Higher-Dimensional Approximations on Spheres

Analysis and Number Theory

Tristan Sun and Jason Mao

August 17, 2026

Table of Contents

1. Two-Dimensional Liouville's Theorem
2. Two-Dimensional Approximation Given Modulo Constraint
3. Rational Approximations on Spheres

Two-Dimensional Liouville's Theorem

Theorem (Two-Dimensional Liouville's Theorem)

Suppose $\{1, a_1, b_1\} \in \mathbb{R}$ *form a basis of a real algebraic field of degree* 3. *Then there exists* $C \in \mathbb{R}^+$ *for which:*

$$\|Ma_1 + Nb_1\| \geq \frac{C}{\max\{M, N\}^2} \text{ for all } (M, N) \in \mathbb{Z}^2 \setminus \{(0, 0)\}.$$

Two-Dimensional Liouville's Theorem

Theorem (Two-Dimensional Liouville's Theorem)

Suppose $\{1, a_1, b_1\} \in \mathbb{R}$ *form a basis of a real algebraic field of degree* 3*. Then there exists* $C \in \mathbb{R}^+$ *for which:*

$$\|Ma_1 + Nb_1\| \geq \frac{C}{\max\{M, N\}^2} \text{ for all } (M, N) \in \mathbb{Z}^2 \setminus \{(0,0)\}.$$

Proof of Two-Dimensional Liouville's

Proof Sketch. Write $b_1 = Xa_1^2 + Ya_1 + Z$ for rational constants $X, Y, Z \in \mathbb{Q}$. Let y denote the integer nearest $Ma_1 + Nb_1$.

Proof of Two-Dimensional Liouville's

Proof Sketch. Write $b_1 = Xa_1^2 + Ya_1 + Z$ for rational constants $X, Y, Z \in \mathbb{Q}$. Let y denote the integer nearest $Ma_1 + Nb_1$.

Recall a_1 is a root of a rational cubic $P(x) \in \mathbb{Q}[x]$ with two other roots a_2 and a_3. Then by Vieta's Formulas,

$$(\bigstar) \quad a_1 + a_2 + a_3, \quad a_1a_2 + a_2a_3 + a_3a_1, \quad \text{and} \quad a_1a_2a_3 \quad \text{are rational.}$$

Proof of Two-Dimensional Liouville's

Proof Sketch. Write $b_1 = Xa_1^2 + Ya_1 + Z$ for rational constants $X, Y, Z \in \mathbb{Q}$. Let y denote the integer nearest $Ma_1 + Nb_1$.

Recall a_1 is a root of a rational cubic $P(x) \in \mathbb{Q}[x]$ with two other roots a_2 and a_3. Then by Vieta's Formulas,

$$(\bigstar) \quad a_1 + a_2 + a_3, \quad a_1a_2 + a_2a_3 + a_3a_1, \quad \text{and} \quad a_1a_2a_3 \quad \text{are rational.}$$

Define $b_2 := Xa_2^2 + Ya_2 + Z$ and $b_3 := Xa_3^2 + Ya_3 + Z$. Consider the quantity:

$$\lambda := \prod_{i=1}^{3} \left[y - (Ma_i + Nb_i)\right].$$

Proof of Two-Dimensional Liouville's

Proof Sketch. Write $b_1 = Xa_1^2 + Ya_1 + Z$ for rational constants $X, Y, Z \in \mathbb{Q}$. Let y denote the integer nearest $Ma_1 + Nb_1$.

Recall a_1 is a root of a rational cubic $P(x) \in \mathbb{Q}[x]$ with two other roots a_2 and a_3. Then by Vieta's Formulas,

$$(\bigstar) \quad a_1 + a_2 + a_3, \quad a_1a_2 + a_2a_3 + a_3a_1, \quad \text{and} \quad a_1a_2a_3 \quad \text{are rational.}$$

Define $b_2 := Xa_2^2 + Ya_2 + Z$ and $b_3 := Xa_3^2 + Ya_3 + Z$. Consider the quantity:

$$\lambda := \prod_{i=1}^{3} \left[y - (Ma_i + Nb_i) \right].$$

View the above as a polynomial in y, M, and N. By $(\bigstar)$, every coefficient is rational, so λ is rational and nonzero.

Proof of Two-Dimensional Liouville's

Proof Sketch. Write $b_1 = Xa_1^2 + Ya_1 + Z$ for rational constants $X, Y, Z \in \mathbb{Q}$. Let y denote the integer nearest $Ma_1 + Nb_1$.

Recall a_1 is a root of a rational cubic $P(x) \in \mathbb{Q}[x]$ with two other roots a_2 and a_3. Then by Vieta's Formulas,

$$(\bigstar) \quad a_1 + a_2 + a_3, \quad a_1a_2 + a_2a_3 + a_3a_1, \quad \text{and} \quad a_1a_2a_3 \quad \text{are rational.}$$

Define $b_2 := Xa_2^2 + Ya_2 + Z$ and $b_3 := Xa_3^2 + Ya_3 + Z$. Consider the quantity:

$$\lambda := \prod_{i=1}^{3} \left[y - (Ma_i + Nb_i) \right].$$

View the above as a polynomial in y, M, and N. By $(\bigstar)$, every coefficient is rational, so λ is rational and nonzero. Thus, for some boundable constant T,

$$|\lambda| \geq \frac{1}{T} \implies |y - (Ma_1 + Nb_1)| \geq \frac{1/T}{|y - (Ma_2 + Nb_2)| \cdot |y - (Ma_3 + Nb_3)|}$$

Proof of Two-Dimensional Liouville's

Proof Sketch. Write $b_1 = Xa_1^2 + Ya_1 + Z$ for rational constants $X, Y, Z \in \mathbb{Q}$. Let y denote the integer nearest $Ma_1 + Nb_1$.

