Ma 6 PSET 6

Victoria Liu

November 24, 2020

Problem 1

Proof. We want to show that any isomorphism f from the group $\mathbb{Q}$ under addition to itself must be of the form $f = cx$. Let us set $f(1) = c$, so that $f(n) = cn$ by virtue of iterated addition. Then, let's say for two integers n and m:

$$f\left(\frac{n}{m}\right) = a \tag{1}$$

Then, if we do iterated addition over $\frac{n}{m}$ m times, then we get:

$$f\left(\frac{nm}{m}\right) = am \tag{2}$$

$$f(n) = am \tag{3}$$

Plugging in $f(n) = cn$, we get:

$$cn = am \tag{4}$$

$$a = c\frac{n}{m} \tag{5}$$

$$f\left(\frac{n}{m}\right) = c\frac{n}{m} \tag{6}$$

From the last equality, we see that the form of f must take the form $f = cx$ for all $x \in \mathbb{Q}$. We can further prove that $f = cx$ actually works as an isomorphism from $\mathbb{Q}$ to itself under addition. Let $\alpha \in \mathbb{Q}$ and $\beta \in \mathbb{Q}$, and we write down the definition of the isomorphism:

$$f(\alpha + \beta) \stackrel{?}{=} f(\alpha) + f(\beta) \tag{7}$$

$$c \cdot (\alpha + \beta) \stackrel{?}{=} c \cdot \alpha + c \cdot \beta \tag{8}$$

This is true by the distributive property of multiplication over addition, so $f = cx$ is indeed an isomorphism from $\mathbb{Q}$ to itself under addition. Interestingly, our initial assumption that $f(1) = c$ implies that c must be a rational number as well, since we are mapping rational numbers to

rational numbers. However, since the distributive property works on all real numbers, c can actually be any real number. The problem did not define any restrictions for c, so we are good. For further proof of this, we can also see that $f(0) = 0$ for all c, so that the identity element maps to the identify element. The set $\mathbb{Q}$ is not cyclic because there are no generators for the identity element, so there is no order of the group that we would need to consider. □

Proof. For the second part of the question, yes, $f = cx$ also holds for the group $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. We will do a direct proof. We note that because $\sqrt{2}$ is not a rational number, multiplying it by any rational number will still result in an irrational number from which $\sqrt{2}$ can be factored out. We easily see that addition of a number in $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ to another number in $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ will result in a number in $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Put simply, this set is closed under addition; this makes sense, because the problem actually tells us that $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a group, so it would have to be closed under its operation of addition anyway. Now, we can take a hint from linear algebra and think of of the number $a + b\sqrt{2}$ as having two orthogonal "bases"–1 and $\sqrt{2}$. Now, we are just concerned about the coefficients of our bases, and we borrow the idea of direct products from group theory to finish our proof. Specifically, since the coefficients a and b are both elements of $\mathbb{Q}$, we say that our direct product is of $\mathbb{Q}$ x $\mathbb{Q}$ and consists of ordered pairs (a, b) where $a \in \mathbb{Q}$ and $b \in \mathbb{Q}$. This is the exact definition of the coefficients given in the problem, but we have now converted them into direct products, and now we can use the fact that this direct product is a group.

Now, we repeat the exact proof from above. Say that we have an isomorphism f such that:

$$f(0, 1) = (0, c) \tag{9}$$

$$f(1, 0) = (c, 0) \tag{10}$$

Then, by iterated addition, for $m, n, c \in \mathbb{Z}$, we have:

$$f(0, n) = (0, cn) \tag{11}$$

$$f(m, 0) = (cm, 0) \tag{12}$$

Now, let's define a new set of mappings, and we sub in the previous two equalities. Let p be an

integer, so that $\frac{n}{p}$ and $\frac{m}{p}$ are both rational numbers.

