# What is a Proof? — Some Challenges for Automated Theorem Proving

Dana S. Scott
University Professor Emeritus
Carnegie Mellon University
Visiting Scholar
University of California, Berkeley

## Some Quotations

# What is a Proof?

"Proofs really aren't there to convince you something is true — they're there to show you *why* it is true."

— Andrew Gleason

# Do We Need Proofs?

"Logic, Padoa says, is not in a particularly fortunate position. On the one hand, philosophers prefer to speak of it *without using it*, while on the other hand mathematicians prefer to use it *without speaking of it* — and even without desiring *to hear it spoken of*."

— C.H. Langford (1937)

# Are Proofs Good for You?

“There is a real conflict between the logician's goal and the educator's. The logician wants to minimize the variety of ideas and doesn't mind a long, thin path. The educator (rightly) wants to make paths short and doesn't mind — in fact, prefers — connections to many of other ideas. And he cares almost nothing about the direction of the link.”

— Marvin Minsky
“Form and Content in Computer Science” (1970)

# Logic and Computation?

"It is reasonable to hope that the relationship between ***computation*** and ***mathematical logic*** will be as fruitful in the next century as that between analysis and physics in the last. The development of this relationship demands a concern for both applications and for mathematical elegance."

— John McCarthy

# Automated Deduction?

"Despite the significant advances automated reasoning has seen over the past decades, the impact of automated reasoning on the practice of doing ***mathematics*** is small."

— Bruno Buchberger (IJCAR 2006)

# Future Coming Soon?

"Today it is state of the art that hardware manufacturers have complete formal models of processors and verify much of their functionality. Thanks to theorem provers the same level of formality will in the future be applied to ***core software components*** like programming languages and compilers."

— Tobias Nipkow (2006)

# Verifying the Verifiers?

“The HOL Light prover is based on a logical kernel consisting of about 400 lines of mostly functional OCaml, whose complete formal verification seems to be quite feasible. We would like to formally verify

(i) that the abstract logic HOL is supposed to implement is indeed correct, and
(ii) that the OCaml code does correctly implement this logic.”

— John Harrison (IJCAR 2006)
Towards self-verification of HOL Light

# The Question We Should Ask

**Q: What is needed for great computer proofs?**

**A: Better *interfaces* to users, to special purpose devices, and to better *libraries*.**

# Scott's Thesis

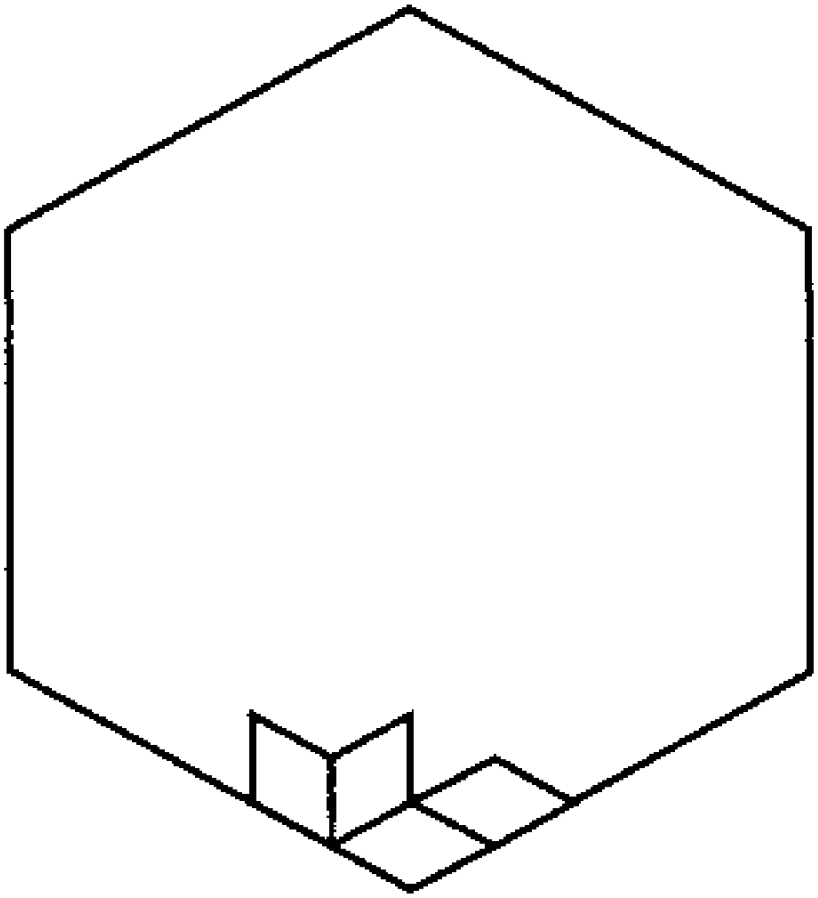
Mathematics does not progress just by searching for ***longer and longer proofs***!

Advances come by finding attractive ***new concepts*** and by uncovering interesting ***new problems***.

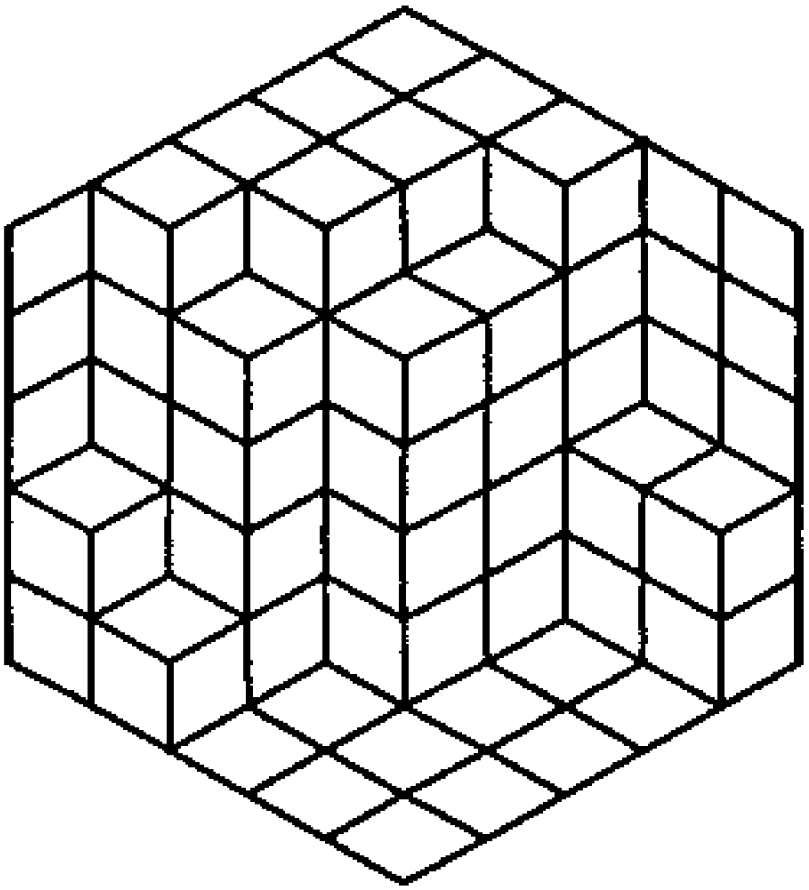
This is done by ***people*** (not machines) steeped in mathematical ***culture***.

## Filling the Box

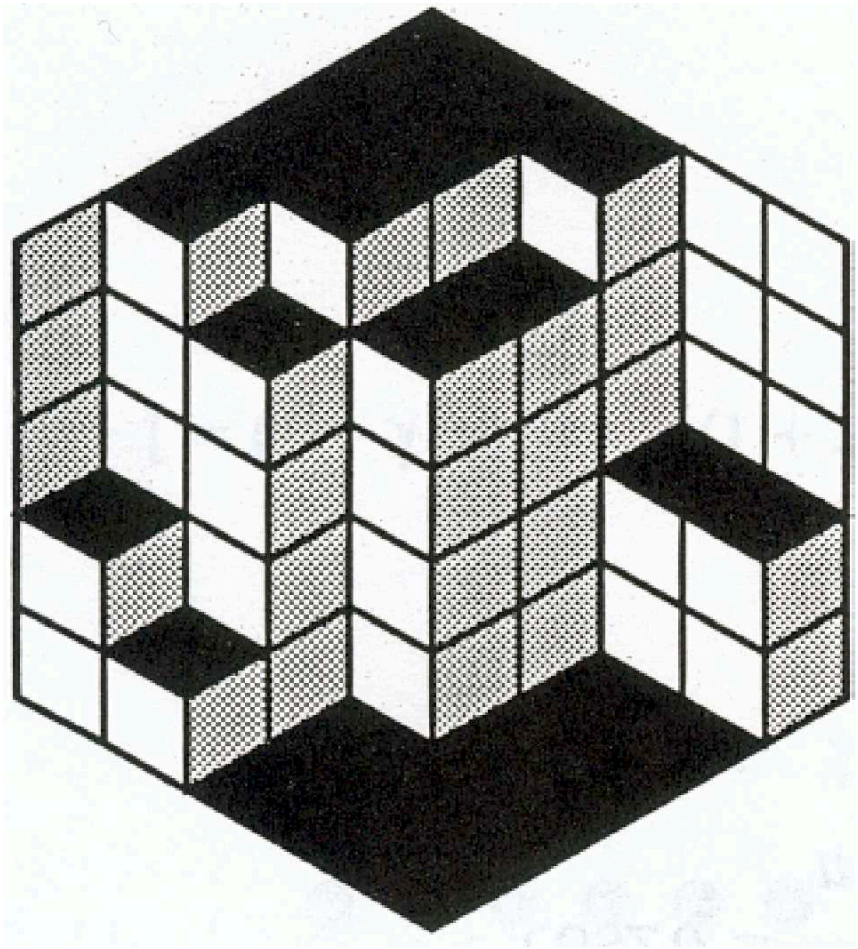
**How can the box be filled with rhombi?  Note the three orientations.**



**However you do it, there are the *same number* of each kind!**



## Is this a *proof*?



## References

G. David and C. Tomei. ***The problem of the calissons***, American Mathematical Monthly, vol. 96 (1989), pp. 429–431.

The late Prof. Dr. Edsger W. Dijkstra in his handwritten, privately circulated note, EWD 1055, of 5 July, 1989, strongly rejected this method of argument. He writes that they "give a very unsatisfactory treatment of the problem ... [and] come up with an elaborate non proof." His note gives a rigorous proof, but it is perhaps one that would need some effort to automate. Dijkstra's notes can be downloaded over the internet.

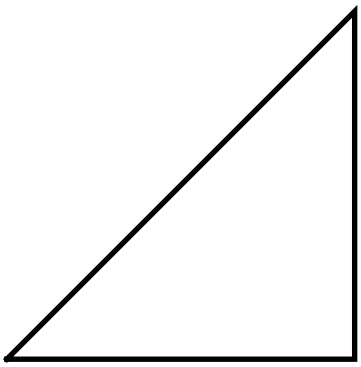
Prof. N.G. de Bruijn has also written on this problem at: `alexan-`

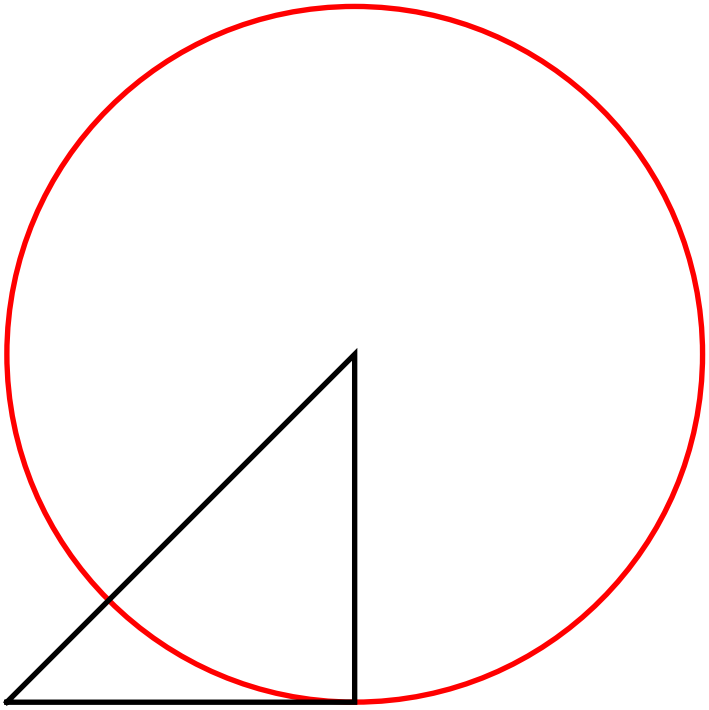
dria.tue.nl/repository/freearticles/599882.pdf.

