Modular Arithmetic

0.1 Integer Division

We all know very well how to divide one positive integer by another. For example, if you were asked to compute 41/9, you might write $9\overline{)41}$ and proceed to carry out the division algorithm. Of course in doing this you would rely heavily on your knowledge of multiplication. It comes as no surprise to us that division requires some guesswork followed by multiplication to check the guesswork. Thus, you would say 9 goes into 41 4 times with 5 left over. We can express this as

$$41 = 9 \cdot 4 + 5.$$

In this equation, the number 41 is called the *dividend*, 9 is the *divisor*, 4 is the *quotient*, and 5 is the *remainder*. So, in general, we have

$$\textit{dividend} = \textit{divisor} \cdot \textit{quotient} + \textit{remainder}.$$

Using the letters D for dividend, d for divisor, q for quotient, and r for remainder, we write $D = d \cdot q + r$. Notice that our remainder 5 is in the range $0, 1, 2, 3, 4 \ldots, 8$. Why can we insist that this always happens when we are dividing by 9? What would a remainder larger than 9 mean? What would a negative remainder mean? If we insist, as we shall from here on that the remainder r be in the range $0, 1, 2, \ldots, d-1$, we may then assert the division algorithm:

Division Algorithm Given any integer D and any nonzero integer d, there exist unique integers q and r satisfying both

a. $D = d \cdot q + r$ and

b. $0 \leq r \leq |d| - 1$.

Note that in case $r = 0$, we call d a *divisor* of D. Notice also that neither D nor d is required to be positive. When either or both is negative, the equations and uniqueness still hold. For example, when $D = -31$ and $d = 9$, we get

$$-31 = 9(-4) + 5.$$

You'll see that this is very important when we use the division algorithm to find the representation of a positive or negative integer when the base number is negative.

Look at the two examples, $41 = 9 \cdot 4 + 5$, and $-31 = 9(-4) + 5$. In both cases we can say that q is the largest number such that $9q$ is less than D. Geometrically,

think of marking of segments of length 9 units to the right if $D > 0$, and to the left if $D < 0$ until we get to the multiple of 9 that is 8 or fewer units to the left of D.

see pics here. There is a nice way to write q and r in terms of D and d. To explore this, define the *floor* function $\lfloor x \rfloor$ of a number x as the largest integer that is not bigger than x. This useful function has a companion function, the *ceiling* function, $\lceil x \rceil$ which is the smallest integer that is not less than x. Another function we will need to know about is the fractional part function $\langle x \rangle$ which is defined as follows: $\langle x \rangle = x - \lfloor x \rfloor$. See the exercises and those in the module that covers place value.

1. For each of the real numbers x listed, find $\langle x \rangle$, $\lfloor x \rfloor$ and $\lceil x \rceil$.
   (a) $x = 3.14$
   (b) $x = -3.14$
   (c) $x = 4.216$
   (d) $x = -4.216$
2. Sketch the graphs of the three functions on the cartesian coordinate system.
3. For each of the pairs D and d listed, find q and r using the formulas $q = \lfloor D/d \rfloor$ and $r = D - \lfloor D/d \rfloor \cdot d$. Notice that your graphing calculator has the functions $\langle x \rangle$, $\lfloor x \rfloor$ and $\lceil x \rceil$ built in.
   (a) $D = 77, d = 5$
   (b) $D = -77, d = 5$
   (c) $D = 77, d = -5$
   (d) $D = -77, d = -5$

0.2 Modulo 9 congruence

Now we see that both 41 and -31 are 5 units larger than some multiple of 9. Note that their difference $41 - (-31) = 72$ is a multiple of 9. Of course this happens for any two numbers D_1 and D_2 whenever the remainders, upon division by 9, are the same. To prove this, suppose r is that remainder. Then

$$D_1 = 9 \cdot q_1 + r \quad \text{and} \quad D_2 = 9 \cdot q_2 + r.$$

Then

$$\begin{aligned} D_1 - D_2 &= 9 \cdot q_1 + r - (9 \cdot q_2 + r) \\ &= 9 \cdot q_1 + r - (9 \cdot q_2 + r) \\ &= 9 \cdot q_1 - 9 \cdot q_2 + r - r \\ &= 9 \cdot (q_1 - q_2). \end{aligned}$$

