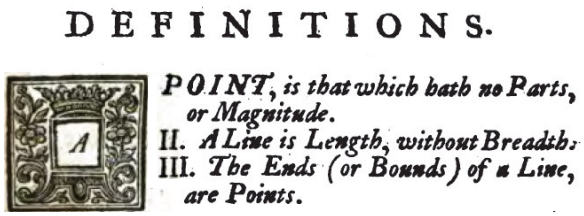
Baffling points

By Francisco Monteiro

What is the simplest and most fundamental geometric idea you can think of?
Euclid certainly asked himself this question when he was selecting and organising ideas to include in his *Elements* around 300 B.C. He had much to say and much to select from. Not only his own findings but also what generations of mathematicians had already discovered until then. His major work had to start with definitions. And for the first line of the first page, Euclid chose the definition of a point.


DEFINITIONS.

A POINT, is that which hath no Parts, or Magnitude.
II. A Line is Length, without Breadth.
III. The Ends (or Bounds) of a Line, are Points.

First lines from Euclid's Elements.

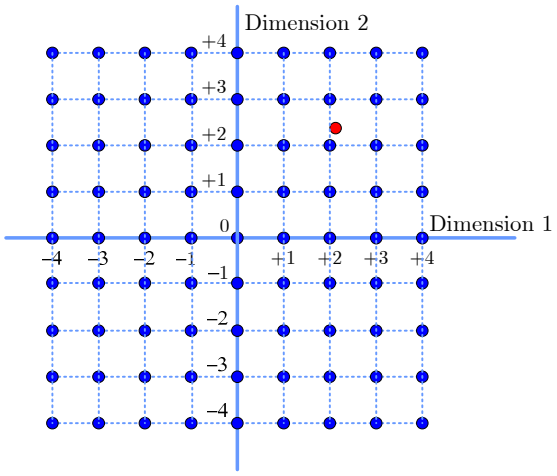
Whether simple or not, new ideas may ignite creative processes one day, even centuries after, which may be at the core of a technology that will dramatically change the world. I am going to tell you of a succession of simple ideas regarding regular structures of points, ideas whose applications would be unthinkable to their authors, and that now lie at the heart of the most advanced communication technologies, which shape our information age.

Seriously!

Consider an infinite collection of uniformly spaced blue points over a line. If you are given a random red location on the line, I bet you can you tell which blue point is the closest one to the red point.

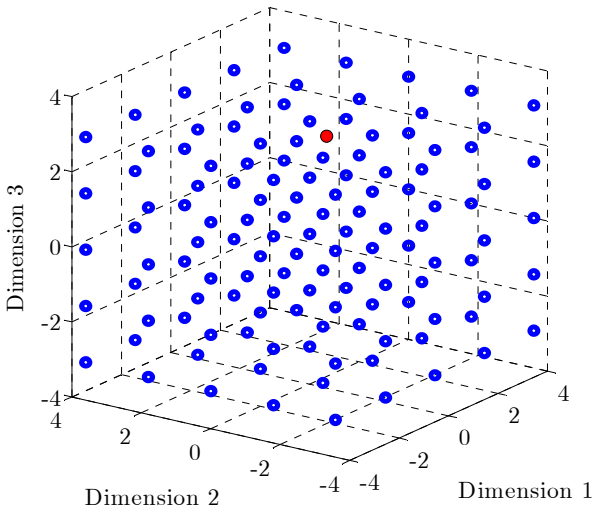
Which blue point is closest to the red one?

It is simple to devise an extension of this problem to an infinite regular grid of points. Can you still identify which blue point is the closest one to a given red point in the plane?



Which blue point is closed to the red one?

Finally, and without difficulty, you can already imagine an extension of this problem to the 3-dimensional space we live in, and imagine an infinite and uniform structure of points. It would be more difficult, but looking from more than one point of view, we would all still be able to identify the correct blue point.



Which blue point is closed to the red one?

