Chapter I

Introduction

by Nicola Oswald and Jörn Steuding

The concept of number and the evolution of number systems are topics of utmost importance in the history of mathematics. An early observation was the discovery of irrational quantities in geometrical figures by ancient Greek mathematicians. Interestingly, the foundation of integers was established much later, namely by Richard Dedekind and Giuseppe Peano in 1888/89, almost two decades after the constructions of real numbers due to Dedekind himself, Georg Cantor, Charles Méray, and others. These works reflect very well a new way of thinking about numbers in particular, and mathematics and logic more generally, indicating that mathematics had achieved a certain maturity in the second half of the 19th century. In the very beginning the human concept of number was tied to practical purposes such as counting quantities. Later, however, a larger supply of numbers was needed, for example, for solving polynomial equations or for studying processes by analytic means. This applies not only to integers or real numbers but to complex numbers too, although their invention followed a somehow different path.

Whereas the construction of real numbers relies on rather advanced – and at that time completely new methods (e.g. Dedekind cuts or Cauchy sequences) – the foundation of complex numbers is, at least from today's point of view, realized by a simple quadratic extension of the field of real numbers. However, adjoining such an imaginary square root $\sqrt{-1}$ has caused a lot of controversial discussions. For centuries, mathematicians could hardly accept that a square can be negative (which is counterintuitive to our usual way of thinking, having geometrical figures in mind where squares do have a positive area).

The new numbers, sets and methods, in combination with a novel way of thinking in mathematics, led to a variety of powerful and omnipresent structures, for instance, groups, rings and fields, as well as substructures like semigroups and ideals. In the context of numbers we list here the semigroup of positive integers, the ring of integers, and the fields of rationals, real and complex numbers, denoted by

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Further concepts of numbers have been introduced and used for various reasons, e.g. p-adic numbers and hypercomplex numbers. While the first type of numbers yields number-theoretically relevant completions of $\mathbb{Q}$, the latter numbers were, at least in their early days, expected to be as useful as the complex numbers with respect to

various mathematical disciplines. Here we shall only sketch the developments around complex and hypercomplex numbers.[1]

In 1545, Girolamo Cardano solved in his *Artis magnae sive de regulis algebraicis liber unus* the equation

$$X(10 - X) = 40$$

by

$$x = 5 \pm \sqrt{-15}$$

and called $\sqrt{-15}$ a formal quantity ("quantitas sophistica"). A little later, in 1572, Rafael Bombelli computed with complex quantities and used them for solving cubic equations. Indeed, applying Cardano's formula, square roots of negative numbers appear naturally besides real solutions of cubic equations. The word "imaginary" was coined by René Descartes who wrote in his *La Géométrie* (1637) that, "along with any equation one can imagine as many roots as the degree, though these imagined roots sometimes do not correspond to real quantities." This statement may be considered as an early unprecise formulation of the celebrated fundamental theorem of algebra, which states that every non-constant polynomial has a zero (or that the field of complex numbers $\mathbb{C}$ is algebraically closed). Whereas for Isaac Newton in his *Universal Arithmetic*, complex numbers indicated unsolvable problems. Gottfried Wilhelm Leibniz called imaginary roots "almost a hermaphrodite by nature in between being and non-being"[2], and found astonishing identities, such as

$$\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}} = \sqrt{6}$$

(appearing in a letter to Christiaan Huygens from 1674/5). In his ground-breaking *Introductio in analysin infinitorum* (1748) [81], Leonhard Euler viewed complex numbers $z = x + \mathrm{i}y$ in the complex plane with right angular real coordinates (x, y) and the imaginary unit

$$\mathrm{i} = \sqrt{-1}$$

(meaning that $\mathrm{i}^2 = -1$), as well as in polar coordinates (r, ϕ) as $z = r(\cos\phi + \mathrm{i}\sin\phi)$, with real r measuring the distance of z from the origin and an angle ϕ between the positive real axis and the straight line passing through z and the origin; in this context the imaginary unit i was treated as a number linearly independent from 1. Euler's famous formula

$$\exp(\mathrm{i}\phi) = \cos\phi + \mathrm{i}\sin\phi$$

[1] For a more complete history (including references) we refer to the collection of essays, entitled *Numbers* [72] by Heinz-Dieter Ebbinghaus et al. as well as Bartel van der Waerden's *History of Algebra* [254].

[2] The original Latin is "inter ens et non ens amphibio"; see *Acta Eruditorum*, 1702.

relates the complex exponential function with trigonometric functions and provides a parametrization of the unit circle. The first published proof of the fundamental theorem of algebra was given by Jean d'Alembert in 1746; the gaps in his reasoning can now be fixed by standard methods. Moreover, it was Jean Robert Argand in his *Essay sur une manière de représenter les quantités imaginaires dans les constructions géométriques* (1806), who interpreted multiplication with i as a rotation around the origin by 90 degrees. The big change around complex numbers, their arithmetic, geometry and, last but not least, their acceptance, however, came with the eminent Carl Friedrich Gauss.

