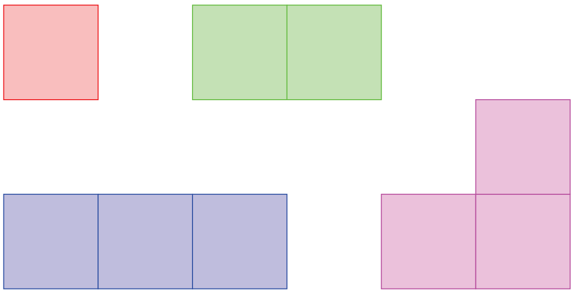
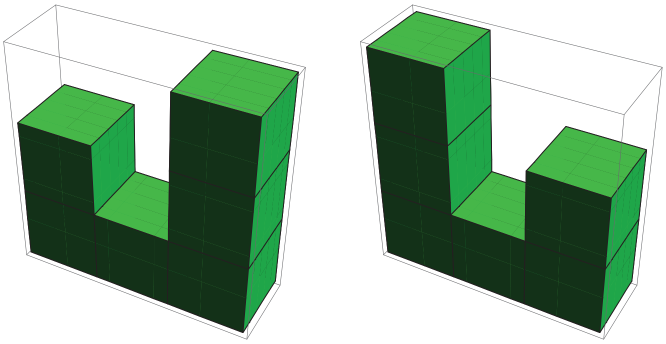
# Combinatorics I

Combinatorics is the study of discrete objects. Combinatorial problems are usually simple to define, but can be very difficult to solve. For example, a *polyomino* is a set of unit squares connected edge-to-edge, such that the vertices are positioned at integer coordinates. The four polyominoes with three or fewer squares are shown below:

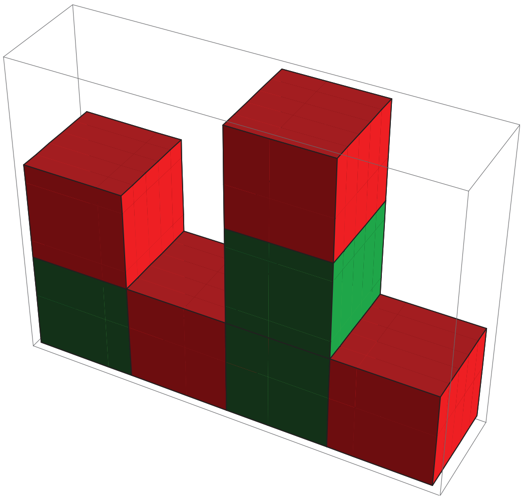


A natural question to ask is how many polyominoes there are of size $n$. We have already proved by exhaustion that this sequence begins $\{1, 1, 2, \ldots\}$. After a little effort, you will discover that there are five *tetrominoes* (polyominoes of size 4) and twelve *pentominoes* (polyominoes of size 5). Although this is a very simple problem to state, it is very difficult to find a formula for the number of polyominoes of a particular size. Indeed, there is no known formula as of the time of writing, and no-one knows how many polyominoes there are of size 60. Even the conjectured asymptotic formula, $P(n) \sim \frac{c\,\lambda^n}{n}$, is unproved (it is possible that, for instance, $P(n) \sim \frac{c\,\lambda^n}{n^{1.000001}}$ instead).

Counting polyominoes is a hard problem. Variants of this problem are substantially easier. For instance, suppose we restrict ourselves to polyominoes that can be created by stacking cubes in a vertical plane. To make things even easier, we consider rotations and reflections to be distinct, so the following arrangements are counted as two different polyominoes:



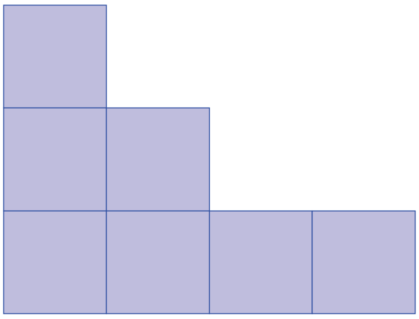
Many seemingly different combinatorial problems can be shown to be equivalent. This question can be converted into an equivalent one by colouring the top cube in each column red, and the remainder green. We then proceed up each column in turn, noting the colour of each cube. The configuration below is associated with the string $G\,R\,R\,G\,G\,R\,R$. Every string must end in $R$ for obvious reasons, so we may as well omit the final $R$ and just consider the string of $n-1$ letters, $G\,R\,R\,G\,G\,R$.



Since each of these polyominoes has a unique string, and vice-versa, we have a *bijection* between the two sets. Counting strings of a particular length is very easy (mathematicians would call this *trivial*); there are $2^{n-1}$ strings of $n-1$ letters chosen from $\{G, R\}$. Hence, there are $2^{n-1}$ of these restricted polyominoes. A third way of viewing this problem is to consider it to be an *ordered partition* of $n$; the above configuration corresponds to the sum $7 = 2 + 1 + 3 + 1$. So, we have solved a third combinatorial problem: there are $2^{n-1}$ ordered partitions of $n$ identical objects into non-empty subsets.

1. How many ordered partitions are there of $n$ into precisely $k$ subsets?

What if we consider the partitions $2 + 1 + 3 + 1$ and $3 + 1 + 1 + 2$ to be equivalent? In other words, what if order doesn't matter? This problem can be rephrased by forcing the elements of the partition to be arranged in decreasing order of size, *i.e.* $3 + 2 + 1 + 1$. The associated diagram of this partition is known variably as a *Ferrers diagram* or *Young diagram*.

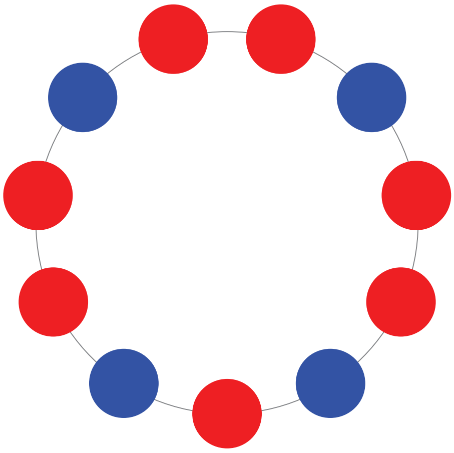


The partition numbers are $\{1, 2, 3, 5, 7, 11, \ldots\}$, as opposed to the ordered partition numbers $\{1, 2, 4, 8, 16, 32, \ldots\}$. Whereas the latter have a very simple formula, the formula for the unordered partition numbers is given by an extremely complicated infinite series by Hardy, Ramanujan and Rademacher:

- $p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} \sqrt{k} \left( \sum_{m \bmod k;\, \gcd(m,k)=1} e^{\frac{\pi i}{4k}\left(\left(\sum_{n=1}^{k-1} \cot\left(\frac{\pi n}{k}\right) \cot\left(\frac{\pi n m}{k}\right)\right) - 8 n m\right)} \right) \frac{d}{dn} \left( \frac{\sinh\left(\frac{\pi}{k} \sqrt{\frac{2}{3}\left(n - \frac{1}{24}\right)}\right)}{\sqrt{n - \frac{1}{24}}} \right)$

Don't be perturbed by this; the combinatorics explored in this chapter are several orders of magnitude easier than the partition problem. We begin with the problem of colouring $p$ beads on a necklace, where $p$ is a prime number. This leads to an intuitive proof of Fermat's little theorem, and a similarly combinatorial approach yields Wilson's theorem. The idea of symmetry is essential, so we contemplate some group theory as well.

