

Copyright Notice

The following manuscript

EWD 538: A collection of beautiful proofs

is held in copyright by Springer-Verlag New York.

The manuscript was published as pages 174–183 of

Edsger W. Dijkstra, *Selected Writings on Computing: A Personal Perspective*,
Springer-Verlag, 1982. ISBN 0-387-90652-5.

**Reproduced with permission from Springer-Verlag New York.
Any further reproduction is strictly prohibited.**

A collection of beautiful proofs.

This chapter contains a compilation of beautiful proofs, proofs of which I expect that all mathematicians will agree that they are beautiful. The purpose of this compilation is to collect the material that may enable us to come to grips with the main qualities that together constitute "mathematical elegance". Further analysis and comparisons of these gems will be postponed until the collection is thought to be large enough. In order to avoid too much of a personal bias (and, also, to build up a larger collection than I could think of myself) I have asked others for their contribution to the collection. The only constraint was that the proof could be appreciated by the "generally educated"; all contributions that required specialized mathematical knowledge had, alas, to be rejected.

1. A classical example.

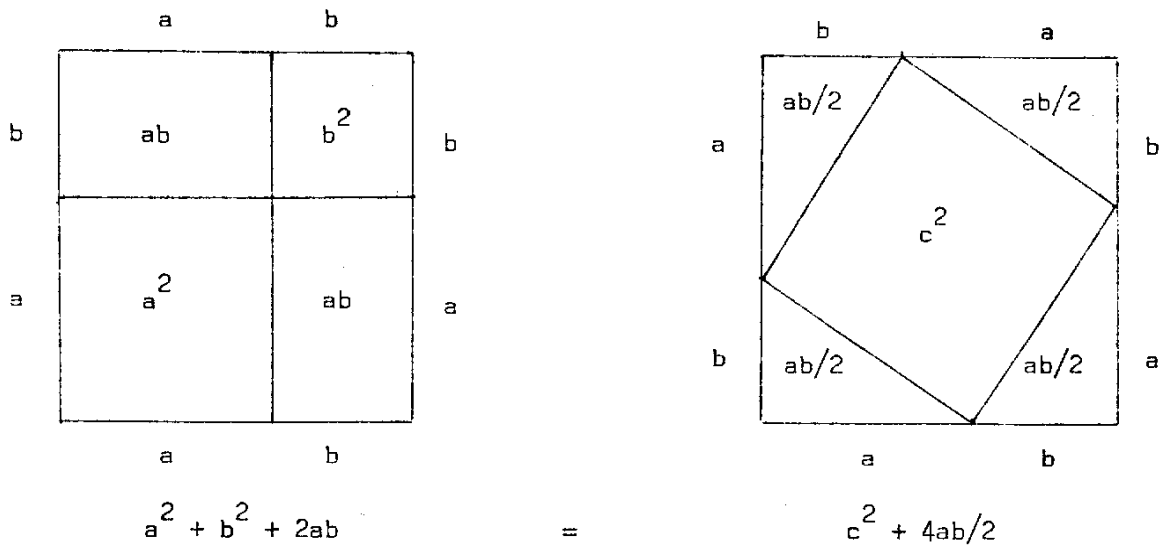
In the late 18th century a German schoolmaster gave --with the intention of keeping his pupils busy for another hour-- the task to sum hundred terms of an arithmetic progression to a class of little boys who, of course, had never heard of arithmetic progressions. The youngest pupil, however, wrote down the answer instantaneously and waited gloriously, with his arms folded, for the next hour while his classmates toiled: at the end it turned out that little Johann Friederich Carl Gauss had been the only one to hand in the correct answer. Young Gauss had seen instantaneously how to sum such a series analytically: the sum equals the number of terms multiplied by the average of the first and the last term. (To quote E.T.Bell: "The problem was of the following sort, $81297 + 81495 + 81693 + \dots + 100899$, where the step from one number to the next is the same all along (here 198), and a given number of terms (here 100) are to be added.")

In two respects this is a classical example: firstly young Gauss produced his answer about a thousand times as fast as his classmates, secondly he was the only one to produce the correct answer. So much for the effective ordering of one's thoughts!

2. The Pythagorean Theorem, proof I.

When I was twelve years old, I learned the following proof, in which

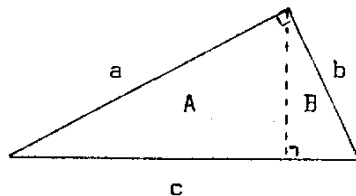
a square with sides $a + b$ is considered in two different ways.



