

# Modular Arithmetic Practice Sheet

Katherine E. Stange, CU Boulder

## Basic Practice

Compute the modular arithmetic quantities, modulo  $n$ , in such a way that your answer is an integer  $0 \leq k < n$ .

Do NOT use a calculator. Do these in your head.

1.  $4 + 1 \pmod{5}$
2.  $11 + 1 \pmod{6}$
3.  $12 + 17 \pmod{8}$
4.  $5 \cdot 3 \pmod{12}$
5.  $3^3 \pmod{8}$
6. Compare to the answer key at the end.

## What's wrong with this computation?

Let's suppose I want to compute  $6^{10} \pmod{7}$ .

Here's one way:

$$6^{10} \equiv (-1)^{10} \equiv 1 \pmod{7}.$$

Here's another way:

$$6^{10} \equiv 6^3 \equiv 36 \cdot 6 \equiv 1 \cdot 6 \equiv 6 \pmod{7}.$$

Only one of these can be correct. Which one is wrong and why?

See the answer key only after you have committed yourself fully to your answer.

## Addition and Multiplication Tables

Complete the addition and multiplication tables modulo 6. Compare to the answer key.

Addition Table Mod 6

	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Multiplication Table Mod 6

	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

## You'll need to reduce along the way

Here are some more modular arithmetic calculations. Again, you may NOT use a calculator. Instead, find ways to reduce the computation along the way, as demonstrated in the video. Find the most *efficient* approach: with a little cleverness, you should get to where you can do it in your head.

1.  $10040 + 10101 \pmod{2}$
2.  $123451 + 1987891 \pmod{10}$
3.  $131235321 \cdot 22 \pmod{11}$
4.  $(100 + 201 + 334) \cdot (997^3) \pmod{3}$
5.  $33335^8 \pmod{3}$
6. Compare to the answer key.

## Answer Key

### Basic Practice

0, 0, 5, 3, 3

### What's wrong with this computation?

In the second computation, the exponent is reduced from 10 to 3 because these are equivalent modulo 7. However, only *summands* and *factors* can be reduced, i.e. you can reduce numbers that are part of a sum or part of a product. But in an exponent, such reductions aren't allowed. The exponents are what they are (as integers). In the "Modular Arithmetic: User's Manual" video, we've only stated that you can reduce summands and factors. In the "Modular Arithmetic: Under the Hood" video, we will prove it. This example is a proof that you can't, in general, reduce the exponents with respect to the modulus.

### Addition and Multiplication Tables

Mod 6

	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

Mod 6

	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

### You'll need to reduce along the way

1, 2, 0, 2, 1