# On constructing solutions to S-unit equations in $\mathbb{Q}_{\infty,\ell}$

Maxim Li, Misheel Otgonbayar

July 2023

Mentor: Minh-Tam Trinh
Project suggested by: Bjorn Poonen, Andrew Sutherland

**Abstract**

A theorem of Siegel states that there are only finitely many solutions to an $S$-unit equation over a number field. Iwasawa theory tells us that $\mathbb{Q}_{\infty,\ell}$, in some ways, behaves like a number field, so one might expect Siegel's theorem to hold when the field is replaced with $\mathbb{Q}_{\infty,\ell}$. However, in a recent paper by Siksek and Visser, they constructed infinitely many solutions to an $S$-unit equation in $\mathbb{Q}_{\infty,\ell}$ for $\ell = 2, 3, 5, 7$ by finding equations involving certain products of cyclotomic polynomials. We will present a more general framework to understand these equations, and show why these polynomials aren't as easily constructed for $\ell \geq 11$.

# 1 Introduction

Let $S$ be a finite set of places of a number field $K$, including all the infinite places. Then $S$-units, denoted $\mathcal{O}_{K,S}^{\times}$, are elements $x \in K$ such that $v(x) = 0$ for all $v \notin S$. $S$-units naturally have a multiplicative group structure, so we can ask whether it has some sort of additive structure. To that end, we look for a triple of $S$-units such that sum of two equals the third, or a solution to

$$x + y = 1 \text{ where } x, y \in \mathcal{O}_{K,S}^{\times}.$$

This is known as the $S$-unit equation, and a theorem by Siegel [1, theorem 0.2.8] show that there are only a finite number of solutions. This result makes a certain heuristic sense as, in the $K = \mathbb{Q}$ case, the $S$-units become exponentially sparse for in $\mathbb{R}$, making it unlikely to find those with a difference of 1.

At the same time, developments into Iwasawa theory suggested that certain infinite $\mathbb{Z}_\ell$ extensions $K_{\infty,\ell}/K$ (defined in section 2) behave remarkably similar to number fields. For example, Mazur [4] conjectured that the Mordell–Weil theorem holds over $K_{\infty,\ell}$, which has been proven for certain elliptic curves [3].

**Conjecture 1.1** (Mazur)**.** Let $A/K_{\infty,\ell}$ be an abelian variety. Then $A(K_{\infty,\ell})$ is finitely generated.

Parshin and Zarhin [8] conjectured that Faltings's theorem also holds over $K_{\infty,\ell}$.

**Conjecture 1.2** (Parshin–Zarhin)**.** Let $X/K_{\infty,\ell}$ be a curve of genus $\geq 2$. Then $X(K_{\infty,\ell})$ is finite.

A theorem by Zarhin [7] shows that Tate's homomorphism conjecture holds over $K_{\infty,\ell}$.

**Theorem 1.3** (Zarhin)**.** Let $A, B$ be abelian varieties defined over $K_{\infty,\ell}$ and denote their respective $\ell$-adic Tate modules by $T_\ell(A)$ and $T_\ell(B)$. Then the natural embedding

$$\mathrm{Hom}_{K_{\infty,\ell}}(A, B) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{K_{\infty,\ell}}/K_{\infty,\ell})}(T_\ell(A), T_\ell(B))$$

is an isomorphism.

Thus, it is natural to ask if Siegel's result on $S$-units generalizes to $K_{\infty,\ell}$. However, the generalization does not hold, as Siksek and Visser [6] showed in the case of $K = \mathbb{Q}$ and $\ell \leq 7$.

In their paper, Siksek and Visser construct cyclically symmetric polynomials $F, G, H$ that are "super-cyclotomic" (defined in section 2). These properties allow them to generate an infinite number of solutions to the $S$-unit equation by substituting in $\ell^n$-th roots of unity. The cyclic symmetry ensures that it is in $\mathbb{Q}_{\infty,\ell}$, while the latter ensures that it's an $S$-unit when $S$ is the unique prime above $\ell$.

In this paper, we develop the framework to understand the conditions necessary to generalize Siksek and Visser's method to larger primes $\ell$. Section 2 details the construction of $\mathbb{Q}_{\infty,\ell}$ and Siksek–Visser's method. In section 3, we reduce the problem of finding such polynomials to finding a pair of finite sets $S, T$ in a lattice such that they satisfy a certain congruence relation. In section 4, we explore the difficulty of satisfying this congruence relation, which gives a heuristic for why solutions were easier to construct for $\ell \leq 7$ than for larger primes. Finally, in section 5, we note some promising directions for generalizing the heuristic to a full proof.

**Acknowledgements**. The project was sponsored by the Massachusetts Institute of Technology, Department of Mathematics. The authors would like to thank our mentor Dr. Minh-Tam Trinh and Prof. David Jerison for great discussions and providing useful pointers and references. We would like to thank Prof. Jerison, Prof. Ankur Moitra and Mr. Andre Lee Dixon for organizing the program. We would also like to thank Prof. Andrew Sutherland and Prof. Bjorn Poonen for proposing our project.

# 2 Background

## 2.1 $\mathbb{Q}_{\infty,\ell}$ construction

Let $\Omega_{n,\ell} = \mathbb{Q}(\zeta_{\ell^n})$ where $\zeta_N$ is the primitive $N$-th root of unity. Then, write $\Omega_{\infty,\ell} = \bigcup \Omega_{n,\ell}$. We have that

$$\mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\Omega_{n,\ell}/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/\ell^n\mathbb{Z})^\times = \mathbb{Z}_\ell^\times \cong (\mathbb{Z}/\ell\mathbb{Z})^\times \times \mathbb{Z}_\ell$$

for $\ell > 2$. Thus we can form the subfield of $\Omega_{\infty,\ell}$ elements fixed by the subgroup $(\mathbb{Z}/\ell\mathbb{Z})^\times$, namely

$$\mathbb{Q}_{\infty,\ell} \coloneqq \Omega_{\infty,\ell}^{(\mathbb{Z}/\ell\mathbb{Z})^\times},$$

which gives us a field extension with $\mathbb{Z}_\ell$ as its Galois group over $\mathbb{Q}$. We write $\mathbb{Q}_{n,\ell}$ for the unique degree-$\ell^n$ subfield of $\mathbb{Q}_{\infty,\ell}$ (consistent with [6]). We have that

$$\mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}_{\infty,\ell}) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times$$

and we fix a generator $a$ for the rest of this paper, as the group of units mod $\ell$ are cyclic.

**Notation 2.1.** For a field extension $L/K$, $x \in L$ and $\sigma \in \mathrm{Gal}(L/K)$, we will write $x^\sigma$ instead of $\sigma(x)$.

**Remark 2.2.** We define $K_{\infty,\ell} \coloneqq K \cdot \mathbb{Q}_{\infty,\ell}$, used in section 1.

## 2.2 Siksek and Visser's construction

Let $\Psi_n(X,Y) = Y^{\varphi(n)}\Phi_n(X/Y)$ be the homogenization of the $n$th cyclotomic polynomial. If $F(x_1,\dots,x_n)$ is of the form $f_0 \prod_k \Psi_{n_k}(f_k,g_k)$, where each $f_i$ and $g_i$ is a monomial in the $x_i$'s, then we call it super-cyclotomic. Then the following theorem holds.

**Theorem 2.3.** (Siksek–Visser) If $F(x_1,\dots,x_{\ell-1})$ is a super-cyclotomic integral polynomial in $(\ell-1)$ variables, invariant under the cyclic shift $x_i \mapsto x_{i+1}$ where $x_\ell = x_1$, then $F(\zeta,\zeta^a,\dots,\zeta^{a^{\ell-2}})$ is an $S$-unit in $\mathbb{Q}_{\infty,\ell}$ for any $\zeta = \zeta_{\ell^n}$ with $n$ sufficiently large.

