Optimal ancilla-free Clifford+T approximation of z-rotations

Neil J. Ross and Peter Selinger

Dalhousie University
Halifax, Canada

Happy birthday Prakash!

How I learned quantum mechanics from Prakash in 2000

How I learned quantum mechanics from Prakash in 2000

Peter: Please teach me about quantum mechanics.

How I learned quantum mechanics from Prakash in 2000

Peter: Please teach me about quantum mechanics.

Prakash: Do you know about vector spaces and linear maps?

How I learned quantum mechanics from Prakash in 2000

Peter: Please teach me about quantum mechanics.

Prakash: Do you know about vector spaces and linear maps?

Peter: Yes.

How I learned quantum mechanics from Prakash in 2000

Peter: Please teach me about quantum mechanics.

Prakash: Do you know about vector spaces and linear maps?

Peter: Yes.

Prakash: Great, then you already know quantum mechanics!

How I learned quantum mechanics from Prakash in 2000

Peter: Please teach me about quantum mechanics.

Prakash: Do you know about vector spaces and linear maps?

Peter: Yes.

Prakash: Great, then you already know quantum mechanics!

The end.


Bellairs Quantum Workshop April 1937.

Optimal ancilla-free Clifford+T approximation of z-rotations

Neil J. Ross and Peter Selinger

Dalhousie University
Halifax, Canada

Thesis: Good algorithms come from good mathematics

- **Solovay-Kitaev algorithm** (ca. 1995):
  Geometry.

$$ABA^{-1}B^{-1}.$$

- **New efficient synthesis algorithms** (ca. 2012):
  Algebraic number theory.

$$a + b\sqrt{2}.$$

Gate complexity, in numbers.

Precision	Solovay-Kitaev	Lower bound
	$O(\log^{3.97}(1/\epsilon))$	$3\log_2(1/\epsilon) + K$
$\epsilon = 10^{-10}$	$\approx 4,000$	≈ 102
$\epsilon = 10^{-20}$	$\approx 60,000$	≈ 198
$\epsilon = 10^{-100}$	$\approx 37,000,000$	≈ 998
$\epsilon = 10^{-1000}$	$\approx 350,000,000,000$	≈ 9966

Part I: Grid problems

The ring $\mathbb{Z}[\sqrt{2}]$

Consider $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

This is a ring (addition, subtraction, multiplication).

It has a form of *conjugation*: $(a + b\sqrt{2})^\bullet = a - b\sqrt{2}$.

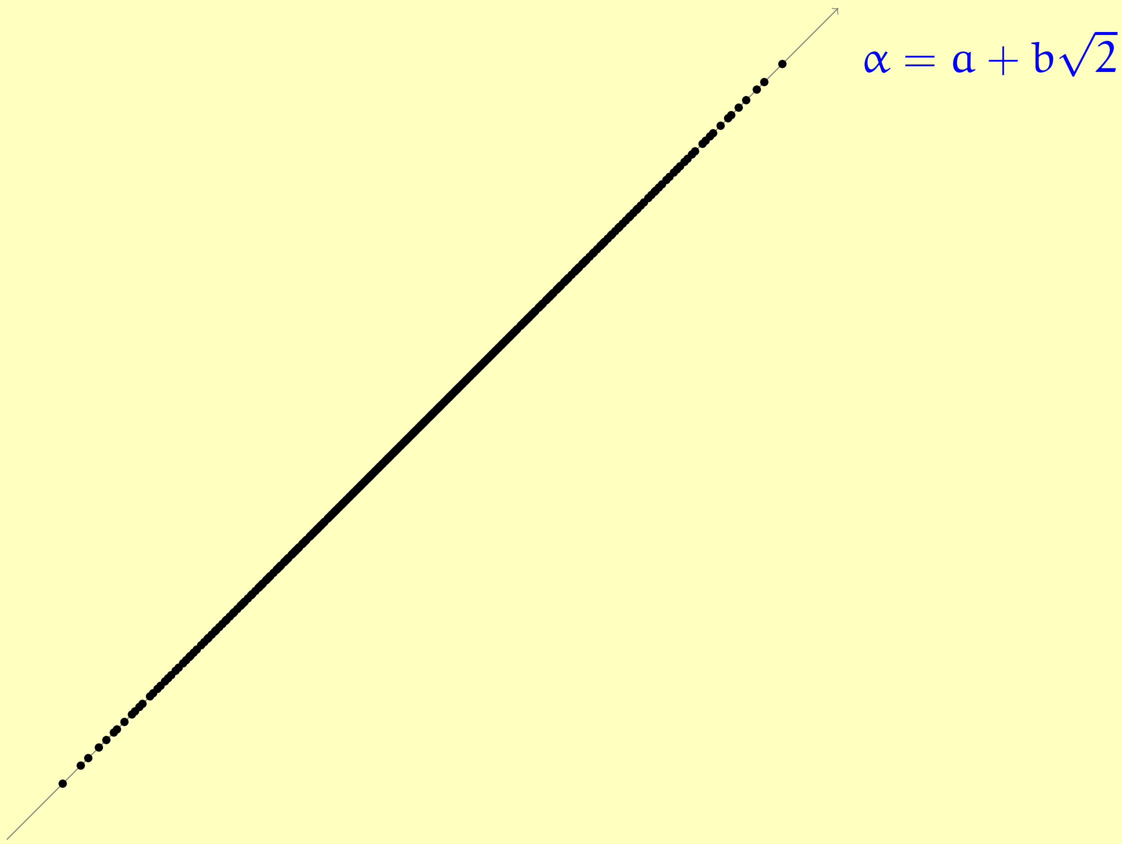
The map "$\bullet$" is an automorphism:

$$\begin{aligned}(\alpha + \beta)^\bullet &= \alpha^\bullet + \beta^\bullet \\ (\alpha - \beta)^\bullet &= \alpha^\bullet - \beta^\bullet \\ (\alpha\beta)^\bullet &= \alpha^\bullet\beta^\bullet\end{aligned}$$

Finally, $\alpha^\bullet\alpha = a^2 - 2b^2$ is an integer, called the *norm* of α.

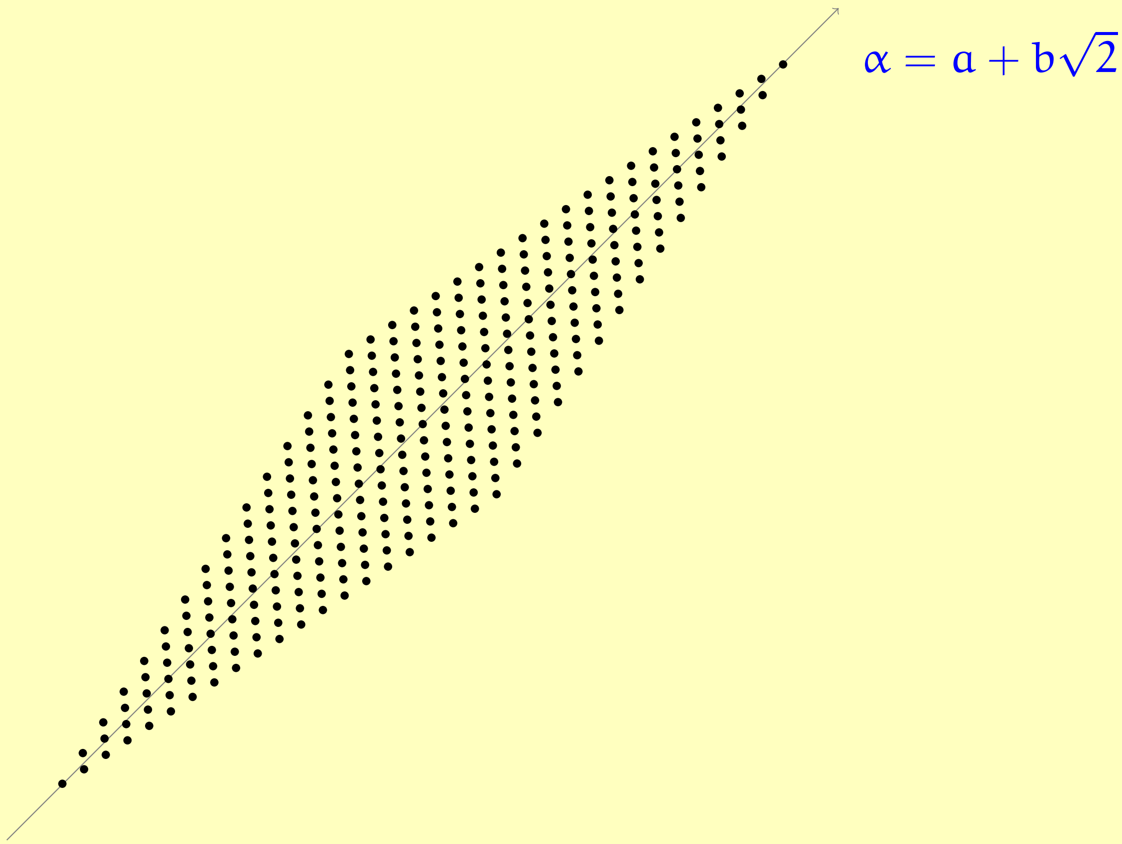
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



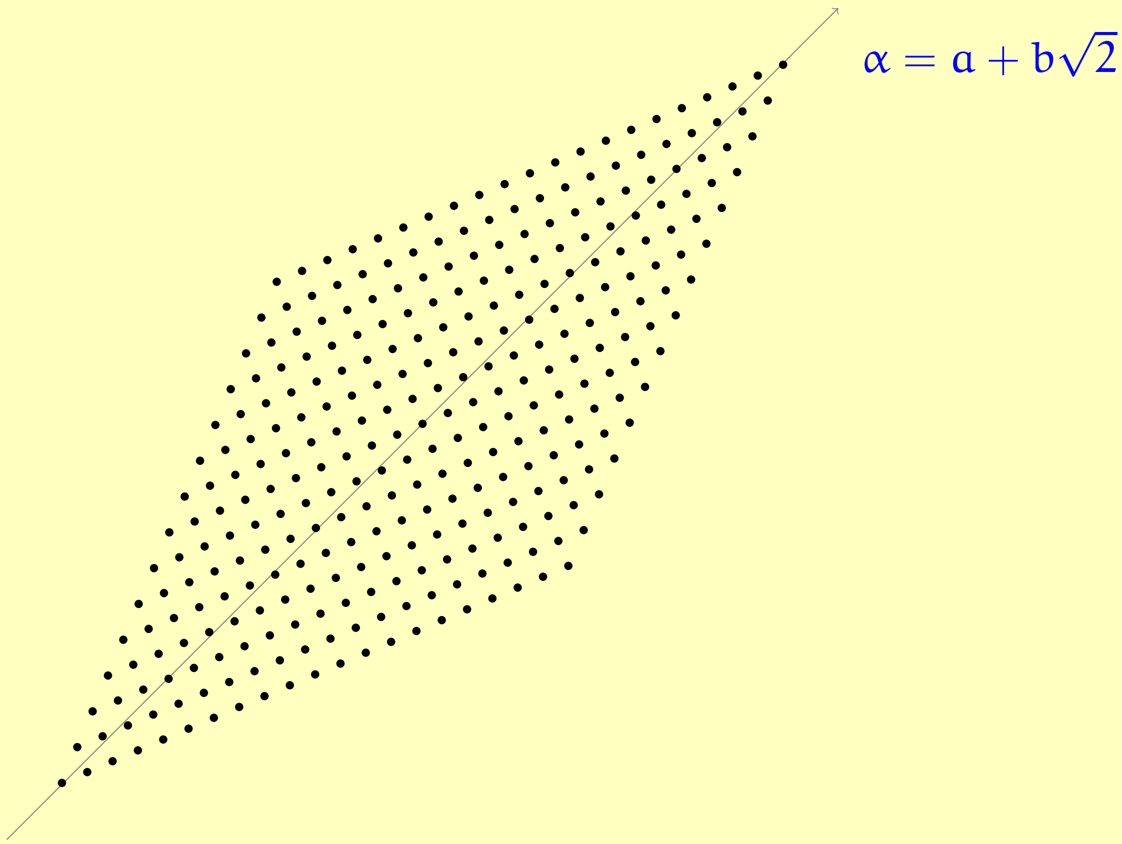
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



