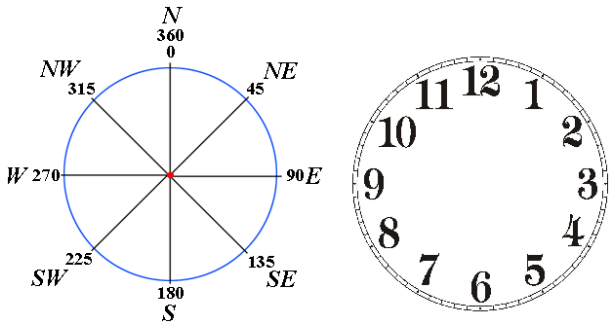
Modular Arithmetic Investigation

The basics

Definition: Two numbers are considered **congruent, modulo n** if they are exactly a multiple of n apart. Equivalently, if the two numbers are the same distance away from a multiple of n.
Example: 17 and 122 are congruent, modulo 5, because $17 = 5 \times 3 + 2$ and $122 = 5 \times 24 + 2$. They are both 2 more than a multiple of 5.

Definition: The **residue** of a number, modulo n, is the smallest number (always between 0 and $n - 1$) which is congruent to the original number, modulo n.
Example: The residue of 34, modulo 10, is 4, because it is the smallest number which is, like 34, also 4 more than a multiple of 10.



Notation: The statement "17 is congruent to 302, modulo 3" can be written as: "$\mathbf{17}\ \boldsymbol{mod}\ \mathbf{3} \equiv \mathbf{302}\ \boldsymbol{mod}\ \mathbf{3}$", or often just "$\mathbf{17} \equiv \mathbf{302}\ \boldsymbol{mod}\ \mathbf{3}$". If the modulus is known, you can get away with abbreviating this further to "$\mathbf{17} \equiv \mathbf{302}$". For instance, if we are just dealing with $mod\ 10$, it is fine to write $31415 \equiv 66435 \equiv 5$, etc.

The investigation

The aim is to investigate how the rules of *adding* and *multiplying* apply to modular arithmetic.

Getting started

As with any open investigation, conclusions are most readily found through a clear, structured approach which relies on the use of conjectures to direct your efforts. A conjecture is simply an observation which you think may be true. You do not need to be convinced by it, but by clarifying the pattern or rule you think you have observed you will be in a better position to investigate further and hopefully prove or disprove your conjecture – either is beneficial. If you prove a conjecture correct, see if you can strengthen or extend it. If you prove it false, consider how it might be modified or improved to make it true. If you find a conjecture is partially true, but breaks down in certain cases, consider what makes those cases different and try to develop or modify your conjecture accordingly.

Problem solving

Begin by following these three simple steps:

1. Clarify the question	Even if the problem you are working on is given in deliberately vague terms (like this one!) you should do your best to narrow down what is being asked. • How will you know when you've solved the problem? • What would a satisfactory answer look like? • Will you need to demonstrate how you got your answer?
2. Consider your position	Having a clear view of your starting point will help you see where to go next. • What do you already know that may be helpful? • What relevant information have you been given?
3. Choose an approach	• When you get stuck, try a different tack. • Use conjectures to test your ideas, and when you think you have found a valid conclusion, try to explain why it must be true. • If the problem is too hard to tackle, try to simplify it. Solve an easier version, then see if you can extend the ideas to the harder one.

Modular Arithmetic Investigation
Hints, suggestions and challenges

Hints & suggestions for how to proceed

- Start by choosing a modulus, and calculate the residue of a few numbers with this modulus.
- Try adding a pair of numbers, and see what happens to the residue. Make a table listing the residue of the numbers you added and the residue of the answer. See if you can form a rule that describes what is happening, and explain why it works.
- Follow a similar approach to investigate multiplication. List some numbers, and their residue, then tabulate the residue of their product. Look for a rule that links the two original residues with the result.
- As an extension, consider powers. To begin with, use a modulus of 10, and investigate this for successive powers of, say 2. Is there a pattern to the residues? Will there be a pattern for different moduli? Or for powers of a different number?