*Proof.* We include a sketch of the proof. See [6, section 2] for the full version.

We have that $N_{\Omega_{n,\ell}/\mathbb{Q}}(1-\zeta^k)$ is a power of $\ell$ when $\zeta^k \neq 1$. Thus, $1-\zeta^k$ is an $S$-unit. Thus $F$ being super-cyclotomic ensures that the substitution in the statement gives an $S$-unit as long as it is nonzero.

On the other hand, $F(\zeta,\zeta^a,\dots) \in \mathbb{Q}_{\infty,\ell}$ if and only if it is fixed by $\mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}_{\infty,\ell})$, or equivalently the generator $a$. This is exactly equivalent to $F$ being invariant under cyclic shift as it is a polynomial with integer coefficients. $\square$

Call the subgroup of the $S$-units generated by $1-\zeta_{\ell^n}^k$ and $\zeta_{\ell^n}^k$ to be *cyclotomic $S$-units*. Siksek and Visser's construction can only construct cyclotomic $S$-unit solutions, so we might worry that we're losing a lot of information. However, these actually form a finite index subgroup in the group of all $S$-units [6, lemma 8].

Call a polynomial *good* if it satisfies the hypotheses in the above theorem. To construct $S$-unit equation solutions, Siksek–Visser produced good polynomials $F, G, H$ for $\ell = 5, 7$ satisfying $F+G = H$, which gives solutions to the $S$-unit equation upon substituting $\zeta^{a^i}$ to $x_i$ to $(F/H, G/H)$.

A natural question to ask is if this construction can generalize.

# 3 A More General Framework

## 3.1 Big picture

Our motivating problem is to find solutions to the $S$-unit equation. As cyclotomic-$S$-units are finite index, we are not too far from full generality if we only consider cyclotomic-$S$-units solutions.

We focus further on certain families of $S$-unit solutions, specifically ones that come from polynomials described in Siksek–Visser. This approach allows us to reduce the search to a polynomial instead, as described in section 3.2.

By exploring what properties are required of our polynomial, we reduce the problem to finding 3 sets of points in a lattice of rank $\varphi(\ell-1)$ in section 4.1.

We then show why in the $\ell \leq 7$ case good polynomial solutions to $F + G = H$ have been particularly simple to find, and note the difficulties in generalizing to larger primes.

## 3.2 Formalization Through Formal Exponents

In Siksek and Visser's construction, they substitute $\zeta, \zeta^a, \ldots$ into their polynomials, where $\zeta$ is any $\ell^n$-th root of unity for large enough $n$. Call this substition map $\psi$.

$$\begin{aligned} \psi : \mathbb{Z}[x_1, \ldots x_{\ell-1}] &\to \Omega_{\infty,\ell} \\ x_i &\mapsto \zeta^{a^i} \end{aligned}$$

Note that these are all units, so we could instead have worked in the ring of Laurent polynomials $\mathbb{Z}[x_1^{\pm 1}, \ldots, x_{\ell-1}^{\pm 1}]$. Now consider the formal relabeling $x_i \mapsto x^{t^{i-1}}$ with the exponents living in the free $\mathbb{Z}$-module generated by $1, t, t^2, \ldots t^{\ell-2}$. This gives us an isomorphism to the ring

$$\mathbb{Z}[x^f \mid f \in \mathbb{Z}[t]/(t^{\ell-1}-1)],$$

and being cyclically symmetric in the ring of Laurent polynomials is equivalent to being fixed under the isomorphism $x \mapsto x^t$. Then a good polynomial is equivalent to a polynomial of the form $x^{f_0} \prod_k \Phi_{n_k}(x^{f_k})$ that is fixed under $x \mapsto x^t$. These will also be called good polynomials.

Note also that the original $\psi$ induces

$$\begin{aligned} \psi : \mathbb{Z}[x^f \mid f \in \mathbb{Z}[t]/(t^{\ell-1}-1)] &\to \Omega_{\infty,\ell} \\ x^f &\mapsto \zeta^{f(a)} \end{aligned}$$

where we consider $f(a)$ as an element of $\mathbb{Z}[\mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}_{\infty,\ell})]$.

**Lemma 3.1.** We have that $\zeta^{\Phi_{\ell-1}(a)} = 1$ for any $\ell^n$-th root of unity $\zeta$ and $n \geq 0$.

*Proof.* We have $a \in \mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}_{\infty,\ell}) \subset \mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}) \cong \mathbb{Z}_\ell^\times$. The Galois element acts by

$$\zeta^a = \zeta^{a \bmod \ell^n}$$

where the reduction is in $\mathbb{Z}_\ell^\times$, for any $n$. Thus the additive structure of $\mathbb{Z}[\mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}_{\infty,\ell})]$ is compatible with addition in $\mathbb{Z}_\ell^\times \subset \mathbb{Z}_\ell$.

Now, if $f(a) = 0$ in $\mathbb{Z}_\ell$, then $\zeta^{f(a)} = 1$. As $\mathbb{Z}_\ell$ is an integral domain, and the multiplicative order of $a$ is $\ell - 1$, we have that $a$ is a root of $x^{\ell-1} - 1$ but not lower powers. Thus, we must have

$$\Phi_{\ell-1}(a) = 0$$

and the lemma follows. $\square$

Thus, $\psi$ factors through the ring $\mathbb{Z}[x^f \mid f \in \mathbb{Z}[\mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}_{\infty,\ell})]/\Phi_{\ell-1}(a)]$, and so we have the following commutative diagram:

$$\begin{tikzcd}
\mathbb{Z}[x_1^{\pm 1}, \dots, x_{\ell-1}^{\pm 1}] \arrow[r, "\sim"] \arrow[d, "\psi"] & \mathbb{Z}[x^f \mid f \in \mathbb{Z}[t]/(t^{\ell-1} - 1)] \arrow[d, "t \mapsto a"] \\
\Omega_{\infty,\ell} & \mathbb{Z}[x^f \mid f \in \mathbb{Z}[\mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}_{\infty,\ell})]/\Phi_{\ell-1}(a)] \arrow[l]
\end{tikzcd}$$

We extend the definition of good polynomials to those fixed under $x \mapsto x^a$ in the bottom right ring. Note that the quotient map preserves good polynomials, so it suffices to work in the ring $\mathbb{Z}[x^f \mid f \in \mathbb{Z}[\mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}_{\infty,\ell})]/\Phi_{\ell-1}(a)]$. We have the following lemma.

**Notation 3.2.** We abuse notation to write $\mathbb{Z}[a]$ for $\mathbb{Z}[\mathrm{Gal}(\Omega_{\infty,\ell}/\mathbb{Q}_{\infty,\ell})]/\Phi_{\ell-1}(a)$.

**Lemma 3.3.** Given good polynomials $F, G, H$ satisfying $F + G = H$, there exists multisets $S, T, R$ with elements in $\mathbb{Z}[a]$ and vectors $s_0, t_0, r_0 \in \mathbb{Z}[a]$ such that

$$x^{s_0} \prod_{s \in S} (x^s - 1) + x^{t_0} \prod_{t \in T} (x^t - 1) = x^{r_0} \prod_{r \in R} (x^r - 1)$$

where each factor appears with the same multiplicity as it does in the corresponding multiset.

