Number-theoretic methods for unitary approximation problems

Peter Selinger

Dalhousie University
Halifax, Canada

MAP 2016 Workshop on Effective Analysis
CIRM, January 11-15, 2016

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.

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

Part I: Some number theory

Some number theory: Fermat's theorem on sums of two squares

Which integers can be written as a sum of two squares?

Some number theory: Fermat's theorem on sums of two squares

Which integers can be written as a sum of two squares?

Theorem. If n and m can each be written as a sum of two squares, then nm can be written as a sum of two squares.

Some number theory: Fermat's theorem on sums of two squares

Which integers can be written as a sum of two squares?

Theorem. If n and m can each be written as a sum of two squares, then nm can be written as a sum of two squares.

Proof. This is easiest seen using complex numbers. Note that $a^2 + b^2 = (a + bi)(a - bi)$.

Therefore, n is a sum of two squares if and only if it can be written in the form $t^\dagger t$, for some Gaussian integer $t = a + bi \in \mathbb{Z}[i]$.

The claim follows because $nm = (t^\dagger t)(u^\dagger u) = (tu)^\dagger (tu)$. $\square$

First lesson of number theory

We can learn more about the integers by moving to a larger ring, such as $\mathbb{Z}[\mathrm{i}]$.

Fermat's theorem on sums of two squares, continued

What about the converse?

Theorem. If nm can be written as a sum of two squares, and if n, m are relatively prime, and $n, m \geq 0$, then n and m can each be written as a sum of two squares.

Fermat's theorem on sums of two squares, continued

What about the converse?

Theorem. If nm can be written as a sum of two squares, and if n, m are relatively prime, and $n, m \geq 0$, then n and m can each be written as a sum of two squares.

Proof. Suppose $nm = a^2 + b^2 = (a + bi)(a - bi)$.

$\mathbb{Z}[i]$ is a Euclidean domain, so has greatest common divisors. Let $t = \mathsf{gcd}(n, a + bi)$ and $s = \mathsf{gcd}(m, a + bi)$ in $\mathbb{Z}[i]$.

An easy argument (using uniqueness of prime factorizations in $\mathbb{Z}[i]$) shows that $n = t^\dagger t$ and $m = s^\dagger s$. Hence both n and m can be written as a sum of two squares.

Second lesson of number theory

The fact that $\mathbb{Z}[\mathrm{i}]$ is a Euclidean domain, and in particular, the ability to take greatest common divisors and prime factorizations in $\mathbb{Z}[\mathrm{i}]$, is very helpful.

Definition. A ring is called a *Euclidean domain* if it is equipped with a notion of *division with remainder*. Specifically, such a ring must have:

1. A *Euclidean function*, i.e., a function f assigning a natural number to each ring element;

2. *Division with remainder*: For all a, b with $b \neq 0$, there exist q, r such that

$$a = bq + r$$

and $f(r) < f(b)$.

Main properties. In a Euclidean domain, the concepts of *divisor*, *greatest common divisor*, and *prime* make sense. The Euclidean algorithm can be used to compute greatest common divisors $d = \gcd(a, b)$, as well as x, y such that $d = xa + yb$. Euclidean domains satisfy unique prime factorization.

Fermat's theorem on sums of two squares, continued

By the previous theorems, it suffices to consider primes. Which primes can be written as a sum of two squares?

Obvious necessary condition: $p > 0$.

p		$a^2 + b^2$
2	$=$	$1 + 1$
3	$=$	—
5	$=$	$1 + 4$
7	$=$	—
11	$=$	—
13	$=$	$4 + 9$
17	$=$	$1 + 16$
19	$=$	—
23	$=$	—
29	$=$	$4 + 25$

p		$a^2 + b^2$
31	$=$	—
37	$=$	$1 + 36$
41	$=$	$16 + 25$
43	$=$	—
47	$=$	—
53	$=$	$4 + 49$
59	$=$	—
61	$=$	$25 + 36$
67	$=$	—
71	$=$	—

Fermat's theorem on sums of two squares, continued

By the previous theorems, it suffices to consider primes. Which primes can be written as a sum of two squares?

Obvious necessary condition: $p > 0$.

p		a^2+b^2	$p \pmod 4$
2	$=$	$1+1$	2
3	$=$	—	3
5	$=$	$1+4$	1
7	$=$	—	3
11	$=$	—	3
13	$=$	$4+9$	1
17	$=$	$1+16$	1
19	$=$	—	3
23	$=$	—	3
29	$=$	$4+25$	1

p		a^2+b^2	$p \pmod 4$
31	$=$	—	3
37	$=$	$1+36$	1
41	$=$	$16+25$	1
43	$=$	—	3
47	$=$	—	3
53	$=$	$4+49$	1
59	$=$	—	3
61	$=$	$25+36$	1
67	$=$	—	3
71	$=$	—	3

Fermat's theorem on sums of two squares, continued

Theorem. A positive odd prime p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$.

Proof. "$\Rightarrow$": $a^2 \equiv 0, 1 \pmod 4$, hence $a^2 + b^2 \equiv 0, 1, 2 \pmod 4$.

"$\Leftarrow$" Suppose p is a positive prime with $p \equiv 1 \pmod 4$.

(1) We can find $h \in \mathbb{Z}_p$ such that $h^2 = -1$. (This follows from Fermat's Little Theorem). W.l.o.g. $h < p/2$.

(2) Therefore, $h^2 + 1 = kp$, for some $k \in \mathbf{Z}$. So kp can be written as a sum of two squares. It follows from the previous theorem that p can be written as a sum of two squares. $\square$

Moreover: There is an efficient algorithm to compute a, b.

Summary: Algorithm for $n = a^2 + b^2$

We shows that there exists an efficient (probabilistic) algorithm which,

- **given** a number $n \in \mathbb{Z}$, and
- **given** a prime factorization of n,
- **decides** whether there exists $a, b \in \mathbb{Z}$ with $a^2 + b^2 = n$, and
- **computes** such a, b if they exist.

Part II: An algebraic characterization of Clifford+T circuits

Subgroups of $SO(3)$

Consider the following elements of $SO(3)$:

- S_x: a 90°rotation about the x-axis;
- S_y: a 90°rotation about the y-axis;
- S_z: a 90°rotation about the z-axis.

$$S_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \quad S_y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \quad S_z = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let $\mathbf{C}_{90}$ be the group generated by these elements. It is a finite group, consisting of the 24 symmetries of the cube.

Algebraic characterization

Note that an element of $SO(3)$ is in $\mathbf{C}_{90}$ if and only if the matrix entries are integer coefficients. In other words, $\mathbf{C}_{90} = SO_3(\mathbb{Z})$.

Generators and relations

Two generators S_x, S_z suffice because $S_y = S_z^{-1} S_x^{-1} S_z$. The group is presented by these relations:

- $(S_x S_z)^3 = 1$;
- $(S_z)^4 = 1$;
- $(S_x S_z S_x)^2 = 1$.

Adding 45°rotations

Consider the following additional elements of $SO(3)$:

- T_x: a 45°rotation about the x-axis;
- T_y: a 45°rotation about the y-axis;
- T_z: a 45°rotation about the z-axis.

$$T_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \quad T_y = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ 0 & 1 & 0 \\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \quad T_z = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let $\mathbf{C}_{45}$ be the generated group. It is infinite; in fact, it is a dense subgroup of in $SO(3)$.

Algebraic characterization

Consider the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}]$. Its elements are numbers of the form

$$\frac{a+b\sqrt{2}}{\sqrt{2}^k},$$

where $a, b \in \mathbb{Z}$ and $k \in \mathbb{N}$.

It is obvious that the matrix entries of T_x, T_y, T_z are in $\mathbb{Z}[\frac{1}{\sqrt{2}}]$, and therefore the same is true for every member of $\mathbf{C}_{45}$.

Remarkably, the converse is true as well:

Theorem. An element of $SO(3)$ is in $\mathbf{C}_{45}$ if and only if its matrix entries are in the ring $\mathbb{Z}[\frac{1}{\sqrt{2}}]$.

In other words, $\mathbf{C}_{45} = SO_3(\mathbb{Z}[\frac{1}{\sqrt{2}}])$.

Proof idea.

Let $U \in SO_3(\mathbb{Z}[\frac{1}{\sqrt{2}}])$. By definition, U is of the form

$$U = \frac{1}{\sqrt{2}^k} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

where each $a_{ij} \in \mathbb{Z}[\sqrt{2}]$. Let k be smallest. The proof is by induction on k.

First note that $\sqrt{2}$ is a prime in the ring $\mathbb{Z}[\sqrt{2}]$, and $\mathbb{Z}[\sqrt{2}]/(\sqrt{2}) = \{0, 1\}$.

- If $k = 0$, then a simple argument shows that $U \in SO_3(\mathbb{Z}) = \mathbf{C}_{90}$ and we are done.

Proof idea, continued.

- If $k > 0$, then consider the matrix

$$\bar{U} = \begin{pmatrix} \bar{a}_{11} & \bar{a}_{12} & \bar{a}_{13} \\ \bar{a}_{21} & \bar{a}_{22} & \bar{a}_{23} \\ \bar{a}_{31} & \bar{a}_{32} & \bar{a}_{33} \end{pmatrix},$$

  where each $\bar{a}_{ij} \in \{0, 1\}$ is the residue class of a_{ij} modulo $\sqrt{2}$.

  Since U is orthogonal, each row and column of $\bar{U}$ contains an even number of 1's, and any two columns overlap in an even number of 1's. It follows that there are only 3 possible patterns (up to a permutation of columns):

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Proof idea, continued.

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

- If $\bar{u}$ is of the first form, apply T_x.
- If $\bar{u}$ is of the second form, apply T_y.
- If $\bar{u}$ is of the third form, apply T_z.

Each of these transformations reduces k by exactly 1!

Therefore, $SO_3(\mathbb{Z}[\frac{1}{\sqrt{2}}]) = \mathbf{C}_{45}$.

Normal form

In fact, we have shown a stronger result! We have shown that every operator $U \in SO_3(\mathbb{Z}[\frac{1}{\sqrt{2}}])$,

$$U = \frac{1}{\sqrt{2}^k} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

can be written in the form

$$T_1\, T_2 \, \ldots \, T_k \, C,$$

where each $T_i \in \{T_x, T_y, T_z\}$ and $C \in \mathbb{C}_{90}$.

Moreover, the number of T's is exactly equal to k, and therefore *minimal*. It follows that no two consecutive T_i's are equal.

Uniqueness

Moreover, essentially the same argument shows that the normal form $U = T_1\,T_2\,\ldots\,T_k\,C$ is *unique*. Namely:

- if $T_1 = T_x$, the residue class of U is $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}$.
- similarly if $T_1 = T_y$ or $T_1 = T_z$.

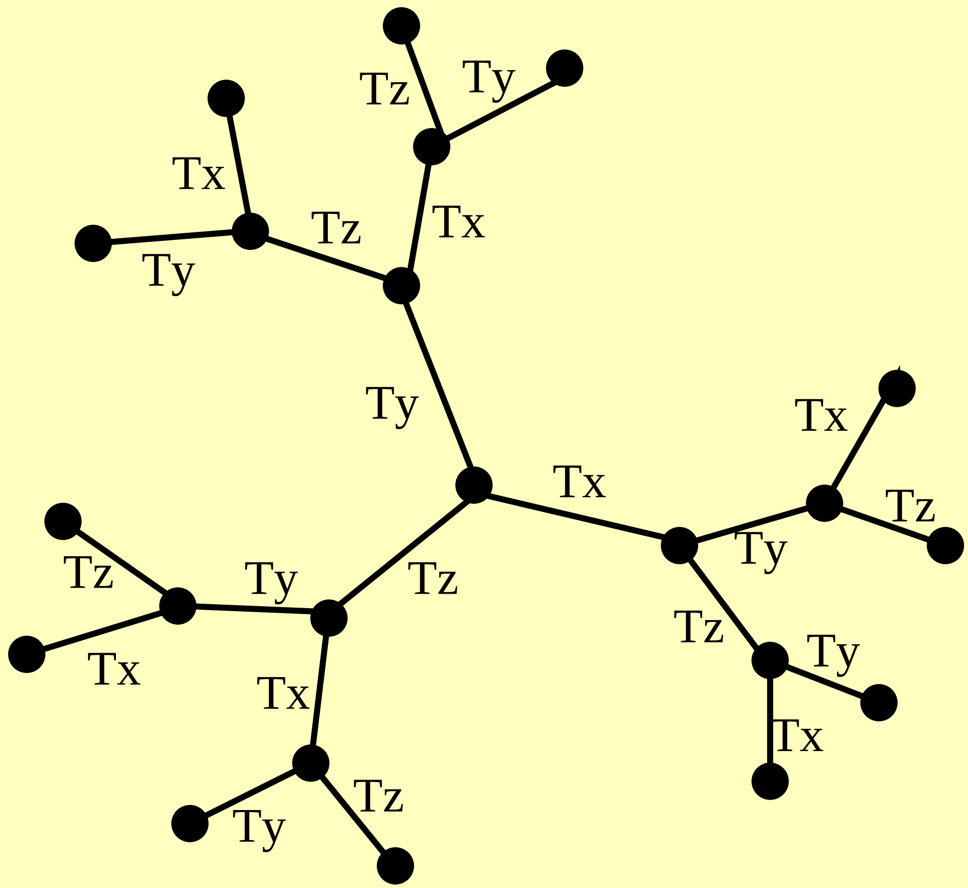
In summary, we have the following theorem:

Theorem. Every element $U \in SO_3(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ can be *uniquely* written in the form

$$T_1\,T_2\,\ldots\,T_k\,C,$$

where each $T_i \in \{T_x, T_y, T_z\}$, $C \in \mathbb{C}_{90}$, and no two consecutive T_i's are equal.

Another way to say this is that the set $\mathbb{C}_{45}/\mathbb{C}_{90}$ has the structure of a *regular tree*.