In his doctoral thesis of 1799, the young Gauss gave another proof of the fundamental theorem (claiming that his proof was the first satisfying one). And in his theory of cyclotomy (included in his *Disquistiones Arithmeticae* (1801) [100, Section 7]), he used roots of unity for number theoretical investigations. In 1831/2, Gauss coined the name "complex number" in his *Theoria residuorum biquadraticorum, commentatio secunda* [101] on biquadratic residues and a biquadratic reciprocity law. Moreover, it was here that the *Gaussian integers*

$$a + \mathrm{i}b \quad \text{with } a, b \in \mathbb{Z}$$

and their sophisticated multiplicative structure first saw the light of day. In this context Gauss wrote:

> *After we had already begun to think about this subject in 1805, we soon came to the conclusion that the natural source of a general theory is to be found in an* extension of the field *of arithmetic* [...] *While the higher arithmetic in the questions dealt with so far only has to do with real integers, the propositions relating to the biquadratic remainders only appear in all their simplicity and natural beauty when the field of arithmetic is also extended to the* imaginary *numbers* [...][3]

Then, Gauss continued with defining the Gaussian integers as the counterparts of the ordinary rational integers in this extension. Indeed, Gauss observed that the set $\mathbb{Z}[\mathrm{i}]$ of those complex numbers has the structure of a factorial ring and may be considered as the counterpart of the ring $\mathbb{Z}$ of the rational integers within the field $\mathbb{Q}(\mathrm{i})$ of rational

[3] „Nachdem wir schon im Jahr 1805 über diesen Gegenstand nachzudenken begonnen hatten, kamen wir bald zu der Überzeugung, dass die natürliche Quelle einer allgemeinen Theorie in einer *Erweiterung des Feldes* der Arithmetik zu suchen sei [...] Während nämlich die höhere Arithmetik in den bisher behandelten Fragen es nur mit ganzen reellen Zahlen zu thun hat, erscheinen die auf die biquadratischen Reste bezüglichen Sätze nur dann in ihrer ganzen Einfachheit und natürlichen Schönheit, wenn das Feld der Arithmetik auch auf die *imaginären* Zahlen erstreckt wird [...]" [101, p. 540]. The text emphases are similar to those of the original.


Figure 1. Carl Friedrich Gauss (left) and Sir William Rowan Hamilton (right). The drawings were approximately made when Gauss studied the Gaussian integers and Hamilton discovered the quaternions, respectively. Hamilton was knighted in 1835 for his work in physics, however, Gauss was considered to be "princeps mathematicorum", which is Latin for *the foremost of mathematicians*.

Gaussian numbers. Of course, the notions of *ring* and *field* were not fixed at that time. Nevertheless, one may say that the rise of complex numbers and investigations into the arithmetic of algebraic number fields started with this influential paper.[4]

Another important contribution at that time appeared in the analytic studies of Augustin-Louis Cauchy. Inspired by Gauss's work on quadratic forms, Cauchy made calculations with complex numbers by computing real polynomials modulo $X^2 + 1$ which, in modern terms, rely on the isomorphism between the field of complex numbers and the quotient ring of real polynomials modulo the maximal ideal generated by $X^2 + 1$ (the minimal polynomial of $\sqrt{-1}$), i.e.,

$$\mathbb{C} = \mathbb{R}[\mathrm{i}] \simeq \mathbb{R}[X]/(X^2 + 1);$$

an important result that Leopold Kronecker would later generalize for the construction of field extensions.

[4]Euler had already used the imaginary unit as a tool for factoring quadratic forms, e.g. $xx + yy = (x + y\sqrt{-1})(x - y\sqrt{-1})$, and considered notions such as prime and coprimality; however, his investigations did not lead to a coherent theory. Jeremy Gray writes that, "[i]t is this combination of deep intuitive perceptiveness, going for the significance of numbers of a certain form, while making elementary errors in the logic of proof that provides an illustration of Euler's amazing ability to take the 'right' risks." [109, p. 20]

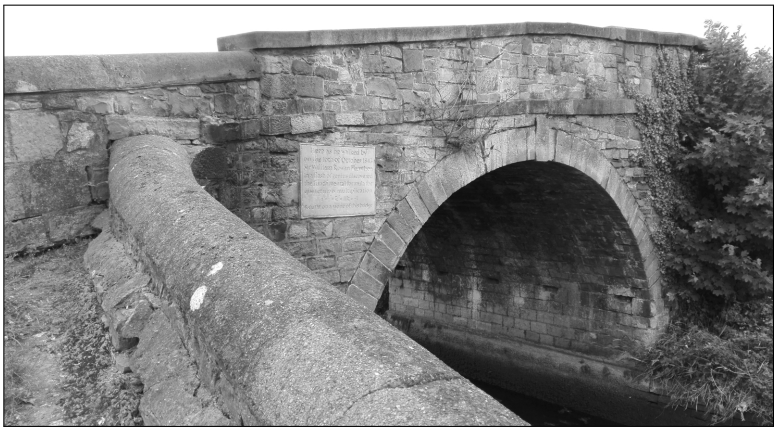


Figure 2. The inscription at Brougham (or Broom) Bridge in Dublin reads, "Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ & cut it on a stone of this bridge". Photo: Athanasios Sourmelidis

Quaternions are generalizations of complex numbers, first discovered by William Rowan Hamilton about 175 years ago.[5] At first, Hamilton tried to generalize complex numbers by triples of real numbers, and his son's daily question, "Well, Papa, can you multiply triplets?"[6] was always answered negatively. The innocent reader, who is unaware of the story and the mathematics behind it, may attempt to solve this problem on her or his own (but we suggest to do so only for short time).