On the other hand, the converse is also true: If two numbers D_1 and D_2 differ by a multiple of 9, upon division by 9, the remainders are the same. To see this, suppose $D_1 = 9 \cdot q_1 + r_1$ and $D_2 = 9 \cdot q_2 + r_2$. Since $D_1 - D_2$ is a multiple of 9, we can write $D_1 - D_2 = 9 \cdot q_1 + r_1 - (9 \cdot q_2 + r_2) = 9k$, for some integer k. We can solve this for $r_1 - r_2$ to get $r_1 - r_2) = 9k - (9 \cdot q_1 - 9 \cdot q_2) = 9(k - q_1 + q_2)$, so $r_1 - r_2$ is a multiple of 9. Since both r_1 and r_2 are in the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, the largest they could differ by is 8 and the least they could differ by is -8. The only multiple of 9 in that range is 0, so $r_1 - r_2 = 0$, which is what we wanted to prove.

We encounter two integers D_1 and D_2 that have this relationship often enough to give the relationship a special name: *modular congruence*. Two numbers that differ by a multiple of 9 are said to be congruent modulo 9, and we write $D_1 \equiv D_2 \pmod 9$.

Of course there is nothing special about the number 9 except that it is positive. Hence we have the following definition.

Congruence Modulo m Let m be a positive integer. Two numbers D_1 and D_2 are congruent modulo m, and we write $D_1 \equiv D_2 \pmod m$ if $D_1 - D_2$ is a multiple of m.

The definition of congruence, which has nothing to do with the same word used in geometry, is due to Carl Gauss. Gauss noticed that the relationship that two numbers D_1 and D_2 have the same remainder upon division by another number m kept turning up in his examples and proofs. For example, the set of even numbers are those which yield a zero remainder when divided by 2. Thus congruence modulo 2 means that the two integers are either both even or both odd. This is a good time to practice with congruences.

0.3 Properties of Modular Congruence

In this section, we discuss three important properties of modular congruence and in the next section, two more. The first three are the properties required for an equivalence relation. An *equivalence* relation is a binary relation that satisfies the three properties of *reflexivity*, *symmetry*, and *transitivity*, defined below. In the Discrete Math course, you will learn all about binary relations. However, we do not assume here that you are familiar with the properties of binary relations.

1. Congruence modulo m is a *reflexive* relation. That is, for every integer u, $u \equiv u \pmod{m}$. This is clearly true because $u - u = 0$ is a multiple on m.

2. Congruence modulo m is a *symmetric* relation. This means that if u and v are integers satisfying $u \equiv v \pmod{m}$, then $v \equiv u \pmod{m}$. This property follows from the fact that the negative of a multiple of m is also a multiple of m.

3. Congruence modulo m is a *transitive* relation. This means that for any three integers u, v and w satisfying $u \equiv v \pmod{m}$ and $v \equiv w \pmod{m}$, it is also true that $u \equiv w \pmod{m}$. To prove this, let u, v and w satisfy the hypothesis. Then $u - v = km$ and $v - w = lm$, where k and l are integers. Now $u - w = u - v + v - w = km + lm = (k + l)m$. In other words, $u - w$ is a multiple of m.

Of course you recognize that equality ($=$) satisfies all three of these, and indeed, modular congruence **is** a relation very much like equality. Besides discrete math, you might see *equivalence relations* in the course that develops the number system and in the abstract algebra course. Relations satisfying properties 1, 2, and 3, that is, equivalence relations, above are common in mathematics. The most important property of equivalence relations is that each one gives rise to a partition of the set on which it is defined. The sets in the partition are called the *cells* of the relation. See theorem 1 below.

In discussing the next two properties, we'll consider again the special case $m = 9$. Although the properties are true for any positive integer m, we are going use the case $m = 9$ repeatedly in the problems, and the proofs are simplified a tiny bit using the 9 where we otherwise use m.