# Burnside's lemma



Consider how many ways there are of colouring the 11 beads of this necklace either red or blue. This is an ambiguous question and there are many ways in which it can be answered:

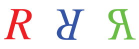
- "There are 2048 ways of colouring the necklace."
- "There are 188 ways of colouring the necklace."
- "There are 126 ways of colouring the necklace."

These answers are all valid, since the question was vague. If rotations and reflections are considered to be distinct, then the first answer is clearly correct (as $2^{11} = 2048$). If rotations are considered to be equivalent, but reflections are distinct, then the second is correct. The third answer applies when both rotations and reflections are equivalent.

It is easy to derive the answer 2048 in the first instance, but the others are somewhat trickier. Probably the best way to count the number of possibilities is to use a result known as *Burnside's lemma*. Firstly, we define what we mean by a symmetry.

■ A *symmetry* is an operation we can perform on an object. Moreover, the set of symmetries must form a group under composition. For example, a group of rotations can be regarded as symmetries. **[Definition of symmetry]**

In the first case of the necklace problem, we only consider the trivial group of one symmetry: the identity. In the second instance, we have the cyclic group of eleven symmetries (ten rotations and the identity). Finally, the third case requires the dihedral group of twenty-two symmetries (eleven reflections, ten rotations and the identity).



A *direct* symmetry can be expressed as a sequence of rigid transformations, such as translations and rotations. For example, the red and blue $R$s are related by a direct symmetry (rotation by $\pi$ through their common barycentre), By comparison, the green $R$ cannot be obtained from the red $R$ by a sequence of rotations and translations, so is related to the red $R$ by an *indirect* symmetry (in this case, a reflection). The composition of two direct or two indirect transformations is a direct transformation; the composition of a direct and indirect transformation is an indirect transformation. This idea can be succinctly represented as a $2 \times 2$ *Cayley table*:

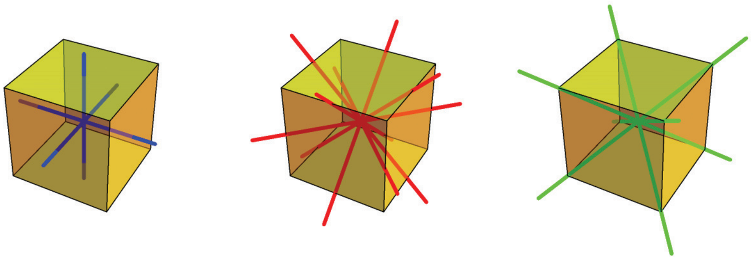
| $\circ$ | D | I |
|---|---|---|
| D | D | I |
| I | I | D |

■ An object is said to be *fixed* by a symmetry if it is unchanged by applying that symmetry. **[Definition of 'fixed']**

For example, the hyperbola $x^2 = y^2 + 1$ is fixed by a rotation of $\pi$ about the origin, whereas the parabola $y = x^2$ is not.

- The number of distinct objects is equal to the mean number of objects fixed by each symmetry. **[Burnside's lemma]**

For the second case of the necklace problem, there are 11 symmetries. The identity symmetry fixes all 2048 objects, whereas the ten rotations only fix two objects (the monochromatic necklaces). So, Burnside's lemma gives us a total of $\frac{1}{11}(2048 + 10 \times 2) = 188$ unique necklaces. Similarly, for the third case, we observe that there must be $2^6 = 64$ objects fixed by each of the 11 reflections, so we have $\frac{1}{22}(2048 + 10 \times 2 + 11 \times 64) = 126$ unique necklaces. That this gives an integer answer is a useful way to check your arithmetic.

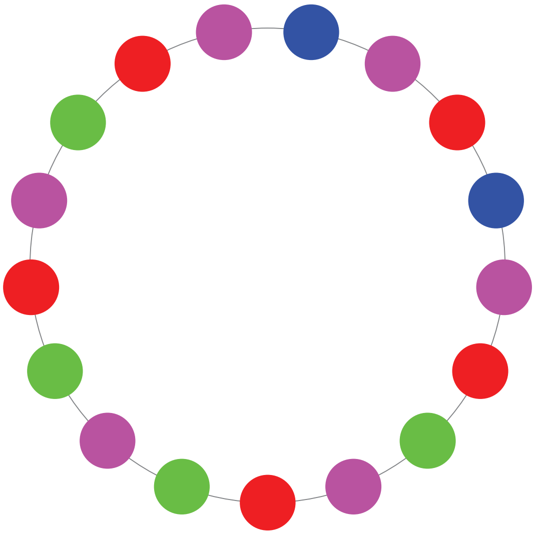


The cube has a group of 24 direct symmetries (and the same number of indirect symmetries). We can classify those 24 direct symmetries into five *conjugacy classes*:

- 1 identity symmetry;
- 6 rotations by $\frac{1}{2}\pi$ about the blue axes;
- 3 rotations by $\pi$ about the blue axes;
- 6 rotations by $\pi$ about the red axes;
- 8 rotations by $\frac{2}{3}\pi$ about the green axes.

**2.** Suppose we colour each face of a cube one of $k$ colours. By considering the number of colourings fixed by each of the above symmetries, deduce the number of distinct colourings of the cube where rotations are considered equivalent.

# Fermat's little theorem



We now generalise the previous question to a necklace of $p$ beads (where $p$ is prime) and $c$ different colours.

**3.** How many distinct ways can a necklace of $p$ beads be coloured with $c$ colours, where $p$ is prime and $c \geq 2$? Rotations are considered to be equivalent, whereas reflections are distinct.

**4.** Hence show that $c^p \equiv c \pmod{p}$. **[Fermat's little theorem]**

Fermat's little theorem only applies when the modulus is prime. If, instead, the modulus is composite, it is necessary to use a generalisation by Euler. Unlike Fermat's little theorem, Euler's generalisation does not appear to be a consequence of applying Burnside's lemma to necklaces of $n$ beads.

■ If $a$ and $n$ are coprime, then $a^{\varphi(n)} \equiv 1 \pmod{n}$, where $\varphi(n)$ is Euler's totient function (the number of positive integers $k \leq n$ which are coprime to $n$). **[Euler-Fermat]**

Euler's totient function can easily be computed when the prime factorisation of $n$ is known. Specifically, we have the rule $\varphi(a\,b) = \varphi(a)\,\varphi(b)$ if $a$ and $b$ are coprime, and $\varphi(p^n) = (p-1)\,p^{n-1}$.

Suppose $N = p\,q$ is a product of two distinct primes, each of which has hundreds of digits. Given $N$, there is no known algorithm capable of factorising it to find $p$ and $q$ in a reasonable (polynomial) amount of time. This can be used as the basis of a cryptographic system known as *RSA* (after its creators, Rivest, Shamir and Adleman). The idea is that we define a function, $f : \mathbb{Z}_N \to \mathbb{Z}_N$, which the general public has access to. However, we keep the inverse function $f^{-1}$ secret.