Recall a_1 is a root of a rational cubic $P(x) \in \mathbb{Q}[x]$ with two other roots a_2 and a_3. Then by Vieta's Formulas,

$$(\bigstar) \quad a_1 + a_2 + a_3, \quad a_1 a_2 + a_2 a_3 + a_3 a_1, \quad \text{and} \quad a_1 a_2 a_3 \quad \text{are rational.}$$

Define $b_2 := Xa_2^2 + Ya_2 + Z$ and $b_3 := Xa_3^2 + Ya_3 + Z$. Consider the quantity:

$$\lambda := \prod_{i=1}^{3} \left[y - (Ma_i + Nb_i) \right].$$

View the above as a polynomial in y, M, and N. By ($\bigstar$), every coefficient is rational, so λ is rational and nonzero. Thus, for some boundable constant T,

$$|\lambda| \geq \frac{1}{T} \implies |y - (Ma_1 + Nb_1)| \geq \frac{1/T}{|y - (Ma_2 + Nb_2)| \cdot |y - (Ma_3 + Nb_3)|}$$

The RHS of the above is at least $\frac{C}{\max\{M,N\}^2}$ for an appropriate constant C. ■

Table of Contents

1. Two-Dimensional Liouville's Theorem
2. Two-Dimensional Approximation Given Modulo Constraint
3. Rational Approximations on Spheres

Two-Dimensional Approximation Given Modulo Constraint

Theorem (Two-Dimensional Approximation Given Modulo Constraint)

For any two (nonzero) real numbers β_1 and β_2, there exist infinitely many ordered triples $(b_1, b_2, q) \in \mathbb{Z}$ for which

$$|q\beta_1 - b_1|^2 + |q\beta_2 - b_2|^2 < 1 \quad \text{and} \quad b_1^2 + b_2^2 \equiv 0 \pmod{q}.$$

Two-Dimensional Approximation Given Modulo Constraint

Theorem (Two-Dimensional Approximation Given Modulo Constraint)

For any two (nonzero) real numbers β_1 and β_2, there exist infinitely many ordered triples $(b_1, b_2, q) \in \mathbb{Z}$ for which

$$|q\beta_1 - b_1|^2 + |q\beta_2 - b_2|^2 < 1 \quad \text{and} \quad b_1^2 + b_2^2 \equiv 0 \pmod{q}.$$

Proof Outline. Recall **Minkowski's Convex Body Theorem.**

Theorem (Minkowski's Convex Body Theorem)

If S is a convex, bounded subset of $\mathbb{R}^d$ symmetric about the origin with volume greater than 2^d, then S contains a nonzero lattice point.

Two-Dimensional Approximation Given Modulo Constraint

Theorem (Two-Dimensional Approximation Given Modulo Constraint)

For any two (nonzero) real numbers β_1 and β_2, there exist infinitely many ordered triples $(b_1, b_2, q) \in \mathbb{Z}$ for which

$$|q\beta_1 - b_1|^2 + |q\beta_2 - b_2|^2 < 1 \quad \text{and} \quad b_1^2 + b_2^2 \equiv 0 \pmod{q}.$$

Proof Outline. Recall **Minkowski's Convex Body Theorem.**

Theorem (Minkowski's Convex Body Theorem)

If S is a convex, bounded subset of $\mathbb{R}^d$ symmetric about the origin with volume greater than 2^d, then S contains a nonzero lattice point.

Define bodies $\mathbf{R}_t, \mathbf{B} \subseteq \mathbb{R}^4$. Find lattice points $(w, x, y, z) \in \mathbf{R}_t \subseteq \mathbf{B}$, where $\mathbf{R}_t$ is a convex symmetric set with volume $\frac{16\pi}{3} > 2^4$. Take $(b_1, b_2, q) = (y, z, w)$.

- The condition $(w, x, y, z) \in \mathbf{B}$ guarantees $b_1^2 + b_2^2 \equiv 0 \pmod{q}$.
- The condition $(w, x, y, z) \in \mathbf{R}_t$ guarantees $|q\beta_1 - b_1|^2 + |q\beta_2 - b_2|^2 < 1$.

Proof (1/4): Defining Bodies

Define $f : \mathbb{R}^4 \to \mathbb{R}$ by $f(w, x, y, z) = wx - y^2 - z^2$, and define:

$$\mathbf{B} := \{(w, x, y, z) \in \mathbb{R}^4 : |f(w, x, y, z)| < 1\}.$$

Proof (1/4): Defining Bodies

Define $f : \mathbb{R}^4 \to \mathbb{R}$ by $f(w, x, y, z) = wx - y^2 - z^2$, and define:

$$\mathbf{B} := \{(w, x, y, z) \in \mathbb{R}^4 : |f(w, x, y, z)| < 1\}.$$

If $(w, x, y, z) \in \mathbb{Z}^4$ is in $\mathbf{B}$, then $y^2 + z^2 \equiv 0 \pmod{w}$.

Proof (1/4): Defining Bodies

Define $f : \mathbb{R}^4 \to \mathbb{R}$ by $f(w,x,y,z) = wx - y^2 - z^2$, and define:

$$\mathbf{B} := \{(w,x,y,z) \in \mathbb{R}^4 : |f(w,x,y,z)| < 1\}.$$

If $(w,x,y,z) \in \mathbb{Z}^4$ is in $\mathbf{B}$, then $y^2 + z^2 \equiv 0 \pmod{w}$.

Define $\mathbf{R} \subseteq \mathbb{R}^4$ as follows.

$$\mathbf{R} := \{(w,x,y,z) \in \mathbb{R}^4 : |w+x| < 2 \text{ and } |w-x| < 2\sqrt{1-y^2-z^2}\}.$$

Proof (1/4): Defining Bodies

Define $f : \mathbb{R}^4 \to \mathbb{R}$ by $f(w,x,y,z) = wx - y^2 - z^2$, and define:

$$\mathbf{B} := \{(w,x,y,z) \in \mathbb{R}^4 : |f(w,x,y,z)| < 1\}.$$

If $(w,x,y,z) \in \mathbb{Z}^4$ is in $\mathbf{B}$, then $y^2 + z^2 \equiv 0 \pmod{w}$.

Define $\mathbf{R} \subseteq \mathbb{R}^4$ as follows.

$$\mathbf{R} := \{(w,x,y,z) \in \mathbb{R}^4 : |w+x| < 2 \text{ and } |w-x| < 2\sqrt{1 - y^2 - z^2}\}.$$

The set $\mathbf{R}$ is convex, symmetric, has volume $\frac{16\pi}{3} > 2^4$, and is a subset of $\mathbf{B}$.