$$f\left(0, \frac{n}{p}\right) = (0, b) \tag{13}$$

$$f(0, n) = (0, bp) \tag{14}$$

$$(0, cn) = (0, bp) \tag{15}$$

$$f\left(0, \frac{n}{p}\right) = \left(0, c\frac{n}{p}\right) \tag{16}$$

$$f\left(0, \frac{n}{p}\right) = c\left(0, \frac{n}{p}\right) \tag{17}$$

And now, we do the same thing for m:

$$f\left(\frac{m}{p}, 0\right) = (a, 0) \tag{18}$$

$$f(m, 0) = (ap, 0) \tag{19}$$

$$(cm, 0) = (ap, 0) \tag{20}$$

$$f\left(\frac{m}{p}, 0\right) = \left(c\frac{m}{p}, 0\right) \tag{21}$$

$$f\left(0, \frac{m}{p}\right) = c\left(0, \frac{m}{p}\right) \tag{22}$$

Let's define two rational numbers as $a = \frac{m}{p}$ and $b = \frac{n}{p}$:

$$f(a, b) = f((0, b) + (a, 0)) \tag{23}$$

$$f(a, b) = c(0, b) + c(a, 0) \tag{24}$$

$$f(a, b) = c(a, b) \tag{25}$$

Recall that the direct product actually represents the two coefficients of the bases 1 and $\sqrt{2}$, so what we actually have is:

$$f(a + b\sqrt{2}) = c(a + b\sqrt{2}) \tag{26}$$

Thus, we have shown that $f = cx$ is the only isomorphism mapping $\mathbb{Q}$ under addition to itself.

□

Problem 2

Since $q \mid 2^p - 1$, we can write

$$2^p - 1 \equiv 0 \pmod{q} \tag{27}$$

$$2^p \equiv 1 \pmod{q} \tag{28}$$

Since we are looking at the group $\{1, 2, ..., q-1\}$ under multiplication mod q, we see that the order of 2 is at most p, because 2^p already gives $1 \pmod{q}$. Interestingly, the order cannot be less than p either. For example, say that there exists a $r < p$ such that $2^r \equiv 1 \pmod{q}$. Then, there exists a k such that $p = k \cdot r$ such that $2^{k \cdot r} \equiv 2^p \equiv 1 \pmod{q}$. However, since p is prime, no such r (or k) exists. Thus, we've shown that 2 has order p in this group. Let's use this result to show that there are infinite primes.

Proof. We do a proof by contradiction. Let's assume to the contrary that there are a finite number of primes, with p being the greatest prime. We let q be a prime divisor of $2^p - 1$, and we know that 2 has order p in the group G, defined as: $\{1, 2, ..., q-1\}$ under multiplication. But according to LaGrange's theorem, since G is of finite order $q-1$, any subgroup of G must have order m such that $m|q-1$. Thus, $p|q-1$. This suggests that $q > p$. Since q is also prime, we have shown that there exists a prime greater than p, and our initial assumption of finite prime numbers is wrong.

□

Problem 3

tldr: Since this is a long problem, my final solution is: $a_n = \frac{25}{6}5^n - \frac{23}{2}3^n + \frac{22}{3}2^n$.

We have $a_0 = 0$, $a_1 = 1$, and $a_n = 5a_{n-1} - 6a_{n-2} + 5^n$. Let's write the generative function and play around with it:

$$A(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n + ... \tag{29}$$

$$A(x) = 0 + x + (5a_1 - 6a_0 + 5^2)x^2 + (5a_2 - 6a_1 + 5^3)x^3 + ... + (5a_{n-1} - 6a_{n-2} + 5^n)x^n + ... \tag{30}$$

$$A(x) = x + 5(a_1 x^2 + a_2 x^3 + ...) - 6(a_0 x^2 + a_1 x^3 + ...) + (1 + 5x + 5^2 x^2 + 5^3 x^3 + ...) - 1 - 5x \tag{31}$$

$$A(x) = x + 5xA(x) - 6x^2 A(x) + \sum_{n \geq 0}^{\infty} 5^n x^n - 1 - 5x \tag{32}$$

We use the fact that $(1 - ax)^{-m} = \sum_{n \geq 0} \binom{m+n-1}{n} a^n x^n$ to get:

$$A(x) = -1 - 4x + 5xA(x) - 6x^2A(x) + \frac{1}{1-5x} \tag{33}$$

$$\tag{34}$$

Continuing to simplify, we get:

$$A(x) - 5xA(x) + 6x^2A(x) = -1 - 4x + \frac{1}{1-5x} \tag{35}$$

$$A(x) = \frac{20x^2 + x}{(1-5x)(1-2x)(1-3x)} \tag{36}$$

Let's now use partial fraction decomposition.