After a struggle of 13 years, however, Hamilton had a breakthrough:

> *But on the 16th day of the month* [*October 1843*] *which happened to be a Monday and a council day of the Royal Irish Academy – I was walking along* [...] *the Royal Canal.* [...] *An electric current seemed to close, and a spark flashed forth, the herald (as I foresaw immediately) of many long years to come of definitely directed thought and work... I pulled out on the spot a pocket-book, which still exists, and made an entry there and then. Nor could I resist the impulse – unphilosophical as it may have been – to cut with a knife on a stone of Brougham Bridge the fundamental formula with the symbols* i, j, k*:*
>
> $$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1,$$

[5] The word *quaternion* is probably related to a scene in the New Testament where Herod the Great sends Saint Peter to jail: "he put him in prison, and delivered him to four quaternions of soldiers to keep him"; see *Acts of the Apostles*, 12.4.

[6] cf. [157, p. 153]

which contains the solution of the problem, but of course, as an inscription it has long since mouldered away.[7]

These are Hamilton's own words a short time before his death in 1865. In order to establish the quaternions Hamilton had to give up commutativity; for example,

$$\mathrm{ij} = \mathrm{k} \neq -\mathrm{k} = \mathrm{ji},$$

as follows from Hamilton's inscription on this very bridge in Dublin (by multiplying with k from the right and so forth). The (probably) *first* instance of non-commutativity appears in geometry with the symmetries of a regular triangle (or, using modern terms the non-commutative dihedral group D_3, isomorphic to the symmetric group S_3); matrices entered the stage only about a decade after the quaternions.

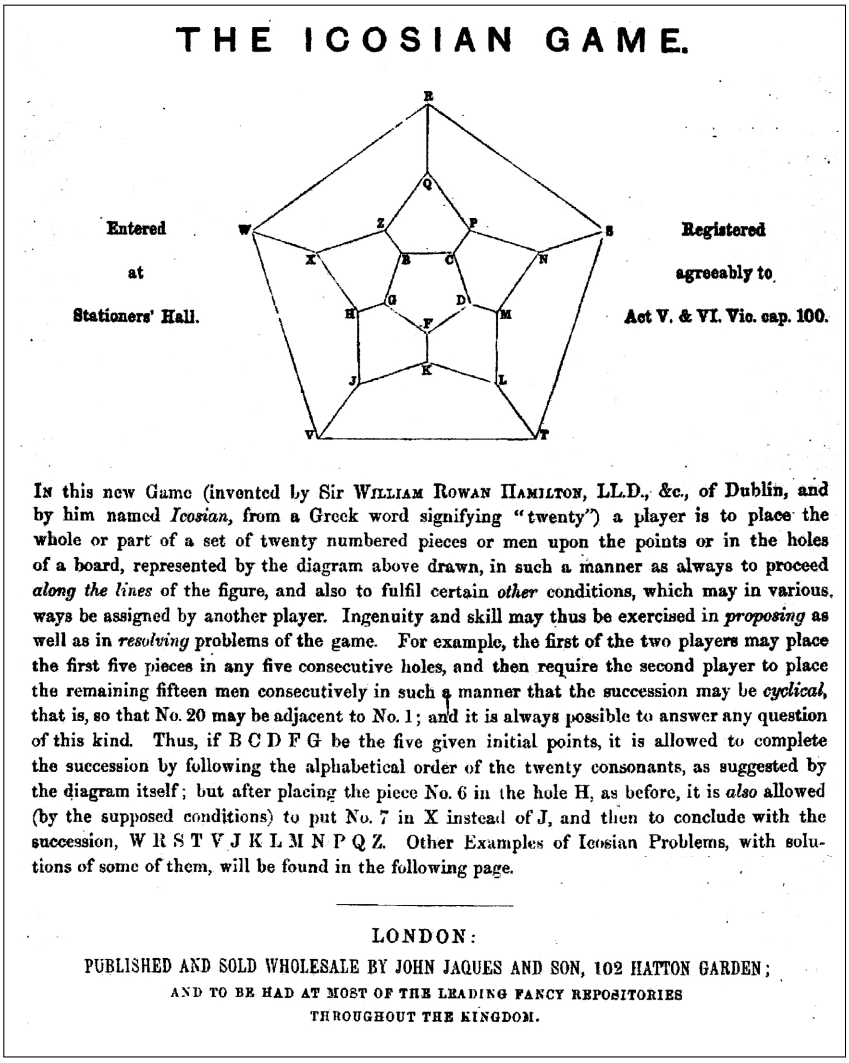
When it is about numbers, we want to add and subtract them, we want to multiply them and, if possible, to divide them. Moreover, there are further assumptions (or rules) about numbers in the background, like commutativity or associativity (although that was not explicitly mentioned in old texts since the 'classical numbers' simply follow these rules). Looking for extensions of the complex numbers, of course, one may have a *principle of permanence* in mind that certain properties of addition and multiplication should transfer to hypercomplex numbers. In this respect, the need to give up commutativity must have been an unexpected step!