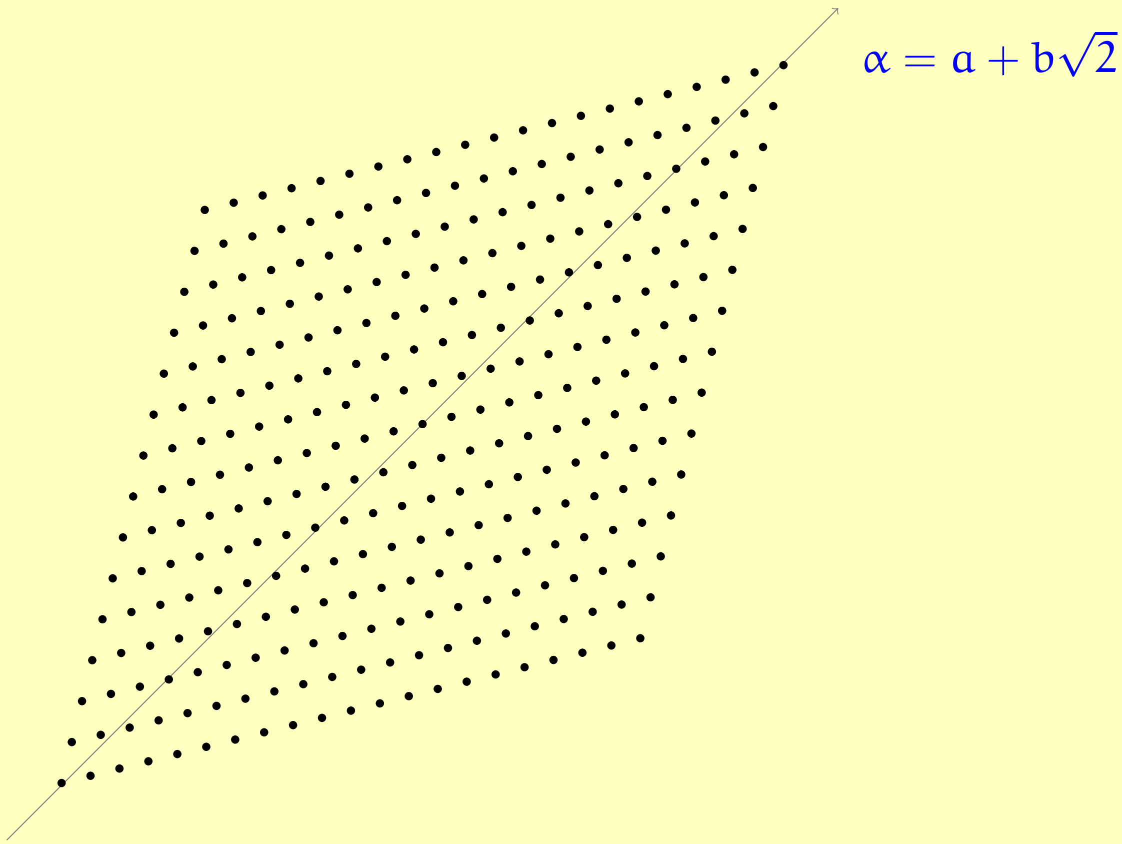
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



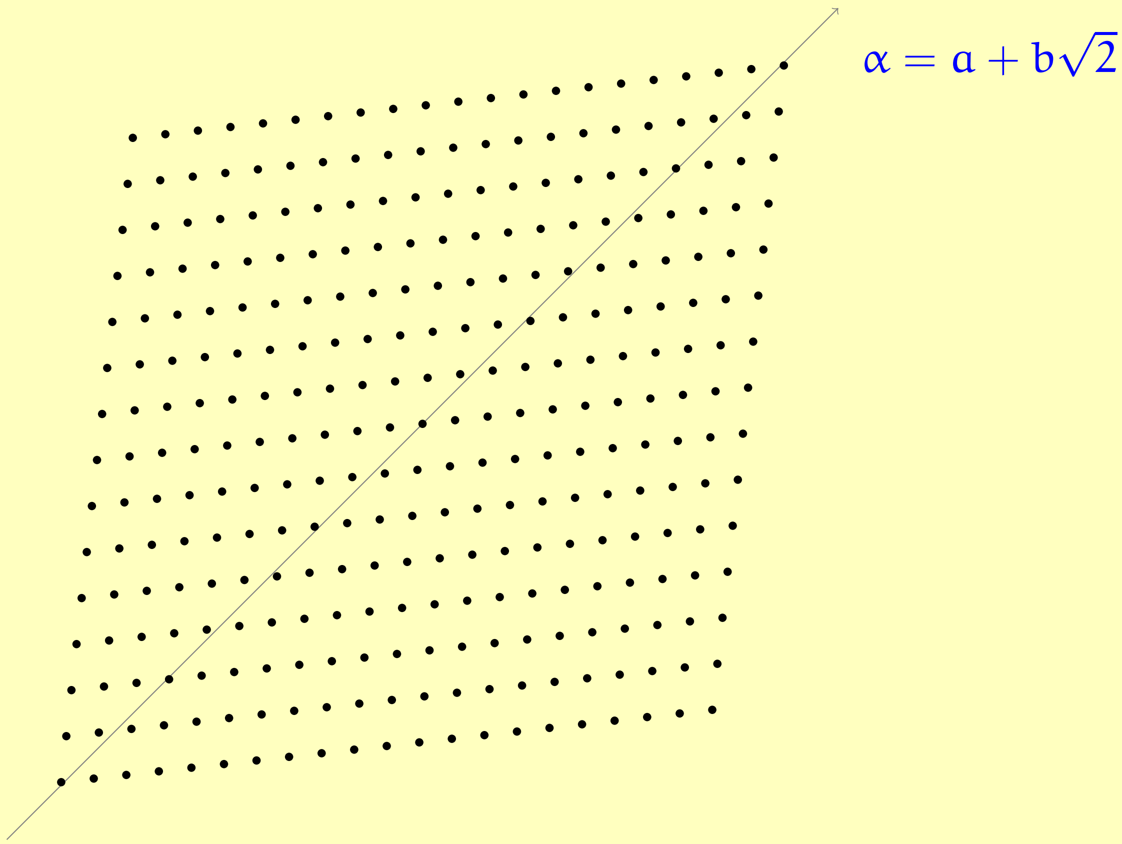
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



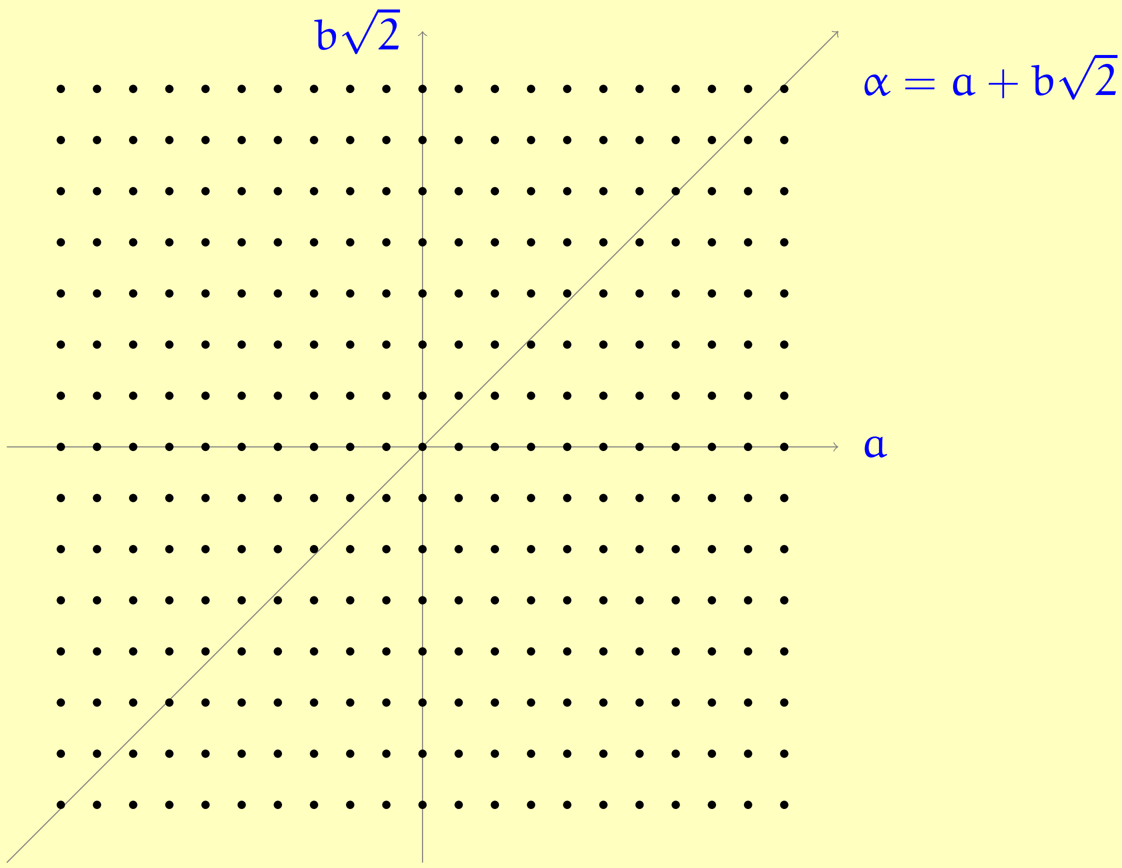
Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



Dense or discrete?

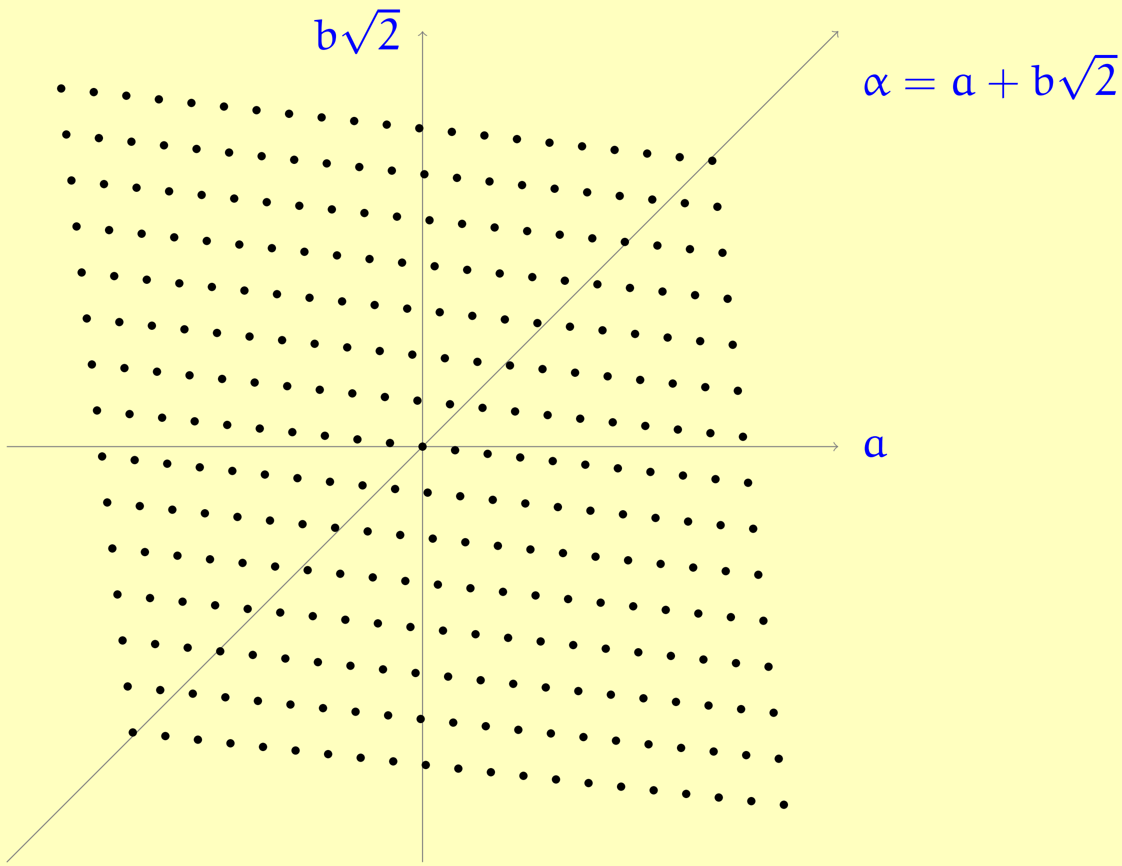
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

