

## ! On Provability Versus Consistency in Elementary Mathematics

Shailesh A Shirali  
Rishi Valley School  
A.P.

A reader asks, “*Why is 1 not listed as a prime? After all, does it not satisfy the stated criteria for primality?*” This note is written in response to this question.

The layperson usually thinks that mathematics deals with absolute truths, and indeed this was how mathematics was viewed during earlier centuries. However ever since the epochal discoveries of Bolyai, Lobachevsky and Riemann that there can be geometries (note the plural) other than the one presented in Euclid’s text *The Elements*, this implicit notion had to be dropped. Even the notion that everything in mathematics is provably true or provably false had to be abandoned, after the astonishing results obtained by Gödel in 1930. Alongside this development, mathematics has seen a pioneering and extremely productive method: the axiomatic method, in which new areas of mathematics get created merely by defining suitable sets of axioms. As a result, the accent in mathematics has to some extent shifted to the study of axiomatic systems, and the essential question in such cases has become one of consistency and richness of the axiom system rather than its intrinsic truth or falsity. Much of modern algebra, starting with group theory, the theory of fields and rings and vector spaces and so on can be viewed in this light. Loosely speaking, one might say that in the modern mathematical paradigm, *true* is roughly equivalent to *consistent* while *false* is equivalent to *self-contradictory*<sup>1</sup>.

Here are some instances to illustrate the theme of consistency as opposed to absolute truth. In school arithmetic, one encounters the question, “*Why is  $-1 \times -1 = 1$ ?*” Many ‘proofs’ are offered, but the plain fact is that the relation is a *convention*, not an absolute truth, and therefore there is no question of proving it<sup>2</sup>. One adopts it because of its implication for the law of distributivity of

<sup>1</sup>It is an interesting commentary on the psychology of modern mathematicians that, when pressed, most of them will readily say that there is no such thing as absolute truth in mathematics, and that a mathematical proposition is true or false only with reference to a particular axiomatic system. But amongst themselves most mathematicians ‘know’ that what they deal with does indeed refer to something ‘concrete’, ‘real’ and ‘absolute’!

<sup>2</sup> Here is a particularly preposterous proof which I encountered a few years back: the parabola  $y=x^2$  is symmetric in the  $y$ -axis, therefore minus times minus equals plus!



multiplication over addition (LDMA for short), according to which  $a(b+c) = ab+ac$  for all  $a, b, c$ . The LDMA is too valuable an axiom to lose! Here is roughly how it happens. Starting with  $\mathbf{N}$  the set of positive integers, with  $\times$  and  $+$  defined on  $\mathbf{N}$  in the usual manner, we enlarge the set by including 0 and imposing the following rules:

$$a+0 = 0+a = a, \quad a \times 0 = 0 \times a = 0.$$

Note that the two statements are consistent with one another because of the LDMA. For example,  $2 \times 3 = 2 \times (3+0) = 2 \times 3 + 2 \times 0$ , so we must have  $2 \times 0 = 0$ . Next, one constructs the negative numbers via the rule  $a + (-a) = 0$ . To do addition we call upon commutativity and associativity. For instance we have:

$$(-2) + (-3) + (2+3) = (-2) + 2 + (-3) + 3 = 0 + 0 = 0.$$

Therefore  $(-2) + (-3) + 5 = 0$  and  $(-2) + (-3) = -5$ .

Finally, multiplication is taken up, and here one invokes distributivity. We find that we are forced to adopt the convention that  $-1 \times 1 = -1$  and  $-1 \times -1 = 1$ :

$$0 = 0 \times 1 = \{(1+(-1))\} \times 1 = \{1 \times 1\} + \{(-1) \times 1\} = 1 + \{(-1) \times 1\},$$

therefore  $(-1) \times 1 = -1$ ; and,

$$0 = \{1+(-1)\} \times (-1) = \{1 \times (-1)\} + \{(-1) \times (-1)\} = -1 + \{(-1) \times (-1)\},$$

therefore  $(-1) \times (-1) = +1$ . *The point is that we need these relations if we are to preserve the LDMA, which we cannot afford to lose. The consistency of the system must be preserved at all cost<sup>3</sup>.*

<sup>3</sup> Sacrificing the LDMA would mean that we lose the ring structure of  $\mathbf{Z}$ .