A central role was played by those number systems which are closed with respect to these operations. For centuries, mathematicians worked implicitly with such number systems, e.g. $\mathbb{Q}$ and $\mathbb{R}$, without giving a definition of the underlying structures. It is worth noting that the first definition of a field had only been given by Dedekind in his supplements [40] from 1879 to Peter Gustav Lejeune Dirichlet's influential treatise [62] on number theory. Hamilton's quaternions, however, form a *skew field* (or division algebra in some literature), an alien object not observed before. At this time some contemporary mathematicians may have felt uncomfortable with the new concepts of complex or even hypercomplex numbers. On the contrary, Hamilton and some of his followers were rather enthusiastic about these numbers.

It is an interesting aside that in 1895 even an *International Association for Promoting the Study of Quaternions* was founded[8]. Actually, the turn of the century was the time of professionalization, global movements and, last but not least, internationalization. Felix Klein, however, was not too excited about this particular association. In his monograph on the development of mathematics in the 19th century [156], he wrote the rather harsh comment:

[7] cf. [254, p. 182]

[8] with 68 members in March 1900; see Hubert Kennedy's article [148] on one of the promoters, James Mills Peirce, in particular, and the cult of quaternions, in general.



THE ICOSIAN GAME.

Entered at Stationers' Hall.

Registered agreeably to Act V. & VI. Vic. cap. 100.

IN this new Game (invented by Sir WILLIAM ROWAN HAMILTON, LL.D., &c., of Dublin, and by him named *Icosian*, from a Greek word signifying "twenty") a player is to place the whole or part of a set of twenty numbered pieces or men upon the points or in the holes of a board, represented by the diagram above drawn, in such a manner as always to proceed *along the lines* of the figure, and also to fulfil certain *other* conditions, which may in various ways be assigned by another player. Ingenuity and skill may thus be exercised in *proposing* as well as in *resolving* problems of the game. For example, the first of the two players may place the first five pieces in any five consecutive holes, and then require the second player to place the remaining fifteen men consecutively in such a manner that the succession may be *cyclical*, that is, so that No. 20 may be adjacent to No. 1; and it is always possible to answer any question of this kind. Thus, if B C D F G be the five given initial points, it is allowed to complete the succession by following the alphabetical order of the twenty consonants, as suggested by the diagram itself; but after placing the piece No. 6 in the hole H, as before, it is *also* allowed (by the supposed conditions) to put No. 7 in X instead of J, and then to conclude with the succession, W R S T V J K L M N P Q Z. Other Examples of Icosian Problems, with solutions of some of them, will be found in the following page.

LONDON:

PUBLISHED AND SOLD WHOLESALE BY JOHN JAQUES AND SON, 102 HATTON GARDEN;

AND TO BE HAD AT MOST OF THE LEADING FANCY REPOSITORIES THROUGHOUT THE KINGDOM.

Figure 3. In the course of his investigations of quaternions, Hamilton designed the *Icosian game* about traveling along the edges of a dodecahedron. This turned out to be the birth of *Hamiltonian circuits* in graph theory; the game itself, however, was not too successful after its publication in 1857. For more information, we refer to Biggs et al. [17].

> *As I indicated before, Hamilton was followed by a school which surpassed their master in rigidity and intolerance.* [...] *The quaternions are fine and useful in their place; but their significance does not come up with the usual complex numbers.* [...] *The simplicity and elegance with which far-reaching theorems can be derived are indeed surprising and this may grasp the by far not hostile enthusiasm of the quaternionists for their system, which* [...] *soon grew beyond all rational limits neither being beneficial for mathematics in general nor for the theory of quaternions in particular.*[9]

The history of quaternions has been documented and studied quite intensively[10] (and some episodes can be found in this book). Our intention, however, is different. We focus on number-theoretical aspects of quaternions here. In order to motivate this theme, we first need to discuss the arithmetic of squares.