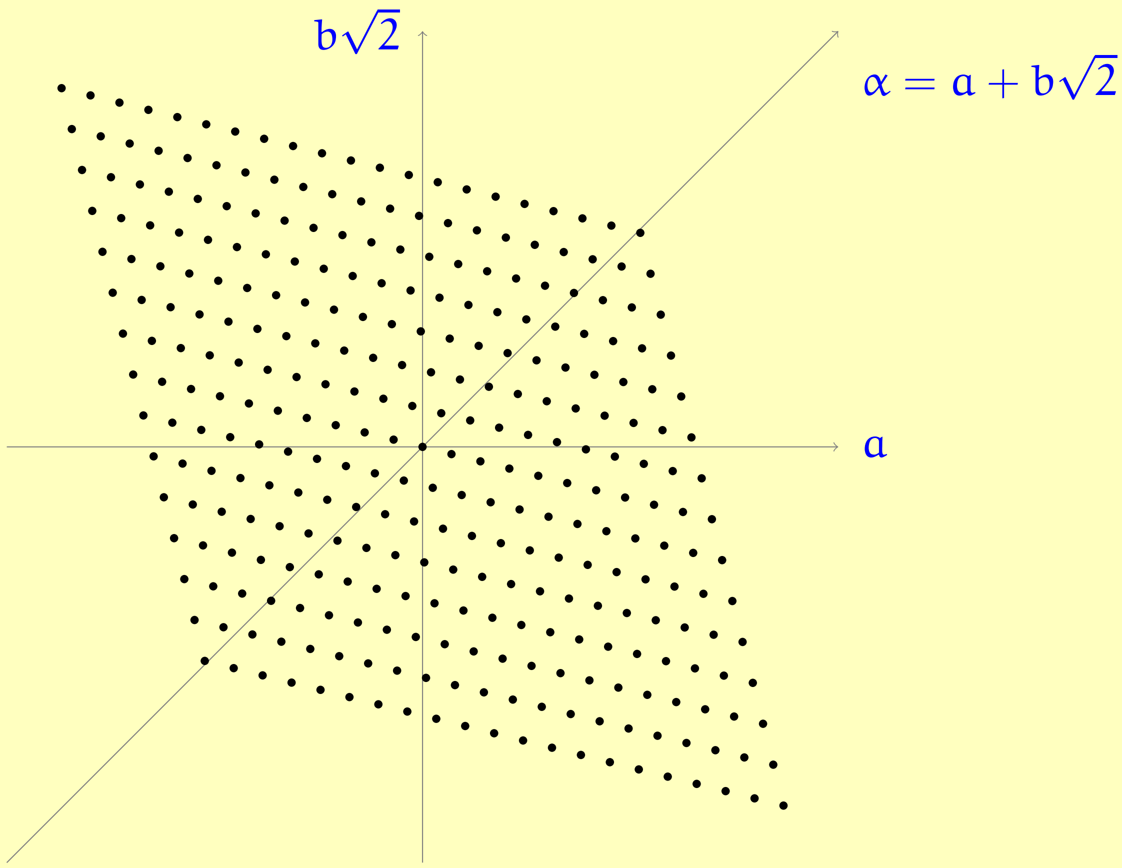
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

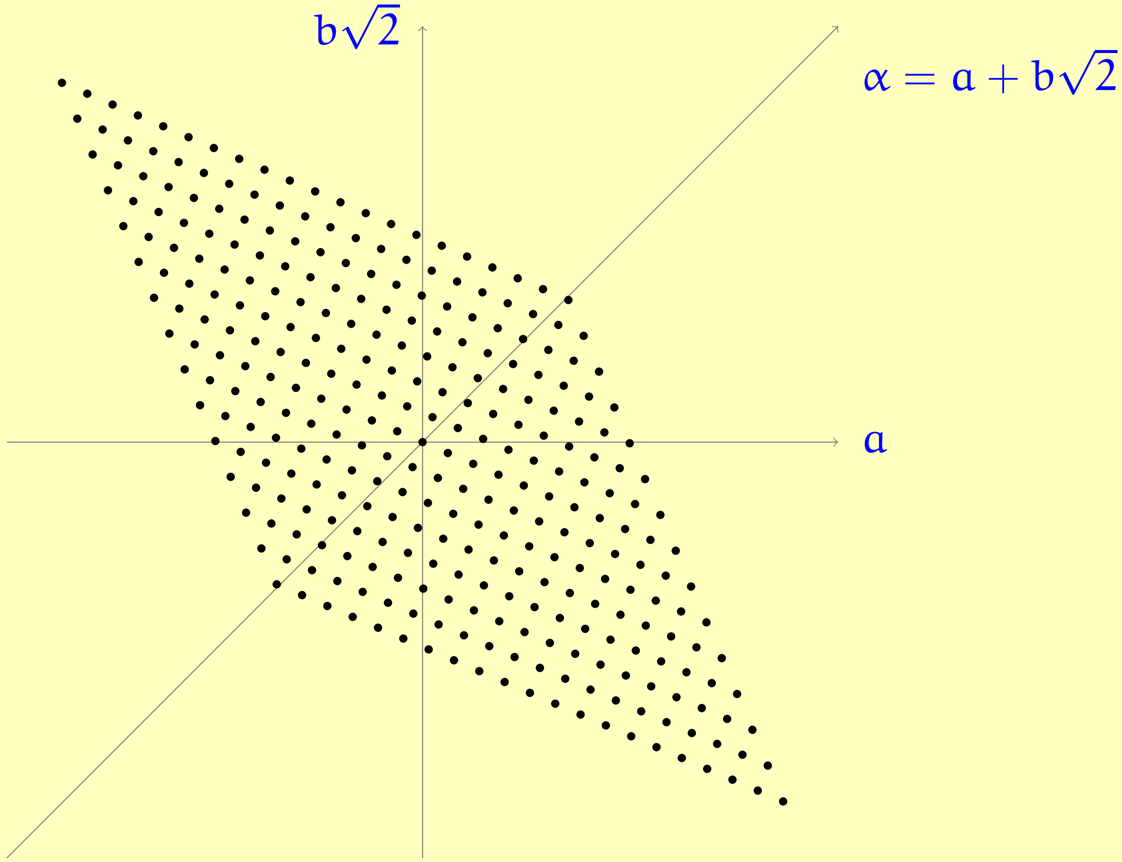
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

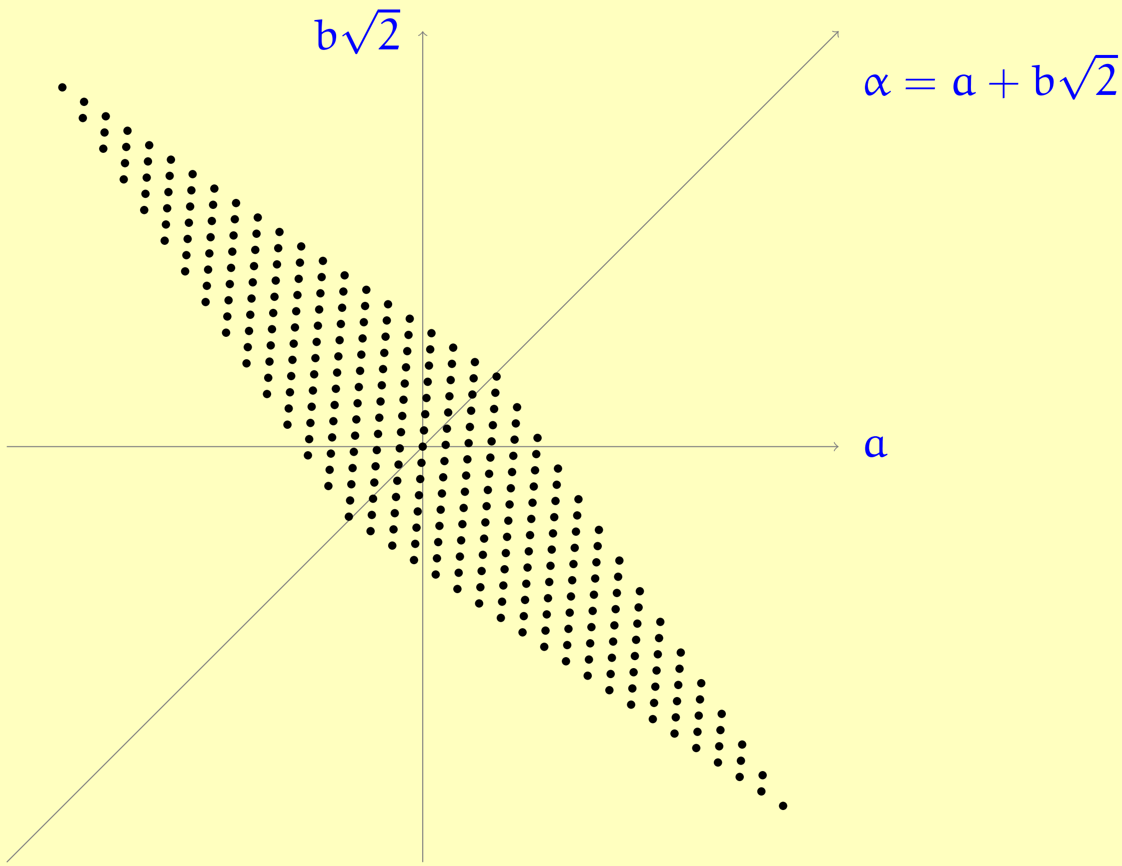
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

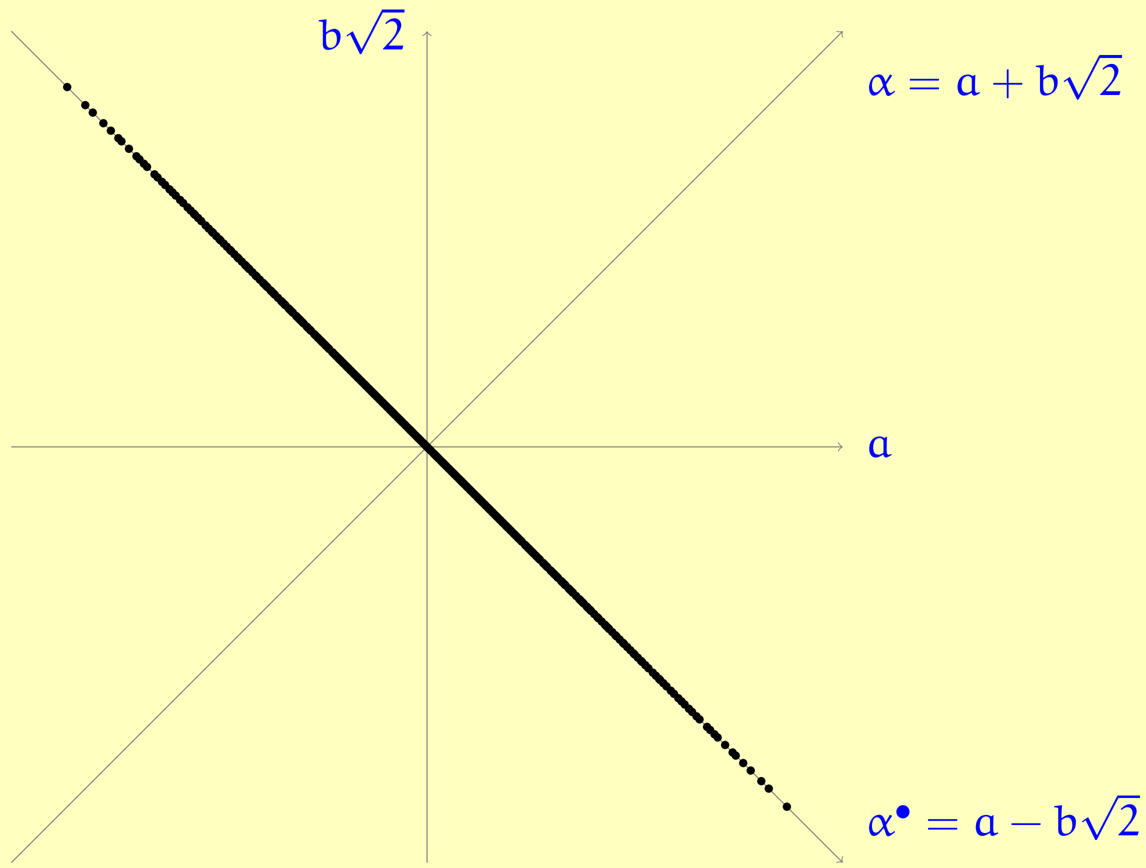
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

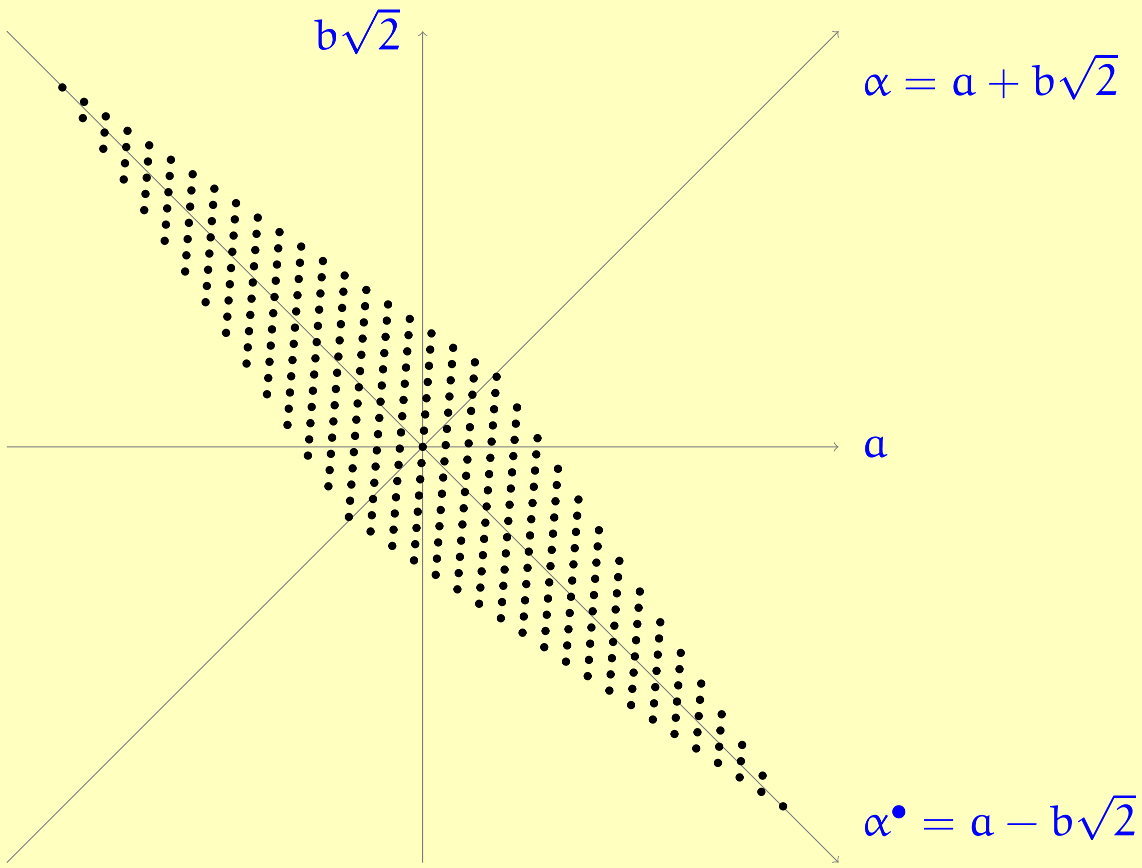
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