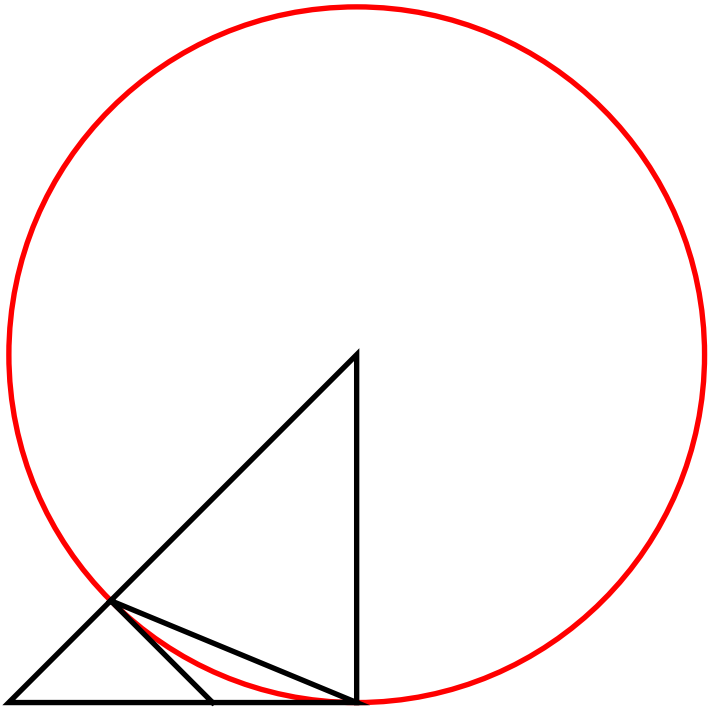
This puzzle is only one of many amusing tiling problems which show that even simple combinatorial questions require special techniques to automate owing to the large number of possible configurations to be considered, as many authors have remarked. And they make us again ask: “What is a proof?”

## The Square Root of 2 is Irrational

### Proof by lengths (suggested by Tom Apostol)





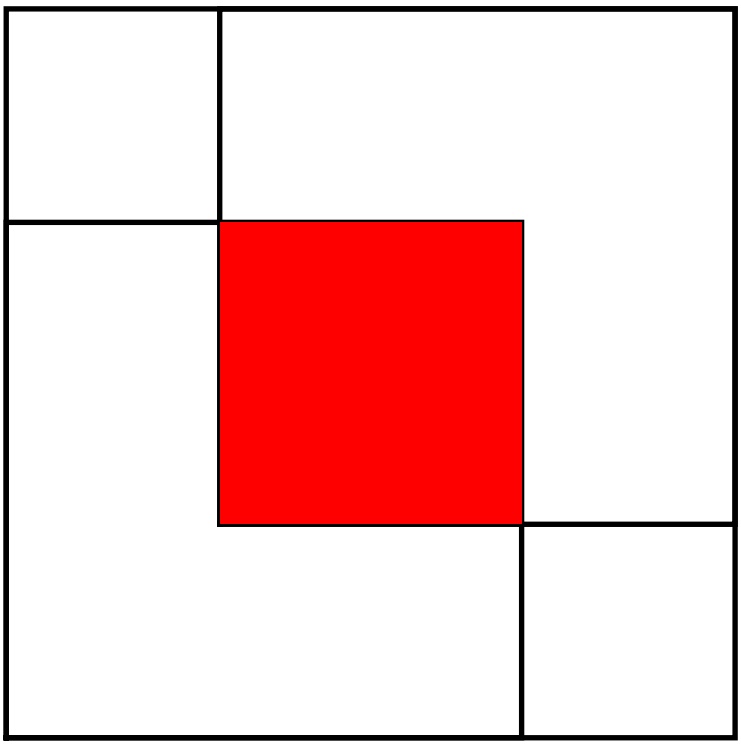


**In words: if you have an integral example, you can find a smaller one.**

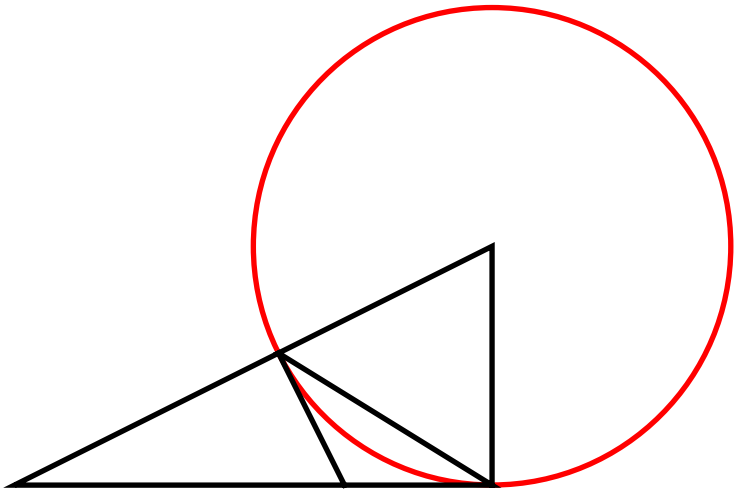
## The algebra

$$2\,a^2 == b^2 \Longrightarrow 2\,(b-a)^2 == (2\,a-b)^2$$

## Proof by areas (suggested by Stanley Tennenbaum)



## Generalization to Square Root of 5 (suggested by Dana Scott)



Call the short leg a and the hypotenuse b. Then $5\,a^2 == b^2$. Thus, if integral, a and b are either both ***even*** or both ***odd***. Hence, b - a is ***even***.

### The algebra

$$5\,a^2 == b^2 \Longrightarrow 5\left(\frac{b-a}{2}\right)^2 == \left(2\,a - \frac{b-a}{2}\right)^2$$

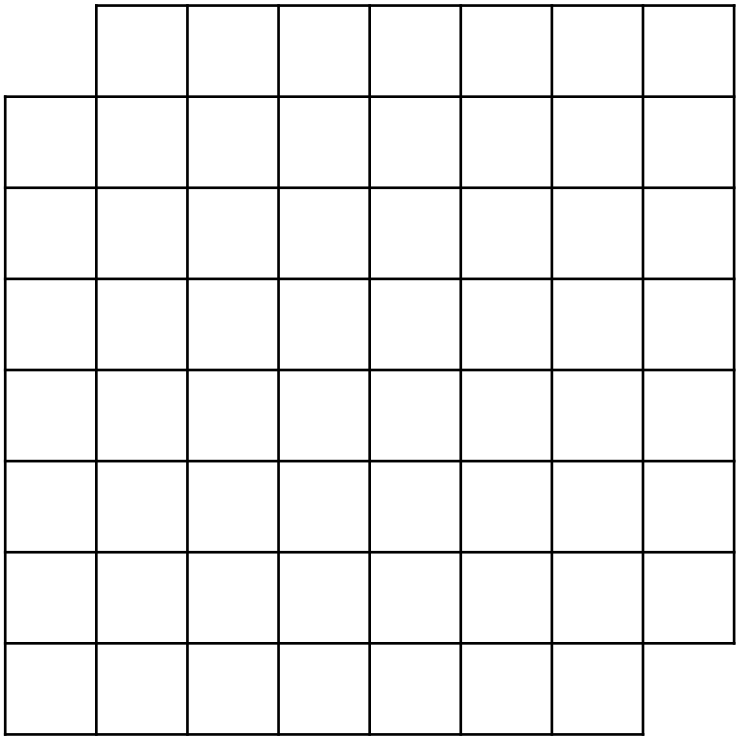
**Can such algebraic deductions be discovered automatically?**

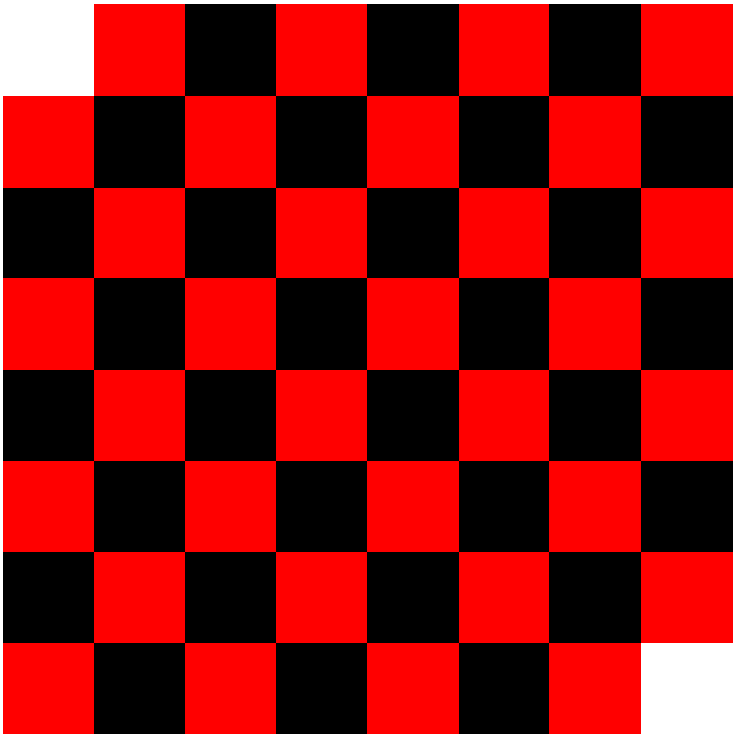
# Tiling with Dominoes

## A very old problem

Can the ***mutilated checkerboard*** (that is, with a pair of ***opposite corners missing***) be ***tiled by dominoes***?

Now, each domino (whether vertical or horizontal) will cover ***one red square*** and ***one black square***. And, in the ***whole*** checkerboard, there are ***as many*** blacks as reds. However, in the ***mutilated*** board, there are ***fewer*** blacks than reds.





# Can such a coloring be discovered automatically?

## Monomials and shape polynomials

Consider all the algebraic ***monomials*** $x^i y^j$ in two variables. We can arrange a limited number of them in the form of a rectangular matrix:

```
Mono[n_, m_][x_, y_] := Table[x^i y^j, {i, 0, n - 1}, {j, 0, m - 1}];
MatrixForm[Mono[8, 8][x, y]]
```

$$\begin{pmatrix} 1 & y & y^2 & y^3 & y^4 & y^5 & y^6 & y^7 \\ x & x\,y & x\,y^2 & x\,y^3 & x\,y^4 & x\,y^5 & x\,y^6 & x\,y^7 \\ x^2 & x^2\,y & x^2\,y^2 & x^2\,y^3 & x^2\,y^4 & x^2\,y^5 & x^2\,y^6 & x^2\,y^7 \\ x^3 & x^3\,y & x^3\,y^2 & x^3\,y^3 & x^3\,y^4 & x^3\,y^5 & x^3\,y^6 & x^3\,y^7 \\ x^4 & x^4\,y & x^4\,y^2 & x^4\,y^3 & x^4\,y^4 & x^4\,y^5 & x^4\,y^6 & x^4\,y^7 \\ x^5 & x^5\,y & x^5\,y^2 & x^5\,y^3 & x^5\,y^4 & x^5\,y^5 & x^5\,y^6 & x^5\,y^7 \\ x^6 & x^6\,y & x^6\,y^2 & x^6\,y^3 & x^6\,y^4 & x^6\,y^5 & x^6\,y^6 & x^6\,y^7 \\ x^7 & x^7\,y & x^7\,y^2 & x^7\,y^3 & x^7\,y^4 & x^7\,y^5 & x^7\,y^6 & x^7\,y^7 \end{pmatrix}$$

The `i` indexes a ***row***, and the `j` indexes a ***column***. Note that the indexing naturally starts counting from `0`.