Integer squares are multiplicative objects in the first place, nevertheless they possess interesting additive features. In particular, sums of squares have been investigated for millennia. The ancient Greek mathematician Diophantus mentioned in his *Arithmetica* [56, Book III, Problem 19] (from the 3rd century), that

$$65 = 7^2 + 4^2 = 8^2 + 1^2$$

due to the fact that $65 = 13 \cdot 5$ and each factor is a sum of two squares.[11] Therefore, some mathematicians believe that he knew about the *two-square identity*

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 \mp b_1b_2)^2 + (a_1b_2 \pm a_2b_1)^2,$$

[9] „Wie ich schon andeutete, schloß sich Hamilton eine Schule an, die ihren Meister an Starrheit und Intoleranz noch überbot. [...] Die Quaternionen sind gut und brauchbar an ihrem Platze; sie reichen aber in ihrer Bedeutung an die gewöhnlichen komplexen Zahlen nicht heran. [...] Die Leichtigkeit und Eleganz, mit der sich hier die weittragendsten Theoreme ergeben, ist in der Tat überraschend, und es läßt sich wohl von hier aus die alles andere ablehnende Begeisterung der Quaternionisten für ihr System begreifen, die [...] nun bald über vernünftige Grenzen hinauswuchs, in einer weder der Mathematik als Ganzem noch der Quaternionentheorie selbst förderlichen Weise.“ [156, p. 184]

[10] For this purpose we refer once more to van der Waerden's *History of Algebra* [254] including an excellent survey on the discovery of algebras starting from complex numbers over Hamilton's quaternions up to the work of Emmy Noether, Helmut Hasse, and others. Another wonderful and even more extensive source on the development of numbers and algebras is the already mentioned collection [72] with valuable contributions by Max Koecher and Reinhold Remmert on divison algebras (including Hamilton's quaternions) amongst others. A highly readable brief account can be found in Chapter 20 of John Stillwell's second edition of his *Mathematics and Its History* [241].

[11] For details we refer to Stillwell [241, p. 417] and Heath [121, p. 167].


Figure 4. Claude Gaspard Bachet de Méziriac (left), Pierre de Fermat (right). Almost nothing is known about Diophantus. The translation of his *Arithmetica* into Latin by Bachet inspired many mathematicians, including Fermat.

which we nowadays may deduce from the multiplication rule for complex numbers,

$$(a_1 \pm \mathrm{i}b_1) \cdot (a_2 \pm \mathrm{i}b_2) = a_1a_2 \mp b_1b_2 \pm \mathrm{i}(a_1b_2 + a_2b_1),$$

by taking the respective norms.[12] The general formula appears in the works of Brahmagupta (in the seventh century), Abu Jafar Al-Khazin (c. 950), and Fibonacci (1225), who also provided a proof. Consequently, the set of sums of two squares is multiplicatively closed. Concerning the multiplicative structure, Pierre de Fermat discovered in 1640 (at the latest) the following remarkable theorem.

Two-square theorem. *Every prime number* $p \equiv 1 \bmod 4$ *can be represented as a sum of two integer squares.*

For instance,

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad \ldots, \quad 30449 = 100^2 + 143^2, \quad \ldots$$

The two-square theorem is indeed a surprising result: multiplicative objects as squares and primes in additive combination. Since squares are congruent to 0 or 1 modulo 4, primes $p \equiv 3 \bmod 4$ cannot be written as sums of two squares. In letters to his contemporaries,[13] Fermat communicated his method of infinite descent with which he

[12] And the even older Babylonian clay tablet 'Plimpton 322' (from around 1700 BCE) contains a list of pythagorean triples which, according to some speculations, are related to the identity above; see Stillwell [241, p. 385].

[13] namely to Pierre de Carcavi (1659) and to Christiaan Huygens (undated); see Walter William Rouse Ball [8, p. 296], Eric Temple Bell [11, p. 89], resp., [41, p. 65].

likely proved his statement on sums of two squares. The mathematical community worked a rather different way at that time; new results were usually distributed by letters to contemporaries, often enough without providing a hint of the proof. Fermat was probably aware of the two-square identity above; its first appearance in print, however, is in a paper from 1748 by Leonhard Euler. In the following year, Euler communicated the first rigorous proof of Fermat's two-square theorem in a letter to Christian Goldbach. A modern algebraic proof relies on the arithmetic of the ring $\mathbb{Z}[\mathrm{i}]$ of Gaussian integers (see Box J), namely the splitting of rational primes $p \equiv 1 \bmod 4$ as, for example,

$$5 = (2 - \mathrm{i})(2 + \mathrm{i}),$$

where neither $2 + \mathrm{i}$ nor $2 - \mathrm{i}$ are units (hence 5 is not a prime in this extended ring of integers). As a spin-off, the product leads via the norm immediately to the desired representation of 5 as a sum of two squares.