0.4 Definition of Cells

Recall that we are discussing the relation that has a pair (u, v) (or u is related to v) provided $u \equiv v \pmod{9}$, or equivalently, $u - v$ is a multiple of 9. For each integer k, the sell of $\overline{k}$, denoted k is the set of integers n to which k is related. Symbolically, $\overline{k} = \{n \mid k \equiv n \pmod{9}\}$. Thus, for example,

$$\overline{0} = \{n \mid 0 \equiv n \pmod{9}\} = \{0, \pm 9, \pm 18, \ldots\}$$

and

$$\overline{1} = \{n \mid 1 \equiv n \pmod{9}\} = \{1, -8, 10, -17, 19, \ldots\}.$$

Notice that $\overline{0} = \overline{9}$ because any number that 0 is congruent to, 9 is also congruent to. To be a little more formal about about it, take an arbitrary member n of $\overline{0}$.

Then $0 \equiv n \pmod 9$. Since $9 \equiv 0 \pmod 9$ and congruence modulo 9 is known to be transitive (see property 3 above), we see that the pair $9 \equiv 0 \pmod 9$ and $0 \equiv n \pmod 9$ implies $9 \equiv n \pmod 9$. So we have proved that if $n \in \overline{0}$ then $n \in \overline{9}$, which in set terms means $\overline{0} \subseteq \overline{9}$. Similarly, we can prove that $\overline{9} \subseteq \overline{0}$. But these two set inequalities are together equivalent to saying $\overline{0} = \overline{9}$.

0.5 The Partition of an Equivalence Relation

In this section we state and prove the theorem mentioned above on partitions induced by equivalence relations. Although a much more general theorem on equivalence relations is provable here, we will simply use the congruence modulo m on the set Z of integers. We proved Theorem 1 in section 3.

Theorem 1. Let m be a positive integer. Congruence mod m is an equivalence relation.

Theorem 2. Let m be a positive integer. For each integer u let $[u]$ denote the cell of u. If $[u]$ and $[v]$ are two cells, modulo m, then either $[u]$ and $[v]$ are disjoint or identical.

Proof. These cells are also called equivalence classes. To see that two cells $[u]$ and $[v]$ are identical if have any integers in common, note that if w belongs to both $[u]$ and $[v]$, then $u \equiv w \pmod m$ and $v \equiv w \pmod m$, by the definition of cell. By symmetry $w \equiv v \pmod m$ and by transitivity $u \equiv v \pmod m$. Then again symmetry by transitivity, any integer z in $[u]$ satisfies $z \equiv u \pmod m$ and hence $z \equiv v \pmod m$, so z belongs to $[v]$.

The Arithmetic of Congruences In order to build a mathematical structure using cells as "numbers", we have to be sure that addition and multiplication are well-defined operations. The method for defining the sum $\oplus$ and the product $\odot$ of two cells is pretty clear. For example, if $[x]$ and $[y]$ are cells modulo 6 we want $[x] \oplus [y]$ to be $[x + y]$ and $[x] \odot [y]$ to be $[x \cdot y]$. But we must be sure that these operations are well-defined. That is, $\oplus$ and $\odot$ must deliver unique values.

Theorem 3. Let x and y be integers and $[x]$ and $[y]$ their cells modulo m. Suppose $a \in [x]$ and $b \in [y]$. Then $a + b \in [x + y]$. In other words, no matter which representatives of $[x]$ and $[y]$ we choose, the sum is always the cell $[x + y]$.

Proof. To say $a \in [x]$ means that $x \equiv a \pmod m$. Likewise, $y \equiv b \pmod m$.

Now $x + y - (a + b) = (x - a) + (y - b)$ is the sum of two multiples of m, and therefore is itself a multiple of m. In other words $a + b \in [x + y]$, as we set out to prove.

Here is a nice application of Theorem 3.

Problem Find the units digit of the Fibonacci number F_{2000}.

Solution: Recall that the Fibonacci numbers are defined by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$. Since the units digit of F_n is the remainder when F_n is divided

by 10, we can solve the problem by finding the cells modulo 10 of the F_n's.

