Sets and Functions

Andrew D Smith
University College Dublin

7 October 2023

Three Functional Equations

Problem Statements

1. Is there a function $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(f(z)) = z + 2023$ for all $z \in \mathbb{Z}$?

2. Is there a function $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(f(z)) = z + 2024$ for all $z \in \mathbb{Z}$?

3. For a fixed integer k, is there a function $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(f(z)) = z + k$ for all $z \in \mathbb{Z}$?

Based on Q4 from 1987 International Maths Olympiad (La Habana, Cuba)

Problem 2 is Easy but Problem 1 is Hard

It is easy to find a solution to $f(f(z)) = z + 2024$. We can set $f(z) = z + 1012$.

This trick does not work for question 1, because 2023 is an odd number. The function $f(z) = z + 1011\frac{1}{2}$ is not a solution because of the requirement that $f : \mathbb{Z} \to \mathbb{Z}$, that is, f maps the integers to the integers.

There is no Solution with $k = 1$

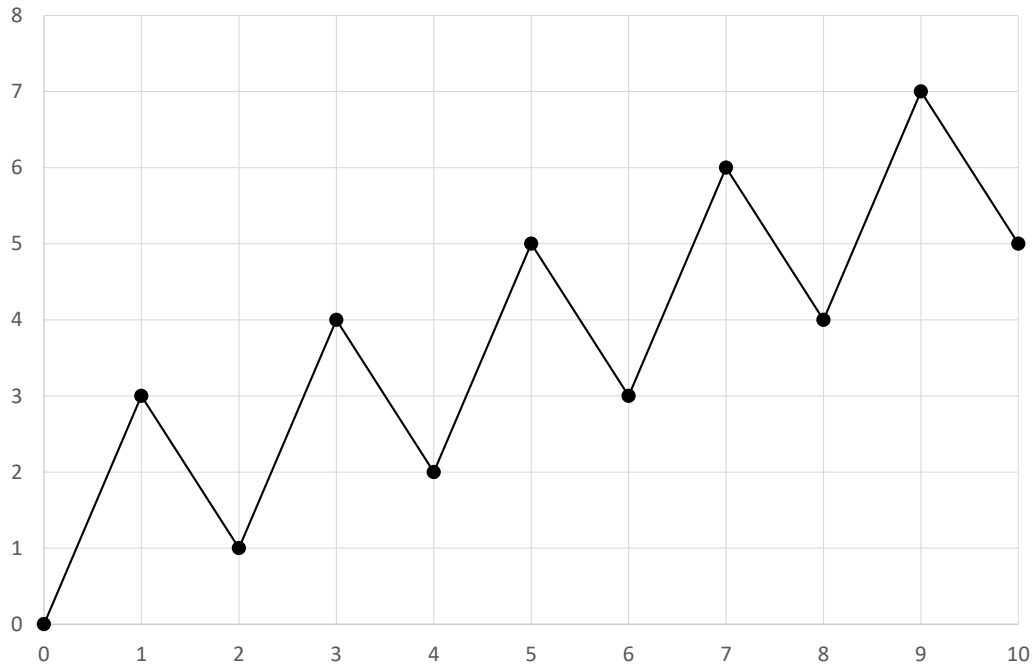
Suppose there is a function $f : \mathbb{Z} \to \mathbb{Z}$ with $f(f(x)) = x + 1$ and derive a contradiction.

Consider the sequence 0, $f(0)$, $f(f(0))$, $f(f(f(0)))$ and so on, starting at zero and applying f repeatedly. This set is called the *forward orbit* of 0 under f.

From the functional equation, this sequence must look like 0, a, 1, $a+1$, 2, $a+2$ etc.

We cannot have $f(0) = 0$ because that would contradict $f(f(0)) = 0$. Likewise, we cannot have $f(0) = 1$ because the functional equation would force $f(1) = f(f(0)) = 1$, contradicting $f(f(1)) = 2$.