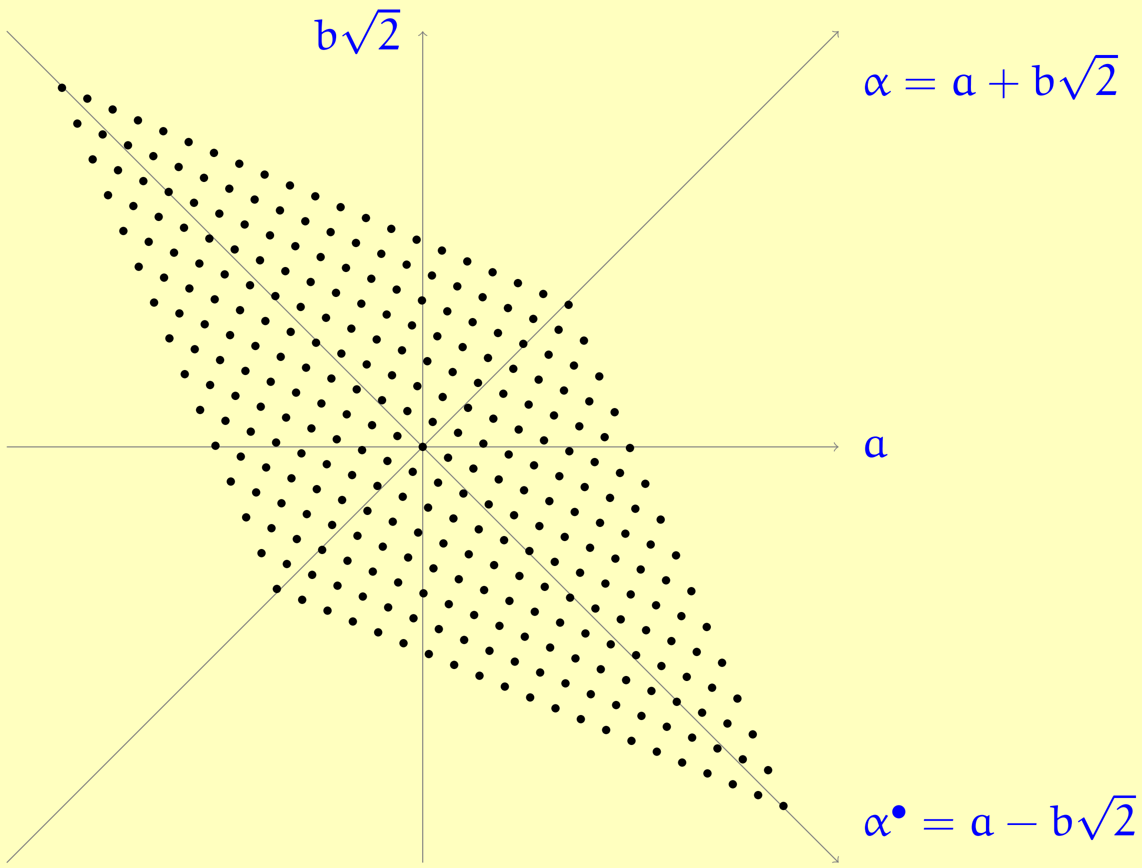
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

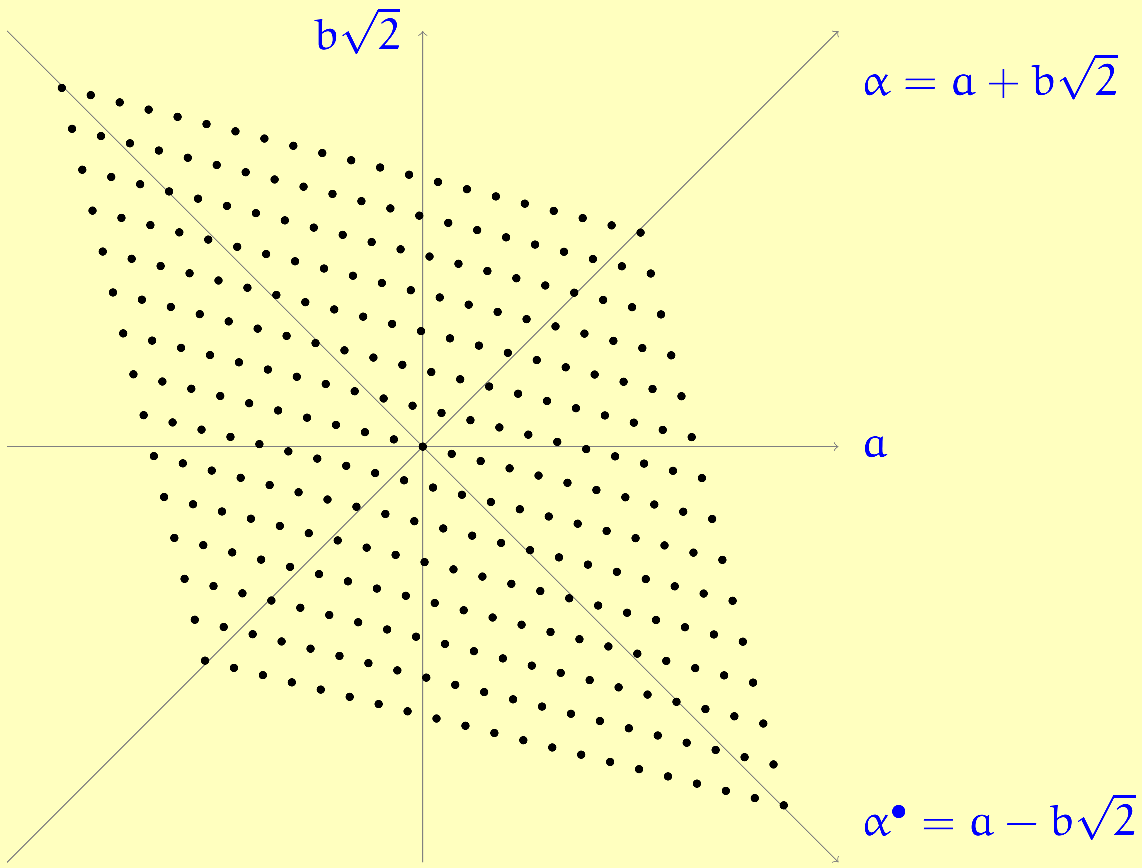
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

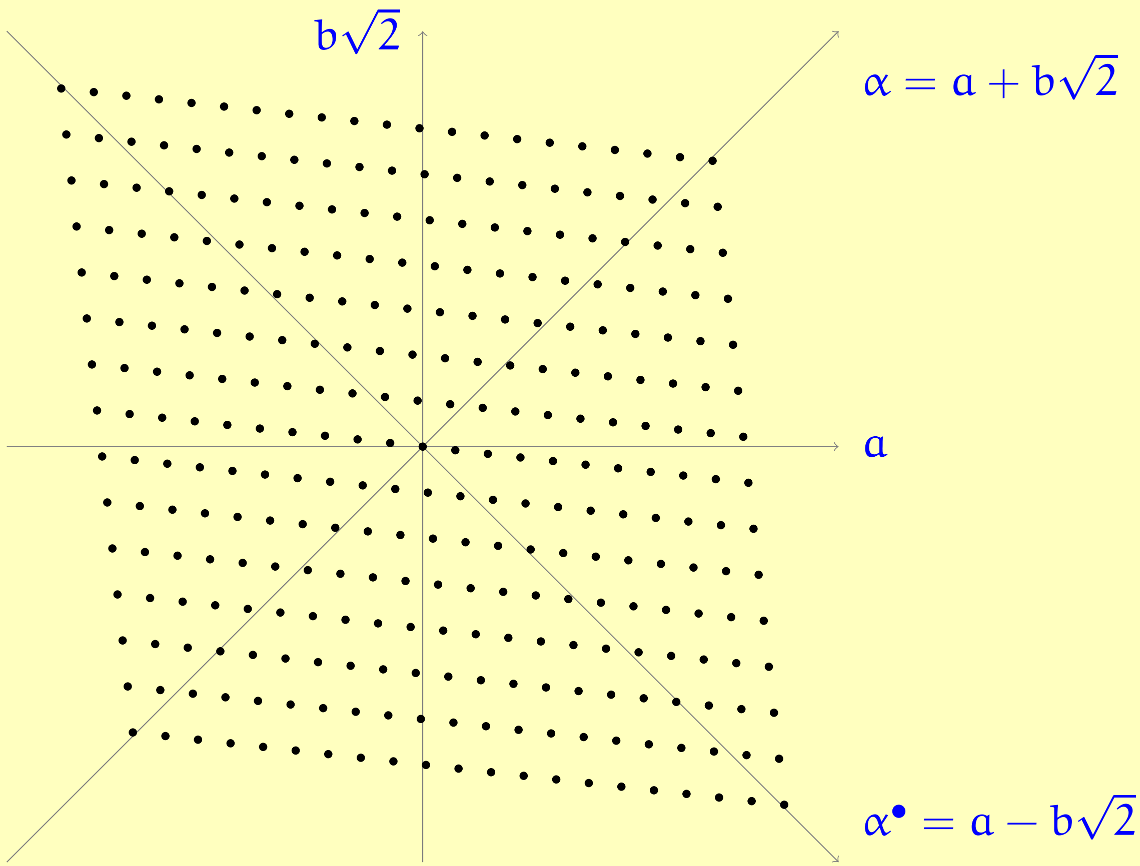
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

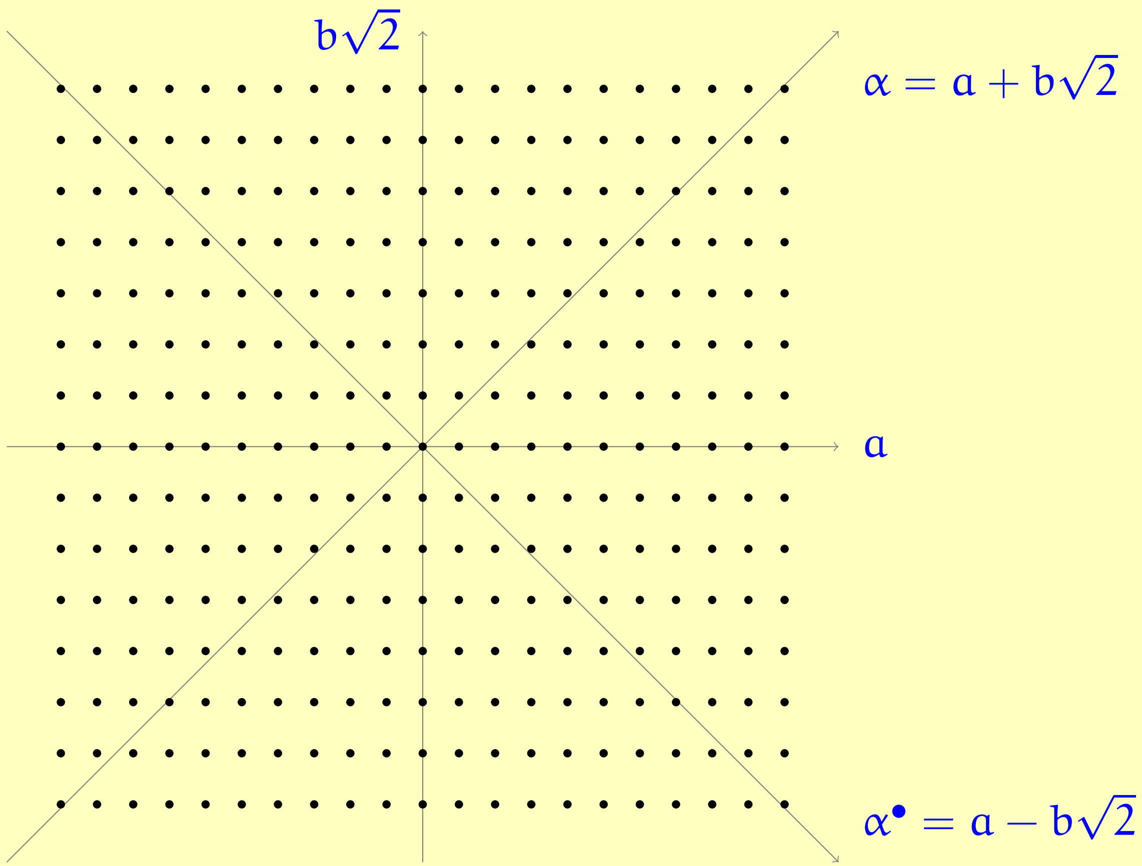
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

Dense or discrete?