Dreaming in many dimensions

One way to represent each point in any of these problems came to the mind of René Descartes (1596-1650) in a dream he had, as he claimed. The idea is to use a set of real numbers, each one indicating the coordinate along each dimension.

$$\underbrace{(x_1, x_2, x_3, x_4, x_5, \cdots, x_n)}_{n \text{ coordinates}}$$

Why should we limit ourselves to 3 dimensions only? Our representation tool can deal with more dimensions despite the limitations of the physical universe we can perceive. Indeed, we can represent as many dimensions as we want.

If this concept does not seem yet very useful to the reader, it should be comforting to know that it was not either for many years among the most prominent mathematicians.

David Eugene Smith (1860–1944) was a mathematician and an avid collector of original material written by the best mathematicians. In 1929 he published a compilation of texts on important mathematical topics written between the 15^{h} and the 19th centuries. Surprised, he found that:

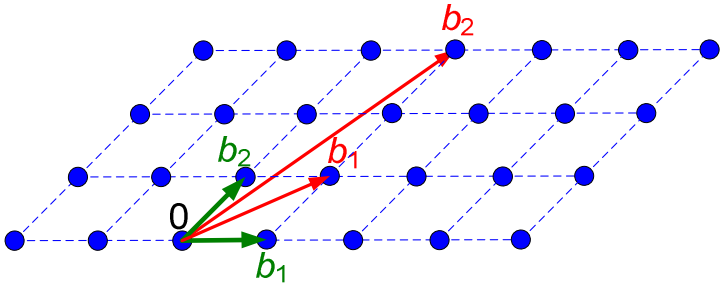
"All references to a geometry of more than three dimensions before 1827 are in the form of single sentences pointing out that we cannot go beyond a certain point in some process because there is no space of more than three dimensions, or mentioning something that would be true if there was such a space."

But by 1884 we would all be more receptive to the concept of worlds with a larger number of dimensions. Edwin Abbott (1838-1926) had published the best seller "Flatland", and stimulated the imaginations of generations of readers with his story of a 2-dimension universe, whose members are oblivious to an intangible third dimension, which is revealed in the dreams of one the inhabitants of that world.
In 1902 the French mathematician Henri Poincaré (1854-1912) in his "Science and Hypothesis" asked his readers to perceive an object living in four dimensions as a succession of 3 dimensional observations, as if we were turning around the fourth dimension.

Our experience of the world is constrained, but mathematical reasoning leads even where we cannot see. With clear rules, as we did from 1 to 2 and 3 dimensions, we can similarly generalise the original problem to any number of dimensions.

Dull universe, interesting problems

The regular arrangements of points that we have imagined are called lattices. They are infinite and so regular that in a lattice universe any observer sitting on any of the points would always see the same stellar sky.
A lattice may be defined by a set of generating vectors (a basis). Each point in the lattice is specified by a certain combination of those vectors. It's simple to see that any blue point can be obtained by adding multiples of the green basis.

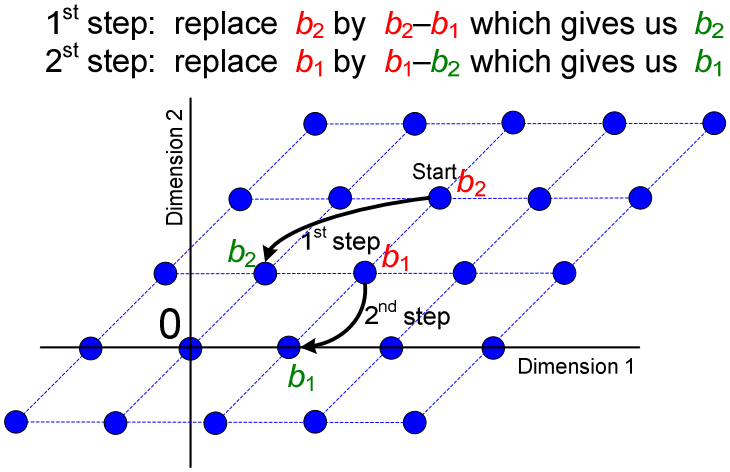


A good basis (green) and a bad basis (red) for a lattice in 2D.