The final challenges

Once you've developed your ideas sufficiently and reached some useful conclusions, you should be able to attempt a few of these (hard) challenges:

(answers should be relatively easily calculated **without** a calculator by using clever simplifying: if you're struggling with the multiplication you're trying too hard!)

1. Find the remainder when $3 + 52 + 97 + 22 + 438$ is divided by 10.
2. Find the remainder when $3 \times 52 \times 97 \times 22 \times 438$ is divided by 10.
3. Find the remainder when $3 \times 52 \times 97 \times 22 \times 438$ is divided by 7.
4. Find the remainder when 2^{64} is divided by 10. (Hint: consider 2^2, then $(2^2)^2$, etc.)
5. The largest known prime, as of 2014, is the 48th Mersenne prime (one in the form $2^p - 1$ where p is prime), which is: $2^{57885161} - 1$. Find the last digit of this number. (Hint: use modulus 10).
6. Find the remainder when $2^{57885161} - 1$ is divided by 11.

What's next?

The powerful nature of modular arithmetic is responsible for the RSA encryption algorithm, which requires computers to calculate otherwise intractable problems involving huge powers. The tricks with the modulus function allow one-way calculations to be done quickly, while reversing the calculations with current knowledge and computing power would take years and years. This is the basis of internet security (look up Public Key RSA encryption for more details).

Modular Arithmetic Investigation SOLUTIONS

Note: the following is designed to resemble a logical approach to the problem. It is not the *only* logical approach by any means, and – since it does not include dead ends or unproductive conjectures it is both unrealistically short compared to a genuine investigation and unrealistically linear in its progress.

Firstly, we can look at **adding**, using a really simple example – modulo 2. This should give us results we are already familiar with (for instance, adding two odd numbers gives an odd number).

$5 \equiv \mathbf{1}\ mod\ 2$	$6 \equiv \mathbf{0}\ mod\ 2$	$5 + 6 \equiv 11 \equiv \mathbf{1}\ mod\ 2$
$10 \equiv \mathbf{0}$	$4 \equiv \mathbf{0}$	$10 + 4 \equiv 14 \equiv \mathbf{0}$
$7 \equiv \mathbf{1}$	$11 \equiv \mathbf{1}$	$7 + 11 \equiv 18 \equiv \mathbf{0}$

Conjecture:
When two numbers are added, the sum of their residues is congruent to the residue of their sums.

In other words:

$$(\boldsymbol{a\ mod\ n}) + (\boldsymbol{b\ mod\ n}) \equiv (\boldsymbol{a + b})\ \boldsymbol{mod\ n}$$

Testing the conjecture with a different modulus:

The residue of the sum:

$$(245 + 16)\ mod\ 10 \equiv 261\ mod\ 10 \equiv \mathbf{1}\ \boldsymbol{mod}\ \mathbf{10}$$

The sum of the residues:

$$(245\ mod\ 10) + (16\ mod\ 10) \equiv (5) + (6) \equiv 11 \equiv \mathbf{1}\ \boldsymbol{mod}\ \mathbf{10}$$

This appears to be true.

Proof:
$a\ mod\ n$ can be written as $pn + q$ where q is the remainder when a is divided by n.
(For instance $29\ mod\ 6$ can be written as $4 \times 6 + 5$).

Then when this is added to $b\ mod\ n$ (which we can assume, similarly, may be written as $rn + s$), we get:

$$(pn + q) + (rn + s) = (p + r)n + (q + s)$$

Finding the residue of this, $mod\ n$, will be equivalent to finding the residue of $q + s$ since the residue of $(p + r)n$ must be 0 (it has n as a factor). Therefore the sum of the original residues ($q + s$) is congruent to the residue of the sum (also $q + s$).

Challenge Question 1 Solution
Find the remainder when $3 + 52 + 97 + 22 + 438$ is divided by 10.

