PUMaC 2015

PUMaC 2015 Power Round

"We have a new theorem—that mathematicians can prove only trivial theorems, because every theorem that's proved is trivial." —Richard Feynman

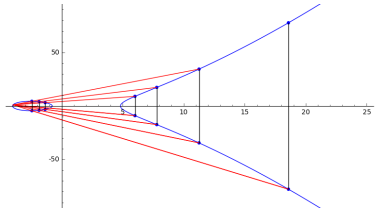

Figure 1: Graphical View of kP.

Updated 11/19/15.

1 Introduction

Elliptic curves appear often in mathematics because they possess remarkably nice properties. For example, elliptic curves relate elegantly to ideas from Galois theory. This Power Round will demonstrate the utility of elliptic curves and Galois theory by using them to prove an interesting fact about the Somos-4 sequence. (Note the test version calls this the "Tiger sequence." This Somos-4 sequence is the proper name for the sequence, and full credit must be given to those who have studied it.) We define the Somos-4 sequence $\{a_n\}$ for non-negative n recursively by $a_0 = a_1 = a_2 = a_3 = 1$ and for $n \geq 4$, the relation

$$a_n a_{n-4} = a_{n-1}a_{n-3} + a_{n-2}^2.$$

We ultimately seek to prove the following theorem.

Theorem 1. *Let $\pi(x)$ be the number of primes less than or equal to x. Then*

$$\lim_{x\to\infty} \frac{|\{p \leq x : p \text{ prime and } p|a_n \text{ for some } n\}|}{\pi(x)} = \frac{11}{21}.$$

This $\frac{11}{21}$ fraction is called the density of primes that divides a term of the Tiger sequence.

While much mathematical machinery is needed to prove this, we have broken down the task into a series of sections that culminate in a final proof in section 9. Please note that while the ultimate goal of this Power Round is to prove the given theorem, the sections may include problems that are not essential to the final proof, but are relevant and good problems to try. We have sorted the problems in as straightforward a manner as possible with regards to the final proof, but as the various topics are very interconnected you may find it useful to refer back to previous sections for ideas on how to proceed. As always, refer to the rules at the start of the document for how to reference other problems.

In a similar vein, we have a couple housekeeping remarks:

- All definitions, propositions, lemmas, and theorems are labeled in increasing order using the same index. For example, this document began by introducing a theorem labeled Theorem 1 and will soon introduce its first lemma labeled Lemma 2 followed by its first official definition labeled Definition 3.
- While this document guides you through the final proof, it will not babysit your progress. In any given part of the document, we may make assertions that will be necessary when solving a later problem. It is your responsibility as the reader to keep track of such material. Details that are absolutely essential will often be written in bold, but this is not an if and only if criterion for discerning important facts.

Lastly, you may be asking yourself: "Why is this interesting?" Well, we could name-drop famous mathematicians who have answered similar questions, or lie and say this is a large area of mathematics (this specific flavor of math isn't). But that would only tell you why this topic is interesting to others. Why will it be interesting to you? Well, if we take a slightly more general view, the question becomes: Why is math interesting to you? You have probably heard people say that math is necessary for science or as a life skill. But, if you have voluntarily decided to take this contest, you might have a different opinion. Sure, the science/life skills part might be true, but that's not why you are here and that's not why we have organized this tournament for you. PUMaC is a competition for many different types of people created by many different types of people, but we all share an interest in and appreciation for math for its own sake. Math is pretty. Back to the original question, we hope that this Power Round will expose you to an area of math you haven't seen before and that is remarkably pretty (but we'll leave that aesthetic judgment to you). Now, please don't get too carried away by the scoring and the fact that this is a competition. It may be cliché, but please have fun as well.

-Heesu Hwang.

We'd like to acknowledge and thank many individuals and organizations without whom this would not have been possible to exist. What has been called the "Tiger sequence" in the test version of this Power

Round is in fact well known as the Somos-4 sequence, and we give thanks to all that is known about it (as well as to the authors of the Somos-5 sequence integrality proof). The author thanks Jeremy Rouse, whose work was repeatedly referenced and whose outline for a paper on iterated galois representations was the inspiration for this power round. By extension, the author thanks the Wake Forest REU where much of this work was learned. Thanks as always to Princeton University, the sponsor of PUMaC, and PUMaC itself. Lastly, the author gives thanks to all the individuals who helped extensively in the revision and editing process, including the contestants themselves.

Contents

List of Problems

2 Let's Get Started

Firstly, if you haven't read the introduction, then go back and read the introduction! It really does add big-picture context to the problems you're doing. Now as a preliminary and as an example of the standards of justification we expect throughout this power round, here is a classical number theory result called Bézout's Lemma, with proof. Very quickly, here is a spot of terminology:

Definition 2. *$\mathbb{Z}$ represents the set of integers. $\mathbb{Q}$ represents the set of rational numbers. $\mathbb{R}$ represents the set of real numbers. $\mathbb{C}$ represents the set of complex numbers. Finally, $\mathbb{N}$ represents the set of positive integers. (A point of interest, Europeans include 0 in this set while Americans do not. Do you agree? Is 0 a natural number?)*

Definition 3. *Sets. A set is a collection of objects. We write that set $A = \{a_i\}$ for integers $1 \leq i \leq n$ if A contains exactly elements a_i and nothing else. We may similarly have infinite sets. Here is some specific notation with sets:*

- *$a \in A$: Let A be a set such that A contains the element A; then we write $a \in A$.*
- *$A \backslash B$: Let A and B both be sets. Then $A \backslash B$ denotes the set of elements that are inside A but not in B.*
- *$A \subset B$: Let A and B both be sets. If every element of A lies inside B, we write $A \subset B$.*
- *$\forall a \in A$: The notation $\forall a \in A$ is read in English as "for all elements a in A", and means we consider all elements of set A.*
- *$\exists a (\in A)$: This notation is read as "there exists an element a (in set A)." It is usually followed up by the phrase "such that." For example, $\exists x \in \mathbb{R}$ such that $x > 0$.*

Lemma 4 (Bézout's Lemma)**.** *Prove that if x and y are coprime integers, then there exist integers a and b such that $ax + by = 1$.*

Proof. We prove the more general case of integers x and y with a general gcd.

Examine the set $S := \{c \in \mathbb{N} : c = ax + by \text{ where } a, b \in \mathbb{Z}\}$. Since $\gcd(x, y)$ divides x and y, $\gcd(x, y)$ divides any element of S.

Suppose that l is the least element of S by the well-ordering principle (which states that every non-empty set of positive integers has a least element); thus let a_0 and b_0 be integers such that $l = a_0x + b_0y$. Take any other arbitrary element of S; for example $k = a_1x + b_1y$. Then by integer division, suppose that $k = l \cdot q + r$ where $0 \leq r < l$. Thus

$$l = a_0x + b_0y \implies lq = a_0qx + b_1qy \implies r = k - lq = (a_1 - a_0q)x + (b_1 - x_0q)y.$$

Since l by assumption was the least positive integer that was a linear combination of x and y, we must have $r = 0$. Thus $k = l \cdot q$, and every element of S is divisible by l.

Note that $|x|, |y| \in S$; thus $l | \gcd(x, y)$. But clearly $\gcd(x, y) | l$, and so they are equal. Thus there is some integer solution to $l = ax + by$. □

3 Group Theory

Groups are fundamental to mathematics. They form the basis (pun!) of algebra, one of the two overarching subjects of math. It is important that anyone who wishes to explore math further understands groups well. A group is defined as follows.

Definition 5. *A group is a set of elements G with a closed binary operation $*$. Binary means $*$ operates on two elements. Closed means that for any $a, b \in G$, $a * b$ is contained inside G. These elements and operation obey the following three rules.*

- *There exists an unique element $e \in G$ such that for all elements $g \in G$, $e * g = g * e = g$. This is called the identity element. (In cases of ambiguity, we will denote this as e_G.)*
- *For any element $g \in G$, there exists a unique element $h \in G$ such that $g * h = h * g = e$. This element h is usually denoted g^{-1} (in additive groups (to be explained), it is denoted $-g$).*
- *For all $a, b, c \in G$, the associative property holds:*

$$a * (b * c) = (a * b) * c.$$

Definition 6. *Suppose $\{G, *\}$ is a group. Suppose $*$ is commutative. That is, for all a and b in the group, $a * b = b * a$. Then G is called commutative or abelian.*

To demonstrate all this, $\mathbb{Z}$ is a group with addition as the operation. This is a group because we may always add two integers and get another integer, 0 is the additive identity, and similarly the other group properties are satisfied. In fact, $\{\mathbb{Z}, +\}$ is an abelian group. Now here are some warm-up problems.

Problem 3.1 (Basic Group Theory; **2, 2, 2, 2**)**.** *Give justification for each of the following.*

a) Is $\{\mathbb{Z}, -\}$, the set of integers under subtraction, a group?

b) Is $\{\mathbb{N}, +\}$, the set of positive integers under addition, a group?

c) Is $\{\mathbb{Q}, \cdot\}$, the set of rationals under multiplication, a group?

d) Is $\{\mathbb{Q}\backslash\{0\}, \cdot\}$, the set of rationals without zero under multiplication, a group?

Proof. a) No. The associative property does not hold. For example, $4 - (2 - 7) = 9 \neq -5 = (4 - 2) - 7$.

b) Nope! Additive inverses do not exist. For example, the inverse of 2 doesn't exist.

c) Still no! Zero still doesn't have a multiplicative inverse.

d) Yes. This is true by definitions.

□

We turn now briefly to the topic of modular numbers where we find groups arising naturally. We denote $\mathbb{Z}/n\mathbb{Z}$ as the integers mod n. Elements of this set are integers m where $0 \leq m < n$. Note that by division, for any integer $z \in \mathbb{Z}$, we may write $z = n \cdot q + r$ where $0 \leq r < n$ and q and r are both integers. Thus in this set of integers mod n, $z \equiv r \pmod{n}$. For examples, in the set of integers mod 7 ($\mathbb{Z}/7\mathbb{Z}$), $10 \equiv 3$

mod 7, $-5 \equiv 4 \mod 9$, and $1063 \equiv 3 \mod 10$. A nice property of mods is that we may substitute equivalent quantities at any time. For example,

$$\begin{aligned} 6546 \cdot 773 - 1650 \cdot 945 + 8^{654651} &= (935 \cdot 7 + 1) \cdot (110 \cdot 7 + 3) - (235 \cdot 7 + 5) \cdot (135 \cdot 7) + (7+1)^{654651} \\ &\equiv 1 \cdot 3 - 5 \cdot 0 + 1^{654651} \pmod 7 \\ &\equiv 4 \pmod 7. \end{aligned}$$

We mention mods because they are very fundamental to number theory and algebra. For one, note that $\mathbb{Z}/n\mathbb{Z}$ is a group with respect to addition (morally, you should really prove this to yourself, but there is no problem to write up). If $n = p$ is prime, we equivalently write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Primes are really nice numbers, and in general "things" like $\mathbb{F}_p$ that are associated with primes are also often very nice, as we shall see in depth later (fields!). For now, here's just a small problem about mods.

Problem 3.2 (Finite Field; **5**). *Let $p \in \mathbb{Z}$ be a prime. Setwise, the unit group of $\mathbb{F}_p$ is $\mathbb{Z}/p\mathbb{Z}\backslash\{0\}$. Prove that the unit group of $\mathbb{Z}/p\mathbb{Z}$, denoted as $\mathbb{Z}/p\mathbb{Z}^\times$, is a group under multiplication.*

Proof. Everything is really easy to check except inverses (but should be written out in full). Having proved Bezout's earlier, let $a \in \mathbb{Z}/p\mathbb{Z}^\times$ be an arbitrary element. Then $a \neq 0$ means that $(a, p) = 1$ and for some $m, n \in \mathbb{Z}$, $ma + np = 1 \implies a \cdot m \equiv 1 \pmod p$. Thus $a^{-1} = m$ exists as desired. □

Turning back now to group theory, if the operation of a group is called "addition," we call it an additive group. Notationally, for any $g \in G$ and n a non-negative integer, $ng := \sum_{i=1}^{n} g$ denotes g added to itself n times and for $n < 0$, $ng = -((-n)g)$. Also, 0 denotes the group identity. Similarly, if the operation is called multiplication, then for any $g \in G$ and n a non-negative number, $g^n = \prod_{i=1}^{n} g$ denotes g multiplied by itself n times, and for $n < 0$, $ng = (|n|g)^{-1}$. Also, 1 is the group identity. When notation is written with powers, it is implicitly implied that the operation is multiplication, and similarly notation that uses scalar multiples of group elements implies the operation is addition. With that, here are a bunch of problems and definitions!

Definition 7. *The order of any element $g \in G$ is the least positive integer l such that $g^l = e$. If no such l exists, then the order is called infinite.*

Secondly, the order of a group G is the number of elements of G. Note if G has infinitely many elements, the order of G is infinity.

For example, 2015 has infinite order in the group of integers under addition. However, 2015 has order 2 in $\mathbb{Z}/4030\mathbb{Z}$.

Problem 3.3 (Finite Group; **5**). *Let G be a finite group. Prove that every element of G has a finite order.*

Proof. Let $g \in G$ be an arbitrary element. Then examine the set $\langle g \rangle := \{g^n : n \in \mathbb{N}\}$. By pigeonhole, there have to be some repetitions. So suppose that $g^i = g^j$ for some WLOG $i > j$. Then $g^i \cdot (g^{-1})^j = g^j \cdot (g^{-1})^j \implies g^{i-j} = 1$. Thus g has finite order. □

We only consider finite groups in depth during this power round. However, we have seen examples of infinite groups (such as the integers under addition). In general, there aren't really large philosophical differences between the two categories. However, we primarily present finite groups here because it's easier to work with them when first starting out.

Definition 8. *Suppose that G is a finite group and $H \subset G$ is a non-empty subset of the elements of G that is itself a group. Then H is called a subgroup of G where H inherits the operation of G.*

The motivation behind such a construction of a subgroup is simple enough; it is a group in its own right that just happens to be contained inside another! You know what, here's a fun trick that you may find useful sometime (you likely won't use it in this power round, unfortunately).

Problem 3.4 (Subgroup Test; **5**)**.** *Let G be a group and $H \subset G$ a non-empty subset of G. Suppose H is a set that has the property that for all $a, b \in H$, $ab^{-1} \in H$. Prove that H is a subgroup of G.*

Proof. It's clear that associativity holds since $H \subset G$. Note that choosing $a = b$ shows $1 \in H$. Furthermore, choosing $a = 1$ shows that $b^{-1} \in H$. Thus the identity and inverse always exists. Note that we just found $b \in H \implies b^{-1} \in H$. Thus for all $a, b \in H$, $a(b^{-1})^{-1} = ab \in H$, and closure holds as well. Thus H is a group. □

Subgroups in fact are very nice, natural constructions from groups. Think back to the group of integers and the group of integers mod n; for example let's take $n = 7$. Another way to think about mods is to imagine that the numbers $0 \leq k < 7$ simply represent the classes of numbers $\{c \cdot 7 + k : c \in \mathbb{Z}\}$. For example, 0 represents the class of numbers $[0] := \{\cdots, -14, -7, 0, 7, 14, \cdots\}$, 1 represents the class $[1] := \{\cdots, -13, -6, 1, 8, 15, \cdots\}$, and so forth. In this manner, note that $[0]$ is a subgroup of $\mathbb{Z}$ under addition. However, $[1]$ is unfortunately not a subgroup. For example, $1 + 1 = 2$ is not in the set $[1]$. However, $[1]$ is still a pretty natural construction; maybe there is a name for it? Yes, there is!

Definition 9. *Let H be a subgroup of G. For all $g \in G$, we call $gH := \{g \cdot h : h \in H\}$ a left coset. For all $g \in G$, we call $Hg := \{h \cdot g : h \in H\}$ a right coset.*

For example, let $H = 7\mathbb{Z}$, the set of numbers that is 7 times an integer, and let $G = \mathbb{Z}$ the integers. Note that H is $[0]$ as mentioned above. Then $1 + H$ is a coset of G (note in this case, this is both a left and right coset) that in this case is the class $[1]$ mentioned directly above.

Cosets are very valuable tools in the proofs of group theory problems. Why? Because they are very symmetric in a sense, and this leads to neat properties. For example, if aH and bH are two cosets of a group G, do you think they have to intersect non-trivially? Well no; $[0]$ and $[1]$ as we saw above do not intersect ($[0]$ is the coset $0 + H$ in our example). Well if aH and bH do intersect, do you think they can intersect only a little bit? That is, can $aH \cap bH$ be non-empty, but $aH \cap bH$ is strictly smaller than both aH and bH? Or if G is a finite group, do you think that aH and bH have to have the same size? Or do you think that every element of G has to be contained inside some coset? These are all questions that you should think about.

Finally, this leads us to a what we call Lagrange's Theorem.

Problem 3.5 (Lagrange's Theorem; **10**)**.** *Suppose G is a finite group of order n. Then prove for all $g \in G$, $g^n = 1$.*

Proof. Let $H \subset G$ be any subgroup. Then examine all cosets $c_i H$ for $1 \leq i \leq k$. It is clear that the cosets are non-intersecting and everything in G is in one of the cosets; also all cosets have the same size. Thus $|G| = k \cdot |H|$, and the size of subgroups divides the size of their parent group.

