Some unsolved problems in mathematics and computation

Sergi Elizalde

Dartmouth College

Odyssey Series - JHU Center for Talented Youth - 10/4/14

Mathematics is...

1. Universal

It is the same in any place of the world and in any time period.
Even an alien in a far-away planet would deduce the same mathematical theories.
Mathematical truths do not depend on physical experiments.

Mathematics is...

2. Useful

Mathematics turns out to be very useful in explaining our world. It plays an important role in physics, chemistry, biology, engineering, music, etc.

Mathematics is...

2. Useful

Mathematics turns out to be very useful in explaining our world. It plays an important role in physics, chemistry, biology, engineering, music, etc.

Mathematics can help solve many real-life problems:

- Determining how species evolved by looking at their DNA sequences.
- Sending secure information over the internet.
- Telling whether a painting is fake.
- Develop fast seach engines.

Mathematics is...

3. Exciting

It is fun to do mathematical research, and to solve problems that nobody has been able to solve before.

Mathematics is...

3. Exciting

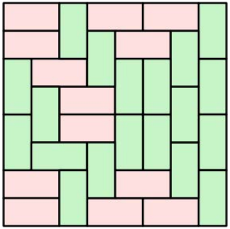
It is fun to do mathematical research, and to solve problems that nobody has been able to solve before.

4. A good choice!

In a recent survey of the best and worst jobs, Mathematician was ranked number 1.

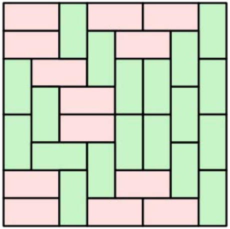
Tilings of a square

In how many ways can we tile an 8×8 board with dominoes?



Tilings of a square

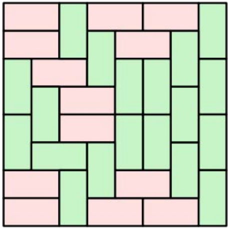
In how many ways can we tile an 8×8 board with dominoes?



Answer: $12,988,816$.

Tilings of a square

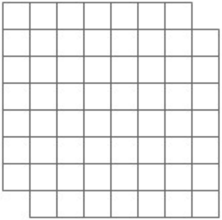
In how many ways can we tile an 8×8 board with dominoes?



Answer: $12,988,816$.
In general, a complicated formula is known for the number of ways to tile an $m \times n$ board.

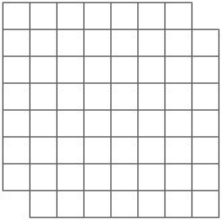
Tilings of a square

If we remove two opposite corners of the board, in how many ways can we tile it now with dominoes?



Tilings of a square

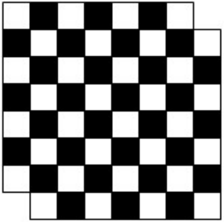
If we remove two opposite corners of the board, in how many ways can we tile it now with dominoes?



Answer: 0.

Tilings of a square

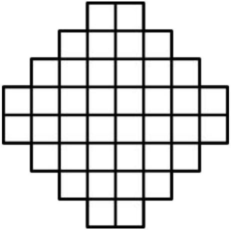
If we remove two opposite corners of the board, in how many ways can we tile it now with dominoes?



Answer: 0.
Coloring the squares as in a chessboard, each domino covers one square of each color, but there are more white squares in total.

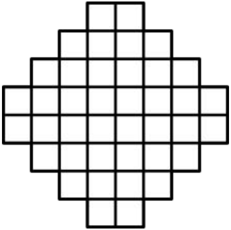
Tilings of an Aztec diamond

In how many ways can we tile the following figure using dominoes?



Tilings of an Aztec diamond

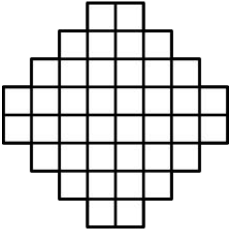
In how many ways can we tile the following figure using dominoes?



Answer: $1024 = 2^{10}$.