**5.** Suppose that $b = f(a) \equiv a^d \pmod{N}$. Show that $f^{-1}(b) \equiv b^e \pmod{N}$, where $d\,e \equiv 1 \pmod{\varphi(N)}$. **[Basis of RSA]**

In other words, we publish $a$, $d$, $N$ (and therefore $f$) but leave $p$, $q$, $e$ secret. As it is impossible to compute $e$ from $d$ without knowledge of $p$ and $q$, the general public cannot calculate $f^{-1}$. Hence, they can encrypt an integer, but not decrypt it. As the numbers in $\mathbb{Z}_N$ can have hundreds of digits, it is possible to store a substantial amount of information in one integer. This is typically used to encrypt passwords, safe in the knowledge that there is no known algorithm for rapidly factorising semiprimes.

Interestingly, there is an algorithm called *AKS* which enables a computer (or, more correctly, Turing machine) to determine whether a number is prime in polynomial time (in the number of digits), but actually factorising the number may require exponential time. Additionally, so-called 'quantum computers' are capable of prime factorisation in cubic time, so a sufficiently powerful quantum computer would render RSA useless. Fortunately, this technology is a long way off, and the largest semiprime factorised by Shor's algorithm as of the time of writing is $15 = 5 \times 3$ using a machine with seven quantum bits.

## Wilson's Theorem

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | *R* | | | | | | | |
| | | | | | *R* | | | | | |
| | | | | | | | | | *R* | |
| | | | | | | | *R* | | | |
| | *R* | | | | | | | | | |
| | | | | *R* | | | | | | |
| | | | | | | | | *R* | | |
| | | *R* | | | | | | | | |
| | | | | | | | | | | *R* |
| *R* | | | | | | | | | | |
| | | | | | | *R* | | | | |

Suppose we have a $p \times p$ chessboard, where $p$ is prime. We label each square with a coordinate $(x, y)$, where $x$ and $y$ are considered modulo $p$ (in effect, forming a toroidal surface). We then place an arrangement of $p$ non-attacking rooks on the chessboard, *i.e.* one in every row and one in every column. We consider the group of $p^2$ symmetries (one identity and $p^2 - 1$ translations).

**6.** Show that there are $p!$ arrangements fixed by the identity symmetry.

**7.** Show that no arrangements are fixed by any of the $2(p - 1)$ horizontal or vertical translations.

**8.** Show that $p$ arrangements are fixed by each of the $(p - 1)^2$ remaining translations.

**9.** Hence determine the number of unique arrangements, where toroidal translations of the board are considered equivalent.

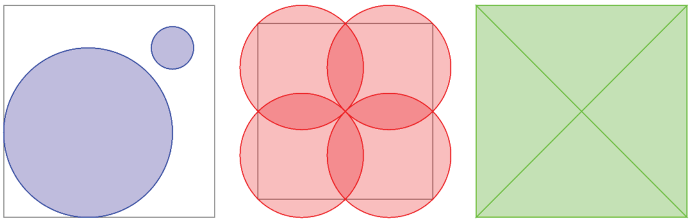
**10.** Prove that $(p - 1)! \equiv -1$ modulo $p$ if $p$ is prime. **[Wilson's theorem]**

If $n$ is composite, then $(n - 1)! \equiv 0$ modulo $n$, except where $n = 4$, in which case $(n - 1)! \equiv 2$. Hence, the converse of Wilson's theorem is also true.

## Packings, coverings and tilings

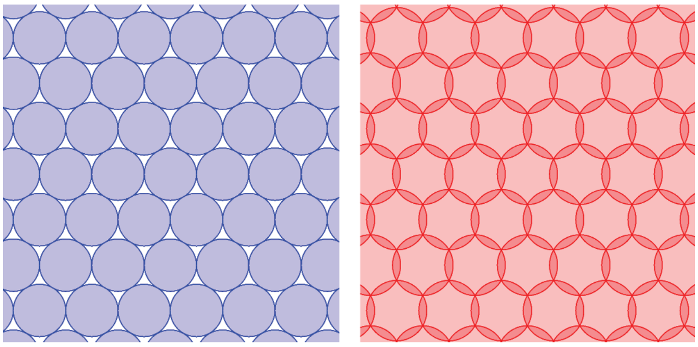
Straddling the boundary between combinatorics and geometry is the idea of *tessellations*, or *tilings*.

Consider a set $S$ of [closed] tiles, each of which is a subset of some region $R$. If the pairwise intersection of any two tiles of $S$ has zero area, then $S$ is a *packing*. If the union of all tiles in $S$ is the entirety of $R$, then $S$ is a *covering*. If both of these conditions hold, it is a *tiling*.

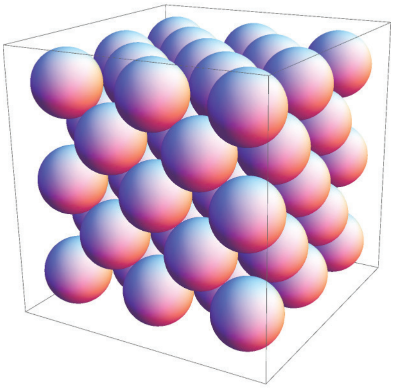


The diagram above highlights the differences. The first diagram is a packing using two blue circles. The second is a covering using four red circles. The third diagram is both a packing and covering, and thus a tiling, using four green isosceles right-angled triangles.

Using circles of unit radius, there are obviously no tilings of the plane. It is of interest to find the packing of the highest density and covering of the lowest density.



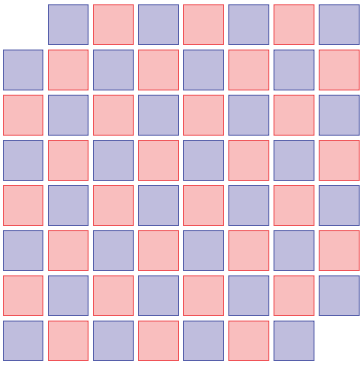
It has been proved that the optimal packings and coverings of the plane using circles of unit radius are obtained by positioning them at the vertices of the regular triangular tiling. Other optimisation problems are solved by the hexagonal lattice, which is why honeybees favour hexagonal honeycombs as opposed to a rectangular Cartesian grid. In higher dimensions, less is known. For three dimensions, the optimal lattice packing of spheres is the *face-centred cubic* lattice $A_3 = \{(x,\ y,\ z) \in \mathbb{Z}^3,\ x + y + z \equiv 0 \pmod 2\}$, whereas the optimal lattice covering is the *body-centred cubic* lattice $A_3{}^* = \{(x,\ y,\ z) \in \mathbb{Z}^3,\ x \equiv y \equiv z \pmod 2\}$.



Each sphere in the face-centred cubic packing is adjacent to twelve other spheres. This suggests another packing problem: what is the maximum number of disjoint unit spheres tangent to a given unit sphere? In two dimensions, the answer is rather trivially six. In three dimensions, Isaac Newton conjectured that the maximum is indeed twelve spheres, whereas David Gregory hypothesised that thirteen could be achieved. It transpires that Newton was correct. The problem has also been solved in 4, 8 and 24 dimensions, again corresponding to the arrangements of spheres in very regular lattice packings (known as $D_4$, $E_8$ and $\Lambda_{24}$, respectively). $\Lambda_{24}$ (the *Leech lattice*) has so many interesting properties and profound connections that I cannot hope to list them all here. Nevertheless, its existence is related to string theory, error-correcting codes, the Monster group, and the curious fact that $1^2 + 2^2 + 3^2 + \ldots + 24^2 = 70^2$.