This splitting of primes in algebraic extensions marks the very beginning of what is now called *class field theory* and this line of investigation has prompted important results in algebraic number theory in the last two centuries. However, there is another idea arising from this observation and this very idea stands, as we shall see, at the beginning of the research started by Rudolf Lipschitz and continued by Adolf Hurwitz. It is the following supplement to the two-square theorem:

Four-square theorem. *Every positive integer can be represented as a sum of at most four integer squares.*

For example,

$$14 = 3^2 + 2^2 + 1^2, \quad 1770 = 41^2 + 9^2 + 2^2 + 2^2 = 42^2 + 2^2 + 1^2 + 1^2.$$

Three squares, however, are in general not sufficient, e.g. 7 or any other integer of the form $4^k(8\ell + 7)$ cannot be written as a sum of three squares (which follows from considering squares modulo 8). The squares constitute a rather small set within the set of positive integers[14], therefore it might be surprising that a small number of squares is sufficient to represent every positive integer. The four-square theorem was first conjectured in 1621 by Claude Bachet in his translation [56] of Diophantus's *Arithmetica* into Latin. This book, with its valuable editorial remarks by Bachet, had been a great inspiration for Fermat (and not only with respect to Fermat's last theorem). Diophantus's book is a collection of exercises which have to be solved numerically[15],

[14] Since there are n integer squares below n^2, their proportion tends with increasing n to zero.

[15] For example, Problem VII, 17 asks for finding a representation as a sum of four rational squares: $(13/3)^2 = 1^2 + (24/10)^2 + (4/3)^2 + (32/10)^2$.

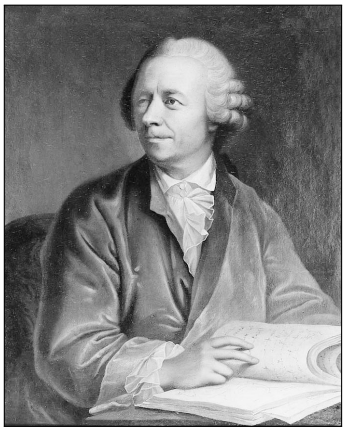
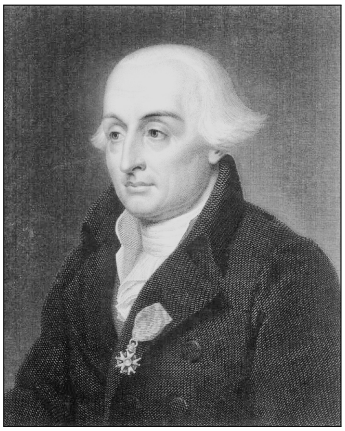



Figure 5. Leonhard Euler (left) and Joseph-Louis Lagrange (right). They established the two-square theorem as well as the four-square theorem; both were working in Berlin at the time of their proofs: Euler in 1748 as a member of the Prussian Academy of Sciences, which he had been offered by Frederick the Great of Prussia, and Lagrange as Euler's successor as the director of mathematics at the academy in 1770.

so his approach was rather explicit and by no means abstract. Nevertheless, Diophantus must have had a deep understanding and some of his exercises are indeed related to quite modern objects (for example, point addition on elliptic curves). In our story, however, more important are Bachet's comments guiding us to general or abstract results beyond the numerical examples.[16] Indeed, this book was an inspiration to many. In a letter to Marin Mersenne from 1636, Fermat first mentioned the statement of the four-square theorem[17] as well as the stronger one that every positive integer is a sum of three triangular numbers.[18]

[16]We refer to the monographs of Thomas Heath [121] and Ad Meskens [191] for this and further details on the reception of Diophantus's *Arithmetica*.

[17]In a letter to Kenelm Digby from 1658, Fermat communicated that he possessed a proof of the four square theorem: "I announce to your illustrious correspondents that I found a complete proof of it"; cf. [21, p. 61]

[18]This latter statement was first proved by the 19-year-old Gauss and is best documented by the entry "EUREKA num $= \Delta + \Delta + \Delta$" in his diary. A positive integer of the form $n = \frac{1}{2}m(m+1)$ is called a triangular number (taking into account that the sum $1 + 2 + \cdots + m$ can be illustrated by a triangle). Since every integer n is the sum of three triangular numbers $\frac{1}{2}m_j(m_j+1)$, it follows that $8n+3$ can be written as a sum of three squares $(2m_j+1)^2$ and this implies that $8n + 7 = 8n + 3 + 2^2$ is a sum of four squares. The remaining cases can be deduced from the two-square theorem and the four-square identitiy.

There is not only a counterpart to the two-square theorem, but also the two-square identity has an analogue, namely the *four-square identity*

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2)\\ = (a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2+(a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2\\ +(a_1b_3-a_2b_4-a_3b_1+a_4b_2)^2+(a_1b_4+a_2b_3-a_3b_2-a_4b_1)^2.\end{aligned}$$

In a remarkable letter to Christian Goldbach (May 1748) in which Euler communicated his proof of the two-square theorem, he also mentioned this four-square identity [98][19] which reduced the original problem to showing that every prime can be written as a sum of four squares; in view of the two-square theorem, the case of primes $p \equiv 1 \bmod 4$ is trivial. In 1770, Euler communicated his four-square identity to the young Joseph-Louis Lagrange who succeeded that same year in treating the remaining case of primes $p \equiv 3 \bmod 4$; his proof was published two years later as [165].

Although the two-square theorem concerns an arithmetical feature of integers, at its core is the multiplication rule for complex numbers. When it is about sums of four squares, however, the quaternions assume the role of the complex numbers.