Approximating unitary operations by quantum circuits

Definition. The *Clifford group* is the subgroup of $\mathrm{U}(2)$ generated by the following operators:

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

The *Clifford+T group* is obtained by further adding the operator

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}.$$

In quantum computing, the generators are called *gates*, and words in the generators are called *quantum circuits*.

The Clifford group is finite. The Clifford+T group is dense in $\mathrm{PSU}(2)$.

The approximate synthesis problem

- The *exact synthesis problem* is: given a unitary operator U in the Clifford+T group, find an actual quantum circuit implementing it.

- The *approximate synthesis problem* is: given a unitary operator U in $SU(2)$ and an $\epsilon > 0$, find a quantum circuit that approximates U to within ϵ.

  Moreover, the circuit should be short, and the solution should be computed by an efficient algorithm.

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 III: Grid problems

Neil J. Ross* and Peter Selinger**

* University of Maryland

** Dalhousie University

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*: $(a + b\sqrt{2})^\bullet = a - b\sqrt{2}$.

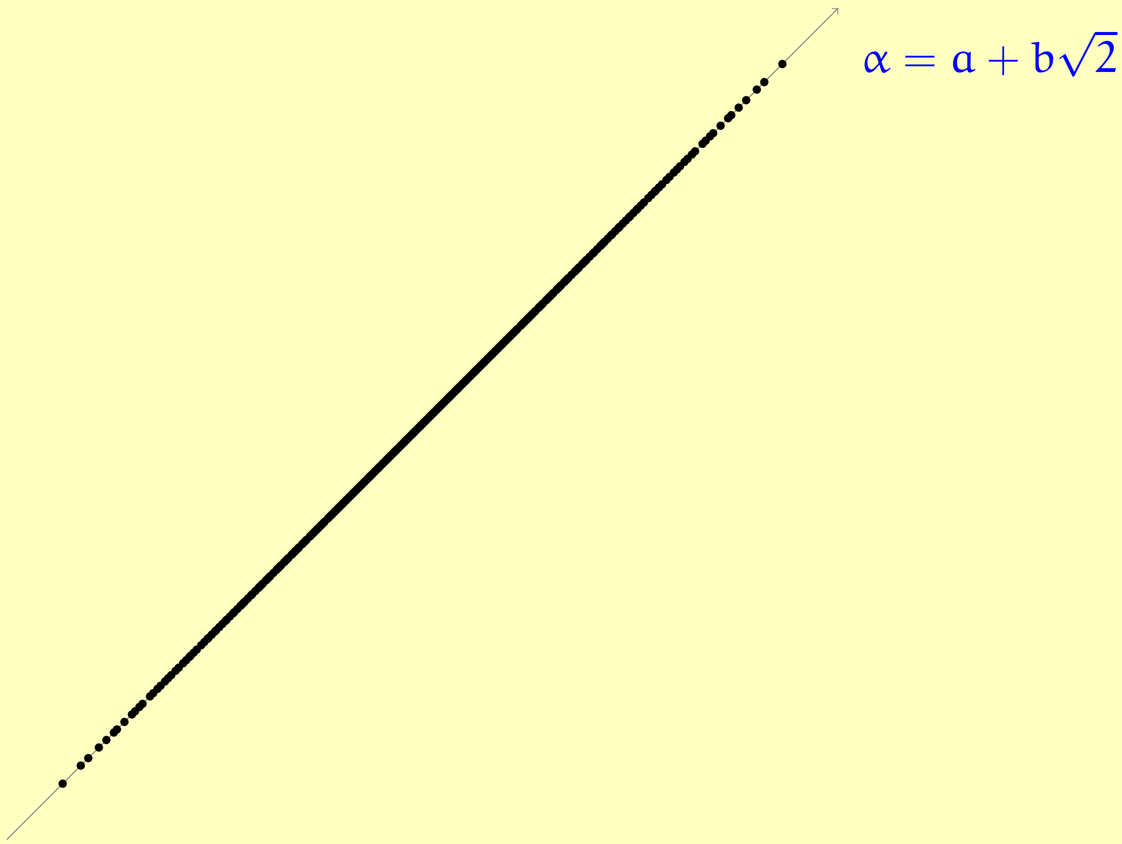
The map "$\bullet$" is an automorphism:

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

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

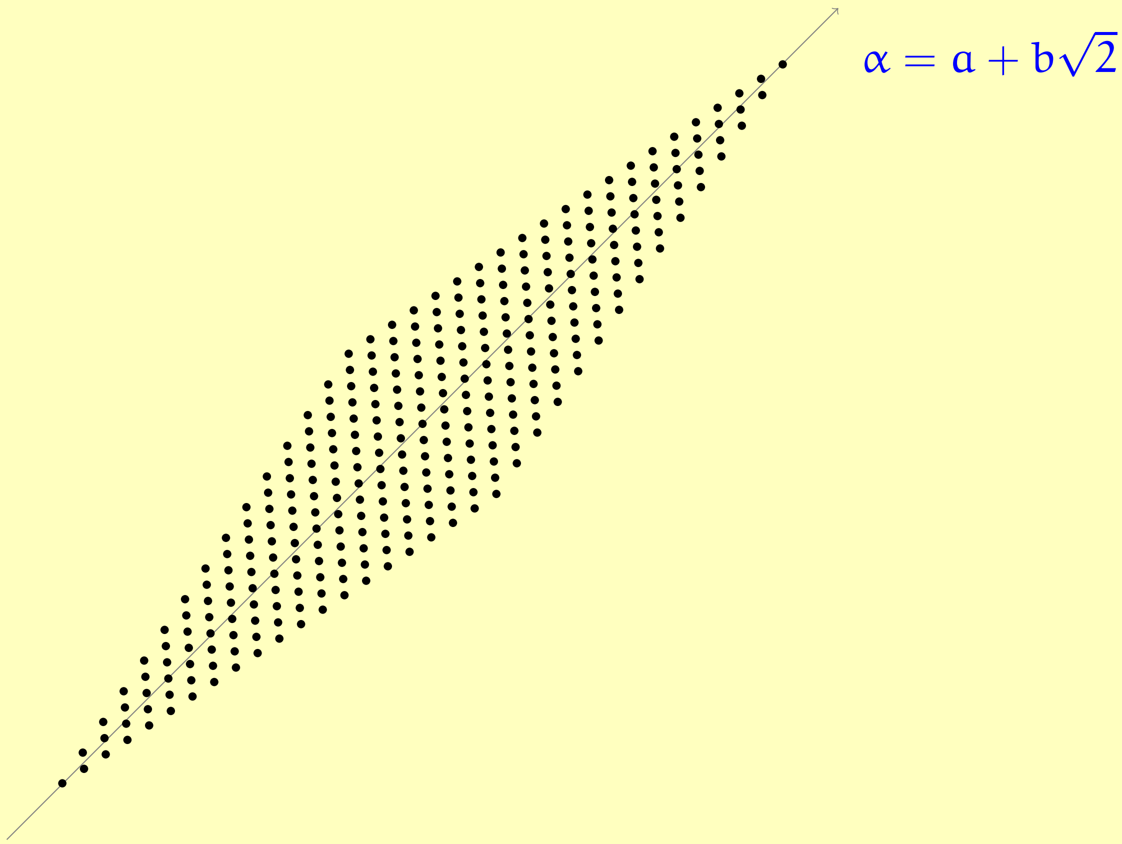
Dense or discrete?

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



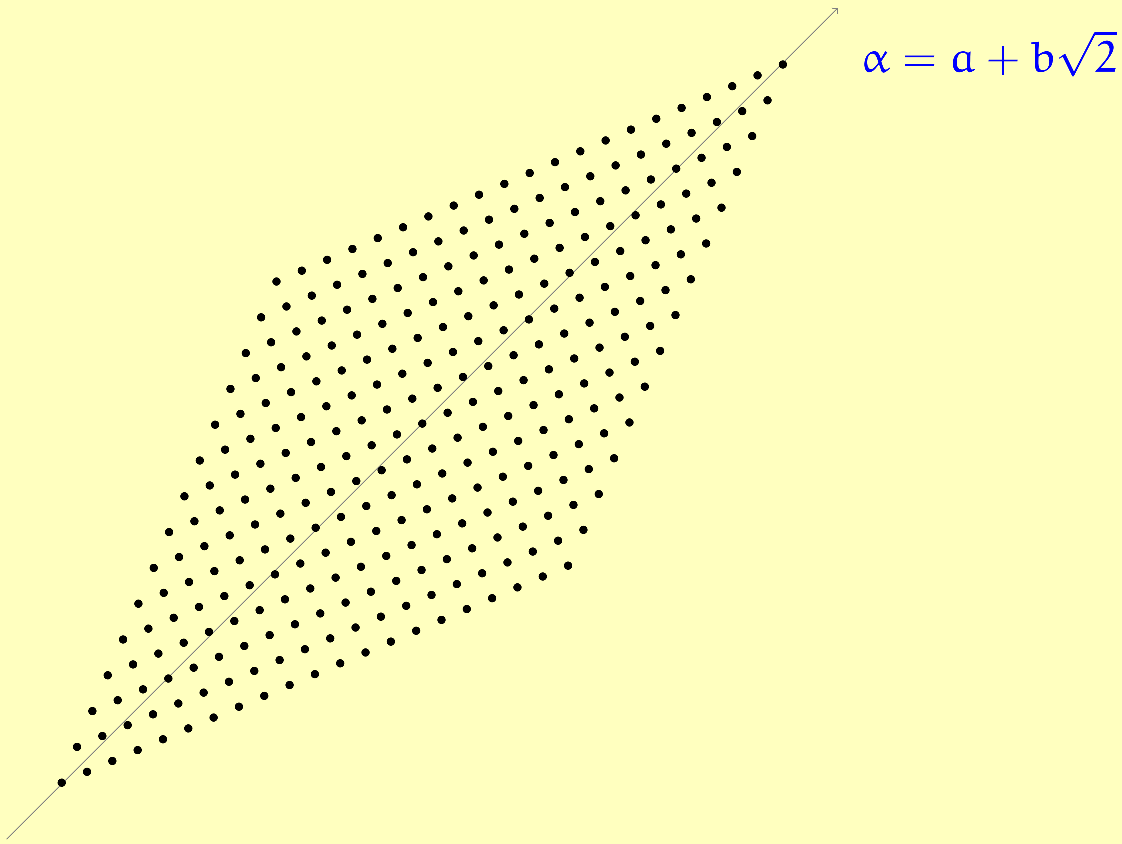
Dense or discrete?

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



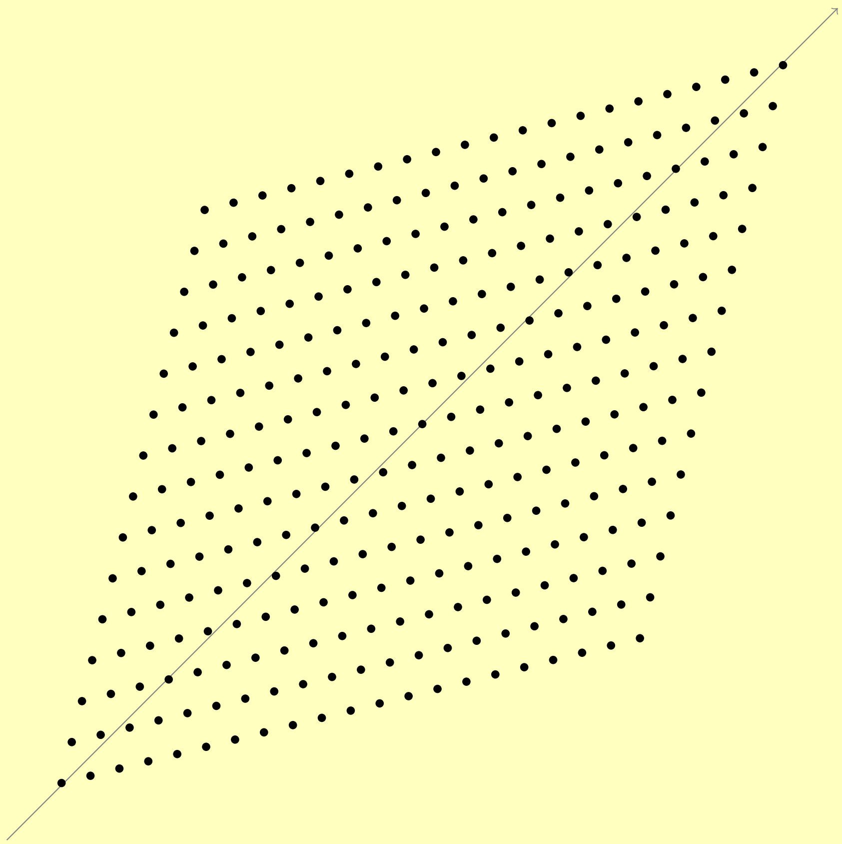
Dense or discrete?

