modulo 4, we find a different result:

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

Every row and column still has the same property, but if we consider some of the diagonals, we see that some of them don't have all 4 remainders.

Exercise 3.2. Again, recall that these diagonals are arithmetic progressions. What choice of a common difference would make only two remainders appear modulo 4, and is it possible to make exactly three remainders appear?

Exercise 3.3. Which types of modulo-n grid have the same nice property as the one in the modulo-7 grid? (Hint: Read the title of this section.)

These patterns won't necessarily help you directly on any problem, but they can give you a nice insight on the patterns you can find in modular arithmetic, to help with your intuition. For example,

Exercise 3.4. Why must there exist some integer n such that $187n$ is 199 more than a multiple of 2017? (Note that 2017 is prime.)

Hold on a second! What we have just discovered in the previous exercise is the following:

There exists a solution to the modular congruence $187x \equiv 199 \pmod{2017}$.

In fact, we now know the following more general statement:

Fact 3.5. For any prime number p, and any integers a and b, with a co-prime to p, there exists a solution to the modular congruence:

$$ax \equiv b \pmod{p}.$$

In terms of algebra, we know that the solution to $ax = b$ is simply $x = \frac{b}{a}$. Fact 3.5 suggests that we might be able to define the "value" of $\frac{b}{a}$ modulo p to be the solution to $ax \equiv b \pmod{p}$. Might we be able to implement division into modular arithmetic?

3.2 When 1/4 Equals 3

Our goal is to analyze solutions to the equation:

$$ax \equiv b \pmod{p}$$

where a, b, and p are certain positive integers. First, let's **try to figure out when these solutions even exist!**

There is one key observation that can be made. Suppose that we had some solution, x_0, to the equation:

$$ax \equiv 1 \pmod{p}.$$

In other words, we consider purely the case where $b = 1$, and we assume that $ax \equiv 1 \pmod{p}$ does, indeed, have a solution. We now claim that $ax \equiv b \pmod{p}$ must have a solution as well.

Exercise 3.6. What is some value of x such that $ax \equiv b \pmod{p}$, given that we already have some x_0 such that $ax_0 \equiv 1 \pmod{p}$?

Thus, we may deduce that, if $ax \equiv 1 \pmod{p}$ has a solution, then $ax \equiv b \pmod{p}$ has a solution as well, for ***all*** choices of b. (This is a powerful statement!) So, a natural question would be the following:

When does $ax \equiv 1 \pmod{p}$ have a solution?

Exercise 3.7. Convince yourself that $ax \equiv 1 \pmod{p}$ has a solution if and only if $\gcd(a, p) = 1$.

A good way to do this might be to explain why, if $\gcd(a, p) \neq 1$, then $ax \equiv 1 \pmod{p}$ cannot have a solution. For example, why does $3x \equiv 1 \pmod{6}$ have no solution?

For the sake of clarity, let's summarize our new discoveries with the (very important) fact below:

Fact 3.8. The congruence $ax \equiv b \pmod{p}$ has a solution if $\gcd(a, p) = 1$.

Note that, if $\gcd(a, p) \neq 1$, it is **not** necessarily the case that $ax \equiv b \pmod{p}$ does not have a solution. We'll discuss this topic in greater detail in a later section.

With this new knowledge, we can actually define fractions in modular arithmetic, but only under specific contexts:

We express the ***modular inverse*** of r modulo p as r^{-1} [a], so that r^{-1} is the solution to:

$$rx = 1 \pmod{p}.$$

(Think back to algebra to convince yourself that this notation makes sense.)

Recall that the modular inverse r^{-1} modulo p is only defined when $\gcd(r, p) = 1$. Otherwise, it might as well be $\frac{1}{0}$.

[a] Recall that r^{-1} is just a fancier way of writing $\frac{1}{r}$.

Time for some applications!