For this problem, examine $\langle g \rangle := \{g^n : n \in \mathbb{N}\}$ for any element $g \in G$. Note that $|\langle g \rangle|$ divides $|G|$, and we are done. □

And now, before we proceed to other sections, here is a final group theory problem.

Problem 3.6 (Odd Order; **5**). *Let G be a finite group. Prove that an element g has odd order in G if and only if for every positive integer k, there exists some element $h_k \in G$ such that $(h_k)^{2^k} = g$. (Note that we do not specify G as abelian; it is sufficient to take G a finite group.)*

Proof. (Note to graders: many proofs of this may get very long and overly convoluted. Make sure that they do not make any more assumptions beyond the given that G is finite).

($\Rightarrow$) Suppose $g^{2l+1} = 1$ is the order. Then $g^{2(l+1)} = g$. By induction, we see that for all $k \in \mathbb{N}$, $\left(g^{(l+1)^k}\right)^{2^k} = g$.
($\Leftarrow$) Note that an element g has odd order iff some odd power of g is 1. So suppose $|G| = 2^l \cdot x$ where x is odd. Then look at $g = h_l^{2^l}$. We see $g^x = 1$, and g has odd order. □

Hopefully you have found these problems illuminating (hint: you may see these things again). However, to end this section, we would just like to present some standard material that we think is enriching to experience.

Suppose we have two groups G and H, and we create a function f between them $f : G \to H$. But we don't want any old functions; we want functions that somehow show that the structure of G and H have similarities. For example, examine $\mathbb{Z}$ and $2\mathbb{Z}$ as additive groups ($2\mathbb{Z}$ is notation for the set of all even numbers). Any addition done with the even numbers is linked to addition done with regular numbers. For example,

$$2 + 46 = 48 \Leftrightarrow 2(1) + 2(23) = 2(24).$$

We want functions between groups to somehow reflect the similarities between them. Thus we impose more conditions on f.

Definition 10. *Let G and H be groups with a function $f : G \to H$. This function f is called a homomorphism if:*

- *For all $a, b \in G$, $f(a *_G b) = f(a) *_H f(b)$ ($*_G$ and $*_H$ represent the operations of G and H respectively).*

For example, let $G = \mathbb{Z}$, $H = 2\mathbb{Z}$, and let $f(a) = 2a$. We encourage you to check that this is indeed a homomorphism, and that it has the property we wanted: that it represents the relationship between the structure of G and H.

Definition 11. *Let $f : G \to H$ be a homomorphism. If every element of H is the image of some element of G, then f is surjective and is a surjection.*

Definition 12. *Let $f : G \to H$ be a homomorphism. If the only element of G that is mapped to e_H, the identity element of H, is e_G, then f is injective and is an injection.*

Definition 13. *If a group homomorphism is both injective and surjective (if it satisfies both, then it is also called bijective), then it is called an isomorphism.*

You may want to convince yourself that in the example above, the homomorphism is indeed bijective. In general, the same terminology applies to general functions. If a function $f : A \to B$ has the property that $\forall b \in B$, $\exists a \in A$ such that $f(a) = b$ (surjective) and that $\forall a, a' \in A$, $f(a) = f(a') \implies a = a'$ (injective),

then f is bijective (this is an adjective) and is a bijection (this is a noun).

Next, we introduce the idea of mashing groups together. Recall that a number line can be represented as $\mathbb{R}$. A coordinate plane is similarly represented by the notation $\mathbb{R}^2$ or $\mathbb{R}\times\mathbb{R}$. This is called a direct product, and elements of $\mathbb{R}^2$ are coordinate pairs (a, b) where a and b both come from $\mathbb{R}$. Well, this is something we can do with groups as well. For example, taking two groups G and H, we denote $G \times H := \{(g, h) : g \in G, h \in H\}$. The group operation on this new set is the combination of the operations of G and H component-wise respectively. One fact that we ask the reader to convince themself (this is clearly grammatically not "correct," but the author strongly believes this should be an official singular, gender-neutral pronoun) is that $G \times H$ is itself a group. While this isn't an official problem, you should convince yourself that this works because it's necessary to understand for the next part.

We first introduce a definition. We will explore this topic more thoroughly in section 7, but the definition is sufficient here for now.

Definition 14. *Let R be a set of elements with a closed binary operation we call addition such that $\{R, +\}$ is an additive, commutative group. Furthermore, suppose R admits another closed binary operation $\cdot$ that we can call multiplication; it is commutative, and $\forall a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$; $a \cdot (b + c) = a \cdot b + a \cdot c$; and $(b + c) \cdot a = b \cdot a + c \cdot a$. Finally, there exists a multiplicative identity we call 1 such that for all $a \in R$, $a \cdot 1 = 1 \cdot a = a$. Then R is called a ring.*

Definition 15. *Let R be a ring. Then $GL_n(R)$ is called the general linear group, and denotes the group of $n \times n$ invertible matrices with elements in R as a group under multiplication.*

There is yet another way to make a group from two smaller groups. As a generalization of the direct product, we introduce the semidirect product. We start with a group G and a group H, where H is a group of functions that act on elements of G. For example, let G be the set of vectors $\mathbb{Z} \times \mathbb{Z}$, and let H be the set of matrices $\mathrm{GL}_2(\mathbb{Z})$.

In other words, G is a set of vectors of the form (a, b) where a and b are both integers, and H is the set of invertible 2×2 matrices with integer coefficients (invertible under multiplication). Elements of H are indeed functions that act on elements of G; for example if $h \in H$ and $g \in G$, then $h \cdot g$ is another vector. Thus we can define a semidirect product as follows.

Proposition 16. *Let the semidirect product setwise be defined as $G \rtimes H := \{(g, h) : g \in G, h \in H\}$ where H is a group of functions that acts on G (yes, groups may have functions as elements). Let $*_g$ and $*_h$ denote the group operations of G and H respectively. Then the group operation on this set for $(g_1, h_1), (g_2, h_2) \in G \rtimes H$ is defined by*

$$(g_1, h_1) * (g_2, h_2) := (g_1 *_g h_1(g_2), h_1 *_h h_2).$$

$G \rtimes H$ is a group.

Thus in our example here, we can define a group $(\mathbb{Z} \times \mathbb{Z}) \rtimes \mathrm{GL}_2(\mathbb{Z})$ (this is an example of an affine general linear group as we shall see later). Here is an example operation:

$$\begin{aligned}\left(\begin{bmatrix}2\\0\end{bmatrix}, \begin{bmatrix}-5 & 2\\2 & -1\end{bmatrix}\right) * \left(\begin{bmatrix}1\\5\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\right) &= \left(\begin{bmatrix}2\\0\end{bmatrix} + \begin{bmatrix}-5 & 2\\2 & -1\end{bmatrix} \cdot \begin{bmatrix}1\\5\end{bmatrix}, \begin{bmatrix}-5 & 2\\2 & -1\end{bmatrix} \cdot \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\right)\\ &= \left(\begin{bmatrix}2\\0\end{bmatrix} + \begin{bmatrix}5\\-3\end{bmatrix}, \begin{bmatrix}-5 & 2\\2 & -1\end{bmatrix} \cdot \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\right)\\ &= \left(\begin{bmatrix}7\\-3\end{bmatrix}, \begin{bmatrix}-5 & 2\\2 & -1\end{bmatrix}\right).\end{aligned}$$

Later on when we revisit this affine general linear group, we use this notation $AGL_2(R)$ to denote $(R)^2 \rtimes \mathrm{GL}_2(R)$ where R is a general ring. We will go in depth about this later. With this, we turn now to the topic of elliptic curves.

4 Elliptic Curves

Elliptic curves are integral (hah! it's a pun!) to mathematics, and in fact have even higher generalizations called varieties. For the purposes of this power round, we define an elliptic curve as follows.

Definition 17. *An elliptic curve E is the curve satisfying an equation of the form*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the coefficients a_i are INTEGERS (can't stress this enough :p).

The strange coefficient numberings are of historical significance. The reason that elliptic curves are interesting is that there is a natural group on the set of points on them.

Very important remarks: for the entirety of this power round, we take coefficients of elliptic curves to be integers. However, we may allow points on the curve to be rational or something else. Unless otherwise specified, any elliptic curve has integer coefficients and any points we consider on it are rational points.

Now, if you're the average person looking at this equation, you may be slightly disgusted by how unwieldy it looks; come on, that xy term looks atrocious. So let's get rid of it.

Problem 4.1 (Transformation of EC; **2, 8**).

a) *Let $f(x) = x^3 + a_2x^2 + a_1x + a_0$ be a polynomial with rational coefficients. Find some linear change of variables $x = mx' + n$ such that $f(x) = x'^3 + b_1x' + b_0$ is another polynomial with rational coefficients.*

b) *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve. Find a change of variables $y \mapsto y'$ and $x \mapsto x'$ such that $y'^2 = x'^3 + Ax' + B$. This gives us another elliptic curve E'; note that E' is an elliptic curve, and so $A, B \in \mathbb{Z}$. (Hint: you may have to use a change of variables that involves two variables at once. Also keep in mind that the starting and final coefficients have to be integral.)*

Proof.

a) Use the change $x = x' - \frac{a_2}{3}$.

b) We use a change of variables $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ to get an equation of the form $y^2 = 4x^3 + b_2x^2 + b_1x + b_0$. Then multiplying by 4^2 gives $(4y)^2 = (4x)^3 + b_2(4x)^2 + 4b_1(4x) + 16b_0$. So another change of variables in x from the question right above gets rid of the x^2 term (also $4y \mapsto y$).

   Thus we find some transformed elliptic curve $F : y^2 = x^3 + Ax + B$ for rational A and B (this entire process involves non-trivial denominators). However, Let $N \in \mathbb{N}$ be an integer such that $NA, NB \in \mathbb{Z}$. Then multiplying by N^6, we find that $(n^3y)^2 = (N^2x)^3 + AN^4(N^2x) + BN^6$. This last change of variables gives us the desired form.

   There are again a few ways to approach this. This is just one of the more compact (another pun!) transformations.

□

This latter form is what is called the short Weierstrass form. This form can be much easier to work with at times. Substitution for y^2 is a lot easier for example. Let's try to work with this form.

Let $E : y^2 = x^3 - 20x - 15$ be an elliptic curve. Note the points $P = (-4, 1)$ and $Q = (-1, -2)$ lie on E. The picture below shows the graph of the elliptic curve in blue with two points on it P and Q. In the picture, notice the black line through points P and Q. It intersects the elliptic curve again at another point we call $P * Q$ at coordinates $(6, -9)$. Finally, the reflection of point $P * Q$ vertically over the x-axis is shown by the red line. This gives us a point we call $P + Q$ at $(6, 9)$. Thus we write $(-1, -2) + (-4, 1) = (6, 9)$.

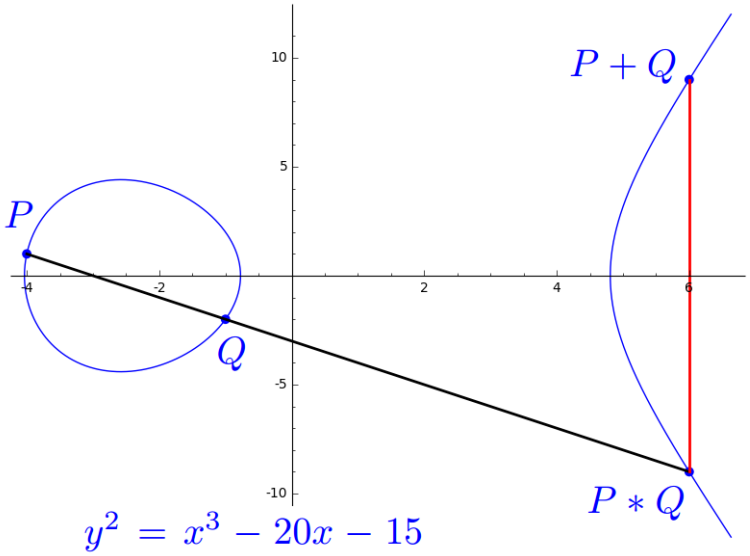

Figure 2: Addition of Two Rational Points.

This method in general gives us a way to define the "addition" of two points that will lead us to a group. Let's do a few more examples first, though. We stress that getting $P + Q$ from $P * Q$ by reflecting over the x-axis only works for elliptic curves in short Weierstrass form.

Problem 4.2 (Addition Computation; **2, 2**). *Let $E : y^2 = x^3 - 20x - 15$ be an elliptic curve. Note that $(6, -9)$, $(-4, 1)$, $(6, 9)$, and $(204, 2913)$ all lie on the curve.*

a) What is $(6, -9) + (-4, 1)$?

b) What is $(6, 9) + (204, 2913)$?

Proof.

a) While we can just bash it out with algebra, note by looking at the example case that these points are very well known. We know $(6, -9) * (-4, 1) = (-1, -2)$ as given. Thus $(6, -9) + (-4, 1) = (-1, 2)$.

b) By calculation, the sum is $(46/9, 109/27)$.

□

We are ready to present the group on an elliptic curve. Again, we reiterate that we have only seen addition for elliptic curves in short Weierstrass form.

Definition 18. *Let E be a general elliptic curve. Then $E(\mathbb{Q})$ denotes the set of rational points on E. That is, those points (α, β) with $\alpha, \beta \in \mathbb{Q}$ such that (α, β) lies on the curve E.*

Definition 19. *Let E be a general elliptic curve with points P and Q on E. Note that line PQ intersects E at a third point. This point is called $P * Q$. (The cautious reader might see some problems with this definition. For example, what if $P = Q$? This statement will be fully justified later, although you may be able to prove it yourself.)*

Proposition 20. *Let E be an elliptic curve in short Weierstrass form. Then $\{E(\mathbb{Q}), +\}$ is a group where the binary operation on two points P and Q is called addition. Namely, $P + Q$ is the reflection of $P * Q$ over the x-axis.*

Proving that this group (incredibly) exists can be unnecessarily complicated in general. For example, the existence of the identity element requires machinery that is a little too complicated to build here (we will build it later though!). Also, digest for a moment the almost magical nature of what this says. Given a line through two rational points on an elliptic curve, you get another rational point! With this in mind, it is a good exercise to prove some of the basic facts of this group law, after which you may assume this proposition is true.

Problem 4.3 (Addition Theory; **2, 8**). *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve with $A, B \in \mathbb{Z}$ and $P = (a, b)$, $Q = (c, d)$, and $H = (e, f)$ be rational points on E. For simplicity, we assume the x-coordinates of P, Q, and H are distinct.*

a) *Prove that $P + Q$ is a rational point.*

b) *Prove that the associative property holds. Namely, show that $(P + Q) + H = P + (Q + H)$. You may furthermore assume the x coordinates of $P+Q$ and H are different, and that of P and $Q+H$ are different as well.*

Proof. As an aside, I apologize to the grader of this problem for part b).

a) There is a linear equation defining line PQ. Substituting this line into the E equation gives a cubic equation in terms of x. Note this cubic already has two rational solutions (the x-coordinates of P and Q), and so it has a third rational solution. This gives a rational solution for $x(P * Q)$, the x-coordinate of $P * Q$, and therefore rational y-coordinate as well.

b) While there are some high-powered ways to do this, the expected way to prove this here is by algebra bash, which is straightforward. Here is a sketch. Let $A = (a, b)$, $B = (c, d)$, and $C = (e, f)$. If any of A, B, C is O, then associativity is clear since the addition cancels out. Thus assume that all $a, b, c, d, e, f \in \mathbb{Q}$. Since it's clear the operation is abelian, it suffices to show $(A+B)+C = (C+B)+A$. For notations sake let $x(P)$ be the x-coordinate of any point P on our curve $E : y^2 = x^3 + 2x + 3$, and similarly for $y(P)$. Note that $x((A + B) + C) = f_1(a, b, c, d, e, f)$ will be a rational function in 6 variables. If we can show that $f_1(a, b, c, d, e, f) = f_1(e, f, c, d, a, b)$, this shows that $x((A+B)+C) = x((C+B)+A)$. Similarly for $y((A + B) + C) = f_2(a, b, c, d, e, f)$.

   For two general points $(m, n), (r, s) \in E(\mathbb{Q})$, note they form the line $y - n = \frac{s-n}{r-m}(x - m)$ and we substitute into E to find the third point. By Vieta's formula, since we know two solutions to E with y substituted (m and r), we may just look at the x^2 coefficient to find the third x-coordinate. Thus $x((m, n) + (r, s)) = \left(\frac{s-n}{r-m}\right)^2 - m - r$. Then $y((m, n) + (r, s)) = -\left(\frac{s-n}{r-m} \cdot (x((m, n) + (r, s)) - m) + n\right)$.

