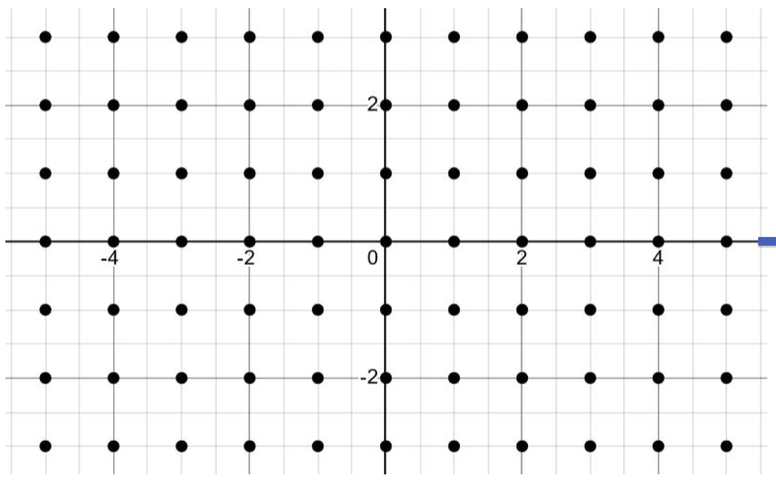
Benjamin Faltin

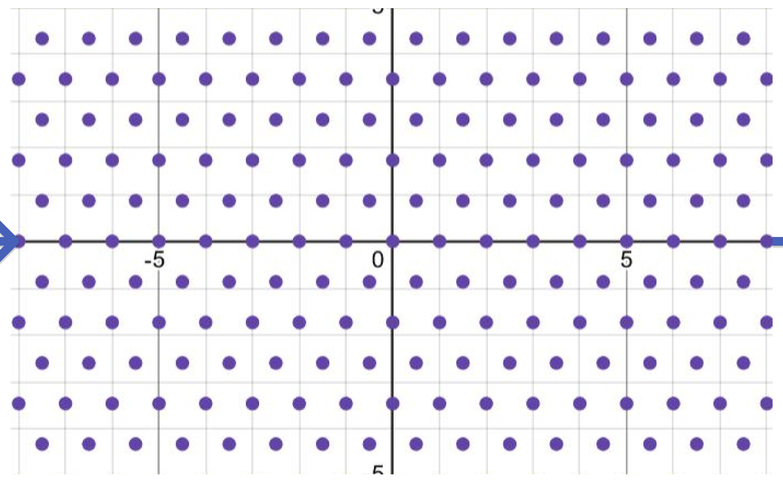
sources

Number of points in a bounded set for number field lattices

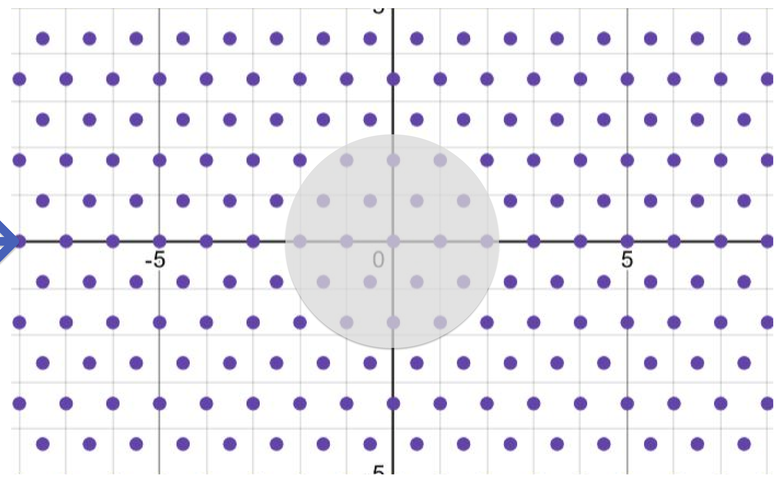
sources



This represents $\mathbb{Z}[i]$ in $\mathbb{C}$



This represents $\mathbb{Z}[\omega_3]$ in $\mathbb{C}$



How many points ?

Main result for a ball of Volume V in a lattice Λ

$$V^2 + V \cdot \omega_{K_i} \leq \mathbb{E}\left[\rho(\Lambda)^2\right] \leq V^2 + V \cdot \omega_{K_i} \cdot (1 + C \cdot e^{-\varepsilon \cdot d_i (t - t_0)}).$$