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



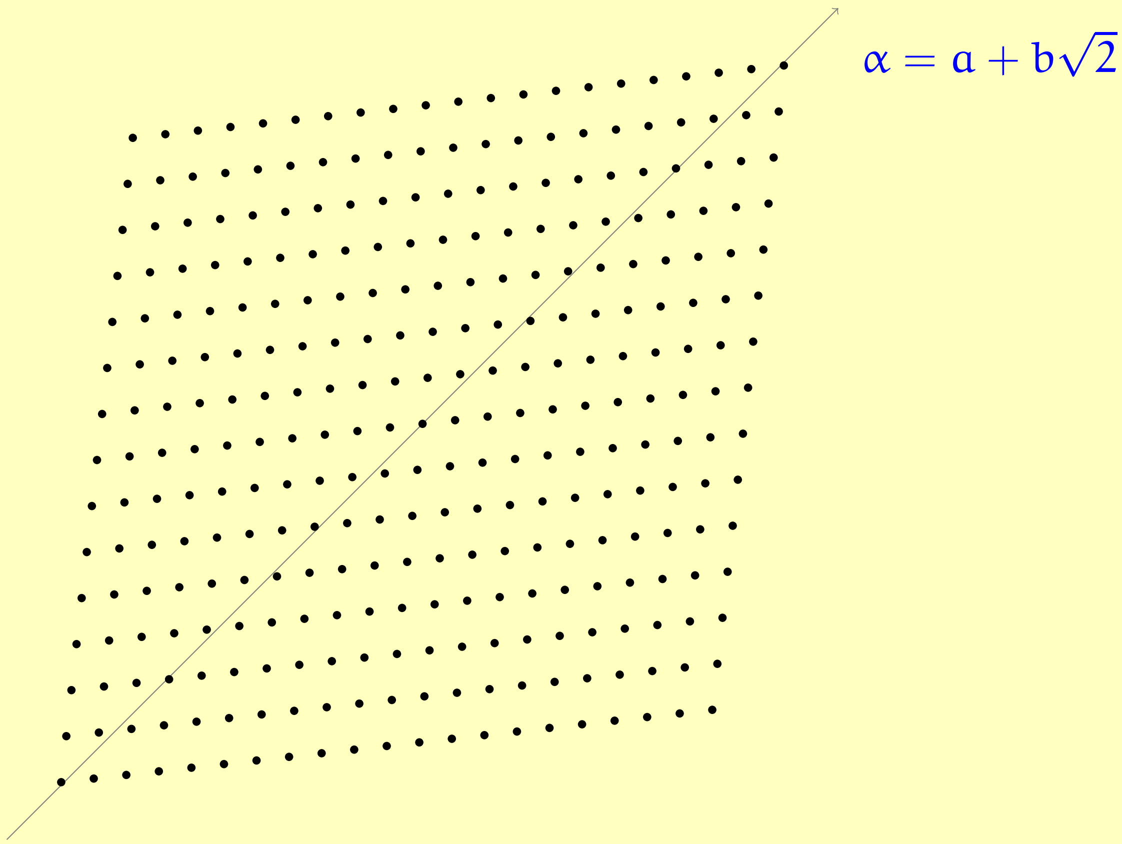
Dense or discrete?

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



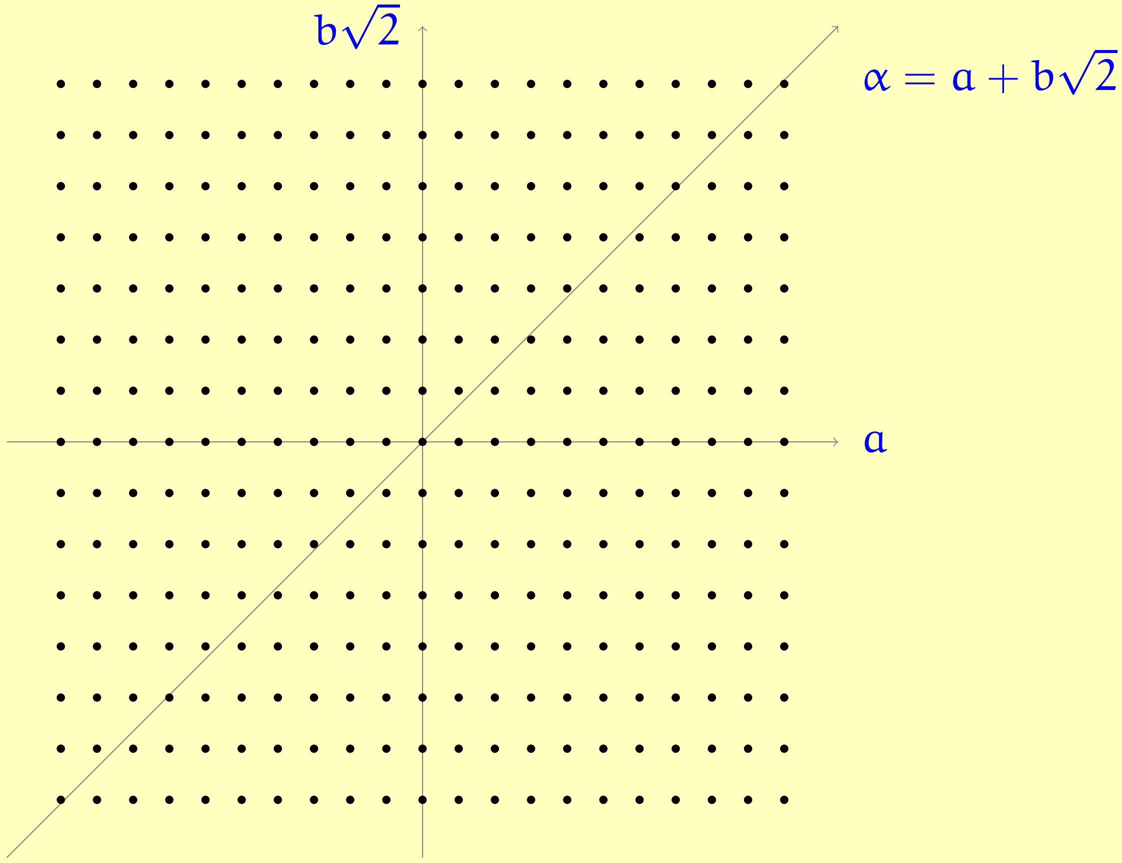
Dense or discrete?

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



Dense or discrete?

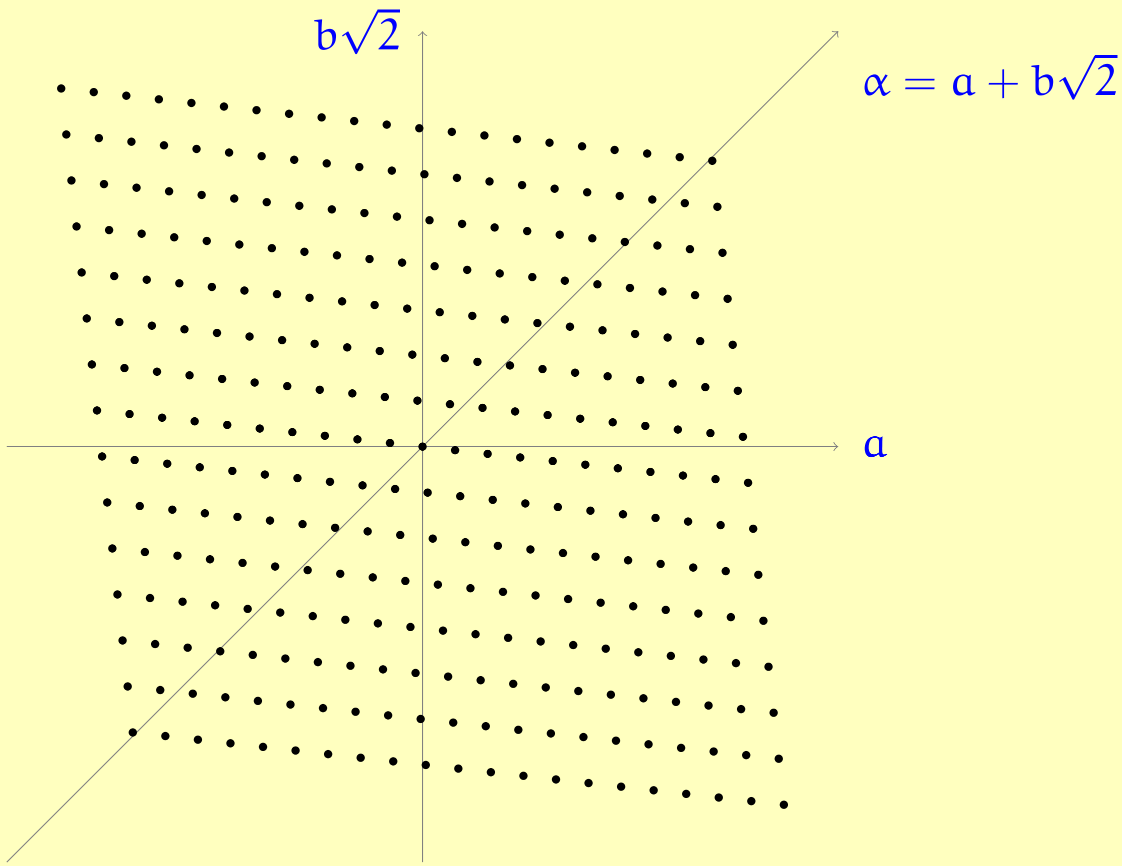
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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

Dense or discrete?

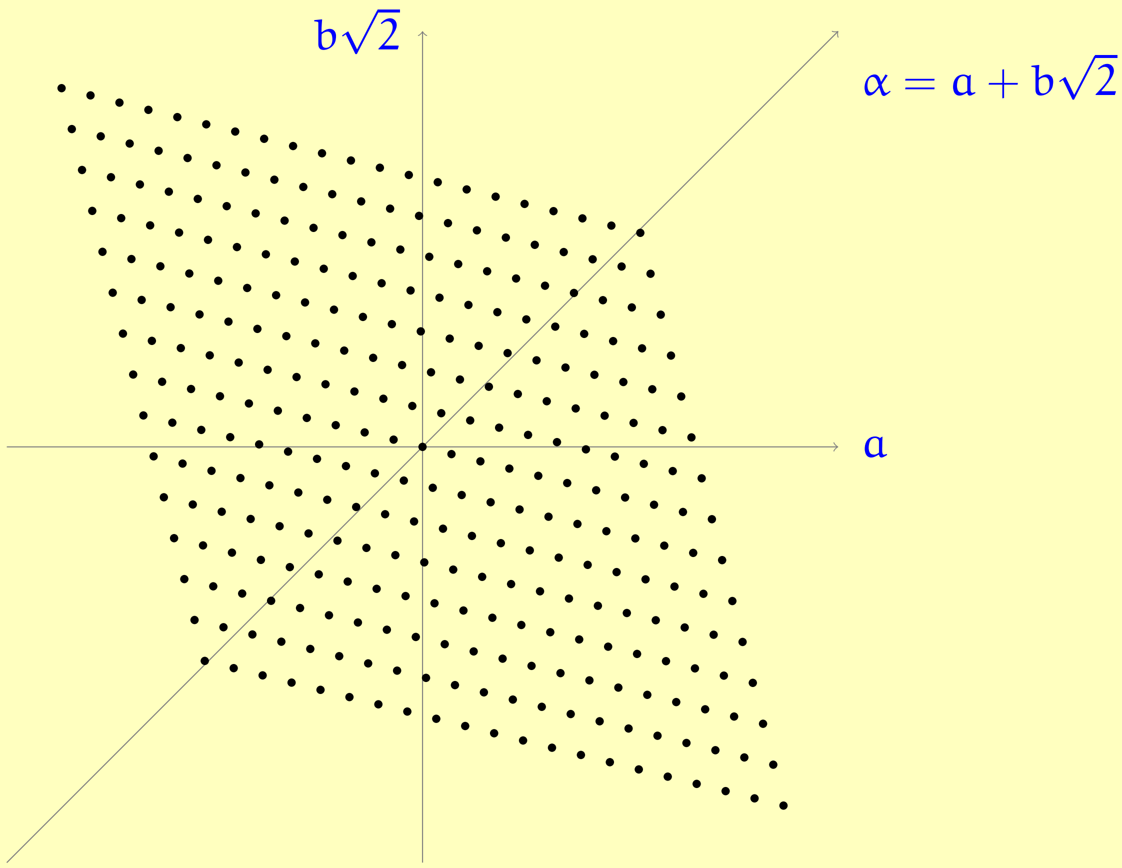
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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

Dense or discrete?

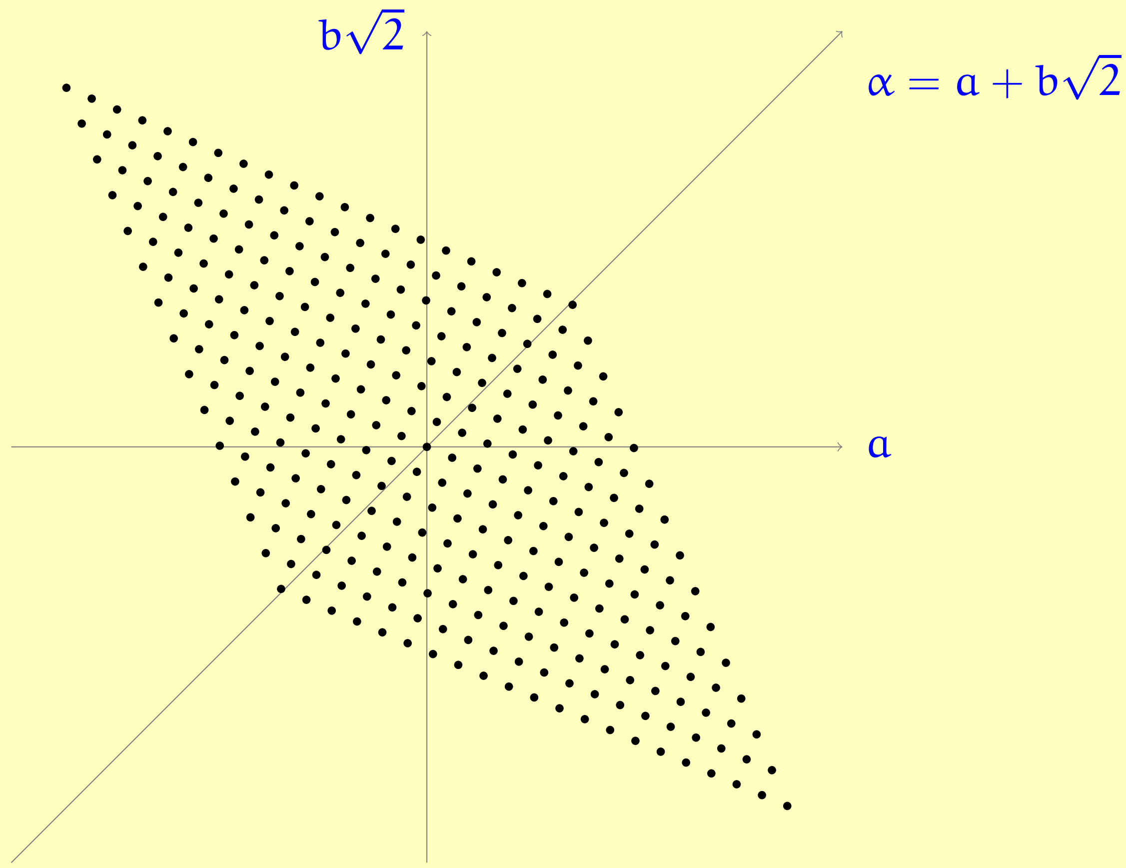
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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

Dense or discrete?