Since adding numbers then finding their residue is equivalent to finding their residue then adding, we can simplify this whole problem to:

$$3 + 2 + 7 + 2 + 8$$

Which gives:

$$22$$

Which is congruent to:

$$\mathbf{2}$$

Next, we will investigate **multiplying**, modulo 5.

$12 \equiv \mathbf{2}\ mod\ 5$	$10 \equiv \mathbf{0}\ mod\ 5$	$12 \times 10 \equiv 120 \equiv \mathbf{0}\ mod\ 5$
$7 \equiv \mathbf{2}$	$6 \equiv \mathbf{1}$	$7 \times 6 \equiv 42 \equiv \mathbf{2}$
$8 \equiv \mathbf{3}$	$9 \equiv \mathbf{4}$	$8 \times 9 \equiv 72 \equiv \mathbf{2}$

Initially it looked like the product of the residues gave the same as the residue of the product, but, as the last example shows, it is not quite that simple. However, notice that $3 \times 4 \equiv 12 \equiv 2$, so the results are congruent, just like when adding.

Conjecture:
When two numbers are multiplied, the product of the residues is congruent to the residue of the product.

Proof:
Let $a\ mod\ n$ be equal to $pn + q$ as in the previous proof, and $b\ mod\ n$ be equal to $rn + s$.

Then:

$$(a\ mod\ n)(b\ mod\ n) \equiv (pn + q)(rn + s) \equiv prn^2 + (qr + ps)n + qs \equiv qs$$

Note that this expression can be written as $n(prn + qr + ps) + qs$, and since all but qs has a factor of n, the residue of this expression is simply the residue of qs. That is, the product of the residues (qs) is congruent to the residue of the product (also qs).

Challenge Question 2 Solution
Find the remainder when $3 \times 52 \times 97 \times 22 \times 438$ is divided by 10.

Just like with adding, we can take residues before we start and make everything simpler:

$$3 \times 2 \times 7 \times 2 \times 8$$

And even as we go along, we can simplify at each step by taking residues again. For instance, $2 \times 8 \equiv 6$:

Grouping in any convenient way you like:

$$(3 \times 2 \times 7) \times (2 \times 8)$$

Multiplying:

$$42 \times 16$$

Taking residues to make the next step easier:

$$2 \times 6$$

Multiplying:

$$12$$

Taking residues again:

$$\mathbf{2}$$

Challenge Question 3 Solution
Find the remainder when $3 \times 52 \times 97 \times 22 \times 438$ is divided by 7.

This is really the same process as above, but residues are just a little less easy to spot since they won't just be the last digit, but the remainder when dividing by 7.

Since $52 \equiv 3$, $97 \equiv 6$, etc:

$$3 \times 3 \times 6 \times 1 \times 4$$

Grouping conveniently:

$$(3 \times 3) \times (6 \times 1 \times 4)$$

Multiplying:

$$9 \times 24$$

Taking residues to make the next step easier:

$$2 \times 3$$

Multiplying:

$$\mathbf{6}$$

Powers are somewhat more confusing, but they build on the concept of multiplying.

Note that if $(a \ mod \ n)(b \ mod \ n) \equiv (ab \ mod \ n)$, as proved above, then $(a \ mod \ n)^2 \equiv a^2 \ mod \ n$.

This can be extended to say that $(a \ mod \ n)^k \equiv a^k \ mod \ n$, which means that we know for certain that, since $37 \equiv 7 \ mod \ 10$, it follows that $37^2 \equiv 7^2 \ mod \ 10$. We can test this: $37^2 \equiv 1369 \equiv 9 \ mod \ 10$, and also we know that $7^2 \equiv 49 \equiv 9 \ mod \ 10$.