We have shown an **8 × 8** arrangement above, but we could use any dimensions. In other words, the monomial $x^i y^j$ is just a place-holder for the ***square*** with corner coordinates **{i, j}**, assuming we put **{0, 0}** in the upper, left corner, and move ***down*** in the **x**-direction as **i** ***increases***.

# So, we have an ***algebraic notation*** for the checkerboard (and any rectangular board).

**Warning.** This indexing above is the ***matrix convention*** on indexing, not the ***graphing convention*** used in the Calculus. Often indices for matrices start counting from **1** rather than from **0**.

We can also ***sum up*** all these monomials to form a ***rectangular polynomial***:

```
RP[n_, m_][x_, y_] := Sum_{i=0}^{n-1} Sum_{j=0}^{m-1} x^i y^j;

RP[8, 8][x, y]
```

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + y + x\,y + x^2\,y + x^3\,y + x^4\,y + x^5\,y + x^6\,y + x^7\,y + y^2 + x\,y^2 + x^2\,y^2 + x^3\,y^2 + x^4\,y^2 + x^5\,y^2 + x^6\,y^2 + x^7\,y^2 + y^3 + x\,y^3 + x^2\,y^3 + x^3\,y^3 + x^4\,y^3 + x^5\,y^3 + x^6\,y^3 + x^7\,y^3 + y^4 + x\,y^4 + x^2\,y^4 + x^3\,y^4 + x^4\,y^4 + x^5\,y^4 + x^6\,y^4 + x^7\,y^4 + y^5 + x\,y^5 + x^2\,y^5 + x^3\,y^5 + x^4\,y^5 + x^5\,y^5 + x^6\,y^5 + x^7\,y^5 + y^6 + x\,y^6 + x^2\,y^6 + x^3\,y^6 + x^4\,y^6 + x^5\,y^6 + x^6\,y^6 + x^7\,y^6 + y^7 + x\,y^7 + x^2\,y^7 + x^3\,y^7 + x^4\,y^7 + x^5\,y^7 + x^6\,y^7 + x^7\,y^7$$

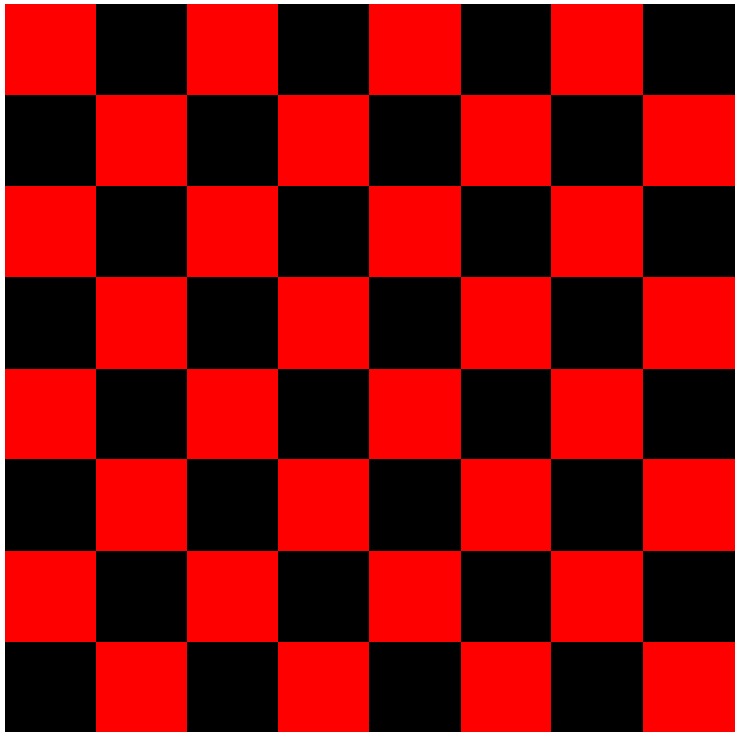
**Important Observation.** This polynomial contains the ***same information*** as the matrix of monomials. And ***any polynomial*** with coefficients all **1**s represents ***some*** 2-dimensional configuration of squares (not just rectangles).

**Definition.** We call this the ***shape polynomial*** of the configuration.

**Note.** The substitution of **-1** for the variables **x** and **y** in the ***matrix*** results in the familiar ***checkerboard pattern*** (where we interpret **1** as ***black*** and **-1** as ***red***). Here it is in the **8 × 8** case. Why is this true in general?

```
mat = Mono[8, 8][-1, -1];
MatrixForm[mat]
ShowMatrix[mat + 2, ColorRule[2]];
```

$$\begin{pmatrix} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$



The ***shape polynomial***, on the other hand, ***vanishes***, for this substitution. (Why?)

```
RP[8, 8][-1, -1]
```

```
0
```

This is, in fact, an automatic ***algebraic verification*** that there are the same number of ***reds*** as ***blacks*** in the checkerboard. (Why?)

The vanishing of the polynomial can be seen in another way if we ***factor*** it:

```
Factor[RP[8, 8][x, y]]
```

$$(1+x)\left(1+x^2\right)\left(1+x^4\right)(1+y)\left(1+y^2\right)\left(1+y^4\right)$$

Now, the shape polynomial representing the ***mutilated checkerboard*** is computed as follows;

```
MCB = RP[8, 8][x, y] - 1 - x^7 y^7
```

$$\begin{aligned}&x+x^2+x^3+x^4+x^5+x^6+x^7+y+x\,y+x^2\,y+x^3\,y+x^4\,y+x^5\,y+x^6\,y+x^7\,y+\\&\ y^2+x\,y^2+x^2\,y^2+x^3\,y^2+x^4\,y^2+x^5\,y^2+x^6\,y^2+x^7\,y^2+y^3+x\,y^3+x^2\,y^3+x^3\,y^3+\\&\ x^4\,y^3+x^5\,y^3+x^6\,y^3+x^7\,y^3+y^4+x\,y^4+x^2\,y^4+x^3\,y^4+x^4\,y^4+x^5\,y^4+x^6\,y^4+\\&\ x^7\,y^4+y^5+x\,y^5+x^2\,y^5+x^3\,y^5+x^4\,y^5+x^5\,y^5+x^6\,y^5+x^7\,y^5+y^6+x\,y^6+x^2\,y^6+\\&\ x^3\,y^6+x^4\,y^6+x^5\,y^6+x^6\,y^6+x^7\,y^6+y^7+x\,y^7+x^2\,y^7+x^3\,y^7+x^4\,y^7+x^5\,y^7+x^6\,y^7\end{aligned}$$

Clearly, it ***does not*** vanish under the substitution. (Why?)

```
MCB /.{x → -1, y → -1}
```

$$-2$$

## Dominoes as polynomials

Now, the two ***dominoes*** (horizontal and vertical) are of course represented by these shape polynomials.

```
RP[1, 2][x, y]
RP[2, 1][x, y]
```

$$1+y$$

$$1+x$$

**Question.** What does this next polynomial represent?

```
Expand[x^i y^j (1 + y)]
```

```
x^i y^j + x^i y^(1+j)
```

**Answer.** It represents the ***horizontal*** domino ***translated over*** so its first square starts at matrix position `{i, j}` rather than `{0, 0}`. And we can supply a similar interpretation for the polynomial `x^i y^j (1 + x)`.

**Next Question.** What does a polynomial `A (1 + x) + B (1 + y)` represent, where `A` and `B` are ***arbitrary*** polynomials (say, with coefficients just `0` and `1`) in `x` and `y`?

**Answer.** It represents ***many copies*** of the two dominoes placed at different positions.

So, if we expand `A (1 + x) + B (1 + y)` and find no coefficients greater that `1`, then we know that the copies of the dominoes are ***non overlapping***.

***Therefore,*** a true algebraic equation of the form

$$A\,(1 + x) + B\,(1 + y) == RP[8, 8][x, y] - 1 - x^7\,y^7$$

would result if we had a tiling of the mutilated checkerboard.

However, there can be ***no*** true equation of this form, because obviously the left-hand side vanishes under the substitution `{x → -1, y → -1}`, while the right-hand side does not. **QED**

## Commentary

This is really the "same" proof as the old ***black/red*** coloring proof, but—in this algebraic form—very little ***discovery*** is needed to find the argument. Indeed, the polynomial `RP[8, 8][x, y]` is just a ***notation*** for the ***checkerboard***, and the polynomial `A (1 + x) + B (1 + y)` is just a ***notation*** for a desired ***configuration of dominoes***.

But, as soon as we have adopted the ***algebraic language***, we see that the polynomial for the configuration ***vanishes*** for an ***obvious substitution***. So it is natural to try out the mutilated polynomial under that substitution, and we find it ***does not vanish***.

In other words, a very ***mechanical*** application of algebra has done all the work in checking that the mutilated checkerboard has ***more reds than blacks***. No special insight was needed, once the algebraic formulation was fixed.

***So what?*** The main point is that this method is open to ***considerable generalization*** to other problems. For example:

If `S[x,y]` is any shape polynomial, then the equation

$$A\left(1 + x + x^2\right) + B\left(1 + y + y^2\right) == S[x, y]$$

has a solution in polynomials with non-negative coefficients iff the shape can be covered with straight ***trominoes***. Perhaps ***complex numbers*** can be used as substitutions.

