

WEEK 3 WORKSHOP
MATH2301, SEMESTER 2, 2025

1. MODULAR ARITHMETIC

1.1. **Problem.** Find all $x \in \mathbf{Z}/8\mathbf{Z}$ such that $[2]x + [4] = [0]$.

Solution.

(1) By checking all 8 possibilities, we find that $x = [2]$ and $x = [6]$.

(2) Suppose $x = [n]$ where n is an integer. Then $[2]x + [4] = [2n + 4]$. So we need 8 to divide $2n + 4$. So we need 4 to divide $n + 2$. This means $n = -2 \pmod{4}$, leading to the solutions $n = 2, 6, 10, -2, -6, -10, \dots$. But modulo 8, there are only 2 distinct solutions: $[2]$ and $[6]$.

1.2. **Problem.** Find the last digit of 3^{101} .

Hint. This is equivalent to finding 3^{101} modulo 10. Calculate a few small powers, say $3^0, 3^1, 3^2, 3^3, \dots$ modulo 10 and see if you can spot a pattern.

Solution. This is an example where computing modulo 10 is much easier than computing with integers. We start by computing the first few powers:

$$[3^0] = [1] \quad [3^1] = [3] \quad [3^2] = [9] \quad [3^3] = [7] \quad [3^4] = [1]$$

. From this, point on wards the cycle must repeat (why?) In particular, every fourth power gives us $[1]$. Sure enough,

$$[3^8] = [3^4] \cdot [3^4] = [1] \cdot [1] = [1],$$

and

$$[3^{12}] = [3^8] \cdot [3^4] = [1] \cdot [1] = [1],$$

and so on. Continuing in this way, we get $[3^{100}] = [1]$ and hence $[3^{101}] = [3]$. So the last digit of $[3^{100}]$ is 3.

1.3. **Problem.** This is a somewhat open ended problem, so please attempt the other problems and come back to it. The quadratic formula says that the solutions to

$$ax^2 + bx + c = 0$$

are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Suppose $a, b, c \in \mathbf{Z}/n\mathbf{Z}$ and we are looking for x also in $\mathbf{Z}/n\mathbf{Z}$. Does the quadratic formula make sense? If it makes sense, is it correct?

Solution. There are multiple problems with the formula modulo n :

(1) Dividing by $2a$ may not make sense. That is, $2a$ may not have a multiplicative inverse in $\mathbf{Z}/n\mathbf{Z}$.

(2) A square root of $b^2 - 4ac$ may not exist.

(3) There may be multiple square-roots, so it is unclear which one the symbol $\sqrt{b^2 - 4ac}$ represents.

But it is possible to overcome these limitations and make sense of the formula.

Theorem. Consider the equation

$$ax^2 + bx + c = 0,$$

where $a, b, c \in \mathbf{Z}/n\mathbf{Z}$. Assume that $2a$ has a multiplicative inverse modulo n . If $b^2 - 4ac$ is not a square in $\mathbf{Z}/n\mathbf{Z}$, then there are no solutions to this equation. If $b^2 - 4ac$ is a square, then all the solutions are given by

$$x = \frac{-b + \delta}{2a},$$

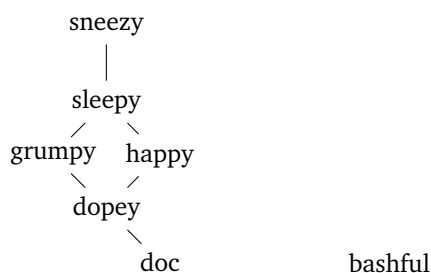
where δ is any square root of $b^2 - 4ac$.

The theorem is true in $\mathbf{Z}/n\mathbf{Z}$ for the same reason it is true in more familiar number systems like \mathbf{Q} or \mathbf{R} . This is going a bit deeper than the course requires, but I will be happy to explain in person.

2. THE SEVEN-DWARVES POSET

2.1. Problem. Consider the set of the names of the dwarfs from Snow White: {Bashful, Doc, Dopey, Grumpy, Happy, Sleepy, Sneezzy}. Consider a partial order relation on this set, where $x \leq y$ if the length of x is less than or equal to the length of y , and if x comes before y in alphabetical order. Draw the Hasse diagram of this partial order relation. Is it a total order?

Solution. The Hasse diagram looks as follows.



This is not a total order—Doc and Bashful are not related, for example.

2.2. Problem. Does the poset have maximum or minimum elements? Find all minimal and maximal elements.

Solution. No, it has neither maximum nor minimum elements.

Sneezzy and bashful are maximal. Doc and bashful are minimal. Note that bashful is both maximal and minimal.

3. THE SUBSET POSET AND THE HYPERCUBE

Let $A = \{1, \dots, n\}$ and let $S = \text{Pow}(A)$. Instead of writing a subset $T \subset A$ by listing its elements, write it as an n -tuple of 0's and 1's so that the i -th place is 1 if $i \in T$ and 0 if $i \notin T$. For example, if $n = 3$, then the subset $\{1, 3\} \subset \{1, 2, 3\}$ is encoded by $(1, 0, 1)$.

3.1. Problem. Describe the subset relation in terms of the corresponding n -tuples. That is, if $T \subset T'$, what can you say about the n -tuples that encode T and T' ?

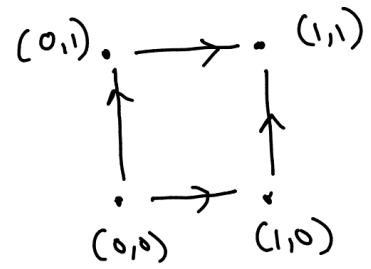
Solution. If $T_1 \subset T_2$, then $i \in T$ implies $i \in T'$. So if there is a 1 in the i -th place for T , then there must be a 1 in the i -th place for T' . So if (t_1, \dots, t_n) is the tuple encoding T and (t'_1, \dots, t'_n) is the tuple encoding T' , then for all $i = 1, \dots, n$, we must have $t_i \leq t'_i$.

3.2. Problem. Describe when an n -tuple is an immediate successor of another n -tuple under this relation.

Solution. The tuple t' is an immediate successor of the tuple t if and only if t' has exactly one additional 1.

3.3. Problem. Take $n = 3$. Draw the Hasse diagram in 3 dimensions by plotting the triples at the corresponding point in \mathbf{R}^3 . So $(0, 0, 0)$ is at the origin and $(1, 1, 1)$ is at the point $(1, 1, 1)$. Draw the arrows representing immediate successors (we can not drop the arrowheads because there is no clear “up” or “down”). What shape do you get? As a warmup, do the exercise with $n = 2$ or even $n = 1$. What shape would you get in higher dimensions?

Solution. For $n = 1$ we get the vertices 0 and 1 joined by an edge $0 \rightarrow 1$. For $n = 2$, we get the square



For $n = 3$, we get the unit cube:



In higher dimension, we get the unit hypercube.