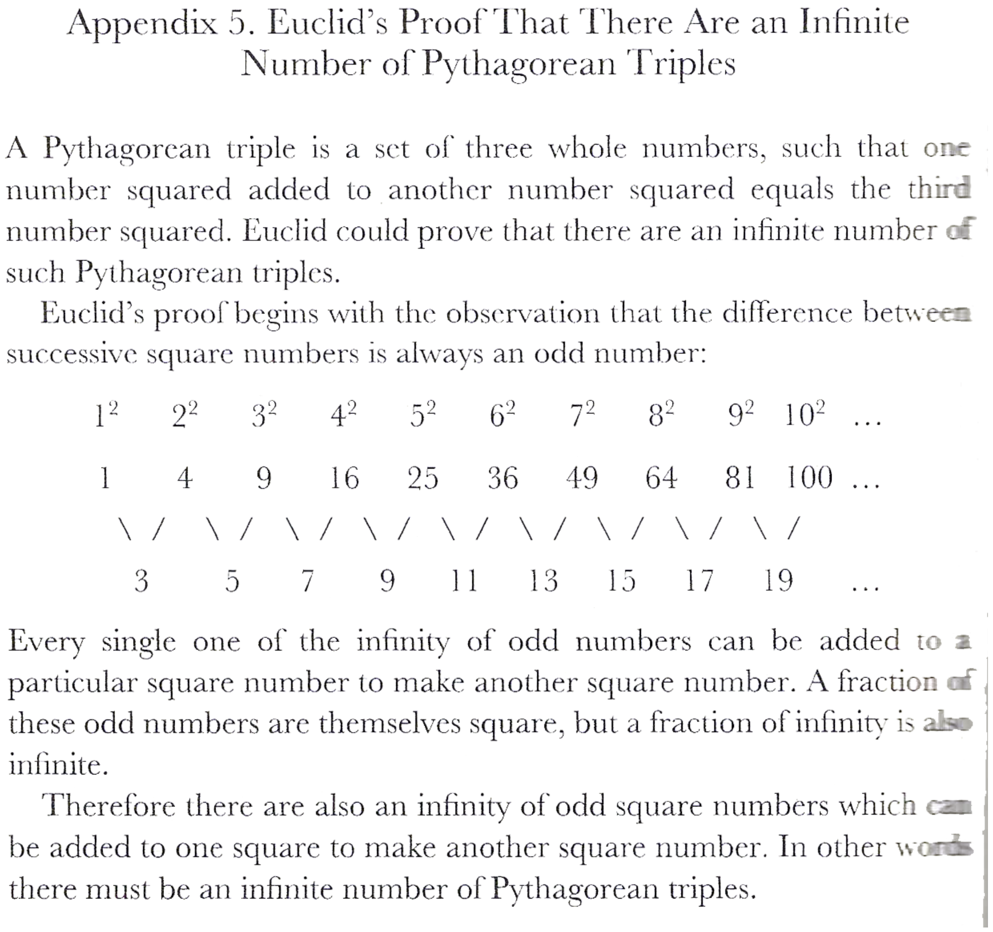
Pythagorean Triples



Appendix 5. Euclid's Proof That There Are an Infinite Number of Pythagorean Triples

A Pythagorean triple is a set of three whole numbers, such that one number squared added to another number squared equals the third number squared. Euclid could prove that there are an infinite number of such Pythagorean triples.

