2.1 GENERAL BACKGROUND: WHAT YOU ALREADY KNOW

Suppose you have to do an addition, say $357 + 586$. How much do you need to know in order to know the last digit of the answer? Would the last digit of each summand be enough? Suppose, instead, that it’s a subtraction problem? A multiplication problem? A division problem?

We think you will immediately see that, to know the last digit of the answer to the addition problem you only need to know the last digit of each of the summands. (In the above example you would simply add 7 to 6, ignore the 1 in the tens position and get 3.) Likewise, to know the last two digits of the answer, you only need the last two digits of the summands (so that, above, you would add 57 to 86, ignore the 1 in the 100 position, and get 43), and so on. Indeed, the traditional algorithm for adding a column of figures exploits this fundamental fact. And what goes for addition is true of subtraction and multiplication, too, though not of division, even where the divisor is an exact factor of the dividend (think of $12 \div 2$, $22 \div 2$).
Let us concentrate for the moment on the last digit. The last
digit of the integer $a$ may be described as the remainder when $a$ is
divided by 10. Then, as we have said above, the remainder when
$a + b$ is divided by 10 may be obtained from the remainders when
$a$ and $b$ are divided by 10; and the same goes for the remainder
when $a - b$ or $ab$ is divided by 10. And what goes for remainders
when you divide by 10 is just as true for remainders when you
divide by 100, 1000, and so on.

Now comes the big, but obvious step—the same goes when you
divide by any integer $m$. Those of you who have done arithmetic
in various bases will already have met this fact, but we feel that
none of our readers will have any real difficulty in understanding
this. Thus, for example, if $a = 44$ and $b = 23$, we see that 44 has
a remainder of 4 and 23 has a remainder of 3 when divided by 5.
Thus we know that the remainder when $a + b (= 67)$ is divided by 5
is the same as the remainder when $4 + 3$ is divided by 5, that is, 2;
and $a - b (= 21)$ leaves a remainder of $4 - 3$, or 1, when divided
by 5. In just the same way we know that $44 \times 23$ leaves the same
remainder as $4 \times 3$ when divided by 5, that is, a remainder of 2. It
is very striking that we don’t need to calculate $44 \times 23$ to get this
last result!

**BREAK**

Check the results of the last paragraph. Then try some
examples with a value of $m$ different from 5.

Mathematicians like to use short, pithy phrases, so, instead of
the long-winded “the remainder when you divide by $m$” they say
“the remainder mod $m$” and the set of all integers leaving the same
remainder mod $m$ is called a **residue class** mod $m$; here “mod” is
short for “modulo,” and $m$ is called the “modulus.” Thus the re­
mainder mod $m$ is a specially chosen member of its residue class,
namely, that integer $r$ in the class which satisfies $0 \leq r < m$. No­
tice that there are only finitely many residue classes mod $m$ (in
fact, there are precisely $m$ such classes), but that a residue class
contains infinitely many integers.

---

1Another example of a short, pithy phrase is “the triangle $ABC$” instead of “the triangle
with vertices $A, B, C$.” Can you think of further examples?