Simultaneous Diophantine Approximation with Excluded Primes

László Babai
Daniel Štefankovič

Dirichlet (1842)
Simultaneous Diophantine Approximation

Given reals $\alpha_1, \alpha_2, \ldots, \alpha_n, Q$

$\exists$ **integers** $r_1, \ldots, r_n$ **and** q

such that $q \le Q$ **and**

$$\left|\alpha_i q - r_i\right| \le Q^{-1/n} \quad \textbf{for all } i$$

$\left|\alpha_i Q - p_i\right| \le 1/2$ **trivial**

Simultaneous Diophantine Approximation with an excluded prime

Given reals $\alpha_1, \alpha_2, \ldots, \alpha_n$ **prime** p

$\exists$**?** **integers** $r_1, \ldots, r_n$ **and** q

such that $\gcd(p, q) = 1$ **and**

$$\left| q\alpha_i - r_i \right| \leq \varepsilon \quad \textbf{for all } i$$

Simultaneous diophantine ε-approximation excluding p

Not always possible

Example $p = 3$

If

$$\alpha_1 = 1/3$$

then

$$\varepsilon \geq |\, q\alpha_1 - r_1 \,| = |\, q/3 - r_1 \,| \geq 1/3$$

Simultaneous diophantine ε-approximation excluding p

obstacle with 2 variables

If

$$\alpha_1 + 2\alpha_2 = 1/\ p$$

then

$$\varepsilon \geq |\ q\alpha_1 - r_1\ |$$

$$\varepsilon \geq |\ q\alpha_2 - r_2\ |$$

$$3\varepsilon \geq |\ q(\alpha_1 + 2\alpha_2) - (r_1 + 2r_2)\ | \geq 1/\ p$$

Simultaneous diophantine ε-approximation excluding p

general obstacle

If

$$b_1\alpha_1 + b_2\alpha_2 + \ldots + b_n\alpha_n = 1/p + t$$

then

$$\varepsilon \sum |b_i| \geq 1/p$$

Simultaneous diophantine ε-approximation excluding p

Theorem:

If there is no ε-approximation excluding p then there exists an obstacle with

$$\sum |b_i| \leq n^{3/2} / \varepsilon$$

Kronecker's theorem ( ):

Arbitrarily good approximation excluding p possible IFF no obstacle.

Simultaneous diophantine ε-approximation excluding p

obstacle with

$$\sum |b_i| \le n^{3/2} / \varepsilon$$

necessary to prevent ε-approximation excluding p

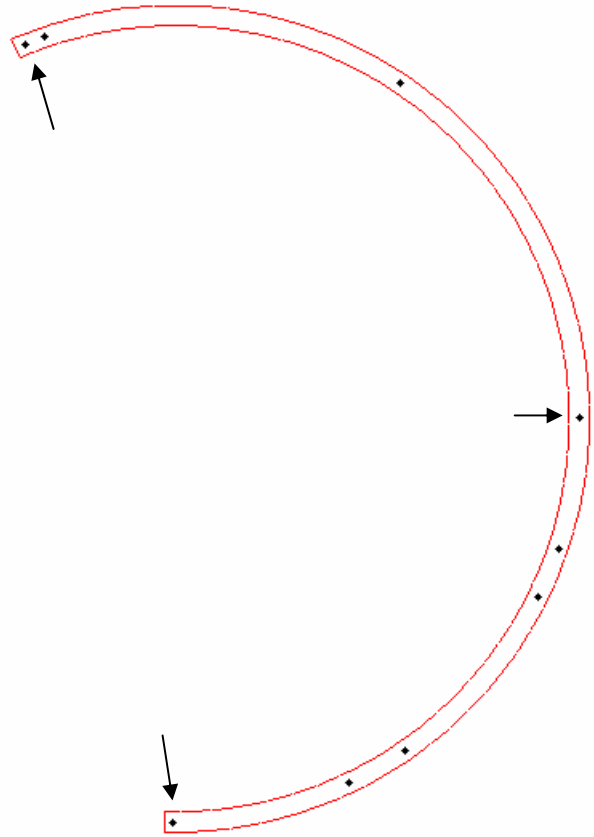
sufficient to prevent $\frac{\varepsilon}{pn^{3/2}}$-approximation excluding p