Example 3.9
It is given that $48^{-1} \equiv 1 \pmod{p}$, for some prime p with 48^{-1} defined. What is the value of p?

Proof. Note that, by definition, if we say $x = 48^{-1}$, then it follows that:

$$48x \equiv 1 \pmod{p}$$

We are also told that $x = 48^{-1} \equiv 1 \pmod{p}$ in the problem statement, so substituting $x \equiv 1 \pmod{p}$ gives:

$$48x \equiv 48 \equiv 1 \pmod{p}.$$

The only choice for p such that $48 \equiv 1 \pmod{p}$ is one in which $48 - 1 = 47$ is divisible by p, or when $p = \boxed{47.}$ □

Remark 3.10. An alternative solution works as follows:

$$\frac{1}{48} \equiv 1 \pmod{p} \Rightarrow 1 \equiv 48 \pmod{p}.$$

Here we simply multiplied by 48 on both sides, just as we would with standard algebra! There's some greater detail hiding behind the scenes here that *technically* prohibits us from doing this, but for now, in the context of computational problems, these kinds of manipulations are perfectly fine.

Example 3.11
What is the "remainder" when $\frac{4}{5}$ is divided by 7?

Proof. From our definition of modular inverses, we note that we may write $x \equiv \frac{1}{5} \pmod{7}$ if and only if

$$5x \equiv 1 \pmod{7}.$$

We can apply some guess-and-check to determine that $x \equiv 3 \pmod 7$, so $\frac{1}{5} \equiv 3 \pmod 7$.

To finish, we simply note that

$$\frac{4}{5} \equiv 4 \cdot \frac{1}{5} \equiv 4 \cdot 3 \equiv \boxed{5} \pmod 7.$$

□

Remark 3.12. Just as in the previous example, we could also have taken the following short-cut:

> Suppose that we defined x so that:
>
> $$x \equiv \frac{4}{5} \pmod 7.$$
>
> Thus, our goal is to express x as an integer. Multiplying by 5 on both sides gives:
>
> $$5x \equiv 4 \pmod 7.$$
>
> We can solve this congruence for x with some quick guess-and-check to find $x \equiv 5 \pmod 7$ as the answer.

Again, this solution is slightly less rigorous, but it is still completely valid. In fact, by comparing this solution with the previous one, you might be able to find a connection with our discussion on the existence of solutions to $ax \equiv b \pmod p$.

Try applying division in modular arithmetic on your own!

Exercise 3.13. Look back at the title of this section. For which choice of p does $\frac{1}{4} \equiv 3 \pmod p$?

Exercise 3.14. What is the "remainder" of $\frac{7}{12}$ when divided by five? How about nine?

Exercise 3.15. Convince yourself that if $a \equiv b \pmod p$, then a and b are interchangeable under division. [a]

[a] Look at how far we've come! All four operations covered, including a bit of exponentiation.

3.3 Dividing Remainders

Let's take a further look at division with a couple of problems: (Don't worry, we're almost done!)

Example 3.16
Solve the following congruences for x.

- $4x \equiv 8 \pmod{37}$
- $4x \equiv 8 \pmod{38}$
- $6x \equiv 10 \pmod{15}$
- $28x \equiv 42 \pmod{126}$

Proof. Instead of trying to just guess solutions to the equation $4x \equiv 1 \pmod{37}$, we can try to take a shortcut. Just like in typical algebra, we may divide both sides of the equation by 4 to find the answer of:

$$\frac{4x}{4} \equiv \frac{8}{4} \pmod{37} \Rightarrow x \equiv \boxed{2} \pmod{37}.$$

But will we always be able to divide both sides like this? We can convince ourselves, in this case, that this manipulation is legal by subtracting by 8 on both sides to get:

$$4(x-2) \equiv 0 \pmod{37}.$$

This is equivalent to saying $4 \cdot (x-2)$ is divisible by 37. However, the factor of 4 cannot contribute to divisibility by 37, so $4 \cdot (x-2)$ is divisible by 37 **if and only if** $x-2$ to be divisible by 37, which only happens when $x \equiv 2 \pmod{37}$, as desired.