Here is another question, also asked at the school level: Why is  $a^0 = 1$  for all  $a > 0$ ? We proceed to resolve this in a similar vein. Let  $x, y \in \mathbf{N}$ ; then  $a^{x+y} = a^x \times a^y$  and  $a^{x-y} = a^x / a^y$  when  $x > y$ . These follow from the very meaning of  $a^n$  when  $n$  is a positive



integer. What do we do with  $a^0$ ? If we wish to have a system of algebra that is consistent and easy to work with, then we need to adopt the convention that  $a^0=1$ . There is nothing absolute about this. Rather, we *choose* to give  $a^0$  a meaning that makes it easy to deal with. In short, we make  $a^0$  a well-behaved object. (Note that  $0^0$  cannot be given any consistent meaning, nor  $0/0$ ; that is, it is not possible to make these objects well-behaved.)

Finally we take up the question: “*Is 1 a prime?*” We recall the fundamental theorem of arithmetic (FTA): *Every integer  $N > 1$  can be expressed in just one way as a product of primes, except possibly for the order of occurrence of the primes.* If 1 were included in the set of primes  $\mathbf{P}$ , then the fact that  $1^n = 1$  for all integers  $n$  would require us to rephrase the FTA by adding the clause “... except that 1 may occur to any arbitrary power.” We would end up labelling 1 as a special prime, to be excluded from most of the interesting theorems about prime numbers. Indeed, what would in all likelihood happen is that theorems about primes would end up being phrased in terms of the set  $\mathbf{P}' = \mathbf{P} \setminus \{1\}$ . Thus giving 1 membership in  $\mathbf{P}$  proves to be a nuisance, and it is simpler to keep it out right at the start.

The matter can be considered from another viewpoint. Let  $\mathbf{Z}$  denote the set of integers, and consider the set of complex numbers of the form  $a + bi$ , where  $a, b \in \mathbf{Z}$ , and  $i = \sqrt{-1}$ . These are the *Gaussian integers* first studied in detail by Gauss, and the set of such numbers is denoted by  $\mathbf{Z}(i)$ . (Note that  $\mathbf{Z}$  is a subset of  $\mathbf{Z}(i)$ .) Now in  $\mathbf{Z}$ , the only elements that possess multiplicative inverses are  $\pm 1$  (that is, their reciprocals lie within the same set); these are the *units* of  $\mathbf{Z}$ . In  $\mathbf{Z}(i)$ , the set of units turns out to be  $\{ \pm 1, \pm i \}$ . (The reader is invited to verify that there are no other units in  $\mathbf{Z}(i)$ .) Arithmetic can be done in  $\mathbf{Z}(i)$  just as it is in  $\mathbf{Z}$ ; for instance, we can factorize numbers:

$$9 + 7i = (2 + 3i)(3 - i), \quad 13 = (2 + 3i)(2 - 3i), \quad \dots$$

Observe that 13, which is prime in  $\mathbf{Z}$ , loses its primality status in  $\mathbf{Z}(i)$ .

The accent in mathematics has to some extent shifted to the study of axiomatic systems, and the essential question in such cases has become one of consistency and richness of the axiom system rather than its intrinsic truth or falsity.



<sup>4</sup> Since this article deals with terminology, it should be pointed out that what we refer to as 'prime' here is usually called 'irreducible' in the standard texts. In the standard definition,  $p$  is prime if we have the implication  $p \mid ab \Rightarrow p \mid a$  or  $p \mid b$ . In the class of rings known as UFD's the two notions coincide. Examples of UFD's are  $\mathbf{Z}$ ,  $\mathbf{Z}(i)$  and  $\mathbf{Z}(\sqrt{2})$ . However  $\mathbf{Z}(\sqrt{10})$  is not a UFD.

<sup>5</sup>Units may enter the picture, hence the use of the words 'essentially only one way'.

We declare a number  $z \in \mathbf{Z}(i)$  to be *prime* if  $z$  is not a unit and if in every factorization  $z = uv$ , with  $u, v \in \mathbf{Z}(i)$ , either  $u$  or  $v$  is a unit<sup>4</sup>. The reader is invited to verify that 3, 7 and  $2+3i$  are Gaussian primes, whereas 2, 5 and 13 are composite (because  $2 = (1+i)(1-i)$ ,  $5 = (1+2i)(1-2i)$ , etc.). We now have the result: *every number in  $\mathbf{Z}(i)$ , not 0 or a unit, can be written as a product of Gaussian primes; moreover, there is essentially only one way of doing this*<sup>5</sup>. That is, we have an analogue of the FTA for the Gaussian integers, provided that the units are not considered as primes.