Motivating example

Shrinking by stretching

Motivating example

set $A \subseteq (\mathbb{Z}/m\mathbb{Z})$



arc length of A

$$\max_{a \in A} |a (\mathrm{mod}\, m)|$$

$$\gcd(x, m) = 1$$

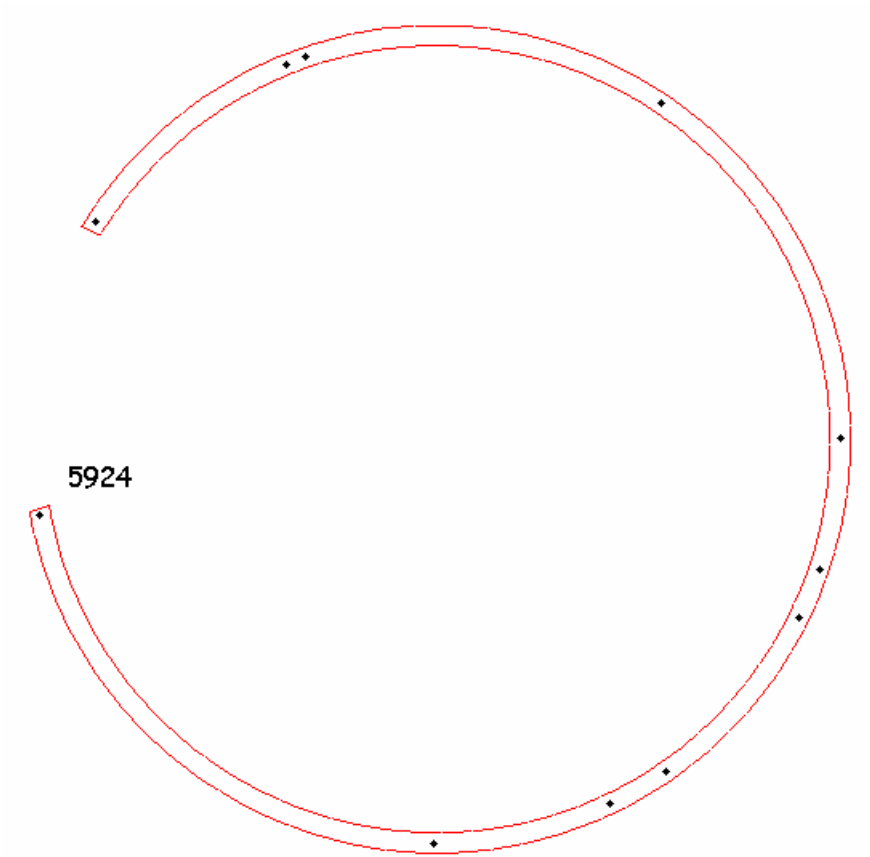
stretching by x

$$a \mapsto ax \bmod m$$

$$Ax = \{ax \,|\, a \in A\}$$

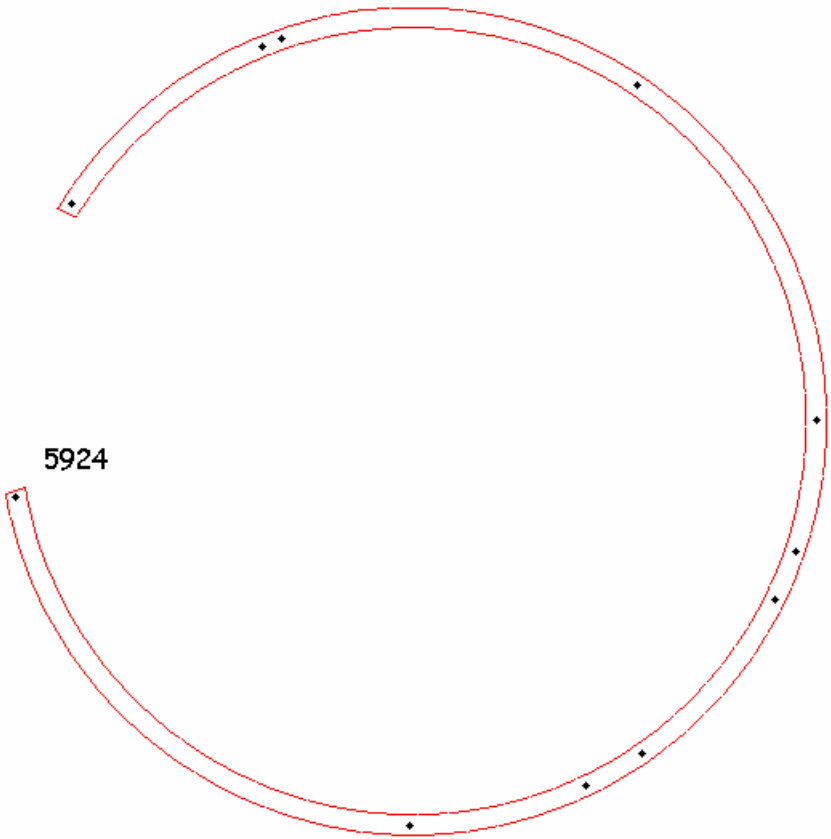
Example of the motivating example

A = 11-th roots of unity mod 11177

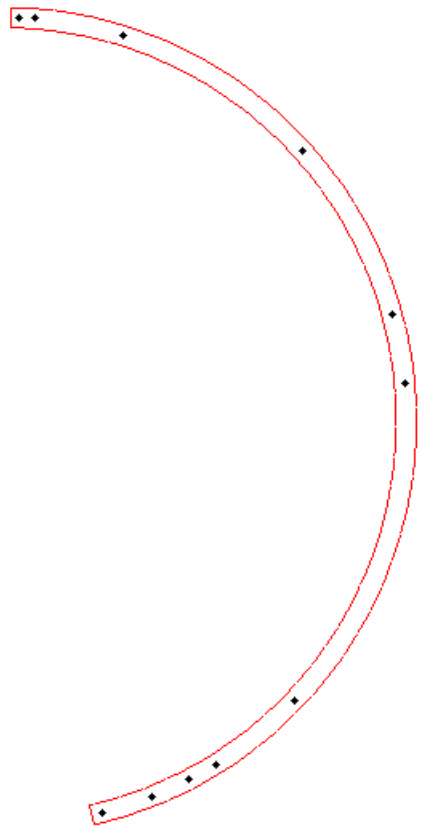


Example of the motivating example

A = 11-th roots of unity mod 11177



168



Shrinking modulo a prime

If m a prime

then

every small set can be shrunk

Shrinking modulo a prime

m **a prime**

$d = |A|$

there exists x **such that**

arc-length of $Ax \leq m^{1-1/d}$

proof:

$$\frac{a_1}{m}, \ldots, \frac{a_d}{m}$$

$$Q := m - 1$$

Dirichlet

$$\exists\, q;\ 0 < q \leq Q$$

$$|q\alpha_i - p_i| \leq \frac{1}{Q^{1/n}}$$

$$x := q$$

Shrinking modulo any number

m ~~a prime~~ $\longrightarrow$ every small set can be shrunk

?

Shrinking modulo any number

m ~~a prime~~ $\longrightarrow$ ~~every small set can be shrunk~~