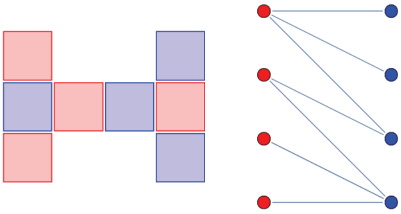
# Colouring arguments

To begin with, we ponder tilings of finite, discrete spaces. For example, consider a standard $8 \times 8$ chessboard with two opposite corners removed. Is it possible to tile the resulting shape with 31 $1 \times 2$ dominoes?



If the chessboard is coloured as above, each domino must occupy precisely one blue and one red square. As there are 32 blue and 30 red squares, it is clearly impossible to tile it with 31 dominoes.

The more general problem of determining whether a polyomino-shaped region can be tiled with dominoes can be embedded in graph theory. We represent the squares with vertices, and join vertices corresponding to adjacent squares. Some regions clearly cannot be tiled, even if they have equal quantities of squares of each parity. One such example is the following 'octomino', shown below with an equivalent bipartite graph:



The lowest blue vertex in the graph is connected to three red vertices, two of which are exclusively connected to this blue vertex. It is therefore impossible to place disjoint dominoes to cover both of the corresponding red squares. However, the basic colour-counting argument is insufficient here, as there are four red and four blue squares.

In effect, we want to find a *bipartite matching* between the red and blue vertices of the graph. A necessary and sufficient condition for there to exist an *injection* from the red vertices to the blue vertices is *Hall's marriage theorem.*

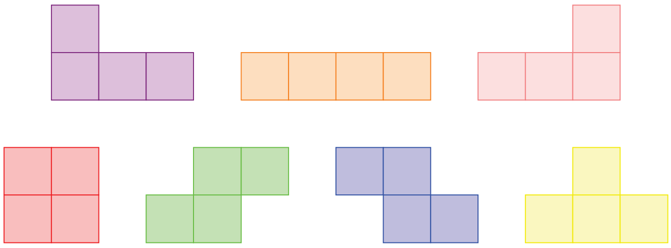
- Let $S$ be the set of red vertices, and $T$ be the set of blue vertices. Consider each subset $S' \subseteq S$, and let $T' \subseteq T$ be the set of vertices directly connected to vertices in $S'$. Then there exists an injection from the red vertices to the blue vertices if and only if $|S'| \leq |T'|$ for all subsets $S'$. **[Hall's marriage theorem]**

For a bijection, it is necessary and sufficient that there are equal numbers of red and blue vertices and the above result also holds. Returning to the octomino problem, note that the two red vertices of degree 1 are connected to the same blue vertex, so the marriage condition does not hold.

Verifying the marriage condition can be a time-consuming process, as there are $2^n$ subsets of red vertices for a bipartite graph with $n$ red and $n$ blue vertices. This is faster than checking every possible bijection, of which there are $n!$. Both of these algorithms are said to take *exponential time*. People are interested in fast, *polynomial-time* algorithms, as they usually can be executed in a reasonable amount of time.

Colouring can solve much more general problems than the domino tiling problem.

**11.** Determine whether it is possible to tile a $4 \times 7$ rectangle with (rotations of) each of the seven tetrominoes (where reflections are considered to be distinct). The seven tetrominoes are shown below:



**12.** Is it possible to tile a 6×6 rectangle with 15 dominoes and 6 non-attacking rooks? **[Ed Pegg Jr, 2002]**

**13.** Show that the maximum number of (grid-aligned) $k \times k$ square tiles that can be packed into a $m \times n$ chessboard is given by $\left\lfloor \frac{m}{k} \right\rfloor \left\lfloor \frac{n}{k} \right\rfloor$.

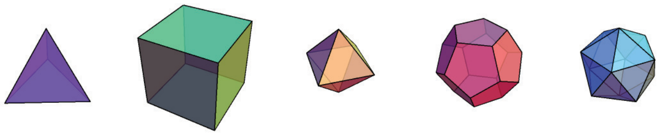
In addition to determining whether or not a region can be tiled, it is occasionally possible to enumerate precisely how many ways in which this can be done. This is typically accomplished using recursion on the size of the region.

**14.** In how many ways can a $2 \times n$ rectangle be tiled with $n$ dominoes?

This is a simple case of what one would initially imagine to be a completely intractable problem: to count the number of domino tilings of a $m \times n$ rectangle. A remarkable discovery by Kasteleyn enumerates this for any planar graph, and thus how many domino tilings exist for any polyomino. In particular, a $m \times n$ chessboard can be tiled by dominoes in exactly $\prod_{k=1}^{n} \prod_{l=1}^{m} \sqrt[4]{4\cos^2 \frac{\pi l}{m+1} + 4\cos^2 \frac{\pi k}{n+1}}$ ways.

## Regular solids and tilings

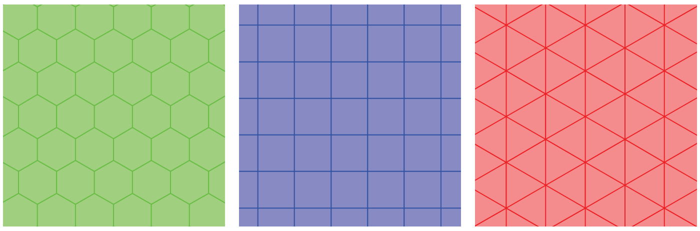
Suppose we attempt to tile a surface with regular $n$-gons, where $k$ $n$-gons meet at each vertex. To avoid trivial cases, we assume that both $k$ and $n$ exceed 2. The cases where the *Schläfli symbol* $\{n, k\}$ is either $\{3, 3\}$, $\{4, 3\}$, $\{3, 4\}$, $\{5, 3\}$ and $\{3, 5\}$ result in the five regular solids, namely the tetrahedron, cube, octahedron, dodecahedron and icosahedron.



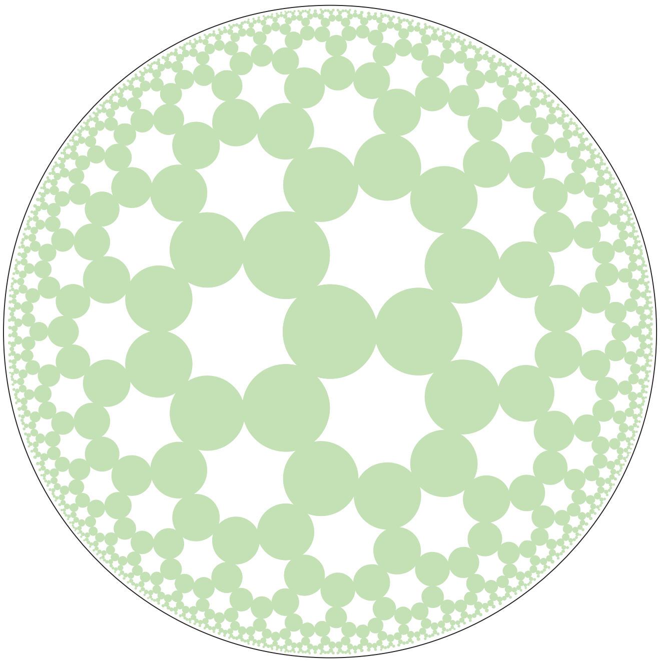
They are also referred to as *Platonic solids*, as Plato believed that all matter was composed (at the atomic level) of minuscule cubes, tetrahedra, octahedra and icosahedra, associating each one with a different classical element. He reserved the dodecahedron for representing the entire universe.