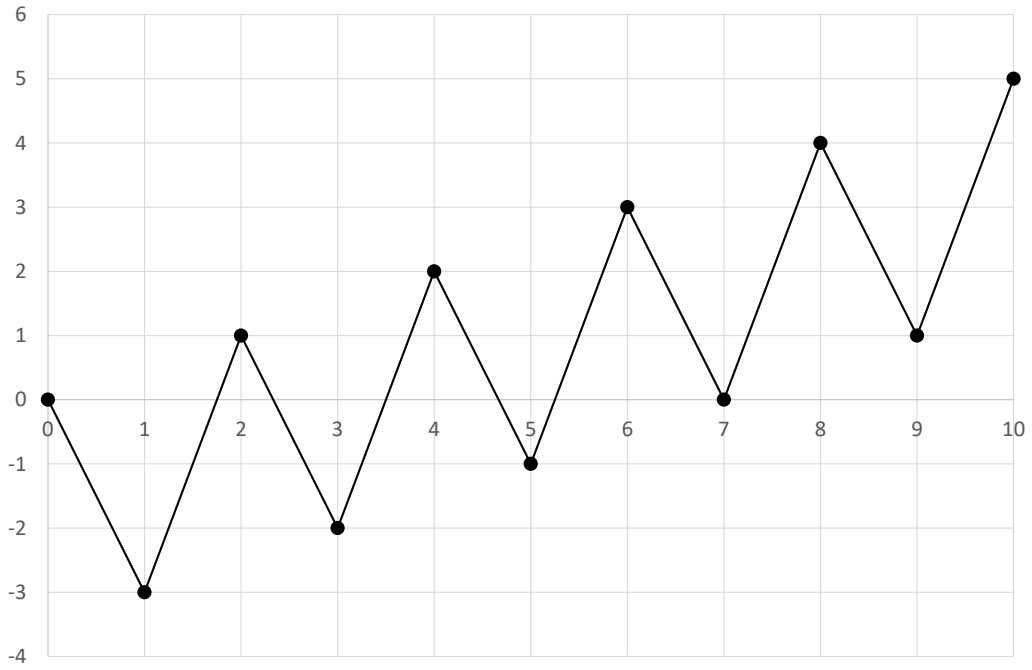
To illustrate the case $f(0) > 1$ let us suppose $f(0) = 3$. Then the forward orbit of 0 must appear as below:



The number 3 appears twice in the orbit; the first time we have

$f(3) = 2$ and the second time $f(3) = 6$; a contradiction. We call this the *clash* argument for this problem.

To illustrate the case $f(0) < 0$, suppose $f(0) = -3$. Then the forward orbit of 0 must appear as below:



Here we have a contradiction because 0 appears twice (another clash), implying $f(0) = -3$ and $f(0) = 7$ which cannot both be true as f is a function.

Exercise: Develop these observations based on $a = \pm 3$ into a general contradiction for all values of $a \in \mathbb{Z}$.

Hints for a Solution: Inductively show that for $k \in \mathbb{Z}_0^+$:

$$f^{2k}(0) = k$$
$$f^{2k+1}(0) = k + a$$

In the case $a > 1$, we have:

$$f(0) = a = f^{2a}(0)$$

Taking f of each side we have:

$$1 = f^2(0) = f^{2a+1}(0) = 2a$$

This is a contradiction. A similar argument applies when $a < 0$.

Sets and Set Operations

A *set* is a collection of *elements*. When we list the elements to define a set, we enclose them in curly brackets.

Finite Sets

P	Provinces of Ireland	{ Connacht, Leinster, Munster, Ulster }
L	Counties of Leinster	{ Carlow, Dublin, Kildare, Kilkenny, Laois, Longford, Louth, Meath, Offally, Westmeath, Wexford, Wicklow }
U	Counties of Ulster	{ Antrim, Armagh, Cavan, Donegal Down, Fermanagh, Derry, Monaghan, Tyrone }

The number of elements in a finite set (also called its *cardinality*) is denoted by vertical bars, so $|P| = 4$, $|L| = 12$, $|U| = 9$.

