

$x \times y$  from

$$x \times y = 2^a \times 2^b = 2^{a+b}$$

by forming the sum  $a+b$  and looking up its “antilogarithm”  $2^{a+b}$ . The logarithm function was originally invented for this purpose, and only later found to be the area under the hyperbola. It seems even more remarkable that the complex exponential function  $e^{i\theta}$  turned out to be  $\cos \theta + i \sin \theta$  (Euler (1748)). However, hints of this relationship had been around for centuries, and we have seen some of them, for example, Viète’s “product of triangles” discussed in Section 7.2.

Perhaps the most remarkable thing is that  $e^z$  can be defined, for complex  $z$ , in a completely geometric manner. Consider the problem of mapping the *cartesian coordinate grid*, of lines  $x = \text{constant}$  and  $y = \text{constant}$ , onto the *polar coordinate grid* of radial lines  $\theta = \text{constant}$  and concentric circles  $r = \text{constant}$ . Putting  $z = x + iy$ , we see that  $e^z = e^x(\cos y + i \sin y)$  does the trick: the line  $x = \text{constant}$  is mapped onto the circle of radius  $e^x$ , and the line  $y = \text{constant}$  is mapped onto the ray  $\theta = y$ .

This map *preserves angles*, not through any special merit of  $e^z$ , because in fact the same is true of most of the complex functions one meets. In this case, one can see immediately that the right angles between the lines  $x = \text{constant}$  and  $y = \text{constant}$  map to right angles between the radial lines and the circles in the polar coordinate grid.

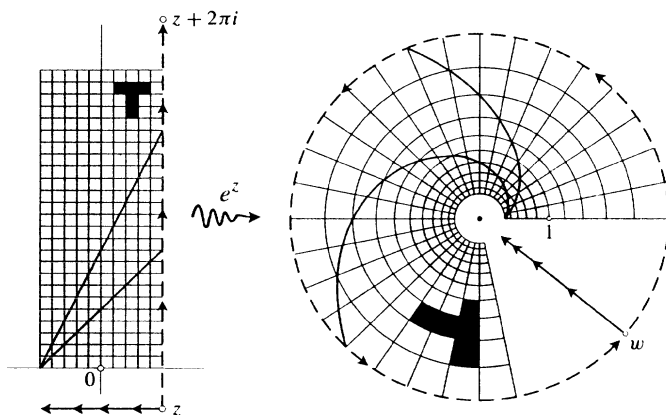


FIGURE 9.10 The exponential map.

It is more interesting to observe what happens to a diagonal through the “little squares” in the cartesian coordinate grid (Figure 9.10). It is mapped to an *equiangular spiral* through the “little quadrilaterals” in the polar coordinate grid, and these “quadrilaterals” have to grow exponentially in size to maintain the constant angle of the spiral.

Conversely, any angle-preserving map from the cartesian grid to the polar grid forces exponential growth on the image circles  $r = \text{constant}$ . Thus if one starts with the circle and the concept of angle, one is led inexorably to the arithmetic of exponentiation. More about the relation between geometric and arithmetic properties of complex functions may be found in the beautiful book of Needham (1997), from which Figure 9.10 is taken.

## From Pythagoras to Pell

The two most important quadratic equations in this book are the Pythagorean equation

$$a^2 + b^2 = c^2$$

and the Pell equation

$$x^2 - dy^2 = 1.$$

We have seen how Pythagoras’ theorem leads to the discovery that the diagonal of the unit square is  $\sqrt{2}$ , which in turn confronts us with the problem of understanding the irrational number  $\sqrt{2}$ .

This leads to the Pell equation  $x^2 - 2y^2 = 1$ , whose integer solutions  $x = x_n$ ,  $y = y_n$  give a sequence of rationals  $x_n/y_n$  converging to  $\sqrt{2}$ . The same rationals arise from the continued fraction

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \ddots}}}$$

and the latter is surely the simplest “explanation” of  $\sqrt{2}$  in terms of rational numbers.

In attempting to understand  $\sqrt{d}$ , for any nonsquare positive integer  $d$ , we follow a similar approach: find the solutions of the Pell

equation  $x^2 - dy^2 = 1$ , and the continued fraction for  $\sqrt{d}$ . The emphasis shifts, however, as one discovers that understanding is helped by actual use of the number  $\sqrt{d}$ . In fact, it is helpful to use all the real numbers and the transcendental functions  $\cosh$  and  $\sinh$ . This is the message of Section 9.6.