The two expressions are different expression for the same area: they are therefore equal. Next we observe $2ab = 4ab/2$ and by subtraction we find $a^2 + b^2 = c^2$. A beautiful proof in the good old Greek tradition that fascinated me when it was shown to me, and satisfied me for more than 30 years.

3. The Pythagorean Theorem, proof II.

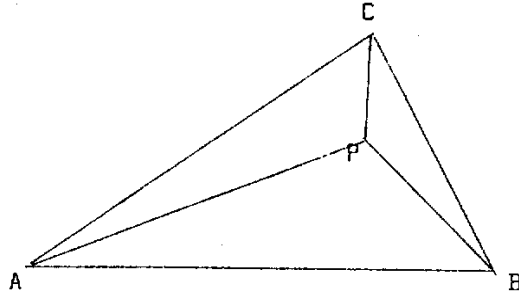
The following proof was shown to me a few years ago. The areas of similar figures have the same relation as the squares of corresponding lines; for three similar figures with areas A , B , and C respectively and corresponding lines a , b , and c respectively, any homogeneous linear relation satisfied by A , B , and C is, therefore, also satisfied by a^2 , b^2 , and c^2 , and vice versa. In particular we know that $A + B = C$ implies $a^2 + b^2 = c^2$.



Here we have three similar triangles with a , b , and c respectively as their hypotenuse; the sum of the areas of the first two equals the area of third triangle, i.e. $A + B = C$, hence $a^2 + b^2 = c^2$.

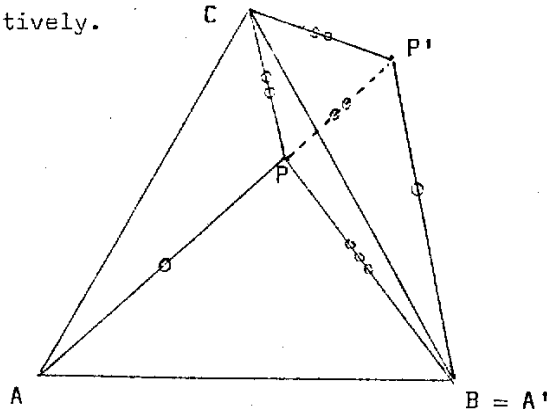
4. The Theorem of Pompeiu.

For a triangle ABC of which at least two sides have different lengths, we can choose a point P such that the lengths AP , BP , and CP are such that no triangle can be formed from those three pieces.



In any triangle, each side must be smaller than the sum of the two others. But, if $AC > BC$, we can choose P so close to C , that $AP > BP + CP$, hence they can not be the lengths of the sides of a triangle.

This observation led the Rumanian mathematician Pompeiu to the conjecture that, conversely, for an equilateral triangle ABC no such point exists, i.e. that for every point P the lengths AP , BP , and CP satisfy the triangular inequalities. He gave a proof, which --I am told-- was very ugly. The following beautiful proof is due to G.R.Veldkamp; it gives a constructive existence proof of such a triangle with sides equal to AP , BP , and CP respectively.



We rotate triangle CAP around point C over 60 degrees, so that A' coincides with B and P gives rise to its corresponding point P' . The process of rotation implies that $AP = BP'$ and $CP = CP'$. But now triangle PCP' is an isosceles triangle with at point C a top of 60 degrees, hence it is equilateral, and we conclude that $CP = PP'$. Triangle PBP' has three sides of the required lengths and the Theorem of Pompeiu has been proved.

5. Euclid's Theorem on Primes.

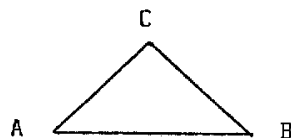
Denoting the integer numbers ≥ 2 by the term "multiples", we can define the primes as those multiples that cannot be written as the product of two multiples. From this definition it follows immediately that for each multiple there exists at least one prime dividing that multiple.

Let P be a prime; define the multiple Q as the product of all primes $\leq P$, increased by 1. The multiple Q has been constructed in such a way, that none of the primes $\leq P$ divides Q ; the prime dividing Q must, therefore, be $> P$. Hence there is no largest prime number.