*Proof.* Recall that for any cyclotomic polyomial, we have $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$. Thus, we can write a good polynomial $F$ as

$$x^{f_0} \prod_k \Phi_{n_k}(x^{f_k}) = x^{f_0} \prod_k \prod_{d|n_k} (x^{df_k} - 1)^{\mu(n_k/d)}$$

Do the same for $G$ and $H$. Now if we clear denominators, the resulting equation will be of the desired form. $\square$

# 4 Obstructions when $\ell \geq 11$

## 4.1 The structure of $S$, $T$, and $R$

We now explore the structure of these multisets $S, T, R$. They live inside some lattice $V$, and we want to understand the properties induced by the group algebra $\mathbb{Z}[V]$.

**Notation 4.1.** For $v \in V$, we let $\langle v \rangle$ denote the rank 1 sublattice generated by $v$.

**Lemma 4.2.** Let $V$ be a finitely-generated lattice, and $r \in V$ a nonzero vector. Then $\mathbb{Z}[V]/(x^r - 1)$ and $\mathbb{Z}[V/\langle r \rangle]$ are naturally isomorphic, and this isomorphism commutes with the natural quotient maps from $\mathbb{Z}[V]$.

*Proof.* Let $\pi : \mathbb{Z}[V] \to \mathbb{Z}[V/\langle r \rangle]$ be the natural quotient map. Then since

$$\pi(x^r - 1) = x^0 - 1 = 0,$$

we get that $(x^r - 1) \subset \ker(\pi)$. Thus it suffices to show that $\ker(\pi) \subset (x^r - 1)$.

Suppose some $\sum a_v x^v$ is sent to 0 under $\pi$. Partitioning the sum by cosets of $\langle r \rangle$, we see that for this to be sent to 0, each individual coset sum must be sent to 0, since these are all $\mathbb{Z}$-linearly independent in $\mathbb{Z}[V/\langle r \rangle]$. Now consider some coset sum,

$$\sum_{v \in w + \langle r \rangle} a_v x^v$$

We see that under $\pi$, this is mapped to $\left(\sum a_v\right) x^{\overline{w}}$, and so $\sum a_v = 0$. But for each $v$, we have $v = w + nr$ for some $n \in \mathbb{Z}$, so $x^v - x^w = x^w(x^{nr} - 1)$, and so it lies in the ideal $(x^r - 1)$ (if $n$ is positive, we can use the $t^n - 1$ factorization, and if $n$ is negative, we can write $x^{nr} - 1 = -x^{nr}(x^{-nr} - 1)$, and do the same thing).

Thus we have,

$$\sum_{v \in w + \langle r \rangle} a_v x^v - \sum a_v x^w \in (x^r - 1).$$

But $\sum a_v = 0$, so in fact, the coset sum lies in $(x^r - 1)$. Summing over all cosets, we see that $\sum a_v x^v \in (x^r - 1)$. Thus, $\ker(\pi) \subset (x^r - 1)$, as desired. $\square$

**Definition 4.3.** A nonzero vector $r \in V$ primitive if it is not of the form $n \cdot v$ with $|n| > 1$ for any $v \in V$.

**Lemma 4.4.** If $r$ is primitive, then it can be extended to an integral basis of $V$.

*Proof.* Note that $r$ being primitive is equivalent to $V/\langle r \rangle$ having no torsion. Thus, by the structure theorem for finitely generated abelian groups, $V/\langle r \rangle$ is isomorphic to $\mathbb{Z}^k$ for some $k$. We can now take a basis in the quotient and take any lift to $V$, which gives us the extension of $r$ to a basis. $\square$

**Corollary 4.5.** The quotient ring $\mathbb{Z}[V]/(x^r - 1)$ is an integral domain if and only if $r$ is primitive.

Given two multisets $A, B$, we write $A \coprod B$ to be the multiset where each element appears with multiplicity equal to the sum of its multiplicities in $A$ and $B$. Additionally, if $A$ and $B$ have elements in $V$, we write $A \equiv B \bmod v$ if, under the map $V \to V/\langle v \rangle$, the two multisets have the same image. The next two theorems give us the main structure of $S$, $T$, and $R$.

**Theorem 4.6.** Let $r$ be a primitive vector. If $x^r - 1$ divides

$$x^{s_0} \prod_{s \in S} (x^s - 1) \pm x^{t_0} \prod_{t \in T} (x^t - 1)$$

and no vectors in $S \coprod T$ are multiples of $r$, then $(S \coprod -S) \equiv (T \coprod -T) \bmod r$.

*Proof.* Consider quotienting $\mathbb{Z}[V]$ by $x^r - 1$. By lemma 4.2, this is equivalent to reducing the exponents of $x$ mod $r$, so if we let $\overline{v}$ denote the image of a vector $v$ in $V/\langle r \rangle$, we have that

$$x^{\overline{s_0}} \prod_{s \in S} (x^{\overline{s}} - 1) = \pm x^{\overline{t_0}} \prod_{t \in T} (x^{\overline{t}} - 1) \tag{1}$$

in $\mathbb{Z}[V/\langle r \rangle]$. Because no vectors in $S \coprod T$ are multiples of $r$, neither side of this equation is 0.

Now pick some $\overline{s}$, and suppose $\overline{s} = n\overline{s}'$, where $\overline{s}'$ is primitive in $V/\langle r \rangle$. Then there exists a way to extend $\overline{s}'$ to an integral basis of $V/\langle r \rangle$ by lemma 4.4, or equivalently, there exists an isomorphism $\mathbb{Z}[V/\langle r \rangle] \cong \mathbb{Z}[x_1^{\pm 1}, \dots, x_k^{\pm 1}]$ such that $x^{\overline{s}'} \mapsto x_1$.

Now consider the map $\mathbb{Z}[x_1^{\pm 1}, \dots, x_k^{\pm 1}] \to \mathbb{C}[x_2^{\pm 1}, \dots, x_k^{\pm 1}]$ with $x_1 \mapsto \zeta_n$. Note that $x^{\overline{s}} - 1$ goes to $x_1^n - 1$ under the isomorphism, which goes to 0 under this map, and so the left side of equation (1) is 0. Thus, the right side must also evaluate to 0. But we also know that under this map, the right side is a product of an invertible monomial, and terms of the form $\zeta_n^{e_1} x_2^{e_2} \dots x_k^{e_k} - 1$. As $\mathbb{C}[x_2^{\pm 1}, \dots x_k^{\pm 1}]$ is an integral domain, the only way for this product to be 0 is if one of these is 0, which is only possible if $n | e_1$ and $e_2 = \dots = e_k = 0$. But then the preimage of this factor must be $x_1^{e_1} - 1$ with $n | e_1$, so through the isomorphism, we see that $x^{\overline{t}} - 1 = x^{e_1 \overline{s}'} = x^{e_1 / n \cdot \overline{s}}$. Thus, for any $\overline{s}$, there exists some $\overline{t}$ that is a multiple of $\overline{s}$.

By symmetry, a similar statement holds for $T$. But now if we take the partial order defined by divisibility, we see that for any maximal $\overline{s}$, there exists $\overline{t}$ equal to $\overline{s}$ or $-\overline{s}$. If it equals $-\overline{s}$, note that we can write $x^{\overline{t}} - 1 = -x^{\overline{t}}(x^{-\overline{t}} - 1)$, and so in both cases, we can factor a $(x^{\overline{s}} - 1)$ out of both sides. By repeating this process, we see that there exists a bijection $f : S \to T$ such that for all $s \in S$, $\overline{s} = \pm \overline{f(s)}$, which means the sets $\{s, -s\}$ and $\{f(s), -f(s)\}$ are the same mod $r$. Taking the disjoint union of all these sets, this means $S \coprod -S \equiv T \coprod -T \bmod r$. □

**Theorem 4.7.** If $x^{s_0} \prod_{s \in S} (x^s - 1)$ is fixed under the isomorphism $x \mapsto x^a$, then $S \coprod -S$ is fixed under multiplication by $a$ in $\mathbb{Z}[a]$.