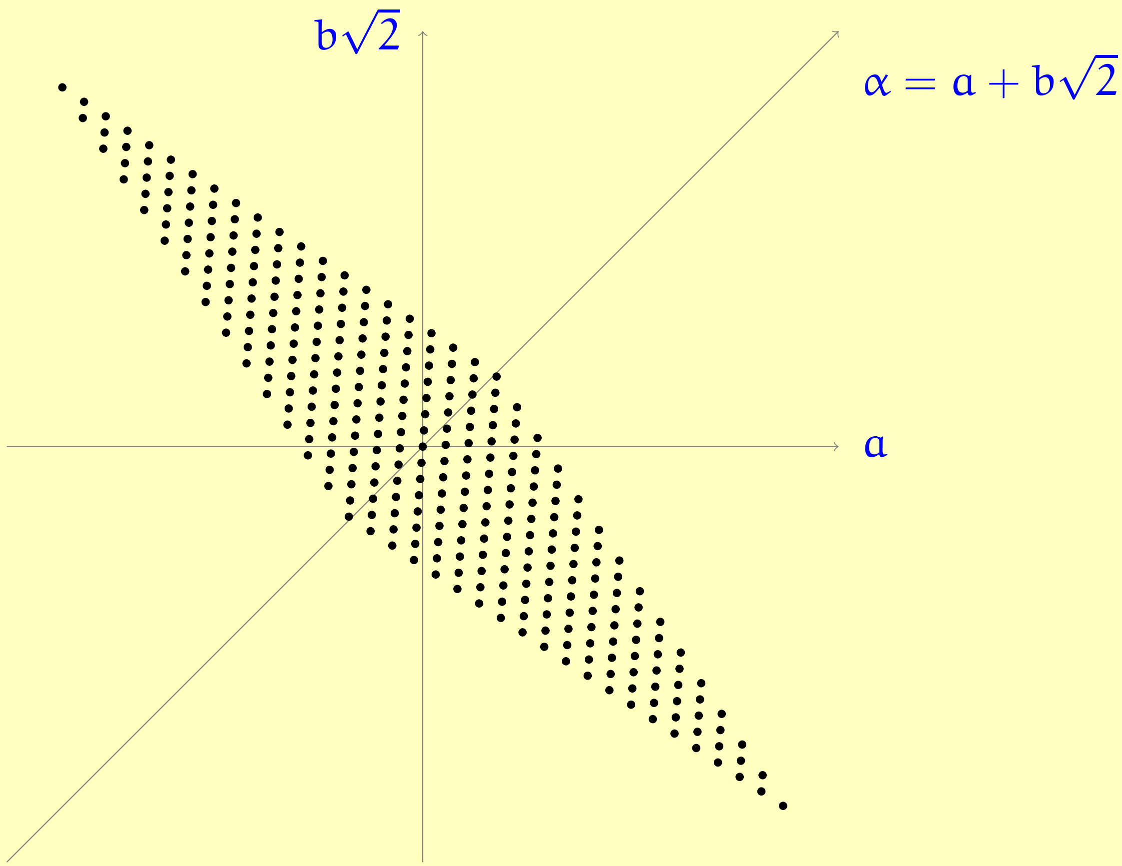
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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

Dense or discrete?

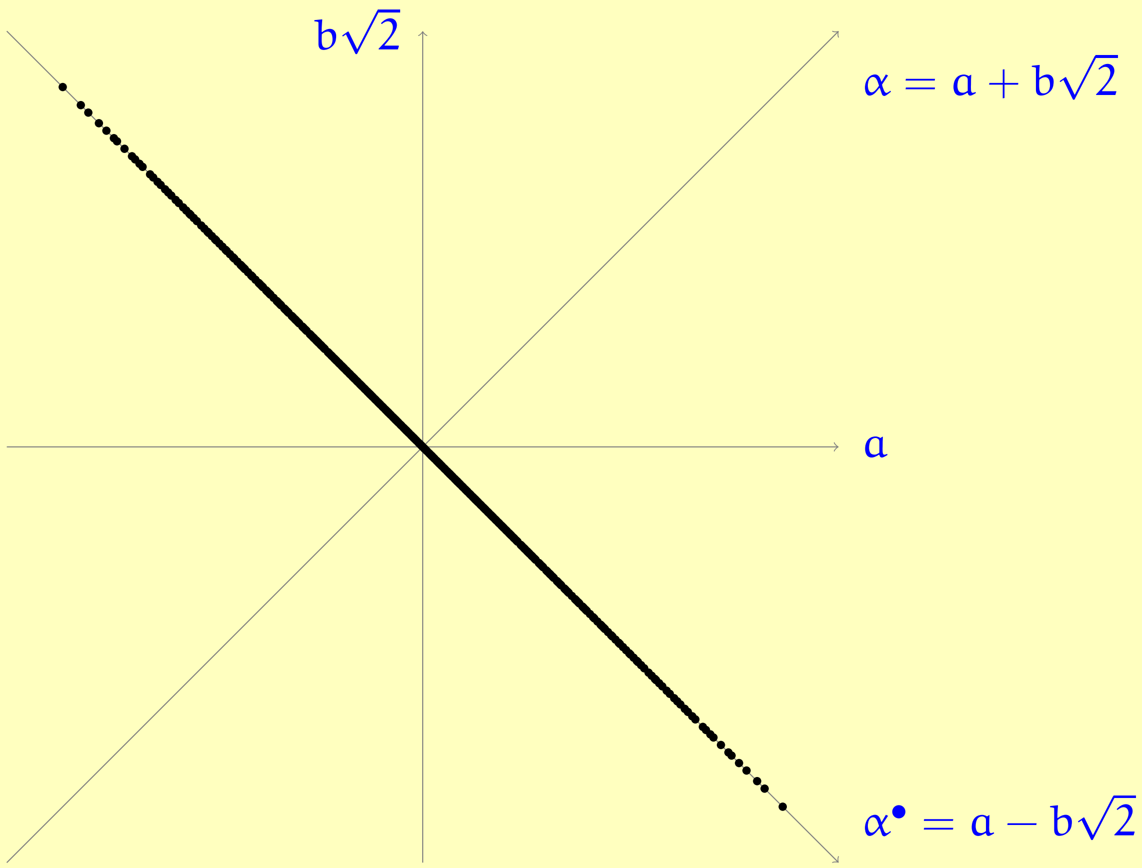
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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

Dense or discrete?

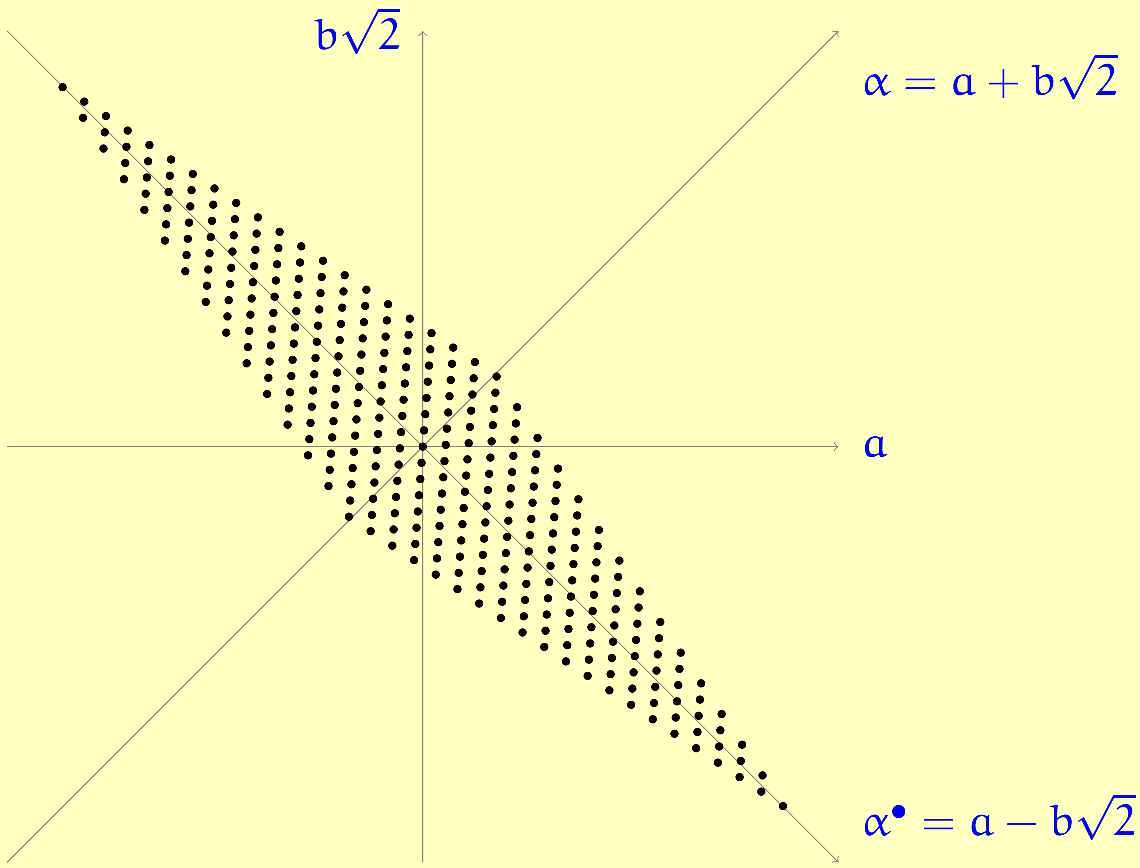
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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

Dense or discrete?

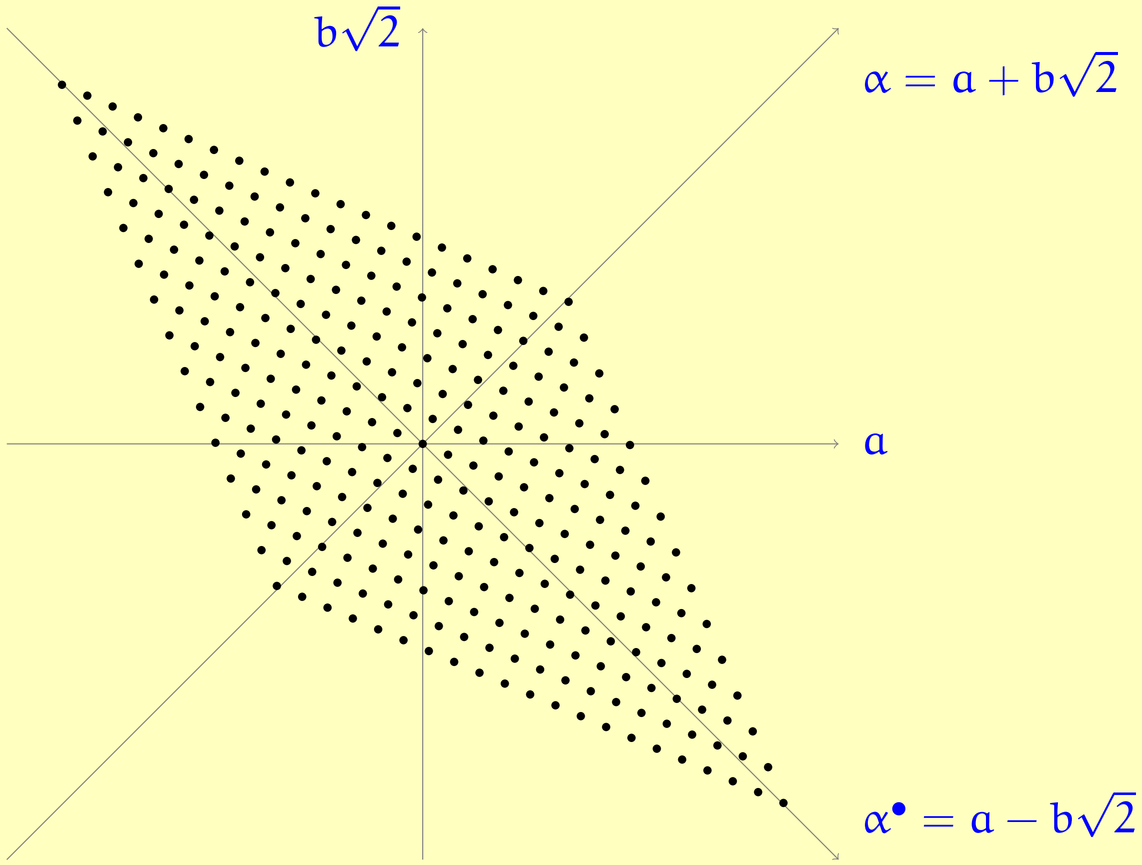
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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

Dense or discrete?