Proof (2/4): Altering Bodies

For parameters $t \in \mathbb{R}$, along with our given real numbers β_1 and β_2, we define:

$$G_t := \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad S := \begin{pmatrix} 1 & 0 & 0 & 0 \\ \beta_1^2 + \beta_2^2 & 1 & -2\beta_1 & -2\beta_2 \\ -\beta_1 & 0 & 1 & 0 \\ -\beta_2 & 0 & 0 & 1 \end{pmatrix}.$$

Proof (2/4): Altering Bodies

For parameters $t \in \mathbb{R}$, along with our given real numbers β_1 and β_2, we define:

$$G_t := \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad S := \begin{pmatrix} 1 & 0 & 0 & 0 \\ \beta_1^2 + \beta_2^2 & 1 & -2\beta_1 & -2\beta_2 \\ -\beta_1 & 0 & 1 & 0 \\ -\beta_2 & 0 & 0 & 1 \end{pmatrix}.$$

1. We have $\det G_t = \det S = 1$ for all choices of t.

Proof (2/4): Altering Bodies

For parameters $t \in \mathbb{R}$, along with our given real numbers β_1 and β_2, we define:

$$G_t := \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad S := \begin{pmatrix} 1 & 0 & 0 & 0 \\ \beta_1^2 + \beta_2^2 & 1 & -2\beta_1 & -2\beta_2 \\ -\beta_1 & 0 & 1 & 0 \\ -\beta_2 & 0 & 0 & 1 \end{pmatrix}.$$

1. We have $\det G_t = \det S = 1$ for all choices of t.
2. For all $(w, x, y, z) \in \mathbb{R}^4$, we have:

$$f(w, x, y, z) = f(G_t(w, x, y, z)) = f(S(w, x, y, z)).$$

In other words, f is invariant under G_t and S.

Proof (2/4): Altering Bodies

For parameters $t \in \mathbb{R}$, along with our given real numbers β_1 and β_2, we define:

$$G_t := \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad S := \begin{pmatrix} 1 & 0 & 0 & 0 \\ \beta_1^2 + \beta_2^2 & 1 & -2\beta_1 & -2\beta_2 \\ -\beta_1 & 0 & 1 & 0 \\ -\beta_2 & 0 & 0 & 1 \end{pmatrix}.$$

1. We have $\det G_t = \det S = 1$ for all choices of t.
2. For all $(w, x, y, z) \in \mathbb{R}^4$, we have:

$$f(w, x, y, z) = f(G_t(w, x, y, z)) = f(S(w, x, y, z)).$$

   In other words, f is invariant under G_t and S.

For any real number $t \in \mathbb{R}$, define:

$$\mathbf{R}_t := S^{-1} G_t \mathbf{R}.$$

Proof (2/4): Altering Bodies

For parameters $t \in \mathbb{R}$, along with our given real numbers β_1 and β_2, we define:

$$G_t := \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t^{-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad S := \begin{pmatrix} 1 & 0 & 0 & 0 \\ \beta_1^2 + \beta_2^2 & 1 & -2\beta_1 & -2\beta_2 \\ -\beta_1 & 0 & 1 & 0 \\ -\beta_2 & 0 & 0 & 1 \end{pmatrix}.$$

1. We have $\det G_t = \det S = 1$ for all choices of t.
2. For all $(w, x, y, z) \in \mathbb{R}^4$, we have:

   $$f(w, x, y, z) = f(G_t(w, x, y, z)) = f(S(w, x, y, z)).$$

   In other words, f is invariant under G_t and S.

For any real number $t \in \mathbb{R}$, define:

$$\mathbf{R}_t := S^{-1} G_t \mathbf{R}.$$

Then $\mathbf{R}_t$ is (still) convex, symmetric, has volume $\frac{16\pi}{3} > 2^4$, and $\mathbf{R}_t \subseteq \mathbf{B}$ holds.

Proof (3/4): Finding One Lattice Point

By Minkowski's Theorem, the set $\mathbf{R}_t$ has a nonzero lattice point (w, x, y, z). Thus,

$$\mathbf{R} \ni G_t^{-1} S \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{t} \cdot w \\ t \cdot \left[w(\beta_1^2 + \beta_2^2) + x - 2\beta_1 y - 2\beta_2 z \right] \\ y - \beta_1 w \\ z - \beta_2 w \end{pmatrix} =: \begin{pmatrix} w_t \\ x_t \\ y_t \\ z_t \end{pmatrix}.$$

Proof (3/4): Finding One Lattice Point

By Minkowski's Theorem, the set $\mathbf{R}_t$ has a nonzero lattice point (w, x, y, z). Thus,

$$\mathbf{R} \ni G_t^{-1} S \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{t} \cdot w \\ t \cdot \left[w(\beta_1^2 + \beta_2^2) + x - 2\beta_1 y - 2\beta_2 z\right] \\ y - \beta_1 w \\ z - \beta_2 w \end{pmatrix} =: \begin{pmatrix} w_t \\ x_t \\ y_t \\ z_t \end{pmatrix}.$$

Since $(w_t, x_t, y_t, z_t) \in \mathbf{R}$, it follows by definition of $\mathbf{R}$ that:

$$\begin{aligned} &|w_t - x_t| < 2\sqrt{1 - y_t^2 - z_t^2} \\ \implies &1 > y_t^2 + z_t^2 = (w\beta_1 - y)^2 + (w\beta_2 - z)^2. \quad (\bigstar_1) \end{aligned}$$

Proof (3/4): Finding One Lattice Point

By Minkowski's Theorem, the set $\mathbf{R}_t$ has a nonzero lattice point (w, x, y, z). Thus,

$$\mathbf{R} \ni G_t^{-1} S \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{t} \cdot w \\ t \cdot \left[w(\beta_1^2 + \beta_2^2) + x - 2\beta_1 y - 2\beta_2 z \right] \\ y - \beta_1 w \\ z - \beta_2 w \end{pmatrix} =: \begin{pmatrix} w_t \\ x_t \\ y_t \\ z_t \end{pmatrix}.$$

Since $(w_t, x_t, y_t, z_t) \in \mathbf{R}$, it follows by definition of $\mathbf{R}$ that:

$$|w_t - x_t| < 2\sqrt{1 - y_t^2 - z_t^2}$$
$$\implies 1 > y_t^2 + z_t^2 = (w\beta_1 - y)^2 + (w\beta_2 - z)^2. \quad (\bigstar_1)$$

Since $(w, x, y, z) \in \mathbf{R}_t \subseteq \mathbf{B}$, it follows by definition of $\mathbf{B}$ that:

$$|wx - y^2 - z^2| < 1 \implies wx - y^2 - z^2 = 0 \implies y^2 + z^2 \equiv 0 \pmod{w}. \quad (\bigstar_2)$$

Proof (3/4): Finding One Lattice Point

By Minkowski's Theorem, the set $\mathbf{R}_t$ has a nonzero lattice point (w, x, y, z). Thus,

$$\mathbf{R} \ni G_t^{-1} S \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{t} \cdot w \\ t \cdot \left[w(\beta_1^2 + \beta_2^2) + x - 2\beta_1 y - 2\beta_2 z \right] \\ y - \beta_1 w \\ z - \beta_2 w \end{pmatrix} =: \begin{pmatrix} w_t \\ x_t \\ y_t \\ z_t \end{pmatrix}.$$