Thus the above gives us that $x(A+B) = \left(\frac{d-b}{c-a}\right)^2 - a - c$, $y(A+B) = \left(\frac{d-b}{c-a}\right)^3 - (2a+c)\frac{d-b}{c-a} + b$, and then

$$x((A+B)+C) = \left(\frac{\left(\frac{d-b}{c-a}\right)^3 - (2a+c)\frac{d-b}{c-a} + b - f}{\left(\frac{d-b}{c-a}\right)^2 - a - c - e}\right)^2 - \left(\left(\frac{d-b}{c-a}\right)^2 - a - c\right) - e,$$

and

$$y((A+B)+C) = \left(\frac{\left(\frac{d-b}{c-a}\right)^3 - (2a+c)\frac{d-b}{c-a} + b - f}{\left(\frac{d-b}{c-a}\right)^2 - a - c - e}\right)^3 - (2e + \left(\frac{d-b}{c-a}\right)^2 - a - c)\frac{\left(\frac{d-b}{c-a}\right)^3 - (2a+c)\frac{d-b}{c-a} + -f}{\left(\frac{d-b}{c-a}\right)^2 - a - c - e} + f.$$

By very careful expansion, we have $(A+B)+C = ((a^7 - a^6c + a^6e - 3a^5c^2 - 2a^5ce - a^5e^2 - 2a^4b^2 + 2a^4bd - 2a^4bf + 3a^4c^3 - a^4c^2e + 3a^4ce^2 + a^4d^2 + 4a^4df - a^4e^3 + a^4f^2 + 2a^3b^2c - 2a^3b^2e - 2a^3bcd + 2a^3bcf + 4a^3bde + 3a^3c^4 + 4a^3c^3e - 2a^3c^2e^2 - 4a^3cd^2 - 10a^3cdf + 4a^3ce^3 - 4a^3cf^2 - 2a^3d^2e + 3a^2b^2c^2 + 2a^2b^2ce + a^2b^2e^2 + 6a^2bc^2f - 4a^2bcde - 2a^2bde^2 - 3a^2c^5 - a^2c^4e - 2a^2c^3e^2 + 3a^2c^2d^2 + 6a^2c^2df - 6a^2c^2e^3 + 6a^2c^2f^2 + 2a^2cd^2e + a^2d^2e^2 + ab^4 - 2ab^3d + 2ab^3f - 4ab^2c^3 + 2ab^2c^2e - 2ab^2ce^2 - 6ab^2df - 2abc^3d - 10abc^3f - 4abc^2de + 4abcde^2 + 2abd^3 + 6abd^2f - ac^6 - 2ac^5e + 3ac^4e^2 + 2ac^3d^2 + 2ac^3df + 4ac^3e^3 - 4ac^3f^2 + 2ac^2d^2e - 2acd^2e^2 - ad^4 - 2ad^3f - b^4c + b^4e + 2b^3cd - 2b^3cf - 4b^3de + b^2c^4 - 2b^2c^3e + b^2c^2e^2 + 6b^2cdf + 6b^2d^2e + 2bc^4d + 4bc^4f + 4bc^3de - 2bc^2de^2 - 2bcd^3 - 6bcd^2f - 4bd^3e + c^7 + c^6e - c^5e^2 - 2c^4d^2 - 2c^4df - c^4e^3 + c^4f^2 - 2c^3d^2e + c^2d^2e^2 + cd^4 + 2cd^3f + d^4e)/(a^6 - 2a^5c + 2a^5e - a^4c^2 - 6a^4ce + a^4e^2 - 2a^3b^2 + 4a^3bd + 4a^3c^3 + 4a^3c^2e - 4a^3ce^2 - 2a^3d^2 + 2a^2b^2c - 2a^2b^2e - 4a^2bcd + 4a^2bde - a^2c^4 + 4a^2c^3e + 6a^2c^2e^2 + 2a^2cd^2 - 2a^2d^2e + 2ab^2c^2 + 4ab^2ce - 4abc^2d - 8abcde - 2ac^5 - 6ac^4e - 4ac^3e^2 + 2ac^2d^2 + 4acd^2e + b^4 - 4b^3d - 2b^2c^3 - 2b^2c^2e + 6b^2d^2 + 4bc^3d + 4bc^2de - 4bd^3 + c^6 + 2c^5e + c^4e^2 - 2c^3d^2 - 2c^2d^2e + d^4), (a^9b - 2a^9d - 2a^9f + 3a^8cd + 6a^8cf - 3a^8ef - 6a^7bc^2 - 3a^7be^2 + 6a^7c^2d + 12a^7cef + 6a^7de^2 - 3a^6b^3 + 9a^6b^2d + 3a^6b^2f + 2a^6bc^3 + 6a^6bce^2 - 6a^6bd^2 - 2a^6be^3 + 3a^6bf^2 - 10a^6c^3d - 16a^6c^3f - 12a^6c^2ef - 21a^6cde^2 - a^6d^3 - 6a^6d^2f + 4a^6de^3 - 6a^6df^2 + a^6e^3f - a^6f^3 - 6a^5b^2cd - 12a^5b^2cf + 6a^5b^2ef + 12a^5bc^4 + 9a^5bc^2e^2 + 3a^5bcd^2 + 6a^5bcdf + 6a^5bce^3 - 9a^5bcf^2 - 12a^5bdef - 6a^5c^4d + 12a^5c^4f - 12a^5c^3ef + 18a^5c^2de^2 + 9a^5cd^3 + 24a^5cd^2f - 18a^5cde^3 + 27a^5cdf^2 - 6a^5ce^3f + 6a^5cf^3 + 6a^5d^2ef + 12a^4b^3c^2 + 6a^4b^3e^2 - 21a^4b^2c^2d + 12a^4b^2c^2f - 18a^4b^2cef - 21a^4b^2de^2 - 6a^4bc^5 - 30a^4bc^3e^2 + 6a^4bc^2d^2 - 24a^4bc^2df + 36a^4bcdef + 24a^4bd^2e^2 + 12a^4c^5d + 12a^4c^5f + 30a^4c^4ef + 15a^4c^3de^2 - 12a^4c^2d^3 - 33a^4c^2d^2f + 30a^4c^2de^3 - 45a^4c^2df^2 + 15a^4c^2e^3f - 15a^4c^2f^3 - 18a^4cd^2ef - 9a^4d^3e^2 + 3a^3b^5 - 12a^3b^4d - 5a^3b^3c^3 - 9a^3b^3ce^2 + 15a^3b^3d^2 - 6a^3b^3df + 2a^3b^3e^3 - 3a^3b^3f^2 + 15a^3b^2c^3d + 12a^3b^2c^3f + 12a^3b^2c^2ef + 39a^3b^2cde^2 - 3a^3b^2d^3 + 18a^3b^2d^2f - 6a^3b^2de^3 + 9a^3b^2df^2 - 10a^3bc^6 + 15a^3bc^4e^2 + 15a^3bc^3d^2 + 36a^3bc^3df - 20a^3bc^3e^3 + 30a^3bc^3f^2 - 24a^3bc^2def - 51a^3bcd^2e^2 - 6a^3bd^4 - 18a^3bd^3f + 6a^3bd^2e^3 - 9a^3bd^2f^2 + 2a^3c^6d - 16a^3c^6f - 12a^3c^5ef - 30a^3c^4de^2 - 5a^3c^3d^3 + 12a^3c^3d^2f - 20a^3c^3de^3 + 30a^3c^3df^2 - 20a^3c^3e^3f + 20a^3c^3f^3 + 12a^3c^2d^2ef + 21a^3cd^3e^2 + 3a^3d^5 + 6a^3d^4f - 2a^3d^3e^3 + 3a^3d^3f^2 + 3a^2b^4cd + 6a^2b^4cf - 3a^2b^4ef - 12a^2b^3c^4 - 9a^2b^3c^2e^2 - 3a^2b^3cd^2 - 6a^2b^3cdf - 6a^2b^3ce^3 + 9a^2b^3cf^2 + 12a^2b^3def + 6a^2b^2c^4d - 33a^2b^2c^4f + 12a^2b^2c^3ef + 9a^2b^2c^2de^2 - 9a^2b^2cd^3 - 18a^2b^2cd^2f + 18a^2b^2cde^3 - 27a^2b^2cdf^2 - 18a^2b^2d^2ef + 6a^2bc^7 + 18a^2bc^5e^2 - 21a^2bc^4d^2 - 24a^2bc^4df + 30a^2bc^4e^3 - 45a^2bc^4f^2 - 24a^2bc^3def + 9a^2bc^2d^2e^2 + 15a^2bcd^4 + 30a^2bcd^3f - 18a^2bcd^2e^3 + 27a^2bcd^2f^2 + 12a^2bd^3ef - 6a^2c^7d - 12a^2c^6ef + 9a^2c^5de^2 + 12a^2c^4d^3 + 12a^2c^4d^2f + 15a^2c^4e^3f - 15a^2c^4f^3 + 12a^2c^3d^2ef - 9a^2c^2d^3e^2 - 6a^2cd^5 - 12a^2cd^4f + 6a^2cd^3e^3 - 9a^2cd^3f^2 - 3a^2d^4ef - 6ab^5c^2 - 3ab^5e^2 + 15ab^4c^2d - 12ab^4c^2f + 6ab^4cef + 15ab^4de^2 + 9ab^3c^5 + 21ab^3c^3e^2 - 9ab^3c^2d^2 + 30ab^3c^2df + 6ab^3c^2e^3 - 9ab^3c^2f^2 - 24ab^3cdef - 30ab^3d^2e^2 + 3ab^2c^5d + 24ab^2c^5f - 18ab^2c^4ef - 51ab^2c^3de^2 - 3ab^2c^2d^3 - 18ab^2c^2d^2f - 18ab^2c^2de^3 + 27ab^2c^2df^2 + 36ab^2cd^2ef + 30ab^2d^3e^2 + 3abc^8 - 21abc^6e^2 - 6abc^5d^2 + 6abc^5df - 18abc^5e^3 + 27abc^5f^2 + 36abc^4def + 39abc^3d^2e^2 + 3abc^2d^4 - 6abc^2d^3f + 18abc^2d^2e^3 - 27abc^2d^2f^2 - 24abcd^3ef - 15abd^4e^2 + 6ac^8f + 12ac^7ef + 6ac^6de^2 - 12ac^5d^2f + 6ac^5de^3 - 9ac^5df^2 - 6ac^5e^3f + 6ac^5f^3 - 18ac^4d^2ef - 9ac^3d^3e^2 + 6ac^2d^4f - 6ac^2d^3e^3 + 9ac^2d^3f^2 + 6acd^4ef + 3ad^5e^2 - b^7 + 5b^6d - b^6f + 3b^5c^3 + 3b^5ce^2 - 9b^5d^2 + 6b^5df - 6b^4c^3d + 6b^4c^3f - 3b^4c^2ef - 15b^4cde^2 + 5b^4d^3 - 15b^4d^2f - b^3c^6 - 9b^3c^4e^2 - 3b^3c^3d^2 - 18b^3c^3df - 2b^3c^3e^3 + 3b^3c^3f^2 + 12b^3c^2def + 30b^3cd^2e^2 + 5b^3d^4 + 20b^3d^3f - 6b^2c^6d - 6b^2c^6f + 6b^2c^5ef + 24b^2c^4de^2 + 15b^2c^3d^3 + 18b^2c^3d^2f + 6b^2c^3de^3 - 9b^2c^3df^2 - 18b^2c^2d^2ef - 30b^2cd^3e^2 - 9b^2d^5 - 15b^2d^4f - 2bc^9 + 6bc^7e^2 + 9bc^6d^2 + 4bc^6e^3 - 6bc^6f^2 - 12bc^5def - 21bc^4d^2e^2 - 12bc^3d^4 - 6bc^3d^3f - 6bc^3d^2e^3 + 9bc^3d^2f^2 + 12bc^2d^3ef + 15bcd^4e^2 + 5bd^6 + 6bd^5f + c^9d - 2c^9f - 3c^8ef - 3c^7de^2 - 3c^6d^3 + 3c^6d^2f - 2c^6de^3 + 3c^6df^2 + c^6e^3f - c^6f^3 + 6c^5d^2ef + 6c^4d^3e^2 + 3c^3d^5 + 2c^3d^3e^3 - 3c^3d^3f^2 - 3c^2d^4ef - 3cd^5e^2 - d^7 - d^6f)/(a^9 - 3a^8c + 3a^8e - 12a^7ce + 3a^7e^2 - 3a^6b^2 + 6a^6bd + 8a^6c^3 + 12a^6c^2e - 15a^6ce^2 - 3a^6d^2 + a^6e^3 + 6a^5b^2c - 6a^5b^2e -$

$12a^5bcd+12a^5bde-6a^5c^4+12a^5c^3e+27a^5c^2e^2+6a^5cd^2-6a^5ce^3-6a^5d^2e+3a^4b^2c^2+18a^4b^2ce-3a^4b^2e^2-6a^4bc^2d-36a^4bcde+6a^4bde^2-6a^4c^5-30a^4c^4e-15a^4c^3e^2+3a^4c^2d^2+15a^4c^2e^3+18a^4cd^2e-3a^4d^2e^2+3a^3b^4-12a^3b^3d-12a^3b^2c^3-12a^3b^2c^2e+12a^3b^2ce^2+18a^3b^2d^2+24a^3bc^3d+24a^3bc^2de-24a^3bcde^2-12a^3bd^3+8a^3c^6+12a^3c^5e-15a^3c^4e^2-12a^3c^3d^2-20a^3c^3e^3-12a^3c^2d^2e+12a^3cd^2e^2+3a^3d^4-3a^2b^4c+3a^2b^4e+12a^2b^3cd-12a^2b^3de+3a^2b^2c^4-12a^2b^2c^3e-18a^2b^2c^2e^2-18a^2b^2cd^2+18a^2b^2d^2e-6a^2bc^4d+24a^2bc^3de+36a^2bc^2de^2+12a^2bcd^3-12a^2bd^3e+12a^2c^6e+27a^2c^5e^2+3a^2c^4d^2+15a^2c^4e^3-12a^2c^3d^2e-18a^2c^2d^2e^2-3a^2cd^4+3a^2d^4e-3ab^4c^2-6ab^4ce+12ab^3c^2d+24ab^3cde+6ab^2c^5+18ab^2c^4e+12ab^2c^3e^2-18ab^2c^2d^2-36ab^2cd^2e-12abc^5d-36abc^4de-24abc^3de^2+12abc^2d^3+24abcd^3e-3ac^8-12ac^7e-15ac^6e^2+6ac^5d^2-6ac^5e^3+18ac^4d^2e+12ac^3d^2e^2-3ac^2d^4-6acd^4e-b^6+6b^5d+3b^4c^3+3b^4c^2e-15b^4d^2-12b^3c^3d-12b^3c^2de+20b^3d^3-3b^2c^6-6b^2c^5e-3b^2c^4e^2+18b^2c^3d^2+18b^2c^2d^2e-15b^2d^4+6bc^6d+12bc^5de+6bc^4de^2-12bc^3d^3-12bc^2d^3e+6bd^5+c^9+3c^8e+3c^7e^2-3c^6d^2+c^6e^3-6c^5d^2e-3c^4d^2e^2+3c^3d^4+3c^2d^4e-d^6))$.