**15.** Each face of a regular dodecahedron is infected with either *E. coli*, *S. aureus* or *T. rychlik* bacteria. In how many ways is this possible, treating rotations as equivalent? **[Adapted from Google Labs Aptitude Test]**

If $\{n, k\}$ is $\{6, 3\}$, $\{4, 4\}$ or $\{3, 6\}$, we obtain the hexagonal, square and triangular tilings, respectively, of the plane. The Platonic solids can be regarded as analogous tilings of the sphere.

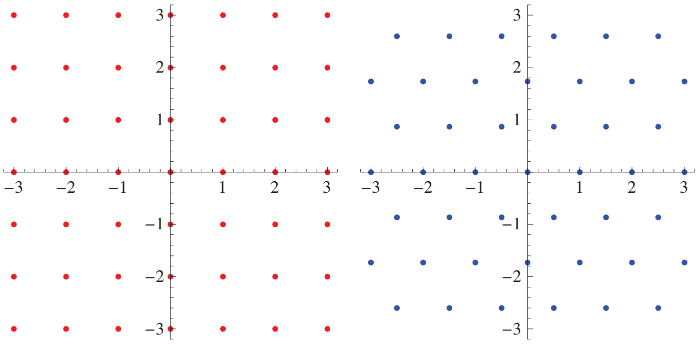


If $\{n, k\}$ is anything other than these eight possibilities, the sum of the angles around each vertex exceeds $2\pi$. This is only possible in the bizarre hyperbolic surfaces described by Bolyai-Lobachevskian geometry.



On the complex plane, numbers of the form $a + b\,i$ ($a, b \in \mathbb{Z}$) form a ring known as the *Gaussian integers*, which are positioned at the vertices of the square tiling. As Euclid's algorithm can be applied to the Gaussian integers, the fundamental theorem of arithmetic still holds: Gaussian integers can be factorised uniquely into a product of *Gaussian primes* (up to multiplication by the *units*, $1$, $-1$, $i$ and $-i$). Not all ordinary primes are Gaussian primes; for example, 2 is not a Gaussian prime, as it can be factorised as $(1 + i)(1 - i)$.

Suppose we have a grasshopper initially positioned at the origin, which can only jump to a Gaussian prime within the disc of radius $R$ centred on its current position. It is an unsolved problem as to whether there is some $R$ for which the grasshopper can visit infinitely many Gaussian primes.



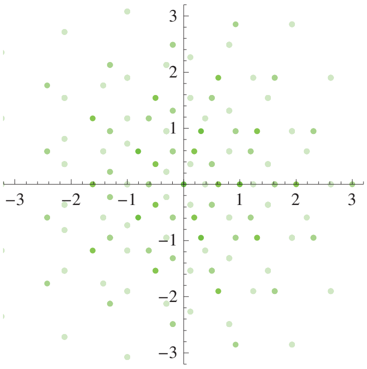
Similarly, numbers of the form $a + b\,\omega$ ($a, b \in \mathbb{Z}$), where $\omega$ is a primitive cube root of unity, form the ring of *Eisenstein integers*. They are positioned at the vertices of the triangular tiling. As with the Gaussian integers, the fundamental theorem of arithmetic applies. The units are the sixth roots of unity, namely $\left\{\pm 1, \pm\omega, \pm\omega^2\right\}$. It is possible to find the squared distance between two Eisenstein integers $a$ and $b$ by expressing the vector $a - b$ in terms of $\{1, \omega, \omega^2\}$ and calculating $|a - b|^2 = (a - b)(a^* - b^*)$, remembering that $1 + \omega + \omega^2 = 0$ and $\omega^3 = 1$.

**16.** A set $S$ of 99 points are drawn in the plane, such that no two are within a distance of 2 units. Prove that there exists some subset $T \subset S$ of 15 points, such that no two are within a distance of $\sqrt{7}$ units.

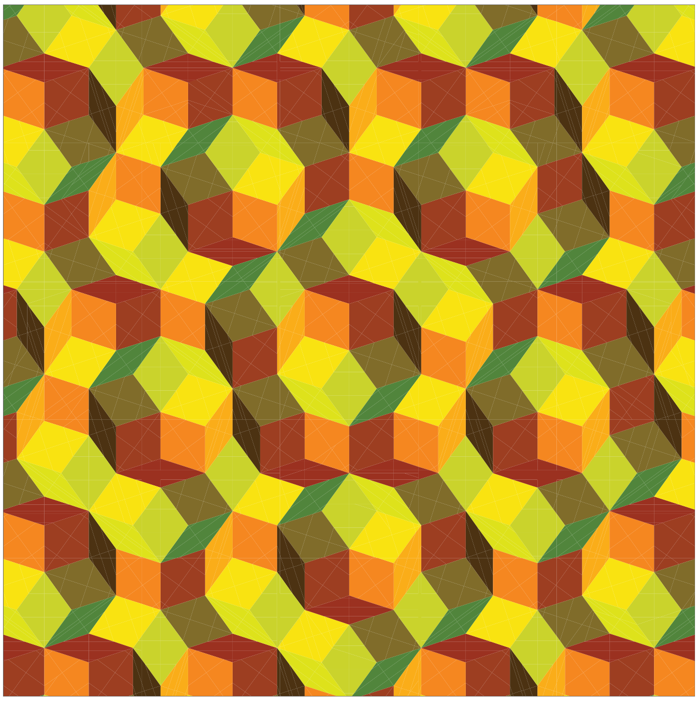
# Aperiodic tilings

As we noted, the only regular polygons capable of tiling the Euclidean plane are the triangle, square and hexagon. Pentagons cannot, as three pentagons at each vertex have an interior angle sum of $\frac{9}{5}\pi$, which is slightly less than $2\pi$ and causes the pentagons to 'curl up' into a dodecahedron. Similarly, attempting to place four or more pentagons around each vertex results in a hyperbolic tiling, as $\frac{12}{5}\pi > 2\pi$.

More strongly, there is no tiling of the plane which exhibits both translational symmetry and order-5 rotational symmetry. To prove this, we assume without loss of generality that the tiling is fixed by both a translation parallel to the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and a rotation by $\frac{2}{5}\pi$ about the origin. In that case, it is possible to map the origin to any point expressible as the sum of fifth roots of unity.



The points on the real axis expressible in this way are those of the form $a + b\,\phi$, where $a, b \in \mathbb{Z}$ and $\phi = \frac{1}{2}\left(1 + \sqrt{5}\right)$. As $\phi$ is an irrational number, these points form a *dense subset* of the reals, *i.e.* for every $\varepsilon > 0$, every point $x$ on the real axis is within a distance of $\varepsilon$ from a point of the form $a + b\,\phi$. This means that the tiling must be composed of infinitesimally small tiles, which contradicts our notion of discrete tiles.