Note. It is not unusual that, after the construction of Q , the proof considers the two cases "Q is a prime" and "Q is not a prime" separately. The above proof shows that this case analysis is superfluous; the case analysis has probably been induced by the linguistic distinction between singular and plural forms. (End of note.)

6. Euclid's Theorem on the Base Angles of an Isosceles Triangle.

Using the theorem that any two triangles which have two sides and the included angle equal to two sides and the included angle of the other are congruent, it should be proved that the base angles of an isosceles triangle are equal, more precisely, that from $AC = BC$ follows that the angles A and B are equal to each other.

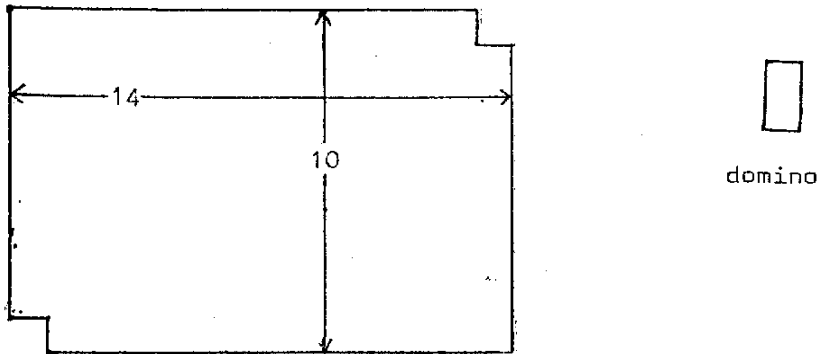


Because $AC = BC$, we have also $CB = CA$; angle C is equal to itself and the theorem allows us to conclude that the triangles ACB and BCA are congruent. These two triangles have angles A and B as corresponding parts, hence they are equal.

Note. It is not necessary --as Euclid seems to have done-- to bisect angle C and then to use the theorem to show that the original triangle is cut into two congruent parts. (End of note.)

7. A covering problem.

Given the figure as shown below that could be covered by 138 squares, and 69 dominoes of two squares each --one such domino is shown below--



the question to be answered is: can the figure be covered by the 69 dominoes? The answer is negative, and the argument is as follows.

Consider the 10×14 rectangle before the two opposite squares have been removed, and colour its squares alternately black and white as with a chess board: the rectangle then shows 70 white squares and 70 black ones. The two squares to be removed have, however, the same colour, and our figure, therefore, has 70 squares of the one colour and 68 squares of the other colour. Each domino covers one white and one black square; together the dominoes cover, no matter how they are placed, 69 black and 69 white squares. As a result they cannot cover the given figure.

8. The Harmonic Series Diverges.

Consider

$$S_n = 1/1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + 1/7 + 1/8 + \dots + 1/n .$$

It has to be shown, that by choosing n sufficiently large, we can achieve $S_n > M$ for arbitrarily large value M ; in other words we have to show that the sequence S_1, S_2, S_3, \dots is unbounded. We observe that

$$S_2 - S_1 = 1/2$$

$$S_4 - S_2 = 1/3 + 1/4 > 1/4 + 1/4 = 1/2$$

$$S_8 - S_4 = 1/5 + 1/6 + 1/7 + 1/8 > 1/8 + 1/8 + 1/8 + 1/8 = 1/2 \quad \text{etc.}$$

In other words: starting with $n = 1$, S_n is increased by at least $1/2$ each time n is doubled.

9. The Eigenvalues of a Hermitean Matrix are Real.

A Hermitean matrix is the generalization of a real, symmetric matrix; its transpose equals its complex conjugate

$$A^T = A^* \quad (1)$$

For a given matrix A , λ is an eigenvalue, if and only if the equation

$$A \cdot x = \lambda \cdot x \quad (2)$$

has a non-null vector x as solution.