Similarly, we find that $(C+B)+A=((-a^3c^4+4a^3c^3e-6a^3c^2e^2+4a^3ce^3-a^3e^4-a^2c^5+3a^2c^4e-2a^2c^3e^2+a^2c^2d^2-2a^2c^2df-2a^2c^2e^3+a^2c^2f^2-2a^2cd^2e+4a^2cdef+3a^2ce^4-2a^2cef^2+a^2d^2e^2-2a^2de^2f-a^2e^5+a^2e^2f^2+ac^6-2ac^5e-ac^4e^2-2ac^3d^2+4ac^3df+4ac^3e^3-2ac^3f^2+2ac^2d^2e-4ac^2def-ac^2e^4+2ac^2ef^2+2acd^2e^2-4acde^2f-2ace^5+2ace^2f^2+ad^4-4ad^3f-2ad^2e^3+6ad^2f^2+4ade^3f-4adf^3+ae^6-2ae^3f^2+af^4+b^2c^4-4b^2c^3e+6b^2c^2e^2-4b^2ce^3+b^2e^4-2bc^4d+4bc^4f+2bc^3de-10bc^3ef+6bc^2de^2+6bc^2e^2f+2bcd^3-6bcd^2f-10bcde^3+6bcdf^2+2bce^3f-2bcf^3-2bd^3e+6bd^2ef+4bde^4-6bdef^2-2be^4f+2bef^3+c^7-c^6e-3c^5e^2-2c^4d^2+2c^4df+3c^4e^3+c^4f^2+2c^3d^2e-2c^3def+3c^3e^4-4c^3ef^2+3c^2d^2e^2-3c^2e^5+3c^2e^2f^2+cd^4-2cd^3f-4cd^2e^3-2cde^3f+2cdf^3-ce^6+2ce^3f^2-cf^4-d^4e+2d^3ef+d^2e^4+2de^4f-2def^3+e^7-2e^4f^2+ef^4)/(a^2c^4-4a^2c^3e+6a^2c^2e^2-4a^2ce^3+a^2e^4+2ac^5-6ac^4e+4ac^3e^2-2ac^2d^2+4ac^2df+4ac^2e^3-2ac^2f^2+4acd^2e-8acdef-6ace^4+4acef^2-2ad^2e^2+4ade^2f+2ae^5-2ae^2f^2+c^6-2c^5e-c^4e^2-2c^3d^2+4c^3df+4c^3e^3-2c^3f^2+2c^2d^2e-4c^2def-c^2e^4+2c^2ef^2+2cd^2e^2-4cde^2f-2ce^5+2ce^2f^2+d^4-4d^3f-2d^2e^3+6d^2f^2+4de^3f-4df^3+e^6-2e^3f^2+f^4),(a^3bc^6-6a^3bc^5e+15a^3bc^4e^2-20a^3bc^3e^3+15a^3bc^2e^4-6a^3bce^5+a^3be^6-2a^3c^6d+4a^3c^6f+6a^3c^5de-18a^3c^5ef+30a^3c^4e^2f+2a^3c^3d^3-6a^3c^3d^2f-20a^3c^3de^3+6a^3c^3df^2-20a^3c^3e^3f-2a^3c^3f^3-6a^3c^2d^3e+18a^3c^2d^2ef+30a^3c^2de^4-18a^3c^2def^2+6a^3c^2ef^3+6a^3cd^3e^2-18a^3cd^2e^2f-18a^3cde^5+18a^3cde^2f^2+6a^3ce^5f-6a^3ce^2f^3-2a^3d^3e^3+6a^3d^2e^3f+4a^3de^6-6a^3de^3f^2-2a^3e^6f+2a^3e^3f^3-3a^2c^7d+6a^2c^7f+6a^2c^6de-21a^2c^6ef+9a^2c^5de^2+18a^2c^5e^2f+6a^2c^4d^3-21a^2c^4d^2f-30a^2c^4de^3+24a^2c^4df^2+15a^2c^4e^3f-9a^2c^4f^3-9a^2c^3d^3e+39a^2c^3d^2ef+15a^2c^3de^4-51a^2c^3def^2-30a^2c^3e^4f+21a^2c^3ef^3-a^2c^2d^3e^2+9a^2c^2d^2e^2f+18a^2c^2de^5+9a^2c^2de^2f^2+9a^2c^2e^5f-9a^2c^2e^2f^3-3a^2cd^5+15a^2cd^4f+21a^2cd^3e^3-30a^2cd^3f^2-51a^2cd^2e^3f+30a^2cd^2f^3-21a^2cde^6+39a^2cde^3f^2-15a^2cdf^4+6a^2ce^6f-9a^2ce^3f^3+3a^2cf^5+3a^2d^5e-15a^2d^4ef-9a^2d^3e^4+30a^2d^3ef^2+24a^2d^2e^4f-30a^2d^2ef^3+6a^2de^7-21a^2de^4f^2+15a^2def^4-3a^2e^7f+6a^2e^4f^3-3a^2ef^5-3abc^8+12abc^7e-12abc^6e^2+6abc^5d^2-12abc^5df-12abc^5e^3+6abc^5f^2-18abc^4d^2e+36abc^4def+30abc^4e^4-18abc^4ef^2+12abc^3d^2e^2-24abc^3de^2f-12abc^3e^5+12abc^3e^2f^2-3abc^2d^4+12abc^2d^3f+12abc^2d^2e^3-18abc^2d^2f^2-24abc^2de^3f+12abc^2df^3-12abc^2e^6+12abc^2e^3f^2-3abc^2f^4+6abcd^4e-24abcd^3ef-18abcd^2e^4+36abcd^2ef^2+36abcde^4f-24abcdef^3+12abce^7-18abce^4f^2+6abcef^4-3abd^4e^2+12abd^3e^2f+6abd^2e^5-18abd^2e^2f^2-12abde^5f+12abde^2f^3-3abe^8+6abe^5f^2-3abe^2f^4-b^3c^6+6b^3c^5e-15b^3c^4e^2+20b^3c^3e^3-15b^3c^2e^4+6b^3ce^5-b^3e^6+3b^2c^6d-6b^2c^6f-9b^2c^5de+27b^2c^5ef-45b^2c^4e^2f-3b^2c^3d^3+9b^2c^3d^2f+30b^2c^3de^3-9b^2c^3df^2+30b^2c^3e^3f+3b^2c^3f^3+9b^2c^2d^3e-27b^2c^2d^2ef-45b^2c^2de^4+27b^2c^2def^2-9b^2c^2ef^3-9b^2cd^3e^2+27b^2cd^2e^2f+27b^2cde^5-27b^2cde^2f^2-9b^2ce^5f+9b^2ce^2f^3+3b^2d^3e^3-9b^2d^2e^3f-6b^2de^6+9b^2de^3f^2+3b^2e^6f-3b^2e^3f^3-2bc^9+6bc^8e+3bc^6d^2-16bc^6e^3-6bc^6f^2-12bc^5d^2e+6bc^5def+12bc^5e^4+24bc^5ef^2+12bc^4d^2e^2-24bc^4de^2f+12bc^4e^5-33bc^4e^2f^2-6bc^3d^3f+12bc^3d^2e^3+18bc^3d^2f^2+36bc^3de^3f-18bc^3df^3-16bc^3e^6+12bc^3e^3f^2+6bc^3f^4+6bc^2d^4e-6bc^2d^3ef-33bc^2d^2e^4-18bc^2d^2ef^2-24bc^2de^4f+30bc^2def^3+12bc^2e^4f^2-12bc^2ef^4-12bcd^4e^2+30bcd^3e^2f+24bcd^2e^5-18bcd^2e^2f^2+6bcde^5f-6bcde^2f^3+6bce^8-12bce^5f^2+6bce^2f^4-bd^6+6bd^5f+6bd^4e^3-15bd^4f^2-18bd^3e^3f+20bd^3f^3-6bd^2e^6+18bd^2e^3f^2-15bd^2f^4-6bde^3f^3+6bdf^5-2be^9+3be^6f^2-bf^6+c^9d-2c^9f+3c^8ef-6c^7de^2+6c^7e^2f-3c^6d^3+9c^6d^2f+2c^6de^3-6c^6df^2-10c^6e^3f-c^6f^3-6c^5d^2ef+12c^5de^4+3c^5def^2-6c^5e^4f+9c^5ef^3+12c^4d^3e^2-21c^4d^2e^2f-6c^4de^5+6c^4de^2f^2+12c^4e^5f-12c^4e^2f^3+3c^3d^5-12c^3d^4f-5c^3d^3e^3+15c^3d^3f^2+15c^3d^2e^3f-3c^3d^2f^3-10c^3de^6+15c^3de^3f^2-6c^3df^4+2c^3e^6f-5c^3e^3f^3+3c^3f^5+3c^2d^4ef-12c^2d^3e^4-3c^2d^3ef^2+6c^2d^2e^4f-9c^2d^2ef^3+6c^2de^7-21c^2de^4f^2+15c^2def^4-6c^2e^7f+12c^2e^4f^3-6c^2ef^5-6cd^5e^2+15cd^4e^2f+9cd^3e^5-9cd^3e^2f^2+3cd^2e^5f-3cd^2e^2f^3+3cde^8-6cde^5f^2+3cde^2f^4-d^7+5d^6f+3d^5e^3-9d^5f^2-6d^4e^3f+5d^4f^3-d^3e^6-3d^3e^3f^2+5d^3f^4-6d^2e^6f+15d^2e^3f^3-9d^2f^5-2de^9+9de^6f^2-12de^3f^4+5df^6+e^9f-3e^6f^3+3e^3f^5-f^7)/(a^3c^6-6a^3c^5e+15a^3c^4e^2-20a^3c^3e^3+15a^3c^2e^4-6a^3ce^5+a^3e^6+3a^2c^7-15a^2c^6e+27a^2c^5e^2-3a^2c^4d^2+6a^2c^4df-15a^2c^4e^3-3a^2c^4f^2+12a^2c^3d^2e-24a^2c^3def-15a^2c^3e^4+12a^2c^3ef^2-18a^2c^2d^2e^2+36a^2c^2de^2f+27a^2c^2e^5-18a^2c^2e^2f^2+12a^2cd^2e^3-24a^2cde^3f-15a^2ce^6+12a^2ce^3f^2-3a^2d^2e^4+6a^2de^4f+3a^2e^7-$

$3a^2e^4f^2+3ac^8-12ac^7e+12ac^6e^2-6ac^5d^2+12ac^5df+12ac^5e^3-6ac^5f^2+18ac^4d^2e-36ac^4def-30ac^4e^4+18ac^4ef^2-12ac^3d^2e^2+24ac^3de^2f+12ac^3e^5-12ac^3e^2f^2+3ac^2d^4-12ac^2d^3f-12ac^2d^2e^3+18ac^2d^2f^2+24ac^2de^3f-12ac^2df^3+12ac^2e^6-12ac^2e^3f^2+3ac^2f^4-6acd^4e+24acd^3ef+18acd^2e^4-36acd^2ef^2-36acde^4f+24acdef^3-12ace^7+18ace^4f^2-6acef^4+3ad^4e^2-12ad^3e^2f-6ad^2e^5+18ad^2e^2f^2+12ade^5f-12ade^2f^3+3ae^8-6ae^5f^2+3ae^2f^4+c^9-3c^8e-3c^6d^2+6c^6df+8c^6e^3-3c^6f^2+6c^5d^2e-12c^5def-6c^5e^4+6c^5ef^2+3c^4d^2e^2-6c^4de^2f-6c^4e^5+3c^4e^2f^2+3c^3d^4-12c^3d^3f-12c^3d^2e^3+18c^3d^2f^2+24c^3de^3f-12c^3df^3+8c^3e^6-12c^3e^3f^2+3c^3f^4-3c^2d^4e+12c^2d^3ef+3c^2d^2e^4-18c^2d^2ef^2-6c^2de^4f+12c^2def^3+3c^2e^4f^2-3c^2ef^4-3cd^4e^2+12cd^3e^2f+6cd^2e^5-18cd^2e^2f^2-12cde^5f+12cde^2f^3-3ce^8+6ce^5f^2-3ce^2f^4-d^6+6d^5f+3d^4e^3-15d^4f^2-12d^3e^3f+20d^3f^3-3d^2e^6+18d^2e^3f^2-15d^2f^4+6de^6f-12de^3f^3+6df^5+e^9-3e^6f^2+3e^3f^4-f^6))$.

Factorization by Magma tells us that a factor of the numerator of $x((C+B)+A)-x((A+B)+C)$ is

$$a^3c-a^3e-ac^3+ad^2+ae^3-af^2-b^2c+b^2e+c^3e-ce^3+cf^2-d^2e. \tag{1}$$

However, note that by virtue of $A,B,C\in E(\mathbb{Q})$, $b^2=a^3+2a+3$, $d^2=c^3+2c+3$, and $f^2=e^3+2e+3$. Substitution of all three shows that expression 1 is in fact 0:

$$\begin{aligned}
&a^3c-a^3e-ac^3+ad^2+ae^3-af^2-b^2c+b^2e+c^3e-ce^3+cf^2-d^2e\\
&=a^3c-a^3e-ac^3+a(c^3+2c+3)+ae^3-a(e^3+2e+3)-(a^3+2a+3)c+(a^3+2a+3)e\\
&\quad+c^3e-ce^3+c(e^3+2e+3)-(c^3+2c+3)e\\
&=a^3c-a^3e-ac^3+ac^3+2ac+3a+ae^3-ae^3-2ae-3a-a^3c-2ac-3c+a^3e+2ae+3e\\
&\quad+c^3e-ce^3+ce^3+2ce+3c-c^3e-2ce-3e\\
&=0.
\end{aligned}$$

Thus $x((A+B)+C)=x((C+B)+A)$. Similarly, Magma shows that expression 1 is a factor of $y((A+B)+C)-y((C+B)+A)$; thus $y((A+B)+C)=y((C+B)+A)$.

Therefore $(A+B)+C=A+(B+C)$, and addition of rational points is associative for $E:y^2=x^3+2x+3$. Therefore $E(\mathbb{Q})$ is indeed a group.

For reference, the following is code for Magma that was used to simplify the algebraic expressions.

```
{
Addition := function(x_0,y_0,x_1,y_1)
x:=(y_1-y_0)^2/(x_1-x_0)^2-x_0-x_1;
y:=(y_1-y_0)/(x_1-x_0)*(x-x_0)+y_0;
return x, -y;
end function;


R<a,b,c,d,e,f>:=FunctionField(Rationals(),6);
x1,y1:=Addition(a,b,c,d);
x2,y2:=Addition(e,f,x1,y1);

m1,n1:=Addition(e,f,c,d);
m2,n2:=Addition(m1,n1,a,b);

Factorization(Numerator(m2-x2));

Factorization(Numerator(n2-y2));

mminusx:=a^3*c - a^3*e - a*c^3 + a*(c^3+2*c+3) + a*e^3 - a*(e^3+2*e+3) - (a^3+2*a+3)*c
+ (a^3+2*a+3)*e + c^3*e - c*e^3 + c*(e^3+2*e+3) - (c^3+2*c+3)*e;
}
```

□

Problem 4.4 (Reduced Rational Point; **5**). *Let $E : y^2 + e_1xy + e_3y = x^3 + e_2x^2 + e_4x + e_6$ be an elliptic curve with integer coefficients. Suppose that $P = \left(\frac{a}{b}, \frac{c}{d}\right)$ on E is a rational point in reduced form (i.e. both the coordinates are reduced fractions). We may assume b and d are positive (since a or c can be negative). Give an equality relating b and d by writing one as a positive power of the other.*

Proof. Take the equation of E and stick in a/b and c/d for x and y. Clearing the denominators in least form and seeing what divides what gives a series of information that will bound b and d in terms of each other. We have the following equation (call it H):

$$\frac{c^2}{d^2} + e_1\frac{ac}{bd} + e_3\frac{c}{d} = \frac{a^3}{b^3} + e_2\frac{a^2}{b^2} + e_4\frac{a}{b} + e_6.$$

1. Multiply H by b^2d^2 shows that $b|d^2$.
2. Multiply H by b^3d shows that $d|b^3$.
3. Item 2 and multiplying H by b^4 shows that $d^2|b^4 \implies d|b^2$.
4. Item 3 and multiplying H by db^2 shows that $b|d$.
5. Item 4 and multiplying by d^2 shows that $b^3|d^2$.
6. Item 3 and multiplying by b^3 shows that $d^2|b^3$.

Therefore $d^2 = b^3$. Accept either $d = b^{3/2}$ or $b = d^{2/3}$. □

So if you are morally convinced by now that $E(\mathbb{Q})$ should be a group (as you should be), then you might also morally accept that Proposition 20 is also true for any elliptic curve, not just those written in short Weierstrass form. And it is! However, the definition of addition is slightly different in the general case. The reason we took $P+Q$ as the reflection of $P*Q$ in the short Weierstrass case is that for elliptic curves written in short Weierstrass form, there is a natural horizontal line of symmetry at the x-axis. In the general case, we can find another natural horizontal line of symmetry; and so in the general case, while $P * Q$ is always the same, $P + Q$ will be different.

For example, consider the curve $y^2 - 2015y = x^3 - 36x^2 + x$. Notice that for all points (a, b) on the curve, by how left hand side is written, the point $(a, 2015 - b)$ is also on the curve. Thus the horizontal line of symmetry in this case is $\frac{2015}{2}$. For this curve then, $P * Q$ is defined as the third point of intersection of the line PQ and the curve, and $P+Q$ is defined as the reflection of $P*Q$ over the line $y = \dfrac{2015}{2}$. More generally for all the curves we consider in this power round, this process of reflecting over the line of symmetry applies.

Definition 21. *Let E be an elliptic curve. Then $P + Q$ is the reflection of $P * Q$ over the horizontal line of symmetry of E.*

Consider now the elliptic curve $E : y^2 + y = x^3 - x$ and the point $P = (0, 0)$ on this curve. From this point on, we mostly refer to this curve and point P. It is the most important curve that we examine in order answer our question about prime density.

Problem 4.5 (E Symmetry; **2, 2**). *Let E be the elliptic curve $y^2 + y = x^3 - x$.*

a) For every point (a, b) on E, there is another point (a, c) on E as well. What is c?

b) There is the horizontal line of symmetry $y = \alpha$ for this curve E. What is α?

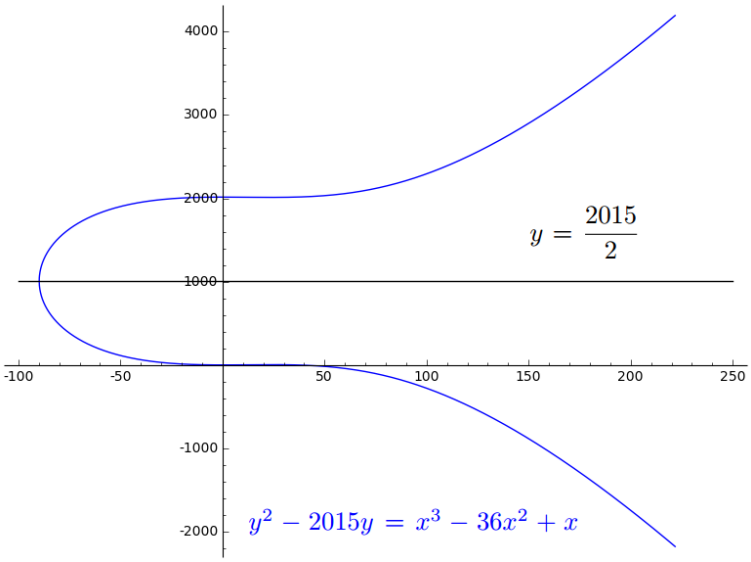

Figure 3: Horizontal Line of Symmetry.

Proof.

a) Given b, it's clear that $c = -1 - b$.

b) This leads to $\alpha = \frac{-1}{2}$.

□

Now, remember that sequence we mentioned in the introduction? Recall that the Somos-4 sequence $\{a_n\}$ is defined by $a_0 = a_1 = a_2 = a_3 = 1$ and recursively by $a_n a_{n-4} = a_{n-1}a_{n-3} + a_{n-2}^2$. You'll get to prove some facts about this sequence later. This following problem should keep you occupied with it until then. Keep in mind that we fixed a curve E and point P above. One fact about E and P is that $P + P = (1, 0)$ (for the interested, adding a point to itself requires the use of a tangent line; learn calculus!).

