

# HW03

Sam Ly

September 25, 2025

**Total Points: 20**

## Required Exercise 1 [2]

1. Type `\(726 \equiv 23 \pmod{19}\)` to get  $726 \equiv 23 \pmod{19}$ .
2. Prove or disprove that  $726 \equiv 23 \pmod{19}$ .

*Proof.* We start by stating the definition.  $726 \equiv 23 \pmod{19}$  is the same as saying  $19 \mid (726 - 23)$ . Simplifying the expression, we get  $19 \mid (703)$ .

We see that  $19 \times 37 = 703$ . Therefore,  $726 \equiv 23 \pmod{19}$ . □

## Required Exercise 2 [4]

Suppose  $a \equiv a' \pmod{m}$  and  $b \equiv b' \pmod{m}$ . Prove the following:

1.  $a + b \equiv a' + b' \pmod{m}$ .

*Proof.* We begin with by defining  $a \equiv a' \pmod{m}$  as  $m \mid (a - a')$ . Similarly,  $m \mid (b - b')$ .

Following from these definitions, we write:

$$a - a' = m \times k_1 \tag{1}$$

$$b - b' = m \times k_2 \tag{2}$$

We can add equations 1 and 2 together to get  $a + b - a' - b' = m \times k_1 + m \times k_2$ .

With some factoring, we get  $(a + b) - (a' + b') = m(k_1 + k_2)$ .

By definition, we find that  $m \mid (a + b) - (a' + b')$ , and thus  $a + b \equiv a' + b' \pmod{m}$ . □

2.  $a - b \equiv a' - b' \pmod{m}$ .

*Proof.* Following from Proof 1, we can instead subtract equation 1 and 2 to get  $a - b - a' + b' = m \times k_1 - m \times k_2$ .

With some factoring, we get  $(a - b) - (a' - b') = m(k_1 - k_2)$ .

By definition, we find that  $m \mid (a - b) - (a' - b')$ , and thus  $a - b \equiv a' - b' \pmod{m}$ . □

3.  $a \times b \equiv a' \times b' \pmod{m}$ .

Following from equation 1, we get

$$a = a' + m \times k_1. \quad (3)$$

Similarly, from equation 2, we get

$$b = b' + m \times k_2. \quad (4)$$

By multiplying equations 3 and 4, we get  $a \times b = (a' + m \times k_1)(b' + m \times k_2)$ .

From now on, I will omit the  $\times$  symbol.

By distributing, we get

$$ab = a'b' + a'mk_2 + b'mk_1 + m^2k_1k_2.$$

We can factor out  $m$  to find

$$ab = a'b' + m(a'k_2 + b'k_1 + mk_1k_2).$$

We can subtract  $a'b'$  from both sides to find

$$ab - a'b' = m(a'k_2 + b'k_1 + mk_1k_2).$$

By definition, we see that  $m \mid (ab - a'b')$ , and, by extension,  $ab \equiv a'b' \pmod{m}$ .

## Required Exercise 3 [4]

**Problem 8.2** Give two reasons why ' $f : \mathbb{R} \rightarrow \mathbb{R}$  where  $f(x) = \pm\sqrt{x}$ ' is not a function.

1. The first reason that  $f$  is not a function is because of an invalid domain. The function *should* map all reals (domain) to a subset of the reals (codomain), but negative values actually map to imaginary numbers.
2. The second reason that  $f$  is not a function is because of the "non-unique" output. One of the requirements for a function is that one value from the domain maps to one and only one value from the codomain. However,  $f$  maps a single value  $x$  to two values due to the  $\pm$ .

## Choice Exercise 4 [4]

2. Show that every positive integer is a sum of one or more numbers of the form  $2^r 3^s$ , where  $r$  and  $s$  are nonnegative integers and no summand divides another. (For example,  $23 = 9 + 8 + 6$ ).

*Proof.* We begin by showing that such summations exist for small  $n$ . This will act as a base case for an inductive step later.

$n = 0$  Trivially true.

$n = 1$   $1 = 2^0 3^0$ .

Now, we create the inductive hypothesis that all nonnegative integers strictly less than  $n$  have such summation.

If  $n$  is even, we can construct a valid summation by noticing that, from our inductive hypothesis,  $\frac{n}{2}$  has a valid summation  $\sum_{i=1}^k 2^{r_i} 3^{s_i}$ . Since none of these summands divide any other summand, multiplying all summands by 2 also creates a set of summands such that no summand divides another.

If  $n$  is odd, we can also construct a valid summation by picking a value  $3^t$  that is the biggest power of 3 that is less than or equal to  $n$ . Our proposition is trivially true if  $n = 3^t$ . Otherwise, we must find a value  $m = n - 3^t$ .

Since  $n$  and  $3^t$  are both odd,  $m$  must be even. Also notice that  $m < n$ . Thus, there must exist a valid summation  $m = \sum_{j=1}^k 2^{r_j} 3^{s_j}$  where all  $r_j \geq 1$ .

Since all summands of  $m$  are even,  $3^t$  can not be divisible by any of the summands of  $m$ . Also, since  $r_j \geq 1$ , there must not be any summand where  $s_j \geq t$  because if such summand existed, we would find at least a value of  $n = 3^t + 2(3^t) = 3^{t+1}$ . This is a contradiction, since we defined  $3^t$  as the largest power of 3 less than or equal to  $n$ .

Thus,  $n = \sum 2^r 3^s$  where no summand divides another for all nonnegative integers  $n$ . □

## Choice Exercise 8 [6]

Look up the Tower of Hanoi puzzle. Prove that given a stack of  $n$  disks, you can solve the puzzle in  $2^n - 1$  moves.

*Proof.* We begin by defining the Tower of Hanoi problem.

In this problem, we begin with a stack of  $n$  disks. The disks are ordered from largest at the bottom to smallest at the top. We are also given 3 ‘spots’ to place our disks under one condition: that we never place a larger disk on top of a smaller disk.

Following these rules, what is the minimum number of moves required to move the entire pile to a new ‘spot’?

We define the function  $f : \mathbb{N} \rightarrow \mathbb{N}$  such that it maps the starting stack height  $n$  to the minimum number of moves required to move the entire pile  $f(n)$ .

Before immediately proving that  $f(n) = 2^n - 1$ , it is more intuitive to first define  $f$  as a recurrence relation, then prove that the recurrence relation is equal to  $2^n - 1$ .

We notice that moving the entire pile of  $n$  disks essentially requires 3 ‘phases’:

1. Moving the top  $n - 1$  disks onto a single pile.
2. Moving the  $n$ th disk to another vacant spot.
3. Moving the top  $n - 1$  disks onto the new spot.

Thus, we know that  $f(n) = f(n - 1) + 1 + f(n - 1) = 1 + 2f(n - 1)$ , where  $f(1) = 1$ . We can then prove  $f(n) = 2^n - 1$  using induction.

We begin with our base cases:

$n$	$f(n)$
1	$1 = 2^1 - 1$
2	$3 = 2^2 - 1$
3	$7 = 2^3 - 1$

Now, we assume that  $f(k) = 2^k - 1$  for all  $1 \leq k \leq n$ .

We see that

$$\begin{aligned} f(k+1) &= 1 + 2f(k) \\ f(k+1) &= 1 + 2(2^k - 1) \\ f(k+1) &= 2^{k+1} - 1. \end{aligned}$$

Thus,  $f(n) = 2^n - 1$ . □