$$A(x) = \frac{A}{1-5x} + \frac{B}{2x-1} + \frac{C}{3x-1} \tag{37}$$

$$\tag{38}$$

Expanding, we get:

$$x^2 + 20x = A(6x^2 - 5x + 1) + B(-10x^2 + 7x - 1) + C(-15x^2 + 8x - 1) \tag{39}$$

$$\tag{40}$$

Adding up coefficients for 1, x, and x^2, we end up with the following systems of equations:

$$A - B - C = 0 \tag{41}$$

$$6A - 10B - 15C = 20 \tag{42}$$

$$-5A + 7B + 8C = 1 \tag{43}$$

We can use linear algebra to solve, and we get:

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 \\ 6 & -10 & -15 \\ -5 & 7 & 8 \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ 20 \\ 1 \end{pmatrix} \tag{44}$$

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} \frac{25}{6} & \frac{1}{6} & \frac{5}{6} \\ \frac{9}{2} & \frac{1}{2} & \frac{3}{2} \\ -\frac{4}{3} & -\frac{1}{3} & -\frac{2}{3} \end{pmatrix} \begin{pmatrix} 0 \\ 20 \\ 1 \end{pmatrix} \tag{45}$$

$$\begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} \frac{25}{6} \\ \frac{23}{2} \\ -\frac{22}{3} \end{pmatrix} \tag{46}$$

Plugging A, B, and C back into our partial frations, we have:

$$A(x) = \frac{25}{6(1-5x)} + \frac{23}{2(3x-1)} - \frac{22}{3(2x-1)} \tag{47}$$

We want our denominators to look like: $(1-ax)^{-m}$ so that we can use the fact that $(1-ax)^{-m} = \sum_{n\geq 0} \binom{m+n-1}{n} a^n x^n$ to rewrite our expressions in power series. We have:

$$A(x) = \frac{25}{6(1-5x)} - \frac{23}{2(1-3x)} + \frac{22}{3(1-2x)} \tag{48}$$

$$A(x) = \frac{25}{6}\sum_{n\geq 0} 5^n x^n - \frac{23}{2}\sum_{n\geq 0} 3^n x^n + \frac{22}{3}\sum_{n\geq 0} 2^n x^n \tag{49}$$

$$A(x) = \sum_{n\geq 0} x^n \left(\frac{25}{6}5^n - \frac{23}{2}3^n + \frac{22}{3}2^n\right) \tag{50}$$

The coefficient in the power series is now devoid of recursion, and we have our solution:

$$a_n = \frac{25}{6}5^n - \frac{23}{2}3^n + \frac{22}{3}2^n \tag{51}$$

I also calculated the first 10 expressions using both the recursive and non-recursive expressions, and they seem to agree. I did this with pen/paper, but it seemed more elegant to code it up. The non-recursive function has float precision, so I simply rounded it.

[10]:
```
import numpy as np

def recur(n):
    if n <= 1:
        return n
    else:
        return 5 * recur(n - 1) - 6 * recur(n - 2) + 5 ** n

def nonrecur(n):
    tmp = 5 ** n * 25 / 6
    tmp2 = - 3 ** n * 23 / 2
    tmp3 = 2 ** n * 22 / 3
    return tmp + tmp2 + tmp3
```

```python
for i in range(10):
    print(f'recursion a{i} :', recur(i))
    print(f'non-recursion a{i} :', np.round(nonrecur(i)))
    print()
```

```
recursion a0 : 0
non-recursion a0 : 0.0

recursion a1 : 1
non-recursion a1 : 1.0

recursion a2 : 30
non-recursion a2 : 30.0

recursion a3 : 269
non-recursion a3 : 269.0

recursion a4 : 1790
non-recursion a4 : 1790.0

recursion a5 : 10461
non-recursion a5 : 10461.0

recursion a6 : 57190
non-recursion a6 : 57190.0

recursion a7 : 301309
non-recursion a7 : 301309.0

recursion a8 : 1554030
non-recursion a8 : 1554030.0

recursion a9 : 7915421
non-recursion a9 : 7915421.0
```

Problem 4

This problem is actually pretty straightforward, since we are not asked to find a non-recursive formula, and we just need to find the recurrence relation. Let's begin by considering b_n for $n \geq 4$, since we can easily define b_1 to b_4 with base cases. For sequences of length greater than or equal to 4, there are two possibilities: either the first digit is a 0, or the first three digits are 1. In the first scenario, there are b_{n-1} different ways to fill the last b_{n-1} digits. In the second scenario, it gets more complicated, and can itself be split into two scenarios. The first three digits are always 1's, and we could have any number, up to $n-4$, of 1's following these first three, until we get two a 0. After this 0, the rest of the number can defined through recursion of previously defined b's. Let's draw a diagram to be clear.