**Reference:** This method of using polynomials is written up in the book

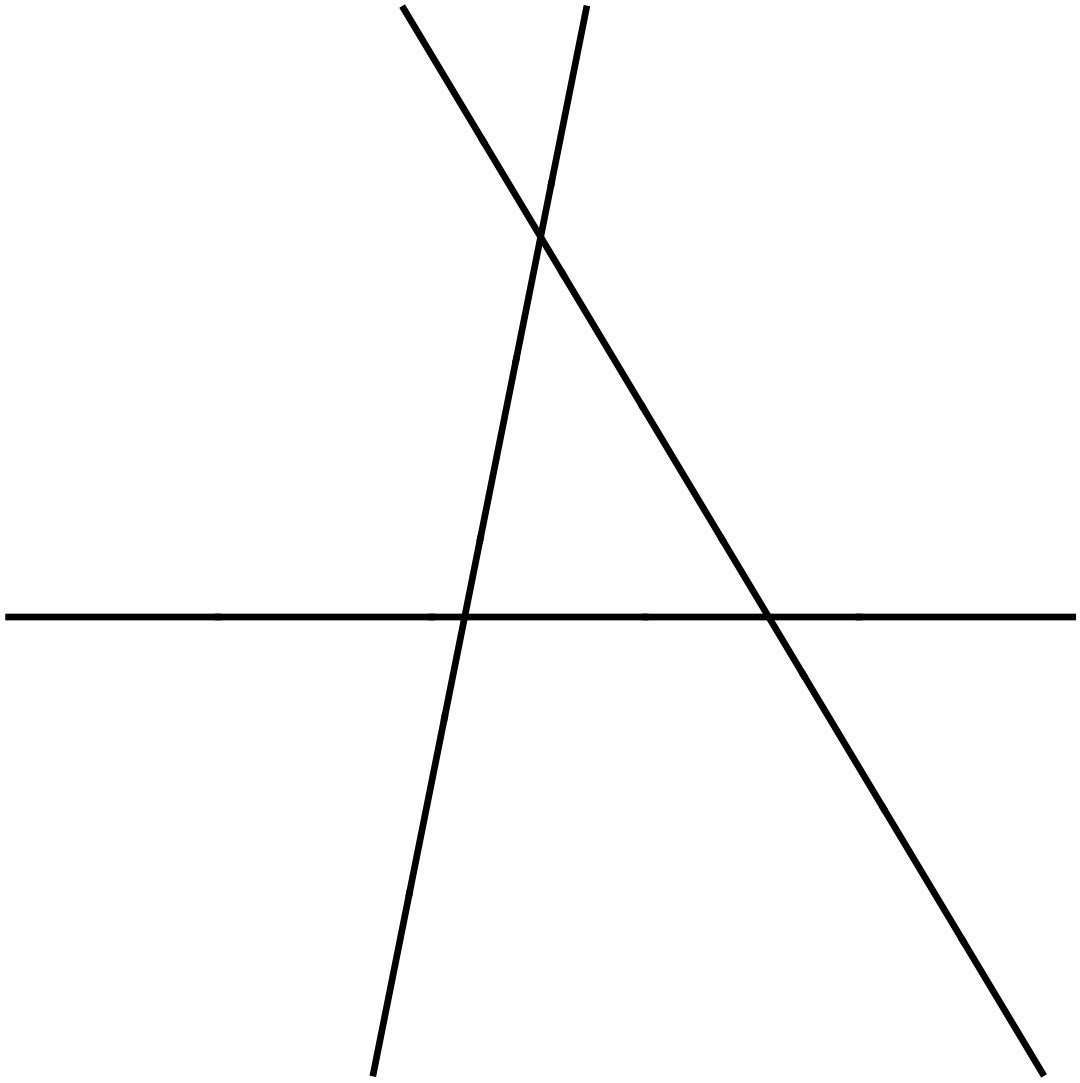
"***Algebra and Tiling: Homomorphisms in the Service of Geometry***"

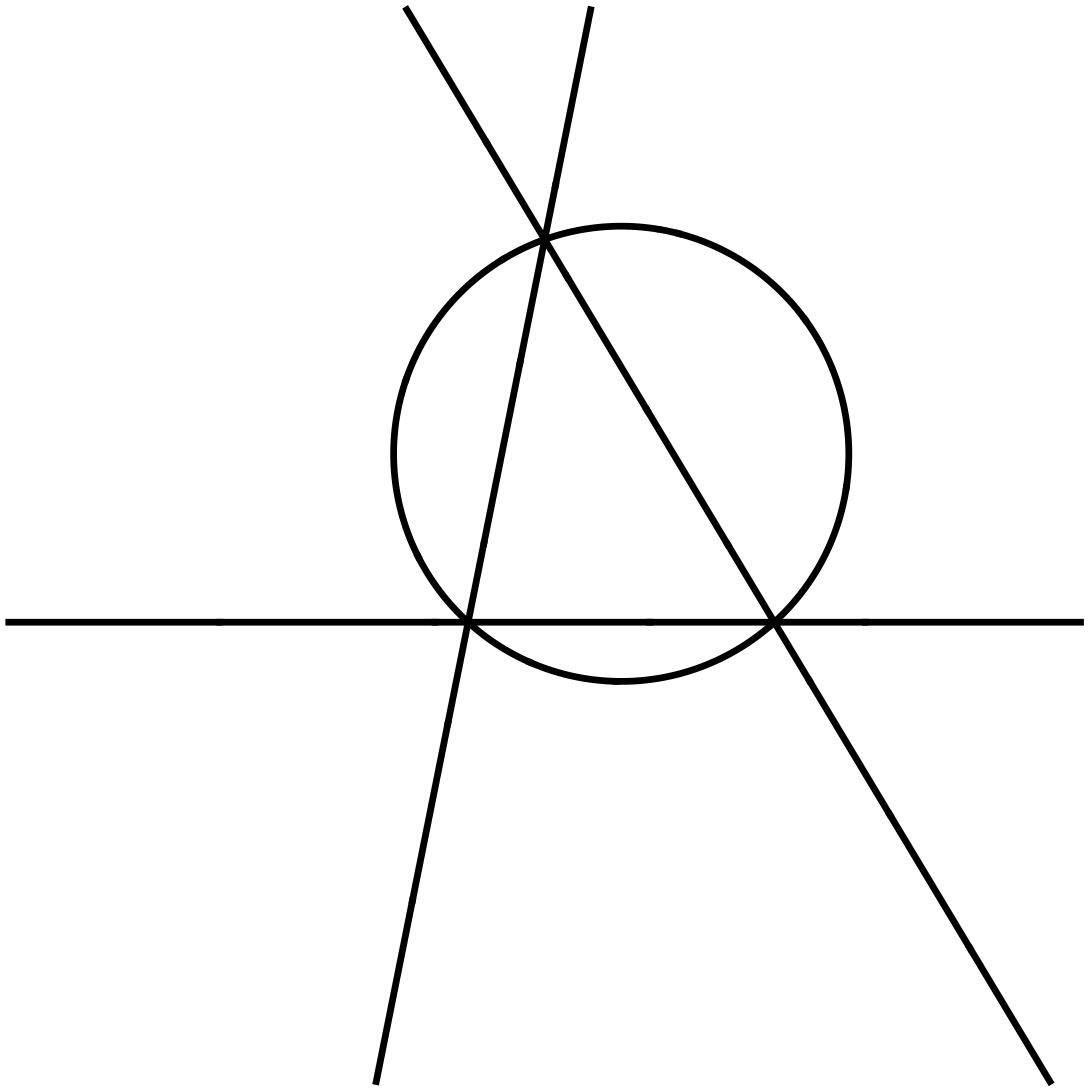
by Sherman Stein and Sandor Szabo, MAA 1994, 224 pp.

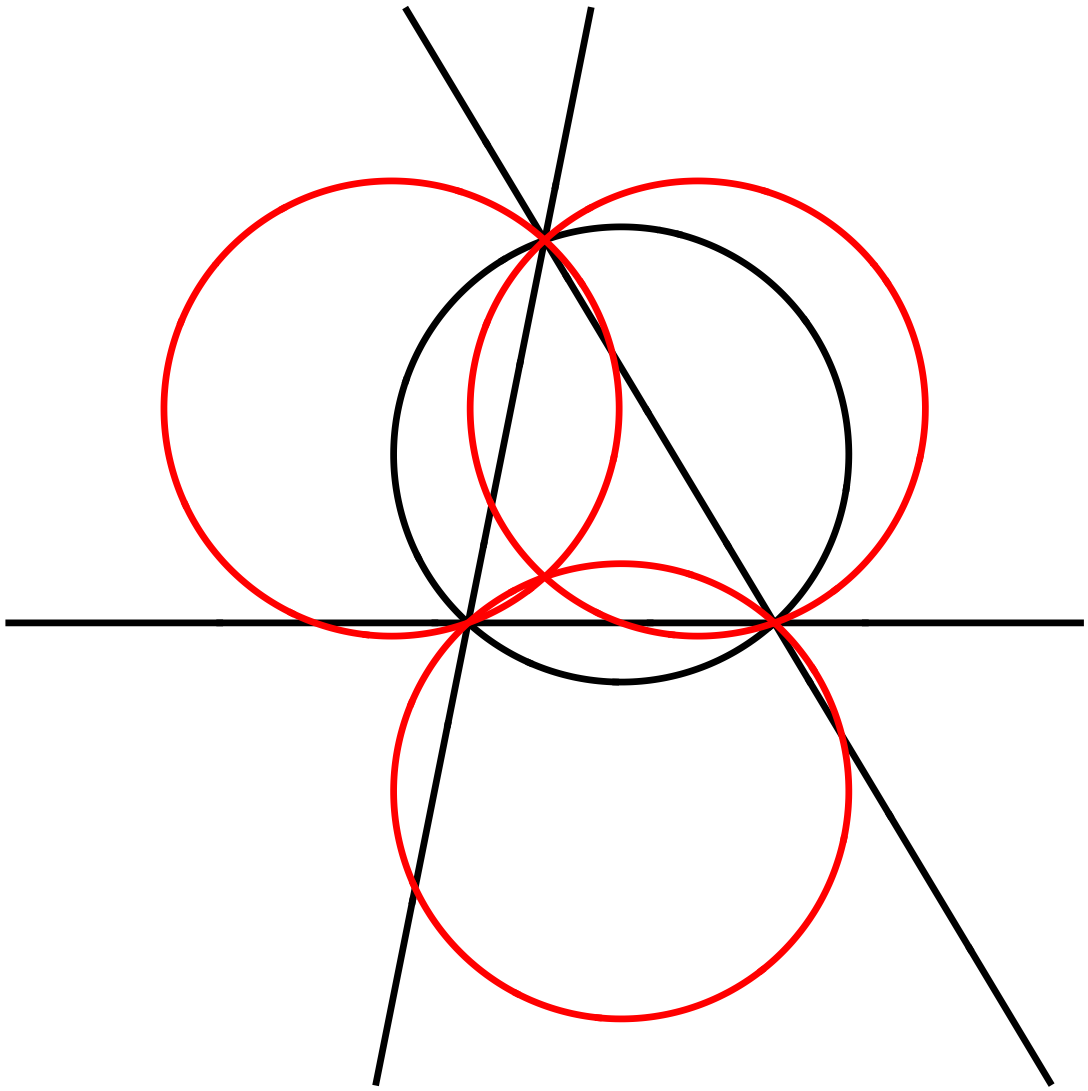
## Triangle Reflections

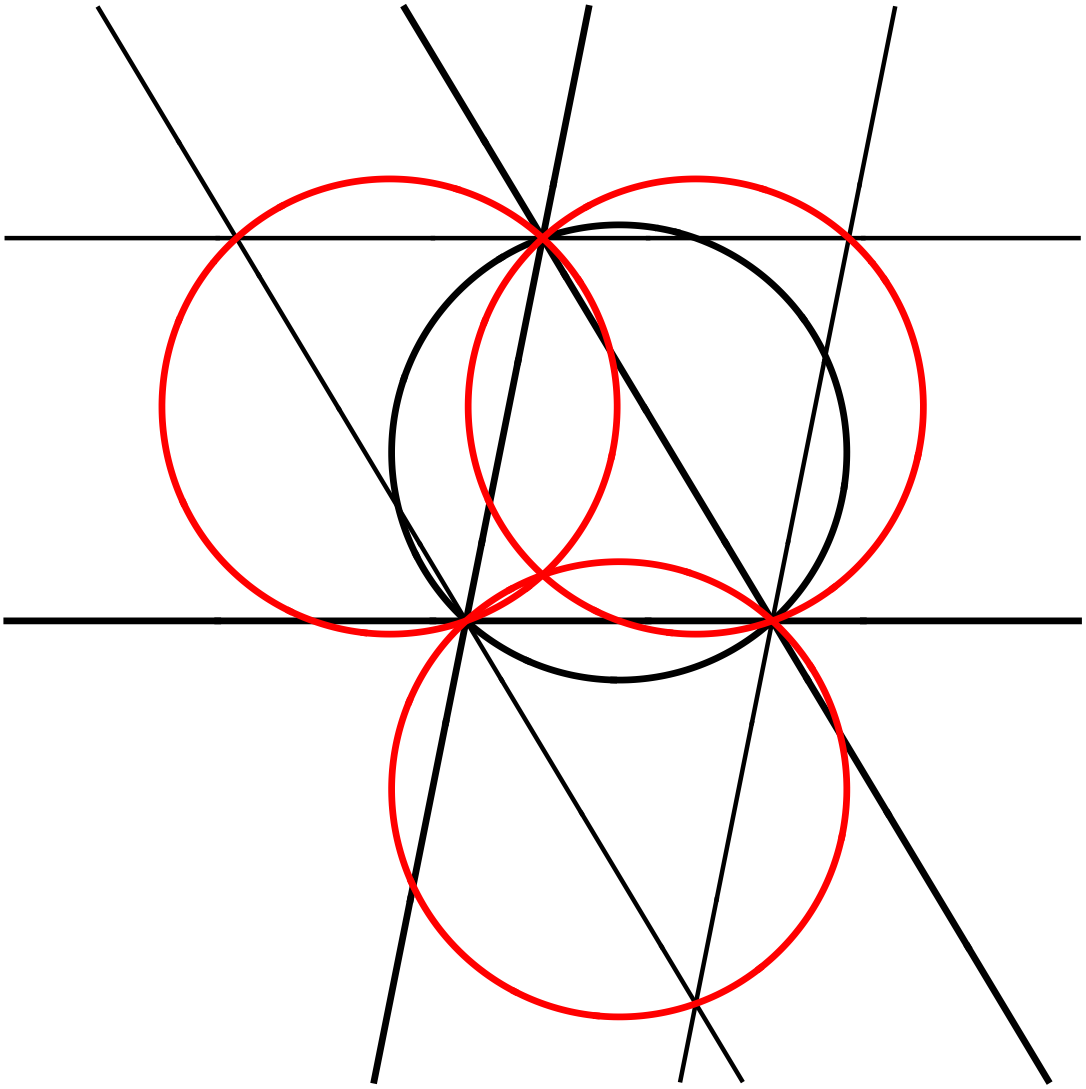
**Theorem.** The three circles resulting from the ***reflections*** of the ***circumscribed circle*** of a triangle in the sides of the triangle meet at a ***common point***.

