$\mathcal{F}_p$ is

$$(p^2)(1)(p) + (p^2)(p-1)\left(\frac{p+1}{2}\right) = \frac{p^2}{2}\left(p^2 + 2p - 1\right),$$

as desired.

Acknowledgment. This paper was written while the author was supported by NSF grant DMS-0344082.

REFERENCES

1. G. Olšavský, The number of 2 by 2 matrices over $\mathbb{Z}/p\mathbb{Z}$ with eigenvalues in the same field, this MAGAZINE, **76** (2003), 314–317.

Irrationality of Square Roots

PETER UNGAR
71 Standish Dr
Scarsdale, NY 10583-6728
peterungar@yahoo.com

We present a very simple proof of the irrationality of noninteger square roots of integers. The proof generalizes easily to cover solutions of higher degree monic polynomial equations with integer coefficients. It is based on the following criterion.

> A real number α is irrational if there are arbitrarily small positive numbers of the form
>
> $$m + n\alpha; \text{ where } m \text{ and } n \text{ are integers.} \tag{1}$$

Indeed, if α were a fraction with denominator q, then $m + n\alpha$ would also be fraction with denominator q. Such a fraction is either zero or at least $1/q$ in magnitude.

Let us first note some previous proofs of irrationality based on this criterion. Arbitrarily small numbers $m + n\alpha$ have been constructed using Euclid's Algorithm, starting with α and 1. To prove that one gets arbitrarily small nonzero numbers, one must show that the sequence of numbers produced by Euclid's algorithm does not terminate. For certain numbers α, this can be done by finding a pair of consecutive numbers whose ratio is the same as the ratio of a previous pair of consecutive numbers. The sequence of ratios of consecutive numbers is periodic from then on.

Kalman, Mena, and Shariari [**1**] give a geometric proof that this sequence is periodic for $\alpha = \sqrt{2}$. Geometric proofs must be tailored to each specific number and they are bound to get very complicated. For instance, one can show by computation that for $\alpha = \sqrt{43}$, the ratios repeat only after 10 steps; a geometric proof would therefore have to contain dozens of points and line segments.

Using algebra, Joseph Louis Lagrange proved that Euclid's algorithm is periodic for all square roots. This result can be found in books discussing continued fractions. For other kinds of irrationals such as cube roots Euclid's algorithm is not periodic and the author does not know of a direct way of showing it will not terminate.

Kalman, Mena, and Shariari [1] get around these difficulties by ingenious use of matrix algebra instead of Euclid's algorithm. In the present note we obtain the arbitrarily small numbers using only algebra of the simplest kind.

The simple proof Let $\lfloor x \rfloor$ denote the greatest integer $\leq x$. If $\sqrt{d}$ is not an integer then $\sqrt{d} - \lfloor \sqrt{d} \rfloor$ is positive and < 1. Hence the positive expression $(\sqrt{d} - \lfloor \sqrt{d} \rfloor)^k$ can be made smaller than any given positive number by taking a large enough exponent. Expanding the product creates an expression of the form (1). We can conclude that $\sqrt{d}$ is not a fraction.

Next we prove the irrationality of a noninteger real root α of an nth degree equation with integer coefficients and leading coefficient 1,

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0. \tag{2}$$

(Note that if the coefficient of α^n is a nonzero integer c instead of 1 then $c\alpha$ satisfies an equation of the form (2). Real or complex numbers that satisfy such an equation are called *algebraic integers*. They were originally studied in the effort to prove Fermat's Theorem.)

If α were rational, $\alpha = p/q$, then a positive sum of the form

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}, \tag{3}$$

where $c_0, \ldots, c_{n-1}$ are integers, would have to be $\geq 1/q^{n-1}$. We can construct arbitrarily small positive expressions of the form (3) by expanding $(\alpha - \lfloor \alpha \rfloor)^k$ in powers of α and eliminating terms with exponents $\geq n$ by repeated use of

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$

We conclude that α is irrational.

Acknowledgment. The author wishes to thank a referee of a previous version of this paper for calling his attention to [1]. Any reader who has seen or thought of this proof before is urged to inform the author.

REFERENCES

1. Dan Kalman, Robert Mena, and Shariat Shariari, Variations on an irrational theme—geometry, dynamics, algebra, this MAGAZINE, **70**:2 (April, 1997),93–104. (Also available at http://www.american.edu/academic.depts/cas/mathstat/People/kalman/pdffiles/irrat.pdf

Is Teaching Probability Counterproductive?

There could also be a danger to teaching too much math. In many states, the proceeds from the lottery go to education. If you teach people about probability, they'll be much less likely to play the lottery. So paradoxically, the better you teach math, the less funding you may have to teach it.

Alan Chodos, Associate Executive Officer, American Physical Society