Other sets of vectors may generate exactly the same arrangement of points. Actually, the number of possible basis is infinite. Check yourself that combinations

of the red vectors also generate the same lattice! You would agree that the green basis seems "nicer" than the red basis: the vectors are shorter and the angle between them is closer to 90 degrees.

In 1801 Gauss published an algorithm to convert a bad basis into the nicest one possible for the case of lattices in 2D. His algorithm is rooted in the idea of keep subtracting the shorter vector from the larger, while observing some rules regarding the angles of the parallelogram they form at each step.



Example of Gauss' method to obtain a good basis for a 2D lattice, starting from a given bad basis.

But our problems are just starting, as we do not even have a unique representation for the structure, and we have not even considered yet that any rotation of the structure of points would surely preserve the structure of the lattice. Indeed, there is an infinite number of ways of describing the same lattice.

"The curse of dimensionality"

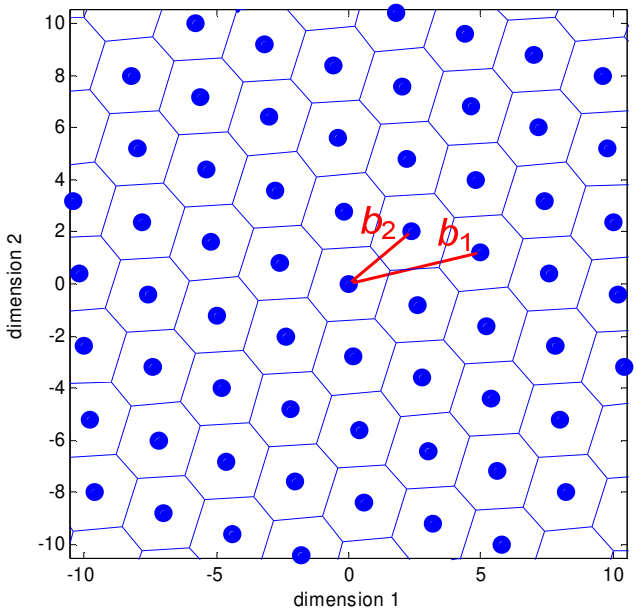
In spaces with many dimensions our geometrical intuition completely fails to grasp the surprising results achieved by rigorous calculations. For instance, volumes easily become so large that a variable depending on a volume of the space can grow to unmanageable numbers of the order of the number of stars in the universe. This was dubbed by the mathematician Richard E. Bellman (1920-1984) "the curse of dimensionality". Playing *Where's Wally?* in several dimensions would be maddening!

Imagine a cookie-cutter limiting an infinite lattice to a finite region. Extend this scene to cookie-cutters and lattices with increasing number of dimensions. If in 1D we counted 9 points, in 2D we would have 9x9=81 and 9x9x9=729 points in 3D. An hyper-dimensional cookie-cuter in 8 dimensions would capture 9^8 = 43,046,721 points!

In orthogonal lattices the task is easier, but in the general case finding the closest point involves measuring the distance from the given location to each one of members of the lattice. Even in "just" 8 dimensions, the task is intimidating. In 500,

it is deemed so hard that the problem can be used as a cryptographic tool even against attackers using the most powerful computers.

The correct solution to our problem is geometrically defined by the Voronoy cell, which encapsulates the space that is closer to a lattice point than to any other point. This concept was first formulated by Georgy Voronoy (1868-1908), and was only published on the year of his death.



Voronoy cells of a lattice in 2D.

This problem arises, for instance, in digital communications. If we want to keep real time communications, the problem needs to be solved in a microsecond. Without a quantum computer in every electronic device, a clever idea is needed for this job, and having a nice basis for the lattice is of paramount importance.