Exercise 3.17. Convince yourself that, if $\gcd(A, p) = 1$, then the solution to $Ax \equiv An \pmod{p}$ is $x \equiv n \pmod{p}$.

Exercise 3.18. Solve the equation $6x \equiv 12 \pmod{37}$ for x.

From Exercise 3.17, we may derive the following crucial fact:

Fact 3.19. Suppose both sides of a congruence have some common factor g. The congruence might look something like the following, where A and B are arbitrary expressions:

$$g \cdot A \equiv g \cdot B \pmod{p}.$$

If $\gcd(g, p) = 1$, then we are allowed to divide both sides of the congruence by g, just as we would in ordinary algebra!

Looking at the congruence $4x \equiv 8 \pmod{38}$, it seems like all we need to do is the following:

⚠ Dividing both sides by 4, we find the solution to be $x \equiv \boxed{2} \pmod{38}$.

However, not only is $x \equiv 2 \pmod{38}$ a solution, but so is $x \equiv 21 \pmod{38}$! What caused us to miss this second solution?

If we try to make a more rigorous argument, the same way we did previously by subtracting 8 on both sides, we find the congruence to be the same as:

$$4(x-2) \equiv 0 \pmod{38}.$$

This is equivalent to saying $4 \cdot (x-2)$ is divisible by 38. However, this does **not** imply that $x-2$ is divisible by 38; rather, it *only implies that* $x-2$ *must be divisible by* 19,[3] since the factor of 4 already provides the required power of two. Therefore, the solution set is:

$$x \equiv 2 \pmod{19}.$$

(Note that this is equivalent to saying that x is congruent to either 2 or 21 modulo 38.)

[3] In case you're not sure why this is the case, ask yourself: If $x-2$ were divisible by 19, why would $4 \cdot (x-2)$ be divisible by 38?

Exercise 3.20. Solve the equation $4x \equiv 8 \pmod{64}$ for x. (Hint: Subtract 8 from both sides and factor, like we have done in the past two exercises!)

In the case of $6x \equiv 10 \pmod{15}$, we notice that the left and right sides of this congruence share a factor of 2:

$$2(3x) \equiv 2(5) \pmod{15}.$$

In this case, since $\gcd(2, 15) = 1$, we can use Fact 3.19 to freely divide both sides of the congruence by 2 and work with the resulting congruence instead:

$$3x \equiv 5 \pmod{15}.$$

Now the left and right sides don't have any common factors, so we can't simplify the congruence any further. However, it turns out that this congruence has no solutions! To prove this, note that

$$3x \equiv 5 \pmod{15} \Rightarrow 3x - 5 \text{ is a multiple of } 15.$$

If $3x - 5$ is a multiple of 15, that also implies that $3x - 5$ is a multiple of 3. However, this is clearly impossible[4], so $3x \equiv 5 \pmod{15}$ cannot have any solutions.

Exercise 3.21. Which of the following congruences have a solution?

- $4x \equiv 3 \pmod{54}$
- $7x \equiv 14 \pmod{25}$
- $4x \equiv 12 \pmod{24}$
- $6x \equiv 9 \pmod{24}$

In the congruence $28x \equiv 42 \pmod{126}$, we might recognize that $28x$ and 42 both have factors of 14, so we might be willing to divide both sides of the equation by 14:

$$\frac{28x}{14} \equiv \frac{42}{14} \pmod{126} \Rightarrow 2x \equiv 3 \pmod{126}.$$

However, as we saw in the case of $4x \equiv 8 \pmod{38}$, this is not always allowed! In the statement of Fact 3.19, we are also required to have $\gcd(g, p) = 1$. In this case, $g = 14$, and $p = 126$, but $\gcd(14, 126)$ certainly does not equal one!