.

Elements

The order of elements in a set does not matter. Two sets are equal if they have exactly the same elements.

We use the symbol $\in$ for elements so that, for example Carlow $\in L$ but Carlow $\notin U$. We sometimes write this in reverse order, meaning *contains*, so $L \ni$ Carlow.

It is OK for one set to be an element of another set, for example we can think of the provinces Connacht, Leinster, Munster, Ulster each to be a set of counties, and also each of which is an element of P.

It is not OK for a set to be a member of itself. We have to rule this out to dodge Russell's paradox: consider the set of all sets that are not members of themselves. Is that set a member of itself, or not?

Unions, Intersections, Subsets

For two sets L and U, the union $L \cup U$ means all elements that are in one set or the other (or both). Repeated elements are not counted twice. If L is the counties of Leinster and U is the counties of Ulster than $L \cup U$ is all the counties in Leinster or Ulster.

For two sets L and U, the intersection, $L \cap U$ is the set of

elements that are in both L and U. With our example, $L \cap U = \emptyset$, the empty set, because there are no counties in both Leinster and Ulster. If two sets have no common elements, we say they are *disjoint*. A union of two or more sets is a disjoint union if the intersection of any two sets is empty.

For general finite sets A and B we have:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

For a disjoint union, $|A \cap B| = 0$ and so the cardinality of the union is the union of the cardinalities.

A set A is a *subset* of B if every element of A is also an element of B and we write $A \subseteq B$. The empty set is a subset of every set.

A set A is a *proper* subset of B, written $A \subset B$ if $A \subseteq B$ but $A \neq B$, ie there is at least one element of B that is not an element of A. The empty set $\emptyset$ is a proper subset of any non-empty set.

For two sets A and B, the *set difference* $A \backslash B$ is all elements of A that are not in B.

Sets of Numbers

Addition and multiplication do not have to be defined for elements of a set. There is no mathematical meaning to Carlow $\times$ Dublin, and we do not have to invent one to have a set of Counties in Leinster. But if our set is a set of numbers then we can define addition and multiplication.

Here are some examples of sets of numbers:

Positive integers	$\mathbb{Z}^+$
Integers	$\mathbb{Z}$
Rational numbers	$\mathbb{Q}$
Real numbers	$\mathbb{R}$
Irrational numbers	$\mathbb{R}\backslash\mathbb{Q}$
Complex numbers	$\mathbb{C}$

We write sub-intervals of the real line with square brackets or round brackets indicating whether the endpoints are included. Assuming $a \leq b$, we write:

$$\begin{aligned}
[a,b] &= \{x \in \mathbb{R} : a \leq x \leq b\} \quad \text{closed interval} \\
[a,b) &= \{x \in \mathbb{R} : a \leq x < b\} \\
(a,b] &= \{x \in \mathbb{R} : a < x \leq b\} \\
(a,b) &= \{x \in \mathbb{R} : a < x < b\} \quad \text{open interval}
\end{aligned}$$

Functions

Function Definitions

Let A and B be two sets. A *function* f is a map such that every element $a \in A$ is associated with an image $f(a) \in B$.

The set A is called the *domain* of the function and B is called the *co-domain* of the function.

Two functions f and g are equal if they have the same domain, the same co-domain and their values are the same for all elements of the domain.

Example: The functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to [0, \infty)$ defined by $f(x) = x^2$ and $g(x) = x^2$ are different functions because the co-domains are different.

Example: The map $y : [0, \infty) \to \mathbb{R}$ given by $y = \pm\sqrt{x}$ is not a function, because each value of $x > 0$ gives rise to two (not one) values of x.