$$m = 2^k \qquad A = \{1, 1 + 2^{k-1}\}$$

If

$$\gcd(x, m) = 1$$

then the arc-length of Ax

$$\geq 2^{k-2}$$

Where does the proof break?

$$m = 2^k$$

proof:

$$\frac{a_1}{m}, \ldots, \frac{a_d}{m}$$

$$Q := m - 1$$

$$x := q$$

Dirichlet

$$\exists\, q;\ 0 < q \leq Q$$

$$\left| q\alpha_i - p_i \right| \leq \frac{1}{Q^{1/n}}$$

Where does the proof break?

$$m = 2^k$$

need:

approximation excluding 2

proof:

$$\frac{a_1}{m}, \ldots, \frac{a_d}{m}$$

$$Q := m - 1$$

$$x := q$$

Dirichlet

$$\exists\, q; 0 < q \leq Q$$

$$|q\alpha_i - p_i| \leq \frac{1}{Q^{1/n}}$$

Shrinking cyclotomic classes

m ~~a prime~~ $\longrightarrow$ ~~every small set can be shrunk~~

set of interest – cyclotomic class
(i.e. the set of r-th roots of unity mod m)

- **locally testable codes**
- **diameter of Cayley graphs**
- **Warring problem mod p^k**
- **intersection conditions modulo p^k**

Shrinking cyclotomic classes

cyclotomic class

can be shrunk

Shrinking cyclotomic classes

cyclotomic class

can be shrunk

Show that there is no small obstacle!