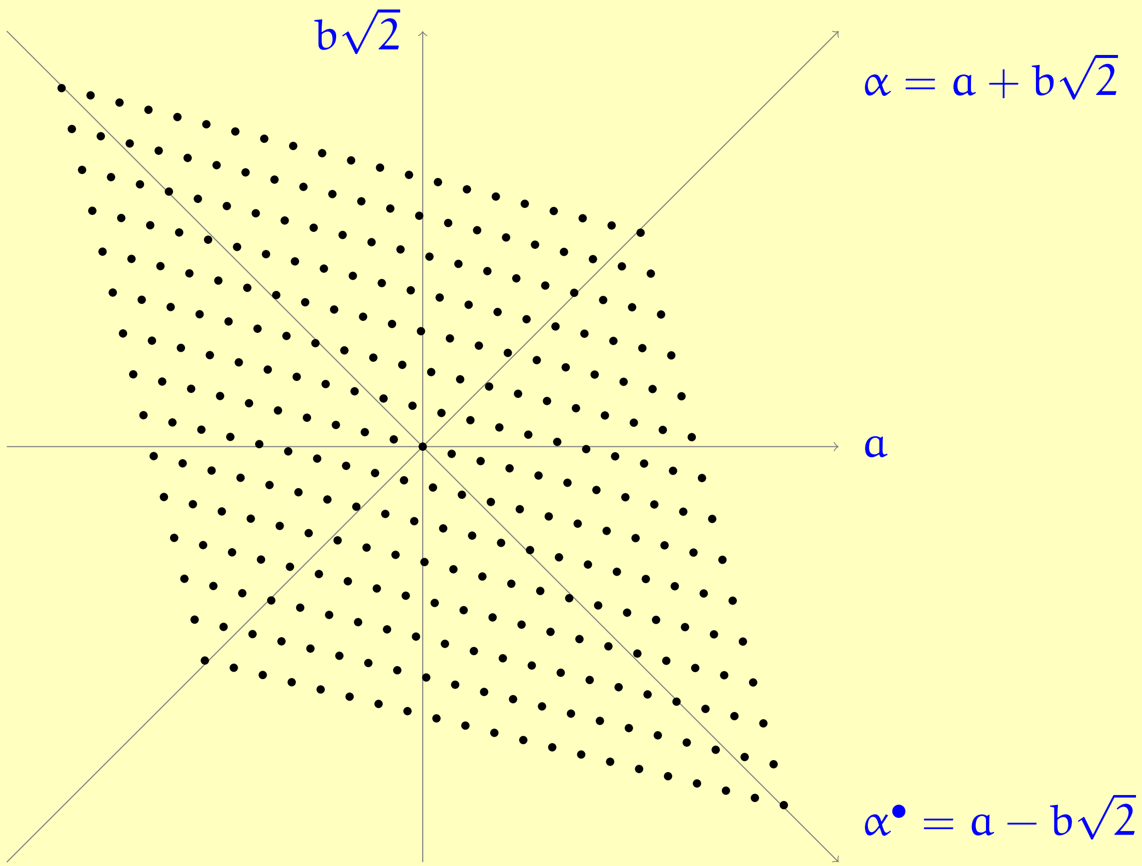
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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

Dense or discrete?

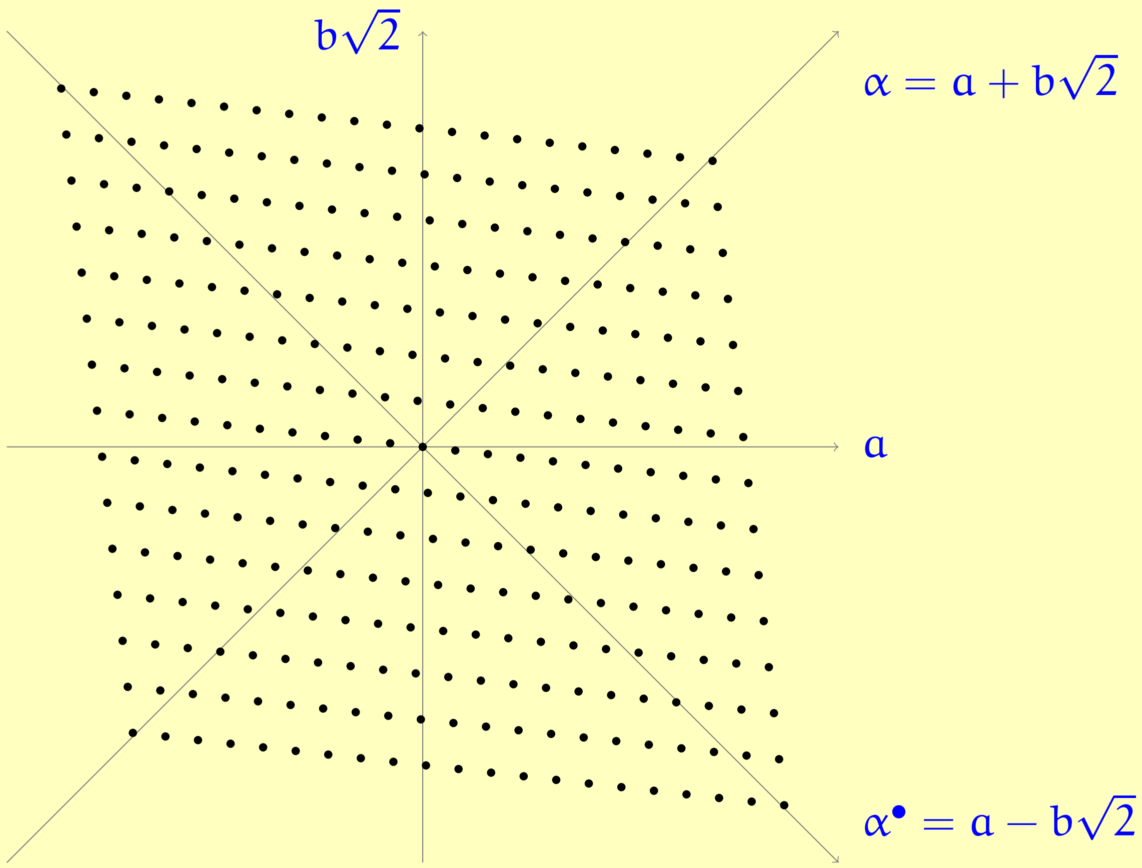
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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

Dense or discrete?

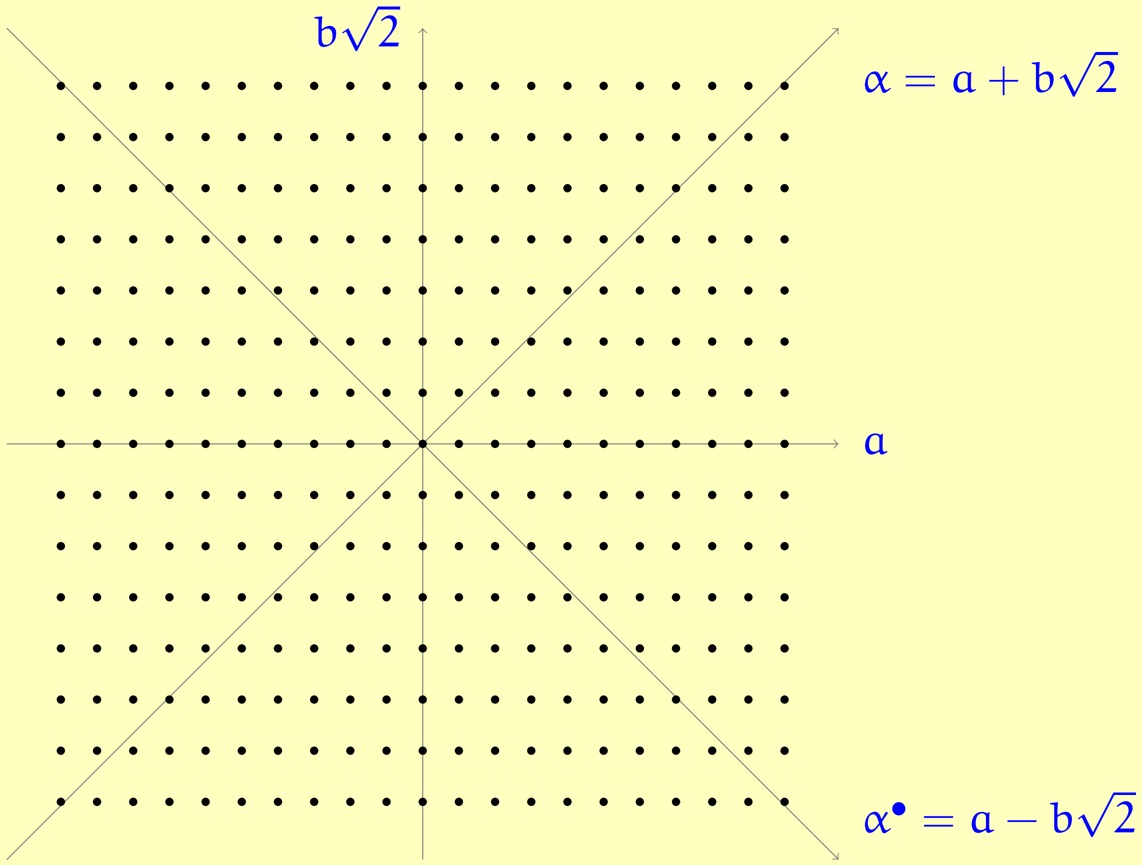
The ring $\mathbb{Z}[\sqrt{2}]$ is *dense* in the real numbers.



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.

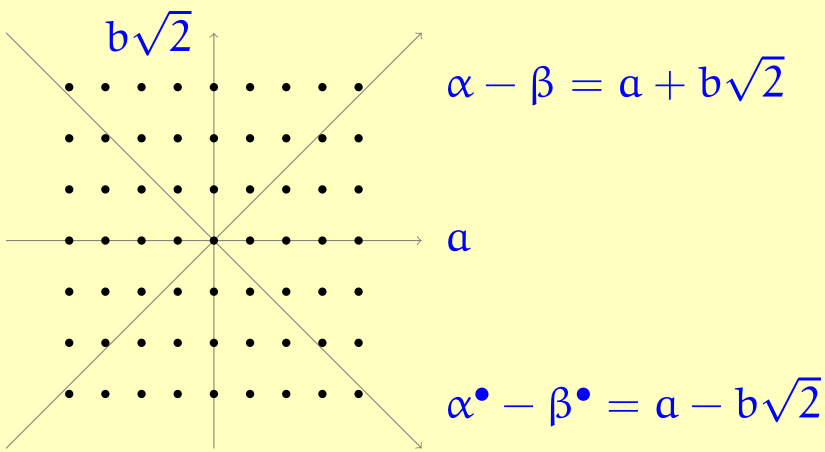


But it is better to think of $\mathbb{Z}[\sqrt{2}]$ as *discrete*.

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 $\alpha = \beta$).

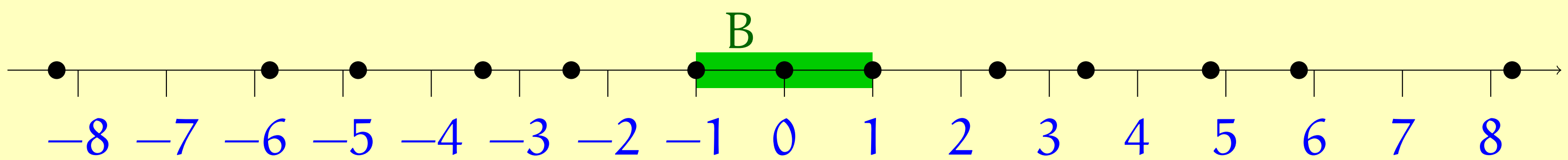
Proof: let $\alpha - \beta = a + b\sqrt{2}$. Then $|\alpha - \beta| \cdot |\alpha^\bullet - \beta^\bullet| = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$, which is an integer.



1-dimensional grid problems

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

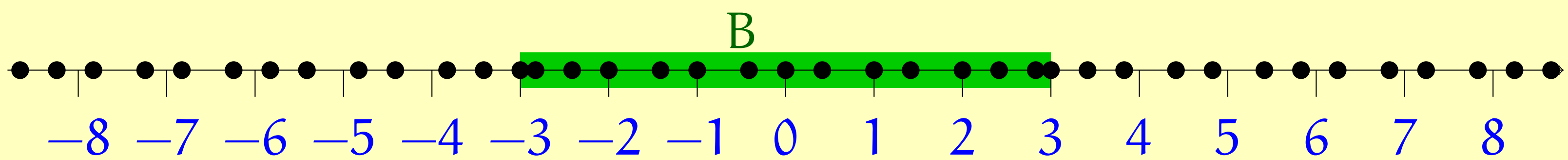
$$\mathrm{grid}(B) = \{\alpha \in \mathbb{Z}[\sqrt{2}] \mid \alpha^{\bullet} \in B\}.$$



1-dimensional grid problems

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

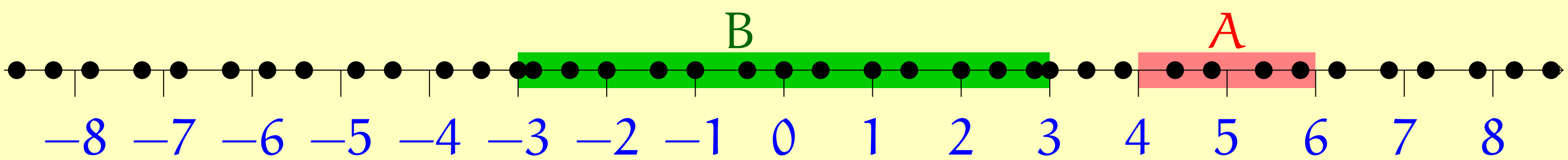
$$\mathrm{grid}(B) = \{\alpha \in \mathbb{Z}[\sqrt{2}] \mid \alpha^{\bullet} \in B\}.$$