Tilings of an Aztec diamond

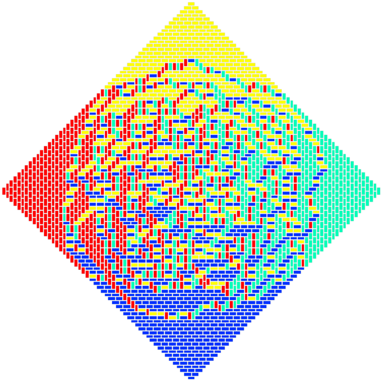
In how many ways can we tile the following figure using dominoes?



Answer: $1024 = 2^{10}$.
In general, for a similar diamond having n corners on each side, the number of tilings is $2^{n(n+1)/2}$.

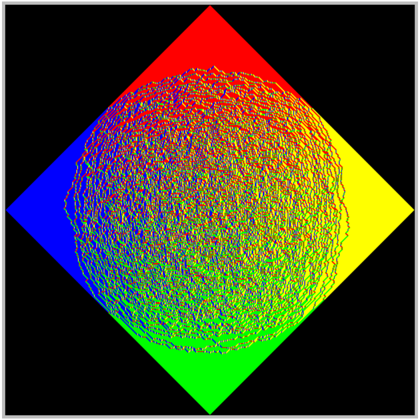
Tilings of an Aztec diamond

This is how a typical tiling of a large Aztec diamond looks like:



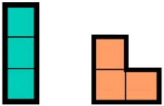
Tilings of an Aztec diamond

Here's an even larger one:



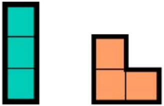
Polyominoes

Instead of dominoes, we can consider larger tiles. For example, trominoes are tiles formed with 3 little squares:

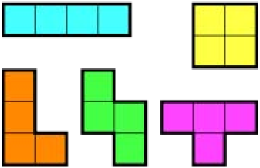


Polyominoes

Instead of dominoes, we can consider larger tiles. For example, trominoes are tiles formed with 3 little squares:



Tetrominoes are tiles formed with 4 squares:



Polyominoes

How many different polynominoes can we form with n squares?

# of squares	1	2	3	4	5	6	...	n	...
# of polyominoes	1	1	2	5	12	35	...		...

Polyominoes

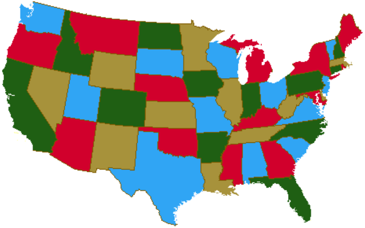
How many different polynominoes can we form with n squares?

# of squares	1	2	3	4	5	6	...	n	...
# of polyominoes	1	1	2	5	12	35	...	??	...

No formula is known!

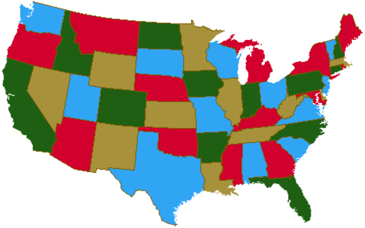
Coloring maps

How many colors are needed to color a map so that regions sharing a border get different colors?



Coloring maps

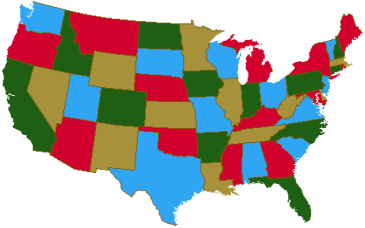
How many colors are needed to color a map so that regions sharing a border get different colors?



The Four-Color Theorem states that 4 colors always suffice, regardless of the map.

Coloring maps

How many colors are needed to color a map so that regions sharing a border get different colors?



The Four-Color Theorem states that 4 colors always suffice, regardless of the map.

Proving it took over a century of human effort and many hours of computer time.

The Millenium Prize Problems

In 2000, the Clay Mathematics Institute offered $\$1,000,000$ to anyone who could solve one of seven problems, considered to be among the main unsolved questions in mathematics.