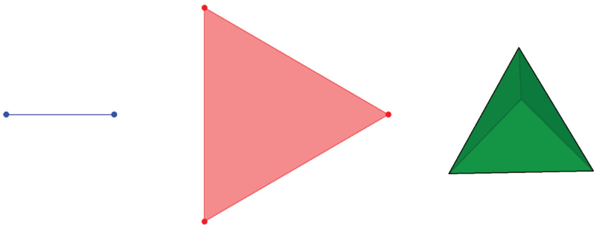


If we dispose of the translational symmetry, we can indeed have tilings with order-5 rotational symmetry. Perhaps the most famous is an aperiodic tiling known as the *Penrose tiling* (above), formed from interlocking ‘thin’ and ‘thick’ rhombi in the ratio $1 : \phi$. It is a remarkable fact that every tiling of the plane with these two tiles (and certain matching rules) exhibits this ratio, and is thus aperiodic (since $\phi$ is irrational). An unsolved problem is whether there is a *single* connected shape (an ‘aperiodic monotile’), which can only tile the plane aperiodically. Joshua Socolar and Joan Taylor recently (2010) discovered a disconnected aperiodic monotile based on the hexagonal honeycomb, suggesting that there may indeed be a connected variant waiting to be found.

There is a three-dimensional analogue of the Penrose tiling. It is formed from equilateral parallelepipeds (three-dimensional rhombi) and displays icosahedral symmetry. Crystallographers were very surprised to find naturally occurring crystals with this structure, termed ‘quasicrystals’. It was previously believed that solids could only be either periodic crystals or totally irregular.

# Invariants

An *invariant* is, as suggested by the name, something that doesn’t change. One of the simplest invariants is parity: whether something is even or odd. Integers are one of the most common things to display parity; however, the idea is equally applicable to other things such as permutations. To realise that permutations have a parity, it is necessary to consider them in a more geometrical light.



An *n-simplex* is a regular $n$-dimensional figure (polytope) with $n + 1$ vertices, which is fixed under any permutation of the vertices. The 1-simplex, 2-simplex and 3-simplex are the line segment, triangle and tetrahedron, respectively, as in the above diagram. Interchanging two of the vertices of a simplex can be regarded as a reflection. For example, reflecting a regular tetrahedron $ABCD$ with circumcentre $O$ in the plane $OCD$ causes the vertices $A$ and $B$ to be swapped.

This suggests two different sets of permutations: the *odd* permutations, which correspond to indirect isometries of $\mathbb{R}^n$; and *even* permutations, which correspond to direct isometries. A $k$-cycle (cyclic permutation of some subset containing $k$ elements) is an odd permutation if $k$ is even, and *vice-versa*. In particular, 2-cycles (or swaps) are odd permutations.

The set of even permutations of $n$ elements forms a group known as the *alternating group* $A_n$. This is a subgroup of the group of all permutations, known as the *symmetric group* $S_n$. Any composition of even permutations is itself an even permutation, which can form a useful invariant. For example, it shows that not all conceivable configurations of a Rubik's cube can be attained by applying legal moves to the initial 'solved' position.

**17.** Suppose we have a hollow $4\times4$ square containing 15 unit square tiles and one empty space, into which any adjacent tile can be moved. The fifteen tiles are numbered from 1 to 15. Determine whether it is possible to get from the left-hand configuration to the right-hand configuration in the diagram below. **[Sam Loyd's 15 puzzle]**

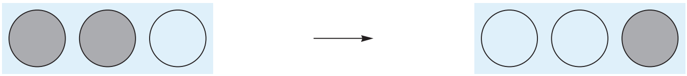
$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & \end{array} \quad \xrightarrow{?} \quad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 15 & 14 & \end{array}$$

Instead of an invariant, it is possible to define a value that only changes in one direction, known as a *monovariant*. This is useful for proving that a process (such as a perturbation argument) eventually terminates.

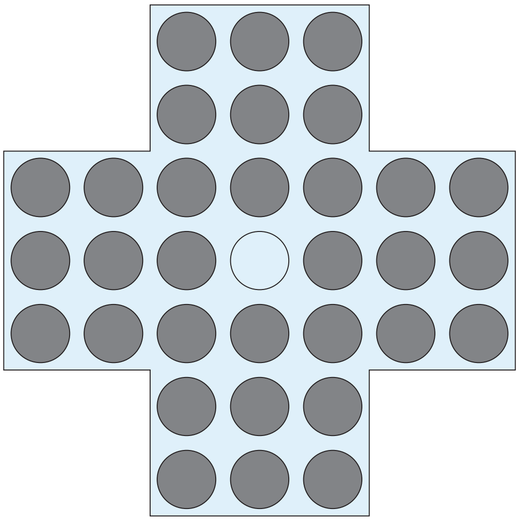
**18.** There are $n$ red points and $n$ blue points in the plane, no three of which are collinear. Prove that it is possible to pair each red point with a distinct blue point using $n$ non-intersecting line segments. **[EGMO 2012, Friday bulletin]**

## Solitaire

Quite a few interesting problems pertain to the game of peg solitaire. We have a (possibly infinite) board, which is a subset of $\mathbb{Z}^2$ containing some (possibly infinite) initial configuration of identical counters. The only allowed move is to jump horizontally or vertically over an occupied square to an unoccupied one; the piece that has been jumped over is removed. This is demonstrated below.



**19.** Suppose we have a game of solitaire on a bounded board beginning with the configuration of 32 pieces shown below. Show that if we can reach a position where only one piece remains on the board, then we can do so where the piece is in the centre.



**20.** We begin with an infinite chessboard, and divide the board into two half-planes with a straight horizontal line. All squares below the line are occupied with counters; all squares above the line are unoccupied. Show that it is impossible, after a finite sequence of moves, for a counter to occupy the fifth row above the line. **[Conway's soldiers]**

**21.** Suppose we have an infinite chessboard with an initial configuration of $n^2$ pieces occupying $n^2$ squares that form a square of side length $n$. For what positive integers $n$ can the game end with only one piece remaining on the board? **[IMO 1993, Question 3]**

## Solutions

**1.** We are enumerating strings containing precisely $k-1$ $R$s and $n-k$ $G$s. Hence, the number of ordered partitions of $n$ into $k$ subsets is given by the binomial coefficient $\binom{n-1}{k-1} = \frac{(n-1)!}{(k-1)!\,(n-k)!}$.

**2.** All $k^6$ colourings of the cube are fixed by the identity. Consider a rotation by $\frac{1}{2}\pi$ about the vertical blue axis. The top and bottom faces can be any colour, whereas the four other faces must all be the same colour. Hence, each of the 6 symmetries in this conjugacy class fix $k^3$ colourings. By similar reasoning, the 3 rotations by $\pi$ about the blue axes each fix $k^4$ colourings. The 6 rotations about the red axes each fix $k^3$ colourings, whereas the 8 rotations by $\frac{2}{3}\pi$ about the green axes fix only $k^2$ colourings. Applying Burnside's lemma, the total number is $\frac{1}{24}\left(k^6 + 3\,k^4 + 12\,k^3 + 8\,k^2\right)$.

**3.** There are $p$ symmetries, namely the identity and $p-1$ rotations. The former fixes all $n^p$ colourings, whereas the latter fixes only the $n$ monochromatic necklaces. Hence, we have $\frac{1}{p}\,(n^p + n(p-1))$ unique necklaces.

**4.** The result of the previous question is an integer, so $c^p + c(p-1)$ is divisible by $p$. Hence, $c^p + c\,p - c \equiv 0$. As $c\,p \equiv 0$, this means that $c^p \equiv c \pmod{p}$.