Identity, Indicator, Inclusion and Restrictions

The emphidentity function $\iota : A \to A$ is the the function that maps every element of A to itself. We also use the notation ι for inclusion maps (see below).

If $A \supseteq C$, then the *indicator function* of C, written $1_C : A \to \{0, 1\}$ is a function defined by:

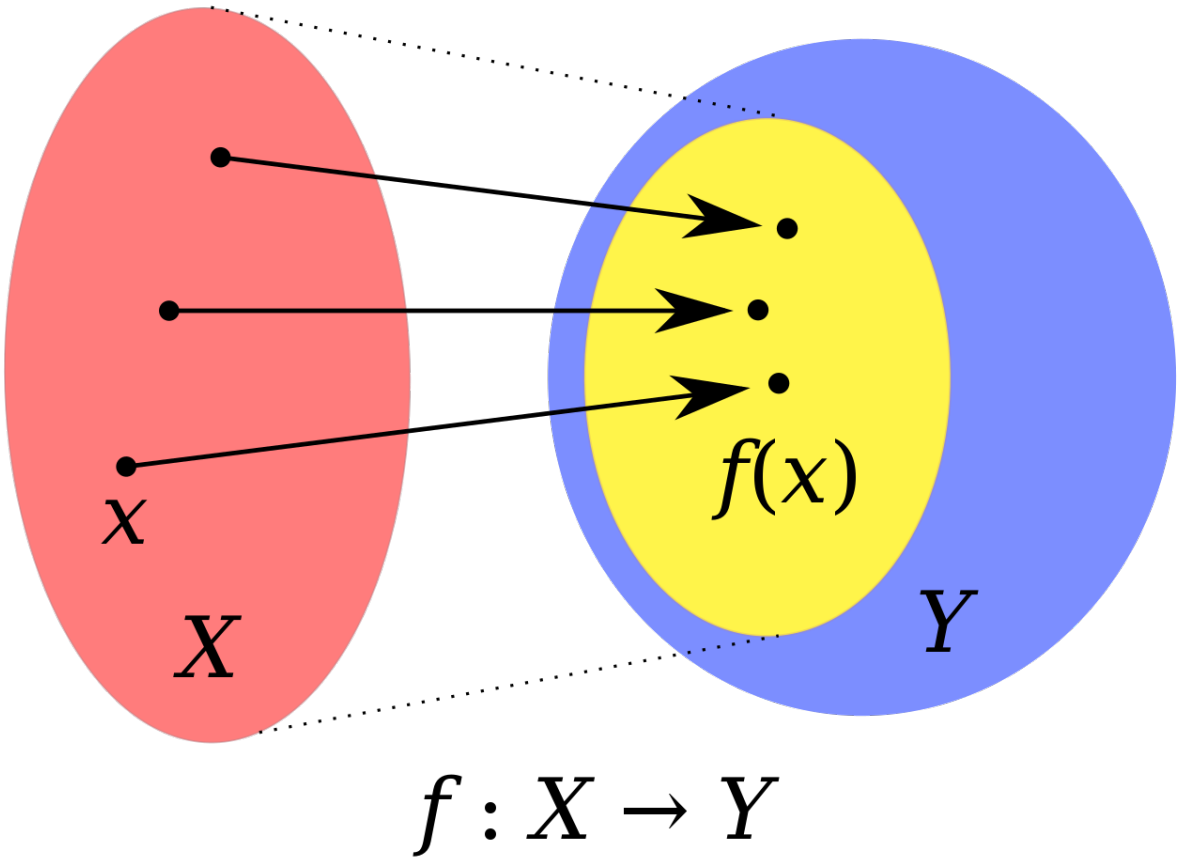
$$1_C(x) = \begin{cases} 1 & x \in C \\ 0 & x \notin C \end{cases}$$

If $C \subseteq A$ then there is an *inclusion map* $\iota : C \to A$ defined by $\iota(c) = c$ for $c \in \mathbb{C}$. Sometimes we write $\iota : C \hookrightarrow A$, where the hooked arrow reminds is this is an inclusion.