In retrospect, it is not easy to understand Hamilton's path to his quaternions. Lacking knowledge of the works of Euler and Lagrange, he first aimed to generalize the two-square identity arising from the multiplication of two complex numbers to sums of three squares, although for anyone with a background in number theory, it is easy to produce a counterexample. For instance,

$$(1^2+1^2+1^2)(4^2+2^2+1^2) = 3\cdot 21 = 63 \neq x^2+y^2+z^2$$

for any integers x, y, z.[20] Precisely this example appeared in the third edition of Adrien-Marie Legendre's textbook [174] in 1830. Bartel van der Waerden commented on Hamilton's struggle: "Fortunately, he did not read Legendre: he was self-taught."[21]

[19] According to his notebooks, Euler discovered this formula between 1636 and 1640 (cf. [188, p. 604]). This result illustrates Euler's attempt to prove Fermat's open statements on sums of squares. What Euler could show about four squares was that every positive integer can be written as a sum of four *rational* squares, an example of such an identity can already be found in Diophantus's *Arithmetica* as Problem VII, 17; see [234] and footnote 15. Euler mentioned this result in a letter to Goldbach from 1749, and published it in 1754/60 as [82]. Goldbach and Euler discussed this, and further questions about sums of squares, in many letters during the 1740s. For further information on Euler's number-theoretical investigations, see Andre Weil's historical account [267].

[20] Since squares are $\equiv 0, 1$ or $4 \bmod 8$, it follows that $x^2+y^2+z^2 \not\equiv 7 \bmod 8$.

[21] [253, p. 234]. There is an interesting letter from Graves to Hamilton from 1844 about Euler's four square identity given in Legendre's book; cf. [241].

From our modern perspective on science, it is sometimes not easy to distinguish between the small progress made in developing a theory further and the great breakthroughs. We have been educated in a rather different context than that of Hamilton and his contemporaries, or the – soon to enter the stage – protagonists, Lipschitz and Hurwitz. It may serve as a good illustration to point out the parallel development of another non-mathematical subject. For instance, the first application for a patent for a lighter-than-air aircraft is from 1843, due to William Samuel Henson of London. This was in the same year that another William made his discovery of hypercomplex numbers about 288 ($= 12^2 + 12^2$) miles away on a neighboring island. Ferdinand Graf Zeppelin filed a patent for *his* aircraft in 1895 in Stuttgart, around the same time as Adolf Hurwitz began his studies on quaternions in Zurich; a distance of about 164 ($= 10^2 + 8^2$) kilometers.

The 19th century is well known for the Industrial Revolution and technological breakthroughs (such as aircraft), however, mathematics was also to develop from a shadowy existence to a modern discipline in the same period. In particular, through the rise of structures such as groups, invented by Évariste Galois, algebras by Hamilton, John Thomas Graves[22], Arthur Cayley, etc., and fields by Dedekind, to name just a few. Another – though not unrelated – example of the drastic changes in mathematical thinking from this period are the foundations of the number universes, the topic with which we started.

The first to investigate quaternions from a number theoretical point of view in a serious way was Rudolf Lipschitz in 1885/6 with his treatise *Untersuchungen über die Summen von Quadraten* [183]. However, his approach is rather difficult to read and his reasoning, in particular, not easy to follow. Nevertheless, Lipschitz gave a first quaternionic proof of Lagrange's four-square theorem. In 1896, Adolf Hurwitz published his notes [135] on the arithmetic of quaternions in the *Göttinger Nachrichten* and in 1919 he extended these studies to a booklet of 74 pages entitled *Vorlesungen über die Zahlentheorie der Quaternionen* [137], which appeared only half a year before Hurwitz's death (its English translation follows in Chapter II). The main difference between the work of Lipschitz and Hurwitz is the definition of what should be understood as the counterpart of integers within the set of quaternions. Here, it is worth recalling how Dedekind began his supplement to Dirichlet's treatise [40]:

[22] A Dublin born professor of jurisprudence at University College, London, fellow of the Royal Society of London and, in addition, hobby mathematician who was first teacher and later friend of Hamilton; he should not be confused with his younger brother Charles, who also became a notable mathematician.

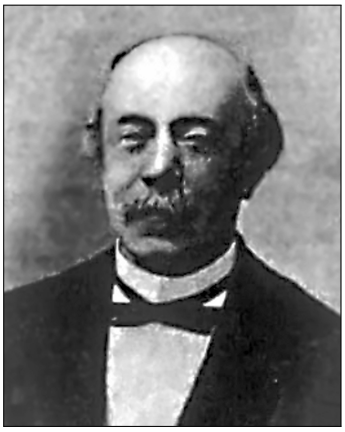



Figure 6. Portraits of Adolf Hurwitz (left) and Rudolf Lipschitz (right). The picture of Hurwitz was taken approximately when he started his studies on the arithmetic of quaternions in 1896. The quality of Lipschitz's picture does not allow to guess his age.