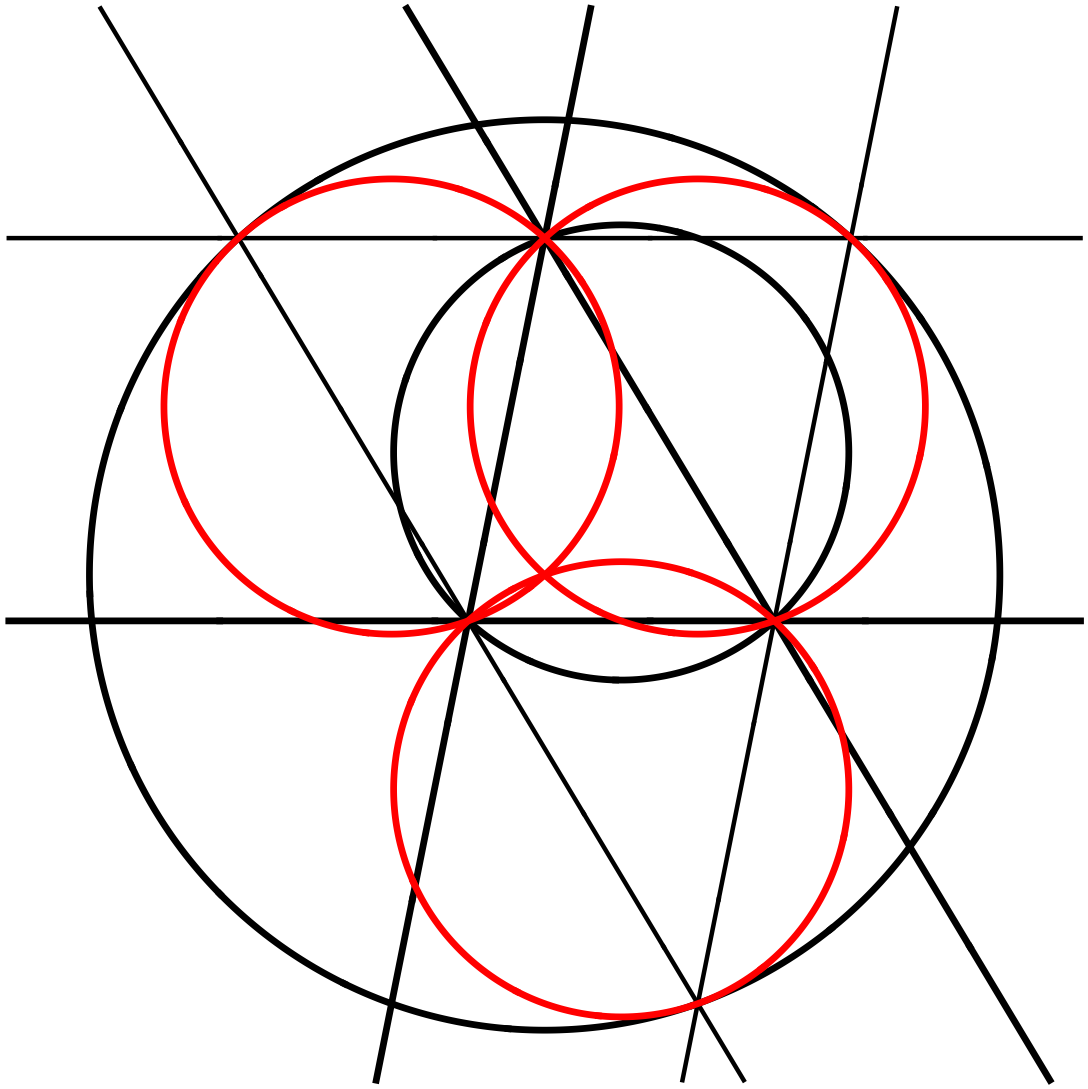
# First Proof (Euclidean Style)

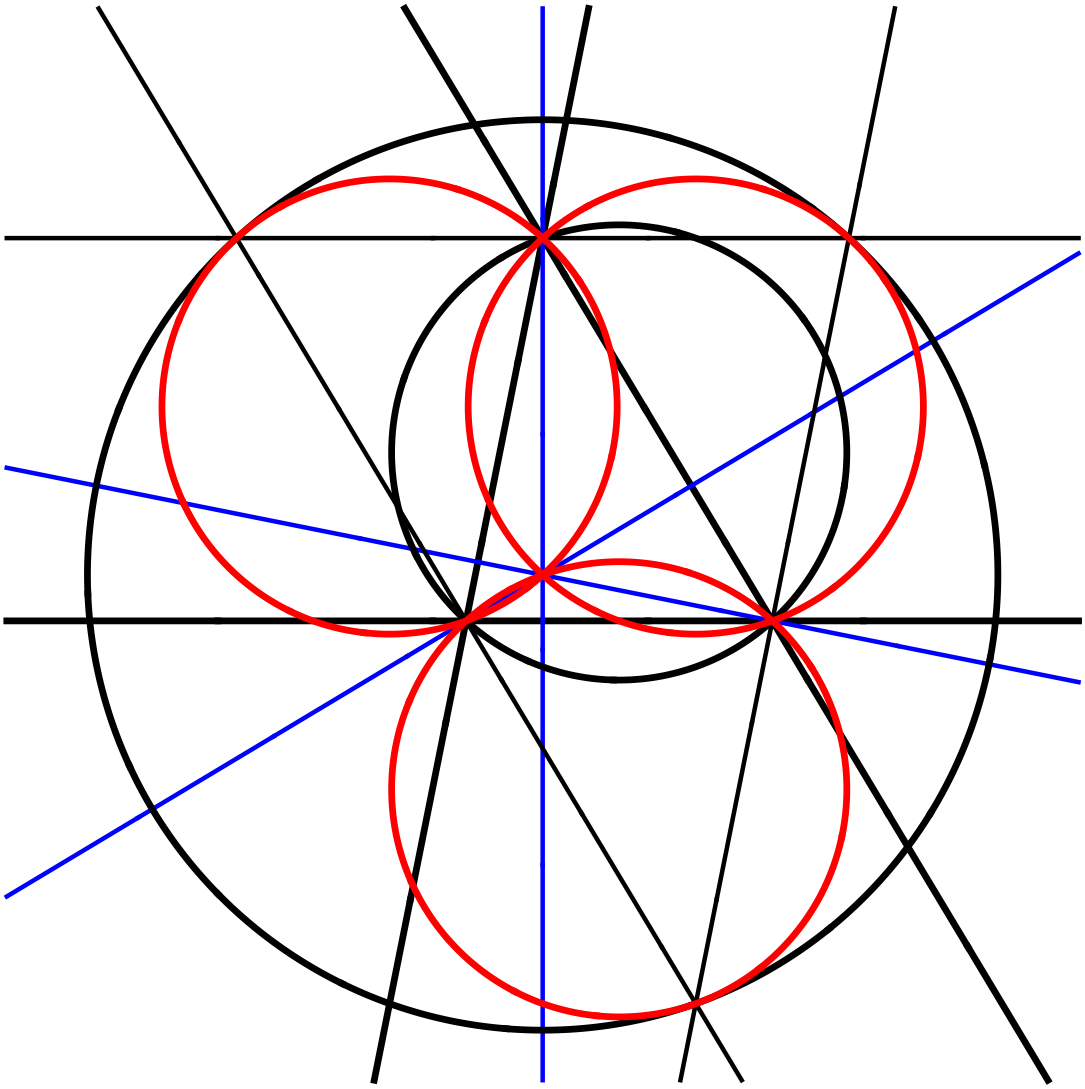




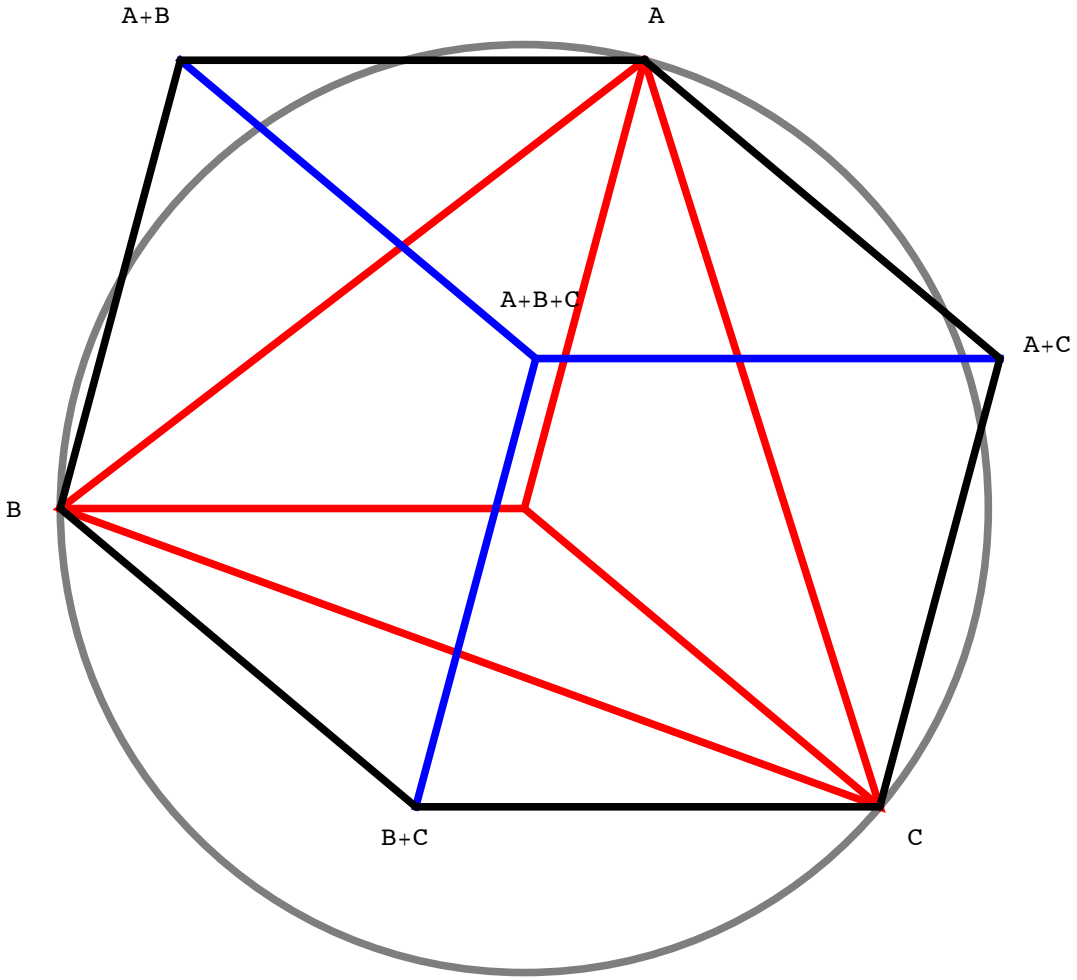








# Another Proof (by Vectors)




## ■ Those altitudes

The vector from A to A+B+C is B+C.