Since $(w_t, x_t, y_t, z_t) \in \mathbf{R}$, it follows by definition of $\mathbf{R}$ that:

$$|w_t - x_t| < 2\sqrt{1 - y_t^2 - z_t^2}$$
$$\implies 1 > y_t^2 + z_t^2 = (w\beta_1 - y)^2 + (w\beta_2 - z)^2. \quad (\bigstar_1)$$

Since $(w, x, y, z) \in \mathbf{R}_t \subseteq \mathbf{B}$, it follows by definition of $\mathbf{B}$ that:

$$|wx - y^2 - z^2| < 1 \implies wx - y^2 - z^2 = 0 \implies y^2 + z^2 \equiv 0 \pmod{w}. \quad (\bigstar_2)$$

Facts $(\bigstar_1)$ and $(\bigstar_2)$ show $(b_1, b_2, q) = (y, z, w)$ satisfies the theorem.

Proof (4/4): Finding Infinite Lattice Points

The sole purpose of G_t is to generate infinitely many solutions (w, x, y, z).

Proof (4/4): Finding Infinite Lattice Points

The sole purpose of G_t is to generate infinitely many solutions (w, x, y, z).

Assume we always choose (by convention) (w, x, y, z) so that $w < 0$ and $x > 0$, and that we always choose t positive.

Proof (4/4): Finding Infinite Lattice Points

The sole purpose of G_t is to generate infinitely many solutions (w, x, y, z).

Assume we always choose (by convention) (w, x, y, z) so that $w < 0$ and $x > 0$, and that we always choose t positive.

Suppose two choices $t = t_0$ and $t = t_1$ yield lattice points $(w_0, x_0, y_0, z_0) \in \mathbf{R}_{t_0}$ and $(w_1, x_1, y_1, z_1) \in \mathbf{R}_{t_1}$, respectively. Now assume for the sake of contradiction that $w_1 = w_0$, $y_1 = y_0$, and $x_1 = x_0$ for all t_1.

Proof (4/4): Finding Infinite Lattice Points

The sole purpose of G_t is to generate infinitely many solutions (w, x, y, z).

Assume we always choose (by convention) (w, x, y, z) so that $w < 0$ and $x > 0$, and that we always choose t positive.

Suppose two choices $t = t_0$ and $t = t_1$ yield lattice points $(w_0, x_0, y_0, z_0) \in \mathbf{R}_{t_0}$ and $(w_1, x_1, y_1, z_1) \in \mathbf{R}_{t_1}$, respectively. Now assume for the sake of contradiction that $w_1 = w_0$, $y_1 = y_0$, and $x_1 = x_0$ for all t_1.

Since $(x_1, w_1, y_1, z_1) \in \mathbf{R}$, we have:

$$\begin{aligned} & |x_1 - w_1| < 2 \\ \implies & \left| t_1 \cdot \left[w_0(\beta_1^2 + \beta_2^2) + x_1 - 2\beta_1 y_0 - 2\beta_2 z_0 \right] - \frac{w_0}{t_1} \right| < 2 \quad \text{for all } t_1 \in \mathbb{R}^+ \end{aligned}$$

Proof (4/4): Finding Infinite Lattice Points

The sole purpose of G_t is to generate infinitely many solutions (w, x, y, z).

Assume we always choose (by convention) (w, x, y, z) so that $w < 0$ and $x > 0$, and that we always choose t positive.

Suppose two choices $t = t_0$ and $t = t_1$ yield lattice points $(w_0, x_0, y_0, z_0) \in \mathbf{R}_{t_0}$ and $(w_1, x_1, y_1, z_1) \in \mathbf{R}_{t_1}$, respectively. Now assume for the sake of contradiction that $w_1 = w_0$, $y_1 = y_0$, and $x_1 = x_0$ for all t_1.

Since $(x_1, w_1, y_1, z_1) \in \mathbf{R}$, we have:

$$
\begin{aligned}
& \left|x_1 - w_1\right| < 2 \\
\Longrightarrow \quad & \left| t_1 \cdot \left[w_0(\beta_1^2 + \beta_2^2) + x_1 - 2\beta_1 y_0 - 2\beta_2 z_0 \right] - \frac{w_0}{t_1} \right| < 2 \quad \text{for all } t_1 \in \mathbb{R}^+ \\
\Longrightarrow \quad & \left| t_1 x_1 - \frac{w_0}{t_1} \right| < 2 \quad \text{for all sufficiently small } t_1 \in \mathbb{R}^+
\end{aligned}
$$

Proof (4/4): Finding Infinite Lattice Points

The sole purpose of G_t is to generate infinitely many solutions (w, x, y, z).

Assume we always choose (by convention) (w, x, y, z) so that $w < 0$ and $x > 0$, and that we always choose t positive.

Suppose two choices $t = t_0$ and $t = t_1$ yield lattice points $(w_0, x_0, y_0, z_0) \in \mathbf{R}_{t_0}$ and $(w_1, x_1, y_1, z_1) \in \mathbf{R}_{t_1}$, respectively. Now assume for the sake of contradiction that $w_1 = w_0$, $y_1 = y_0$, and $x_1 = x_0$ for all t_1.

Since $(x_1, w_1, y_1, z_1) \in \mathbf{R}$, we have:

$$\begin{aligned} & |x_1 - w_1| < 2 \\ \implies & \left| t_1 \cdot \left[w_0(\beta_1^2 + \beta_2^2) + x_1 - 2\beta_1 y_0 - 2\beta_2 z_0 \right] - \frac{w_0}{t_1} \right| < 2 \quad \text{for all } t_1 \in \mathbb{R}^+ \\ \implies & \left| t_1 x_1 - \frac{w_0}{t_1} \right| < 2 \quad \text{for all sufficiently small } t_1 \in \mathbb{R}^+ \end{aligned}$$

But the final inequality is a contradiction, since $w_0 < 0$ and $x_1 > 0$. ■

Table of Contents

1. Two-Dimensional Liouville's Theorem
2. Two-Dimensional Approximation Given Modulo Constraint
3. Rational Approximations on Spheres

Two-Dimensional Circular Approximations

Define $\mathbb{S}^1 \subseteq \mathbb{R}^2$ by $\mathbb{S}^1 := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$. (This is the unit circle.)