Whenever this happens, we can the trick of subtracting 42 from both sides and noting that $14 \cdot (2x - 3)$ must be a multiple of $126 = 14 \times 9$. The question now becomes: When is $14 \cdot (2x - 3)$ a multiple of 14×9?

You should be able to convince yourself that this happens if and only if $2x - 3$ is a multiple of 9, or when:

$$2x \equiv 3 \pmod{9}.$$

From here, we cannot simplify both sides of the equation any further, and it is not the case that this congruence has no solutions, so we simply guess-and-check[5] to discover $x \equiv 6 \pmod{9}$ to be the answer. □

[4] Why?

[5] We can also quicken this guesswork by noting that x must be a multiple of 3. Why is this true?

As you may have noticed so far, every time we want to divide both sides of a congruence by some number, we need to spend quite a long time checking all of the details. To quicken this process, we introduce the following "short-cut":

Fact 3.22. Suppose we wish to divide both sides of a congruence by some number A:

$$Am \equiv An \pmod{p}.$$

After dividing both sides of the congruence by A, we might need to change the modulus as well. If $g = \gcd(A, p)$, then if we want to divide both sides of the equation by A, we also need to divide by the modulus by g:

$$m \equiv n \pmod{\frac{p}{g}}.$$

In particular, if $g = \gcd(A, p) = 1$, then the modulus does not change.

The exact explanation for why this fact is true is not incredibly important; it essentially condenses the arguments we've been using for the past couple of problems into one easy-to-remember theorem.

Exercise 3.23. Solve the following congruences for x by using Fact 3.23:

- $4x \equiv 12 \pmod{14}$.
- $8x \equiv 6 \pmod{16}$.
- $5x \equiv 125 \pmod{17}$.
- $21x \equiv 28 \pmod{35}$.

And we're done!

4 Summary

For your convenience, here is a summary of this handout, all on one page!

Modular Arithmetic is an extension of the study of integers, stretching past the simple analyses of divisibility and prime factorization and venturing further into the examination of remainders and congruences. Here is a quick recap of everything we have discussed relating to modular arithmetic as of now:

- We say that two numbers are ***congruent modulo*** p if and only if they have the same remainder when divided by p, which is denoted as $a \equiv b \pmod{p}$.
- Note that $-4 \equiv 6 \pmod{10}$, not 4. Be careful with negative numbers in modular arithmetic!
- The significance of modular arithmetic comes from the fact that if $a \equiv b \pmod{p}$, then a and b are ***interchangeable*** under addition, subtraction, multiplication, division, and at the base (but not ceiling!) of an exponent.
- If we wanted to find the remainder when 6^7 were divided by 7, for example, we could note that $6 \equiv -1 \pmod{7}$ and write:
$$6^7 \equiv (-1)^7 \equiv -1 \equiv 6 \pmod{7},$$
rather than writing out 6^7 and dividing it by 7.
- Arithmetic sequences modulo primes tend to cycle through lots of numbers, while arithmetic sequences modulo composites sometimes repeat. Look back to page 9 for some more intuition.
- We say that:
$$\frac{a}{b} \equiv a \cdot \frac{1}{b} \equiv a \cdot b^{-1} \pmod{p}$$
in order to define fractions in modular arithmetic. Note that b^{-1}, called the inverse of b modulo p, is defined to be the solution to $bx \equiv 1 \pmod{p}$.
- When dividing in modular arithmetic, we need to take care of both the left and right sides of the congruence, along with the modulus. We do this by following this rule:

> **Fact 4.1.** Suppose we wish to divide both sides of a congruence by some number A:
> $$Am \equiv An \pmod{p}.$$
> After dividing both sides of the congruence by A, we might need to change the modulus as well. If $g = \gcd(A, p)$, then if we want to divide both sides of the equation by A, we also need to divide by the modulus by g:
> $$m \equiv n \pmod{\frac{p}{g}}.$$
> In particular, if $g = \gcd(A, p) = 1$, then the modulus does not change.