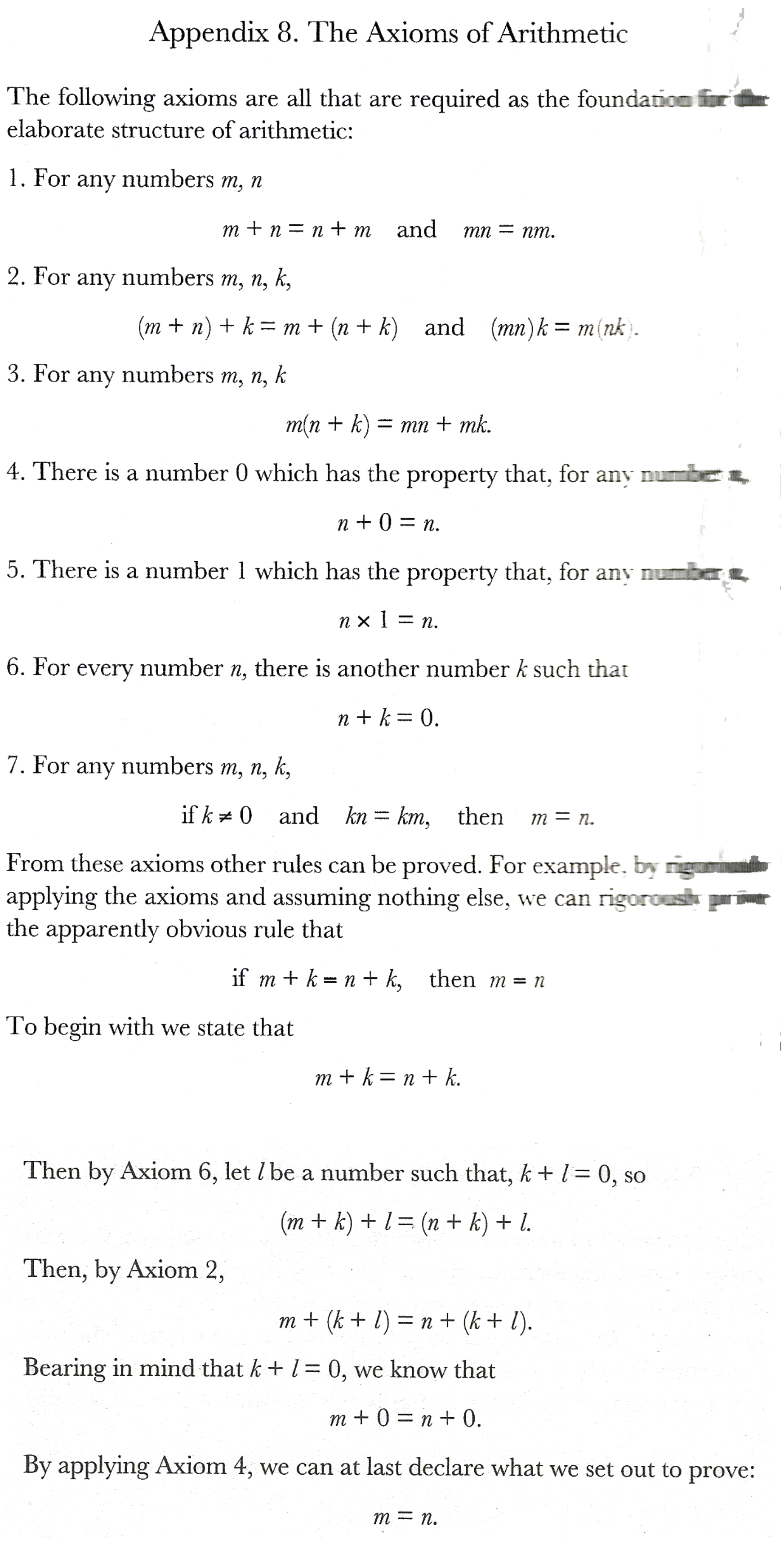
Euclid's proof begins with the observation that the difference between successive square numbers is always an odd number:

$$
\begin{array}{ccccccccccccccccccccc}
1^2 & & 2^2 & & 3^2 & & 4^2 & & 5^2 & & 6^2 & & 7^2 & & 8^2 & & 9^2 & & 10^2 & & \ldots \\
1 & & 4 & & 9 & & 16 & & 25 & & 36 & & 49 & & 64 & & 81 & & 100 & & \ldots \\
\backslash & / & \backslash & / & \backslash & / & \backslash & / & \backslash & / & \backslash & / & \backslash & / & \backslash & / & \backslash & / & & & \\
 & 3 & & 5 & & 7 & & 9 & & 11 & & 13 & & 15 & & 17 & & 19 & & & \ldots
\end{array}
$$

Every single one of the infinity of odd numbers can be added to a particular square number to make another square number. A fraction of these odd numbers are themselves square, but a fraction of infinity is also infinite.

Therefore there are also an infinity of odd square numbers which can be added to one square to make another square number. In other words there must be an infinite number of Pythagorean triples.

The Axioms of Arithmetic



Appendix 8. The Axioms of Arithmetic

The following axioms are all that are required as the foundation for the elaborate structure of arithmetic:

1. For any numbers m, n

$$m + n = n + m \quad \text{and} \quad mn = nm.$$

2. For any numbers m, n, k,

$$(m + n) + k = m + (n + k) \quad \text{and} \quad (mn)k = m(nk).$$

3. For any numbers m, n, k

$$m(n + k) = mn + mk.$$

4. There is a number 0 which has the property that, for any number n,

$$n + 0 = n.$$

5. There is a number 1 which has the property that, for any number n,

$$n \times 1 = n.$$

6. For every number n, there is another number k such that

$$n + k = 0.$$

7. For any numbers m, n, k,

$$\text{if } k \neq 0 \quad \text{and} \quad kn = km, \quad \text{then} \quad m = n.$$

From these axioms other rules can be proved. For example, by rigorously applying the axioms and assuming nothing else, we can rigorously prove the apparently obvious rule that

$$\text{if } m + k = n + k, \quad \text{then } m = n$$

To begin with we state that

$$m + k = n + k.$$

Then by Axiom 6, let l be a number such that, $k + l = 0$, so

$$(m + k) + l = (n + k) + l.$$

Then, by Axiom 2,

$$m + (k + l) = n + (k + l).$$

Bearing in mind that $k + l = 0$, we know that

$$m + 0 = n + 0.$$

By applying Axiom 4, we can at last declare what we set out to prove:

$$m = n.$$

Rational, Irrational, Rational

2.1.3 Theorem

Between any two distinct rationals there is an irrational.