There we gave an arbitrary point  $(x, y)$  on the hyperbola  $x^2 - dy^2 = 1$  the coordinate  $\theta$  such that

$$x = \cosh \theta, \quad y = \frac{1}{\sqrt{d}} \sinh \theta.$$

We represented each *integer* point  $(x, y)$  by the quadratic integer  $x + y\sqrt{d}$ . Notice that

$$x + y\sqrt{d} = \cosh \theta + \sinh \theta = e^\theta,$$

so the integer points are represented by quadratic integer values of the exponential function  $e^\theta$ .

The quadratic integers  $x + y\sqrt{d}$  such that  $x^2 - dy^2 = 1$  have the property that the product of any two of them,  $x_1 + y_1\sqrt{d}$ ,  $x_2 + y_2\sqrt{d}$ , is another quadratic integer  $x_3 + y_3\sqrt{d}$  with the same property. It follows that they form an abelian group under  $\times$ , and their logarithms form an abelian group under  $+$ . The essence of the proof in Section 9.6 is to use logarithms to convert the group of quadratic integers with the  $\times$  operation to the group of  $\theta$  values with the  $+$  operation, which is easier to understand.

In this instance it is possible to understand the multiplicative group without the help of logarithms, and many number theory books do this. However, the current proof has certain merits. The exponential function is naturally associated with the hyperbola  $x^2 - dy^2 = 1$  anyway, and the proof is a model for a more general theorem in which logarithms are always used: *Dirichlet's unit theorem*. The Pell equation solution is essentially the one-dimensional case of this theorem; the general case may be found in books on algebraic number theory, for example, Samuel (1970).

The solution of  $x^2 - dy^2 = 1$  shows that all solutions are generated in a simple way from the smallest nontrivial solution, but the nature of this smallest solution remains a mystery. Dirichlet's pigeonhole argument shows that it must exist (Section 8.7\*) but does not relate it to  $d$  in any reasonable way. In fact, its dependence on  $d$  is highly

irregular, judging from notorious values like  $d = 61$ , for which the smallest positive solution is  $x = 1766319049$ ,  $y = 226153980$ .

There is probably no *simple* relationship between  $d$  and the smallest solution, but there is an extremely interesting relationship, also discovered by Dirichlet. It is called his *class number formula*, and it relates the smallest solution of  $x^2 - dy^2 = 1$  to the so-called *class number* of the quadratic integers  $x + y\sqrt{d}$ , a measure of their deviation from unique prime factorization. For an introduction to this deep and complicated subject, see Scharlau and Opolka (1985), or see Dirichlet's own treatment in Dirichlet (1867).

The hidden depths of the Pell equation opened into a yawning chasm in recent decades, with unexpected discoveries in mathematical logic. Since the time of Lagrange, mathematicians have known general algorithms for finding integer solutions of quadratic equations, or more importantly, deciding whether solutions exist. (The solution of the Pythagorean equation was the first success in this field, and Lagrange found that the solution of the Pell equation opened the door to all other quadratics.) But no general algorithms for higher-degree equations were ever discovered, and in 1970 Yuri Matijasevič proved that *there is no such algorithm*. The idea of his proof is to show that polynomial equations are complex enough to “simulate” arbitrary computations, because results from logic tell us that no algorithm can answer all questions about computation. The biggest technical difficulty is finding a single equation that is manageable yet sufficiently complex. It turns out to be none other than the Pell equation! The proof, which has now been boiled down to simple number theory, may be seen in Jones and Matijasevič (1991).

# Bibliography

- Artin, M. (1991). *Algebra*. Prentice-Hall.
- Artmann, B. (1988). *The Concept of Number*. Halsted Press.
- Baker, A. (1984). *A Concise Introduction to the Theory of Numbers*. Cambridge University Press.
- Beltrami, E. (1868). Teoria fondamentale degli spazii di curvatura costante. *Annali di Matematica pura et applicata, series II*, **II**, 232–255. English translation, *Fundamental Theory of Spaces of Constant Curvature*, in Stillwell (1996), 41–62.
- Bombelli, R. (1572). *L'Algebra*. Reprinted by Feltrinelli Editore, Milan, 1966.
- Cassels, J. W. S. (1991). *Lectures on Elliptic Curves*. Cambridge University Press.
- Colebrooke, H. T. (1817). *Algebra, with Arithmetic and Mensuration, from the Sanscrit of Brahme Gupta and Bháskara*. John Murray, London. Reprinted by Martin Sandig, Wiesbaden, 1973.