Problem 4.6 (Sequence and Curve; **10**). *Prove for $n > 1$ that $(2n-3)P = \left(\frac{f(n)}{a_n^2}, \frac{g(n)}{a_n^3}\right)$ where $f(n) = a_n^2 - a_{n-1}a_{n+1}$ and $g(n) = a_{n-1}^2 a_{n+2} - 2a_{n-1}a_n a_{n+1}$. (Recall from section 3, the group theory section, that $kP = \sum_{i=1}^{k} P$.)*

Proof. When $n = 1$, $(2n-3)P = -P$. Given that the line of symmetry of this curve is $y = -1/2$, $-P = (0, -1)$. Checking the base case, we find $\left(\frac{1^2 - 1 \cdot 1}{1^2}, \frac{1^2 \cdot 1 - 2 \cdot 1 \cdot 1 \cdot 1}{1^3}\right) = (0, -1)$ as desired; thus the case $n = 1$ is true.

Now suppose for the sake of induction that for some $k \in \mathbb{N}$, for all $n \geq k$, our claim is true. Then $(2k-3)P = \left(\frac{a_k^2 - a_{k-1}a_{k+1}}{a_k^2}, \frac{a_{k-1}^2 a_{k+2} - 2a_{k-1}a_k a_{k+1}}{a_k^3}\right)$. Let $Q = 2P = (1, 0)$ as given. Thus we may directly add $(2k-3)P + 2P = (2(k+1) - 3)P$, and check that the equations do match.

Adding the points is very straightforward using the following lemma: Let $\{a_{k-1}, a_k, a_{k+1}, a_{k+2}\}$ be any four consecutive elements of our sequence. Then $a_{k-1}^2 a_{k+2}^2 - 4a_{k-1}a_k a_{k+1}a_{k+2} + a_{k-1}a_{k+1}^3 + a_k^3 a_{k+2} + a_k^2 a_{k+1}^2 = 0$. (This is easily verified through standard induction, and by substitution for larger terms. In fact, we may find $\frac{a_{k+3}}{a_{k-1}} \cdot (a_{k-1}^2 a_{k+2}^2 - 4a_{k-1}a_k a_{k+1}a_{k+2} + a_{k-1}a_{k+1}^3 + a_k^3 a_{k+2} + a_k^2 a_{k+1}^2) = a_k^2 a_{k+3}^2 - 4a_k a_{k+1}a_{k+2}a_{k+3} + a_k a_{k+2}^3 + a_{k+1}^3 a_{k+3} + a_{k+1}^2 a_{k+2}^2$.

We present a general method of solving for the x-coordinate. Note that we may create an equation of the line with points $(2k-3)P$ and $Q = 2P$. Let this be equation $y = mx+b$. Secondly, we have the equation for the line $y^2 + y = x^3 - x$. Substituting, $m^2x^2 + 2mbx + b^2 + mx + b = x^3 - x$. By Vieta's formulas, the sum of the three solutions in x is $-m^2$. We know two solutions already, 1 from $2P = (1, 0)$ and $(\frac{a_k^2 - a_{k-1}a_{k+1}}{a_k^2}$ from $(2k-3)P$. Thus the third solution, $x((2k-1)P)$, is $-m^2$ minus these. (Simplification of this using the above lemma shows us the x-coordinate is exactly as we desired. Similar algebraic substitutions show the y-coordinates match as well.

Thus the inductive step holds, and therefore the formula holds for all $n \in \mathbb{N}$ as desired. □

5 Sequences

So we turn now to the Somos-4 sequence again. A priori, we know nothing about this sequence. From the definition, it's not even clear that it's integral! (Hint: it is). As reference, here are some of the first few values starting with a_0: 1, 1, 1, 1, 2, 3, 7, 23, 59, 314, $\cdots$. Well, that is royally unhelpful. Let's try to get our hands dirty working with these types of non-linear recurrences. Note by the recursive definition of the Somos-4 sequence that we may define terms of the sequence for negative n. For example, $a_{-1}a_3 = a_0a_2 + a_1^2$ gives a way to define a_{-1}. This may be necessary for you to establish base cases.

Definition 22. *For $n \in \mathbb{N}$, define $s_n := a_{n-3}a_{n+3} - a_{n-2}a_{n+2}$.*

As it turns out, this new sequence of numbers is intimately related to the Somos-4 sequence, which may help us prove integrality.

Problem 5.1 (Secondary Sequence; **5, 2**)**.**

a) Prove that $a_n^2 s_{n-1} = a_{n-1}^2 s_n$ for $n \in \mathbb{N}$.

b) Prove that $s_n = 4a_n^2$ for $n \in \mathbb{N}$.

Proof.

1. This is a purely arithmetic fact. Most derivations all likely involve two instances of substitutions of s_k and $a_k a_{k-4} = a_{k-3}a_{k-1} + a_{k-2}^2$. One example is shown where the substituted parts are underlined:

$$\begin{aligned}
a_n^2\underline{s_{n-1}} &= a_{n-1}^2\underline{s_n} \\
a_{n-4}a_n^2a_{n+2} - a_{n-3}a_n^2a_{n+1} &= a_{n-3}a_{n-1}^2a_{n+3} - a_{n-2}a_{n-1}^2a_{n+2} \\
a_{n+2}(\underline{a_{n-4}a_n^2} + a_{n-2}a_{n-1}^2) &= a_{n-3}(\underline{a_{n-1}^2a_{n+3}} + a_n^2a_{n+1}) \\
a_{n+2}(a_n(a_{n-1}a_{n-3} + a_{n-2}^2) + a_{n-2}a_{n-1}^2) &= a_{n-3}(a_{n-1}(a_na_{n+2} + a_{n+1}^2) + a_n^2a_{n+1}) \\
a_{n-3}a_{n-1}a_na_{n+2} + a_{n-2}^2a_na_{n+2} + a_{n-2}a_{n-1}^2a_{n+2} &= a_{n-3}a_{n-1}a_na_{n+2} + a_{n-3}a_n^2a_{n+1} + a_{n-3}a_{n-1}a_{n+1}^2 \\
a_{n-2}a_{n+1}(\underline{a_{n-2}a_n + a_{n-1}^2}) &= a_{n-3}a_{n+1}(\underline{a_{n-1}a_{n+1}a_n^2}) \\
a_{n-3}a_{n-2}a_{n+1}a_{n+2} &= a_{n-3}a_{n-2}a_{n+1}a_{n+2}.
\end{aligned}$$

2. This is true by induction. The base cases are easy. Then using the previous part a) above for the inductive step, note that

$$s_n = 4a_n^2 \iff \frac{a_n^2 s_{n-1}}{a_{n-1}^2} = 4a_n^2.$$

□

Problem 5.2 (Is Integral; **10**)**.** *Prove that a_n is integral for $n \in \mathbb{N}$ and that the following are true,* $\gcd(a_n, a_{n-1}) = \gcd(a_n, a_{n-2}) = 1$.

Proof. The main idea of this proof is the following. We induct on a_{k+3} for some k. For some x and y where $(x, y) = 1$, we show that both $a_{k+3}x$ and $a_{k+3}y$ are both integers. By Bezout's lemma, this means there exist some integers r and s such that $rx + sy = 1 \implies rxa_{k+3} + sya_{k+3} = a_{k+3}$. So this implies a_{k+3} is an integer. Separately, we induct to prove the coprimeness condition using the fact that for integers a and b such that $(a, b) = 1$, both $(a + b, b) = (a, a + b) = 1$.

The first few base cases are easily checked for both integrality and coprimeness. We induct on some $k \in \mathbb{N}$ such that for all $n \leq k+2$, both a_n is an integer and $(a_n, a_{n-1}) = (a_n, a_{n-2}) = 1$. Then by the definition of the sequence and the previous problem, note that

$$a_{k+3}a_{k-3} = 4a_k^2 + a_{k-2}a_{k+2},$$
$$a_{k+3}a_{k-1} = a_{k+2}a_k + a_{k+1}^2.$$

By the inductive hypothesis, the right sides of both equations are integers, and so both $a_{k+3}a_{k-3}$ and $a_{k+3}a_{k-1}$ are integers. Furthermore by the inductive hypothesis, we know $(a_{k-3}, a_{k-1}) = 1$, and so by Bezout's lemma, we have that for some integers r and s that

$$ra_{k-3} + sa_{k-1} = 1 \implies a_{k+3} = ra_{k-3}a_{k+3} + sa_{k+3}a_{k-1},$$

and a_{k+3} is an integer as desired.

To check the coprime condition, we again induct to show that a_{k+3} is coprime to the two previous terms. Note that by the inductive hypothesis, $(a_{k+2}a_k, a_{k+1}^2) = 1$. This implies

$$(a_{k-1}a_{k+3}, a_{k+1}^2) = (a_{k+2}a_k + a_{k+1}^2, a_{k+1}^2) = 1 \implies (a_{k+3}, a_{k+1}) = 1.$$

Adding the other way shows that $(a_{k+1}^2, a_k a_{k+2}) = 1$, which shows $(a_{k+3}, a_{k+1}) = 1$ as desired. Thus by induction the coprime condition holds as well. □

Because there are so many ways to create a recursive sequence, there aren't really centralized strategies for dealing with them in much generality. But maybe this set of problems was interesting. As a parting shot, here are few more problems.

Problem 5.3 (Sequence Divisibility; **5**). *We define a recursive sequence $\{b_n\}$ by $b_0 = b_1 = b_2 = 1$ and for $n \geq 3$, $b_n = b_{n-1}b_{n-2} + b_{n-3}$. Prove that for all integers $n > 1$, there exists a $k \geq 0$ such that $n | b_k$.*

Proof. First let's fix $n > 1$ and consider the function $f : (\mathbb{Z}/n\mathbb{Z})^3 \to (\mathbb{Z}/n\mathbb{Z})^3$ which maps $(x, y, z) \mapsto (y, z, yz + x)$. This is an injective function because $f(x, y, z) = (0, 0, 0) \implies x = y = z = 0$ and it is surjective because for any $(x, y, z) \in (\mathbb{Z}/n\mathbb{Z})^3$, we have $f(z - xy, x, y) = (x, y, z)$. So this is a bijective function from $(\mathbb{Z}/n\mathbb{Z})^3$ to itself and since there are only a finite number of pairs (x, y, z) mod n, the function f is a permutation of the elements.

The special part of the function is that it corresponds with our recurrence relation with $f(b_i, b_{i+1}, b_{i+2}) = (b_{i+1}, b_{i+2}, b_{i+3})$. Now denote $f^k(x, y, z)$ to be the result by applying f k times to (x, y, z) with the convention that f^0 is the identity. Considering the sequence fo triplets $f^0(1, 1, 1), f^1(1, 1, 1), f^2(1, 1, 1), \ldots$, since there are only a finite number of values f can take on and this is an infinite sequence, we know that $\exists i < j$: $f^i(1, 1, 1) = f^j(1, 1, 1)$ and since f is bijective, it has an inverse so $f^{-i}f^i(1, 1, 1) = f^{-i}f^j(1, 1, 1) \implies (1, 1, 1) = f^{j-i}(1, 1, 1)$ for some $j - i > 0$. But now we are done because we can see that $f(0, 1, 1) = (1, 1, 1)$ and since f is injective, we have that $f^{j-i-1}(1, 1, 1) = (0, 1, 1)$ but $f^{j-i-1}(1, 1, 1) = (b_{j-i-1}, b_{j-i}, b_{j-i+1})$ and hence $b_{j-i-1} \equiv 0 \pmod{n}$ or $n \mid b_{j-i-1}$ with $j - i - 1 \geq 0$.

□

Problem 5.4 (Integrality, Integrality!; **8, 12**).

a) *We define a recursive sequence $\{c_n\}$ by $c_0 = c_1 = c_2 = c_3 = c_4 = 1$ and for $n \geq 5$, $c_n c_{n-5} = c_{n-4}c_{n-1} + c_{n-2}c_{n-3}$. Prove that this sequence is integral for $n \geq 0$.*

b) *We define a recursive sequence $\{d_n\}$ by $d_0 = 1$, $d_1 = 2$, $d_2 = 1$, and $d_3 = -3$ and for $n \geq 4$,*

$$d_n = \begin{cases} \dfrac{d_{n-1}d_{n-3} - d_{n-2}^2}{d_{n-4}} & \text{if } n \equiv 0, 1 \pmod 3 \\ \dfrac{d_{n-1}d_{n-3} - 3d_{n-2}^2}{d_{n-4}} & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Prove that the sequence $\{d_n\}$ is an integral sequence for $n \geq 0$.

Proof.

a) The proof of this is very similar to the proof of the Somos-4 sequence. The main difference is that we use $s'_n := c_n^2 + c_{n-2}c_{n+2}$ which gives $c_{n-3}s'_n = c_{n+1}s'_{n-2}$, which by corollary gives $s_n := -2c_{n-1}c_{n+1}$ if n is even and $s_n = 3c_{n-1}c_{n+1}$ if n is odd, and the rest of the proof is nearly identical. A full proof is given at http://www.maths.ed.ac.uk/ mwemyss/Somos5proof.pdf with all due credit to its authors.

b) The flavor of proof is identical to that of the problem above and the outline of the Somos-4 sequence. A full proof is attached in Appendix A

□

6 Interlude

As the reader may have noticed by now, this Power Round is a rather eclectic collection of math topics. The following rephrases our previous work into a form we may use later.

We introduce projective space, specifically projective 2-space, denoted $\mathbb{P}^2(\mathbb{R})$ (this means that coordinates are elements of $\mathbb{R}$; we can also work instead in $P^2(\mathbb{Q})$, but that is not necessary). The motivation of such a system of numbers is hard to flesh out fully here. (For the interested reader, consider this system as an attempt to fix the "problem" that two parallel lines do not intersect by adding points at infinity. For the artists out there, this is a formalization of the concept of perspective drawings in which parallel lines do in fact converge. Unfortunately, the implementation we present here may not make it clear why these things are true.)

Elements of $\mathbb{P}^2(\mathbb{R})$ represent the lines in $\mathbb{R}^3$, real 3-space, that pass through the origin. Examine such a line ℓ that passes through the origin $(0,0,0)$. We represent ℓ by a triplet of coordinates $(a:b:c)$ where ℓ passes through points $(0,0,0)$ and (a,b,c). This clearly doesn't give a unique representation of ℓ. Under this representation, for all real numbers s, $(sa:sb:sc)$ and $(a:b:c)$ will always represent the same line. For example, if ℓ is a line that passes through $(0,0,0)$ and $(2,4,3)$, then we can denote this line in $P^2(\mathbb{R})$ in many ways: $(2:4:3) \cong (4:8:6) \cong (\pi : 2\pi : \frac{3\pi}{2})$, and so forth. When possible, it is convention to standardize the way we represent these vectors by making the last coordinate 1; thus if $c \neq 0$, then $(a:b:c) = (\frac{a}{c} : \frac{b}{c} : 1)$, and the latter is the preferred form.

Definition 23. *Let $\mathbb{P}^2(\mathbb{R})$ represent projective 2-space. Then elements $\alpha \in \mathbb{P}^2(\mathbb{R})$ are represented as $\alpha = (a:b:c)$ where if $c \neq 0$, we may assume $c = 1$.*

The reason we introduce this space is because it is in some sense the "correct" medium in which to examine elliptic curves.

Definition 24. *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve. Denote another curve in three variables (adding z) as $F : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$. We say that F has been homogenized because each term has the same degree (degree is the sum of the powers of all variables). F is an elliptic curve in $\mathbb{P}^2(\mathbb{R})$.*

By the three variables given by homogenization, we can start to look at F as a curve lying in projective 2-space. It's clear that if (a,b) is a solution to E, then $(a:b:1)$ is a solution to F. We may say more.

Proposition 25. *There is a bijective correspondence between an elliptic curve E and a homogenized F with a further bijective correspondence between points on E and F.*

We check this by proof by example! (Note this is not actually a proof. Never actually do this, but this example should illustrate clearly why this proposition is true.) Examine the elliptic curve $E : y^2 = x^3 - 20x - 15$ again. Then the homogenization is $F : y^2z = x^3 - 20xz^2 - 15z^3$. Since $(-4,1)$ is a solution to E, we see $(-4:1:1)$ is clearly a solution to F. Conversely note $(1284:-5601:64)$ is a solution to F (you may way want to check this). Then it is clear $\left(\frac{321}{16} : \frac{-5601}{64} : 1\right)$ is also a solution to F, and so $\left(\frac{321}{16}, \frac{-5601}{64}\right)$ is a solution to E. Note the importance of homogenization in this work. For example, what would have failed if F were made by simply multiplying every term by exactly one factor z?

And finally, here is why we needed projective space: how do we look at elliptic curves over a finite field? An example of a finite field is $\mathbb{F}_p$ (you know enough to verify that is indeed a field). Fields are explored more thoroughly in section 7.

Definition 26. *Let K be a ring. Furthermore let K also have the additional property that for all non-zero elements a, $\exists a^{-1} \in K$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Then K is called a field.*

Perhaps it is unclear here why we would want to look at elliptic curves over $\mathbb{F}_p$, but you'll see why soon enough. So, is there a notion of an elliptic curve over $\mathbb{F}_p$ where p is a prime? In case you haven't noticed by now how these rhetorical questions go... Yes! There is. Suppose $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ is an elliptic curve with integer coefficients. We can look at points in $E/\mathbb{F}_p$ (read E over $\mathbb{F}_p$ meaning that we take E as an equation and points on E all inside $\mathbb{F}_p$) in two ways: by solving E in $\mathbb{F}_p$ from the start, or by reducing points from $E/\mathbb{Q}$. The first is easy to do: simply solve $E : y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$.