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

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

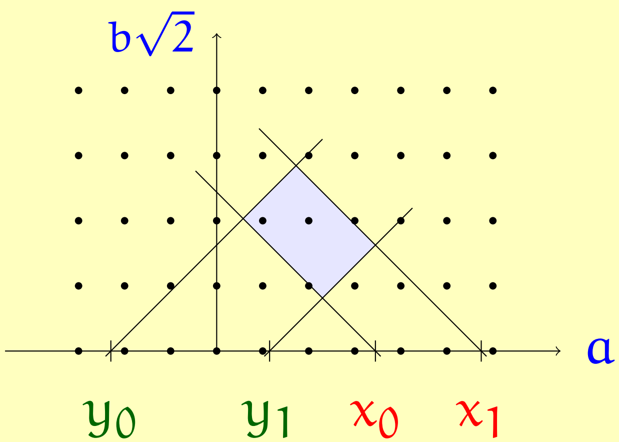
1-dimensional grid problems

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:

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

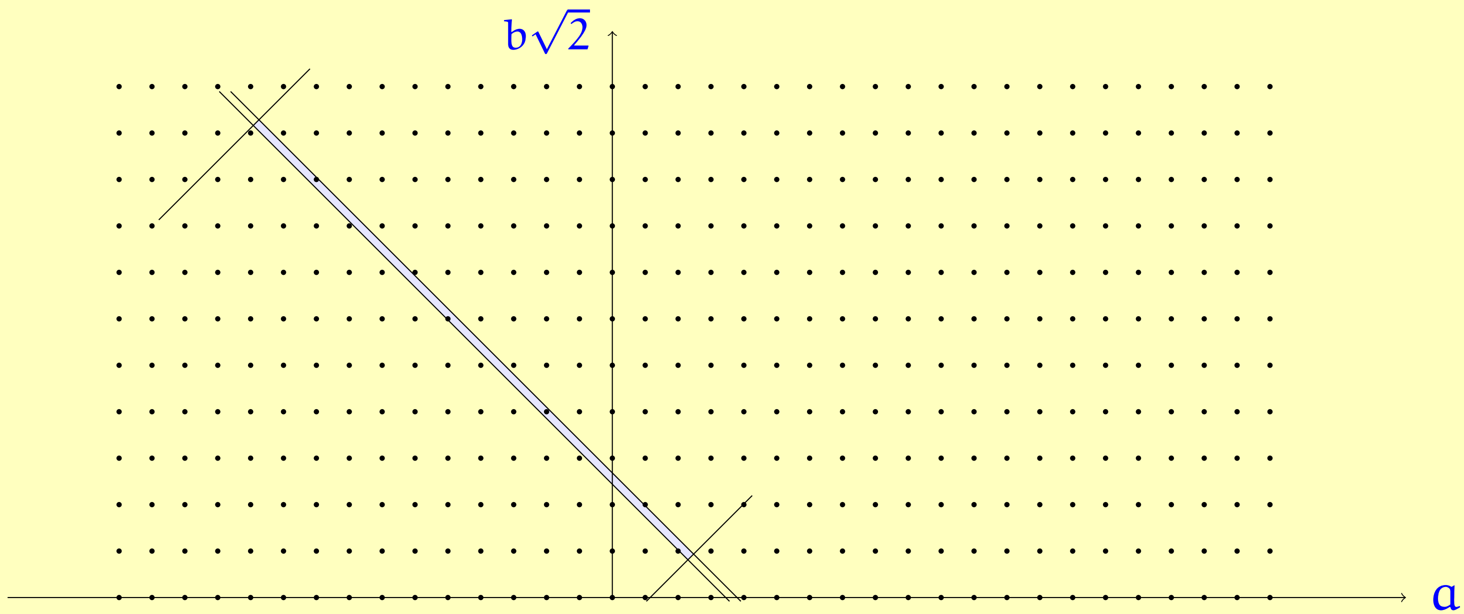


$A = [x0, x1], \quad B = [y0, y1]$

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.

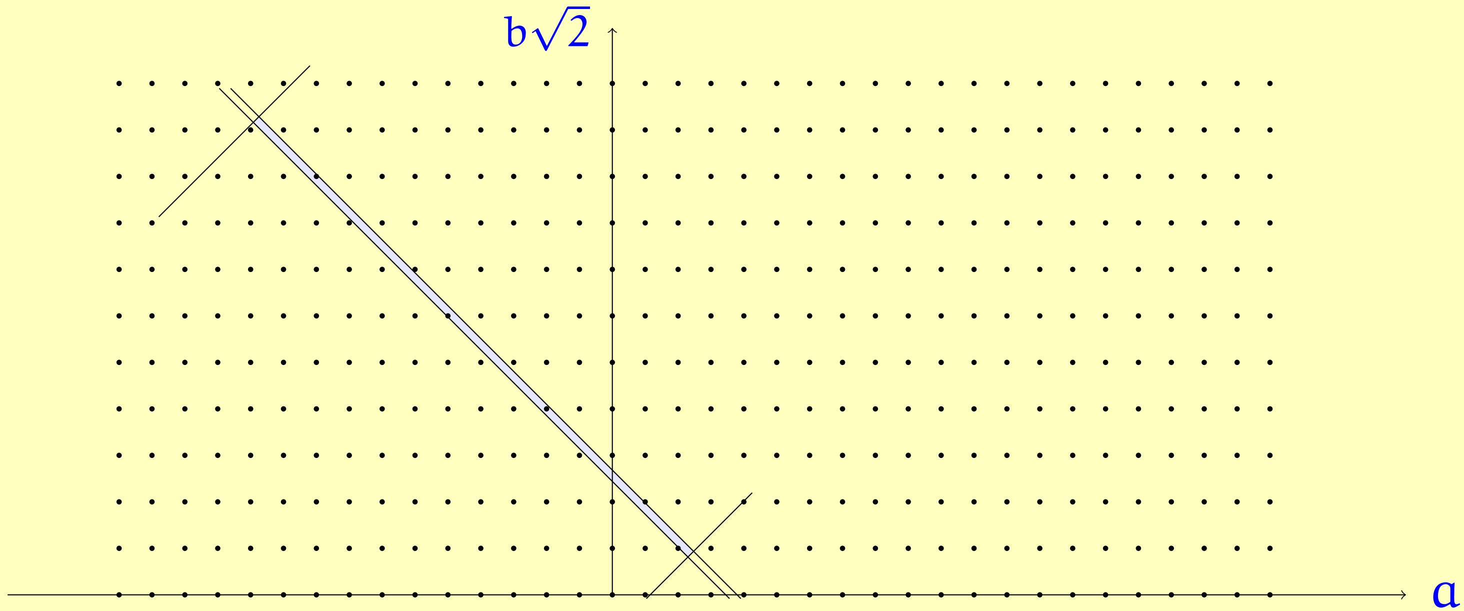
The problematic case: long and skinny

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

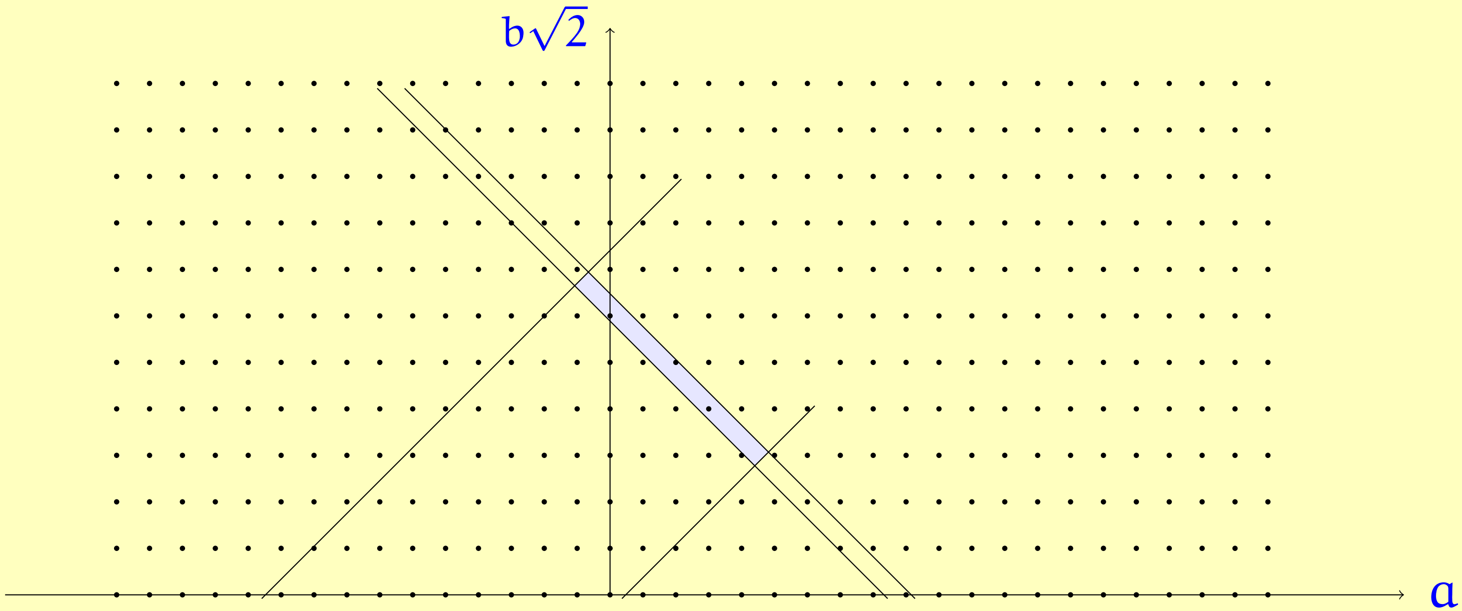
Suppose $|A|$ is tiny and $|B|$ is large, so that we end up with a long and skinny rectangle:



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

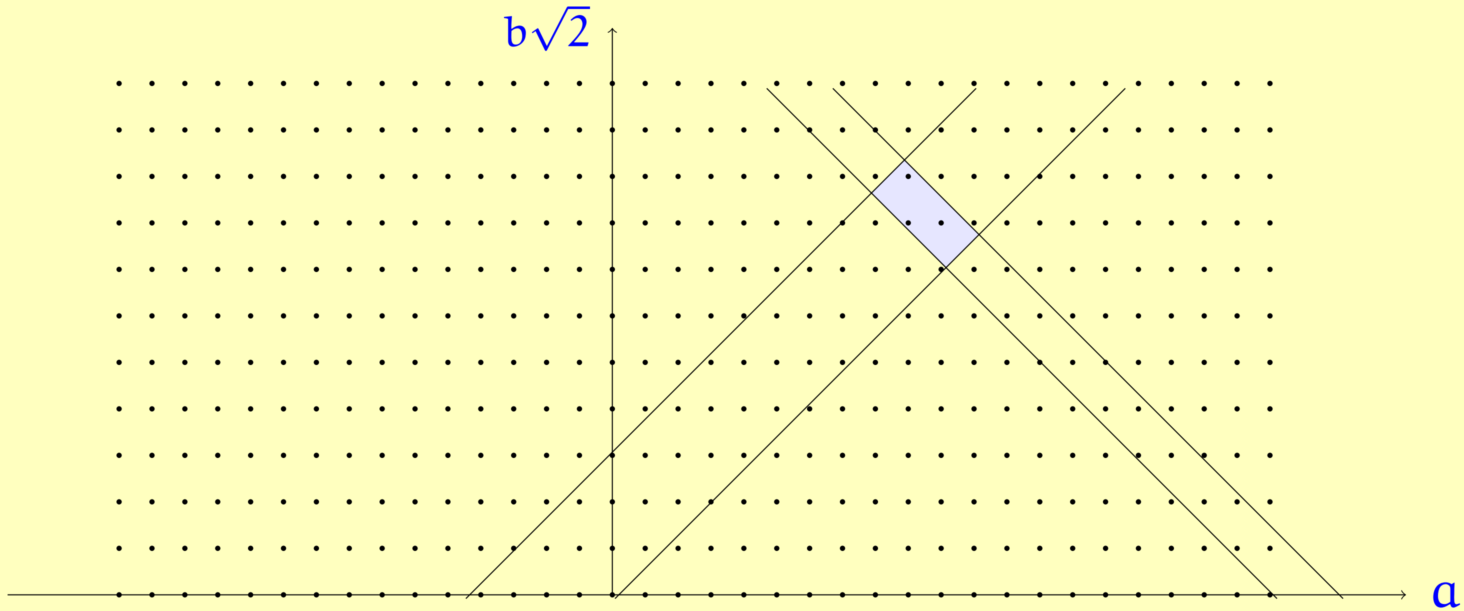
Suppose $|A|$ is tiny and $|B|$ is large, so that we end up with a long and skinny rectangle:



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

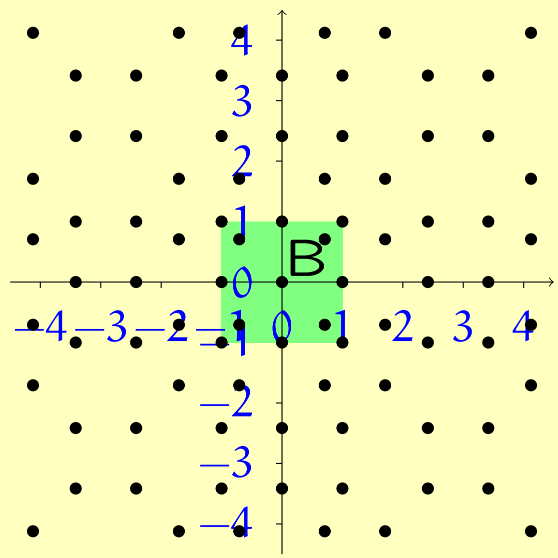
Theorem. Let A and B be finite real intervals. There exists an efficient algorithm that enumerates all solutions of the grid problem for A and B.