Other such number systems can be constructed. Indeed, once one grasps the idea, such systems seem to be available in abundance and can be spotted in many settings. For instance, consider the set  $\mathbf{Z}(\sqrt{2})$  whose elements are number of the form  $a + b\sqrt{2}$  where  $a, b \in \mathbf{Z}$ . This system presents itself quite naturally when one tries to solve the equation  $x^2 - 2y^2 = \pm 1$  in integers. A striking fact about  $\mathbf{Z}(\sqrt{2})$  is that it has infinitely many units. (The reader is invited to solve this. Hint: Show that  $\sqrt{2} - 1$  and its integral powers are units; (harder) show that these are the *only* units of  $\mathbf{Z}(\sqrt{2})$ .) What are the primes of  $\mathbf{Z}(\sqrt{2})$ ? It turns out that  $\sqrt{2}$  is prime, as are the numbers 3, 5 and 11, but not 7, because  $7 = (3 - \sqrt{2}) \times (3 + \sqrt{2})$ , nor 17, because  $17 = (5 - 2\sqrt{2}) \times (5 + 2\sqrt{2})$ . It is an interesting exercise to classify the primes of  $\mathbf{Z}(i)$  and  $\mathbf{Z}(\sqrt{2})$ . Is there an analogue of the FTA for  $\mathbf{Z}(\sqrt{2})$ ? The answer is "yes", though it is hard work to prove it. However there are numerous number systems that closely resemble  $\mathbf{Z}(i)$  and  $\mathbf{Z}(\sqrt{2})$  but which do not have the FTA property. An example is  $\mathbf{Z}(\sqrt{10})$ : it can be shown that 2, 3,  $4 - \sqrt{10}$  and  $4 + \sqrt{10}$  are primes in  $\mathbf{Z}(\sqrt{10})$ , yet

$$6 = 2 \times 3 = (4 - \sqrt{10}) \times (4 + \sqrt{10}),$$

providing a counter example to the FTA. Perhaps it is phenomena of this type that make number theory a fascinating subject. As the reader will have noted by now, the word *prime* no longer carries a fixed meaning; it acquires meaning only with



reference to a particular context<sup>6</sup>. The interested reader could consult the well-known text by G H Hardy and E M Wright (*An Introduction to the Theory of Numbers*, Chapters XIV and XV) for further details.

<sup>6</sup>Historically, many of these developments were a result of efforts to prove Fermat's last theorem. See *Resonance*, Volume 1, No. 1 for more details.

Here is another example of axiomatic generalization. A rational number can be thought of as a root of the equation  $mx+n=0$ , with  $m, n \in \mathbf{Z}, m \neq 0$ ; here  $m=1$  gives us the integers — we call these the *rational integers*. Generalizing, we define an *algebraic number* as a root of the polynomial equation  $ax^n + bx^{n-1} + cx^{n-2} + \dots = 0$  with  $a, b, c, \dots \in \mathbf{Z}, a \neq 0$  and  $n \in \mathbf{N}$ ; if  $a=1$  then we have an *algebraic integer*. It is a non-trivial fact that the set  $\mathbf{A}$  of *algebraic integers* is closed under addition and multiplication but not under division. Thus  $\mathbf{A}$  behaves very much like  $\mathbf{Z}$ , and we have at hand a genuine generalization of the notion of integer.

These examples may serve to highlight the extraordinary freedom that the axiomatic approach brings into mathematics. Some critics complain, however, that in exercising this freedom mathematicians tend to “go too far”; but that is another matter altogether and we shall not address it in this note.

---

TAILPIECE: Mr T B Nagarajan of Thanjavur has sent me the following problem: *Find four distinct positive integers such that the sum of any two of them is a square*. He writes that the problem is not too hard if the restriction on positivity is removed, or if one is content with solutions having very large integers. In support of this statement, he lists the following solutions:

{55967, 78722, 27554, 10082}, {15710, 86690, 157346, 27554}.

Readers are invited to take a crack at the problem. (To find a *triple* with the stated property is much easier; an example is provided by {6, 19, 30}. Readers may enjoy trying to list further such triples before going on to the more challenging four-number problem.)