Problem 6.1 (EC over Finite Field; **5**). *Let $E : y^2 = x^3 + 3x + 9$ be an elliptic curve over $\mathbb{F}_{13}$. Find all the elements of $E(\mathbb{F}_{13})$. (Hint: there are 14 total elements. You may have to read on first to find the identity element.)*

Proof. It is sufficient to give a list of all of them. As given later in this section, the identity element is $(0 : 1 : 0)$. Every other element $(a : b : c)$ has $c = 1$ as usual, thus we simply solve $y^2 \equiv x^3 + 3x + 9 \pmod{13}$. There are 13 solutions here. Thus the total list of solutions is $\{(0 : 1 : 0), (0 : 3 : 1), (0 : 10 : 1), (1 : 0 : 1), (2 : 6 : 1), (2 : 7 : 1), (6 : 3 : 1), (6 : 10 : 1), (7 : 3 : 1), (7 : 10 : 1), (8 : 5 : 1), (8 : 8 : 1), (10 : 5 : 1), (10 : 8 : 1)\}$. □

Otherwise, we can find points on E over finite fields by mapping rational points of E over $\mathbb{Q}$ by the "obvious" mapping to try. Suppose that $(\frac{a}{b}, \frac{c}{d}) \in E(\mathbb{Q})$ is a rational point on E. We look at the reduction of E onto $\mathbb{F}_p$ by first translating to projective space; this point naturally maps to $(ad : bc : bd)$. Here in projective space, we divide by any powers of p necessary such that $\gcd(ad/p^k, bc/p^k, bd/p^k) = 1$ (else the point would vanish trivially over $\mathbb{F}_p$). Finally we translate into $\mathbb{F}_p$ by taking these coordinates modulo p. Thus in summary, $\left(\frac{a}{b}, \frac{c}{d}\right) \mapsto (ad \pmod{p}, bc \pmod{p}, bd \pmod{p})$, modulo some conditions on clearing denominators with powers of p.

As promised before, we can now present the identity of the group $E(\mathbb{Q})$: it's $(0 : 1 : 0)$. This furthermore shows that the identity of $E(\mathbb{F}_p)$ is also $(0 : 1 : 0)$. This gives us the following corollary (corollary of what I wonder...)

Problem 6.2 (An Odd Divisor; **5**). *Let p be a prime. Prove p divides some term of the Somos-4 sequence $\{a_n\}$ if and only if $P = (0, 0)$ has odd order in the group $E(\mathbb{F}_p)$ where $E : y^2 + y = x^3 - x$.*

Proof. This is a corollary of problems 4.6 and 5.2.

($\Rightarrow$) Suppose $p | a_n$ for some $n \geq 1$, and then note that $(2n-3)P = \left(\frac{a_n^2 - a_{n-1}a_{n+1}}{a_n^2}, \frac{a_{n-1}^2 a_{n+2} - 2a_{n-1}a_n a_{n+1}}{a_n^3}\right)$. Note that the side-results of problem 5.2 show that the denominators and numbers of the x and y-coordinates of $(2n-3)P$ as written are coprime. Therefore, $(2n-3)P \pmod{p} = \left(a_n(a_n^2 - a_{n-1}a_{n+1}) : a_{n-1}^2 a_{n+2} - 2a_{n-1}a_n a_{n+1} : a_n^3\right) \equiv (0 : 1 : 0) \pmod{p}$. Therefore, note an odd multiple of P equals the identity; thus P has odd order.

($\Leftarrow$) Secondly if $kP = (0 : 1 : 0) \pmod{p}$ where k is odd, then $(2 \cdot (\frac{k+3}{2}) - 3)P = (0 : 1 : 0)$, and $p | a_{(k+3)/2}$. □

This is a rather magical connection between divisibility of a sequence and elliptic curves, don't you think? However, strangely enough, we will soon be able to make even weirder equivalent statements.

7 Galois Theory

Unfortunately, for the sake of time (we can't build up all of Galois theory from scratch for this Power Round!), we won't be able to give more than a heuristic of some of the methods we use here. (Un)Luckily for you, the reader, this also means there aren't many problems directly on Galois theory :(. We hope that regardless of your mathematical background, this section is still interesting enough to try to understand. We describe first some of the necessary groundwork.

We previously introduced a fundamental object of algebra: groups. This was essentially the most basic "thing" we could do math on. We have only one operation on a group at all times. Anything simpler would have *very* little to it. Since then, we further saw a taste of more complicated algebraic objects, which as promised, we explore here. One step up from the group is another essential object of mathematics: a ring. Rings in some sense can be thought of as an extension of (additive) groups.

Definition 27. *Let R be a set of elements that has a closed, binary operation we call addition such that $\{R, +\}$ is an additive, commutative group and a second closed, binary, commutative operation $\cdot$ that we can call multiplication. Suppose R has these properties:*

- *The operation $\cdot$ is associative.*
- *For all $a, b, c \in R$,*
$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
and
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$
- *Finally, there exists a multiplicative identity we call 1 such that for all $a \in R$, $a \cdot 1 = 1 \cdot a = a$.*

Then R is called a ring.

The consequences of such a definition is that R contains 0 (necessary by the addition law), and 1 (necessary by the multiplication law). Many definitions also add that $1 \neq 0$, but this is not strictly necessary.

Problem 7.1 (0 Ring; **5**). *Let $A := \{0\}$ be the set of just the element 0. Let $+$ and $\cdot$ be operations on A such that $0 + 0 = 0 \cdot 0 = 0$. Prove or disprove that A is a ring.*

Proof. Note that A is a set of elements that has a closed, binary operation labelled $+$. Verifying every condition of rings boils down to the fact that for all $a \in A$, $a = 0$, and so any operation evaluations to 0. For example, $0 + 0 = 0$ is indeed commuatative, $0 \cdot (0 \cdot 0) = (0 \cdot 0) \cdot 0 = 0$, etc. Thus every property holds, and this ring, the trivial ring, is indeed a ring. □

If you find the definition of rings a little scary looking, all it really says is that a ring is something like the integers $\mathbb{Z}$. (Mathematicians have this tendency of taking familiar objects like the integers and building abstractions of them. If you see one of these abstractions first, they can seem intimidating. But, if you know where the abstraction came from, you might see that it is quite natural. Rings are one example of this.) However, if you recall from the exercises in section 3, the integers are missing something. This leads us to something else called a field.

Definition 28. *Let K be a ring where $1 \neq 0$. Furthermore let K also have the additional property that for all non-zero elements a, $\exists a^{-1} \in K$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Then K is called a field.*

Again, this is an example of an abstraction of a natural object. A field really emulates the properties of the rational numbers $\mathbb{Q}$. In the same way $\mathbb{Q}$ is built from $\mathbb{Z}$, fields are built from rings. Also, note the relationship between rings and fields. A field is always a ring, but not the other way around.

There are many examples of fields. While $\mathbb{Q}$ may have been a motivating example for the abstraction for a field (history fun fact: I have no idea if this is true. I made it up because this might be true...), fields are so common that you probably already know many other examples. A few more examples of fields are the real numbers $\mathbb{R}$; the complex numbers $\mathbb{C}$; and finite fields $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Something of interest is that the rational numbers are a subset of the real numbers; we write this $\mathbb{Q} \subset \mathbb{R}$ and say that $\mathbb{Q}$ is a sub-field of $\mathbb{R}$; equivalently, we also say that $\mathbb{R}$ is a field extension of $\mathbb{Q}$. Another example is $\mathbb{R} \subset \mathbb{C}$. We can say much more about the relationships between fields than characterizing them as subsets of each other.

The only thing that $\mathbb{R}$ really lacks compared to $\mathbb{C}$ is the number i. Every complex number is the combination of a real part and an imaginary part. This gives us another way to construct $\mathbb{C}$. We may write $\mathbb{C} \cong \mathbb{R}[i]$. This notation $\mathbb{R}[i]$ means we take the set of real numbers $\mathbb{R}$, and also add in the element i. We can then take any finite sum of scalar multiples of powers of i. More formally,

$$\mathbb{R}[i] := \{c_0 + c_1 \cdot i + c_2 \cdot i^2 + c_3 \cdot i^3 + c_4 \cdot i^4 + \cdots + c_n \cdot i^n : n \in \mathbb{N}, c_i \in \mathbb{R}\}.$$

Notice that since $i^2 = -1 \cdot i^0$, any power of i greater than 1 may be re-written as a power less than 2. Thus in practice, we may also write $\mathbb{R}[i] = \{c_0 + c_1 \cdot i : c_i \in \mathbb{R}\}$. This shows us why we call $\mathbb{R}$ a field extension of $\mathbb{Q}$—we build the former by literally adding things to the latter.

In general, if R is a ring, $R[\alpha]$ is defined similarly.

Definition 29. *Let R be an arbitrary ring. If α is algebraic over R, then $R[\alpha] := \{\sum_{i=0}^{n} c_i \alpha^i : n \in \mathbb{N}, c_i \in R\}$.*

There are some conditions necessary on the value of α—namely that α be algebraic. However, algebraic numbers are something we do not address here (for interested readers, this is what transcendental numbers pertain to). Now to make sure things make sense so far, here is a problem.

Problem 7.2 (Fields; **4, 2, 2, 4**).

a) *Examine $\mathbb{Q}[\sqrt{2}]$. Setwise, are $\mathbb{Q}[\sqrt{2}]$ and $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ equivalent? Why or why not? (Keep in mind the justification of $\mathbb{R}[i] = \{c_0 + c_1 \cdot i : c_i \in \mathbb{R}\}$ was not fully fleshed out. You must start with an arbitrary maximum degree n and reduce it to 1.)*

b) *Is $\frac{1}{8}$ inside $\mathbb{Z}[\frac{1}{2}]$? Why or why not?*

c) *Is $\frac{1}{3}$ inside of $\mathbb{Z}[\frac{1}{6}]$? Why or why not?*

d) *Are $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ equivalent? (Two fields are equivalent if they are setwise equivalent; i.e. K and F are equivalent fields if $K \subset F$ and $F \subset K$.) Why or why not?*

Proof. a) Yes, they are equivalent. It's clear that $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subset \mathbb{Q}[\sqrt{2}]$ by definition since we basically just take the first two terms of the infinite sum. To see the other direction, take an arbitrary element of $\mathbb{Q}[\sqrt{2}]$, $\alpha = \sum_{i=0}^{N} a_i \cdot \sqrt{2}^i$ for $c_i \in \mathbb{Q}$. Note that when i is even, we get a rational number for the term. Thus we re-write α as

$$\begin{aligned}
\alpha &= \sum_{i=0}^{N} a_i \cdot \sqrt{2}^i \\
&= \sum_{\substack{i=0 \\ i \text{ even}}}^{N} a_i \cdot 2^{i/2} + \sum_{\substack{i=0 \\ i \text{ odd}}}^{N} a_i \cdot 2^{\frac{i-1}{2}} \sqrt{2} \\
&= \left(\sum_{\substack{i=0 \\ i \text{ even}}}^{N} a_i \cdot 2^{i/2} \right) + \left(\sum_{\substack{i=0 \\ i \text{ odd}}}^{N} a_i \cdot 2^{\frac{i-1}{2}} \right) \sqrt{2}.
\end{aligned}$$

So we see that every element of $\mathbb{Q}[\sqrt{2}]$ is also an element of $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, and so they are equivalent.

b) Yes. By definition, $\frac{1}{8} = 0 \cdot 1 + 0 \cdot \frac{1}{2} + 0 \cdot \frac{1}{4} + 1 \cdot \frac{1}{8}$ is inside $\mathbb{Z}[\frac{1}{2}]$.

c) Yes. Yup, by definition, $\frac{1}{6} = 0 \cdot 1 + 2 \cdot \frac{1}{6}$ is inside $\mathbb{Z}[\frac{1}{6}]$.

d) No. We saw that every element of $\mathbb{Q}[\sqrt{2}]$ can be written as $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$. So it suffices to show that $\sqrt{3}$ cannot be written in this form. This is clear by writing $\sqrt{3} = a + b\sqrt{2}$, and squaring both sides to find a contradiction to that $\sqrt{2}$ is irrational.

□

Finally, a more "professional" way to think about $\mathbb{R}[i] \cong \mathbb{C}$ comes from realizing that i is a root of the polynomial $x^2 + 1$. Notice that the two roots of $x^2 + 1$ are $\pm i$. This leads to the construction denoted $\mathbb{R}[x]/(x^2 + 1)$, which we take to mean that we adjoin to $\mathbb{R}$ a root of the polynomial $x^2 + 1$ (it doesn't matter if we take i or $-i$ since they give equivalent fields). In this case, adjoining to $\mathbb{R}$ a root of $x^2 + 1$ is exactly the same as adjoining i. Thus we now have three ways of representing the complex numbers: $\mathbb{C} \cong \mathbb{R}[i] \cong \mathbb{R}[x]/(x^2 + 1)$. This latter notation is most important for us. It demonstrates a way of thinking about field extensions: adjoining roots of polynomials. This leads naturally to the concept of Galois groups.

Definition 30. *For certain rational polynomials $f(x)$, the details of which we omit for the sake of time, $\mathbb{Q}[x]/(f(x))$ is called a Galois extension.*

(The specifics of what polynomials are necessary is omitted. They involve definitions which are unnecessary in the scheme of this Power Round, but specific polynomials make their field extensions Galois.) Examine all the roots of $f(x)$ that exist in this new field K but don't exist in $\mathbb{Q}$. We can form a group (of functions) that acts on these roots by sending them to each other. For example, for the construction $\mathbb{Q}[x]/(x^2 + 1)$, we can imagine a function that sends i to $-i$ and vice versa (this is conjugation). The important thing about conjugation is that it sends rational numbers to rational numbers: it fixes elements that were in the base field. We assert that conjugation and the "do nothing" function (the identity function) are the only such functions that exist. They act on $\mathbb{Q}[x]/(x^2 + 1)$ but are the identity function when restricted to $\mathbb{Q}$. Thus our group of functions has two elements: the conjugation function, and the identity function. We encourage the reader to convince themself that this small thing is indeed a group. In general, this group that we construct of functions is known as the Galois group of the field extension.

Definition 31. *Suppose $K = \mathbb{Q}[x]/(f(x))$ is a Galois extension. Then $\sigma : K \to K$ is a Galois automorphism if the following hold:*

- *If $a \in \mathbb{Q}$, $\sigma(a) = a$ (this is called "fixing a").*
- *Let $A = \{r \in K, r \notin \mathbb{Q} : f(r) = 0\}$. Then $\sigma : A \to A$ is a bijection.*
- *If α, β are two elements of K, then $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ and $\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta)$.*

Definition 32. *Let G be the set of all Galois automorphisms of a field extension K of $\mathbb{Q}$. Then G is a group that is denoted $\mathrm{Gal}(K/\mathbb{Q})$ and called the Galois group of K.*

In practice, to form a Galois automorphism, focus first on the second condition. If you impose conditions on where the roots are sent and let rational numbers remain unchanged, the other properties tend to work out as well.

Problem 7.3 (Galois Automorphisms; **2, 8**). *Let* $f(x) = x^4 - 70x^2 + 25$.

a) *What are the roots of* $f(x)$*?*

b) *You are given that* $f(x)$ *is a nice enough polynomial that* $\mathbb{Q}[x]/(f(x))$ *is a Galois. Give four examples of Galois automorphisms—an isomorphism from one set to itself. (You may just tell us where each root is sent for each automorphism).*

Proof. a) We have that the roots of f are $\sqrt{20}+\sqrt{15}$, $\sqrt{20}-\sqrt{15}$, $-\sqrt{20}+\sqrt{15}$, and $\sqrt{20}-\sqrt{15}$.

b) Let $\alpha = \sqrt{20}+\sqrt{15}$, and $\beta = \sqrt{20}-\sqrt{15}$, here are all of them:

$$\sigma_1(\alpha, -\alpha, \beta, -\beta) \mapsto (\alpha, -\alpha, \beta, -\beta),$$

$$\sigma_2(\alpha, -\alpha, \beta, -\beta) \mapsto (-\alpha, \alpha, -\beta, \beta),$$

$$\sigma_3(\alpha, -\alpha, \beta, -\beta) \mapsto (\beta, -\beta, \alpha, -\alpha),$$

$$\sigma_4(\alpha, -\alpha, \beta, -\beta) \mapsto (-\beta, \beta, -\alpha, \alpha).$$

The motivation for this comes from our example of $\mathbb{Q}[i]$. A very natural thing to try is sending $i \mapsto -i$. If we try a similar method here, we may guess and check how the signs flip.

□

Before moving on though, we can go even further than what we have done here; we can adjoin multiple roots of many different polynomials at once to $\mathbb{Q}$. For example, a classic example you may see if you study mathematics more is adjoining to $\mathbb{Q}$ the roots of both x^2+x+1 and x^3-2 at the same time to yield $\mathbb{Q}[\omega, \sqrt[3]{2}]$ for ω a primitive 3rd root of unity.

