Parabola Volume 25, Issue 2 (1989)

WHICH INTEGERS HAVE RATIONAL SQUARE ROOTS?

Werner Ricker*

Recall that a real number is called rational if it can be expressed in the form p/q where p and q are integers with $q \neq 0$. Numbers which are not rational are called irrational. The theme of this article is to address the problem of how to determine whether the square root α of a positive integer is rational or not. As the definition suggests, we have to exhibit a pair of integers p and q (with $q \neq 0$) such that $\alpha = p/q$ or show that no such pair p and q exists. Which of these two possibilities is the case depends, of course, on the properties particular to the number α under consideration.

Let us begin with our "old friend" $\sqrt{2}$ which, by definition, is the unique positive number β satisfying $\beta^2 = 2$ (we will assume that such a number β actually exists). If $\sqrt{2}$ was a rational number there would exist positive integers p and q satisfying $\sqrt{2} = p/q$. By cancelling (if necessary) it can be assumed that p and q have no common divisors (other than 1 and -1, of course). Now $p^2/q^2 = 2$ and so

$$p^2 = 2q^2. \tag{1}$$

This shows that 2 divides $p^2 = pp$ (as 2 certainly divides the right-hand- side of (1)). Now 2 has the property that if it divides the product ab of two integers a and b, then it divides either a or b. Accordingly, 2 must divide p and so $p = 2k$ for some positive integer k. Substituting this into (1) gives $4k^2 = 2q^2$ or, equivalently,

$$q^2 = 2k^2. \tag{2}$$

This shows that 2 also divides $q^2 = qq$ (as 2 surely divides the right-hand-side of (2)) and so, arguing as before, we can conclude that 2 must divide q itself. Hence, it has been shown that 2 divides both p and q which is contrary to the choice of p and q having no common divisor. This contradiction arises from the original assumption that $\sqrt{2}$ is rational. Accordingly, this assumption is invalid and so $\sqrt{2}$ is irrational.

This simple argument was deliberately spelt out in detail because its method of reasoning can be used to establish much more. The essential point is that the number 2 has

* Lecturer in mathematics at the University of N.S.W.

the property that if it divides a product ab of two integers a and b, then it divides at least one of them. There is a familiar set of positive integers having the same property, namely the prime numbers $\{2, 3, 5, 7, 11, 13 \cdots\}$; these are (by definition) those positive integers α with the property that their only (positive) divisors are 1 and α. We will need the following two properties of prime numbers.

Property 1. *Every positive integer n has a unique factorization of the form $n = b_1^{m_1} b_2^{m_2} \cdots b_k^{m_k}$, where the $b_1, \cdots, b_k$ are the distinct prime factors of n and the $m_1, \cdots, m_k$ are positive integers.*

For example, $1500 = 2^2.3^1.5^3$ and so we can choose $b_1 = 2, b_2 = 3, b_3 = 5$ and $m_1 = 2, m_2 = 1, m_3 = 3$.

Property 2. *If $\{\alpha_1, \cdots, \alpha_r\}$ is a finite collection of positive integers and b is a prime number dividing their product $\alpha_1.\alpha_2.\cdots\alpha_r$, then b divides at least one of the numbers $\alpha_1, \alpha_2, \cdots, \alpha_r$.*

If you experiment with a few examples it quickly becomes evident that these properties are at least plausible; they are established in any reasonable book on elementary number theory (see the reference [1], for example).

Equipped with these two properties and the proof of the irrationality of $\sqrt{2}$ we can now describe <u>all</u> positive integers n for which $\sqrt{n}$ is irrational. Call a positive integer n a <u>perfect square</u> if there exists another positive integer m such that $n = m^2$. For such an integer n it is clear that $\sqrt{n}$ is a rational number; indeed, $\sqrt{n} = m$ is actually an integer. The following result shows that these are the only positive integers whose square root is rational.

Fact. *Let n be a positive integer which is not a perfect square. Then $\sqrt{n}$ is irrational.*

Proof. Let $b_1, \cdots b_k$ be all the (distinct) prime numbers which divide n. By Property 1 there exist positive integers $m_1, \cdots, m_k$ such that $n = b_1^{m_1} b_2^{m_2} \cdots b_k^{m_k}$. The numbers $m_1, \cdots, m_k$ split into two groups, the even ones and the odd ones. By relabelling the prime divisors of n (if necessary) we may assume that the odd ones are $m_1, \cdots, m_r$ and the even ones are $m_{r+1}, \cdots, m_k$ for some integer r between 1 and k. Note that r must be

at least one by the assumption that n is not a perfect square. Write $m_j = 2t_j + 1$, for $1 \leq j \leq r$, and $m_j = 2s_j$, for $r+1 \leq j \leq k$, where the s_j are positive integers and the t_j are non-negative integers. Then

$$n = (b_1 \cdots b_r).(b_1^{t_1} \cdots b_r^{t_r} b_{r+1}^{s_{r+1}} \cdots b_k^{s_k})^2$$