**5.** Note that $\varphi(N) = \varphi(p)\,\varphi(q) = (p-1)\,(q-1)$. Expressing $b$ in terms of $a$, we obtain $b^e = a^{d\,e}$. As $a^{\varphi(N)} \equiv 1 \pmod{N}$ by Euler-Fermat, and $d\,e \equiv 1 \pmod{\varphi(N)}$, $a^{d\,e} \equiv a^1 = a \pmod{N}$, so is precisely the inverse function we are looking for.

**6.** The position of the rooks can be regarded as a bijection mapping rows to columns. There are $p\,!$ permutations of $p$ elements.

**7.** Without loss of generality, just consider horizontal translations by $(a,\,0)$. If there is a rook in $(x,\ y)$, there must also be a rook in $(x+a,\ y)$, contradicting the assumption that the rooks are non-attacking.

**8.** Consider the rook positioned at the coordinates $(x,\,0)$, and let the translation be parallel to vector $(a,\,b)$. This forces there to be rooks in positions $(x+a,\,b)$, $(x+2\,a,\,2\,b)$, …, $(x-a,\,-b)$. Hence, the arrangement is determined uniquely by the abscissa of the rook in the 0th row, of which there are $p$ possibilities. Hence, $p$ arrangements are fixed by each of these translations.

**9.** We have $\frac{1}{p^2}\left(p\,! + p(p-1)^2\right)$ distinct arrangements by Burnside's lemma.

**10.** The previous answer must be an integer, so $p\,! + p(p-1)^2 \equiv 0 \left(\operatorname{mod} p^2\right)$. Dividing throughout by $p$, we obtain $(p-1)\,! + (p-1)^2 \equiv 0 \pmod{p}$. We can expand this to yield $(p-1)\,! + p^2 - 2\,p + 1 \equiv 0 \pmod{p}$. As $p^2$ and $2\,p$ are divisible by $p$, we can eliminate those terms, resulting in the statement of Wilson's theorem.

**11.** Colour the squares black and white, as on a standard chessboard. The T-shaped tetromino must cover three black squares and one white square (or *vice-versa*), whereas each of the other tetrominoes cover precisely two squares of each colour. As the chessboard features equal numbers of black and white squares, this is indeed impossible.

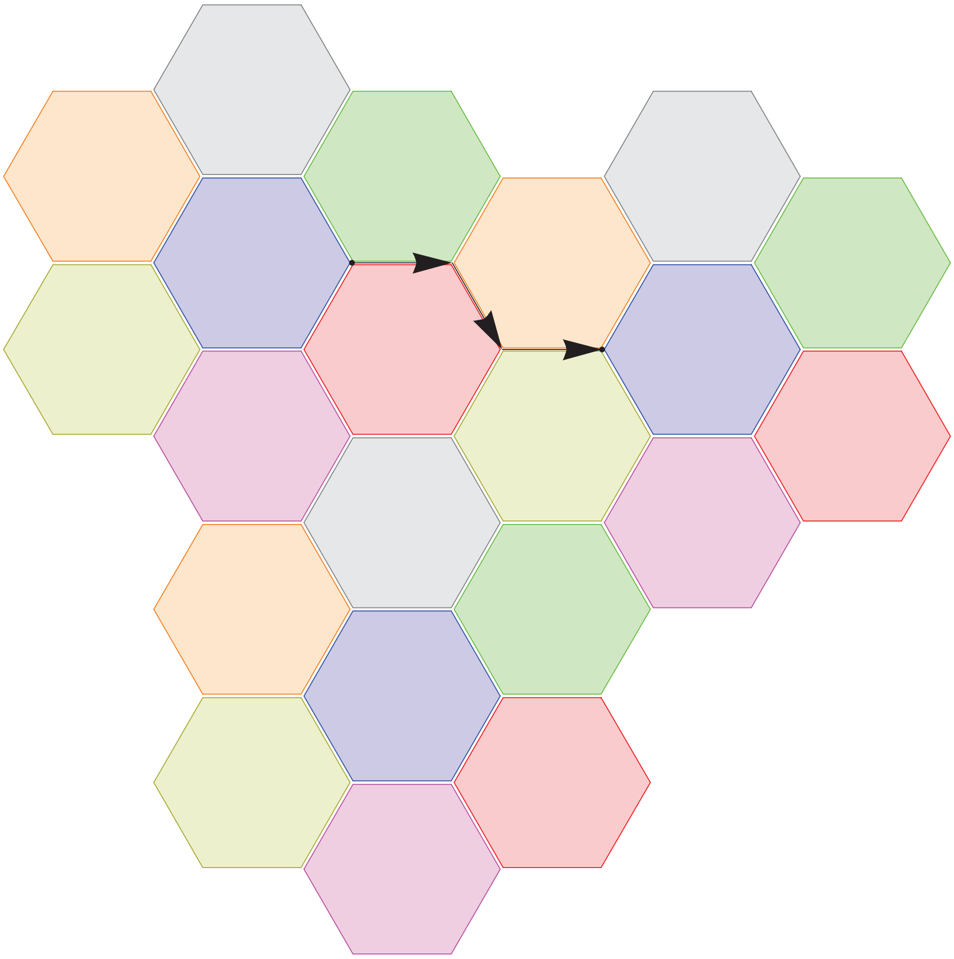
**12.** Colour the squares black and white, as on a standard chessboard. The six rooks are positioned on squares $(i,\ \sigma(i))$, where $\sigma$ is a permutation of $\{1, 2, 3, 4, 5, 6\}$. Select two rooks at positions $(i,\ \sigma(i))$ and $(j,\ \sigma(j))$, and move them to $(i,\ \sigma(j))$ and $(j,\ \sigma(i))$, respectively. Applying this move does not alter the parity of rooks on white squares. Since we can do this until they lie on the long diagonal of white squares, it is clear that there must have been an even number of rooks on white squares to begin with. However, the constraint that the remaining 30 squares can be tiled by dominoes forces the rooks to occupy three white and three black squares, which contradicts the previous statement. Hence, it is impossible.

**13.** Represent each square with coordinates $(x, y)$, where $x \in \{1, 2, \ldots, m\}$ and $y \in \{1, 2, \ldots, n\}$. Colour the square blue if $x \equiv y \equiv 0 \pmod k$, and white otherwise. Clearly, each tile must conceal precisely one blue square, and there are only $\left\lfloor \frac{m}{k} \right\rfloor \left\lfloor \frac{n}{k} \right\rfloor$ of them. This bound is attainable.

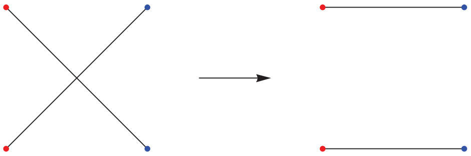
**14.** Let this number be denoted $f(n)$. Either the rightmost $2 \times 1$ rectangle is a (vertical) domino or the rightmost $2 \times 2$ rectangle is a pair of horizontal dominoes. Now consider how many ways there are of tiling the remaining area. In the first case, there are $f(n-1)$ possible configurations; in the second, there are $f(n-2)$. This gives us the recurrence relation $f(n) = f(n-1) + f(n-2)$. Together with the obvious fact that $f(1) = 1$ and $f(2) = 2$, this generates the Fibonacci sequence, $f(n) = F(n+1)$.