Theorem (Rational Approximations on the Unit Circle)

Consider a point $(\alpha_1, \alpha_2) \in \mathbb{S}^1 \setminus \mathbb{Q}^2$. Then for all reals $\varepsilon > 0$, there are infinitely many pairs of rationals $(\frac{A_1}{Q}, \frac{A_2}{Q}) \in \mathbb{S}^1 \cap \mathbb{Q}^2$ where $A_1, A_2, Q \in \mathbb{Z}$ for which

$$\sqrt{\left(\alpha_1 - \frac{A_1}{Q}\right)^2 + \left(\alpha_2 - \frac{A_2}{Q}\right)^2} < \frac{1}{Q\sqrt{2}} + \varepsilon.$$

Generating Rational Points on Circles

Theorem (Pythagorean Triple Generation)

All rational points $\left(\frac{A_1}{Q}, \frac{A_2}{Q}\right)$ *on* $\mathbb{S}^1$ *are of the following form for some* $m, n \in \mathbb{Z}$.

$$\left(\frac{A_1}{Q}, \frac{A_2}{Q}\right) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right)$$

Generating Rational Points on Circles

Theorem (Pythagorean Triple Generation)

All rational points $\left(\frac{A_1}{Q}, \frac{A_2}{Q}\right)$ *on* $\mathbb{S}^1$ *are of the following form for some* $m, n \in \mathbb{Z}$.

$$\left(\frac{A_1}{Q}, \frac{A_2}{Q}\right) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right)$$

Proof Sketch. Rational points on $\mathbb{S}^1$ are generated by intersecting lines of slope $\lambda \in \mathbb{Q}$ through $(-1, 0)$ with $\mathbb{S}^1$ at X_λ.

$$X_\lambda = \left(\frac{1 - \lambda^2}{1 + \lambda^2}, \frac{2\lambda}{1 + \lambda^2}\right) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right) \quad \text{(Vieta's)} \quad \blacksquare$$

Generating Rational Points on Circles

Theorem (Pythagorean Triple Generation)

All rational points $\left(\frac{A_1}{Q}, \frac{A_2}{Q}\right)$ *on* $\mathbb{S}^1$ *are of the following form for some* $m, n \in \mathbb{Z}$.

$$\left(\frac{A_1}{Q}, \frac{A_2}{Q}\right) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right)$$

Proof Sketch. Rational points on $\mathbb{S}^1$ are generated by intersecting lines of slope $\lambda \in \mathbb{Q}$ through $(-1, 0)$ with $\mathbb{S}^1$ at X_λ.

$$X_\lambda = \left(\frac{1 - \lambda^2}{1 + \lambda^2}, \frac{2\lambda}{1 + \lambda^2}\right) = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right) \quad \text{(Vieta's)} \quad \blacksquare$$

Theorem ("Pythagorean" Tuple Generation)

Points $\left(\frac{A_1}{Q}, \dots, \frac{A_n}{Q}\right) \in \mathbb{S}^{n-1} \cap \mathbb{Q}^n$ *are of this form for some* $f, g_1, \dots, g_{n-1} \in \mathbb{Z}$.

$$\frac{A_1}{Q} = \frac{f^2 - g_1^2 - \cdots - g_{n-1}^2}{f^2 + g_1^2 + \cdots + g_{n-1}^2} \quad \text{and} \quad \frac{A_i}{Q} = \frac{2fg_{i-1}}{f^2 + g_1^2 + \cdots + g_{n-1}^2}$$

Proof (1/3): Setting Up

An equivalent restatement of the theorem:

Theorem (Rational Approximations on the Unit Circle, Restated)

Consider a point $(\alpha_1, \alpha_2) \in \mathbb{S}^1 \setminus \mathbb{Q}^2$. *Then for all reals* $\varepsilon > 0$, *there are infinitely many triples of integers* $(A_1, A_2, Q) \in \mathbb{Z}^3$ *for which*

$$A_1^2 + A_2^2 = Q^2 \text{ and } |Q\alpha_1 - A_1|^2 + |Q\alpha_2 - A_2|^2 < \frac{1}{2} + \varepsilon.$$

Proof (1/3): Setting Up

An equivalent restatement of the theorem:

Theorem (Rational Approximations on the Unit Circle, Restated)

Consider a point $(\alpha_1, \alpha_2) \in \mathbb{S}^1 \setminus \mathbb{Q}^2$. Then for all reals $\varepsilon > 0$, there are infinitely many triples of integers $(A_1, A_2, Q) \in \mathbb{Z}^3$ for which

$$A_1^2 + A_2^2 = Q^2 \text{ and } |Q\alpha_1 - A_1|^2 + |Q\alpha_2 - A_2|^2 < \frac{1}{2} + \varepsilon.$$

Main Idea. We instead seek pairs of integers $(m, n) \in \mathbb{Z}^2$ and set $(A_1, A_2, Q) = (m^2 - n^2, 2mn, m^2 + n^2)$, chosen so that:

$$A_1 : A_2 \approx \alpha_1 : \alpha_2 \implies m : n \approx (\alpha_1 + 1) : \alpha_2.$$

Proof (1/3): Setting Up

An equivalent restatement of the theorem:

Theorem (Rational Approximations on the Unit Circle, Restated)

Consider a point $(\alpha_1, \alpha_2) \in \mathbb{S}^1 \setminus \mathbb{Q}^2$. Then for all reals $\varepsilon > 0$, there are infinitely many triples of integers $(A_1, A_2, Q) \in \mathbb{Z}^3$ for which

$$A_1^2 + A_2^2 = Q^2 \text{ and } |Q\alpha_1 - A_1|^2 + |Q\alpha_2 - A_2|^2 < \frac{1}{2} + \varepsilon.$$

Main Idea. We instead seek pairs of integers $(m, n) \in \mathbb{Z}^2$ and set $(A_1, A_2, Q) = (m^2 - n^2, 2mn, m^2 + n^2)$, chosen so that:

$$A_1 : A_2 \approx \alpha_1 : \alpha_2 \implies m : n \approx (\alpha_1 + 1) : \alpha_2.$$

In particular, pick $(m, n) = (p_k, q_k)$ where $\frac{p_k}{q_k}$ is a CF convergent of $\frac{\alpha_1+1}{\alpha_2}$.

$$m = n\left(\frac{\alpha_1 + 1}{\alpha_2}\right) + \frac{1}{C \cdot n} \text{ for some boundable constant } C.$$

Proof (2/3): Computations

Express the desired inequality in terms of α_1, α_2, n, and C.