*Proof.* If the polynomial is fixed by $x \mapsto x^a$, we must have

$$x^{as_0} \prod_{s \in S} (x^{as} - 1) = x^{s_0} \prod_{s \in S} (x^s - 1)$$

Consider quotienting by $(x^s - 1)$ and $(x^{as} - 1)$. By similar logic to the previous theorem, we see that there exists a bijection $f : S \to S$ such that $as = \pm f(s)$, which means the sets $\{as, -as\}$ and $\{f(s), -f(s)\}$ are the same. Taking the disjoint union across all $s$, this implies $aS \coprod -aS = S \coprod -S$, so $S \coprod -S$ is fixed by multiplication by $a$. □

This motivates the following definition.

**Definition 4.8.** A multiset $S \subset \mathbb{Z}[a]$ is *stable* if it is fixed under multiplication by $a$.

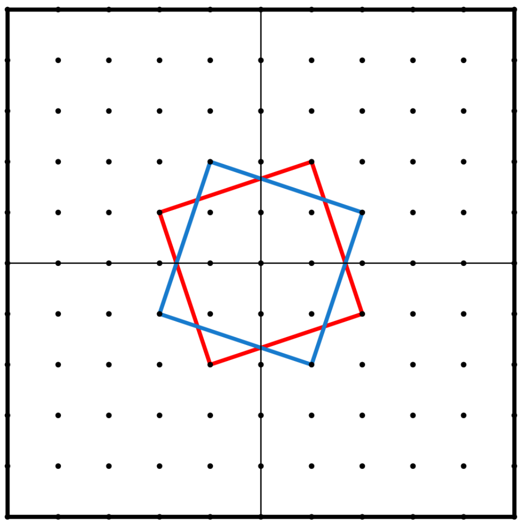
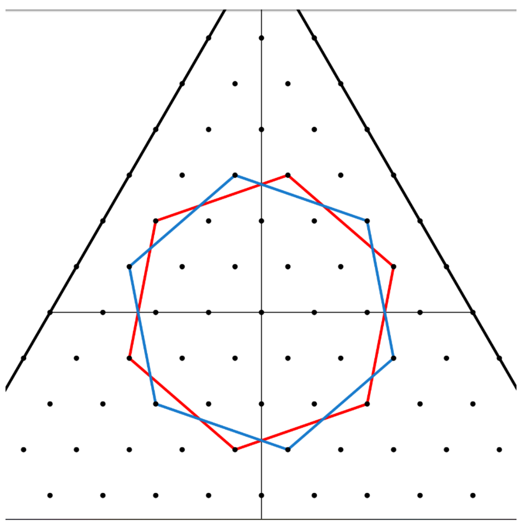
Thus, our problem about good polynomials has been reduced to the following problem: given stable multisets $S, T$, for which $r$ can we have $S \equiv T \bmod r$?

### 4.2 Obstructions to $S$, $T$, and $R$

Note that there is a very natural lattice isomorphic to $V \cong \mathbb{Z}[a] \cong \mathbb{Z}[x]/\Phi_{\ell-1}(x)$, namely $\mathbb{Z}[\zeta_{\ell-1}]$, which we can embed into $\mathbb{C}$. Then the multiplication-by-$a$ action is just a rotation by $\frac{2\pi}{\ell-1}$ about the origin, and $a$-invariant sets are exactly sets of regular $(\ell-1)$-gons centered at 0.

#### 4.2.1 One orbit

Under this framework, Siksek and Visser's constructions for $\ell = 5, 7$ can be visualized as $S, T$ being one orbit.

Here the vertices of the red and blue polygon represent the orbits of $S$ and $T$ respectively. In both pictures, we see a natural pairing of vertices that give rational (in fact, integral) differences, corresponding to $r = 1$.

So the question arises: do such simple (one orbit) constructions exist for larger $\ell$? The following theorem gives a definitive answer.

**Theorem 4.9.** If $\ell \geq 11$, $S$ and $T$ only consist of one orbit, and $S \neq T$, then there does not exist any $r$ such that $S \equiv T \bmod r$.

*Proof.* Assume not. Since both $S$ and $T$ consist of one orbit, they must be regular $(\ell-1)$−gons centered at 0. Then $S \equiv T \bmod r$ means there is some bijection $f : S \to T$ such that $s - f(s) \in \mathbb{Z}r$, or $sr^{-1} - f(s)r^{-1} \in \mathbb{Z}$. But if we replace $S$ and $T$ with $Sr^{-1}$ and $Tr^{-1}$, we see that they still must form regular $(\ell-1)$-gons in $\mathbb{Q}(\zeta_{\ell-1})$, and the condition now reads $s - f(s) \in \mathbb{Q}$.

Let $S = \{Re^{i\theta}, \zeta_{\ell-1}Re^{i\theta}, \dots\}$, with imaginary parts forming the set $\{R\sin(\theta), R\sin(\theta+\frac{2\pi}{\ell-1}), \dots\}$. The mod $r$ constraint implies the imaginary parts of $T$ form the same set. Now consider summing the squares of these numbers. We have that

$$\sum_{k=0}^{\ell-2} R^2 \sin^2\left(\theta + \frac{2\pi k}{\ell-1}\right) = \sum_{k=0}^{\ell-2} R^2 \left(\frac{1-\cos\left(2\theta+\frac{4\pi k}{\ell-1}\right)}{2}\right)$$
$$= \frac{\ell-1}{2}R^2 - R^2\sum_{k=0}^{\ell-2}\cos\left(2\theta + \frac{4\pi k}{\ell-1}\right).$$

However,

$$\begin{aligned}\sum_{k=0}^{\ell-2}\cos\left(2\theta+\frac{4\pi k}{\ell-1}\right)&=\operatorname{Re}\left(\sum_{k=0}^{\ell-2}e^{2i\theta}\zeta_{\ell-1}^{2k}\right)\\&=\operatorname{Re}\left(e^{2i\theta}\frac{\zeta_{\ell-1}^{2(\ell-1)}-1}{\zeta_{\ell-1}^{2}-1}\right)\\&=0\end{aligned}$$

since $\ell-1\neq 2$, which means the sum of squares just equals $\frac{\ell-1}{2}R^2$.

In particular, since this sum must be the same for both $S$ and $T$, the two polygons must have the same radius $R$. But for any given pure imaginary number, there are at most two points with that imaginary part and distance $R$ away from 0, and they are reflections over the imaginary axis, which means $S$ and $T$ must be reflections over the imaginary axis since $S\neq T$.

By above, every point in $S$ must be a rational distance away from it's reflection over the imaginary axis, so we must have $\operatorname{Re}(s)\in\mathbb{Q}$ for all $s\in S$. Let $s=Re^{i\theta}$. Then the real parts of $s,\zeta_{\ell-1}s,\zeta_{\ell-1}^2 s$ are $R\cos(\theta), R\cos(\theta+\frac{2\pi}{\ell-1})$, and $R\cos(\theta+\frac{4\pi}{\ell-1})$. But by basic trig, we have that

$$2R\cos\left(\theta+\frac{2\pi}{\ell-1}\right)\cos\left(\frac{2\pi}{\ell-1}\right)=R\cos(\theta)+R\cos\left(\theta+\frac{4\pi}{\ell-1}\right)$$

so as long as $\cos(\theta+\frac{2\pi}{\ell-1})\neq 0$ (we can always pick $s$ so this happens), this implies $\cos\left(\frac{2\pi}{\ell-1}\right)\in\mathbb{Q}$, which is impossible for $\ell\geq 11$. $\square$

### 4.2.2 Multiple orbits

With the one orbit case resolved, we now have to consider what happens if there are multiple orbits. Optimistically, one might hope that finding $S\equiv T \bmod r$ is impossible, even with multiple orbits. Unfortunately, the next theorem shows that this is always possible for large enough orbits.