Taking the transpose of both sides of (2) we get

$$x^T \cdot A^T = \lambda \cdot x^T$$

and then post-multiplying both sides by x^* we get

$$x^T \cdot A^T \cdot x^* = \lambda \cdot x^T \cdot x^* \quad (3)$$

Taking the complex conjugate of both sides of (2) we get

$$A \cdot x^* = \lambda^* \cdot x^*$$

and then pre-multiplying both sides by x^T we get

$$x^T \cdot A \cdot x^* = \lambda^* \cdot x^T \cdot x^* \quad (4)$$

On account of (1) we conclude that (3) and (4) have equal left-hand sides, and hence

$$0 = (\lambda - \lambda^*) \cdot x^T \cdot x^*$$

Because x is a non-null vector and $x^T \cdot x^*$ is a sum of absolute values, we conclude that $x^T \cdot x^* > 0$, and hence

$$\lambda = \lambda^* \quad \text{Q.E.D.}$$

10. The Cauchy-Schwarz inequality.

Let a_1, \dots, a_n and b_1, \dots, b_n be $2n$ real numbers; then the following inequality holds:

$$(a_1 b_1 + \dots + a_n b_n)^2 \leq (a_1^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2)$$

Consider the following quadratic form $Q(x)$ in x , defined by

$$Q(x) = (a_1 + b_1 x)^2 + \dots + (a_n + b_n x)^2$$

Because, for real x , $Q(x)$ is defined as the sum of the squares of n real numbers, for real x the inequality $Q(x) \geq 0$ must hold. In other words, the equation $Q(x) = 0$ has at most one real root, and its discriminant is ≤ 0 . Collecting powers of x in the definition of $Q(x)$ we find:

$$Q(x) = (a_1^2 + \dots + a_n^2) + 2(a_1 b_1 + \dots + a_n b_n) \cdot x + (b_1^2 + \dots + b_n^2) \cdot x^2$$

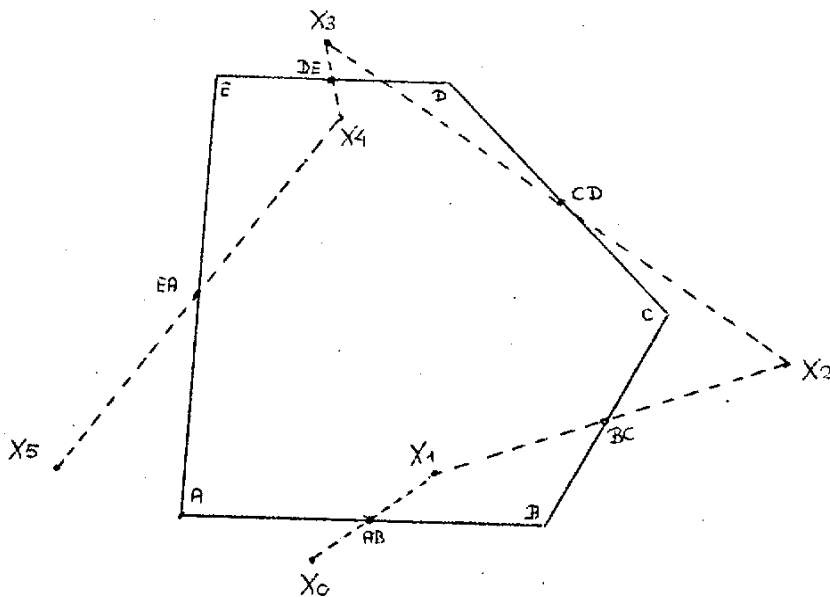
with the discriminant

$$(a_1 b_1 + \dots + a_n b_n)^2 - (a_1^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2)$$

The conclusion that this discriminant is nonpositive proves our inequality.

11. Reconstructing an odd polygon from the midpoints of its sides.

We shall show the construction for poly = 5 .



For the pentagon ABCDE , the points marked AB, BC, CD, DE, and EA respectively are the midpoints of its successive sides. Given the positions of those five midpoints, it is requested to reconstruct the original pentagon ABCDE.

Consider what happens when we subject a plane to five successive rotations of 180 degrees each with AB, BC, CD, DE, and EA as the successive centers of rotation. The point that originally coincided with A , coincides with B after the first rotation, with C after the second rotation, etc. and coincides again with A after the fifth and last rotation. Because the

pentagon has an odd number of sides, the total transformation of that plane is therefore a rotation of 180 degrees with A as its center of rotation.

We now trace a point in the rotated plane that originally coincides with an arbitrary point X0 . Rotating it around AB gives us its position X1 after the first rotation, rotating that around BC gives us its position X2 after the second rotation, etc. until we have constructed its final position X5 . As that could also have been reached by rotating X0 over 180 degrees around the --still unknown-- point A , we conclude that A is the midpoint of the line from X0 to X5 ! The positions of the other four vertices B, C, D, and E now follow trivially.