$$\frac{1}{2} + \varepsilon > (\alpha_1 Q - A_1)^2 + (\alpha_2 Q - A_2)^2$$

Proof (2/3): Computations

Express the desired inequality in terms of α_1, α_2, n, and C.

$$\begin{aligned}\frac{1}{2} + \varepsilon &> (\alpha_1 Q - A_1)^2 + (\alpha_2 Q - A_2)^2 \\ &= \left(\frac{2}{C}(-\alpha_2) + \frac{\alpha_1 - 1}{C^2 n^2}\right)^2 + \left(\frac{2}{C}(\alpha_1) + \frac{\alpha_2}{C^2 n^2}\right)^2\end{aligned}$$

Proof (2/3): Computations

Express the desired inequality in terms of α_1, α_2, n, and C.

$$\begin{aligned}\frac{1}{2} + \varepsilon > (\alpha_1 Q - A_1)^2 + (\alpha_2 Q - A_2)^2 \\ = \left(\frac{2}{C}(-\alpha_2) + \frac{\alpha_1 - 1}{C^2 n^2}\right)^2 + \left(\frac{2}{C}(\alpha_1) + \frac{\alpha_2}{C^2 n^2}\right)^2 \\ = \frac{4}{C^2} + \mathcal{O}\left(\frac{1}{n^2}\right).\end{aligned}$$

Proof (2/3): Computations

Express the desired inequality in terms of α_1, α_2, n, and C.

$$\begin{aligned}\frac{1}{2} + \varepsilon &> (\alpha_1 Q - A_1)^2 + (\alpha_2 Q - A_2)^2 \\ &= \left(\frac{2}{C}(-\alpha_2) + \frac{\alpha_1 - 1}{C^2 n^2}\right)^2 + \left(\frac{2}{C}(\alpha_1) + \frac{\alpha_2}{C^2 n^2}\right)^2 \\ &= \frac{4}{C^2} + \mathcal{O}\left(\frac{1}{n^2}\right).\end{aligned}$$

Conclusion. It remains to prove $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Proof (3/3): Bounding the Constant

We want $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \dots] + [0; a_k, a_{k-1}, \dots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Proof (3/3): Bounding the Constant

We want $\frac{4}{C^2} < \frac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \ldots] + [0; a_k, a_{k-1}, \ldots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Case 1. Infinitely many partial quotients satisfy $a_k \geq 3$.

Proof (3/3): Bounding the Constant

We want $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \dots] + [0; a_k, a_{k-1}, \dots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Case 1. Infinitely many partial quotients satisfy $a_k \geq 3$. Pick $(m, n) = (p_k, q_k)$ when $a_{k+1} \geq 3$. Then:

$$C > (3) + (0) = 3 > 2\sqrt{2}. \qquad \checkmark$$

Proof (3/3): Bounding the Constant

We want $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \ldots] + [0; a_k, a_{k-1}, \ldots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Case 2. Infinite k satisfy $a_k = 1$, and infinite k satisfy $a_k = 2$.

Proof (3/3): Bounding the Constant

We want $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \dots] + [0; a_k, a_{k-1}, \dots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Case 2. Infinite k satisfy $a_k = 1$, and infinite k satisfy $a_k = 2$. Pick $(m, n) = (p_k, q_k)$ when $a_{k+1} = 2$ and $a_{k+2} = 1$. Then:

$$C > ([2; 1, \overline{1, 2}]) + \left(\frac{1}{3}\right) = \left(2 + \frac{\sqrt{3}}{3}\right) + \left(\frac{1}{3}\right) > 2\sqrt{2}. \qquad \checkmark$$

Proof (3/3): Bounding the Constant

We want $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \ldots] + [0; a_k, a_{k-1}, \ldots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Case 3. For all $k > N$, we have $a_k = 2$.

Proof (3/3): Bounding the Constant

We want $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \dots] + [0; a_k, a_{k-1}, \dots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Case 3. For all $k > N$, we have $a_k = 2$. Pick $(m, n) = (p_k, q_k)$ for large k. Then:

$$C > ([2; \overline{2}]) + ([2; \overline{2}] - \varepsilon_k) = \left(\sqrt{2} + 1\right) + \left(\sqrt{2} - 1 - \varepsilon_k\right) = 2\sqrt{2} - \varepsilon_k.$$

The error ε_k tends to zero for large k. ✓

Proof (3/3): Bounding the Constant

We want $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \ldots] + [0; a_k, a_{k-1}, \ldots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Case 4. For all $k > N$, we have $a_k = 1$.

Proof (3/3): Bounding the Constant

We want $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \ldots] + [0; a_k, a_{k-1}, \ldots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Case 4. For all $k > N$, we have $a_k = 1$. Pick $(m, n) = (p_k, q_k)$ for large k. Then:

$$C > ([1; \overline{1}]) + ([0; \overline{1}] - \varepsilon_k) = \left(\frac{\sqrt{5}+1}{2}\right) + \left(\frac{\sqrt{5}-1}{2}\right) - \varepsilon_k = \sqrt{5} - \varepsilon_k.$$

Proof (3/3): Bounding the Constant

We want $\dfrac{4}{C^2} < \dfrac{1}{2} + \varepsilon$, or equivalently, $C > 2\sqrt{2} - \varepsilon$.

Let a_k denote the k^{th} partial quotient of $\frac{\alpha_1+1}{\alpha_2} \approx \frac{m}{n}$. Then:

$$C = [a_{k+1}; a_{k+2}, a_{k+3}, \dots] + [0; a_k, a_{k-1}, \dots]$$

We proceed in **four cases** based on properties of the partial quotients $\{a_i\}$.

Case 4. For all $k > N$, we have $a_k = 1$. Pick $(m, n) = (p_k, q_k)$ for large k. Then:

$$C > ([1; \overline{1}]) + ([0; \overline{1}] - \varepsilon_k) = \left(\frac{\sqrt{5}+1}{2}\right) + \left(\frac{\sqrt{5}-1}{2}\right) - \varepsilon_k = \sqrt{5} - \varepsilon_k.$$

Observe $(m, n) = (p_k, q_k)$ are both odd for infinitely many k. For these values of k, we may choose $(A_1, A_2, Q) = \left(\frac{m^2-n^2}{2}, \frac{2mn}{2}, \frac{m^2+n^2}{2}\right)$ instead.