and hence, $\sqrt{n}$ is the product of $\sqrt{(b_1 \cdots b_r)}$ and the integer

$$\beta = b_1^{t_1} \cdots b_r^{t_r} b_{r+1}^{s_{r+1}} \cdots b_k^{s_k}.$$

Suppose that $\sqrt{n}$ is a rational number. Then also $\sqrt{n}/\beta$ (which equals $\sqrt{(b_1 \cdots b_r)}$) is a rational number. Accordingly, there exist positive integers p and q, with no common divisor, such that $\sqrt{(b_1 \cdots b_r)} = p/q$. That is,

$$p^2 = q^2(b_1 \cdots b_r). \tag{3}$$

Since b_1 divides p^2 (as it divides the right-hand-side of (3)) and b_1 is a prime number it follows that b_1 divides p, that is, $p = kb_1$ for some positive integer k. Substitute this into (3) gives $k^2 b_1^2 = q^2(b_1 \cdots b_r)$ or, equivalently

$$q^2(b_2 \cdots b_r) = k^2 b_1. \tag{4}$$

If $r = 1$, then (4) actually becomes $q^2 = k^2 b_1$ and so b_1 divides q^2 (as it divides $k^2 b_1$). If $r \geq 2$, then b_1 divides $q^2(b_2 \cdots b_r)$, as it divides the right-hand-side of (4), and hence b_1 divides q^2 or $b_2 \cdots b_r$. But, since $b_2, \cdots, b_r$ are all prime numbers distinct from b_1 it follows from Property 2 that b_1 cannot divide the product $b_2 \cdots b_r$. Accordingly, b_1 must divide q^2. Hence, in either case (that is, $r = 1$ or $r \geq 2$) we can conclude that b_1 divides $q^2 = qq$. But, b_1 is prime and thus it must divide q itself. So, b_1 has been shown to divide both p and q which is contrary to the fact that p and q have no common divisors. This contradiction stems from the assumption that $\sqrt{n}$ is rational. Accordingly, $\sqrt{n}$ must be irrational.□

We have seen that a rather simple proof of an elementary fact (in our case, the proof of the irrationality of $\sqrt{2}$), if properly analyzed, can be exploited to establish somewhat

more than originally anticipated. This is a useful lesson for all students of mathematics (even university professors).

Let us now turn our attention to a number of a rather different kind, namely the one usually denoted by the letter e. This number has several equivalent expressions. For example, given the function $f(x) = 1/x$, for $x > 0$, and a number $u \geq 1$, let $F(u)$ denote the area determined by the graph of f and the X-axis between $x = 1$ and $x = u$. Then e is that (unique) number u such that $F(u) = 1$. The difficulty here is that we need to know what is meant by "area". The number e can also be specified as the limit of the numbers $(1 + 1/n)^n, n = 1, 2, \cdots$, as n tends to infinity; this time the catch is in the phase "limit as n tends to infinity". Both of these (equivalent) definitions of e involve concepts which are not yet available to us in a precise form. We prefer to use still another definition of e (equivalent, of course, to the two suggested above) which is based on one of the defining properties (called Dedekind's principle) of the real numbers.

Recall that a sequence of real numbers $x_n, n = 1, 2, \cdots$, is said to be

(i) increasing if $x_n \leq x_{n+1}$, for every $n = 1, 2, \cdots$, and

(ii) bounded from above if there exists a number M such that $x_n \leq M$, for every $n = 1, 2 \cdots$

One of the fundamental properties of the real numbers states that if $x_n, n = 1, 2, \cdots$, is an increasing sequence (of numbers) bounded from above, then there exists a unique real number x satisfying

(I) $x_n \leq x$, for every $n = 1, 2, \cdots$, and

(II) if u is another real number satisfying $x_n \leq u$, for every $n = 1, 2, \cdots$, then $x \leq u$.

Let us proceed to define the number e. For each integer $n \geq 0$, let

$$e_n = 1/0! + 1/1! + 1/2! + \cdots + 1/n! = \sum_{j=0}^{n} 1/j!,$$

where we recall the notation $n! = 1.2 \cdots (n-1).n$, for $n \geq 1$, and $0! = 1$. It is clear that the so defined sequence $e_n, n = 0, 1, \cdots$, is increasing. Noting that

$$m! = 1.2.3 \cdots (m-1).m \geq 1.2.2. \cdots 2.2,$$

where 2 occurs $(m-1)$-times, it follows that $1/m! \leq 1/2^{m-1}$, for every integer $m \geq 1$.