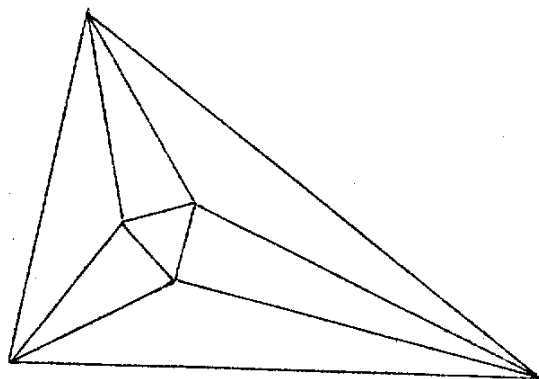
12. The number of factors p (for p prime) in n!

Let n be a natural number, let p be a prime number; let $s(n, p)$ denote the sum of the digits of the representation of n in the number system with radix p . Then the number of factors p in n! equals

$$\frac{n - s(n, p)}{p - 1} \quad (1)$$

Expression (1) is clearly correct for $n = 1$. Its general validity is proved by mathematical induction. Suppose that $n + 1$ has k factors p ; the transition from $n!$ to $(n + 1)!$ then increases that number of factors p by k . But replacing n by $n + 1$ also increases (1) by k , because when 1 is added to n , the carry is propagated over k digits = $p - 1$, which all turn into zero.

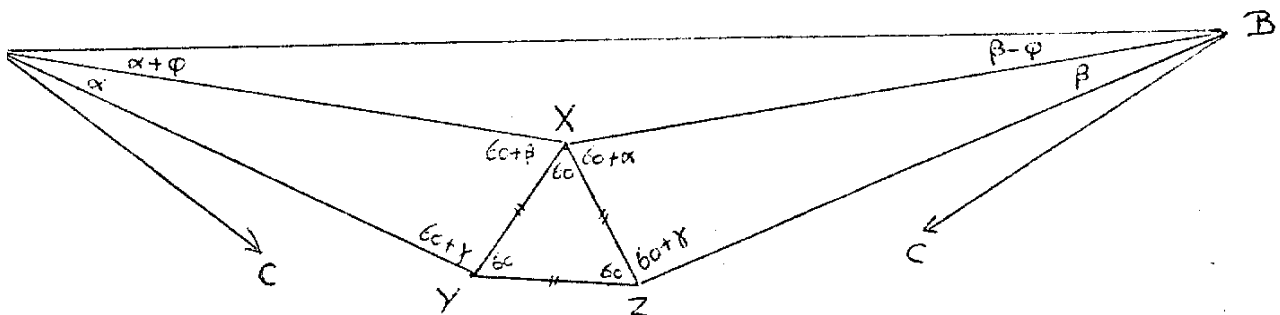
13. Frank Morley's Theorem.



In 1904 Frank Morley discovered the following theorem --see previous picture--:

The adjacent pairs of the trisectors of the angles of a triangle always meet at the vertices of an equilateral triangle.

The shortest proof I know for this theorem proves, in fact, a stronger theorem, that also determines the orientation of that equilateral triangle. We start in our proof not with the arbitrary triangle, but with the equilateral one.



Choose the three positive angles α , β , and γ such that $\alpha + \beta + \gamma = 60^\circ$. Draw an equilateral triangle XYZ and construct the triangles AXY and BXZ with the angles as indicated in the above picture. Because $\angle AXB = 180^\circ - (\alpha + \beta)$, it follows that if $\angle BAX = \alpha + \phi$, $\angle ABX = \beta - \phi$. Using the rule of sines three times (in triangles AXB , BXZ , and AXY), we deduce

$$\frac{\sin(\alpha + \phi)}{\sin(\beta - \phi)} = \frac{BX}{AX} = \frac{XZ \cdot \sin(60^\circ + \gamma) / \sin(\beta)}{XY \cdot \sin(60^\circ + \gamma) / \sin(\alpha)} = \frac{\sin(\alpha)}{\sin(\beta)}$$

Because in the range considered the left-hand side of this equation is a monotonically increasing function of ϕ , we conclude that $\phi = 0$ is in this range its only root. Completing the picture and repeating the argument twice we conclude that the angles at A , B , and C are trisected, and thus Morley's Theorem is proved without the aid of any additional lines.

(To be continued in a later report.)