Theorem:

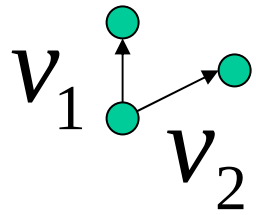
If there is no ε-approximation excluding p then there exists an obstacle with

$$\sum |b_i| \leq n^{3/2} / \varepsilon$$

Lattice

$$v_1, \ldots, v_n \in \mathbb{R}^n$$

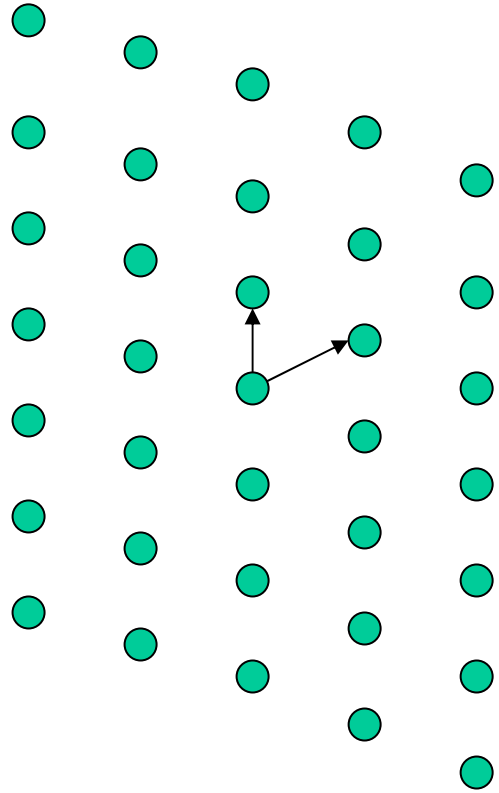
linearly independent



Lattice

$$v_1, \ldots, v_n \in \mathbb{R}^n$$

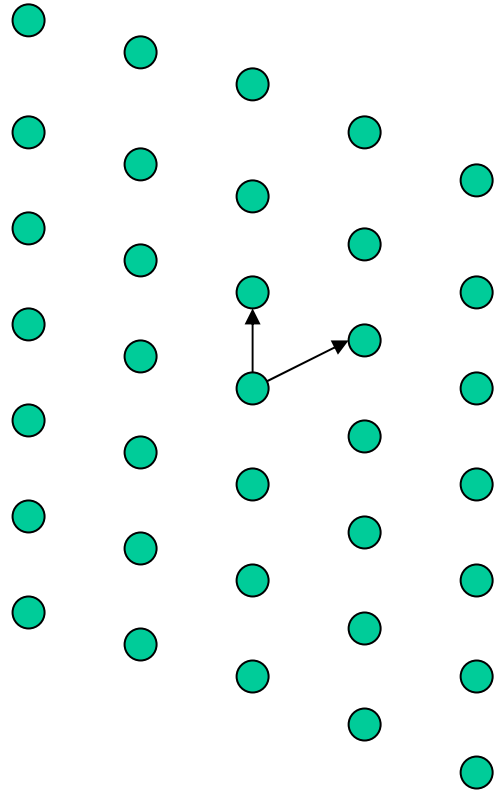
$$v_1\mathbb{Z} + \ldots + v_n\mathbb{Z}$$



Lattice

$$v_1, \ldots, v_n \in \mathbb{R}^n$$

$$v_1\mathbb{Z} + \ldots + v_n\mathbb{Z}$$



Dual lattice

$$L^* = \{u | (\forall v \in L) v^T u \in \mathbb{Z}\}$$

Banasczyk's technique (1992)