The L's in the lattice story

In 1982 three mathematicians, the two brothers Arjen Lenstra and Hendrik Lenstra, and László Lovász found an algorithm that has become famous a"LLL". They found the recipe to get a remarkably nice basis with short and almost orthogonal vectors. Other techniques existed for that purpose. However, their breakthrough allows us to find a basis with an algorithm whose complexity scales not exponentially, but only as a polynomial function of the number of dimensions.
They were able to find an extension of the Gaussian algorithm for lattices with any number of dimensions. Today, we understand that the Gaussian algorithm is an instance of the LLL algorithm and that even the Euclidean algorithm to find the Greatest Common Divisor of natural numbers, also published in his "Elements", is an instance of the Gaussian algorithm.

Arjen Lenstra, Hendrik Lenstra and László Lovász

The discovery of LLL opened doors to finding solutions for numerous problems that can be translated into the language of lattices. In 2007 a conference was organised to celebrate the 25th anniversary of their discovery, and unforeseen applications keep coming up. The new generations of wireless broadband digital communications will employ it, and are actually dependent on lattice in multi-dimensional spaces. If only Euclid would know!

Bibliography

Edwin A. Abbot, Flatland. London, UK: Penguin Classics, 1998, (first edition in Great Britain in 1884 by Seeley & Co).

Erik Agrell, Alexander Vardy Thomas Eriksoon, and Kenneth Zeger, "Closest point in lattices," IEEE Transactions on Information Theory, vol. 48, no. 8, pp. 2201-2214, August 2002.

Tomaso Aste and Denis Weaire, "Packings and kisses in high dimensions," in The Persuit of the Perfect Packing. Bristol, UK: Institute of Physics Publishing, 2000, pp. 113-118.

Christopher M. Bishop, "The curse of dimensionality," in Pattern Recognition and Machine Learning. New York, NY: Springer, 2006, ch. 1.4, pp. 33-38.

J. W. S. Cassels, An Introduction to the Geometry of Numbers, 2nd ed. Berlin, Germany: Springer, 1971.

Henri Cohen, "Algorithms for Linear Algebra and Lattices," in A Course in Computational Algebraic Number Theory. Berlin, Germany: Springer, 1995, ch. 2.

J. H Conway and N. J. A. Sloane, Sphere Packings, Lattices and Groups, 3rd ed. New York, NY: Springer, 1999.

Keith Devlin, Mathematics - The New Golden Age. New Yourk, NY: Columbia Univesity Press, 1999, pp. 9, 12, 23, 212.

Keith Devlin, "When Computers Fail - The P vs NP Problem," in The Millennium Problems. London, UK: Granta Books, 2002, ch. 3, pp. 105-129.

Marcus du Sautoy, The Music of the Primes. London, UK: Harper Perennial, 2003, (References to Arjen

Lenstra and Hendrik Lenstra).

Euclid, Elements. London, UK, 1723, (PDF file from Google Books; book in public domain).

Joachim von zur Gathen and Jürgen Gerhard, "Short vectors in lattices," in Modern Computer Algebra. Cambridge, UK: Cambridge University Press, 2003, ch. 16, pp. 461-475.

Carl F. Gauss, Disquisitiones Arithmeticae. Leipzig, Germany, 1801.

Timothy Gowers, "Dimension," in Mathematics - a Very Short Introduction. Oxford, UK: Oxford University Press, 2002, ch. 5, pp. 70-85.

Harold R. Jacobs, "Mathematical Mosaics," in Mathematics - a Human Endeavor. San Francisco, California: W. H. Freeman and Company, 1970.

Arnold R. Krommer and Christoph W. Ueberhuber,. Philadelphia, PA: Society for Industrial and Applied Mathematics (SIAM), 1998, pp. 213-233.

Hendrik W. Lenstra, "Lattices," in Algorithmic Number Theory, J. P. Buhler and P. Stevenhagen, Eds. Cambridge, UK: Cambridge University Press, 2008, pp. 127-181.

László Lovász, An Algorithmic Theory of Numbers, Graphs and Convexity. Philadelphia, Pennsylvania, USA: Society for Industrial and Applied Mathematics (SIAM), 1986, ch. 1, pp. 15-38.

Daniele Micciancio, "Shortest vector problem," in Encyclopedia of Algorithms, Ming-Yang Kao, Ed. Berlin, Germany: Springer, 2008, pp. 841-843.