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

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

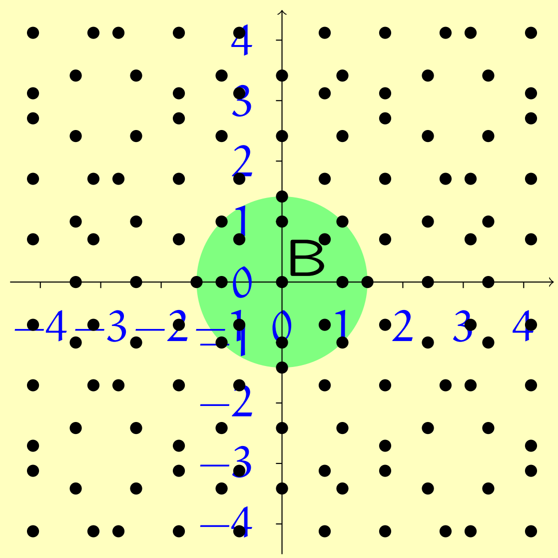


2-dimensional grid problems

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

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

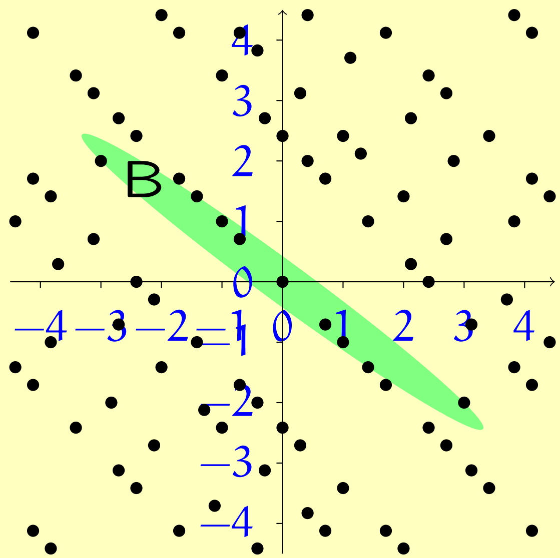


2-dimensional grid problems

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

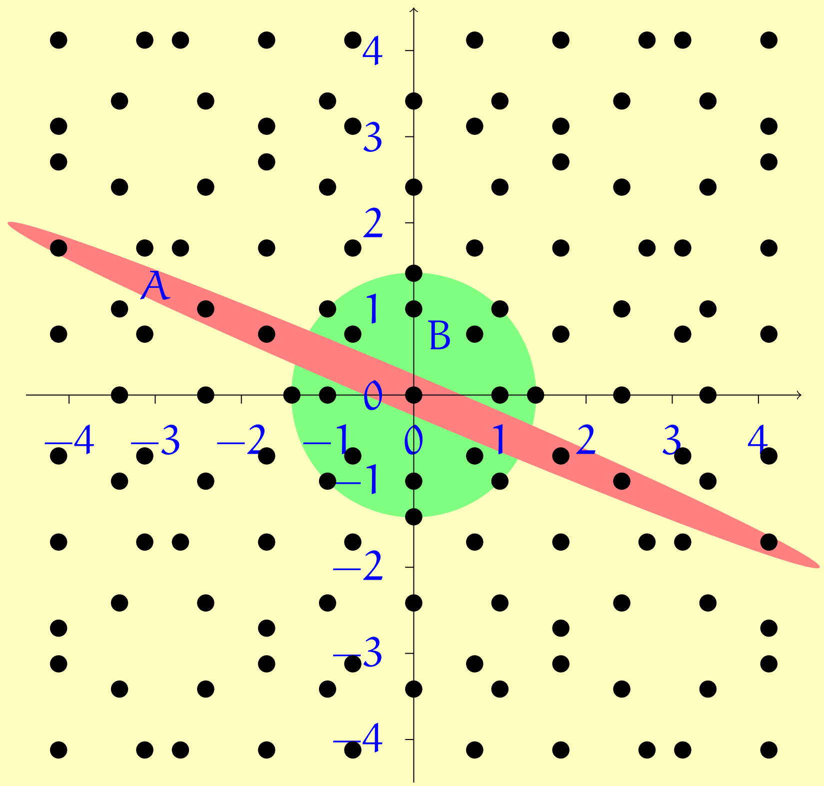
$$\text{grid}(B) = \{\alpha \in \mathbb{Z}[\omega] \mid \alpha^\bullet \in B\}.$$



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

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

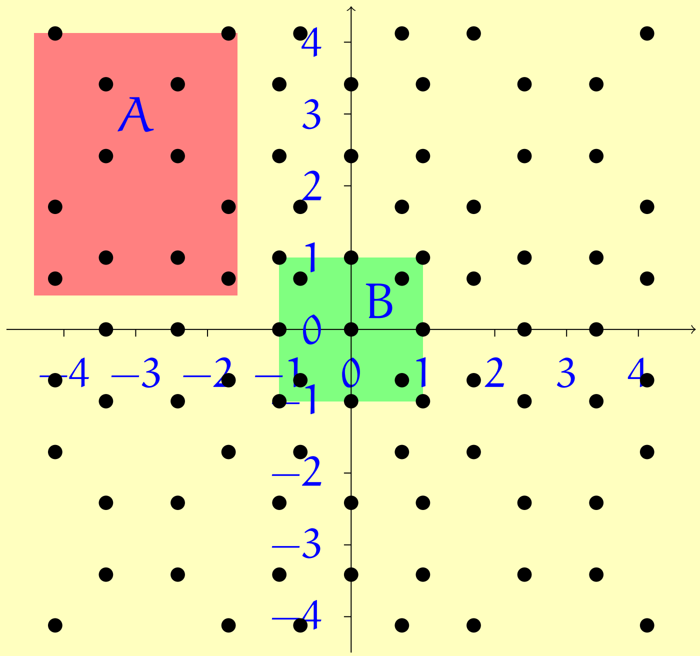


The easiest case: upright rectangles

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:

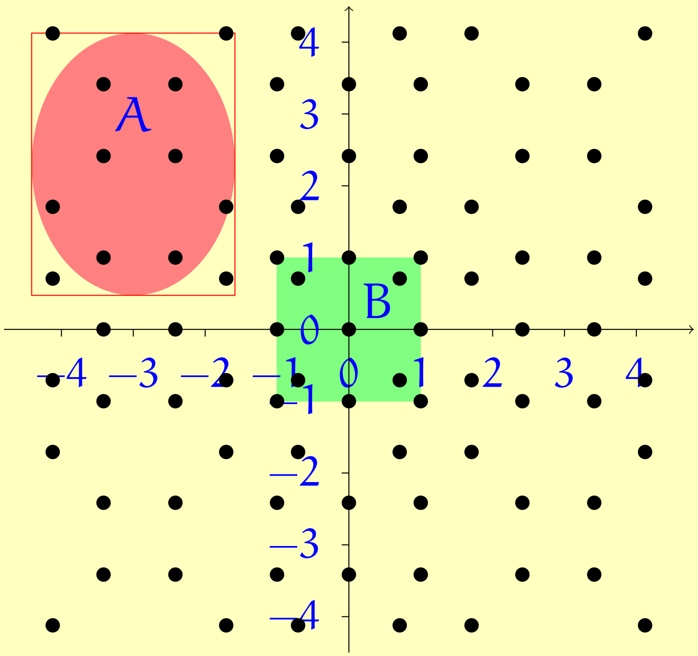
$$\alpha \in [x_0, x_1], \quad \alpha^\bullet \in [x'_0, x'1] \quad \text{and} \quad \beta \in [y_0, y_1], \quad \beta^\bullet \in [y'_0, y'_1],$$

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



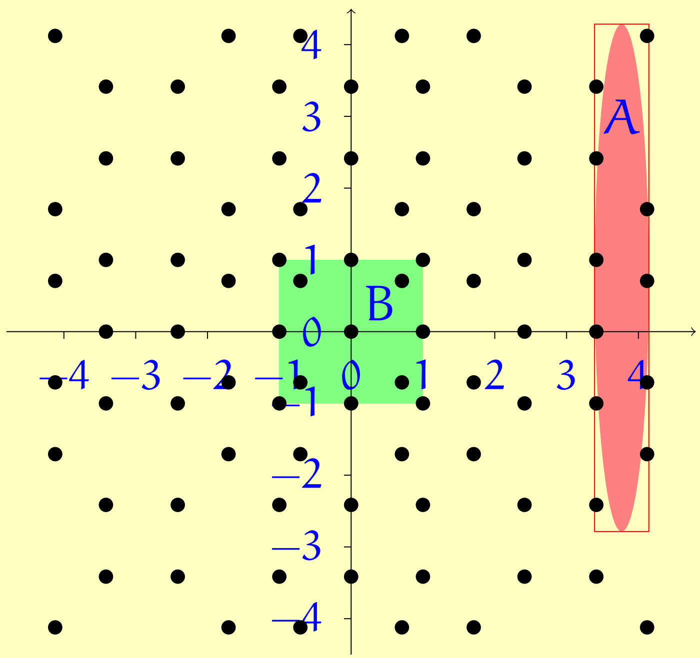
Also easy: upright sets

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.



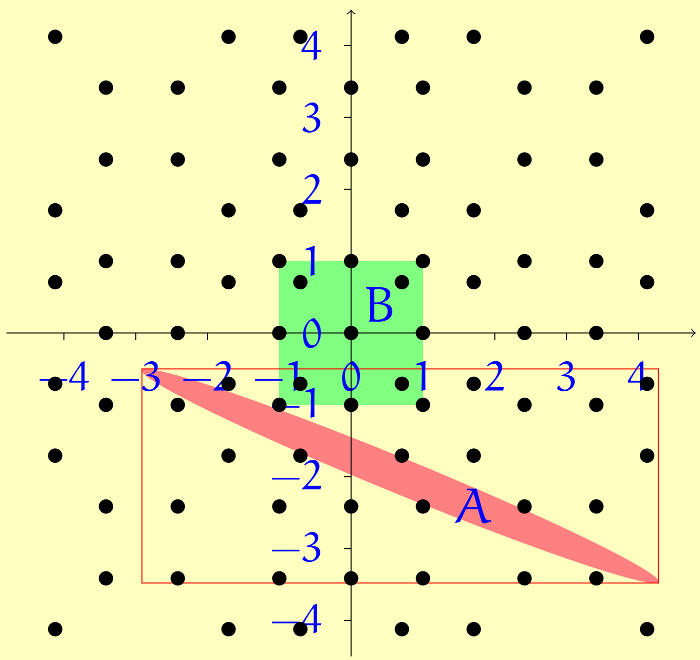
Also easy: upright sets

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:

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

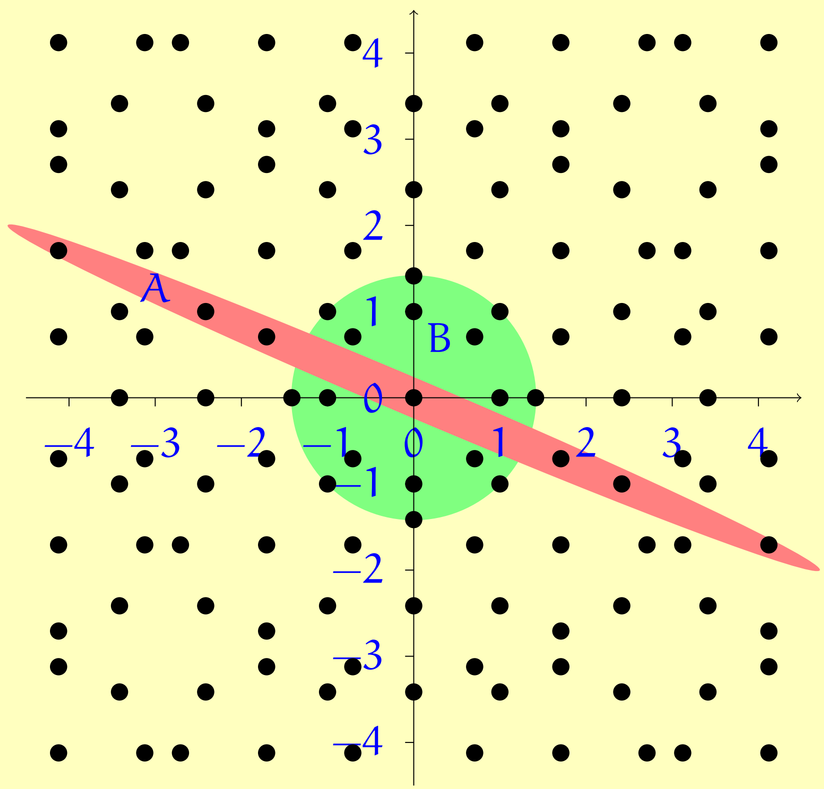
$$\mathbf{K} = \frac{1}{\sqrt{2}} \begin{bmatrix} -\lambda^{-1} & -1 \\ \lambda & 1 \end{bmatrix} \quad \mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

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 $G(\alpha)^\bullet \in G^\bullet(B)$.