Proof

Suppose that $m/n < p/q$. This gives $p/q - m/n > 0$. Hence

$$\frac{m}{n} < \frac{m}{n} + \frac{\sqrt{2}}{2}\left(\frac{p}{q} - \frac{m}{n}\right)$$

and, since $\sqrt{2}/2 < 1$,

$$\frac{m}{n} + \frac{\sqrt{2}}{2}\left(\frac{p}{q} - \frac{m}{n}\right) < \frac{m}{n} + \left(\frac{p}{q} - \frac{m}{n}\right) = \frac{p}{q}$$

Thus the irrational

$$\frac{m}{n} + \frac{\sqrt{2}}{2}\left(\frac{p}{q} - \frac{m}{n}\right)$$

lies between the rationals m/n and p/q. □

The Axioms of Arithmetic

2.2.1 The axioms of arithmetic

A1 $a + (b + c) = (a + b) + c$

A2 $a + b = b + a$

A3 There exists a unique element 0 in $\mathbb{R}$ satisfying $a + 0 = a$

A4 For any a in $\mathbb{R}$, there exists a unique element x in $\mathbb{R}$ satisfying $a + x = 0$

A5 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

A6 $a \cdot b = b \cdot a$

A7 There exists a unique element 1 in $\mathbb{R}$, $1 \neq 0$, satisfying $a \cdot 1 = a$

A8 For any a in $\mathbb{R}$, $a \neq 0$, there exists a unique element y in $\mathbb{R}$ satisfying $a \cdot y = 1$

A9 $a \cdot (b + c) = a \cdot b + a \cdot c$

Notes

(1) Each axiom holds for all $a, b, c \in \mathbb{R}$.

(2) Any set satisfying A1–A9 is called a **field**.

(3) The x in A4 is called the **negative** of a and is usually denoted by $(-a)$.

(4) The y in A8 is called the **reciprocal** of a and is written as $1/a$ or a^{-1}.

(5) Axioms A1 and A5 allow us to omit brackets in expressions such as $a + b + c$ or $a \cdot b \cdot c \cdot d$.

(6) The axioms give names to only two particular elements of $\mathbb{R}$, namely 0 and 1, whose roles are defined in A3 and A7.

(7) 0^{-1} is not defined – see A8. In fact, no such element exists by Example 1(a) below.

(8) **Subtraction** can be defined by $a - b = a + (-b)$.

(9) **Division** can be defined by $a \div b = a \cdot (b^{-1})$, $b \neq 0$.

It is assumed that the reader is quite familiar with axioms A1–A9. From these axioms, many further algebraic properties can be deduced. Since these axioms are so basic, several elementary consequences are needed first.

■■ EXAMPLE 2

Prove the algebraic identity $(a - b) \cdot (a + b) = a^2 - b^2$.

Solution

$$\begin{aligned}
(a - b) \cdot (a + b) &= (a + (-b)) \cdot (a + b) && \text{using Note (8)} \\
&= (a + (-b)) \cdot a + (a + (-b)) \cdot b \\
& && \text{by A9} \\
&= a \cdot (a + (-b)) + b \cdot (a + (-b)) \\
& && \text{by A6} \\
&= a \cdot a + a \cdot (-b) + b \cdot a + b \cdot (-b) \\
& && \text{by A9 and A1} \\
&= a \cdot a + (-(a \cdot b)) + b \cdot a + (-(b \cdot b)) \\
& && \text{using Example 1(b)} \\
&= a \cdot a + (a \cdot b + (-(a \cdot b)) + (-(b \cdot b))) \\
& && \text{by A6, A2 and A1} \\
&= (a \cdot a + 0) + (-(b \cdot b)) && \text{by A4 and A1} \\
&= a \cdot a + (-(b \cdot b)) && \text{by A3} \\
&= a^2 - b^2 && \text{using Note (8)} \quad \blacksquare
\end{aligned}$$

Direct Proof Questions

Prove that the result of multiplying two odd numbers together is always odd.

Prove that the sum of two consecutive square numbers is always odd.

Prove that, for any prime number p greater than 3, $p^2 - 1$ is always a multiple of 24.

Prove the following identities:

$$(x+y)^2 + (x-y)^2 \equiv 2(x^2+y^2)$$

$$(x+y)^2 - (x-y)^2 \equiv 4xy$$

$$x^3 + y^3 \equiv (x+y)(x^2 - xy + y^2)$$

$$x^3 - y^3 \equiv (x-y)(x^2 + xy + y^2)$$