The vector from C to B is B–C.

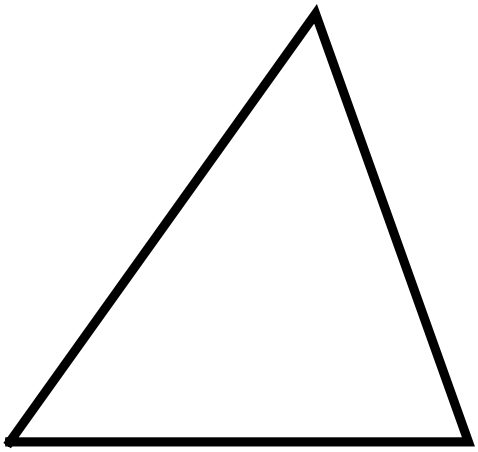
The dot product is (B+C).(B–C) = B.B–C.C = 0. (Why?)

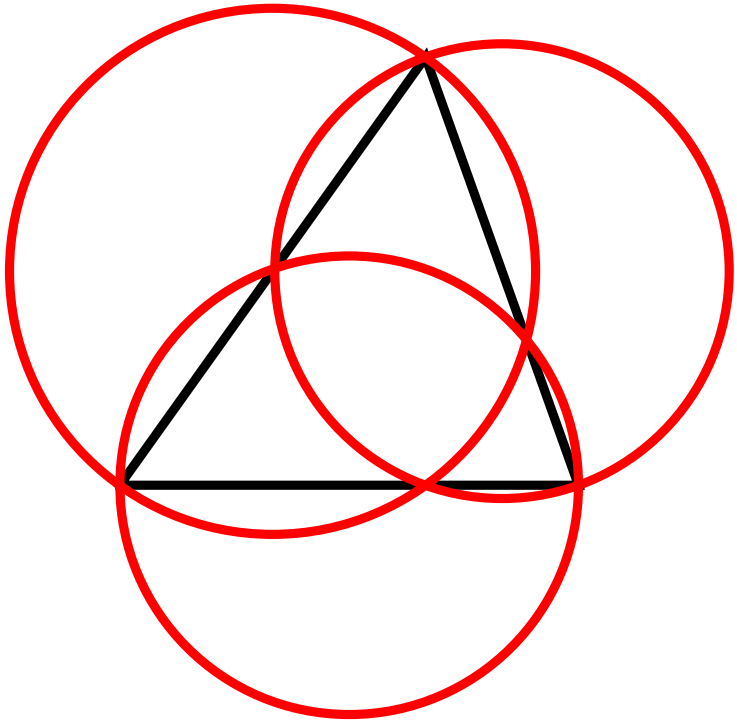
Therefore, the *point* A+B+C is the *intersection of the altitudes*. (Why?)

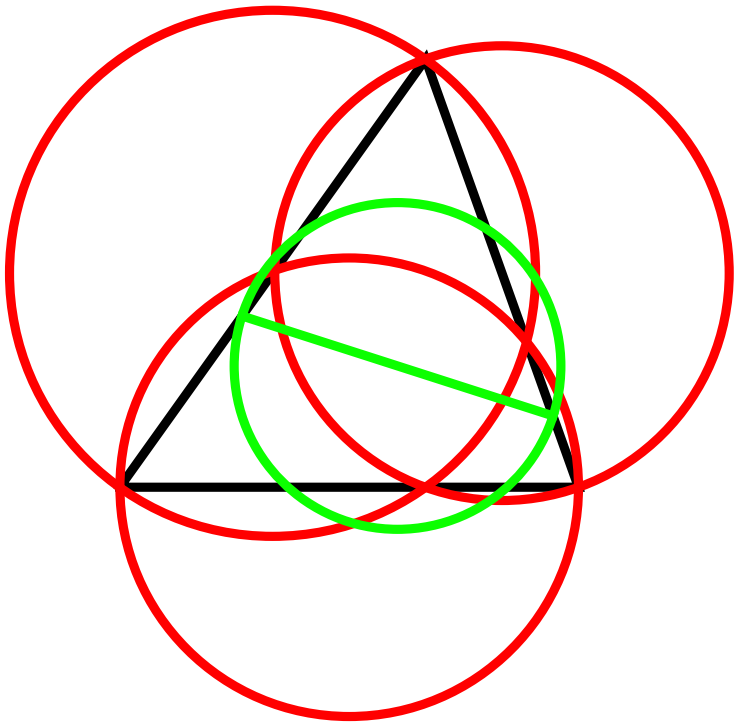
## Disk Covering

### The Problem

**Theorem.** Place three circular disks on a triangle using the sides as ***diameters***. Then any other disk with a diameter lying inside (or on) the triangle is ***covered*** by the union of the three original disks. **(Suggested by Gary Miller, CMU.)**







## Proof by Vector Algebra

**Lemma**. Let `X = {x, y}` be a variable point, and let `P` and `Q` be fixed points. Then the ***equation*** of the ***circle*** with the segment `PQ` as a diameter can be written in vector notation as:

`(X - P) . (X - Q) = 0`. (Why?)

Moreover, the ***interior*** of the circle is characterized by the ***inequality***:

`(X - P) . (X - Q) < 0`. (Why?)

***Proof of the theorem.*** Now, let `P`, `Q`, and `R` be three given points forming a triangle. We are asking what is covered by the ***union*** of

the three (closed) disks:

$$(X - P) \cdot (X - Q) \leqslant 0,$$
$$(X - Q) \cdot (X - R) \leqslant 0, \text{ and}$$
$$(X - R) \cdot (X - P) \leqslant 0.$$

In particular, we want to prove that any disk with a diameter included in the triangle is covered.

**Remark:** Any point **S** in the (closed) ***convex hull*** determined by the three vertices of the triangle can be written as a ***weighted average***:

$$S = a\,P + b\,Q + c\,R,$$

where the scalars **a**, **b**, and **c** are ***non negative*** and also

$$a + b + c = 1.$$

Thus, at least one of **a**, **b**, and **c** has to be ***positive***.

Also, let

$$T = d\,P + e\,Q + f\,R$$

be another such point. The formula for the disk with diameter **ST** is:

$$(X - a\,P - b\,Q - c\,R) \cdot (X - d\,P - e\,Q - f\,R) \leqslant 0.$$

Note that we have two ways to write **X**:

$$X = a\,X + b\,X + c\,X = d\,X + e\,X + f\,X.$$ (Why?)

Therefore, the formula for the disk can also be written as

$$(a\,(X - P) + b\,(X - Q) + c\,(X - R)) \cdot (d\,(X - P) + e\,(X - Q) + f\,(X - R)) \leqslant 0$$

Multiplying out the above (***carefully!***) we get:

```
a d (X - P).(X - P) +                              .
 b e (X - Q).(X - Q) + c f (X - R).(X - R)
+(a e + b d) (X - P).(X - Q) +
   (b f + c e) (X - Q).(X - R) +
   (a f + c d) (X - R).(X - P) ⩽ 0
```

Call the left-hand side of the above **L[X]**. We remark that ***all*** of the ***coefficients*** are ***non negative***, but, since ***some*** of the coefficients of **S** and of **T** have to be ***positive***, ***at least one*** of the coefficients of **L[X]** has to ***positive*** as well.

Now if **X** is a point (vector) where **L[X] ⩽ 0**, then ***at least one*** of the terms of **L[X]** with a positive coefficient must be ***non positive*** as well.

There are two cases:

• If it is one of the first three terms, then **X** has to ***be equal to*** **P** or **Q** or **R**.

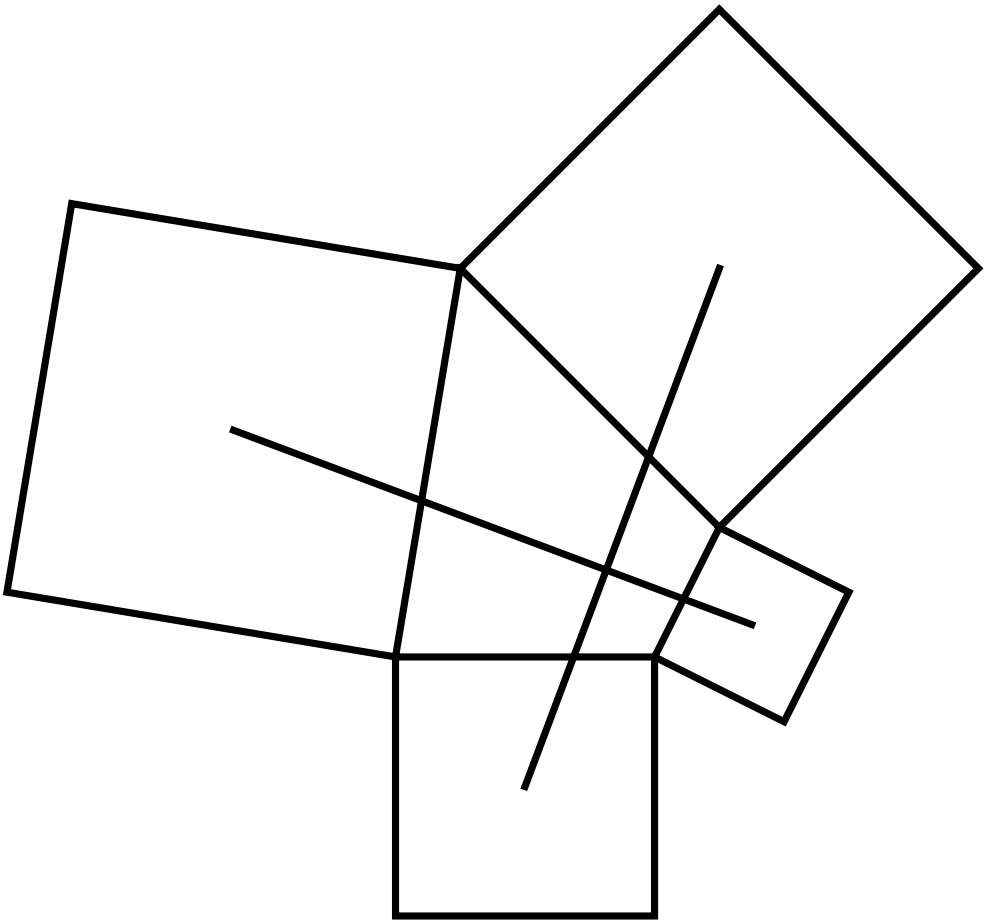
• If it is one of the last three, then **X** is ***a member of*** the interior of one of the original disks.