gaussian weight of a set

$$\rho(A) = \sum_{x \in A} e^{-\pi \|x\|^2}$$

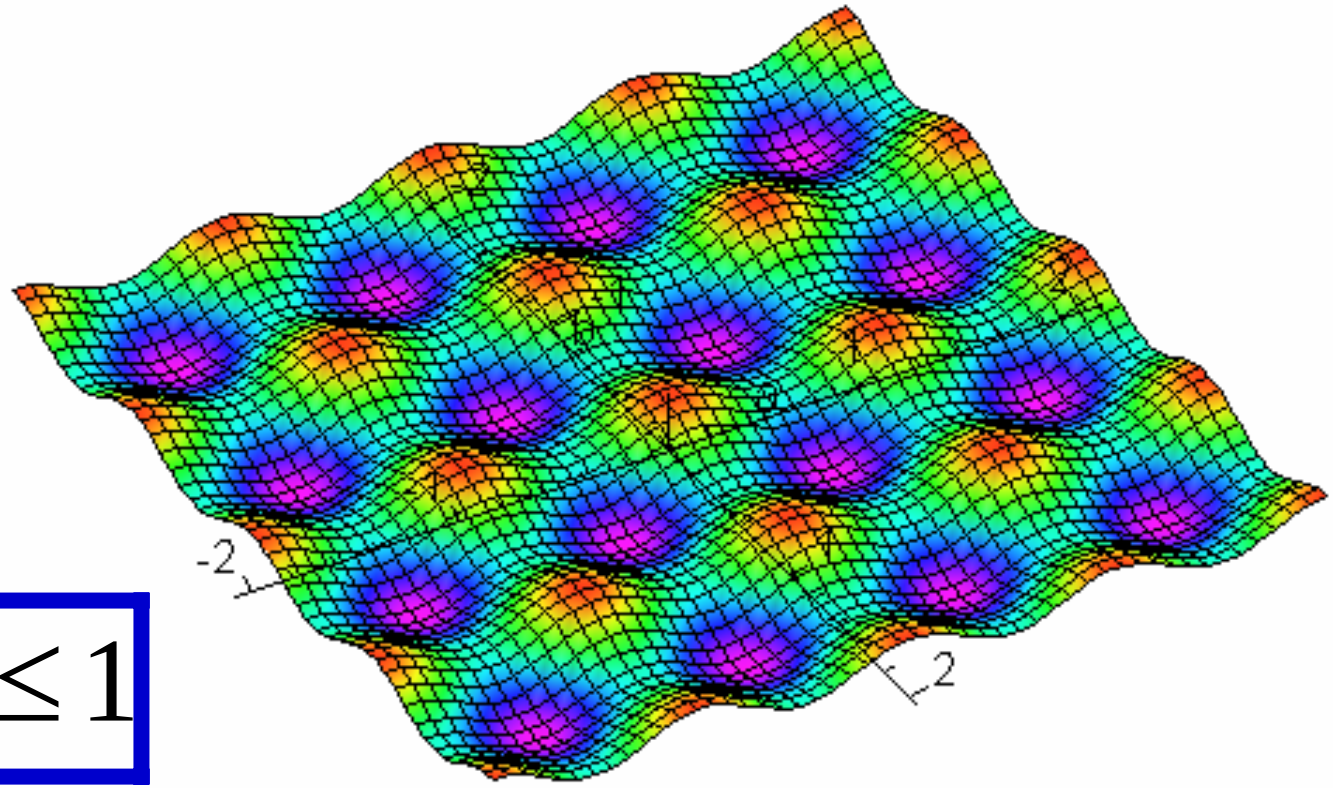
mass displacement function of lattice

$$\phi_L(x) = \rho(L + x) / \rho(L)$$

Banasczyk's technique (1992)

mass displacement function of lattice

$$\phi_L(x) = \rho(L+x)/\rho(L)$$



properties:

$$0 \le \phi_L(x) \le 1$$

$$\mathrm{dist}(x, L) \ge \sqrt{n} \quad \Rightarrow \quad \phi_L(x) \le 1/4$$

Banasczyk's technique (1992)

discrete measure

$$\sigma_L(A) = \rho(L \cap A) / \rho(L)$$

relationship between the discrete measure and the mass displacement function of the dual

$$\boxed{\widehat{\sigma}_L(x) = \phi_{L^*}(x)}$$

$$\widehat{\sigma}_L(x) = \frac{1}{\rho(L)} \sum_{y \in L} \exp(-\pi \| y \|^2) \exp(2\pi i y^T x)$$

Banasczyk's technique (1992)

discrete measure defined by the lattice

$$\sigma_L(A) = \rho(L \cap A) / \rho(L)$$

$$\widehat{\sigma}_L(x) = \phi_{L^*}(x)$$

$$\frac{1}{\rho(L)} \sum_{\|x\| \le s}^{*} \qquad \frac{1}{\rho(L)} \sum_{\|x\| > s}^{*}$$

$$\widehat{\sigma}_L(x) = \frac{1}{\rho(L)} \sum_{y \in L} \exp(-\pi \| y \|^2) \exp(2\pi i y^T x)$$