Then we only need $C > \frac{\sqrt{2}}{2} - \varepsilon$, which is true. ✓

Rational Approximations on Spheres

Theorem (Rational Approximations on the Unit Sphere)

Consider a point $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{S}^2 \setminus \mathbb{Q}^3$*. Then for all reals* $\varepsilon > 0$*, there are infinitely many triples of rationals* $(\frac{A_1}{Q}, \frac{A_2}{Q}, \frac{A_3}{Q}) \in \mathbb{S}^2 \cap \mathbb{Q}^3$ *where* $A_1, A_2, A_3, Q \in \mathbb{Z}$ *for which*

$$\sqrt{\left(\alpha_1 - \frac{A_1}{Q}\right)^2 + \left(\alpha_2 - \frac{A_2}{Q}\right)^2 + \left(\alpha_3 - \frac{A_3}{Q}\right)^2} < \frac{2}{Q}.$$

Proof (1/4): Setting Up

An equivalent restatement of the theorem:

Theorem (Rational Approximations on the Unit Sphere, Restated)

Consider a point $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{S}^2 \setminus \mathbb{Q}^3$. *Then for all reals* $\varepsilon > 0$, *there are infinitely many triples of integers* $(A_1, A_2, A_3 Q) \in \mathbb{N}^3$ *for which*

$$A_1^2 + A_2^2 + A_3^2 = Q^2 \text{ and } |Q\alpha_1 - A_1|^2 + |Q\alpha_2 - A_2|^2 + |Q\alpha_3 - A_3|^2 < 4.$$

Proof (1/4): Setting Up

An equivalent restatement of the theorem:

Theorem (Rational Approximations on the Unit Sphere, Restated)

Consider a point $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{S}^2 \setminus \mathbb{Q}^3$. *Then for all reals* $\varepsilon > 0$, *there are infinitely many triples of integers* $(A_1, A_2, A_3 Q) \in \mathbb{N}^3$ *for which*

$$A_1^2 + A_2^2 + A_3^2 = Q^2 \text{ and } |Q\alpha_1 - A_1|^2 + |Q\alpha_2 - A_2|^2 + |Q\alpha_3 - A_3|^2 < 4.$$

Main Idea. We instead seek triples of integers $(f, g_1, g_2) \in \mathbb{Z}^3$ and set $(A_1, A_2, A_3, Q) = (f^2 - g_1^2 - g_2^2, 2fg_1, 2fg_2, f^2 + g_1^2 + g_2^2)$, chosen so that:

$$A_1 : A_2 : A_3 \approx \alpha_1 : \alpha_2 : \alpha_3 \implies f : g_1 : g_2 \approx (\alpha_1 + 1) : \alpha_2 : \alpha_3.$$

Proof (1/4): Setting Up

An equivalent restatement of the theorem:

Theorem (Rational Approximations on the Unit Sphere, Restated)

Consider a point $(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{S}^2 \setminus \mathbb{Q}^3$. Then for all reals $\varepsilon > 0$, there are infinitely many triples of integers $(A_1, A_2, A_3 Q) \in \mathbb{N}^3$ for which

$$A_1^2 + A_2^2 + A_3^2 = Q^2 \textit{ and } |Q\alpha_1 - A_1|^2 + |Q\alpha_2 - A_2|^2 + |Q\alpha_3 - A_3|^2 < 4.$$

Main Idea. We instead seek triples of integers $(f, g_1, g_2) \in \mathbb{Z}^3$ and set $(A_1, A_2, A_3, Q) = (f^2 - g_1^2 - g_2^2, 2fg_1, 2fg_2, f^2 + g_1^2 + g_2^2)$, chosen so that:

$$A_1 : A_2 : A_3 \;\approx\; \alpha_1 : \alpha_2 : \alpha_3 \;\implies\; f : g_1 : g_2 \;\approx\; (\alpha_1 + 1) : \alpha_2 : \alpha_3.$$

We formally express the above approximation with the equations below.

$$g_1 = \left(\frac{\alpha_2}{\alpha_1 + 1}\right) + \frac{1}{C_1 \cdot f} \text{ and } g_2 = \left(\frac{\alpha_3}{\alpha_1 + 1}\right) + \frac{1}{C_2 \cdot f}.$$

Proof (2/4): Computations

Express the desired inequality in terms of α_1, α_2, α_3, n, and constants C_1, C_2.

$$4 > (Q\alpha_1 - A_1)^2 + (Q\alpha_2 - A_2)^2 + (Q\alpha_3 - A_3)^2$$

Proof (2/4): Computations

Express the desired inequality in terms of α_1, α_2, α_3, n, and constants C_1, C_2.

$$\begin{aligned} 4 &> (Q\alpha_1 - A_1)^2 + (Q\alpha_2 - A_2)^2 + (Q\alpha_3 - A_3)^2 \\ &= \text{(some very messy computations)} \\ &= \frac{4}{C_1^2} + \frac{4}{C_2^2}. \end{aligned}$$

Proof (2/4): Computations

Express the desired inequality in terms of α_1, α_2, α_3, n, and constants C_1, C_2.

$$\begin{aligned} 4 &> (Q\alpha_1 - A_1)^2 + (Q\alpha_2 - A_2)^2 + (Q\alpha_3 - A_3)^2 \\ &= \text{(some very messy computations)} \\ &= \frac{4}{C_1^2} + \frac{4}{C_2^2}. \end{aligned}$$

Conclusion. It remains to prove $\frac{1}{C_1^2} + \frac{1}{C_2^2} < 1$, where:

$$\frac{1}{C_1} = g_1 f - \left(\frac{\alpha_2}{\alpha_1 + 1}\right) f^2 \quad \text{and} \quad \frac{1}{C_2} = g_2 f - \left(\frac{\alpha_3}{\alpha_1 + 1}\right) f^2.$$

Proof (2/4): Computations

Express the desired inequality in terms of α_1, α_2, α_3, n, and constants C_1, C_2.

$$\begin{aligned} 4 > &\ (Q\alpha_1 - A_1)^2 + (Q\alpha_2 - A_2)^2 + (Q\alpha_3 - A_3)^2 \\ &= \text{(some very messy computations)} \\ &= \frac{4}{C_1^2} + \frac{4}{C_2^2}. \end{aligned}$$

Conclusion. It remains to prove $\frac{1}{C_1^2} + \frac{1}{C_2^2} < 1$, where:

$$\frac{1}{C_1} = g_1 f - \left(\frac{\alpha_2}{\alpha_1 + 1}\right) f^2 \quad \text{and} \quad \frac{1}{C_2} = g_2 f - \left(\frac{\alpha_3}{\alpha_1 + 1}\right) f^2.$$