Theorem 3 makes this easy. It says that the units digit of the sum of two F's is the units digit of the sum of the units digits of those F's. The table below shows the units digits of the first 60 Fibonacci numbers in groups of 10. The first 30 entries are given by

1	1	2	3	5	8	3	1	4	5
9	4	3	7	0	7	7	4	1	5
6	1	7	8	5	3	8	1	9	0

Notice that the next 30 entries are

9	9	8	7	5	2	7	9	6	5
1	6	7	3	0	3	3	6	9	5
4	9	3	2	5	7	2	9	1	0

We are now in position to build the table for $\oplus$ modulo m. Let's choose $m = 6$ again. In the exercises you'll get to do this for $m = 7$. Since division by 6 produces the 6 remainders 0,1,2,3,4, and 5, we use these numbers as names of cells. What is $[3] \oplus [5]$? To see this, divide $3 + 5$ by 6, getting a remainder of 2, so $[3] \oplus [5] = [3 + 5] = [2]$.

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

Theorem 4. Let x only be integers and $[x]$ and $[y]$ their cells modulo m. Suppose $a \in [x]$ and $b \in [y]$. Then $a \cdot b \in [x \cdot y]$. In other words $[x] \odot [y] = [x, y]$ is a well-defined binary operation.

Proof. As before, the hypothesis means that $x - a$ and $y - b$ are multiples of m. Let's say $x - a = km$ and $y - b = lm$. Then $xy - ab = xy - ay + ay - ab = (x - a)\, y + a\,(y - b) = kmy + alm = m\,(ky + al)$ which, of course, is a multiple of m since $ky + al$ is an integer.

We can now build the $\odot$ for any positive integer m. Again we use $m = 6$.

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

The next theorem follows easily from Theorem 4. We'll use it to find remainders when the n^{th} power of an integer k is divided by another integer m.

Theorem 5. If $a \equiv b \pmod{m}$ then, for every positive integer n, $a^n \equiv b^n \pmod{m}$.

The proof is by mathematical induction on n. Skip ahead if you need to, to see how proofs by induction work. First note that $a' \equiv b' \pmod{m}$, the base case, is the hypothesis. Next, suppose $a^{n-1} \equiv b^{-1} \pmod{m}$. Now apply Theorem 2 with $x \equiv b$ and $y = b^{n-1}$. Then $a \equiv b \pmod{m}$ and $a^{n-1} \equiv b^{n-1} \pmod{m}$. Therefore $a \cdot a^{n-1} \equiv b \cdot b^{n-1} \pmod{m}$, and we are done.

The next example is of the type promised just before Theorem 5. **Problem** Find the remainder when 7^{2009} is divided by 5.

Solution: Note that $7 \equiv 2 \pmod{5}$. Theorem 3 implies that $7^2 \equiv 2^2 \pmod{5}$. Now $2^2 = 4 \equiv -1 \pmod{5}$. Putting all this together we have $7^4 \equiv (2^2)^2 \equiv (-1)^2 \equiv 1 \pmod{5}$. Thus, $7^{2009} \equiv 7^{2008+1} \equiv 7^{4.502+1} \equiv 7^{4.502} \cdot 7 \equiv (7^4)^{502} \cdot 7 \equiv 1^{502} \cdot 7 \equiv 1 \cdot 7 \equiv 2 \pmod{5}$. So the remainder is 2.

0.6 Divisibility by 9, 3 and 11

The aim of this section is to demonstrate an easy method for finding the cell of a positive integer written in decimal notation modulo 3 or 9 or 11. by the way, the cell is often referred to as the residue class of the number. For example, we could say that the residue class of 101 modulo 9 is 2 because you get a remainder of 2 when you divide 101 by 9.