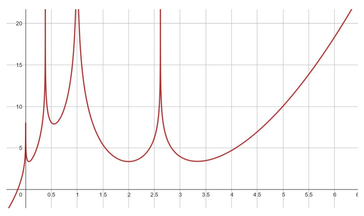
for $t_0 \geq 27$

Improve $t_0 \geq 27$

To do this, we look at heights of algebraic integers

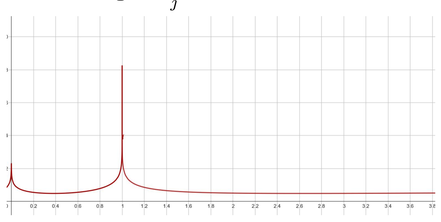
Cassels height

$$\mathscr{M}(\beta) := \frac{1}{\deg \beta} \sum_j |\beta_j|^2 \geq 3.3678$$



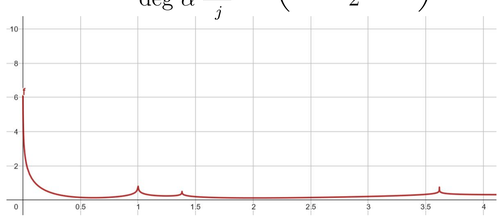
Weil height

$$h(\alpha) = \frac{1}{\deg \alpha} \sum_j \log_+(|\alpha_j|) \geq \frac{1}{2} \log \varphi$$



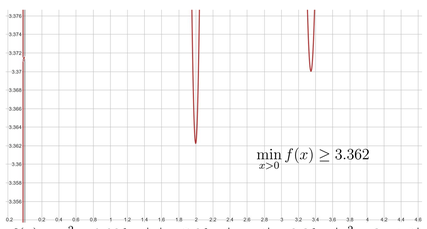
Practical height

$$m(\alpha) = \frac{1}{\deg \alpha} \sum_j \log\left(\frac{|\alpha_j| + |\alpha_j|^{-1}}{2}\right)$$

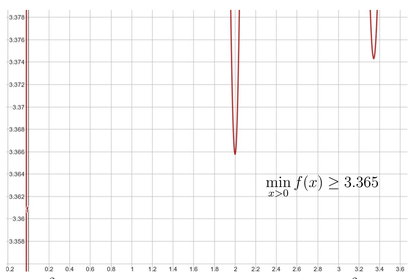


auxiliary functions

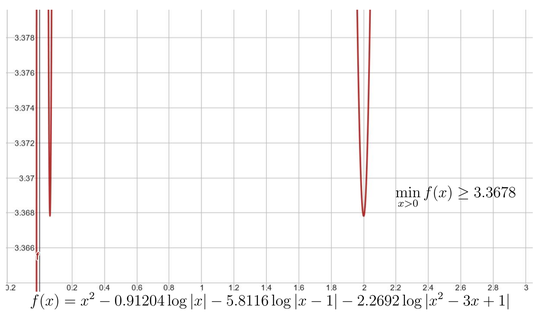
Cassels height



$f(x) = x^2 - 0.92 \log|x| - 5.8 \log|x-1| - 2.3 \log|x^2 - 3x + 1|$



$f(x) = x^2 - 0.915 \log|x| - 5.82 \log|x-1| - 2.28 \log|x^2 - 3x + 1|$



$f(x) = x^2 - 0.91204 \log|x| - 5.8116 \log|x-1| - 2.2692 \log|x^2 - 3x + 1|$

?

What can we conclude?

Hypothesis

Somehow 3.3678 is very close to $3 + \frac{1}{e} \approx 3.3678794$

Can we find a sequence of totally positive algebraic number $(\alpha_i)_{i=0}^{\infty}$ such that $\lim_{n\to\infty} \alpha_n = 3 + \frac{1}{e}$?

One can write $\frac{1}{e} = \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \dots$

And approach it from the top with

$$\frac{1}{e} = \frac{1}{2!} + \left(-\frac{1}{3!} + \frac{1}{4!}\right) + \left(-\frac{1}{5!} + \frac{1}{6!}\right) + \dots$$

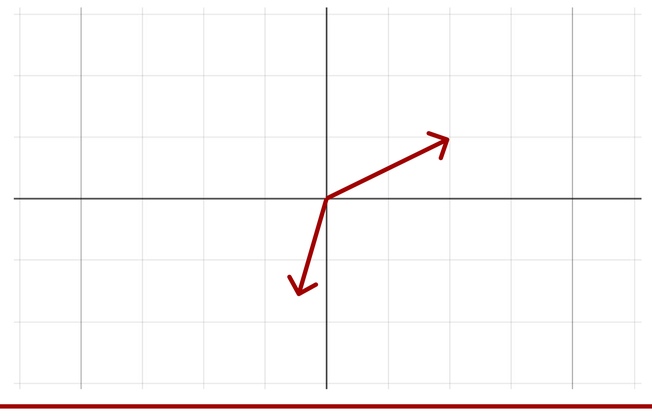
$$\mathscr{M}(\varphi^2) = 3.5 = 3 + \frac{1}{2!}$$

Unfortunately, we could not find any totally positive integer with Cassels height equal to $3 + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!}$

still the unknown

Applications

Shortest Vector Problem



Explanation

One of the central concerns in lattice-based cryptography is to prove or disprove the existence of fast algorithms that can find, even if approximately, the length of the shortest vectors of a lattice. The non-existence of such algorithms is still a wide-open question.

EPFL

September 19, 2024

LAIDLAW SCHOLARS