Therefore, the whole disk **L[X] ⩽ 0** is ***covered***. **Q.E.D.**

## Skewed Squares

### The Theorem

**Theorem.** If squares are erected (outside) on edges of a quadrilateral, then the segments joining the centers of opposite squares are ***equal in length*** and are ***perpendicular***.



## Proof by Complex Numbers

```
AA = a0 + a1 i;
BB = b0 + b1 i;
CC = c0 + c1 i;
DD = d0 + d1 i;
```

```
mid[x_, y_] := 1/2 (x + y - (y - x) i);
```

```
U = mid[CC, DD] - mid[AA, BB] // Expand
```

$$\left(-\frac{1}{2}-\frac{i}{2}\right) a_0+\left(\frac{1}{2}-\frac{i}{2}\right) a_1- \left(\frac{1}{2}-\frac{i}{2}\right) b_0-\left(\frac{1}{2}+\frac{i}{2}\right) b_1+\left(\frac{1}{2}+\frac{i}{2}\right) c_0- \left(\frac{1}{2}-\frac{i}{2}\right) c_1+\left(\frac{1}{2}-\frac{i}{2}\right) d_0+\left(\frac{1}{2}+\frac{i}{2}\right) d_1$$

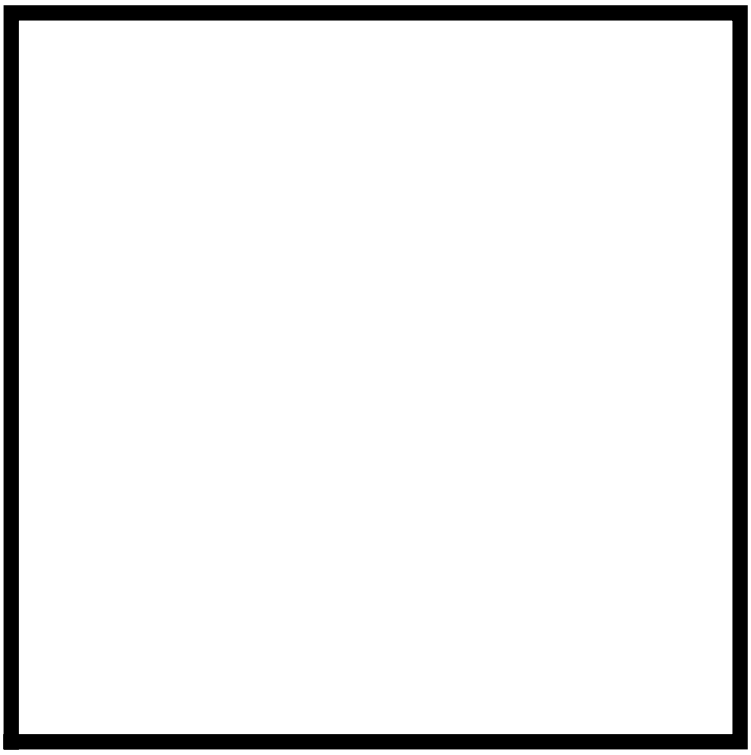
```
V = mid[DD, AA] - mid[BB, CC] // Expand
```

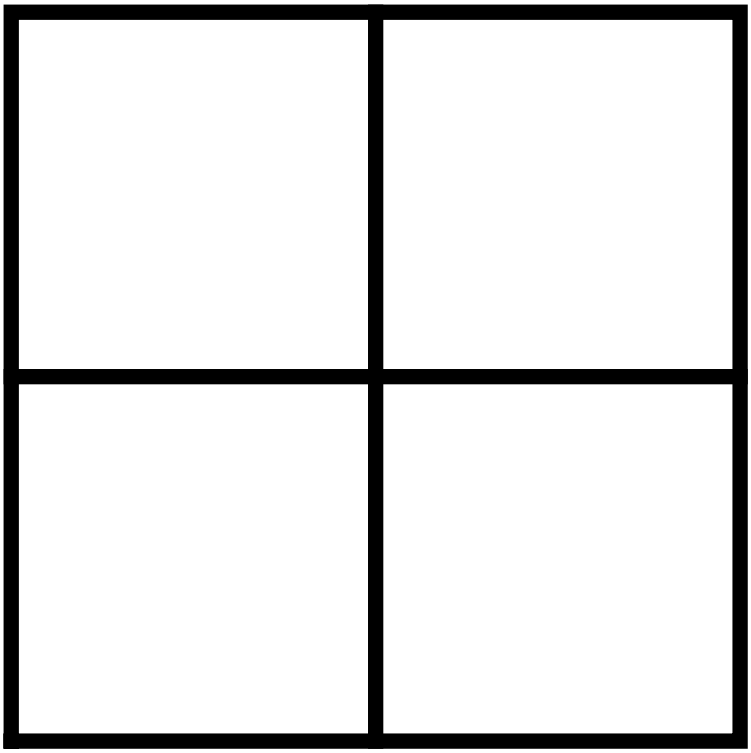
$$\left(\frac{1}{2}-\frac{i}{2}\right) a_0+\left(\frac{1}{2}+\frac{i}{2}\right) a_1- \left(\frac{1}{2}+\frac{i}{2}\right) b_0+\left(\frac{1}{2}-\frac{i}{2}\right) b_1-\left(\frac{1}{2}-\frac{i}{2}\right) c_0- \left(\frac{1}{2}+\frac{i}{2}\right) c_1+\left(\frac{1}{2}+\frac{i}{2}\right) d_0-\left(\frac{1}{2}-\frac{i}{2}\right) d_1$$

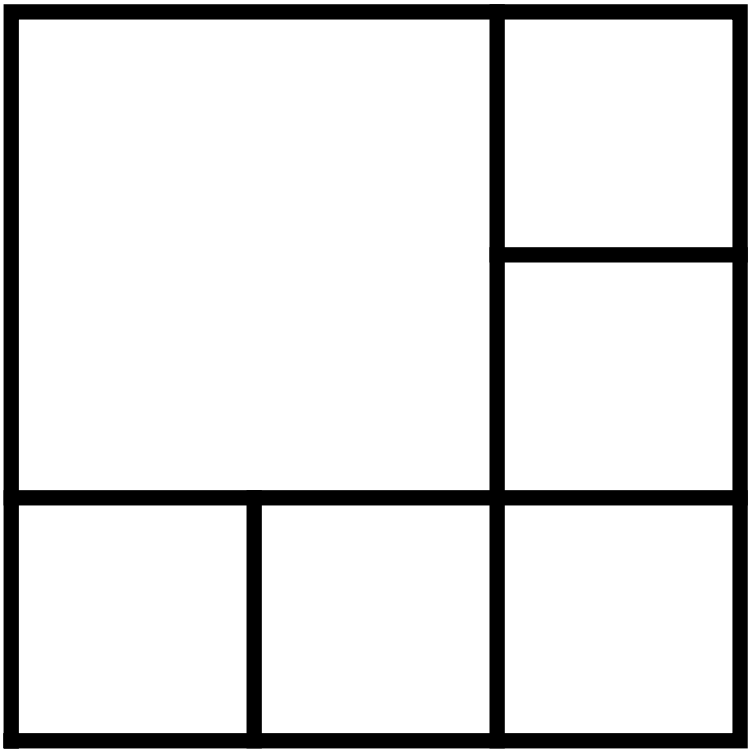
```
V - i U // Expand
```

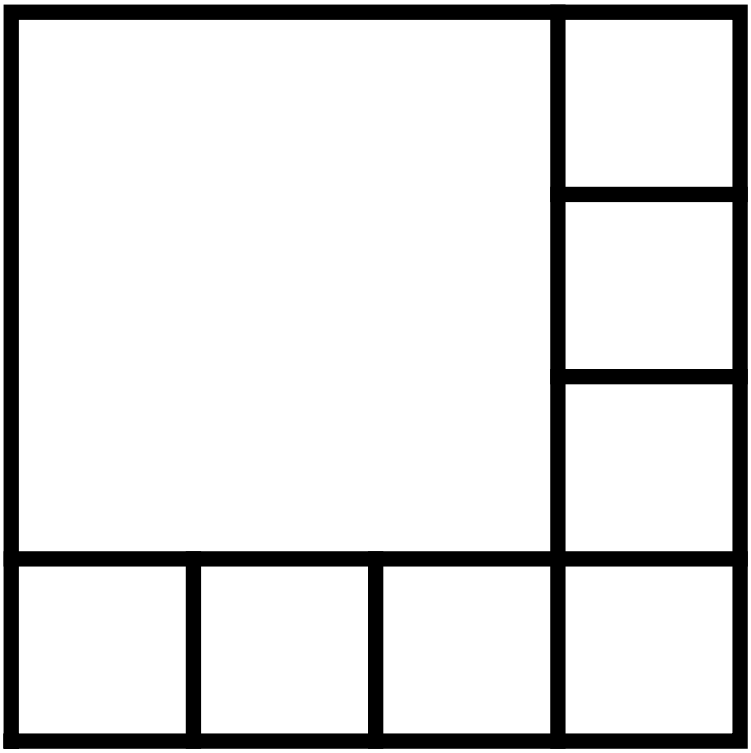
```
0
```

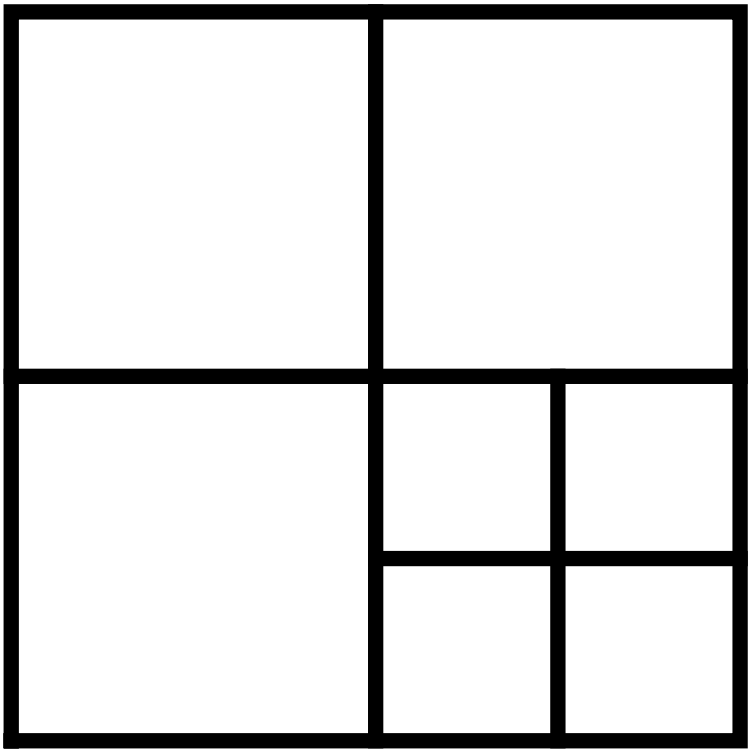
# Quilted Squares











**Comments**

**You can cut a square into 1, 4, 6, 7, 8 squares.**

**If you can cut a square into *n* squares, you can cut a square into**

***n* + 3 squares.**

**Hence, for all *n* ≥ 6, you can cut a square into *n* squares.**

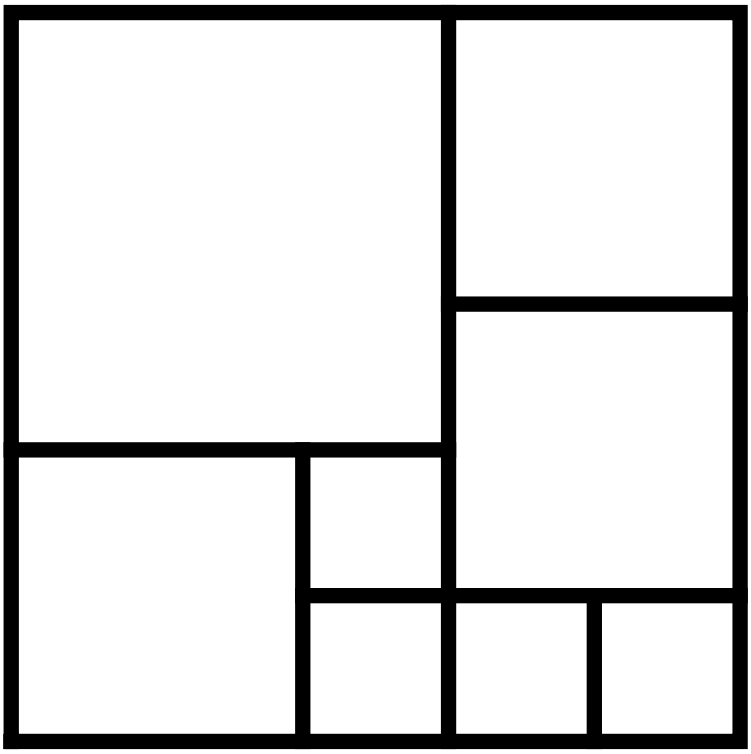
**Question 1: Why can you *not* cut a square into 2, 3, or 5 squares?**