8 Elliptic Curves and Galois Theory

Galois theory is incredibly rich, but unfortunately there are details we must omit about the subject for the sake of time, and this is sufficient background; we can now relate Galois theory and elliptic curves. Suppose you have a general elliptic curve E and a general point P on it. We define a k-division point of P as some point Q on E such that $kQ = P$. A fact of elliptic curves is that there are exactly k^2 such k-division points in $\mathbb{C}$ (the coordinates of Q may be complex numbers), but likely many of them won't be rational points. But examine for a moment such a non-rational point β_k such that $k\beta_k = P$. Suppose we take the x and y coordinates of β_k and adjoined them to $\mathbb{Q}$. What would we get? Going further, suppose we took all such β_{k_i} such that $k\beta_{k_i} = P$ and adjoined to $\mathbb{Q}$ all of the x and y coordinates of these division points. We get some large field extension we label K_k. This directly gives us a way to use Galois theory in a way that gives us information about our initial E and P.

Take on faith that $K_k/\mathbb{Q}$ is indeed a Galois extension, and examine some Galois automorphism σ of this extension; it acts on all these coordinates we just adjoined. Let (a, b) be one of the k-division points; then $\sigma((a, b)) = (\sigma(a), \sigma(b))$. Now we have a curious situation: we have found a Galois automorphism that acts on points on an elliptic curve! Weee.

That these Galois automorphisms act on the set of k-division points is important. Can you visualize how they are acting? These functions send coordinate pairs, essentially vectors, to other vectors. This is quite similar to how matrices act on vectors! In fact, this leads to what is called a Galois representation: a homomorphism from the Galois group to a linear algebra construct. Here we become guilty of omitting some details, but it would take too much work to present in full rigor. But please take these two propositions to be true.

Proposition 33. *Let $E : y^2 + y = x^3 - x$, $P = (0, 0)$, and let K_k be the field described above, namely the field extension of Q by adjoining all the coordinates of the k-division points of P. Then there is a surjective homomorphism from the Galois group $\mathrm{Gal}(K_k/\mathbb{Q})$ to $AGL_2(\mathbb{Z}/2^k\mathbb{Z}) = (\mathbb{Z}/2^k\mathbb{Z})^2 \rtimes GL_2(\mathbb{Z}/2^k\mathbb{Z})$. Denote this by $\varphi : \mathrm{Gal}(K_k/\mathbb{Q}) \to AGL_2(\mathbb{Z}/2^k\mathbb{Z})$.*

A quick word on notation here. We defined the semidirect product in Proposition 16, and here we see an example of one. For an element of such a group $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$, we will write it as $(\vec{v}, M)$ where $\vec{v} \in (\mathbb{Z}/2^k\mathbb{Z})^2$ and $M \in GL_2(\mathbb{Z}/2^k\mathbb{Z})$.

Proposition 34. *Let $E : y^2 + y = x^3 - x$ and $P = (0, 0)$ be a point on E. Let ℓ be a prime larger than 37. Then P has odd order in $E(\mathbb{F}_\ell)$, the reduction of the curve to this finite field, if and only if for all $k \in \mathbb{N}$, $\exists(\vec{v}, M) \in \mathrm{im}(\left[\frac{K_k/\mathbb{Q}}{\ell}\right]) \subset AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ such that $\vec{v}$ lies in the column space of $M - I$ (the column space of a matrix such as $(M - I)$ is the set $\{(M - I) \cdot \vec{v}, \vec{v} \in (\mathbb{Z}/2^k\mathbb{Z})^2\}$), where im is the image under the mapping defined in Proposition 33. (This symbol $\left[\frac{K_k/\mathbb{Q}}{\ell}\right]$ is called the Artin symbol, which we unfortunately do not have the time to define thoroughly. It is, however, a subset of $\mathrm{Gal}(K_k/\mathbb{Q})$. Hint: most important for you, the contestant, is Proposition 37.)*

Let's parse this last proposition; recall from the interlude that prime ℓ divides some term of the sequence if and only if P has odd order in $E(\mathbb{F}_\ell)$. We saw earlier as well in problem 3.6 that this happens if and only if for all integers i, there exists some element $\beta_i \in E(\mathbb{F}_\ell)$ such that $2^i \cdot \beta_i = P$. Finally, this condition is equivalent to the latter part of the above proposition. If you are familiar with Galois theory, as a hint of why this might be true, the fact that such a β_i exists implies that it is fixed by the Fröbenius automorphism. This leads to the fact that $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ acting on $(\mathbb{Z}/2^k\mathbb{Z})^2$ fixes some element $\vec{x}$. Thus $(\vec{v}, M)(\vec{x}) := M \cdot \vec{x} + \vec{v} = \vec{x} \implies (M - I)\vec{x} = -\vec{v}$. From here it's easy to see that $\vec{v} \in \mathrm{im}(M - I) \Leftrightarrow -\vec{v} \in \mathrm{im}(M - I)$.

Definition 35. *Let $(\vec{v}, M) \in AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ be an element of the affine general linear group. We call $(\vec{v}, M)$ a ruminative element if $\vec{v}$ is in the column space of $M - I$.*

For the observant reader, another way to describe this element $(\vec{v}, M)$ is to say that M fixes a vector $\vec{x} \in (\mathbb{Z}/2^k\mathbb{Z})^2$ where the action of $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ on $(\mathbb{Z}/2^k\mathbb{Z})^2$ is as described above.

Thus we have come from an original question about primes dividing terms of a sequence to a question about the column space of matrices. This latter is something that we can much more likely solve directly. (In general, this is a useful strategy. Linear algebra is a subject that is very well understood compared to other mathematical subjects. This is the motivation behind group representations, for example. In fact, that linear algebra is so well understood has given rise to the half-serious joke of dismissing a problem by saying, "it's just linear algebra!") For one final step before we try to use linear algebra to find a fraction, we present the Chebotarev Density Theorem.

Theorem 36. *Suppose $K/\mathbb{Q}$ is a Galois extension with $G := \mathrm{Gal}(K/\mathbb{Q})$ where $C \subset G$ is a conjugacy class of G. Define $\pi_C(x) := \#\{p \le x : p \text{ is a prime that is unramified in } K \text{ and } \left[\frac{K/\mathbb{Q}}{p}\right] = C\}$. Then*

$$\lim_{x\to\infty} \frac{\pi_C(x)}{\pi(x)} = \frac{|C|}{|G|}.$$

(The definition of unramified is unimportant for us. In our specific case, this equivalently means primes that are greater than 37.) As written, this doesn't seem to necessarily apply to anything we've written so far. However, one of the facts that we obscured in our presentation of the two propositions above is that the images of the Galois groups above are in fact images of conjugacy classes. The ultimate result of all of this is the following.

Proposition 37. *Let $\pi(x)$ denote the number of primes less than x, and let $\pi'(x)$ denote the number of primes less than x that divide some term of the Tiger sequence. Let S represent $\left[\frac{K_k/\mathbb{Q}}{\ell}\right]$, the conjugacy class inside $\mathrm{Gal}(K_k/\mathbb{Q})$ where the k was such that β_k such that $2^k \cdot \beta_k = P$. Let $S' := \mathrm{im}(S)$ and $AGL_2(\mathbb{Z}/2^k\mathbb{Z}) = \mathrm{im}(\mathrm{Gal}(K_k/\mathbb{Q}))$ represent the images under the homomorphism $\varphi : \mathrm{Gal}(K_k/\mathbb{Q}) \to AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ from above. Then*

$$\begin{aligned}\lim_{x\to\infty} \frac{\pi'(x)}{\pi(x)} &= \lim_{k\to\infty} \frac{|S|}{|\,\mathrm{Gal}(K_k/\mathbb{Q})|} \\ &= \lim_{k\to\infty} \frac{|S'|}{|AGL_2(\mathbb{Z}/2^k\mathbb{Z})|}.\end{aligned}$$

S here is equal to the Artin symbol of some prime number ℓ.

In other words, the final fraction we have to compute is the last expression in the proposition above. The best way to interpret S' in the above is that S' is the subset of $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ that consists of the ruminative elements.

Here is a final note on the previous two sections. We are not fully defining some definitions such as conjugacy classes and the Artin symbol. They are written here for full formality, but are not necessary for you the contestants to fully understand. The only part of the previous parts to take away is that S' is the subset of $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ of elements that are ruminative, and we may calculate the number of such elements. Hint: this interpretation is the only thing you have to take away from sections 7 and 8 in order to solve section 9.

9 Final Fraction

Thus we are only left with calculating the density! Here are the final steps.

Definition 38. *Let $v_p : \mathbb{Z} \to \mathbb{Z}$ be a function such that $v_p(n) = m$, where m is the exponent of p in the prime factorization of n. For example, $v_2(24) = 3$, $v_3(8) = 0$, and $v_5(-25) = 2$.*

Proposition 39. *Let $M \in \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ be a matrix such that $v_2(\det(M-I)) = r$. Then the number of elements in the column space of $M-I$ is 2^{2k-r}. (Two notes: we do not regard the cases where $\det(M-I) = 0$, and by definition, $\det(M-I)$ is reduced to be the integer n such that $0 \le n < 2^k$ and $n \equiv \det(M-I) \pmod{2^k}$ where $\det(M-I)$ is evaluated in $\mathbb{Z}$.)*

Problem 9.1 (Final Fraction; **10, 10, 10, 10**). *In all but the last sub-problem here, assume that k is a fixed positive integer and we examine elements of $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ or $GL_2(\mathbb{Z}/2^k\mathbb{Z})$ as the problem dictates. Vectors are arbitrary element $(\vec{v}, M) \in AGL_2(\mathbb{Z}/2^k\mathbb{Z})$.*

a) *Error notice: The problem originally stated here was incorrectly phrased. Due to the fact that we are sending out a revision so late, we are awarding everyone the full 10 points for this problem. The problem should have been Proposition 39, which you may assume is true.*

b) *Suppose that $a, b \in \mathbb{Z}/2\mathbb{Z}$, $c \in \mathbb{Z}/2^n\mathbb{Z}$, and $n \ge 2$. Prove the number of pairs $(\alpha, \beta) \in (\mathbb{Z}/2^n\mathbb{Z})^2$ with $\alpha\beta \equiv c \pmod{2^n}$ with $\alpha \equiv a \pmod 2$ and $\beta \equiv b \pmod 2$ is*

$$\begin{cases} 0 & ab \not\equiv c \pmod 2, \\ 2^{n-1} & ab \equiv 0 \pmod 2 \text{ and one of } a \text{ or } b \text{ is nonzero}, \\ (2-1)(v_2(c)-1)2^{n-1} & a \equiv b \equiv c \equiv 0 \pmod 2, c \not\equiv 0 \pmod{2^n}, \\ n2^{n-1} & a \equiv b \equiv c \equiv 0 \pmod 2, c \equiv 0 \pmod{2^n}. \end{cases}$$

c) *For $k \ge 1$, prove the number of matrices $M \in GL_2(\mathbb{Z}/2^k\mathbb{Z})$ with $\det(M-I) \equiv 0 \pmod{2^{k-1}}$ but with $\det(M-I) \not\equiv 0 \pmod{2^k}$ is*

$$\begin{cases} 2 & k = 1, \\ 3 \cdot 2^{3k-2} - 3 \cdot 2^{2k-1} & k \ge 2. \end{cases}$$

d) *Prove that the density of primes dividing a term of the Somos-4 sequence is $\frac{11}{21}$.*

We present the proofs separately. For part b), we may in fact prove a generalization of the problem for any prime ℓ.

Lemma 40 (Generalization of b)). *Suppose that $a, b \in \mathbb{Z}/\ell\mathbb{Z}$, $c \in \mathbb{Z}/\ell^n\mathbb{Z}$, and $n \ge 2$. Then, the number of pairs $(\alpha, \beta) \in (\mathbb{Z}/\ell^n\mathbb{Z})$ with $\alpha\beta \equiv c \pmod{\ell^n}$ with $\alpha \equiv a \pmod \ell$ and $\beta \equiv b \pmod \ell$ is*

$$\begin{cases} 0 & ab \not\equiv c \pmod \ell \\ \ell^{n-1} & ab \equiv c \pmod \ell \text{ and one of } a \text{ or } b \text{ is nonzero}. \\ (\ell-1)(v_\ell(c)-1)\ell^{n-1} & a \equiv b \equiv c \equiv 0 \pmod \ell, c \not\equiv 0 \pmod{\ell^n} \\ (n\ell - n - \ell + 2)\ell^{n-1} & a \equiv b \equiv c \equiv 0 \pmod \ell, c \equiv 0 \pmod{\ell^n}. \end{cases}$$

Proof. We count satisfactory solutions (α, β).

- It is clear that if (α, β) is a solution then $c \equiv \alpha\beta \equiv ab \pmod{\ell}$.
- If a or b is nonzero, then α or β is invertible. If α is invertible it suffices to solve $\beta \equiv \alpha^{-1}c \pmod{\ell^n}$. There are ℓ^{n-1} choices for α, and once α is chosen, β is fixed. Similarly, if β is invertible, there are ℓ^{n-1} solutions.
- If $c \neq 0$ suppose that $i = v_\ell(\alpha)$. Then, the congruence $\alpha\beta \equiv c \pmod{\ell^n}$ is equivalent to

$$\frac{\alpha}{\ell^i}\beta \equiv c' \pmod{\ell^{n-i}},$$

  where $c' \cdot \ell^i \equiv c \pmod{\ell^{n-i}}$. Then, α/ℓ^i is invertible, and hence we have

$$\beta \equiv c\left(\frac{\alpha}{\ell^i}\right)^{-1} \pmod{\ell^{n-i}}.$$

  There are $\ell^{n-i} - \ell^{n-i-1}$ choices for α and there are ℓ^i choices for β. Moreover, $1 \leq i \leq v_\ell(c) - 1$ and hence we have

$$\sum_{i=1}^{v_\ell(c)-1} (\ell-1)\ell^{n-1} = (\ell-1)(\mathrm{ord}_\ell(c) - 1)\ell^{n-1}.$$

- If $c = 0$, and $a = b = 0$ then all that we require is $v_\ell(\alpha) + v_\ell(\beta) \geq n$. The number of solutions is then

$$\begin{aligned}
&\sum_{k=1}^{n-1} \#\{\alpha : v_\ell(\alpha) = k\} \cdot \#\{\beta : \beta \equiv 0 \pmod{\ell^{n-k}}\} + \ell^{n-1} \\
&= \sum_{k=1}^{n-1} (\ell^{n-k} - \ell^{n-k-1}) \cdot \ell^k \\
&= \sum_{k=1}^{n-1} (\ell^n - \ell^{n-1}) + \ell^{n-1} \\
&= (n-1)(\ell-1)\ell^{n-1} + \ell^{n-1} = (n\ell - n - \ell + 2)\ell^{n-1}.
\end{aligned}$$

□

Secondly, here is a lemma necessary for the proof of 9.1*c*):

Lemma 41. *The number of $M \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for a prime ℓ such that $\det(M - I) = 0$ is $\ell^3 - 2\ell$.*

We do not present a full proof here, as it is unnecessary to prove in generality for our problem that only considers $\ell = 2$. Note namely that it holds for $\ell = 2$ because the four such matrices are $\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right]$.

Lemma 42. *For $n \geq 1$, the number of $M \in \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ with $\det(M-I) \equiv 0 \pmod{\ell^{n-1}}$ but $\det(M-I) \not\equiv 0 \pmod{\ell^n}$ is*

$$\begin{cases} \ell^4 - 2\ell^3 - \ell^2 + 3\ell & n = 1 \\ (\ell-1)^2(\ell+1)\ell^{3n-2} - (\ell^2-1)\ell^{2n-1} & n \geq 2. \end{cases}$$

Proof. First we deal with the $n = 1$ case. In this case, it suffices to count the number of $M \in GL_2(\mathbb{F}_\ell)$ with $\det(M - I) = 0$. Using lemma 41 and the fact that $|GL_2(\mathbb{F}_\ell)| = (\ell-1)^2\ell(\ell+1)$, the result follows for $n = 1$.

Now assume that $n \geq 2$. First, we count the number of matrices $M \in GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$ with

$$M - I = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

and $\text{ord}_\ell(\det(M - I)) = n - 1$. If $M - I \equiv \begin{bmatrix} a-1 & b \\ c & d-1 \end{bmatrix} \pmod{\ell}$, then the number of such is

$$\sum_{\epsilon=1}^{\ell-1} \sum_{i=1}^{\ell^n} \#\{(\alpha,\delta) : \alpha\delta \equiv i + \epsilon\ell^{n-1} \pmod{\ell^n}, \alpha \equiv a-1 \pmod{\ell}, \delta \equiv d-1 \pmod{\ell}\}$$
$$\cdot \{(\beta,\gamma) : \beta\gamma \equiv i \pmod{\ell^n}, \beta \equiv b \pmod{\ell}, \gamma \equiv c \pmod{\ell}\}.$$

Case I: $M \not\equiv \begin{bmatrix} 1 & b \\ c & 1 \end{bmatrix} \pmod{\ell}$ and $M \not\equiv \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \pmod{\ell}$.

In this case, we never have $a - 1 \equiv d - 1 \equiv 0$ or $b \equiv c \equiv 0$. Hence, from lemma 40, the number of solutions is either 0 or ℓ^{2n-2}. We must have $(a-1)(d-1) \equiv bc \equiv i \pmod{\ell}$, and hence the only restriction is that i lie in a particular residue class mod ℓ. Hence, any choice of ϵ is fine, and there are ℓ^{n-1} choices for i. Thus, the number of solutions is $(\ell-1)\ell^{3n-3}$. How many matrices $M \in GL_2(\mathbb{F}_\ell)$ satisfy the assumptions of this case?