The Millenium Prize Problems

In 2000, the Clay Mathematics Institute offered $\$1,000,000$ to anyone who could solve one of seven problems, considered to be among the main unsolved questions in mathematics.

One of the problems, called the *Poincaré Conjecture*, has been solved since then.

The Millenium Prize Problems

In 2000, the Clay Mathematics Institute offered $\$1,000,000$ to anyone who could solve one of seven problems, considered to be among the main unsolved questions in mathematics.

One of the problems, called the *Poincaré Conjecture*, has been solved since then.

The other six remain open problems. My favorite one is the so called *P versus NP* problem.

A simple example

Multiplication:

$$7 \times 13 = ?$$

A simple example

Multiplication:

$$7 \times 13 = ?$$

Answer: 91.

A simple example

Factoring:

$$? \times ? \ = 91$$

A simple example

Factoring:

$$? \times ? \ = 91$$

Answer: 7×13.

A bigger multiplication example

$$1,634,773,645,809,253,848,443,133,883,865,090,859,841,783,670,033,092,312,181,110,852,389,333,100,104,508,151,212,118,167,511,579 \times 1,900,871,281,664,822,113,126,851,573,935,413,975,471,896,789,968,515,493,666,638,539,088,027,103,802,104,498,957,191,261,465,571 = ?$$

A bigger multiplication example

$$\begin{array}{c} 1,634,773,645,809,253,848, \\ 443,133,883,865,090,859, \\ 841,783,670,033,092,312, \\ 181,110,852,389,333,100, \\ 104,508,151,212,118,167, \\ 511,579 \end{array} \times \begin{array}{c} 1,900,871,281,664,822,113 \\ 126,851,573,935,413,975 \\ 471,896,789,968,515,493, \\ 666,638,539,088,027,103, \\ 802,104,498,957,191,261, \\ 465,571 \end{array} = ?$$

Answer:

$$\begin{array}{c} 3,107,418,240,490,043,721,350,750,035,888,567,930,037, \\ 346,022,842,727,545,720,161,948,823,206,440,518,081, \\ 504,556,346,829,671,723,386,782,437,916,272,838,033, \\ 415,471,073,108,501,919,548,529,007,337,724,822,783, \\ 525,742,386,454,014,691,736,602,477,652,346,609 \end{array}$$

It took less than a second for a computer to find.

A bigger factoring example

$$? \times ? = \begin{array}{c} 3,107,418,240,490,043,721,350,750,035,888,567,930,037, \\ 346,022,842,727,545,720,161,948,823,206,440,518,081, \\ 504,556,346,829,671,723,386,782,437,916,272,838,033, \\ 415,471,073,108,501,919,548,529,007,337,724,822,783, \\ 525,742,386,454,014,691,736,602,477,652,346,609 \end{array}$$

A bigger factoring example

$$? \times ? = \begin{array}{c} 3,107,418,240,490,043,721,350,750,035,888,567,930,037, \\ 346,022,842,727,545,720,161,948,823,206,440,518,081, \\ 504,556,346,829,671,723,386,782,437,916,272,838,033, \\ 415,471,073,108,501,919,548,529,007,337,724,822,783, \\ 525,742,386,454,014,691,736,602,477,652,346,609 \end{array}$$

Answer:

$$\begin{array}{c} 1,634,773,645,809,253,848, \\ 443,133,883,865,090,859, \\ 841,783,670,033,092,312, \\ 181,110,852,389,333,100, \\ 104,508,151,212,118,167, \\ 511,579 \end{array} \times \begin{array}{c} 1,900,871,281,664,822,113 \\ 126,851,573,935,413,975 \\ 471,896,789,968,515,493, \\ 666,638,539,088,027,103, \\ 802,104,498,957,191,261, \\ 465,571 \end{array}$$

It took 20 computer-years of effort to find.