Using $mod \ 10$ (since it is easy to identify the residue – simply the last digit):

$$7^1 \equiv 7 \ mod \ 10$$

$$7^2 \equiv 49 \equiv 9 \ mod \ 10$$

$$7^4 \equiv (7^2)^2 \equiv 9^2 \equiv 81 \equiv 1 \ mod \ 10$$

$$2^2 \ mod \ 10 \equiv 4 \implies (2^2)^2 \ mod \ 10 \equiv 4^2 \ mod \ 10 \equiv 16 \ mod \ 10 \equiv 6$$

$$\implies \quad ((2^2)^2)^2 \equiv 6^2 \ mod \ 10 \equiv 36 \ mod \ 10 \ \equiv 6 \ mod \ 10$$

Challenge Question 4 Solution
Find the remainder when 2^{64} is divided by 10. (Hint: consider 2^2, then $(2^2)^2$, etc.)

Since $2^2 \equiv 4$, we know $(2^2)^2 \equiv 4^2 \equiv 16 \equiv 6$.

And this means that $((2^2)^2)^2 \equiv 6^2 \equiv 36 \equiv 6$. Turns out, any power of 2 in this form is congruent to 6.

$$2^{64} \equiv (2^{32})^2 \equiv ((2^{16})^2)^2 \equiv (((2^8)^2)^2)^2 \equiv ((((2^4)^2)^2)^2)^2 \equiv (((((2^2)^2)^2)^2)^2)^2 \equiv \mathbf{6}$$

The idea of using the modulus of the power to calculate the modulus of a number is a very powerful tool for dealing with otherwise impossibly large numbers. We can look for patterns within powers, then use those:

Powers of 2	Residue modulo 10
2^1	2
2^2	4
2^3	8
2^4	6
2^5	2
2^6	4
2^7	8
2^8	6

The pattern should be clear. $2^{1+4k} \equiv 2$, and $2^{2+4k} \equiv 4$ etc, for all k. This pattern can be verified by considering multiplication by 2 from one term to the next:

$$2 \times 2 \equiv 4$$
$$4 \times 2 \equiv 8$$
$$8 \times 2 \equiv 6$$
$$6 \times 2 \equiv 2$$
$$etc \ldots$$

Challenge Question 5 Solution

The largest known prime, as of 2014, is the 48th Mersenne prime (one in the form $2^p - 1$ where p is prime), which is: $2^{57885161} - 1$. Find the last digit of this number. (Hint: use modulus 10).

We are looking for the residue of $2^{57885161} - 1$, modulo 10.

First, consider the power: $57885161 \equiv 1 \ mod \ 4$. In other words, it is 1 greater than a multiple of 4, and therefore fits in the same category as 2^5 or 2^9, and must end in a 2.

$$2^{57885161} \equiv 2 \ mod \ 10 \quad \Longrightarrow \quad 2^{57885161} - 1 \equiv 1 \ mod \ 10 \quad \Longrightarrow \quad \boldsymbol{Last\ Digit = 1}$$

To solve the final challenge question, all it takes is examining powers of 2 in relation to a different modulus:

Powers of 2	Residue modulo 11
2^1	2
2^2	4
2^3	8
2^4	5
2^5	10
2^6	9
2^7	7
2^8	3
2^9	6
2^{10}	1

While the pattern for mod 10 seemed nicer, because 2 and 10 are not coprime (that is, they share a common factor), we never got to a point where the residue was 1.

Why is that so useful?
Consider 2^{12345}. It can be written as $(2^{10})^{1234} \times 2^5$.
And since $2^{10} \equiv 1$, this is the same as $1^{1234} \times 2^5$.
Provided we know the residue of powers of 2 up to 2^{10}, we know the residue of all powers of 2.

Challenge Question 6 Solution

Find the remainder when $2^{57885161} - 1$ is divided by 11.

Using the results found above for residues modulo 11, we can think of $2^{57885161}$ as:

$$(2^{10})^{5788516} \times 2^1$$

Taking advantage of the known residues of 2^{10} and 2^1 gives:

$$1^{5788516} \times 2 \equiv 1 \times 2 \equiv 2$$

Therefore $2^{57885161} - 1 \equiv 2 - 1 \equiv 1 \ mod \ 11$

So the remainder when the 48th Mersenne prime is divided by 11 must be 1.