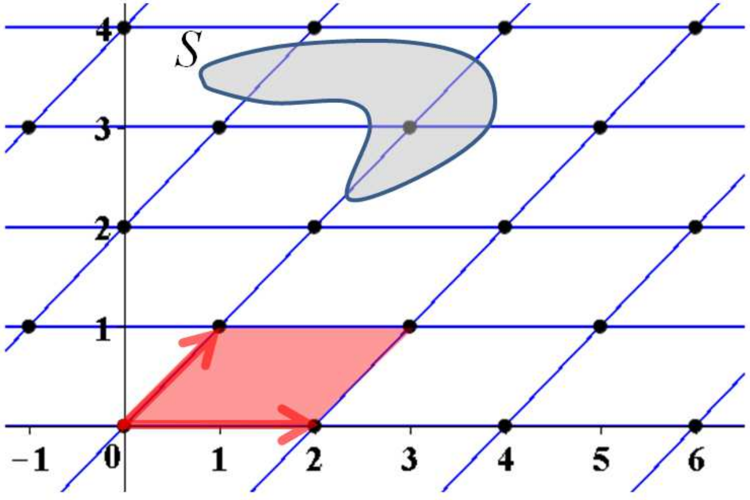
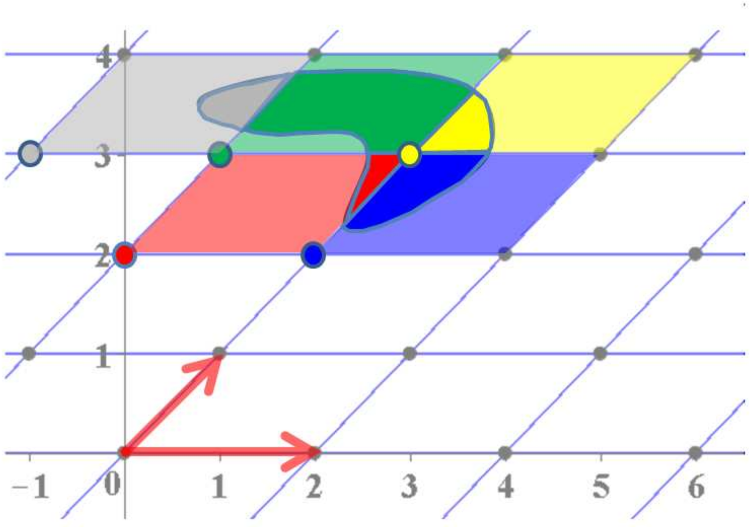
THEOREM OF THE DAY

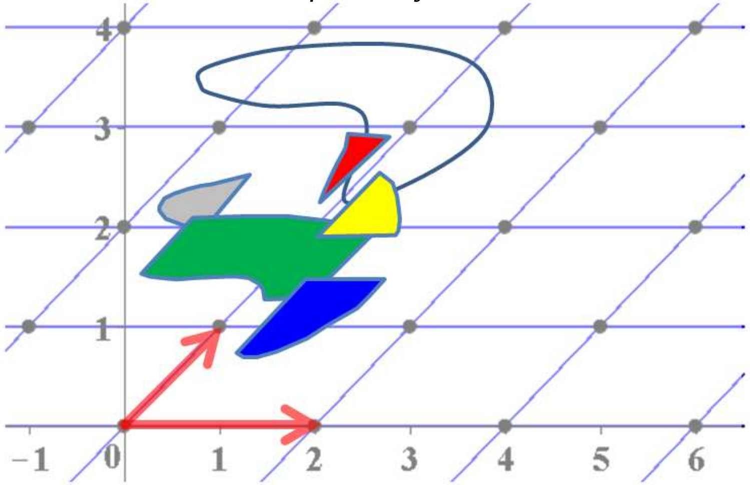
Minkowski's Convex Body Theorem *Let* $L(B) = \{Bx \mid x \in \mathbb{Z}^n\}$ *be the integer lattice whose points are all integer-weighted sums of the n linearly independent basis vectors forming B, an* $n \times n$ *matrix over* $\mathbb{R}$. *Let S be a convex subset of* $\mathbb{R}^n$, *closed under negation, whose volume exceeds* $2^n|\det(B)|$. *Then S contains a nonzero point of* $L(B)$.