Accordingly,

$$e_n \leq 1 + 1 + 1/2 + \cdots + 1/2^{n-1}, \qquad n \geq 1. \tag{5}$$

Now, for any real number $0 < r < 1$ and positive integer m the formula

$$1 + r + r^2 + \cdots + r^{m-1} = (1 - r^m)/(1 - r), \tag{6}$$

can be verified by multiplying both sides by $(1 - r)$ and then expanding the resulting left-hand-side. Substituting $r = 1/2$ (in which case $1/(1 - r) = 2$) and $m = n$ into (6) shows that the right-hand-side of (5) equals $1 + 2(1 - 1/2^n) = 3 - (1/2^{n-1})$. Accordingly, it follows from (5) that

$$e_n \leq 3 - (1/2^{n-1}) \leq 3, \qquad n = 0, 1, 2, \cdots$$

That is, the increasing sequence $e_n, n = 0, 1, 2, \cdots$, is bounded above by the constant 3. Hence, there exists a unique real number, which we denote by e, satisfying

(I') $e_n \leq e$, for every $n = 0, 1, 2, \ldots$, and

(II') if u is another real number satisfying $e_n \leq u$, for every $n = 0, 1, 2, \cdots$, then $e \leq u$.

It was just shown that $u = 3$ satisfies (I') and so (II') implies that $e \leq 3$.

Fact. *The number e is irrational.*

Proof. Suppose that e is rational, equal to p/q say, for some positive integers p and q. For $n > q$ it follows from the definition of e_n that

$$q!e_n = q!(\sum_{j=0}^{q} 1/j!) + q!(\sum_{j=q+1}^{n} 1/j!)$$

or, equivalently, that

$$q!(e_n - \sum_{j=0}^{q} 1/j!) = q!(\sum_{j=q+1}^{n} 1/j!). \tag{7}$$

Now, for any integer $j > q$ it is clear that

$$q!/j! = 1/(q + 1)(q + 2) \cdots j < 1/2^{j-q},$$

from which it follows that

$$q!\Big(\sum_{j=q+1}^{n} 1/j!\Big) < \sum_{j=1+1}^{n} 1/2^{j-q} = 1/2 + 1/2^2 + \cdots + 1/2^{n-q}. \tag{8}$$

But, the right-hand-side of (8) equals $1 - (1/2^{n-q})$; this follows from (6) with $r = 1/2$ and $m = n - q$. Combining this with (7) it follows that

$$q!(e_n - \sum_{j=0}^{q} 1/j!) < 1/2^{n-q}, \qquad n > q. \tag{9}$$

For $n > q$, let w_n denote the left-hand-side of (9). Then w_n, $n = q+1,\ q+2, \cdots$, is an increasing sequence since

$$w_{n+1} - w_n = q!(e_{n+1} - e_n) > 0.$$

Furthermore, none of the numbers w_n, $n > q$, exceeds the constant $q!e$ (just note that $w_n < q!e_n \leq q!e$). Accordingly, there is a unique positive number w satisfying

(I") $w_n \leq w$, for all $n > q$, and

(II") if v is a real number such that $w_n \leq v$, for all $n > q$, then $w \leq v$.

The claim is that w is precisely the number $w^* = q!(e - \sum_{j=0}^{q} 1/j!)$. Indeed, since $e_n \leq e$, for every $n \geq 1$, it is clear that

$$w_n = q!(e_n - \sum_{j=0}^{q} 1/j!) \leq w^*, \qquad n > q.$$

Furthermore, suppose that v is a real number such that $w_n \leq v$, for all $n > q$. It follows from the definition of w_n that

$$e_n \leq q!v + \sum_{j=0}^{q} 1/j!, \qquad n > q. \tag{10}$$

Since $e_k \leq e_n$ for $0 \leq k \leq n$ it follows that (10) actually holds for all $n \geq 0$ (not just $n > q$). Accordingly, property (II') of e implies that $e \leq q!v + \sum_{j=0}^{q} 1/j!$ which, upon rearranging, gives

$$v \leq q!(e - \sum_{j=0}^{q} 1/j!) = w^*.$$

This shows that w^* has the same properties that w has in (I") and (II") and so, by uniqueness of w, it can be concluded that $w^* = w$, that is,

$$w = q!(e - \sum_{j=0}^{q} 1/j!). \tag{11}$$

From $e = p/q$ and (11) it is clear that w is an integer. However, from (9) and the definition of w_n it follows that

$$w_n < 1/2^{n-q} \leq 1/2, \qquad n > q,$$

and so (II") implies (with $v = 1/2$) that $w \leq 1/2$. Since w is clearly a positive integer (after checking $w \neq 0$) this is a contradiction as there are no integers strictly between 0 and 1. Accordingly, e cannot be rational.□

Another number often encountered during our mathematical education is π. It turns out that π is also irrational. For an elegant and not too difficult a proof of this fact (you will need to know some calculus!) we refer the interested reader to page 181 of the reference [2].

References

1. U. Dudley, **Elementary number theory**, W.H. Freeman and Co., San Francisco, 1969.
2. I. Niven and H.S. Zuckerman, **An introduction to the theory of numbers** (4th Edition), J. Wiley and Sons, New York, 1980.