**Question 2: If you  cut a square (or maybe even a rectangle) into squares, are the sides of the squares *commensurable*?**

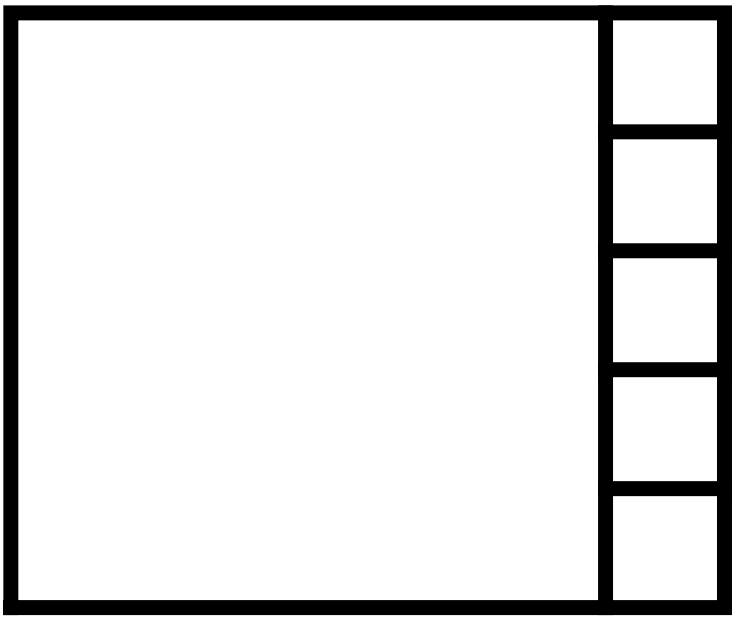
**Solved (!) by Max Dehn: "Über Zerlegung von**

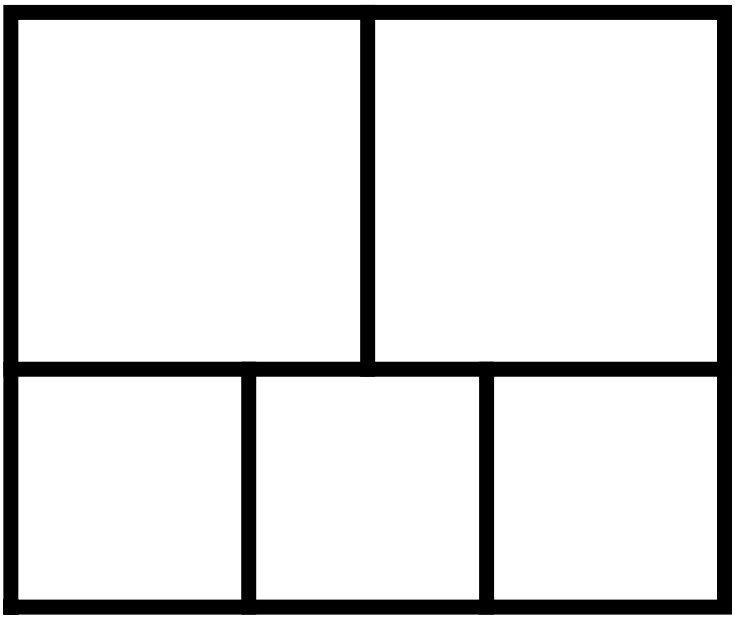
Rechtecken in Rechtecke", Mathematische Annalen, vol. 57 (1903)

**Question 3:** How many ways can you cut a square into *n* squares?



**Question 4:** What is the smallest number of squares needed to cut up an *n* x *m* (integral) rectangle?

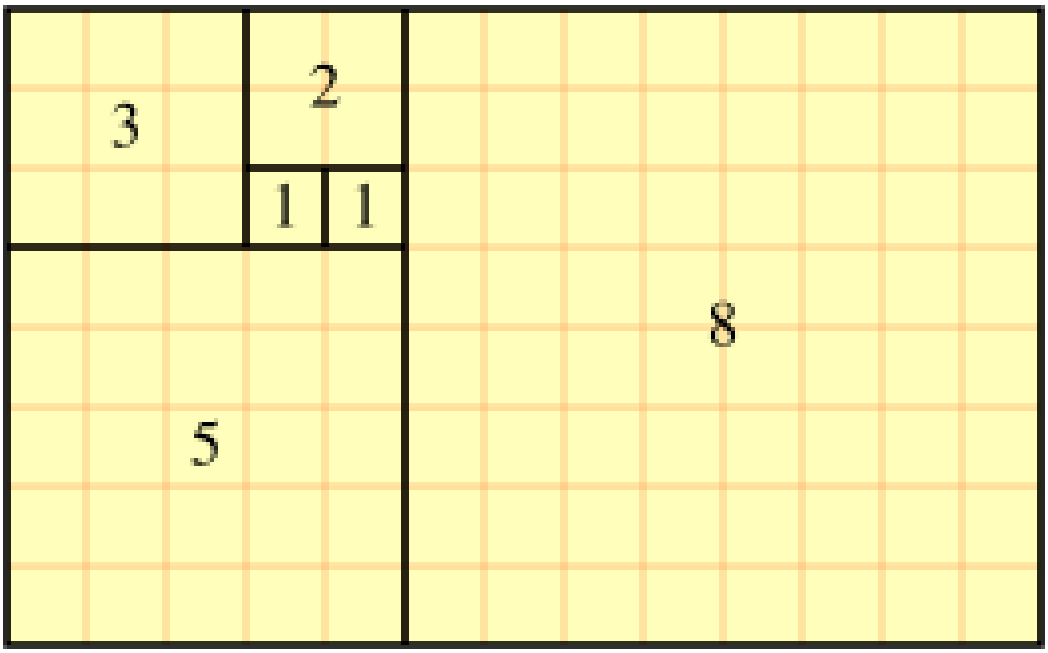




**The Greedy Algorithm *does not* always get the best tiling!**

**Conjecture:** Consider the Fibonacci Numbers:

F(n+2) = F(n+1) + F(n).




Here is a tiling with squares whose sides are successive Fibonacci numbers in length. You can always add another Fibonacci square. Conversely, starting with a rectangle of size F(n+2) x F(n+1), then the Greedy Algorithm works. Yes?

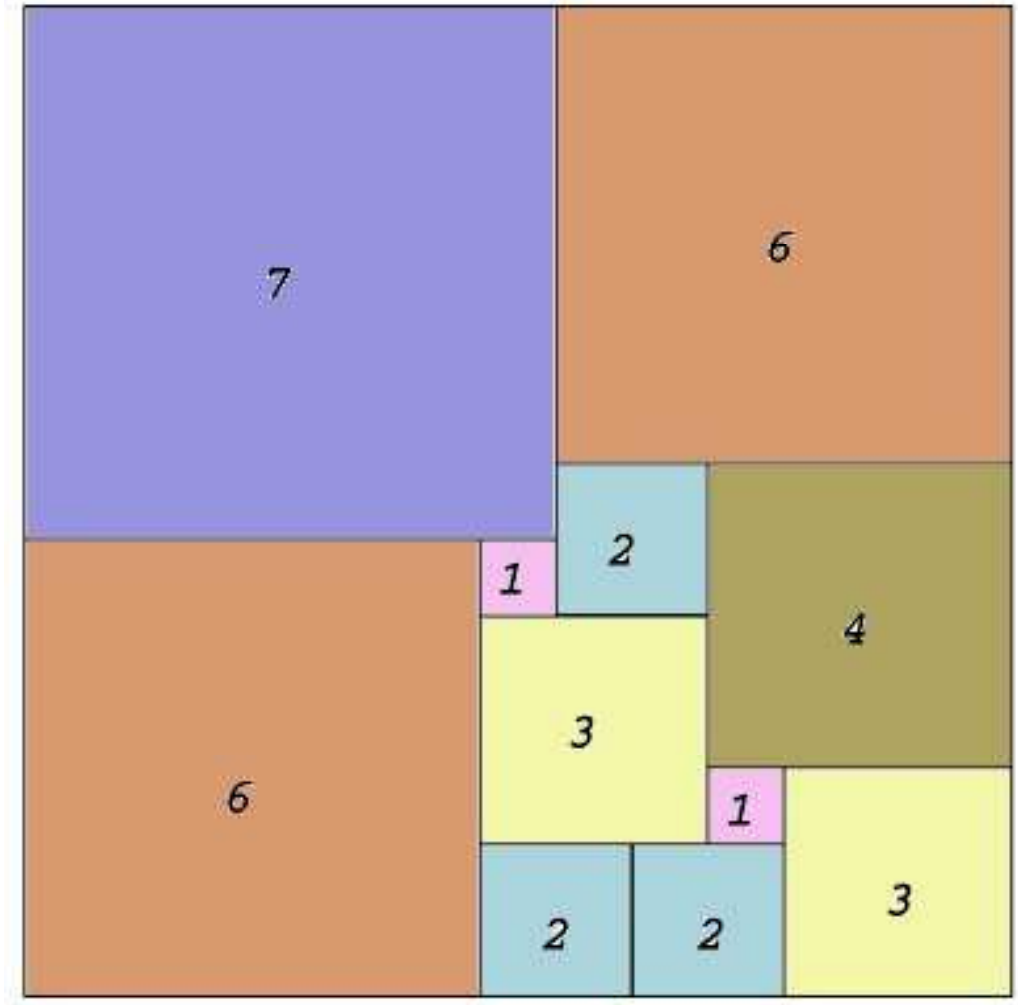
For more information on decompositions of various shapes, search for Mrs. Perkins's Quilt in Goooogle.

In 1914 The Patch Quilt Puzzle appeared in Sam Loyd: "Cyclopedia of Puzzles", privately published by his son after his death (reprinted in "Mathematical Puzzles of Sam Loyd", selected and edited by Martin Gardner, Vol 1, pp. 73, 147-148. Dover, New York, 1959).

This puzzle also appeared in a publication by Henry

**Dudeney as Mrs. Perkins Quilt: Problem 173 in Amusements in Mathematics. 1917.**

**A square quilt made of 169 square patches of the same size is to be divided into the smallest number of square pieces by cutting along lattice lines. The answer, which is *unique*, is composed of 11 squares with sides 1,1,2,2,2,3,3,4,6,6,7. It is neither *perfect* nor *simple*.**




## A Last Quotation

Mathematics is about ***ideas*** which ***explain***
and thus enable us to ***understand*** things.
The solution of a mathematical problem
is ***beautiful*** in proportion to the beauty of
the idea used to solve it.
So, appreciating mathematics means learning to
***recognize*** and ***appreciate*** beautiful ideas....

— David Gale (1921–2008)