**Theorem 4.10.** For all $\ell\geq 5$, there exists $S\neq T\subset\mathbb{Z}[\zeta_{\ell-1}]$, each consisting of $2^{\frac{\ell-3}{2}}$ orbits, such that $S\equiv T \bmod r$ with $r=1$.

*Proof.* Let $z\in\mathbb{Z}[\zeta_{\ell-1}]$ whose value is to be fixed later, and consider all numbers of the form

$$z+\sum_{i=0}^{\frac{\ell-3}{2}}e_i\zeta_{\ell-1}^i,$$

where $e_i\in\{0,1\}$. Let $S'$ denote the set where an even number of $e_i$ are 1, and $T'$ the set where an odd number of $e_i$ are 1. Let $S=\coprod_{k=0}^{\ell-2}\zeta_{\ell-1}^k S'$, and $T=\coprod_{k=0}^{\ell-2}\zeta_{\ell-1}^k T'$. We claim that $S$ and $T$ are our desired sets.

First, note that $|S'|=|T'|=2^{\frac{\ell-3}{2}}$, and that $S$ and $T$ consist of the orbits containing the elements of $S'$ and $T'$ respectively. Thus, $S$ and $T$ both consist of $2^{\frac{\ell-3}{2}}$ orbits.

Next, we will show $S\equiv T \bmod r$. Pick any $s=\zeta^k(z+\sum e_i\zeta_{\ell-1}^i)\in S$. Note that there exists a unique $i\in[0,\frac{\ell-3}{2}]$ such that $\zeta^k=\pm\zeta^{-i}$. Then there exists a unique $t\in T$ with the same $\zeta^k$ in front which only differs from $s$ in $e_i$, and so $s - t = \pm\zeta_{\ell-1}^{-i}(\pm\zeta^i) \in \mathbb{Z}$. Thus, for each $s \in S$, we can associate a unique $t \in T$ with $s \equiv t \bmod r$, so $S \equiv T \bmod r$.

Finally, we must show $S \neq T$. To do this, we will simply show $z \notin T$. First, note that $\mathrm{Im}(\zeta^i) \geq 0$ for all $i \in [0, \frac{\ell-3}{2}]$, with equality holding if and only if $i = 0$. Thus, there is no way for a nonempty sum of these terms to add up to 0, so $z \notin T'$. Now suppose $z \in \zeta_{\ell-1}^k T'$ for some $k \neq 0$. This means that $(1 - \zeta_{\ell-1}^k)z = \sum e_i \zeta_{\ell-1}^i$ for some choice of $e_i$. But since $\zeta_{\ell-1}^k \neq 1$, there are only finitely many such $z$. Thus, since $\mathbb{Z}[\zeta_{\ell-1}]$ is infinite, we can always pick a $z$ such that $S \neq T$, as desired. □

The fact that there always exists such a construction raises the following question: For any $\ell$, what is the minimum number of orbits needed for such an $r$ to exist?

In fact, we no longer make use of the fact that $\ell$ is prime, so we could extend this problem to other values of $\ell$. There exists a 2 orbit construction for $\ell = 9$ and a 3 orbit construction for $\ell = 13$ (see Appendix), showing that the answer is not very straightforward. It is possible that a subexponential bounds exist. We do, however, have a linear lower bound.

**Theorem 4.11.** Both $S$ and $T$ contain at least $\frac{\ell-1}{360}$ orbits.

Note that since each orbit always has $\ell - 1$ points and $|S| = |T|$, it suffices to show this for one of the sets. To prove this, we need the following lemma.

**Lemma 4.12.** Let $P \in \mathbb{Q}[x]$ be a nonzero polynomial with $P(\zeta_{\ell-1}) = 0$. If $P$ has $N$ nonzero monomials, then there exist polynomials $Q_p(x) \in \mathbb{Q}[x]$ for all primes $p < N$ that divide $\ell - 1$ such that

$$P(x) = \sum_{p|\ell-1, p<N} Q_p(x)\Phi_p(x^{\frac{\ell-1}{p}})$$

holds.

*Proof.* Note that $N > 2$. Let $n = \ell - 1$. By [5], we can write

$$P(x) = \sum_{p|n} Q_p(x)\Phi_p(x^{\frac{n}{p}})$$

for some $Q_p$, with no restriction on the size of $p$. Now let $q$ be the largest prime with $Q_q \neq 0$. If $q \leq N$, we are done, so assume not. Then we claim that there exist polynomials $R_p(x)$ with $p < q$ such that $Q_q(x)\Phi_q(x^{\frac{n}{q}}) = \sum_p R_p(x)\Phi_p(x^{\frac{n}{p}})$, which would mean we could lower the value of $q$. Note that we can work mod $x^n - 1$, since this is divisible by $\Phi_2(x^{\frac{n}{2}})$, and $2 < q$. Thus, we can WLOG take all exponents mod $n$, and assume $deg(P) < n$. Additionally, we can take $Q_p$ mod $x^{\frac{n}{p}} - 1$ since $(x^{\frac{n}{p}} - 1)\Phi_p(x^{\frac{n}{p}}) = x^n - 1$, and so we can assume $deg(Q_p) < \frac{n}{p}$. Now note that any polynomial of the form $x^k\Phi_p(x^{\frac{n}{p}})$ only has monomials with exponents within some residue class mod $\frac{n}{p_1 \ldots p_k q}$, where $p_1 \ldots p_k q$ is the product of all the prime factors of $n$ that are at most $q$. Thus, we can work with each residue class separately, and so can replace $n$ with $p_1 \ldots p_k q$. All of the above logic still holds.

Let $(P)_i$ denote the $i$th coefficient of $P$, and define similar notation for the $Q_p$'s. Using a root of unity filter, the $j$th coefficient of $P$ is exactly $\frac{1}{n}\sum_{k=1}^{n} \zeta_n^{-jk} P(\zeta_n^k)$. (Here we use that $deg(P) < n$) Breaking $P$ into the sum, we see that this equals

$$\frac{1}{n}\sum_{k=1}^{n}\sum_{p|n} \zeta_n^{-jk} Q_p(\zeta_n^k)\Phi_p(\zeta_n^{\frac{nk}{p}})$$

But $\Phi_p(\zeta_n^{\frac{nk}{p}}) = 0$ if $p \nmid k$, and $p$ otherwise. Thus, letting $1_{p|k}$ be the indicator function for if $p|k$, this equals

$$\frac{1}{n}\sum_{k=1}^{n}\sum_{p|n} p\zeta_n^{-jk}Q_p(\zeta_n^k)1_{p|k} = \frac{1}{n}\sum_{p|n}\sum_{p|k\leq n} p\zeta_n^{-jk}Q_p(\zeta_n^k)$$

$$= \frac{1}{n}\sum_{p|n} p \sum_{m=1}^{\frac{n}{p}} \zeta_n^{-jpm}Q_p(\zeta_n^{pm})$$

Finally, note that $\zeta_n^p$ is a primitive $n/p$-th root, so by another root of unity filter, this equals

$$\frac{1}{n}\sum_{p|n} p\frac{n}{p}\sum_{i\equiv j \bmod \frac{n}{p}} (Q_p)_i = \sum_{p|n}\sum_{i\equiv j \bmod \frac{n}{p}} (Q_p)_i$$

We also have that

$$Q_p(x)\Phi_p(x^{\frac{n}{p}}) = \sum_{i=0}^{p-1}\sum_{j}(Q_p)_j x^j x^{\frac{ni}{p}} \equiv \sum_{i\equiv j \bmod \frac{n}{p}} (Q_p)_i x^j \bmod x^n - 1$$

since by varying $i$, we can let $j$ take all values that are congruent to $i$ mod $\frac{n}{p}$.