The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.

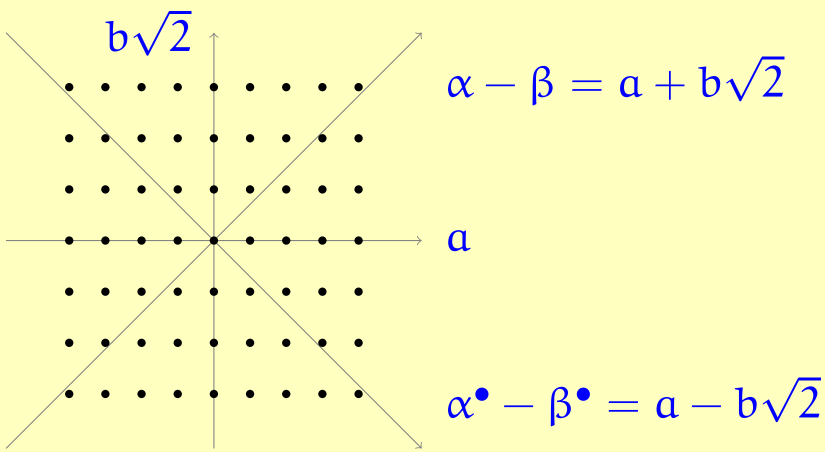


But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

The automorphism "$\bullet$"

The function $\alpha \mapsto \alpha^\bullet$ is *extremely non-continuous*. In fact, it can never happen that $|\alpha - \beta|$ and $|\alpha^\bullet - \beta^\bullet|$ are small at the same time (unless $\alpha = \beta$).

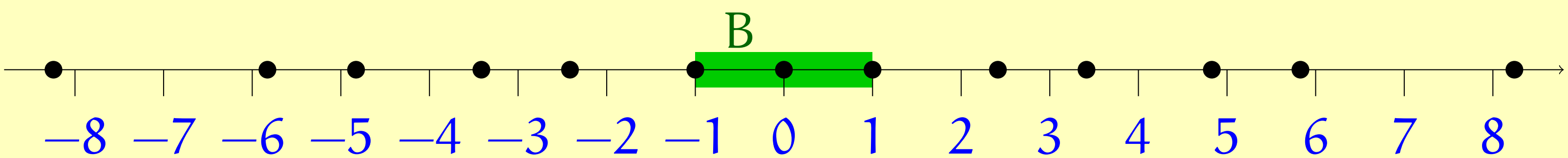
Proof: let $\alpha - \beta = a + b\sqrt{2}$. Then $|\alpha - \beta| \cdot |\alpha^\bullet - \beta^\bullet| = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$, which is an integer.



1-dimensional grid problems

Definition. Let B be a set of real numbers. The *grid* for B is the set

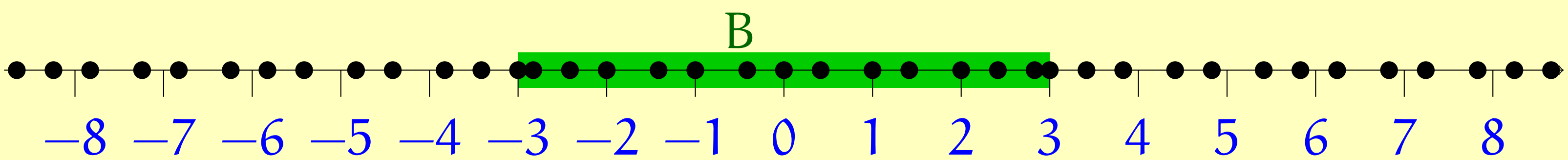
$$\mathrm{grid}(B) = \{\alpha \in \mathbb{Z}[\sqrt{2}] \mid \alpha^\bullet \in B\}.$$



1-dimensional grid problems

Definition. Let B be a set of real numbers. The *grid* for B is the set

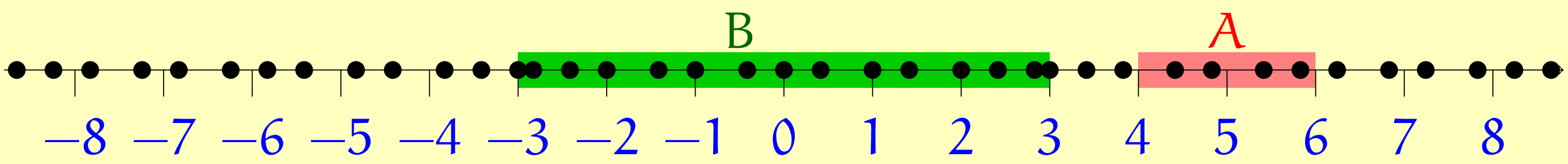
$$\mathrm{grid}(B) = \{\alpha \in \mathbb{Z}[\sqrt{2}] \mid \alpha^\bullet \in B\}.$$



1-dimensional grid problems

Definition. Let B be a set of real numbers. The *grid* for B is the set

$$\mathrm{grid}(B) = \{\alpha \in \mathbb{Z}[\sqrt{2}] \mid \alpha^\bullet \in B\}.$$



Given finite intervals A and B of the real numbers, the *1-dimensional grid problem* is to find $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that

$$\alpha \in A \quad \text{and} \quad \alpha^\bullet \in B.$$

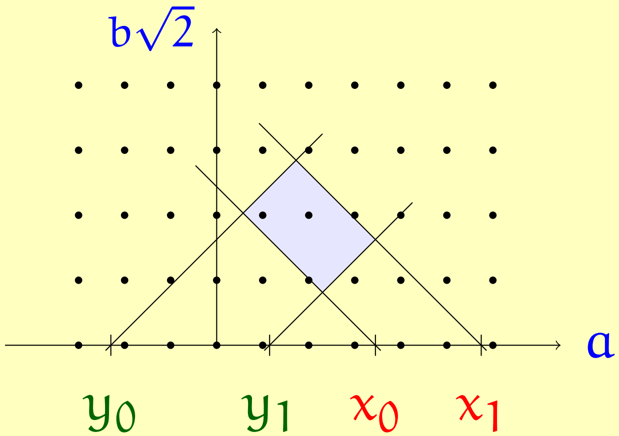
1-dimensional grid problems

Given finite intervals A and B of the real numbers, the *1-dimensional grid problem* is to find $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that

$$\alpha \in A \quad \text{and} \quad \alpha^\bullet \in B.$$

Equivalently, find $a, b \in \mathbb{Z}$ such that:

$$a + b\sqrt{2} \in A \quad \text{and} \quad a - b\sqrt{2} \in B.$$

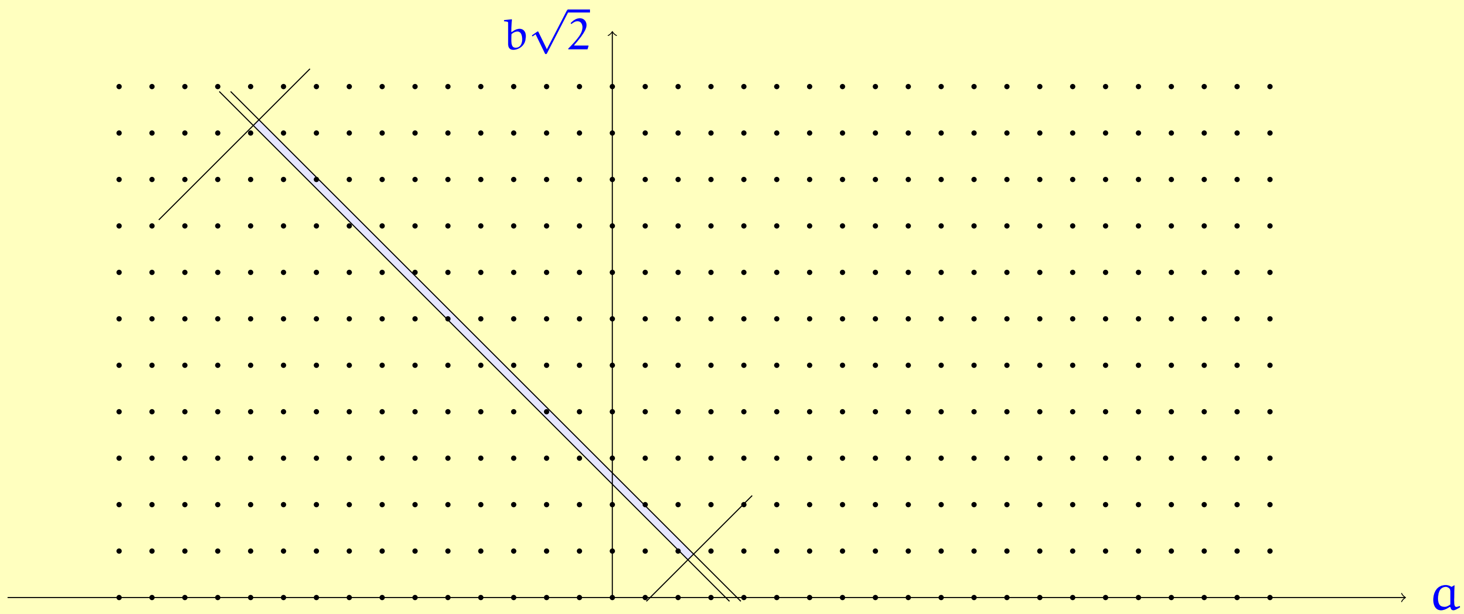


$$A = [x0, x1], \quad B = [y0, y1]$$

It is clear that there will be solutions when $|A|$ and $|B|$ are large. The number of solutions is $O(|A| \cdot |B|)$ in that case.

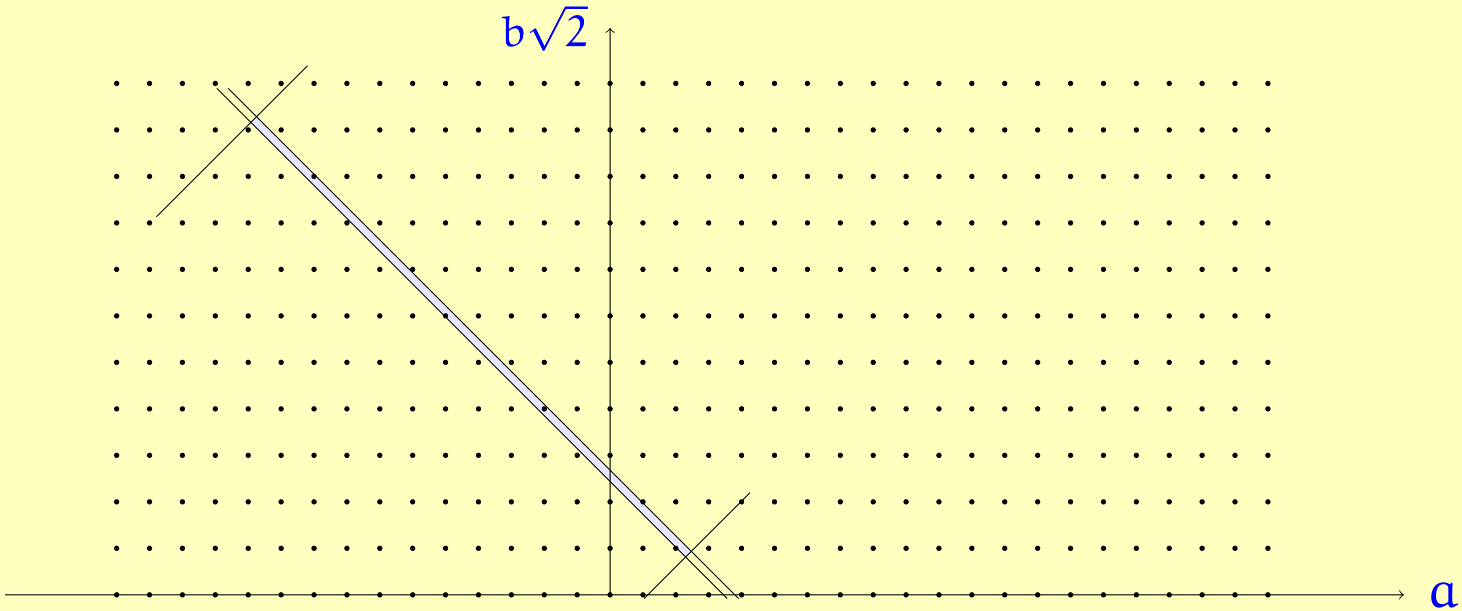
The problematic case: long and skinny

Suppose $|A|$ is tiny and $|B|$ is large, so that we end up with a long and skinny rectangle:



The problematic case: long and skinny

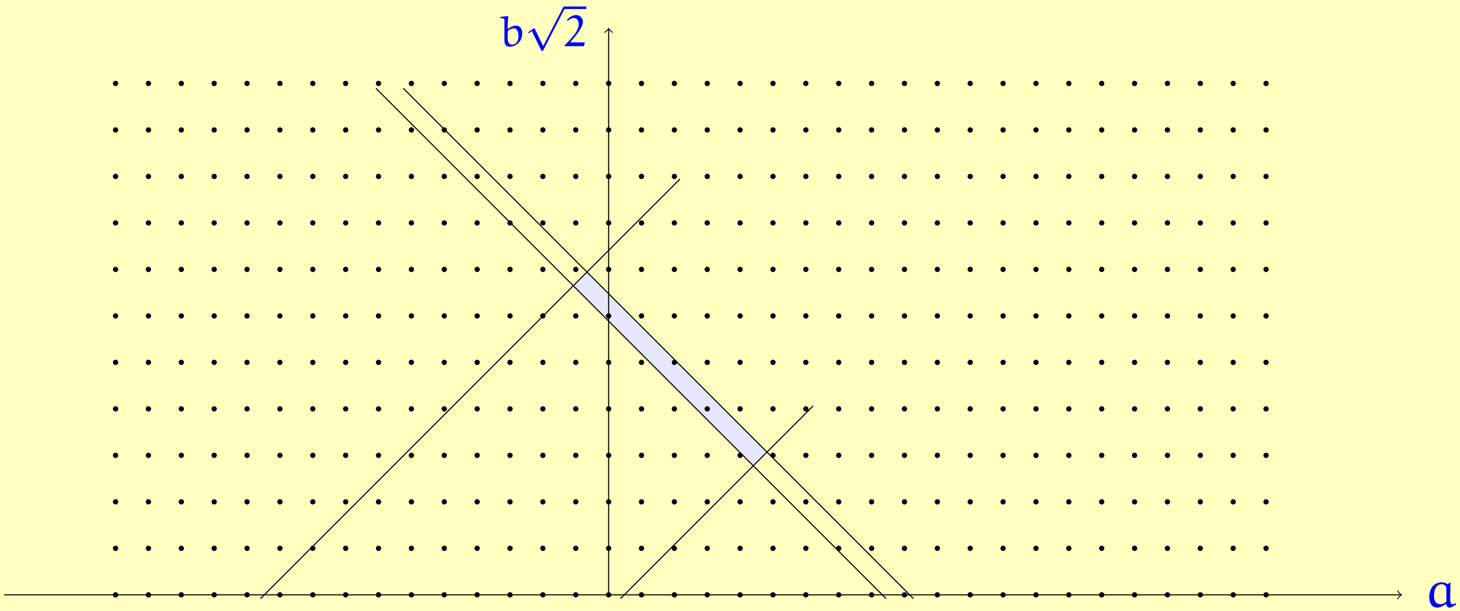
Suppose $|A|$ is tiny and $|B|$ is large, so that we end up with a long and skinny rectangle:



Solution: *scaling*. $\lambda = 1 + \sqrt{2}$ is a unit of the ring $\mathbb{Z}[\sqrt{2}]$, with $\lambda^{-1} = \sqrt{2} - 1$. So multiplication by λ maps the grid to itself. So we can equivalently consider the problem for $\lambda^n A$ and $\lambda^{\bullet n} B$, which takes us back to the "fat" case.

The problematic case: long and skinny

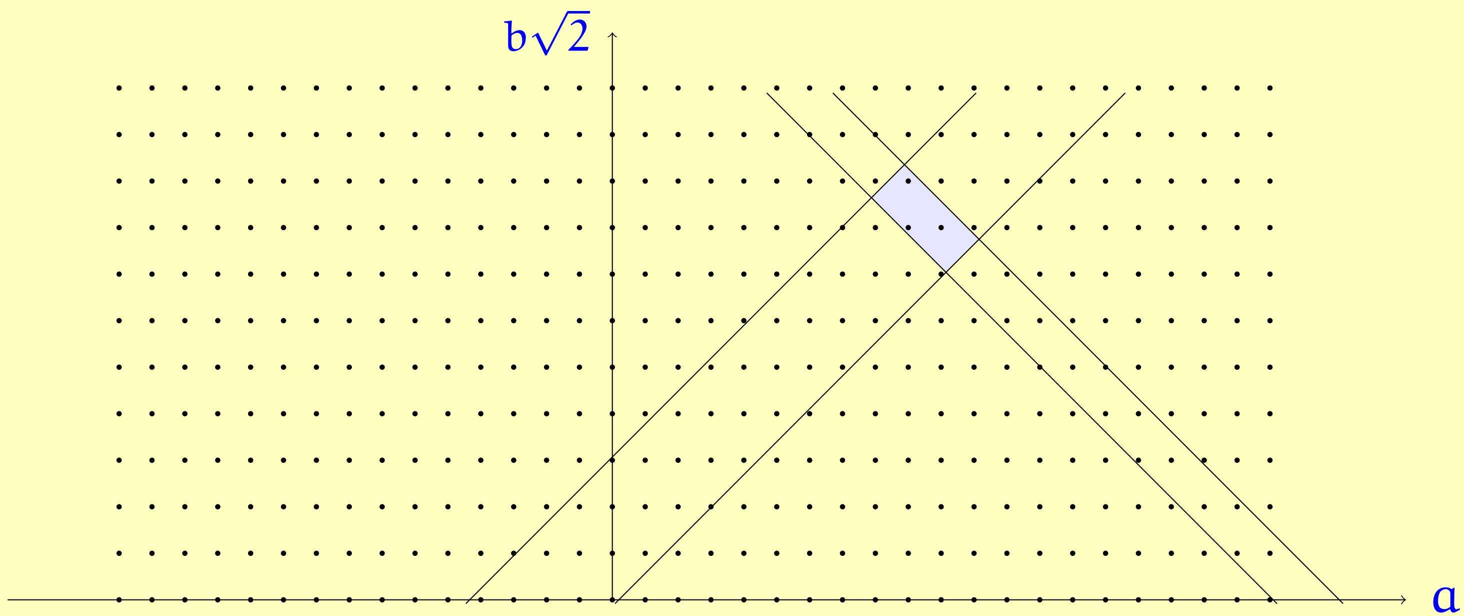
Suppose $|A|$ is tiny and $|B|$ is large, so that we end up with a long and skinny rectangle:



Solution: *scaling*. $\lambda = 1 + \sqrt{2}$ is a unit of the ring $\mathbb{Z}[\sqrt{2}]$, with $\lambda^{-1} = \sqrt{2} - 1$. So multiplication by λ maps the grid to itself. So we can equivalently consider the problem for $\lambda^n A$ and $\lambda^{\bullet n} B$, which takes us back to the "fat" case.

The problematic case: long and skinny

Suppose $|A|$ is tiny and $|B|$ is large, so that we end up with a long and skinny rectangle:



Solution: *scaling*. $\lambda = 1 + \sqrt{2}$ is a unit of the ring $\mathbb{Z}[\sqrt{2}]$, with $\lambda^{-1} = \sqrt{2} - 1$. So multiplication by λ maps the grid to itself. So we can equivalently consider the problem for $\lambda^n A$ and $\lambda^{\bullet n} B$, which takes us back to the "fat" case.

Solution of 1-dimensional grid problems

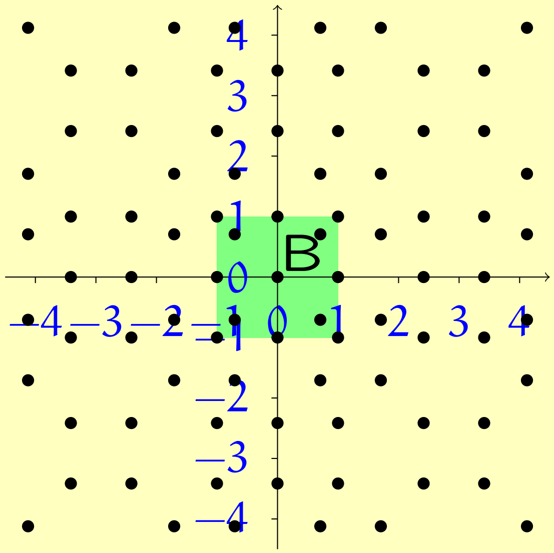
Theorem. Let A and B be finite real intervals. There exists an efficient algorithm that enumerates all solutions of the grid problem for A and B.

2-dimensional grid problems

Consider the ring $\mathbb{Z}[\omega]$, where $\omega = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}$. $\mathbb{Z}[\omega]$ is a subset of the complex numbers, which we can identify with the Euclidean plane $\mathbb{R}^2$.

Definition. Let B be a bounded convex subset of the plane. Just as in the 1-dimensional case, the *grid* for B is the set

$$\text{grid}(B) = \{\alpha \in \mathbb{Z}[\omega] \mid \alpha^\bullet \in B\}.$$

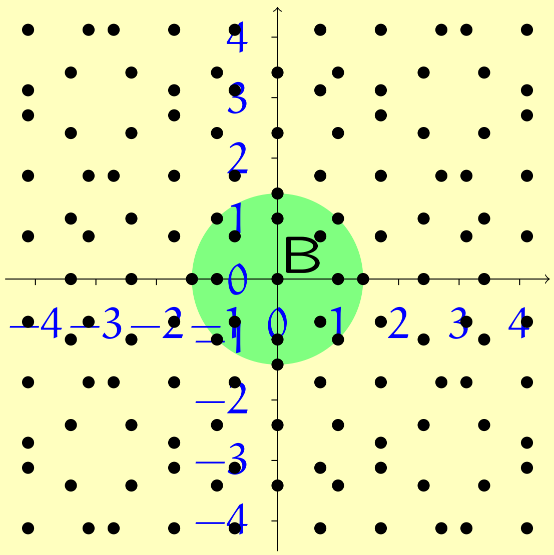


2-dimensional grid problems

Consider the ring $\mathbb{Z}[\omega]$, where $\omega = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}$. $\mathbb{Z}[\omega]$ is a subset of the complex numbers, which we can identify with the Euclidean plane $\mathbb{R}^2$.

Definition. Let B be a bounded convex subset of the plane. Just as in the 1-dimensional case, the *grid* for B is the set

$$\text{grid}(B) = \{\alpha \in \mathbb{Z}[\omega] \mid \alpha^\bullet \in B\}.$$

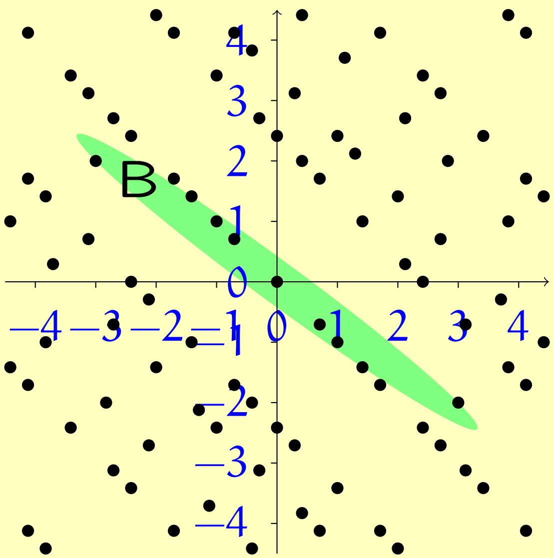


2-dimensional grid problems

Consider the ring $\mathbb{Z}[\omega]$, where $\omega = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}$. $\mathbb{Z}[\omega]$ is a subset of the complex numbers, which we can identify with the Euclidean plane $\mathbb{R}^2$.