**15.** There are 60 symmetries of the regular dodecahedron. The identity symmetry fixes all $3^{12}$ infections. There are 24 rotations about axes passing through the centres of opposite faces, each of which fix $3^4$ infections. The 15 rotations about axes passing through the midpoints of edges each fix $3^6$ infections. Finally, the 20 rotations about axes passing through opposite vertices each fix $3^4$ infections. By Burnside's lemma, there are $\frac{1}{60}\left(3^{12} + 24 \times 3^4 + 15 \times 3^6 + 20 \times 3^4\right) = 9099$ unique infections of the dodecahedron with three strains of bacteria.

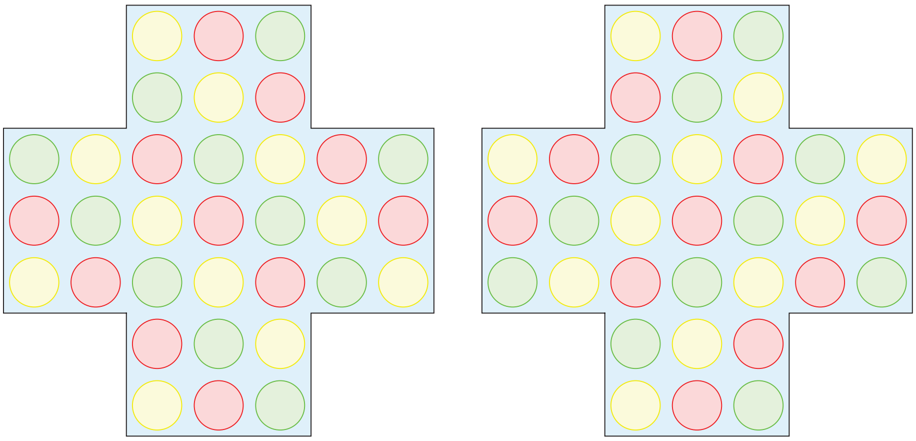
**16.** Tile the plane with the regular hexagonal tiling, where each hexagon has side length 1. Clearly, no two points in $S$ can occupy the same hexagon. 7-colour the hexagons in a repetitive fashion, such that each hexagon is adjacent to six hexagons of different colours. By the pigeonhole principle, at least 15 of the points must lie in identically-coloured hexagons. It is straightforward to show that no two of those points can be within $\sqrt{7}$ of each other, by considering the closest approach of the vertices of the hexagons and using cube roots of unity to calculate the distance: the arrow shown in the honeycomb below has a complex vector of $2 - \omega$, which has squared length $(2 - \omega)\left(2 - \omega^2\right) = 4 - 2\left(\omega + \omega^2\right) + 1 = 7$.



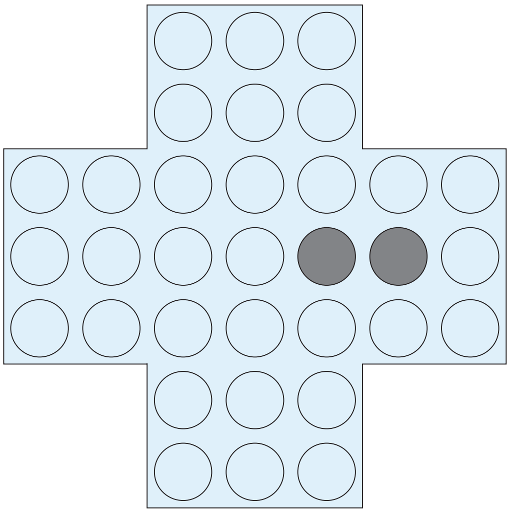
**17.** Label the empty space with 0, so we can regard this as a permutation of $\{0, 1, \ldots, 15\}$. Consider the parity of $x + y$, where $(x, y)$ is the location of the empty space, together with the parity of the permutation $\sigma$. Note that each move flips both parities, thus leaving the total parity of $x + y + \sigma$ unchanged. However, interchanging any two tiles without moving the empty space alters the parity of $x + y + \sigma$, so it is impossible to get from the left configuration to the right configuration.



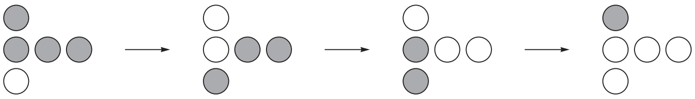
**18.** Biject them in an arbitrary way using $n$ line segments. If we encounter a configuration of four points joined by two intersecting line segments, as above, then we can replace the line segments with disjoint line segments. Let the monovariant $E$ be the total length of line segments. $E$ strictly decreases at each step (by the triangle inequality), so the process cannot cycle. As there are only finitely many bijections between red and blue points, the process must terminate with $n$ disjoint line segments.



**19.** Firstly, colour the tile at coordinates $(x, y)$ either red, green or yellow depending on the value of $x + y$ modulo 3, where we consider the central tile to be the origin (coloured red). As the parities of red, green and yellow counters all change simultaneously when a solitaire move is played, the final counter must be on a red square. However, we can also colour the tiles depending on $x - y$ modulo 3, resulting in a perpendicular pattern of colouring as shown above. The only tiles that are red in both colourings are given by $(3i, 3j)$, where $i$ and $j$ are integers. On the bounded board, there are only five such tiles. Backtracking by one move must result in a configuration equivalent to the one shown below, in which case we can trivially jump to the central square.



**20.** Assume that it is possible to reach a square in the fifth row, in attempt to derive a contradiction. Without loss of generality, we will use $T = (0, 0)$ as the 'target square'. For each square $(x, y)$, we assign a value of $\phi^{-(|x|+|y|)}$, where $|x| + |y|$ is the Manhattan distance between $(x, y)$ and $(0, 0)$, and $\phi = \frac{1+\sqrt{5}}{2}$ is the golden ratio. Let $E$ be the sum of the values of the occupied squares. If a counter on a square of value $\phi^k$ jumps over one of value $\phi^{k+1}$, this results in a single counter on a square of value less than or equal to $\phi^{k+2}$. As $\phi^{k+2} = \phi^{k+1} + \phi^k$, the value of $E$ cannot increase. At the beginning of the game, the value of $E$ can be calculated by summing some geometric progressions; it is simple to show that this value equals 1. As the value of the target square is also 1, it is necessary to use all of the counters to reach it. However, that is impossible in a finite amount of time, as there are infinitely many counters.



**21.** For $n = 1$ and $n = 2$, this is trivial. If we have an arrangement shown above, it is possible to 'delete' three adjacent pieces. This can be used, rather effectively, to reduce a problem from $n = 3k + 4$ to $n = 3k + 2$ by deleting the outermost ‘layer’ of pieces, as in the diagram below. Similarly, we can reduce a problem from $n = 3k + 5$ to $n = 3k + 1$ by deleting the outermost two layers. By induction, we can solve the problem for all $n$ except for multiples of three. If $n$ is a multiple of three, we colour the tile at coordinates $(x, y)$ either red, green or yellow depending on the value of $x + y$ modulo 3. Let the number of pieces on red, green and yellow tiles be indicated by $R$, $G$ and $Y$, respectively. Note that if $(-1)^R = (-1)^G = (-1)^Y$ before a solitaire move, then it will remain true afterwards. This condition is clearly true for a $3k \times 3k$ square of pieces, but false for a single piece. Hence, we cannot reduce the arrangement to a single piece if $n$ is a multiple of 3.