And that's all for the scope of this handout! Next time, we'll take a closer look at exponentiation and find even more curious patterns within modular arithmetic...

5 Problems

Try to aim for [50 ♟]. Problems marked with ♜ are required. (They still count towards the point total.)

> "What is the last digit of $11^{10} - 10^{11}$, written as a base ten numeral?"
>
> *Thomas Lam*

[3 ♟] Problem 1. Suppose the current time is 4 : 00 AM. What time will it be 133×135 hours from now? If your answer is X o'clock, input X as your answer.

[4 ♟] Problem 2. The remainder of $a + b$ divided by 47 is 23, and the remainder of $a - b$ divided by 47 is 34. What is the remainder of a divided by 47? **Hints**: 7

[5 ♜] Problem 3. Find the remainder when

$$2 \times 7 \times 12 \times \ldots \times 102$$

is divided by 5.

[5 ♟] Problem 4 (AoPS). Given that $13x \equiv 8 \pmod{137}$ and $14x \equiv 19 \pmod{137}$, what is the remainder when x^2 is divided by 137? **Hints**: 10 1

[5 ♜] Problem 5 (AoPS). What is the sum of all two-digit positive integers a for which $27a \equiv 17 \pmod{40}$? **Hints**: 6

[6 ♜] Problem 6 (MathCounts). Cards are numbered 1 through 2021. One of these cards is removed, and the values on the remaining 2020 cards are summed. The resulting sum is a multiple of 2017. What is the sum of all possible values of the removed card?

[6 ♟] Problem 7. What is the remainder when 125^{125} is divided by 127?

[6 ♟] Problem 8 (AoPS). For how many integers a satisfying $1 \leq a \leq 23$ is it true that $a^{-1} \equiv a \pmod{24}$? (Ignore when a^{-1} is undefined.)

[7 ♟] Problem 9 (2017 AMC 10A). Let $S(n)$ denote the sum of the digits of a positive integer n. For example, $S(1507) = 13$. For a particular positive integer n, $S(n) = 100$. What is the minimum possible value of $S(n+1)$? **Hints**: 2 16

[7 ♟] Problem 10. Find the remainder when

$$2 \times 9 \times 16 \times \ldots \times 2025$$

is divided by 56. **Hints**: 18

[7 ♟] Problem 11 (AoPS). What is the smallest positive integer a such that a^{-1} is undefined $\pmod{55}$ and a^{-1} is also undefined $\pmod{66}$?

[8 ♟] Problem 12. How many integers A between 1 and 24, inclusive, are such that the congruence:

$$Ax \equiv 14 \pmod{24}$$

has no solution?

[9 ♖] Problem 13. What is the remainder when $(10+2)^{2021}$ is divided by 100? **Hints**: 5 13

[19 ♟] Problem 14. In the following sequence of problems, we will guide you through a discussion of exponents in modular arithmetic:

1. **[3].** What is the sum of all (not necessarily distinct) remainders when 1^2, 2^2, 3^2, 4^2, and 5^2 are divided by 5?
2. **[5].** Cherri claims that the square of her favorite number has a remainder of r when divided by 11. What is the sum of all possible values of r?
3. **[11].** Squareman writes down his favorite perfect square, then erases one of the digits. If the sum of the remaining digits of Squareman's number is equal to 100, what is the sum of all possible values of the digit Squareman erased? **Hints**: 17

[11 ♟] Problem 15. What is the value of the sum:

$$\left\lfloor \frac{1^2}{7} \right\rfloor + \left\lfloor \frac{2^2}{7} \right\rfloor + \left\lfloor \frac{3^2}{7} \right\rfloor + \ldots + \left\lfloor \frac{100^2}{7} \right\rfloor,$$

where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x? **Hints**: 8

[25 ♟] Problem 16. These problems will give you an introduction to the Chinese Remainder Theorem, which will be expanded on in the next section:

1. **[6].** If some positive integer n has a remainder of 3 when divided by 4 and a remainder of 1 when divided by 3, what is its remainder when divided by 12? **Hints**: 3
2. **[8].** If some positive integer n has a remainder of $n-1$ when divided by n, for all positive integers n from 2 to 10, inclusive, what is the smallest possible value of n? **Hints**: 19
3. **[11].** What are the last two digits of 26^{26}? **Hints**: 14

[12 ♟] Problem 17. What is the remainder when:

$$63^1 + 63^2 + 63^3 + \ldots + 63^{100}$$

is divided by 127? **Hints**: 15

[13 ♟] Problem 18 (AOIME). Find the sum of all positive integers n such that when $\frac{n^2(n+1)^2}{4}$ is divided by $n+5$, the remainder is 17. **Hints**: 9

[13 ♟] Problem 19 (AHSME). There are unique integers $a_2, a_3, \ldots, a_7$ such that:

$$\frac{5}{7} = \frac{a_2}{2!} + \frac{a_3}{3!} + \ldots + \frac{a_7}{7!},$$

and $0 \leq a_i < i$ for all i. Find the value of:

$$a_7 \cdot 10^7 + a_6 \cdot 10^6 + \ldots + a_2 \cdot 10^2.$$

Hints: 12 11 4

6 Hints

1. One is equal to Fourteen minus Thirteen.
2. Since when has sums of digits ever been related to remainders? Since when has sums of digits ever been related to divisibility?
3. If we knew that $n \equiv 3 \pmod 4$, what possible remainders could n have when divided by 12? If you're unsure, try testing random values of n, like 3, 7, 11, 27, until you find a pattern.
4. You should have been able to find a_7 from the previous hint. Now, can you find a_6?
5. We didn't write 12^{2021} in the form $(a+b)^{2021}$ for nothing! What does $(a+b)^{2021}$ remind you of?
6. Fill in the blank: "If [blank] has a solution, then $ax \equiv b \pmod p$ has a solution as well."
7. How would you solve for a if it was just plain algebra, without any of the modular arithmetic?
8. It would be really nice if those $\lfloor x \rfloor$ symbols never existed in the first place; then we would be able to find the value of the sum. By how much do the floor functions change the sum?
9. If you've only found one valid choice of n, you missed something. In this case, it may be best to take the safest route possible, to ensure that you don't make any logical errors. [6]
10. Suppose I instead told you that $56x \equiv 3 \pmod 5$ and $57x \equiv 4 \pmod 5$. How might we be able to find x without trying to solve one of the congruences with messy division?
11. Remember that equation you got after removing all those fractions? It's of the form $a = b$. If $a = b$, then we also have $a \equiv b \pmod 7$. What does $a \equiv b \pmod 7$ tell you about a_7?
12. First, get rid of those fractions; we can't do modular arithmetic when we don't have integers! Now, focus on finding a_7 for now. What does the condition, "$0 \leq a_7 < 7$" remind you of?
13. Try giving the Binomial Theorem a shot, why not?
14. If we knew the remainder of n modulo 7 and 8, we would know the remainder modulo 56. If we knew the remainder of n modulo 3 and 11, we would know the remainder modulo 33. If we knew the remainder of n modulo...
15. You'll need to write the summation in closed form first. After that, try thinking about how 63 is related to 127, and you might be able to decrease the absolute values of the numbers you are working with by quite a lot.
16. The answer is an integer between 1 and 9, inclusive.
17. How are digit sums related to modular arithmetic?
18. Why could the remainder **not** equal one? Why not two? Or three? And why does eight seem more likely to be the answer?
19. Consider the properties of $n+1$.

[6] If you're confused on why you may be missing a solution, don't be afraid to contact us for help; this problem is tricky!