Now note that since $N < q$, there is some residue class mod $q$ where $P$ has no nonzero monomials with an exponent in that residue class. Thus, for some $X$ and all $j \equiv X \bmod q$, $(P)_j = 0$, so by above,

$$\sum_{i\equiv j \bmod \frac{n}{q}} (Q_q)_i = -\sum_{p<q}\sum_{i\equiv j \bmod \frac{n}{p}} (Q_p)_i$$

for all $j \equiv X \bmod q$. Thus, we have that

$$Q_q(x)\Phi_q(x^{\frac{n}{q}}) = \sum_{j\equiv X \bmod q}\sum_{i\equiv j \bmod \frac{n}{q}} (Q_q)_i x^j \Phi_q(x^{\frac{n}{q}})$$

$$= -\Phi_q(x^{\frac{n}{q}})\sum_{j\equiv X \bmod q}\sum_{p<q}\sum_{i\equiv j \bmod \frac{n}{p}} (Q_p)_i x^j$$

The first equation holds modulo $x^n - 1$ because by the Chinese Remainder Theorem, every residue class mod $\frac{n}{q}$ has exactly one representative congruent to $X$ mod $q$. Focus on a particular prime $p$, and consider the sum $\sum_{j\equiv X}\sum_{i\equiv j}(Q_p)_i x^j$. Note that for a fixed $i$, any $j$ that is equivalent mod $\frac{n}{p}$ is also equivalent to $X$ mod $q$ since $q|\frac{n}{p}$. Thus, letting $j$ vary, we see that this is just

$$\sum_{i\equiv X \bmod q}\sum_{i\equiv j \bmod \frac{n}{p}} (Q_p)_i x^j$$

which is exactly the $\equiv X$ terms in $Q_p(x)\Phi_p(x^{\frac{n}{p}})$, and so can be written as $Q_p^{\equiv X}(x)\Phi_p(x^{\frac{n}{p}})$, where $Q_p^{\equiv X}$ just means to take the monomials whose exponents are equivalent to $X$ mod $q$. Thus, we have that

$$Q_q(x)\Phi_q(x^{\frac{n}{q}}) = -\Phi_q(x^{\frac{n}{q}})\sum_{p<q} Q_p^{\equiv X}(x)\Phi_p(x^{\frac{n}{p}}) = \sum_{p<q} R_p(x)\Phi_p(x^{\frac{n}{p}})$$

Thus, if $q > N$, we can always write $Q_q(x)\Phi_q(x^{\frac{n}{q}})$ using smaller primes, and so can reduce the value of $q$. By repeating this process, we eventually end up with a sum with only primes at most $N$, as desired. □

**Corollary 4.13.** Let $P \in \mathbb{Q}[x]$ be a nonzero polnomial with $P(\zeta_{\ell-1}) = 0$ and $N$ nonzero monomials. Then if $p_1, \dots, p_k$ are all the primes less than $N$, there exists monomials of $P$ whose exponents differ by a multiple of $\frac{\ell-1}{p_1 p_2 \cdots p_k}$.

*Proof.* By the lemma, $P(x) = \sum_{p|\ell-1, p<N} Q_p(x)\Phi_p(x^{\frac{\ell-1}{p}})$. But everything of the form $x^k\Phi_p(x^{\frac{\ell-1}{p}})$ has exponents lying in the same residue class mod $\frac{\ell-1}{p_1\cdots p_k}$, and by treating every residue class separately, we see that there cannot be a residue class with exactly one monomial. Thus, since $P$ is nonzero, there are two exponents in the same residue class, as desired. □

We now prove the lower bound of Theorem 4.11. Throughout this proof, we will use $\mathbb{Q}\langle x_1, \dots, x_k\rangle$ to denote the $\mathbb{Q}$-vector space in $\mathbb{Q}(\zeta_{\ell-1})$ spanned by $x_1, \dots, x_k$.

*Proof.* WLOG $r = 1$ (multiply by $r^{-1}$). Consider the bijection $f : S \to T$ with $s - f(s) \in \mathbb{Q}r$. We claim that given two orbits $S', T'$ in $S$ and $T$, $|f(S') \cap T'| \leq 360$. Note that this would prove the theorem, since then $\ell - 1 = |f(S')| = \sum_{T' \subset T} |f(S') \cap T'| \leq 360 \cdot \#\{\text{orbits in } T\}$. For ease of notation, let $\zeta = \zeta_{\ell-1}$.

Let $S'$ and $T'$ be the orbits of $s$ and $t$ respectively, let $f(\zeta^i s) = \zeta^{\sigma(i)}t$ whenever $f(\zeta^i s) \in T'$, and let $\Delta i = \sigma(i) - i$. Note that if $\zeta^{\Delta i} = \zeta^{\Delta j}$, then $\zeta^j s - \zeta^{\sigma(j)}t = \zeta^{j-i}(\zeta^i s - \zeta^{\sigma(i)}s)$, and so lies in both $\mathbb{Q}$ and $\zeta^{j-i}\mathbb{Q}$, which is a contradiction unless $j \equiv i \bmod \frac{\ell-1}{2}$.

Next, multiplying by $\zeta^{j-i}$ gives us that $\zeta^j s - \zeta^{j-i+\sigma(i)}t \in \zeta^{j-i}\mathbb{Q}$, and so subtracting $\zeta^j s - \zeta^{\sigma(j)}t$ gives that $(\zeta^{j-i+\sigma(i)} - \zeta^{\sigma(j)})t \in \mathbb{Q}\langle 1, \zeta^{j-i}\rangle$. Multiplying by $\zeta^{-j}$ gives

$$(\zeta^{\Delta i} - \zeta^{\Delta j})t \in \mathbb{Q}\langle \zeta^{-i}, \zeta^{-j}\rangle$$

Now multiplying by $\zeta^{-\Delta i - \Delta j}$ gives

$$(\zeta^{-\Delta i} - \zeta^{-\Delta j})t \in \mathbb{Q}\langle \zeta^{-\Delta i - \sigma(j)}, \zeta^{-\Delta j - \sigma(i)}\rangle$$

Now note that this works for any $i, j$ with $f(\zeta^i s)$ and $f(\zeta^j s) \in T'$. In particular, if we had three such $i, j, k$, adding the values for $i, k$ and $k, j$ gives us

$$(\zeta^{-\Delta i} - \zeta^{-\Delta j})t \in \mathbb{Q}\langle \zeta^{-\Delta k - \sigma(i)}, \zeta^{-\Delta i - \sigma(k)}, \zeta^{-\Delta k - \sigma(j)}, \zeta^{-\Delta j - \sigma(k)}\rangle$$

Since $(\zeta^{-\Delta i} - \zeta^{-\Delta j})t$ lies in both $\mathbb{Q}$ subspaces, this gives us a rational linear relation between 6 powers of $\zeta$, which is a polynomial with at most 6 nonzero monomials. As long as $\Delta i \neq \Delta j$, this polynomial is nonzero, and this can always be achieved as long as there are more than 2 points in $f(S') \cap T'$. Thus, by Corollary 4.13, there are two powers whose exponents differ by a multiple of $\frac{\ell-1}{30}$. In fact, there must be two powers in different subspaces that differ by this much, since otherwise the two subspaces can't interact. Since there are at most 2 values of $k$ that achieve each $\zeta^{\Delta k}$, and $\zeta^{\sigma(k)}$ is uniquely determined by $k$, there are only finitely many possible values for $k$. In fact, for both powers in the 2 dimensional subspace, there are at most $60 + 30 + 60 + 30 = 180$ values of $k$ that could give a difference that is a multiple of $\frac{\ell-1}{30}$. Thus, if there are more than 360 points in $|f(S') \cap T'|$, we could choose a $k$ that doesn't give any differences that are a multiple of $\frac{\ell-1}{30}$, which is a contradiction. Thus, $|f(S') \cap T'| \leq 360$, as desired. □

## 5 Further ideas

While we did not get a definitive conclusion on whether such polynomials exist, there are still further ideas we haven't fully explored.