$$1\ 1\ 1\ 0\ \{b_{n-4} \text{ possibilities}\} \tag{52}$$

$$1\ 1\ 1\ 1\ 0\ \{b_{n-5} \text{ possibilities}\} \tag{53}$$

$$1\ 1\ 1\ ...\ 1\ 0\ \{b_2 \text{ possibilities}\} \tag{54}$$

$$1\ 1\ 1\ ...\ 1\ 1\ 0\ \{b_1 \text{ possibilities}\} \tag{55}$$

Each row represents n numbers in the sequence, so the number of 1's in the ... would just fill in such that the length is n. There are $\sum_{k=1}^{n-4} b_k$ sequences of this type. Notably, this structure does not account for two particular sequences:

$$1\ 1\ 1\ ...\ 1\ 0 \text{ possibilities} \tag{56}$$

$$1\ 1\ 1\ ...\ 1\ 1 \text{ possibilities} \tag{57}$$

In other words, we could have a scenario where the only 0 is the last number of the sequence, or a scenario where it is all 1's. Now, let's sum up all of the different structures we have talked about thus far:

$$b_n = b_{n-1} + \sum_{k=1}^{n-4} b_k + 2 \tag{58}$$

Now, let's get rid of the summation such that we no longer depend on an arbitrary number of points. We subtract the first two equations to get the third:

$$b_n = b_{n-1} + \sum_{k=1}^{n-4} b_k + 2 \tag{59}$$

$$b_{n-1} = b_{n-2} + \sum_{k=1}^{n-5} b_k + 2 \tag{60}$$

$$b_n - b_{n-1} = b_{n-1} - b_{n-2} + b_{n-4} \tag{61}$$

$$b_n = 2b_{n-1} - b_{n-2} + b_{n-4} \tag{62}$$

And thus we get our recursive formula for b_n. It is $b_n = 2b_{n-1} - b_{n-2} + b_{n-4}$. Now, let's define our starting conditions:

$$b_1 = 1 \tag{63}$$

$$b_2 = 1 \tag{64}$$

$$b_3 = 2 \tag{65}$$

$$b_4 = 4 \tag{66}$$

These starting conditions are very intuitive; I list them below for clarity:

$$b_1 : 0 \tag{67}$$

$$b_2 : 0\ 0 \tag{68}$$

$$b_3 : 0\ 0\ 0;\ 1\ 1\ 1 \tag{69}$$

$$b_4 : 0\ 0\ 0\ 0;\ 1\ 1\ 1\ 1;\ 0\ 1\ 1\ 1;\ 1\ 1\ 1\ 0 \tag{70}$$

Problem 5

Proof. We will do a pigeonhole proof. Let's actually create 2020 new numbers. Each new number s_n will be the sum of the first n numbers that we wrote on the blackboard. This will lead to 2020 new numbers. Since we're not limiting the numbers to positive or negative numbers, s_n may get larger or smaller as n increases; however, all numbers added earlier will be present in later sums. For each number s_n, we write it $\pmod{2020}$. There are two scenarios: either there is already a number s_n that can be written as $0 \pmod{2020}$ or there are no numbers of the form s_n that can be written as $0 \pmod{2020}$. In the first scenario, we would be done because s_n would represent the "subset of numbers so that their sum is a multiple of 2020." In the second scenario, the sums can only be congruent to $1 \pmod{2020}$ through to $2019 \pmod{2020}$; if it is congruent to a number greater than 2019, it can be re-written in terms of a number between 1 and 2019. In other words, there are 2019 different congruencies, $\pmod{2020}$. Since we have 2020 sums, at least two sums must have the same congruency. Let's say s_a and s_b are both congruent to $r \pmod{2020}$. Say $a > b$. If $b > a$, simply switch the values of s_a and s_b so that $s_a > s_b$. Then, we have:

$$s_a \equiv r \pmod{2020} \tag{71}$$

$$s_b \equiv r \pmod{2020} \tag{72}$$

$$s_a - s_b \equiv 0 \pmod{2020} \tag{73}$$

Since $s_a > s_b$ and s_n was defined such that all previous sums are included, $s_a - s_b$ will be the sum of a subset of the 2020 numbers, specifically those whose indices are greater than b and less than or equal to a. This sum is also congruent to $0 \pmod{2020}$, so it is a multiple of 2020, and we are done.

□