Definition. Let B be a bounded convex subset of the plane. Just as in the 1-dimensional case, the *grid* for B is the set

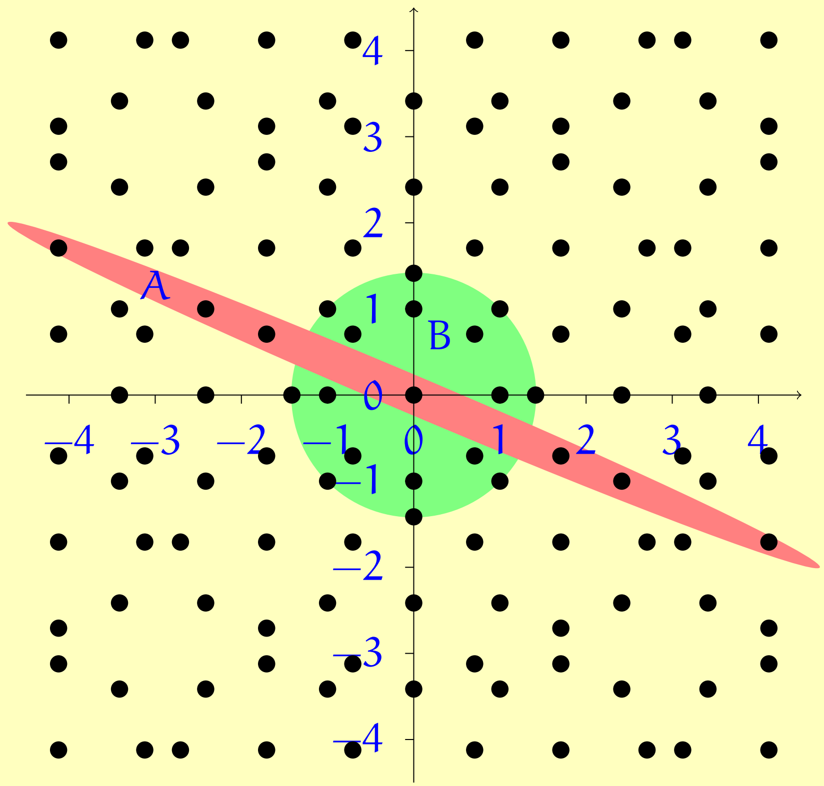
$$\text{grid}(B) = \{\alpha \in \mathbb{Z}[\omega] \mid \alpha^{\bullet} \in B\}.$$



2-dimensional grid problems

Given bounded convex subsets A and B of the plane, the *2-dimensional grid problem* is to find $u \in \mathbb{Z}[\omega]$ such that

$$u \in A \quad \text{and} \quad u^{\bullet} \in B.$$

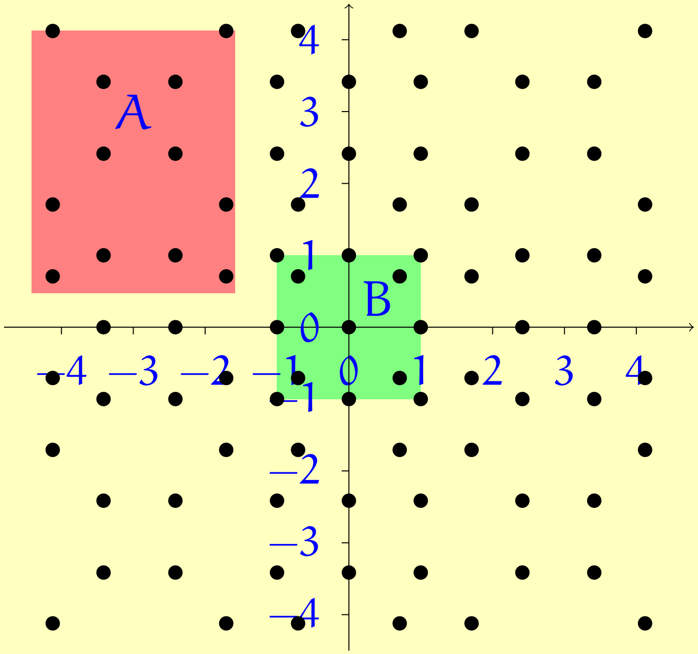


The easiest case: upright rectangles

If $A = [x_0, x_1] \times [y_0, y_1]$ and $B = [x'_0, x'_1] \times [y'_0, y'_1]$, the problem reduces to two 1-dimensional problems:

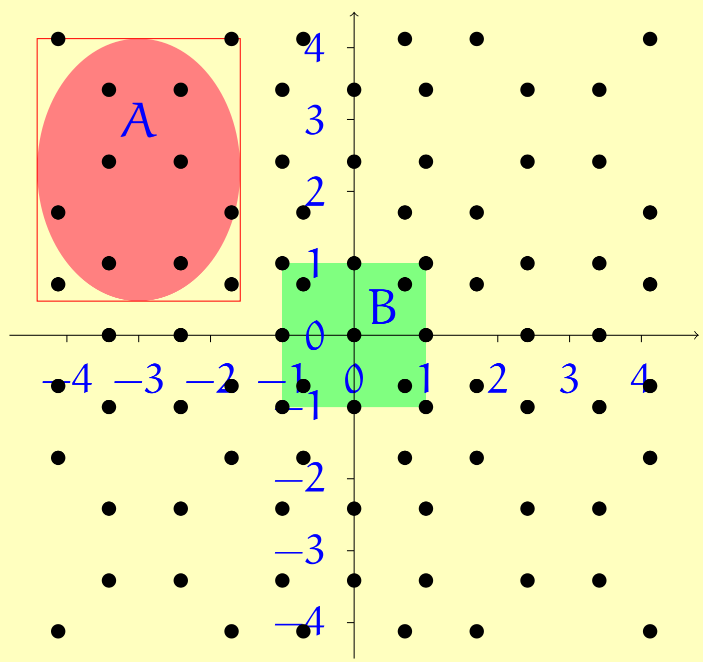
$$\alpha \in [x_0, x_1], \quad \alpha^\bullet \in [x'_0, x'1] \quad \text{and} \quad \beta \in [y_0, y_1], \quad \beta^\bullet \in [y'_0, y'_1],$$

where $u = \alpha + i\beta \in \mathbb{Z}[\omega]$. (This means $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ or $\alpha, \beta \in \mathbb{Z}[\sqrt{2}] + 1/\sqrt{2}$).



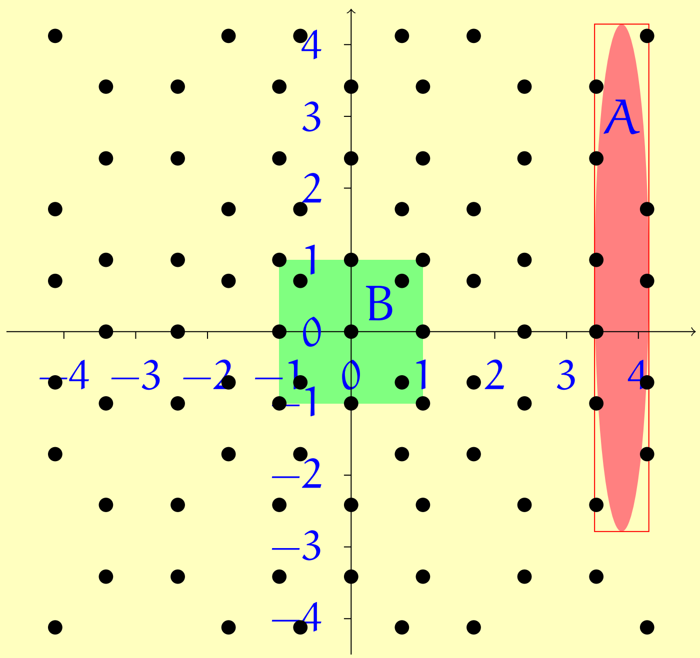
Also easy: upright sets

The *uprightness* of a set A is the ratio of its area to the area of its bounding box. If A and B are upright, the grid problem reduces to that of rectangles.



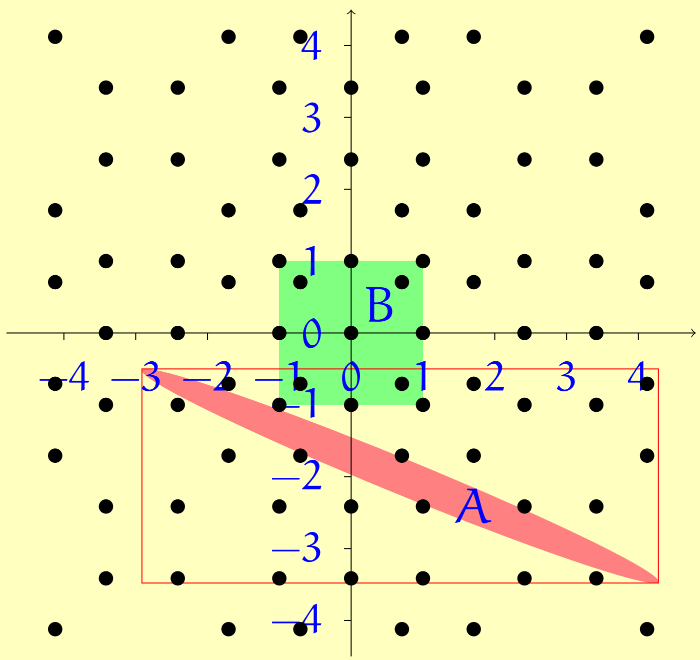
Also easy: upright sets

The *uprightness* of a set A is the ratio of its area to the area of its bounding box. If A and B are upright, the grid problem reduces to that of rectangles.



The hardest case: long and skinny, not upright

Convex sets that are not upright are long and skinny. In this case, finding grid points is a priori a hard problem.



Our solution: grid operators

A linear operator $G : \mathbb{R}^2 \to \mathbb{R}^2$ is called a *grid operator* if $G(Z[\omega]) = Z[\omega]$.

Some useful grid operators:

$$\mathbf{R} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \quad \mathbf{A} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{bmatrix}$$

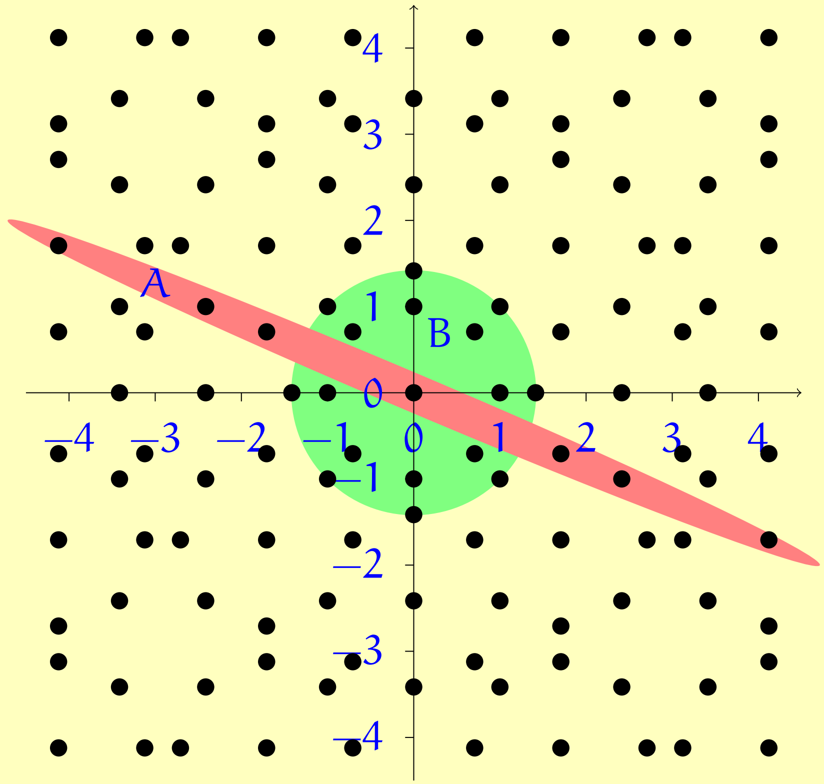
$$\mathbf{K} = \frac{1}{\sqrt{2}}\begin{bmatrix} -\lambda^{-1} & -1 \\ \lambda & 1 \end{bmatrix} \quad \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Proposition. Let G be a grid operator. Then the grid problem for A and B is equivalent to the grid problem for $G(A)$ and $G^{\bullet}(B)$.

Proof: obvious, because $\alpha \in A$ iff $G(\alpha) \in G(A)$, and $\alpha^{\bullet} \in B$ iff $G(\alpha)^{\bullet} \in G^{\bullet}(B)$.

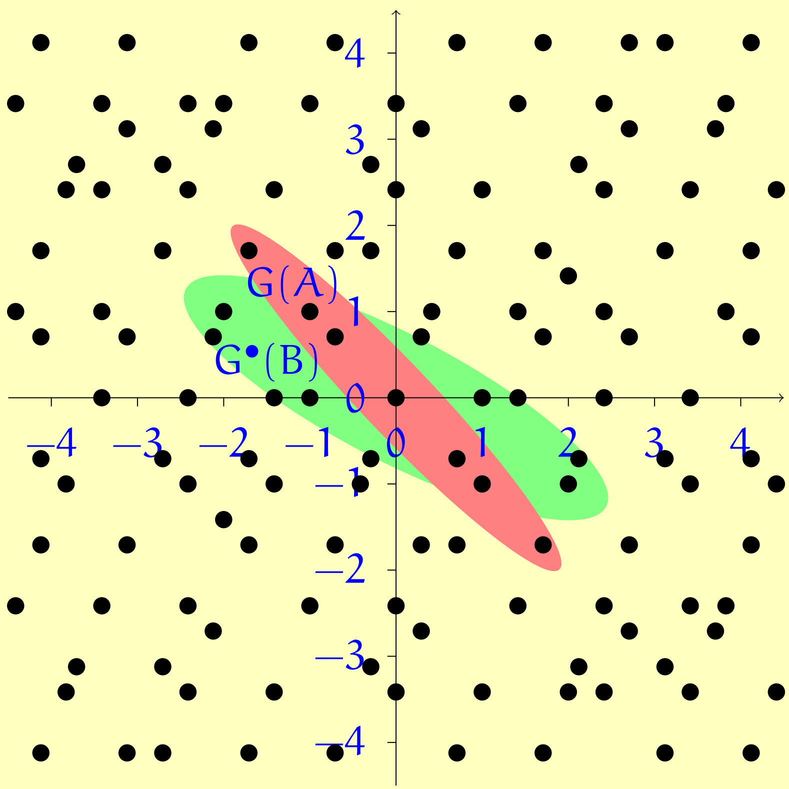
Effect of a grid operator

$$\mathbf{B} = \begin{bmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{bmatrix} \qquad \mathbf{B}^{\bullet} = \begin{bmatrix} 1 & -\sqrt{2} \\ 0 & 1 \end{bmatrix}$$



Effect of a grid operator

$$\mathbf{B} = \begin{bmatrix} 1 & \sqrt{2} \\ 0 & 1 \end{bmatrix} \qquad \mathbf{B}^{\bullet} = \begin{bmatrix} 1 & -\sqrt{2} \\ 0 & 1 \end{bmatrix}$$



Demo

Solution of 2-dimensional grid problems

Main Theorem. Let A and B be bounded convex sets with non-empty interior. Then there exists a grid operator G such that $G(A)$ and $G^{\bullet}(B)$ are $1/15$-upright.