### 5.1 Exploiting roots of unity in $\mathbb{Z}[x^f \mid f \in \mathbb{Z}[a]]$

In theorem 4.6, we only look at primitive vectors $r$ that don't divide vectors in $S \coprod T$. However, there might still be information to be garnered from other cases. If we allow coefficients in $\mathbb{C}$, we could factor everything into the form $x^v - \omega$, where $\omega$ is some root of unity, and $v$ is a primitive vector.

We can then attempt the same method of quotienting by this factor. The analogue of Lemma 4.2 would become

$$\mathbb{C}[V]/(x^v - \omega) \cong \mathbb{C}[V/\langle v\rangle],$$

however, the isomorphism would no longer be canonical. It requires extending $v$ to an integral basis of $V$, and taking an isomorphism $x^v \mapsto \omega x^v$.

Now we have to be careful with whether "primitive" vectors are preserved. For example, we could have $2u + v$ be primitive, but it would not be primitive in $V/\langle v\rangle$.

After reducing all the factors to its primitive factors inside $\mathbb{C}[V/\langle v\rangle]$, we can then state an analogue of Theorem 4.6.

**Definition 5.1.** An *augmented set* of a lattice $V$ is a multiset of tuples $(v, \omega)$ such that $v \in V$ is a primitive vector and $\omega$ is some root of unity.

Before, we represented a polynomial formed by taking product over factors like $(x^s - 1)$ by a multiset $S$ of (not necessarily primitive) vectors $s$. We see that we can extract an augmented set $\tilde{S}$ from a polynomial corresponding to a multiset $S$ with elements in $V$ by,

$$\prod_{ns\in S}(x^{ns} - 1) = \prod_{ns\in S}\prod_{k=0}^{n-1}(x^s - \zeta_n^k)$$

where $s$ is primitive, and forming the multiset by taking the corresponding $(s, \zeta_n^k)$'s. Note that augmented sets are still augmented under isomorphisms such as $x^v \mapsto \omega x^v$.

Under the quotient of $(x^v - \omega)$, we have that augmented set of $V$ may not immediately give an augmented set of $V/\langle v\rangle$ due to the primitive-ness not being preserved. Even still, we may break factors down further to their primitive parts as above.

Thus, under a quotient by $(x^v - \omega)$, the augmented set $\tilde{S}$ of $V$ describing some polynomial $F$ gives another augmented set $\overline{S}$ of $V/\langle v\rangle$ describing the same polynomial $F$ but with the substitution $x^v \mapsto \omega$.

Call $\overline{S}$ the reduction of $\tilde{S}$. By following the same steps as the proof of Theorem 4.6, we can prove that the augmented sets $\overline{S}$ and $\overline{T}$ are in bijection (not just the vectors, but the corresponding roots of unity as well). This however, does not give a bijection of the pre-quotient augmented sets $\tilde{S}$ and $\tilde{T}$.

Now, one can notice that if we start with a good polynomial, the augmented sets we get will satisfy certain Galois symmetries. Indeed, in the $\omega = 1$ case, we take advantage of this fact to get a bijection in the pre-quotient sets. The general case is not as nice. For example consider

$$(x^a + 1)(x^{a+2} + 1) - (x^{2a+2} - x^{a+1} + 1) = x^a(x^2 + x + 1).$$

This example is not $a$-stable, but the corresponding augmented sets are $\tilde{S} = \{(a, -1), (a+2, -1)\}$ and $\tilde{T} = \{(a+1, \zeta_6), (a+1, \zeta_6^{-1})\}$. These are not in bijection (not even the roots of unity are), but under the reduction they are.

Thus, if we can parse this post-quotient bijection along with the Galois symmetry in a better way, we expect to gain a lot more information.

### 5.2 Points on the convex hull of $S \coprod T$

Note that after embedding into the complex plane, if $S \equiv T \bmod r$, then there exists an edge on the convex hull parallel to $r$ (the "furthest" points must be paired). Additionally, we know that if $\pm r$ appears $k$ times in $R$, while no multiple appears in $S \coprod T$, then there exist edges on the convex hull containing at least $2k$ points. This follows from the following theorem.

**Theorem 5.2.** Let $r$ be a primitive vector. If $(x^r - 1)^k$ divides

$$x^{s_0} \prod_{s \in S}(x^s - 1) \pm x^{t_0} \prod_{t \in T}(x^t - 1),$$

no vectors in $S \coprod T$ are multiples of $r$, and $S \cap T = \emptyset$, then for every $s \in S$, there are at least $k-1$ other vectors $s_1, \ldots, s_{k-1} \in S$ such that $s \equiv \pm s_i \bmod r$.

*Proof.* When $k = 1$, the statement is vacuously true, so assume $k \geq 2$. First, by theorem 4.6, $S \coprod -S$ and $T \coprod -T$ are equivalent mod $r$. By writing $x^t - 1 = -x^t(x^{-t} - 1)$, where necessary, we can WLOG assume $S \equiv T$. One can check that this forces the $\pm$ to be a minus sign. Additionally, under quotienting by $(x^r - 1)$, all the factors of the products are the same, which forces $s_0 \equiv t_0 \bmod r$. Now extend $r$ to a basis, giving an isomorphism to $\mathbb{Z}[x_1^{\pm 1}, \ldots, x_k^{\pm 1}]$ with $x^r \mapsto x_1$, and consider taking the derivative with respect to $x^r$. Then the $S$ product becomes

$$(s_0)_r x^{s_0 - r} \prod_{s \in S}(x^s - 1) + x^{s_0} \sum_{s \in S}(s)_r x^{s-r} \prod_{s' \in S \setminus \{s\}}(x^{s'} - 1)$$

where $(v)_r$ denotes the $r$-component of $v$ when decomposed using the chosen basis. A similar expression holds for $T$. Since $k \geq 2$, after taking derivatives, the resulting polynomial should still be divisible by $(x^r - 1)$, so quotient out by it. The resulting expression is

$$(s_0 - t_0)_r x^{\overline{s_0}} \prod_{s \in S}(x^{\overline{s}} - 1) + x^{\overline{s_0}} \sum_{s \in S}(s - f(s))_r x^{\overline{s}} \prod_{s' \in S \setminus \{s\}}(x^{\overline{s}'} - 1)$$

where $f : S \to T$ is the bijection that gives $s - f(s) \in \langle r \rangle$. This holds since $\overline{s} = \overline{f(s)}$ by definition, so we can combine the polynomials together. Now suppose some $s \in S$ has $\overline{s} = n\overline{s_*}$, where $s_*$ is primitive. Then taking the map $x^{s_*} \mapsto \zeta_n$, like in theorem 4.6, almost all terms vanish, and we are left with

$$(s - f(s))_r x^{\overline{s_0}} \prod_{s' \in S \setminus s}(x^{\overline{s}'} - 1) \mapsto 0 \text{ when } x^{s_*} \mapsto \zeta_n$$

Since $S \cap T = \emptyset$, $s \neq f(s)$, so $(s - f(s))_r \neq 0$, and since $x^{\overline{s_0}}$ is a unit, one of the factors inside the product must go to 0, so there exists some $s' \neq s$ with $\overline{s} \mid \overline{s}'$. Since this holds for all $s \in S$, again by similar logic to theorem 4.6, there exists two $s \neq s'$ in $S$ such that $s \equiv \pm s' \bmod r$. By factoring these terms out and repeating, we can show that for any $s \in S$, there is some other $s' \in S$ with $s \equiv \pm s'$. mod $r$. This proves the theorem for $k = 2$, and in general, we can repeat similar arguments after taking more derivatives. $\square$

In particular, if there are $N$ elements of $R$ that don't divide any vectors in $S \coprod T$, then there are at least $2N$ points on the convex hull of $S$ and $T$. If $N = |S| + |T|$, then this means every point of $S$ and $T$ lies on the convex hull, which would greatly restrict the sets, since then any line parallel to an $r$ intersects the convex hull on an edge, or in at most 2 points. And in the constructions for $\ell = 5, 7$, every points does indeed lie on the convex hull, so this condition can actually be satisfied.