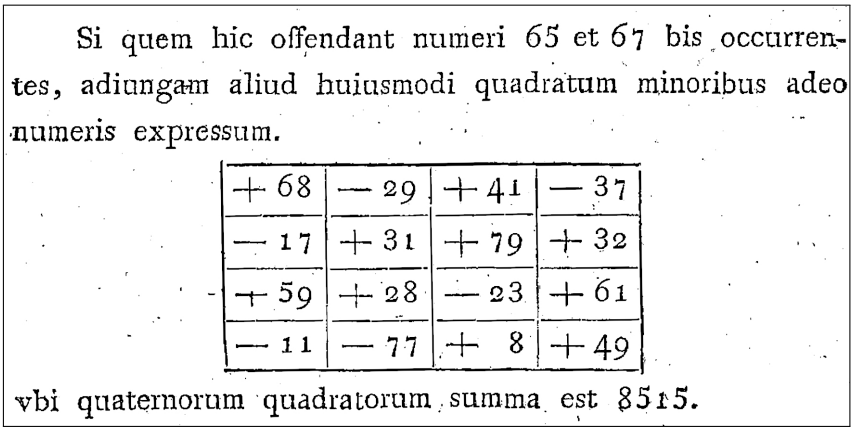
> *The notion of an* integer number *has found an extension in this century leading to entirely new lines in number theory; the first and most important step in this area has been done by Gauss* [...][23]

Dedekind refers here to Gauss's *Theoria residuorum biquadraticorum, commentatio secunda* [101], dealing with the arithmetic of Gaussian integers (and applications, as has already been mentioned above). Lipschitz defined integer quaternions by integral coefficients; for example $3 + 5\mathrm{i} - 7\mathrm{j} + \mathrm{k}$ is a *Lipschitz quaternion integer*. In addition to these quaternions, Hurwitz also considered quaternions with half integral coefficients as quaternion integers, for instance, $\frac{1}{2}(3 + 5\mathrm{i} - 7\mathrm{j} + \mathrm{k})$. On first glimpse it might be surprising that the definition of integer quaternions may lead to significant differences, however, in Lipschitz's arithmetic there is no unique factorization into prime elements in general, whereas Hurwitz obtained this cornerstone for number theory within his setting (up to non-commutativity). In this book we shall discuss why Hurwitz succeeded where Lipschitz failed and this will also explain how mathematics (sometimes) develops.

There is a famous example in number theory that nicely illustrates the role of definition and its impact on structure. In his attempt to solve the cubic Fermat equation

$$X^3 + Y^3 = Z^3,$$

[23] „Der Begriff der *ganzen Zahl* hat in diesem Jahrhundert eine Erweiterung erfahren, durch welche der Zahlentheorie wesentlich neue Bahnen eröffnet sind; den ersten und wichtigen Schritt auf diesem Gebiet hat *Gauss* gethan, [...]" [40, p. 434]


Si quem hic offendant numeri 65 et 67 bis occurrentes, adiungam aliud huiusmodi quadratum minoribus adeo numeris expressum.

+ 68	− 29	+ 41	− 37
− 17	+ 31	+ 79	+ 32
+ 59	+ 28	− 23	+ 61
− 11	− 77	+ 8	+ 49

vbi quaternorum quadratorum summa est 8515.

Figure 7. A magic square of squares found by Euler in 1770. The sums of the squares of all entries in every row, every column and both diagonals are all equal to 8515. Moreover, mixed sums as $68 \cdot (-17) + (-29) \cdot 31 + \cdots$ adds up to zero. This structure is related to orthogonality.

Euler considered the arithmetic of numbers of the form $a + b\sqrt{-3}$ with integer coefficients a and b. For his aim to apply Fermat's method of infinite descent he required unique prime factorization for the ring $\mathbb{Z}[\sqrt{-3}]$ (see [87]), however, this ring is not factorial. Using unique prime factorization in the slightly larger factorial ring $\mathbb{Z}[\frac{1}{2}(1 + \sqrt{-3})]$ of algebraic integers, however, one can make Euler's reasoning watertight. The gap Euler had left was filled by Gauss [102] using indeed complex numbers of the form $\frac{1}{2}(a + b\sqrt{-3})$. Thus, Gauss worked with the *better suited* ring of integers.[24]

In his booklet, Hurwitz established a number theory of quaternions that goes beyond Lipschitz's work (which had a stronger focus on sums of squares and was not intended to build an arithmetic theory). Another example of the power of Hurwitz's approach is a quaternionic solution to Euler's magic square of squares problem (in the final *lecture* according to Hurwitz's naming of the chapters of his booklet). Here, Hurwitz applied quaternion arithmetic to deduce some rational parametrization, which Euler had found for orthogonal 4×4-matrices by educated guesses.

Although there is much more to be said about the history of quaternions and sums of squares, we stop our introduction here and hand the words over to Hurwitz ...

[24] For this and more details on their reasoning with respect to the cubic case of Fermat's last theorem, we refer to Paulo Ribenboim's monograph [221, Chapter I.2], as well as to Günter Bergmann's careful analysis [14].