There are $(\ell-1)^2$ diagonal matrices M, and $\ell^2-\ell+1$ matrices M so that $M = \begin{bmatrix} 1 & a \\ b & 1 \end{bmatrix}$. The only overlap in these two categories is in the identity matrix. Thus, there are a total of

$$(\ell-1)^2 + (\ell^2 - \ell + 1) - 1 = 2\ell^2 - 3\ell + 1$$

excluded matrices. The number of matrices M with $\det(M - I) = 0$ is $\ell^3 - 2\ell$ from lemma 41. Hence, the number of matrices covered in this case is

$$(\ell^3 - 2\ell) - (2\ell^2 - 3\ell + 1) = \ell^3 - 2\ell^2 + \ell - 1.$$

Thus, the total for this case is

$$(\ell-1)(\ell^3 - 2\ell^2 + \ell - 1)\ell^{3n-3}.$$

Case II: $M \not\equiv I \pmod{\ell}$ and $M \equiv \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \pmod{\ell}$.

In this case, $(a-1)$ and $(d-1)$ are not both zero, but b and c are. This implies that $i \equiv 0 \pmod{\ell^2}$. Moreover, any choice for ϵ will work. There are ℓ^{n-1} solutions for (α,δ). However, for (β,γ) there are $(\ell-1)(\text{ord}_\ell(i)-1)\ell^{n-1}$ solutions if $i \neq 0$ and if $i = 0$ there are $(n\ell - n - \ell + 2)\ell^{n-1}$ solutions. This gives a total of

$$\sum_{i \in \ell\mathbb{Z}/\ell^n\mathbb{Z}, i \neq 0} \ell^{n-1}(\ell-1)^2(\text{ord}_\ell(i)-1)\ell^{n-1} + (n\ell - n - \ell + 2)(\ell-1)\ell^{2n-2}$$

solutions. The first term above is

$$(\ell-1)^2\ell^{2n-2} \sum_{i \in \ell(\mathbb{Z}/\ell^n\mathbb{Z}), i \neq 0} \text{ord}_\ell(i) - 1$$
$$= (\ell-1)^2\ell^{2n-2} \sum_{k=2}^{n-1} (k-1)(\ell-1)\ell^{n-k-1}$$
$$= (\ell-1)^3\ell^{2n-2} \sum_{k=1}^{n-2} k\ell^{n-k-2}.$$

Now,

$$\sum_{k=1}^{n-2} k\ell^{n-k-2} = \frac{\ell^{n-1} - (n\ell - n - \ell + 2)}{(\ell-1)^2}.$$

Hence, the total number of these matrices with $M \pmod{\ell}$ fixed is

$$\begin{aligned}&(\ell-1)\ell^{2n-2}(\ell^{n-1}-(n\ell-n-\ell+2))+(\ell-1)\ell^{2n-2}(n\ell-n-\ell+2)\\&=(\ell-1)\ell^{3n-3}.\end{aligned}$$

As there are $\ell^2-2\ell$ choices for the reduction of $M \bmod \ell$, the total number of such matrices is

$$(\ell-2)(\ell-1)\ell^{3n-2}.$$

Case III: $M \equiv \begin{bmatrix}1 & b\\ c & 1\end{bmatrix} \pmod{\ell}$ with b and c not both zero.

In this case it is more convenient to compute

$$\begin{aligned}&\sum_{\beta=1}^{\ell-1}\sum_{i=1}^{\ell^n}\#\{(\alpha,\delta):\alpha\delta\equiv i \pmod{\ell^n},\alpha\equiv a-1 \pmod{\ell},\delta\equiv d-1 \pmod{\ell}\}\\&\cdot\{(\beta,\gamma):\beta\gamma\equiv i-\beta\ell^{n-1} \pmod{\ell^n},\beta\equiv b \pmod{\ell},\gamma\equiv c \pmod{\ell}\}.\end{aligned}$$

Since $a-1\equiv d-1\equiv 0 \pmod{\ell}$ we must have that $i\equiv 0 \pmod{\ell^2}$. Since b and c are not both zero, we have that there are ℓ^{n-1} choices for (β,γ) for any $i\equiv bc \pmod{\ell}$ and any ϵ. Thus, the number of matrices with $M \bmod \ell$ fixed is

$$(\ell-1)\ell^{n-1}\sum_{i\in\ell(\mathbb{Z}/\ell^n\mathbb{Z}),i\neq 0}^{n-1}(\ell-1)(\mathrm{ord}_\ell(i)-1)\ell^{n-1}+(\ell-1)(n\ell-n-\ell+2)\ell^{2n-2}.$$

This is the same contribution as from Case II and is hence $(\ell-1)\ell^{3n-3}$. In this case, there are $\ell^2-\ell$ choices for $M \bmod \ell$ giving a total of

$$(\ell-1)^2\ell^{3n-2}$$

matrices.

Case IV: $M\equiv I \pmod{\ell}$.

In this case, $\beta\equiv\gamma\equiv 0 \pmod{\ell}$ and hence $i\equiv 0 \pmod{\ell^2}$. If $n=2$, then $0\equiv\alpha\delta\equiv i+\epsilon\ell \pmod{\ell^2}$, a contradiction and so there are no solutions in this case. Assume therefore that $n\geq 3$.

We then have that the total number of matrices is

$$\begin{aligned}&(\ell-1)^3\ell^{2n-2}\sum_{i\in\ell(\mathbb{Z}/\ell^n\mathbb{Z}),i\neq 0,i\neq-\epsilon\ell^n}(\mathrm{ord}_\ell(i)-1)(\mathrm{ord}_\ell(i+\epsilon\ell^{n-1})-1)\\&+2(\ell-1)^2(n-2)(n\ell-n-\ell+2)\ell^{2n-2}.\end{aligned}$$

Note that if $i\neq 0$ and $i\neq-\epsilon\ell^n$ then $\mathrm{ord}_\ell(i)=\mathrm{ord}_\ell(i+\epsilon\ell^n)$. Hence, the first term above is

$$(\ell-1)^3\ell^{2n-2}\sum_{k=1}^{n-2}k^2\#\{i\in(\mathbb{Z}/\ell^n\mathbb{Z}):\mathrm{ord}_\ell(i)=k+1\}-(\ell-1)^3\ell^{2n-2}(n-2)^2.$$

The subtracted term takes account for the $i=-\epsilon\ell^{n-1}$ term which was omitted above. The above sum is

$$(\ell-1)^4\ell^{3n-4}\sum_{k=1}^{n-2}\frac{k^2}{\ell^k}-(\ell-1)^3\ell^{2n-2}(n-2)^2.$$

We now make use of the identity

$$\sum_{n=1}^{m}n^2x^n=\frac{m^2x^{m+3}+(1-2m-2m^2)x^{m+2}+(m+1)^2x^{m+1}-x^2-x}{(x-1)^3}.$$

Taking $x=\frac{1}{\ell}$ and $m=n-2$ we obtain

$$\sum_{k=1}^{n-2}\frac{k^2}{\ell^k}=\frac{\ell(\ell+1)}{(\ell-1)^3}-\frac{(n-1)^2\ell^2-(2n^2-6n+3)\ell+(n-2)^2}{\ell^{n-2}(\ell-1)^3}.$$

Hence, the total number of matrices is

$$\begin{aligned}&(\ell-1)(\ell+1)\ell^{3n-3}-(\ell-1)((n-1)^2\ell^2-(2n^2-6n+3)\ell+(n-2)^2)\ell^{2n-2}\\&-(\ell-1)^3\ell^{2n-2}(n-2)^2+2(\ell-1)^2(n-2)(n\ell-n-\ell+2)\ell^{2n-2}\\&=(\ell^2-1)\ell^{3n-3}-(\ell^2-1)\ell^{2n-1}.\end{aligned}$$

Note that this is zero for $n=2$. Summing all the contributions, we get

$$(\ell-1)^2(\ell+1)\ell^{3n-2}-(\ell^2-1)\ell^{2n-1}.$$

□

Now finally, we have to prove the final equation concerning density 11/21.

Proof. By Proposition 37, we have most of what we need to prove the density. We must calculate the fraction in the limit as described. We do this by checking the answer for $k=1$, and then imagine lifting to higher and higher k values. Here are two facts as well: $|AGL_2(\mathbb{Z}/2^k\mathbb{Z})| = 24\cdot 64^{k-1}$ (easily verifiable; exercise for the reader! (it's actually not that bad)).

- Suppose $k=1$. Note that $\left|AGL_2(\mathbb{Z}/2^1\mathbb{Z})\right| = 24$, and we may manually check that $|S'|=8$. Thus the density for $k=1$ is $8/24 = 1/3$.
- Suppose $k=2$. Note that all 8 elements of $AGL_2(\mathbb{Z}/2^1\mathbb{Z})$ that were ruminative lift to elements that are ruminative in $AGL_2(\mathbb{Z}/2^2\mathbb{Z})$. In general, note that $\vec{v} = \left(\left[\begin{smallmatrix}u\\v\end{smallmatrix}\right], \left[\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right]\right) \in AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ has 64 elements $\alpha = \left(\left[\begin{smallmatrix}u+\{0,2^k\}\\ v+\{0,2^k\}\end{smallmatrix}\right], \left[\begin{smallmatrix}a+\{0,2^k\} & b+\{0,2^k\}\\ c+\{0,2^k\} & d+\{0,2^k\}\end{smallmatrix}\right]\right) \in AGL_2(\mathbb{Z}/2^{k+1}\mathbb{Z})$ such that $\alpha \equiv \vec{v} \pmod{2^k}$. In this manner, we see that all 8 ruminative elements of $AGL_2(\mathbb{Z}/2^1\mathbb{Z})$ lift to 64 elements each in $AGL_2(\mathbb{Z}/2^2\mathbb{Z})$ that are also ruminative.

  Next, we must add elements of $AGL_2(\mathbb{Z}/2^2\mathbb{Z})$ that are ruminative but reduce modulo $\mathbb{Z}/2\mathbb{Z}$ to non-ruminative elements. These are the elements $(\vec{v}, M) \in AGL_2(\mathbb{Z}/2^2\mathbb{Z})$ such that $\det(M-I) \equiv 0 \pmod 2$, $\det(M-I) \not\equiv 0 \pmod 4$, and such that $\vec{v}$ is in the column space of $M-I$. By problem 9.1 d), note that there are $3\cdot 2^{6-2} - 3\cdot 2^{4-1} = 24$ such matrices M, and by Proposition 39, each M has 8 such vectors.

  Therefore in total, we have $8\cdot 64 + 24\cdot 8 = 702$ ruminative elements of $AGL_2(\mathbb{Z}/2^2\mathbb{Z})$. Therefore the density for $k=2$ is $\dfrac{704}{24\cdot 64} = \dfrac{11}{24}$. (So we are getting closer!).

Thus in general, we may repeat this process indefinitely.

At this point, we feel any major hurdle a team would have had in processing this problem is over, and leave the rest of the problem as a final exercise for you to think about :)

As one last hint, we claim the number of ruminative elements inside $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$ is $8\cdot 64^{k-1} + \sum_{r=1}^{k}\left((3\cdot 2^{3r-2} - 3\cdot 2^{2r-1})\cdot 2^{r+1}\cdot 64^{k-r}\right)$. Therefore, knowing that $|AGL_2(\mathbb{Z}/2^k\mathbb{Z})| = 24\cdot 64^{k-1}$, it suffices to find the limit. We encourage you to work this out for yourself, but indeed,

$$\lim_{k\to\infty} |S'|AGL_2(\mathbb{Z}/2^k\mathbb{Z}) = \frac{8\cdot 64^{k-1} + \sum_{r=1}^{k}\left((3\cdot 2^{3r-2} - 3\cdot 2^{2r-1})\cdot 2^{r+1}\cdot 64^{k-r}\right)}{24\cdot 64^{k-1}} = \frac{11}{21},$$

and we are done! □

That's it! We hope you've had a fun ride.

Appendices

A Proof of Integrality

We present the following facts about the sequence, including proofs that it is integral. As a quick remark, note one can extend the sequence into negative indices by using the recursive definition of d_n. Noting that

$$d_n = \begin{cases} \frac{d_{n-1}d_{n-3}-d_{n-2}^2}{d_{n-4}} & \text{if } n \not\equiv 2 \pmod 3 \\ \frac{d_{n-1}d_{n-3}-3d_{n-2}^2}{d_{n-4}} & \text{if } n \equiv 2 \pmod 3, \end{cases}$$

One has that for all $n \in \mathbb{Z}$,

$$d_n = \begin{cases} \frac{d_{n+3}d_{n+1}-d_{n+2}^2}{d_{n+4}} & \text{if } n \not\equiv 1 \pmod 3 \\ \frac{d_{n+3}d_{n+1}-3d_{n+2}^2}{d_{n+4}} & \text{if } n \equiv 1 \pmod 3. \end{cases}$$

This fact will be used for establishing base cases in some proofs. Consider the following.

Definition 43. *For $n \in \mathbb{N}$, define $s_n := d_n d_{n+5} - d_{n+2}d_{n+3}$.*

Lemma 44. *For all $n \in \mathbb{N}$, $d_{n+7}s_n = d_{n+1}s_{n+3}$.*

Proof. For all $k \in \mathbb{N}$, we hope to show

$$\begin{aligned} d_{k+7}s_k &= d_{k+1}s_{k+3} \\ \Leftrightarrow d_k d_{k+5}d_{k+7} + d_{k+1}d_{k+5}d_{k+6} - d_{k+2}d_{k+3}d_{k+7} - d_{k+1}d_{k+3}d_{k+8} &= 0. \end{aligned}$$

Again after rewriting this expression with terms d_k through d_{k+4}, factoring, we may find $h(k+3) = 0$ is a factor. And equivalently, $d_{k+2}s_k = d_{k-4}s_{k+3}$ as desired. □

Corollary 45. *For all $n > 1$,*

$$s_n = \begin{cases} d_{n+1}d_{n+4} & \text{if } n \equiv 0, 1 \pmod 3 \\ 3d_{n+1}d_{n+4} & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Proof. Examine first the case $n \equiv 0 \mod 3$. Computationally. $s_3 = d_3 * d_8 - d_5 * d_6 = (-3)(247) - (-17)(2) = -707 = (-7)(101)$ so the claim is true for $n = 3$. Now suppose for the sake of induction, suppose for all $n \leq k$ satisfy the claim for some $k \equiv 0 \mod 3$. Then

$$\begin{aligned} d_{k+1}d_{k+4} &= s_k \\ d_{k+1}d_{k+4} &= \frac{d_{k+1}s_{k+3}}{d_{k+7}} \\ \implies s_{k+3} &= d_{k+4}d_{k+7}. \end{aligned}$$

Thus by induction, for all $n \in \mathbb{N}$, $n \equiv 0 \pmod 3$, our claim is true. The other two cases modulo 3 are identical. □

This is sufficient to see integrality.

Proposition 46. *For $n \geq 3$, both $d_n \in \mathbb{Z}$ and $(d_n, d_{n-2}) = (d_n, d_{n-1}) = 1$.*

Proof. Proceed by induction. Note that the first 4 terms are $1, 2, 1, -3 \in \mathbb{Z}$, so the base case is true.

Suppose for all $n \leq k+4$ for some k that d_n is integral and the coprime condition is true. Note since $k+1 < k+4$ that $(d_k, d_{k+1}) = 1$. By Bezout's lemma, $\exists r, s \in \mathbb{Z}$ such that $1 = rd_k + sd_{k+1} \implies d_{k+5} = rd_kd_{k+5} + sd_{k+1}d_{k+5}$.

By the definition of the sequence, for some coefficient $c_1 \in \{1, 3\}$, $d_{k+1}d_{k+5} = d_{k+4}d_{k+2} - c_1 d_{k+3}^2$. Also by the corollary above,

$$d_kd_{k+5} - d_{k+2}d_{k+3} = s_k = c_2 d_{k+1}d_{k+4} \implies d_kd_{k+5} = c_2 d_{k+1}d_{k+4} + d_{k+2}d_{k+3},$$

for some $c_2 \in \{1, 3\}$. Therefore by the inductive hypothesis, $d_{k+1}d_{k+5}$, $d_kd_{k+5} \in \mathbb{Z}$, and $d_{k+5} = rd_kd_{k+5} + sd_{k+1}d_{k+5} \in \mathbb{Z}$ as desired.

To see that d_{k+5} is coprime to the three terms before it, note that $(d_{k+1}d_{k+4}, d_{k+2}d_{k+3}) = 1$ because by the inductive hypothesis, both d_{k+1} and d_{k+4} are coprime to $d_{k+2}d_{k+3}$. Thus

$$\begin{aligned}(d_{k+1}d_{k+4}, d_{k+2}d_{k+3}) &= 1\\ (d_{k+1}d_{k+4}, c_2 d_{k+1}d_{k+4} + d_{k+2}d_{k+3}) &= 1\\ (d_{k+1}d_{k+4}, d_kd_{k+5}) &= 1.\end{aligned}$$

Therefore d_{k+5} is coprime to d_{k+4} as desired. Similarly, $(d_{k+4}d_{k+2}, d_{k+3}^2) = 1 \implies (d_{k+1}d_{k+5}, d_{k+3}^2) = 1$, and so d_{k+5} is coprime to d_{k+3} as well. Therefore, d_{k+5} is coprime to the two previous terms as desired. □