Theorem (Sufficient Restatement of the Theorem)

There are infinitely many $(f, g_1, g_2) \in \mathbb{Z}^3$ satisfying:

$$\left(f\left(\frac{\alpha_2}{\alpha_1 + 1}\right) - g_1\right)^2 + \left(f\left(\frac{\alpha_3}{\alpha_1 + 1}\right) - g_2\right)^2 < \frac{1}{f^2}.$$

Proof (2/4): Computations

Express the desired inequality in terms of α_1, α_2, α_3, n, and constants C_1, C_2.

$$\begin{aligned} 4 &> (Q\alpha_1 - A_1)^2 + (Q\alpha_2 - A_2)^2 + (Q\alpha_3 - A_3)^2 \\ &= \text{(some very messy computations)} \\ &= \frac{4}{C_1^2} + \frac{4}{C_2^2}. \end{aligned}$$

Conclusion. It remains to prove $\frac{1}{C_1^2} + \frac{1}{C_2^2} < 1$, where:

$$\frac{1}{C_1} = g_1 f - \left(\frac{\alpha_2}{\alpha_1 + 1}\right) f^2 \quad \text{and} \quad \frac{1}{C_2} = g_2 f - \left(\frac{\alpha_3}{\alpha_1 + 1}\right) f^2.$$

Theorem (Sufficient Restatement of the Theorem)

There are infinitely many $(f, g_1, g_2) \in \mathbb{Z}^3$ satisfying:

$$\left(f\left(\frac{\alpha_2}{\alpha_1 + 1}\right) - g_1\right)^2 + \left(f\left(\frac{\alpha_3}{\alpha_1 + 1}\right) - g_2\right)^2 < \frac{1}{f^2}.$$

Concern. The above statement is just, uh, not true.

Proof (3/4): Fixing with GCDs

Here's the fix. Recall that we defined the following:

$$(A_1, A_2, A_3, Q) = (f^2 - g_1^2 - g_2^2, 2fg_1, 2fg_2, f^2 + g_1^2 + g_2^2)$$

$$\implies \text{we seek} \quad \left(f\left(\frac{\alpha_2}{\alpha_1+1}\right) - g_1\right)^2 + \left(f\left(\frac{\alpha_3}{\alpha_1+1}\right) - g_2\right)^2 < \frac{1}{f^2}.$$

Proof (3/4): Fixing with GCDs

Here's the fix. Recall that we defined the following:

$$(A_1, A_2, A_3, Q) = (f^2 - g_1^2 - g_2^2, 2fg_1, 2fg_2, f^2 + g_1^2 + g_2^2)$$

$$\implies \text{we seek} \quad \left(f\left(\frac{\alpha_2}{\alpha_1+1}\right) - g_1\right)^2 + \left(f\left(\frac{\alpha_3}{\alpha_1+1}\right) - g_2\right)^2 < \frac{1}{f^2}.$$

However, if the above has $\gcd(A_1, A_2, A_3, Q) = s > 1$, then we may redefine:

$$(A_1, A_2, A_3, Q) = \left(\frac{f^2 - g_1^2 - g_2^2}{s}, \frac{2fg_1}{s}, \frac{2fg_2}{s}, \frac{f^2 + g_1^2 + g_2^2}{s}\right)$$

$$\implies \text{we seek} \quad \left(f\left(\frac{\alpha_2}{\alpha_1+1}\right) - g_1\right)^2 + \left(f\left(\frac{\alpha_3}{\alpha_1+1}\right) - g_2\right)^2 < \frac{s^2}{f^2}.$$

Proof (3/4): Fixing with GCDs

Here's the fix. Recall that we defined the following:

$$(A_1, A_2, A_3, Q) = (f^2 - g_1^2 - g_2^2, 2fg_1, 2fg_2, f^2 + g_1^2 + g_2^2)$$

$$\implies \text{we seek} \quad \left(f\left(\frac{\alpha_2}{\alpha_1+1}\right) - g_1\right)^2 + \left(f\left(\frac{\alpha_3}{\alpha_1+1}\right) - g_2\right)^2 < \frac{1}{f^2}.$$

However, if the above has $\gcd(A_1, A_2, A_3, Q) = s > 1$, then we may redefine:

$$(A_1, A_2, A_3, Q) = \left(\frac{f^2 - g_1^2 - g_2^2}{s}, \frac{2fg_1}{s}, \frac{2fg_2}{s}, \frac{f^2 + g_1^2 + g_2^2}{s}\right)$$

$$\implies \text{we seek} \quad \left(f\left(\frac{\alpha_2}{\alpha_1+1}\right) - g_1\right)^2 + \left(f\left(\frac{\alpha_3}{\alpha_1+1}\right) - g_2\right)^2 < \frac{s^2}{f^2}.$$

Question. How can we guarantee that $\gcd(A_1, A_2, A_3, Q)$ is large?

Proof (4/4): The Solution

Theorem (Two-Dimensional Approximation Given Modulo Constraint)

For any two (nonzero) real numbers β_1 and β_2, there exist infinitely many ordered triples $(b_1, b_2, q) \in \mathbb{Z}$ for which

$$|q\beta_1 - b_1|^2 + |q\beta_2 - b_2|^2 < 1 \quad \textit{and} \quad b_1^2 + b_2^2 \equiv 0 \pmod{q}.$$

Proof (4/4): The Solution

Theorem (Two-Dimensional Approximation Given Modulo Constraint)

For any two (nonzero) real numbers β_1 and β_2, there exist infinitely many ordered triples $(b_1, b_2, q) \in \mathbb{Z}$ for which

$$|q\beta_1 - b_1|^2 + |q\beta_2 - b_2|^2 < 1 \quad \textit{and} \quad b_1^2 + b_2^2 \equiv 0 \pmod{q}.$$

Proof. Apply the above theorem for $\beta_1 = \dfrac{\alpha_2}{\alpha_1 + 1}$ and $\beta_2 = \dfrac{\alpha_3}{\alpha_1 + 1}$ and take:

$$(A_1, A_2, A_3, Q) = \left(\frac{q^2 - b_1^2 - b_2^2}{q}, \frac{2qb_1}{q}, \frac{2qb_2}{q}, \frac{q^2 + b_1^2 + b_2^2}{q} \right).$$

Then the inequality we seek is:

$$|q\beta_1 - b_1|^2 + |q\beta_2 - b_2|^2 < \frac{q^2}{q^2} = 1,$$

but this immediate from the statement of the above theorem. ■

end of presentaiton

thakns for listening