Daniele Micciancio and Shafi Goldwassel, Complexity of Lattice Problems - A Cryptographic Perspective. Norwell, MA: Kluwer Academic Publishers, 2002.

Wai Ho Mow, "Universal lattice decoding: principles and recent advances," Wireless Communications and Mobile Computing, vol. 3, pp. 553-569, March 2003.

Phong Q. Nguyen and Daniele Micciancio, "Entries on Lattice, Shortest Vector Problem, Closest Vector Problem, and Lattice Based Cryptography," in Encyclopedia of Cryptography and Security, Henk C. A. van Tilborg, Ed. New York, NY: Springer, 2005, pp. 345-349.

Ivars Peterson, Islands of Truth. New York, NY: W. H. Freeman and Company, 1990, pp. 96-103.

Michael E. Pohst, "Topics from the geometry of numbers," in Computational Algebraic Number Theory. Basel, Switzerland: Birkhäuser, 1993, ch. 3.

Henri Poincaré, "Space and Geometry," in Science and Hypothesis. Mineola, NY, USA: Courier Dover Publications, 2003, ch. 4, pp. 68-70, (Dover edition, first published in 1952, is an unabridged republication of the first English translation published in 1905 by the Walter Scott Publishing Company).

C. P. Schnorr and M. Euchner, "Lattice basis reduction: improved practical algorithms and solving subset sum problems," Mathematical Programming, vol. 66, pp. 191-199, 1994.

Alexandre Schrijver, Theory of Linear and Integer Programming.: John Wiley & Sons, 1986, ch. 4, 5, 6.

Carl Ludwig Siegel, Lectures on the Geometry of Numbers. Berlin, Germany: Springer, 1989.

Ian H. Sloan and Stephen Joe, Lattice Methods for Multiple Integration. Oxford, UK: Oxford University Press, 1994.

David Eugene Smith, A Source Book in Mathematics. Mineola, NY, 1984, p. 524, (the Dover edition, first published in 1959, is unabridged republication of the first edition, originally published in 1929 by McGraw-Hill, NY).

Ian Stewart and David Tall, Algebraic Number Theory, 2nd ed. London, UK: Chapman & Hall, 1987, ch. 6.

B. L. van der Waerden, Geometry and Algebra in Ancient Civilizations. Berlin, Germany: Springer, 1983.

Dominic Welsh, "Computational Complexity," in Codes and Cryptography. Oxford, UK: Oxford University Press, 1988, ch. 9, pp. 143-148.

Additional URLs:

- Conference LLL +25: http://lll25.info.unicaen.fr/
- Chris Budd , "How maths can make you rich and famous", + *Plus Magazine*, Issue 24, March 2003: http://plus.maths.org/issue24/features/budd/index.html
- On the life of David Eugene Smith:
  http://education.stateuniversity.com/pages/2424/Smith-David-Eugene-1860-1944.html
  On the life of Georgy Fedoseevich Voronoy:
  http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Voronoy.html
- On the live of Charles Hermite (though not mentioned in the article):
  http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Hermite.html
- On the life of Hermann Minkowski (though not mentioned in the article):
  http://www-history.mcs.st-andrews.ac.uk/Biographies/Minkowski.html

Photos:

- Arjen Lenstra: photo available in Wikipedia and in in prof. Lenstra´s homepage http://people.epfl.ch/arjen.lenstra
- Hendrik Lenstra: from a online Press Release of the Royal Netherlands Academy of Arts and Sciences in http://www.knaw.nl/cfdata/news/pressrelease_detail.cfm?nieuws__id=492
- László Lovász, available from Prof. Lovász webpage http://www.cs.elte.hu/~lovasz/ . Several other photos available in the Wikipedia collection.

Images:

Created by the author using *Matlab* and *Visio* except the extract from Euclid's Elements extracted from book in public domain (as stated in the bibliography) and slightly improved in Visio.

The body text of this article is within 1,500 words, including the captions.