First we'll take an example. What is the residue class of 3742 modulo 9? Notice that $1000 \equiv 999 + 1 \equiv 0 + 1 \equiv 1 (\text{mod } 9)$. Likewise, $100 \equiv 99 + 1 \equiv 0 + 1 \equiv 1 (\text{mod } 9)$. Of course $10 \equiv 1 (\text{mod } 9)$ also. Using the language of modular arithmetic, we have $3742 \equiv 3000 + 700 + 40 + 2 \equiv 3 \cdot 1000 + 7 \cdot 100 + 4 \cdot 10 + 2 \equiv 3 \cdot 1 + 7 \cdot 1 + 4 \cdot 1 + 2 \equiv 3 + 7 + 4 + 2 \equiv 7 (\text{mod } 9)$. Thus 3742 is congruent modulo 9 to the sum of its digits.

Theorem 6. Every positive integer n is congruent modulo 9 to the sum of its decimal digits.

Proof. Recall that the decimal representation of a number is a sum of multiples

of powers of 10. Thus

$$\begin{aligned} n &= (a_k \dots a_0)_{10} \\ &= a_k \left(\underbrace{99\dots9}_{\text{k 9's}} + 1 \right) + a_{k-1} \left(\underbrace{9\dots9}_{\text{(k-1) 9's}} + 1 \right) + \dots + a_1 (9+1) + a_0 \\ &= a_k \left(\underbrace{99\dots9}_{\text{k 9's}} \right) + a_{k-1} \left(\underbrace{9\dots9}_{\text{(k-1) 9's}} \right) + \dots + a_1 (9) + (a_k + a_{k-1} + \cdots a_0) \\ &= 9M + \left(\underbrace{a_k + a_{k-1} + \cdots + a_0}_{\text{sum of digits}} \right). \end{aligned}$$

Notice that the very same reasoning works for congruence modulo 3. Modulo 11 work is a bit more complicated. Note that $1 \equiv 1 (\text{mod } 11)$, $10 \equiv -1 (\text{mod } 11)$, $100 = 10^2 \equiv (-1)^2 \equiv 1 (\text{mod } 11)$. In general $10^n \equiv (-1)^n (\text{mod } 11)$. Thus $3742 \equiv 2 - 4 + 7 - 3 \equiv 2 (\text{mod } 11)$. In other words, when we divide 3742 by 11, we get a remainder of 2. The sum $2 - 4 + 7 - 3$ is called the *alternating sum* of digits.

0.7 Problems and Exercises

1. Find the congruence class of each of the integers given modulo 9.
   (a) 12345
   (b) 637228195
   (c) 12345678910111213 . . . 99 obtained by writing down the positive integers from 1 to 99 next to one another.
2. Find the congruence class of each of the integers given modulo 3.
   (a) 12345
   (b) 637228195
   (c) 12345678910111213 . . . 99 obtained by writing down the positive integers from 1 to 99 next to one another.
3. Find the congruence class of each of the integers given modulo 11.
   (a) 12345

(b) 637228195

(c) 12345678910111213 . . . 99 obtained by writing down the positive integers from 1 to 99 next to one another.

4. Find the congruence class of each of the integers given modulo 99.

   (a) 12345

   (b) 637228195

   (c) 12345678910111213 . . . 99 obtained by writing down the positive integers from 1 to 99 next to one another.

5. Find the congruence class of each of the integers given modulo 66.

   (a) 12345

   (b) 637228195

   (c) 12345678910111213 . . . 99 obtained by writing down the positive integers from 1 to 99 next to one another.

6. Build the $\oplus$ and $\odot$ tables for the congruence classes modulo 7. The mathematical system we get is denoted $(Z_7, \oplus, \odot)$.

   (a) show that $(Z_7, \oplus)$ is a group.

   (b) show that $(Z_7, \{[0]\}, \odot)$ is a group.

   (c) $(Z_7, \oplus, \odot)$ has the other properties (field axioms). This proves that $(Z_7, \oplus, \odot)$ is a field. You'll study structures like this in the abstract algebra course.

   (d) Solve the linear congruences.
   $[2] \odot [x] + [1] = [0]$
   (some texts would write this $2x + 1 = 0$.)

7. Among the integers $1, 2, \ldots, 1997$, what is the maximum number of integers that can be selected such that the sum of any two selected number is not a multiple of 7.