- Cormen, T. H., Leiserson, C. E., and Rivest, R. L. (1990). *Introduction to Algorithms*. MIT Press.
- Dedekind, R. (1872). *Stetigkeit und Irrationalzahlen*. English translation, *Continuity and Irrational Numbers*, in *Essays on the Theory of Numbers*, Open Court, 1901.
- Dedekind, R. (1877). *Sur la Théorie des Nombres Entiers Algébriques*. Gauthier-Villars. English translation, *Theory of Algebraic Integers*, Cambridge University Press, 1996.
- Dedekind, R. (1888). *Was sind und was sollen die Zahlen?* Braunschweig. English translation in *Essays on the Theory of Numbers*, Open Court, Chicago, 1901.
- Descartes, R. (1637). *La Géométrie*. English translation, *The Geometry*, Dover, 1954.
- Dirichlet, P. G. L. (1837). Beweis der Satz, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftliche Factor sind, unendliche viele Primzahlen enthält. *Abhandlungen der Königl. Preussische Akademie der Wissenschaften*, pages 45–81. Also in his *Mathematische Werke*, volume 1, 313–342.
- Dirichlet, P. G. L. (1867). *Vorlesungen über Zahlentheorie*. Vieweg. Fourth edition (1894) reprinted by Chelsea, New York, 1968.
- Ebbinghaus, H.-D., Hermes, H., Hirzebruch, F., Koecher, M., Mainzer, K., Neukirch, J., Prestel, A., and Remmert, R. (1991). *Numbers*. Springer-Verlag.
- Euler, L. (1748). *Introductio in analysin infinitorum*. In his *Opera Omnia*, series 1, volume VIII. English translation, *Introduction to the Analysis of the Infinite*, Springer-Verlag, 1988.
- Euler, L. (1770). *Vollständige Einleitung zur Algebra*. In his *Opera Omnia*, series 1, volume I. English translation, *Elements of Algebra*, Springer-Verlag, 1984.
- Gauss, C. F. (1801). *Disquisitiones Arithmeticae*. In his *Werke*, volume 1. English edition published by Springer-Verlag, 1986.
- Grassmann, H. (1861). Stücke aus dem Lehrbuche der Arithmetik. *Hermann Grassmann's Mathematische und Physikalische Werke*, **II/1**, 295–349.

- Guy, R. K. (1994). *Unsolved Problems in Number Theory*. Springer-Verlag.
- Hasse, H. (1928). Über eindeutige Zerlegung in Primelemente oder in Primhauptideal in Integrätsbereichen. *Journal für reine und angewandte Mathematik*, **159**, 3–12.
- Heath, T. L. (1910). *Diophantus of Alexandria*. Cambridge University Press. Reprinted by Dover, 1964.
- Heath, T. L. (1912). *The Works of Archimedes*. Cambridge University Press. Reprinted by Dover, 1953.
- Heath, T. L. (1925). *The Thirteen Books of Euclid's Elements*. Cambridge University Press. Reprinted by Dover, 1956.
- Hilbert, D. (1899). *Grundlagen der Geometrie*. B. G. Teubner, Stuttgart. English translation, *Foundations of Geometry*, Open Court, Chicago, 1971.
- Jones, G. A., and Singerman, D. (1987). *Complex Functions*. Cambridge University Press.
- Jones, J. P., and Matijasevič, Y. V. (1991). Proof of the recursive unsolvability of Hilbert's tenth problem. *American Mathematical Monthly*, **98**, 689–709.
- Katz, V. (1993). *A History of Mathematics*. HarperCollins.
- Koblitz, N. (1985). *Introduction to Elliptic Curves and Modular Forms*. Springer-Verlag.
- Magnus, W. (1974). *Noneuclidean Tessellations and Their Groups*. Academic Press.
- Needham, T. (1997). *Visual Complex Analysis*. Oxford University Press.
- Neugebauer, O., and Sachs, A. (1945). *Mathematical Cuneiform Texts*. Yale University Press.
- Niven, I., Zuckerman, H. S., and Montgomery, H. L. (1991). *An Introduction to the Theory of Numbers*. Wiley.
- Pascal, B. (1654). *Traité du triangle arithmétique*. *Pascal Œuvres Complètes*. Éditions du Seuil, 1963. English translation, *Treatise on the Arithmetic Triangle*, in *Great Books of the Western World: Pascal*, Encyclopedia Britannica, 1952, 447–473.