Moreover, if A and B are M-upright, then G can be efficiently computed in $O(\log(1/M))$ steps.

Corollary (Solution of 2-dimensional grid problems). Let A and B be bounded convex sets with non-empty interior. There exists an efficient algorithm that enumerates all solutions of the grid problem for A and B.

Part II: An algorithm for optimal Clifford+T approximations

The single-qubit Clifford+T group

The *Clifford+T group* on one qubit is generated by the Hadamard gate H, the phase gate S, the scalar $\omega = e^{i\pi/4}$, and the T- or $\pi/8$-gate:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

$$\omega = e^{i\pi/4} = \frac{1+i}{\sqrt{2}}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}.$$

Exact synthesis of Clifford+T operators

Theorem (Kliuchnikov, Maslov, Mosca). *Let* $U = \begin{pmatrix} u & v \\ t & s \end{pmatrix}$ *be a unitary operator. Then* U *is a Clifford+T operator if and only if* $u, v, t, s \in \frac{1}{\sqrt{2}^k}\mathbb{Z}[\omega]$.

Example.

$$\frac{1}{\sqrt{2}^7}\begin{pmatrix} -3+4\sqrt{2}+(3+5\sqrt{2})\,i & 3+(-1+3\sqrt{2})\,i \\ -3-\sqrt{2}+(3-2\sqrt{2})\,i & 9-(1+3\sqrt{2})\,i \end{pmatrix}$$

$$= T\,HT\,SHT\,SHT\,HT\,SHT\,HT\,SHT\,HT\,HT\,SHT\,SSS\omega^7$$

Moreover, if $\det U = 1$, then the T-count of the resulting operator is equal to $2k-2$.

The approximate synthesis problem

Problem. Given an operator $U \in SU(2)$ and $\epsilon > 0$, find a Clifford+T operator U' of small T-count, such that $\|U' - U\| \leq \epsilon$.

Basic construction

We will approximate a z-rotation

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

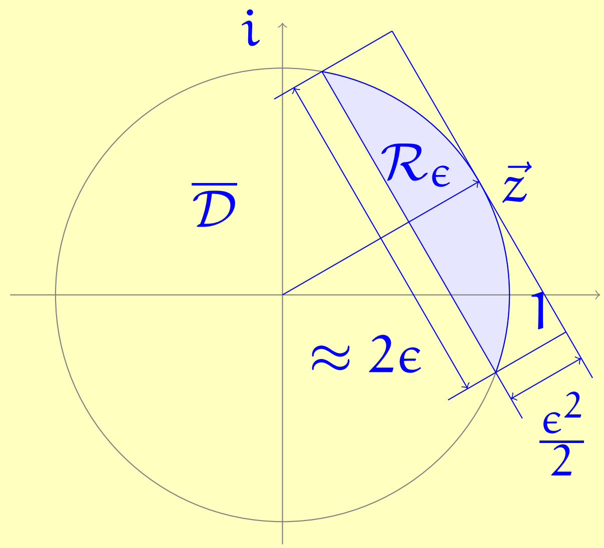
by a matrix of the form

$$U = \frac{1}{\sqrt{2}^k} \begin{pmatrix} u & -t^\dagger \\ t & u^\dagger \end{pmatrix},$$

where $u, t \in \mathbb{Z}[\omega]$.

Observation. The error is a function of u (and not of t). Indeed, setting $z = e^{-i\theta/2}$ and $u' = \frac{u}{\sqrt{2}^k}$, we have

$$\|U - R_z(\theta)\| \leq \epsilon \quad \text{iff} \quad \vec{u}' \cdot \vec{z} \geq 1 - \frac{\epsilon^2}{2}.$$



The problem then reduces to:

(1) Finding $u \in \mathbb{Z}[\omega]$ such that $\frac{u}{\sqrt{2}^k} \in \mathcal{R}_\epsilon$, with small k;

(2) Solving the Diophantine equation $t^\dagger t + u^\dagger u = 2^k$.

Diophantine equations are computationally easy (if we can factor)

Consider a Diophantine equation of the form

$$t^\dagger t = \xi \tag{1}$$

where $\xi \in \mathbb{Z}[\sqrt{2}]$ is given and $t \in \mathbb{Z}[\omega]$ is unknown.

Necessary condition. The equation (1) has a solution only if $\xi \geq 0$ and $\xi^\bullet \geq 0$.

Theorem. There exists a probabilistic polynomial time algorithm which decides whether the equation (1) has a solution or not, and produces the solution if there is one, *provided that the algorithm is given the prime factorization of* $n = \xi^\bullet \xi$.

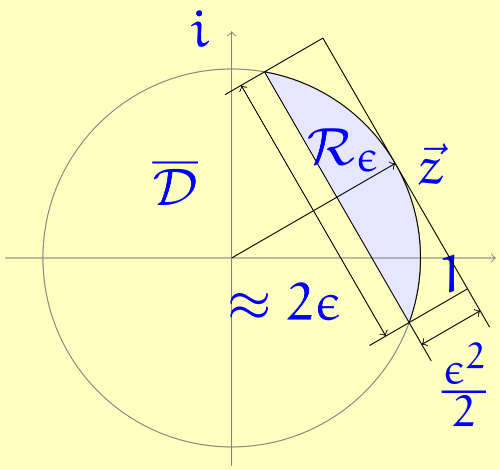
This is okay, because factoring random numbers is not as hard as worst-case numbers.

The candidate selection problem

The only remaining problem is to find suitable u. Note that $\xi^\bullet = (2^k - u^\dagger u)^\bullet \geq 0$ iff $u^\bullet/\sqrt{2}^k$ is in the unit disk.

Candidate selection problem. Find $k \in \mathbb{N}$ and $u \in \mathbb{Z}[\omega]$ such that

1. $u/\sqrt{2}^k$ is in the epsilon-region $\mathcal{R}_\epsilon$;
2. $u^\bullet/\sqrt{2}^k$ is in the unit disk;



But this is a 2-dimensional grid problem, so can be solved efficiently.

Algorithm 1

(1) For all $k \in \mathbb{N}$, enumerate all $u \in \mathbb{Z}[\omega]$ such that $u/\sqrt{2}^k \in \mathcal{R}_\epsilon$ and $u^\bullet/\sqrt{2}^k \in \overline{\mathcal{D}}$.

(2) For each u:
   (a) Compute $\xi = 2^k - u^\dagger u$ and $n = \xi^\bullet \xi$.
   (b) Attempt to find a prime factorization of n.
   (c) If a prime factorization is found, attempt to solve the equation $t^\dagger t = \xi$.

(3) When step (2) succeeds, output U.

Results

- In the presence of a factoring oracle (e.g., a quantum computer), Algorithm 1 is *optimal* in an absolute sense: it finds the solution with the smallest possible T-count whatsoever, for the given θ and ϵ.

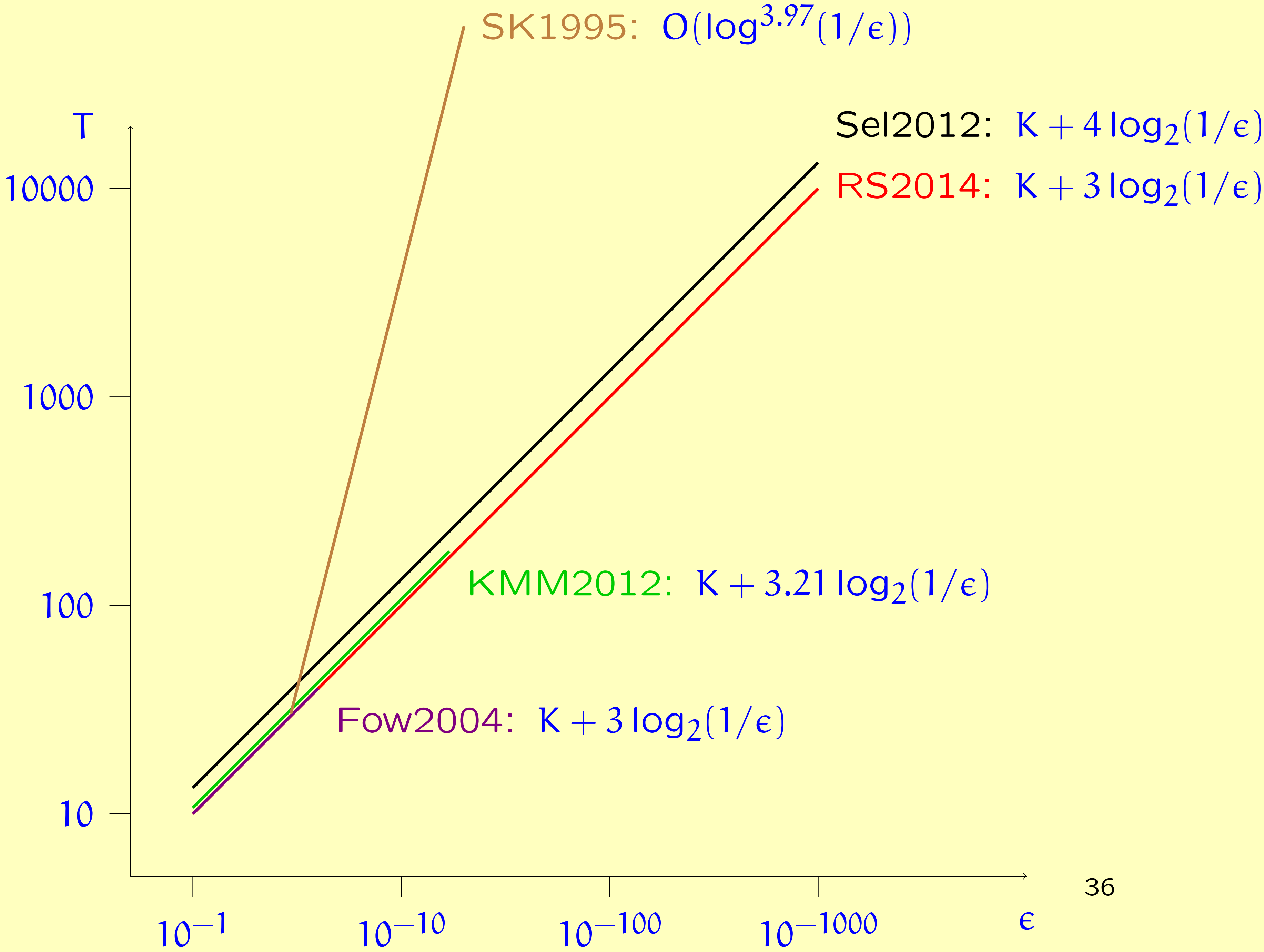
- In the absence of a factoring oracle, Algorithm 1 is *nearly optimal*: it yields T-counts of $m + O(\log(\log(1/\epsilon)))$, where m is the second-to-optimal T-count.

- The algorithm yields an *upper bound* and a *lower bound* for the T-count of each problem instance.

- The runtime is polynomial in $\log(1/\epsilon)$.

Gate complexity, in numbers.

Precision	Solovay-Kitaev	Lower bound	This algorithm
$\epsilon = 10^{-10}$	$\approx 4,000$	102	102
$\epsilon = 10^{-20}$	$\approx 60,000$	198	200
$\epsilon = 10^{-100}$	$\approx 37,000,000$	998	1000
$\epsilon = 10^{-1000}$	$\approx 350,000,000,000$	9966	9974



SK1995: $O(\log^{3.97}(1/\epsilon))$
Sel2012: $K + 4\log_2(1/\epsilon)$
RS2014: $K + 3\log_2(1/\epsilon)$
KMM2012: $K + 3.21\log_2(1/\epsilon)$
Fow2004: $K + 3\log_2(1/\epsilon)$
T
10000
1000
100
10
10^{-1}
10^{-10}
10^{-100}
10^{-1000}
ϵ

The end.