If $C \subset A$ then any function $f : A \to B$ induces a function $f \restriction_C : C \to B$ which agrees with f for elements of C. In that case, $f \restriction_C$ is said to be a *restriction* of f, while f is said to be an *extension* of $f \restriction_C$.

Surjection, Injection

The *image* of the function, written $f(A)$ is the set $\{f(a) : a \in A\}$. If $f : A \to B$ and $f(A) = B$ then we say f is *surjective*, because it covers all the elements of B (from French: *sur* = on).



Mathematicians sometimes talk about the *range* of a function. That might mean the co-domain of the function, or the image of the function. If the function is not surjective, these are different concepts, so it is wise to avoid the term *range*.

We say a function $f : A \to B$ is *injective* if $f(x) = f(y) \implies x = y$, so that no two elements of A map onto the same element of B.

A function f is *bijective* if it is surjective and injective.

Exercise: Suppose $f : \mathbb{Z} \to \mathbb{Z}$ and, for some fixed $k \in \mathbb{Z}$ we have $f(f(z)) = z + k$ for all $z \in \mathbb{Z}$. Can we deduce that f is surjective or injective?

Solution: The function f is surjective because for any $z \in \mathbb{Z}$ we have $f(f(z - k)) = z$ so that f maps $f(z - k)$ onto z.
The function f is injective because

$$f(x) = f(y) \implies f(f(x)) = f(f(y)) \implies x+k = y+k \implies x = y$$

If follows that any such f must be bijective, as it is injective and surjective.

Composition

Let A, B, C be sets and suppose we have functions $f : A \to B$ and $g : B \to C$.

The function composition $g \circ f : A \to C$ is defined by:

$$g \circ f(x) = g(f(x)); x \in A$$

For composition to make sense (to be *well-defined*), it is necessary that the domain of g is the co-domain of f. Unlike addition and (for members of a field) multiplication, the composition of functions is not commutative. It is not that case that $f \circ g = g \circ f$. Indeed, it is possible that $f \circ g$ is well-defined but $g \circ f$ is not.

Exercise: Why is composition of functions associative?

Exercise: Is the composition of two injections an injection? Is the composition of two surjections a surjection? Justify your answers.

Exercise: Construct an example of two functions f and g where $f \circ g$ and $g \circ f$ are both well-defined but are not the same function.

Left and Right Inverses

Suppose $f : A \to B$. We want to define what we mean by applying f in reverse.

Suppose we can find a function g that answers the question: given $f(a)$ determine a unique value of $a \in A$. For this to be possible, f must be injective. Such a g is called a *left inverse* of f. We need to define g on all of B but we do not care about the values for $B \backslash f(A)$. Equivalently, g is a left inverse of f if $g \circ f : A \to A$ is the identity function.

Suppose instead we can find a function g that answers the question: given arbitrary $binB$ find any value of $a \in A$ so that $f(a) = b$. This can only work if f is a surjection. Then we say g is a *right inverse* of f. In symbols, this means that $f \circ g : B \to B$ is the identity function.

We can see that g is a right inverse of f if, and only if, f is a right inverse of g.

We say that g is the *inverse* of f if it is a right inverse and a left inverse. In that case, we write $g = f^{-1}$.

Exercise: Can you construct an example of f and g where g is a right inverse of f but not a left inverse? Hint: think of an example where $|B| < |A|$.

A function $f : A \to B$ has an *inverse*, $f^{-1} : B \to A$ if and only if f is bijective.

A function $f : A \to a$ has a *fixed point* if for some $a \in A$ we have $f(a) = a$. Every point is a fixed point of the identity function.

A function $f : A \to A$ is *self-inverse* if $f(f(x)) = x$ for all $x \in A$. An example of a self-inverse function in a number set is $f(x) = -x$.