One might expect that if $|S|$ and $|T|$ get large, then $|R|$ should also get large, as our polynomials get bigger and bigger, in some sense. However, we were unable to get a definitive lower bound on the number of $r$ in $R$ that don't divide any elements of $S \coprod T$.

### 5.3 The global unit equation for $\mathbb{Q}_{\infty,\ell}$

It is known [2] that there are no solutions to $x + y = 1$ in $\mathbb{Q}_{\infty,\ell}$ where $x, y$ are both units. Now suppose we have polynomials like in Lemma 3.3. If we could factor out every $(x^v - 1)$ factor where $v$ is primitive, we would be left with an equation of the form

$$x^{s_0} \prod_{s \in S} \Phi_{n_s}(x^s) + x^{t_0} \prod_{t \in T} \Phi_{n_t}(x^t) = x^{r_0} \prod_{rinR} \Phi_{n_r}(x^r)$$

where every $n_i$ is at least 2. But we also know from [6, section 2] that if none of the $n_i$ are powers of $\ell$, then taking $x \mapsto \zeta_{\ell^N}$ maps all these polynomials to units in $\mathbb{Q}_{\infty,\ell}$, which would be impossible by above. Thus, we should maybe expect it to be hard for all of the $x^v - 1$'s to factor, and so we should always be able to get $S \equiv T \bmod r$ for some $r$. But we still haven't been able to rule out this case from fully happening.

### 5.4 Arboreal extensions

We note that if $x, y$ are a solution to the rearranged $S$-unit equation

$$x - y = 1 \text{ where } x, y \text{ are } S\text{-units},$$

then we have that $x^{1/\ell}$ and $y^{1/\ell}$ also induce an $S$-unit solution. We have that $x^{1/\ell}$ divides $x$, similar for $y$, and that

$$x^{1/\ell} - y^{1/\ell} \mid x - y$$

which implies that $x^{1/\ell}, y^{1/\ell}, x^{1/\ell} - y^{1/\ell}$ are $S$-units. Thus, taking ratios give us new solutions.

However, we fail to get new solutions in the above manner as there are no new $\ell$-th roots added in the $\mathbb{Q}_{\infty,\ell}$ tower. As the extension is Galois, if a new $\ell$-th root exists, its conjugates also has to exist, which forces $\zeta_\ell$ to exist, but it is not in the totally real field $\mathbb{Q}_{\infty,\ell}$.

Thus, we can try look for an analogue of "$\ell$-th roots" that are more compatible with $\mathbb{Q}_{\infty,\ell}$. More concretely, we are looking for monic $f \in \mathbb{Z}[x]$ with degree $\ell$ such that $f(0) = 0$, which ensures that when $a + b = 1$ and $a, b$ are $S-$units, then roots $y, z$ of $f(x) = a$ and $f(x) = b$ satisfy,

1. As $f(0) = 0$, we have $y, z$ divides $a, b$, thus an $S$-unit.

2. As $y - z$ divides $f(y) - f(z)$, it's also an $S$-unit.

Thus, once we have a more compatible $f$ (one that doesn't get completely ruled out as $x^\ell$), we reduce to a problem of finding starter solutions to the $S$-unit equation, which then ideally gives a tree-like set of solutions (thus arboreal).

We note that this direction is completely different from Siksek and Visser's approach. One possible benefit could be that this approach can give us a family of solutions that are less explicit in construction.

## 6 Appendix (Constructions for $\ell = 9, 13$)

Here, we explain how the two orbit and three orbit constructions for $\ell = 9$ and $\ell = 13$ respectively work. For $\ell = 9$, let $S$ be the orbits generated by $1 + i + 2i\sqrt{2}$ and $-1 - i + 2i\sqrt{2}$, while $T$ are the orbits generated by $-1+i+2i\sqrt{2}$ and $1-i+2i\sqrt{2}$. Note that these lie in $\mathbb{Q}(\zeta_8)$ since $\zeta_8+\zeta_8^3 = i\sqrt{2}$. These points can be visualized as a square centered around $2i\sqrt{2}$, where we take every other vertex. Now instead of showing that $S \equiv T \bmod r = 1$, we will instead show that for every $s \in S$ and $0 \leq k \leq 3$, there exists some $t \in (s + \zeta_8^k \mathbb{Q}) \cap T$. Note that this condition is invariant under rotation by $\zeta_8$, so we only need to focus on $1 + i + 2i\sqrt{2}$ and $-1 - i + 2i\sqrt{2}$. For $k = 0, 2$, it is clear such a $t$ exists, since we can just take the other vertices of the square. Thus, it suffices to consider when $k = 1, 3$. Now consider rotating the square by $\zeta_8^2$. We get another axis-aligned square, now centered at $-2\sqrt{2}$, and so is a translation by $-2\sqrt{2} - 2i\sqrt{2} = -4\zeta_8$ of our original square. Thus, for every vertex of our original square, there's is a vertex of the rotated square with a difference of $4\zeta_8$, and we can show that this pairs up points in different sets. Thus, the $k = 1$ case is finished. By rotating by $\zeta_8^{-2}$, we can also show the $k = 3$ case works. Thus, this is indeed a two orbit construction for $\ell = 9$.

The $\ell = 13$ case is similar, but now we take a regular hexagon of side length 1 centered at $2i = 2\zeta_{12}^3$. We still take every other vertex, and the rotation arguments still hold.

## References


[1] Dan Abramovich. *Birational geometry for number theorists.* 2007. arXiv: `math/0701105 [math.AG]`.

[2] Nuno Freitas, Alain Kraus, and Samir Siksek. "On asymptotic Fermat over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$". *Algebra Number Theory* 14.9 (2020), pp. 2571–2574. DOI: `10.2140/ant.2020.14.2571`. URL: `https://doi.org/10.2140%2Fant.2020.14.2571`.

[3] Ralph Greenberg. "Introduction to Iwasawa theory for elliptic curves". *IAS/Park City Mathematics Series* 9 (2001), pp. 407–464.

[4] Barry Mazur. "Rational points of abelian varieties with values in towers of number fields". *Invent. Math.* 18 (1972), pp. 183–266.

[5] I. J. Schoenberg. "A note on the cyclotomic polynomial". *Mathematika* 11.2 (1964), pp. 131–136. DOI: `10.1112/S0025579300004344`.

[6] Samir Siksek and Robin Visser. *Curves with few bad primes over cyclotomic $\mathbb{Z}_\ell$-extensions.* 2023. arXiv: `2302.02514 [math.NT]`.

[7] Yuri Zarhin. "Endomorphisms of Abelian varieties, cyclotomic extensions and Lie algebras". *Russian Academy of Sciences Sbornik Mathematics* 201 (Jan. 2010), pp. 93–102. DOI: `10.1070/SM2010V201N12ABEH004132;`.

[8] Yuri G. Zarhin and Alexey N. Parshin. *Finiteness Problems in Diophantine Geometry.* 2009. arXiv: `0912.4325 [math.NT]`.