For \$30,000, factor:

$$74,037,563,479,561,712,828,046,796,097,429,573,142,593,188,889,231,289,084,936,232,638,972,765,034,028,266,276,891,996,419,625,117,843,995,894,330,502,127,585,370,118,968,098,286,733,173,273,108,930,900,552,505,116,877,063,299,072,396,380,786,710,086,096,962,537,934,650,563,796,359$$

For \$30,000, factor:

$$74,037,563,479,561,712,828,046,796,097,429,573,142,593,188,889,231,289,084,936,232,638,972,765,034,028,266,276,891,996,419,625,117,843,995,894,330,502,127,585,370,118,968,098,286,733,173,273,108,930,900,552,505,116,877,063,299,072,396,380,786,710,086,096,962,537,934,650,563,796,359$$

See the *RSA Factoring Challenge* for details and payment.

For \$30,000, factor:

$$74,037,563,479,561,712,828,046,796,097,429,573,142,593,188,889,231,289,084,936,232,638,972,765,034,028,266,276,891,996,419,625,117,843,995,894,330,502,127,585,370,118,968,098,286,733,173,273,108,930,900,552,505,116,877,063,299,072,396,380,786,710,086,096,962,537,934,650,563,796,359$$

See the *RSA Factoring Challenge* for details and payment.

Factoring is an essential ingredient in modern cryptography.

What's so hard about factoring?

One can divide by $2, 3, 5, 7, 11, \ldots$ until one finds a factor.

What's so hard about factoring?

One can divide by $2, 3, 5, 7, 11, \ldots$ until one finds a factor.

However, this method (brute force search) is very slow when the search space is huge.

What's so hard about factoring?

One can divide by $2, 3, 5, 7, 11, \ldots$ until one finds a factor.

However, this method (brute force search) is very slow when the search space is huge.

Is searching necessary?

What's so hard about factoring?

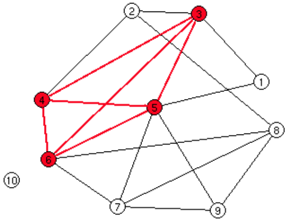
One can divide by $2, 3, 5, 7, 11, \ldots$ until one finds a factor.

However, this method (brute force search) is very slow when the search space is huge.

Is searching necessary? We don't know.

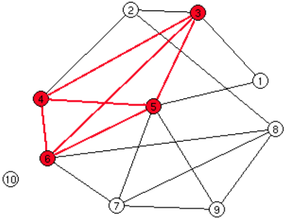
Another example: finding a clique

This graph contains a clique of size 4.



Another example: finding a clique

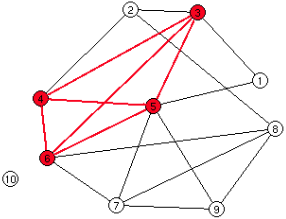
This graph contains a clique of size 4.



For a graph with 100 nodes, finding whether it contains a clique of size 10 may take centuries of computer time by searching.

Another example: finding a clique

This graph contains a clique of size 4.

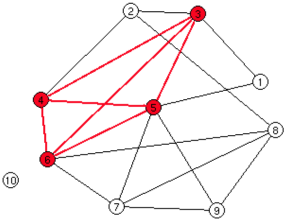


For a graph with 100 nodes, finding whether it contains a clique of size 10 may take centuries of computer time by searching.

Is searching necessary?

Another example: finding a clique

This graph contains a clique of size 4.



For a graph with 100 nodes, finding whether it contains a clique of size 10 may take centuries of computer time by searching.

Is searching necessary? We don't know.

The P versus NP question

- P "polynomial time"
  Quickly solvable problems, such as multiplication.
- NP "nondeterministic polynomial time"
  Quickly checkable problems, such as factoring or clique-finding.

The P versus NP question

- P "polynomial time"
  Quickly solvable problems, such as multiplication.
- NP "nondeterministic polynomial time"
  Quickly checkable problems, such as factoring or clique-finding.

Is $\mathrm{P} = \mathrm{NP}$?
In other words, can we solve search problems without searching?

The P versus NP question

- P "polynomial time"
  Quickly solvable problems, such as multiplication.
- NP "nondeterministic polynomial time"
  Quickly checkable problems, such as factoring or clique-finding.

Is $P = NP$?
In other words, can we solve search problems without searching?

Most people believe that $P \neq NP$, but nobody knows for sure.


That's all Folks!