Example: The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is neither bijective nor surjective, so it has neither a right inverse nor a left inverse.

Iterated Composition and Orbits

If $f : A \to A$ and $n \in \mathbb{Z}^+$ then we can define the iterated composition f^n which means applying f, n times.

By convention, f^0 means the identity.

The *forward orbit* of an element $a \in A$ is the set $\{f^k(a) : k \in \mathbb{Z}_0^+\}$. The forward orbit is not necessarily an infinite set as the iterates of f may loop into a cycle.

If f is bijective than we can also define f^{-1} and so f^n for $n \in \mathbb{Z}^-$.

For bijective f, the *backward orbit* of a is the set $\{f^k(a) : k \in \mathbb{Z}_0^-\}$.

The *orbit* of a is the union of the forward and backward orbits, that is $\{f^k(a) : k \in \mathbb{Z}\}$.

If a function is self-inverse then all its orbits must either be singletons (fixed points) or pairs of two elements. For example, the orbits of the function $f(x) = -x$ are the sets $\pm x$, all of which have two elements except for ± 0 which has a single element.

Nasty and Nice Functions

Mathematicians might classify some functions as *nice*, meaning they are well-behaved in some sense.

For example, a function $f : \mathbb{R} \to \mathbb{R}$ might be *continuous*, or it might not. A continuous function, intuitively, is one whose graph we can draw without taking the pencil off the paper.

A function defined by different formulas on different intervals is said to be defined *piecewise*. Consider for example the absolute value function defined as:

$$|x| = \begin{cases} -x & x \leq 0 \\ x & x \geq 0 \end{cases}$$

If a piecewise function is multiply defined at interval endpoints, then those definitions should agree (as in the example above). This is an example of a (single) continuous function defined piecewise, not an example of two functions.

$f(x) = x^2$ and $g(x) = |x|$ are continuous functions. An example of a discontinuous function is the *Heaviside* function $H(x)$

defined by:

$$H(x) = \mathbf{1}_{[0,\infty)}(x) = \begin{cases} 0 & x < 0 \\ 1 & x \geq 0 \end{cases}$$

There are nasty functions that are discontinuous everywhere, such as the indicator function of the rational numbers as a subset of the real numbers.

Products and Powers of Sets

Cartesian Products

Let A and B be two sets. Then the *Cartesian product*, written $A \times B$ is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.

Explain why:

$$|A \times B| = |A| \times |B|$$

We write A^2 for $A \times A$ and A^3 for $A \times A \times A$ and so on.

Graph of a Function

The *graph* of a function $f : A \to B$ is the subset of $A \times B$ defined by:

$$\{(a, b) \in A \times B : b = f(a)\}$$

Sets of Functions

We write A^B for the set of all functions $f : B \to A$. This is consistent with the notation A^2, A^3 etc. by identifying 2 with any set containing 2 elements and so on.

Explain why

$$\left|A^B\right| = |A|^{|B|}$$

Equivalence Relations and Quotient Sets

Equivalence Relation Definition

An *equivalence relation*, written $\equiv$ (or sometimes $\sim$), is a binary relation between elements of a set A such that:

Reflexive	$a \equiv a$
Symmetric	If $a \equiv b$ then $b \equiv a$
Transitive	If $a \equiv b$ and $b \equiv c$ then $a \equiv c$

For any element $a \in A$, the equivalence class containing a, written $[a]$, is the set:

$$[a] = \{b \in A : b \equiv a\}$$

Geometric Examples

Consider the set of all triangles in the plane.

Congruence as in equivalence relation. Congruent triangles are triangles with the same edge lengths. The set of all triangles congruent to a particular triangle form an equivalence class.

So is similarity. Similar triangles are triangles with the same angles.

Last-Digit Arithmetic

For two non-negative integers, say that $a \equiv b$ if the final digits of a and b are the same.

There are ten equivalence classes, one for each possible final digit (including 0).