Banasczyk's technique (1992)

$$\alpha_1, \alpha_2, \alpha_3 \longrightarrow \begin{pmatrix} 1 & 0 & 0 & \alpha_1 \\ 0 & 1 & 0 & \alpha_2 \\ 0 & 0 & 1 & \alpha_3 \\ 0 & 0 & 0 & \nu \end{pmatrix} \sqrt{n}/\varepsilon$$

there is no short vector $w \in L$
with coefficient of the
last column $\not\equiv 0 (\mathrm{mod}\ p)$

Banasczyk's technique (1992)

there is no short vector $w \in L$ **with coefficient of the last column** $\not\equiv 0 (\mathrm{mod}\ p)$

$$\Downarrow$$

$$\widehat{\sigma}_L(u) \geq 1/2$$

$$\Downarrow$$

$$\phi_{L^*}(u) \geq 1/2$$

$$\Downarrow$$

$$\mathrm{dist}(u, L^*) \leq \sqrt{n}$$

$$\Downarrow$$

obstacle

$$u := \frac{\varepsilon}{pv\sqrt{n}} e_{n+1}$$

QED

Lovász (1982)
Simultaneous Diophantine Approximation

Given rationals $\alpha_1, \alpha_2, \ldots, \alpha_n, Q$

can find in polynomial time

↓

integers $p_1, \ldots, p_n$ $\qquad 0<q \leq Q$

$$\left|q\alpha_i - p_i\right| \leq \frac{2^{n^2}}{Q^{1/n}} \qquad \textbf{for all } i$$

Factoring polynomials with rational coefficients.

Simultaneous diophantine ε-approximation excluding p - algorithmic

Given rationals $\alpha_1, \alpha_2, \ldots, \alpha_n$,prime p

can find in polynomial time

$2C_{n+1}p\varepsilon$-approximation excluding p

where ε is smallest such that there exists ε-approximation excluding p

$$C_n = 4\sqrt{n}\,2^{n/2}$$

Exluding prime and bounding denominator

If there is no ε-approximation excluding p with $q \le Q$

then there exists an

approximate obstacle with

$$\sum |b_i| \le n^{3/2} / \varepsilon$$

$$b_1\alpha_1 + b_2\alpha_2 + \ldots + b_n\alpha_n = 1/p + t + \kappa$$

$$|\kappa| \le n/Q$$

Exluding prime and bounding denominator

the obstacle

necessary to prevent ε**-approximation excluding** p **with** $q \le Q$

sufficient to prevent $\varepsilon/(2n^{3/2}p)$ **-approximation excluding** p **with** $q \le Q/(2pn)$

Exluding several primes

If there is no ε-approximation excluding $p_1, \ldots, p_k$ then there exists

obstacle with

$$\sum |b_i| \le n^{1/2}(\max(n,k))/\varepsilon$$

$$\sum_{i=1}^{n} b_i \alpha_i = \sum_{j \in A \subseteq [k]} 1/p_j + t$$

Show that there is no small obstacle!

$m = 7^k$ $\qquad$ m^*

primitive 3-rd root of unity

know

$$1 + \omega + \omega^2 \equiv 0 \pmod{7^k}$$

obstacle

$$c_0 + c_1\omega = t7^{k-1}, \quad \gcd(t, 7) = 1$$

Show that there is no small obstacle!

$$1+\omega+\omega^2 \equiv 0 \pmod{7^k}$$

$$c_0 + c_1\omega = t7^{k-1}, \quad \gcd(t,7)=1$$

$$\mathrm{Res}(1+x+x^2, c_0+c_1x)$$

$$\begin{bmatrix} 1 & 1 & 1 \\ c0 & c1 & 0 \\ 0 & c0 & c1 \end{bmatrix}$$

$$\neq 0$$

divisible by 7^{k-1}

$$c1^2 - c0\,c1 + c0^2$$

$$\leq 2(c_0^2 + c_1^2)$$

$$\varepsilon = \frac{4}{7^{(k-1)/2}} \quad \rightarrow$$

There is g with all 3-rd roots

$$[-(4\sqrt{7})m^{1/2}, (4\sqrt{7})m^{1/2}]$$

Dual lattice

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\frac{\alpha_1}{\nu} & -\frac{\alpha_2}{\nu} & -\frac{\alpha_3}{\nu} & \frac{1}{\nu} \end{pmatrix} \varepsilon / \sqrt{n}$$

Algebraic integers?

possible that a small integer combination with small coefficients is doubly exponentially close to 1/p