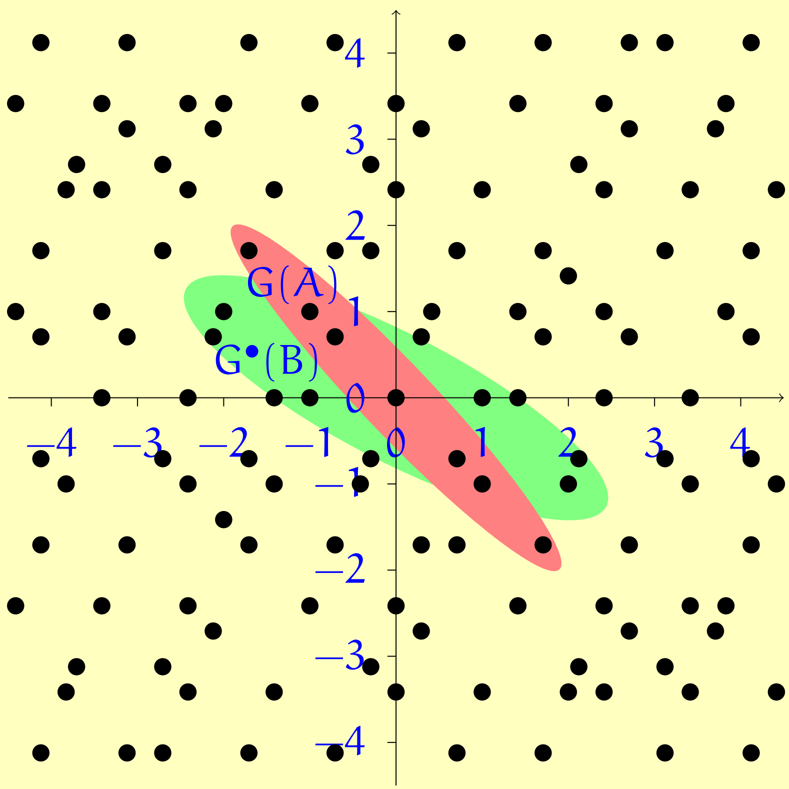
Effect of a grid operator

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



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 IV: 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:

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

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

Recall: normal form

Theorem. *Every Clifford+T operator can be uniquely written of the form*

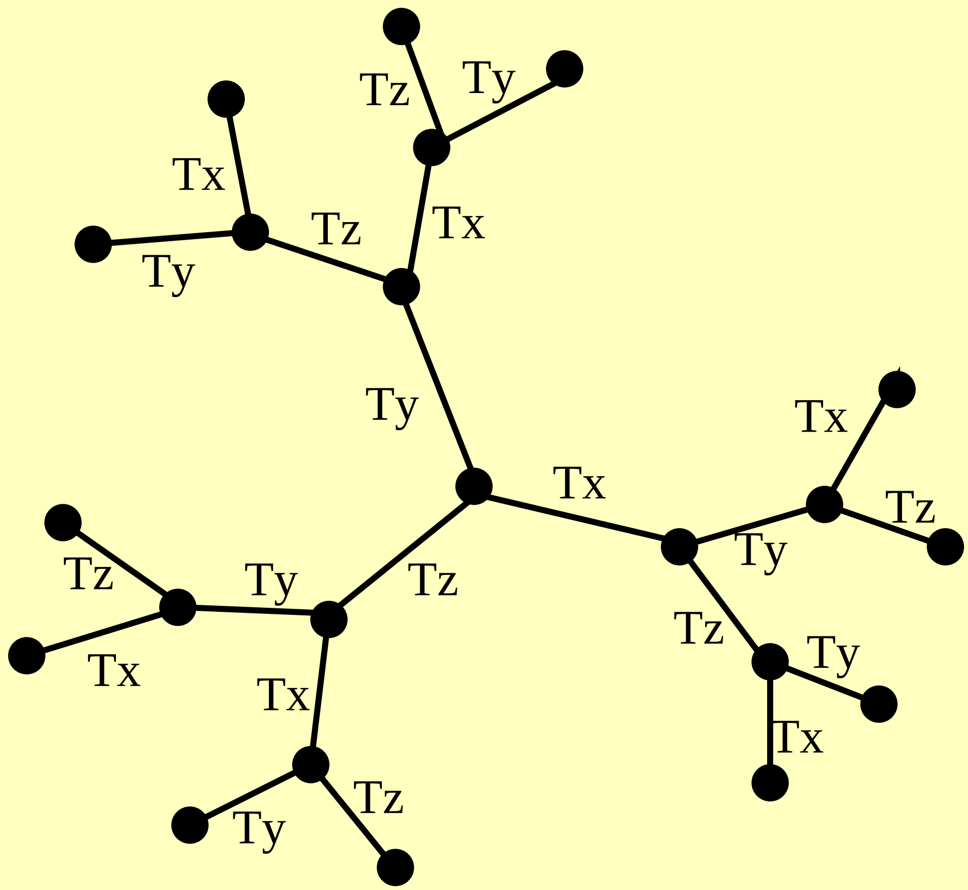
$$T_1\, T_2\, \ldots\, T_k\, C,$$

where each $T_i \in \{T_x, T_y, T_z\}$, $C \in \mathbb{C}_{90}$, *and no two consecutive* T_i*'s are equal.*

Example.

$$U = T_x\, T_z\, T_y\, T_z\, T_x\, T_z\, T_x\, T_z\;\; SSS\omega^7$$

We can measure the "length" of an operator U in terms of its T-count; for example, the above U has T-count 7.



Tz
Ty
Tx
Tx
Tz
Ty
Ty
Tx
Tx
Tz
Ty
Tz
Ty
Tz
Tz
Ty
Tx
Tx
Ty
Tx
Tz
Ty

Information-theoretic lower bound on the T-count

Corollary (Matsumoto and Amano 2008). *There are exactly* $192\cdot(3\cdot 2^n-2)$ *distinct single-qubit Clifford+T operators of T-count at most* n.

Corollary. *To approximate an arbitrary operator up to* ϵ *requires T-count at least* $K+3\log_2(1/\epsilon)$ *in the typical case.*

Proof. Since $SU(2)$ is a 3-dimensional real manifold, it requires $\Omega(1/\epsilon^3)$ epsilon-balls to cover. Let n be the T-count. Using Matsumoto and Amano's result, we have

$$192\cdot(3\cdot 2^n-2)\geq \frac{c}{\epsilon^3},$$

hence

$$n\geq K+3\log_2(1/\epsilon).$$

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.

$$\frac{1}{\sqrt{2}^5}\begin{pmatrix} -\omega^3 - \omega^2 + 4\omega & -2\omega^3 - 3\omega^2 + \omega \\ -\omega^3 + 3\omega^2 + 2\omega & 4\omega^3 - \omega^2 - \omega \end{pmatrix}$$

$$= T_x\, T_z\, T_y\, T_z\, T_x\, T_z\, T_x\, T_z\ SSS\omega^7$$

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

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

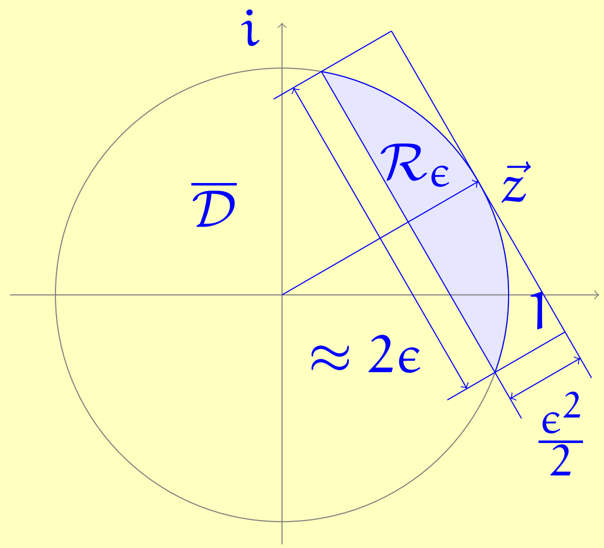
by a matrix of the form

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

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* $n = \xi^\bullet \xi$.

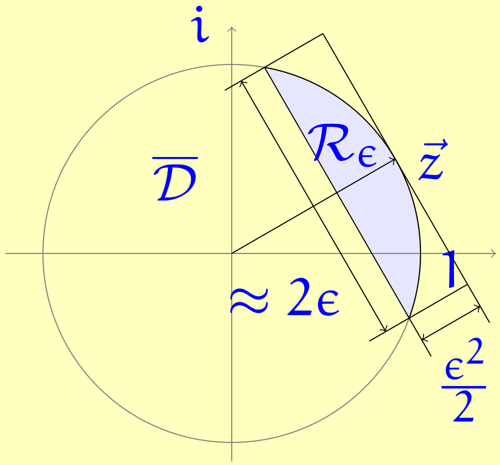
This is okay, because factoring random numbers is not as hard as worst-case numbers.

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.

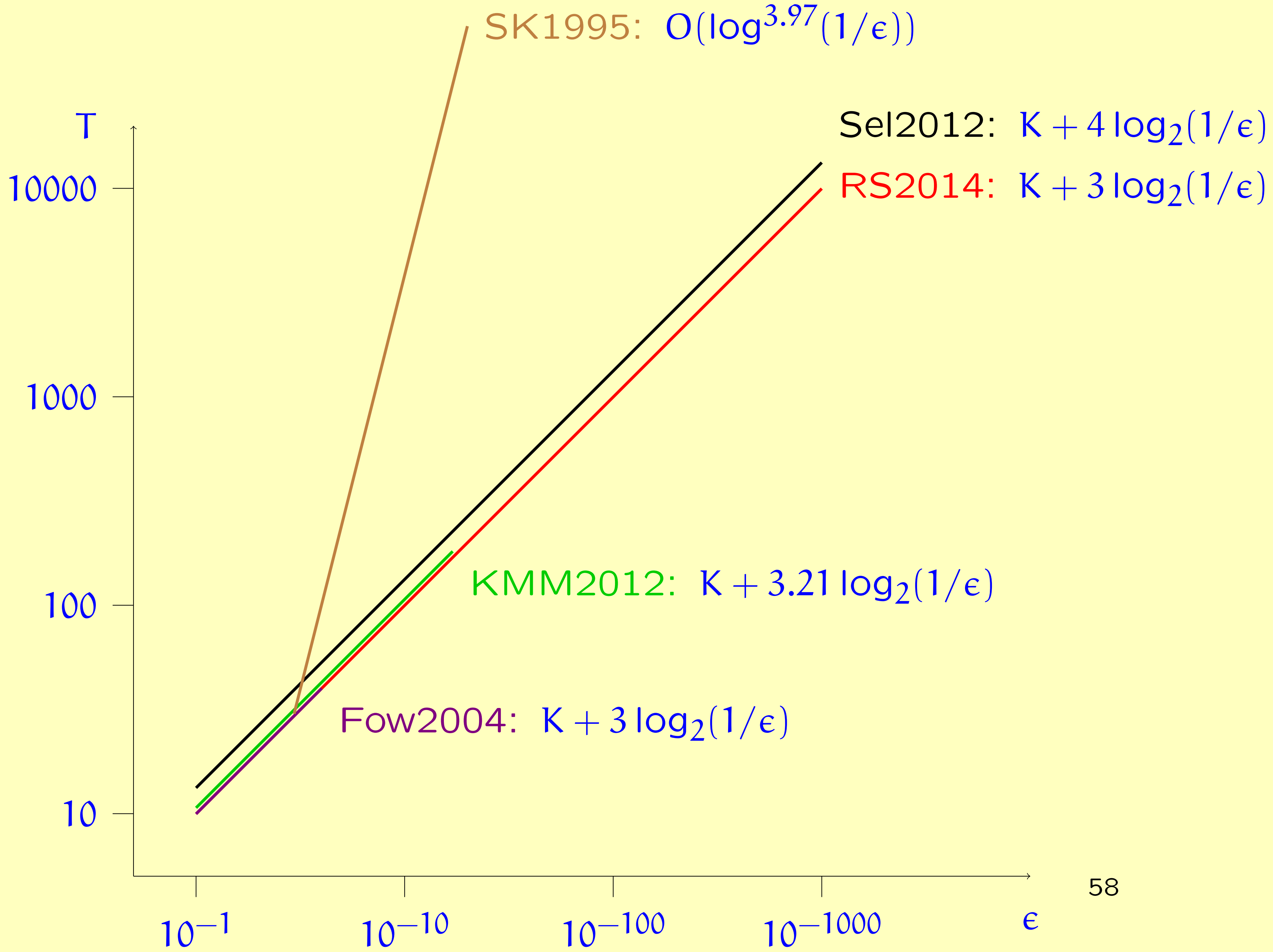
- In the absence of a factoring oracle, Algorithm 1 is *nearly optimal*: it yields T-counts of $m + O(\log(\log(1/\epsilon)))$, where m is the second-to-optimal T-count.

- 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

[Matsumoto and Amano 2008] K. Matsumoto and K. Amano. Representation of quantum circuits with Clifford and $\pi/8$ gates. arXiv:0806.3834, June 2008.

[Amy et al, 2012] M. Amy, D. Maslov, M. Mosca, and M. Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. arXiv:1206.0758, June 2012.

[Kliuchnikov et al. 2012a] V. Kliuchnikov, D. Maslov, and M. Mosca. Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates. arXiv:1206.5236v2, June 2012.

[Selinger 2012a] P. Selinger. Quantum circuits of T-depth one. *Physical Review A* 87, 042302, 2013. Available from arXiv:1210.0974.

[Giles and Selinger 2012] B. Giles and P. Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Physical Review A* 87, 032332, 2013. Available from arXiv:1212.0506.

[Kliuchnikov et al. 2012b] V. Kliuchnikov, D. Maslov, and M. Mosca. Asymptotically optimal approximation of single qubit unitaries by Clifford and t circuits using a constant number of ancillary qubits. arXiv:1212.0822, Dec. 2012.

[Selinger 2012b] P. Selinger. Efficient Clifford+T approximation of single-qubit operators. arXiv:1212.6253.

[Bocharov et al. 2013] A. Bocharov, Y. Gurevich, K. M. Svore. Efficient Decomposition of Single-Qubit Gates into V Basis Circuits. *Physical Review A* 88, 012303, 2013. Available from arXiv:1303.1411.

[Kliuchnikov 2013] V. Kliuchnikov, Synthesis of unitaries with Clifford+T circuits. arXiv:1306.3200, June 2013.

[Kliuchnikov et al. 2013] V. Kliuchnikov, A. Bocharov, K. M. Svore. Asymptotically Optimal Topological Quantum Compiling. arXiv:1310.4150, October 2013.

[Ross and Selinger 2014] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. arXiv:1403.2975, March 2014.