Modular Arithmetic

Let $n \in \mathbb{Z}^+$.

We say $a \equiv b \pmod{n}$ if $n \mid (a - b)$.

The set of equivalence classes is called the *integers mod* n and is written $\mathbb{Z}_n$. This is a finite set with $|\mathbb{Z}_n| = n$.

Equivalence Classes from Iterated Bijections

Let A be a set and left $f : A \to A$ be a bijection.

Say that $a \equiv b$ if $b = f^k(a)$ for some $k \in \mathbb{Z}$.

The equivalence classes are the orbits under f.

Sets of Equivalence Classes

Suppose A is a set with an equivalence relation $\equiv$.

Define the quotient set $A/\equiv$ to be the set of equivalence classes. We call this set A modulo $\equiv$. We have seen examples: integers mod n, orbits under a bijection, triangles regarded as the same if congruent.

Cardinal Numbers

Consider a collection of sets.

Say that two sets A and B are equivalent if there is bijection from A to B.

Exercise: verify that the existence of a bijection is an equivalence relation on a class of sets. To prove transitivity, use function composition.

Exercise: Let A and B be finite sets. Show that there exists a bjiection from A to B if and only if A and B have the same number of elements.

The equivalence classes of sets under bijection existence are called the *cardinal numbers*. These include the natural numbers (for finite sets), but also the cardinalities of infinite sets.

For example, $\aleph_0$ is the cardinality of the natural numbers, which is also the cardinality of the integers, and of the rationals, and of any rational interval.

Exercise: Can you construct a bijection from $\mathbb{Z}^+$ to the interval $[0, 1]$? Hint: think of Farey sequences.

We use $\aleph_1$ for the cardinality of the reals, which is also the cardinality of any real interval and of the complex numbers.

Functions from Equivalence Classes

Suppose we have a function $f : A \to B$ and that $\equiv$ is an equivalence relation on A.

Suppose also that $f(x) = f(y)$ whenever $x \equiv y$. Then we can define an induced function:

$$\overset{\equiv}{f}\colon A/\equiv \to B$$

by

$$\overset{\equiv}{f}\,[a] = f(a)$$

Example: Area of triangles modulo equivalence.

Example: Largest angle of triangles modulo similarity.

Non-example: Area of triangles modulo similarity.

Binary Operations for Equivalence Classes

We know that if we take two positive integers, one ending in 3 and the other ending in 6, then the sum must end in 9 and the product must end in 8.

We can define a new sort of addition and multiplication between the digits 0 to 9, based on the last digit. We call this *arithmetic modulo* 10. We can define $\mathbb{Z}_{10}$ as the set of last digits with that multiplication.

We can define modular arithmetic for a general number base $n \in \mathbb{Z}^+$.

Suppose that $a, b, c, d \in \mathbb{Z}$.

Suppose also $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$.

Explain why $a+b \equiv c+d \pmod{n}$ and $a \times b \equiv c \times d \pmod{n}$.

This allows us to define operators $+$ and $\times$ on $\mathbb{Z}_n$.

If n is composite, then there are $a, b \neq [0] \in \mathbb{Z}_n$ such that $a \times b = [0]$. Therefore $\mathbb{Z}_n$ is not a field. As a result, it lacks some important field properties. For example, over the set $\mathbb{Z}_{10}$, roots of the quadratic polynomial $x^2 - x$ represent numbers whose final digit is unchanged on squaring. The polynomial $x^2 - x$ has has 4 roots in $\mathbb{Z}_{10}$, namely [0], [1], [5] and [6].

Over a field, a quadratic polynomial could have at most 2 roots. For example if n is prime than the only roots of $x^2 - x = 0$ are [0] and [1], because (Euclid's lemma) if $p \mid x(x-1)$ then either $p \mid x$ or $p \mid x - 1$. Indeed, it turns out (not obvious) that $\mathbb{Z}_n$ is a field if and only if n is a prime number. However, not all finite fields arise in this way; we have already seen a field $\mathbb{F}_9$ which is not the same as the (non-field) $\mathbb{Z}_9$.