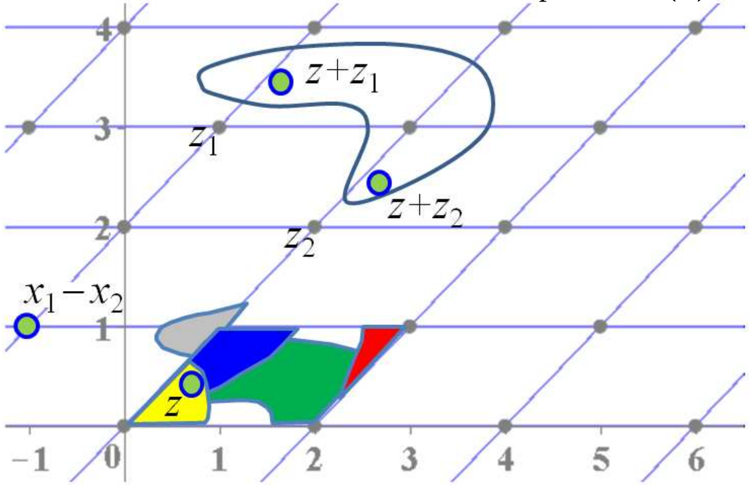
The lattice on the left consists of all points (x, y) where x and y are integers summing to an even number; it is defined by the two column vectors $(1, 1)$ and $(2, 0)$. The shaded parallelogram defined by these two basis vectors is called the *fundamental parallelepiped*, denoted $P(B)$, and its volume (which, in two dimensions is just area) is synonymous with $|\det(B)|$, the (absolute value of the) determinant of the basis matrix. For our vectors this volume is given as 2 units^2. The set S, depicted as a curved region, fails to be convex because some straight lines joining pairs of points in S pass outside of S: technically, for some $x_1, x_2 \in S$ not every sum $tx_1 + (1-t)x_2$, for $0 \le t \le 1$, is a point of S. It also fails to be closed under negation: $x \in S$ does not guarantee $-x \in S$. And the volume of S (≈ 2.8) fails to exceed $2^2 \times \det(B) = 8$. So Minkowski's Theorem does not apply to S; and indeed, if S were translated right or left it might fail to contain a non-zero lattice point. However, we *can* apply:



Blichfeldt's Theorem *If S is any measurable set whose volume exceeds* $|\det(B)|$ *then there exist distinct points* x_1 *and* x_2 *in S such that* $x_1 - x_2$ *is a lattice point in* $L(B)$.



To prove this, observe that sufficient copies of the fundamental parallelepiped $P(B)$, moved to lattice points as shown above right, will cover the set S. If their intersections with S are translated to the origin (see left) then two must overlap, because $\mathrm{vol}(S) > |\det(B)| = \mathrm{vol}(P(B))$. So some point z lies in the two distinct copies of $P(B)$ translated from, say, lattice points z_1 and z_2 (see right). Then $x_1 = z + z_1$ and $x_2 = z + z_2$ lie in S and $x_1 - x_2 = z + z_1 - (z + z_2)$, being a difference of lattice points, is itself a lattice point.



Minkowski's Theorem can now be proved as a corollary: let $\hat{S} = \frac{1}{2}S$ (halving in each of the n dimensions). Then $\mathrm{vol}(\hat{S}) = 2^{-n}\mathrm{vol}(S) > |\det(B)|$, so Blichfeldt supplies $x_1, x_2 \in \hat{S}$ with $x_1 - x_2 \in L(B)$. Then, by definition of $\hat{S}$, closure under negation, and convexity, $2x_1, 2x_2, -2x_2$, and $\frac{1}{2}(2x_1) + \left(1 - \frac{1}{2}\right)(-2x_2)$ are all in S, and the last of these, being equal to $x_1 - x_2$, is a nonzero lattice point.

Hermann Minkowski's 1889 theorem is the foundation of his 'geometry of numbers'. Hans Blichfeldt's theorem dates from 1914.

Web link: ocw.mit.edu/courses/mathematics, course 18.409: an Algorithmists Toolkit, lectures 18 and 19.
Further reading: *Lectures in Discrete Geometry* by Jiří Matoušek, Springer, New York, 2002.