Back to Problem 3

Now let us try to solve the original functional equation $f(f(z)) = z + k$ for all $z \in \mathbb{Z}$, where $k \in \mathbb{Z}^+$.

Three-Fold Iteration

The key to constructing the clash argument was getting two sequences of integers, increasing 1 at a time, that had to clash at some point.

In general we get sequences increasing k at a time, as:

$$f(z+k) = f(f(f(z)) = f(z) + k$$

That implies inductively that for arbitrary $n \in \mathbb{Z}^+$:

$$f(z+nk) = f(z) + nk$$

As f is bijective, we can extend that equation to all $n \in \mathbb{Z}$.

Reduction to $\mathbb{Z}_k$

The equation $f(z+nk) = f(z)+nk$ implies that if $y \equiv z \pmod{k}$ then $f(y) \equiv f(z) \pmod{k}$, as y must have the form of $z + nk$.

This congruence means we can define a function $\overset{\equiv}{f}\colon \mathbb{Z}_k \to \mathbb{Z}_k$ by:

$$\overset{\equiv}{f}([z]) = [f(z)]$$

where $[x]$ is the equivalence class of $z \pmod{k}$. This will help because $\mathbb{Z}_k$ is a finite set, so we can use counting arguments on it.

This function $\overset{\equiv}{f}$ also has the property of being self-inverse, as $f(f(z)) = z + k \equiv z \pmod{k}$.

As $\overset{\equiv}{f}$ is self-inverse, all its orbits are either singletons or pairs.

Finding a Clash Argument when k is Odd

Now suppose k is odd. Then $\mathbb{Z}_k$ has an odd number of elements and is a disjoint union of orbits under $\overset{\equiv}{f}$. As $\overset{\equiv}{f}\colon \mathbb{Z}_k \to \mathbb{Z}_k$ is self-inverse, all its orbits are singletons or pairs.

Not all the orbits can be pairs because $\mathbb{Z}_k$ has an odd number of elements. So there is at least one fixed point, let's say $[w] \in \mathbb{Z}_k$ for which:

$$f(w) \equiv w \pmod{k}$$

Then we must be able to write $f(w) = w + ak$ for some specific a.

Now we are in a position to construct a clash argument. We have for any $n \in \mathbb{Z}$:

$$f(w + nk) = f(w) + nk = w + (n + a)k$$

for all n. So, replacing the general n by the specific a:

$$f(f(w)) = f(w + ak) = w + 2ak = w + k$$

This is the clash; as there is no integer a with $2a = 1$ we have the contradiction and so there is no such function f.

Remark: It is entirely feasible to show the impossibility of $f(f(z)) = z+2023$ without using the language of equivalence relations, congruence, quotient sets, self-inverse functions and orbits. But all known solutions to this problem involve either building on these concepts, or reinventing them from scratch.

Glossary

After today's lectures you should be able to define and apply the following terms:

- Solution set
- Polynomial, monic polynomial
- Associative operation
- Commutative operation
- Distributive law
- Field
- Integers, Rationals, Reals
- Farey sequence
- Rational root, irrational root
- Complex numbers
- Primes, composites, factors
- Unique factorisation
- Greatest common divisor
- Relatively prime
- Linear equation
- Quadratic equation
- Intermediate value
- Fund. Theorem of Algebra
- Algebraic completeness
- Domain, co-domain
- Unions, intersections
- Cardinality, disjoint
- Open and closed intervals
- Injection, surjection, bijection
- Function composition
- Left and Right inverses
- Product sets, graphs
- Forward and backward orbits
- Fixed point
- Equivalence relation
- Equivalence class
- Quotient set
- Integers $\mathbb{Z}_n$ mod n
- Cardinal number