Conclusion In this paper we have proved two theorems that offer extensive characterizations for the number theoretical properties of the numbers of the form $a^n \pm b^n$. The theorems were illustrated to provide very effective tools for solving challenging Olympiad problems involving such numbers.

Acknowledgment. We thank Răzvan Gelca for suggestions on improving the style of the paper.

REFERENCES

1. Titu Andreescu and Kiran Kedlaya, M*athematical Contests 1995-1996: Olympiad Problems and Solutions*, MAA, 1997.
2. Mircea Becheanu, *Probleme din Olimpiade Matematice (Mathematics Olympiad Problems)*, GIL, 1995.
3. Andrei Jorza, Math Archive, Balkan Mathematical Olympiad, 1993, http://ajorza.tripod.com/mathfiles/balkan/balkan10.pdf.
4. Andrei Jorza, Math Archive, IMO Romanian Selection Tests, 2002, http://ajorza.tripod.com/mathfiles/selection2002.pdf.
5. Andrei Jorza, Math Archive, IMO Shortlist, 1991, http://ajorza.tripod.com/mathfiles/imo1991.pdf.
6. Andrei Jorza, Math Archive, IMO Shortlist, 1997, http://ajorza.tripod.com/mathfiles/imo1997.pdf.
7. Mihai Manea, Regandind o Problema de la OIM 2000 (Rethinking a problem proposed for IMO 2000), *Revista Matematica din Timisoara*, No. 2/2001.
8. Laurentiu Panaitopol, IMO Training Problems, *Gazeta Matematic*a, No. 1/2000.

Two by Two Matrices with Both Eigenvalues in $\mathbb{Z}/p\mathbb{Z}$

MICHAEL P. KNAPP
Loyola College
Baltimore, MD 21210-2699
mpknapp@loyola.edu

Suppose that p is a prime number. In a recent article in the MAGAZINE [**1**], Gregor Olšavský counted the number of 2×2 matrices with entries in the field $\mathbb{Z}/p\mathbb{Z}$ that have the additional property that both eigenvalues are also in $\mathbb{Z}/p\mathbb{Z}$. In particular, he showed that there are

$$\frac{p^2}{2}(p^2 + 2p - 1)$$

such matrices.

When I began reading Olšavský's article, I thought that this would be an interesting theorem to present to my number theory class. Unfortunately for me, the key ingredient in his proof is a theorem from algebra relating the number of elements in a given conjugacy class of a group to the cardinality of the centralizer of an element in that conjugacy class. Since many of my students had not yet taken algebra and would not know about such concepts, I began to look for a proof that could be taught in an undergraduate number theory class. The purpose of this note is to provide such a proof.

Our strategy is to use the quadratic formula to find the roots of the characteristic polynomial of a matrix and then count the number of matrices for which these roots are in $\mathbb{Z}/p\mathbb{Z}$. We will follow Olšavský's notation and abbreviate $\mathbb{Z}/p\mathbb{Z}$ by $\mathcal{F}_p$. More-

over, all of the variables and congruences mentioned in the proof should be interpreted modulo p.

If $p = 2$, then we cannot divide by 2 and so cannot use the quadratic formula to find roots of polynomials. However, we can verify by a direct calculation that of the 16 possible 2×2 matrices with entries in $\mathcal{F}_2$, the only two whose eigenvalues are *not* both in $\mathcal{F}_2$ are

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

So there are fourteen 2×2 matrices with entries in $\mathcal{F}_2$ and both eigenvalues in $\mathcal{F}_2$, as desired.

If $p > 2$, then suppose that A is the matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Calculating the characteristic polynomial of A gives us

$$\text{Char}(A) = \lambda^2 - (a + d)\lambda + (ad - bc).$$

We want to count the number of choices of a, b, c, and d such that both roots of this polynomial are in $\mathcal{F}_p$. Since $p \neq 2$, we can use the quadratic formula to find that the roots of $\text{Char}(A)$ are

$$\begin{aligned} \lambda &\equiv \frac{a + d \pm \sqrt{(-(a + d))^2 - 4(ad - bc)}}{2} \\ &\equiv \frac{a + d \pm \sqrt{(a - d)^2 + 4bc}}{2}, \end{aligned}$$

where we interpret dividing by 2 to mean multiplying by the inverse and square roots are interpreted modulo p. Clearly, $\text{Char}(A)$ has both roots in $\mathcal{F}_p$ if and only if the quantity $(a - d)^2 + 4bc$ is a perfect square in $\mathcal{F}_p$. We will count the number of choices of a, b, c, and d such that this is true.

Let a and d be any fixed elements of $\mathcal{F}_p$. There are p^2 choices for their values. If $b \equiv 0$, then for each of the p possible choices of c, we know that

$$(a - d)^2 + 4bc \equiv (a - d)^2$$

is a perfect square in $\mathcal{F}_p$. So we have $(p^2)(1)(p)$ matrices with entries in $\mathcal{F}_p$, both eigenvalues in $\mathcal{F}_p$ and $b \equiv 0$.

If b is one of the $p - 1$ possible nonzero values, then we use the fact that, including 0, there are precisely $(p + 1)/2$ perfect squares in $\mathcal{F}_p$ (these being

$$0^2, 1^2 \equiv (p - 1)^2, \ldots, \left(\frac{p - 1}{2}\right)^2 \equiv \left(\frac{p + 1}{2}\right)^2).$$

Hence there are $(p + 1)/2$ values that can be added to $(a - d)^2$ to obtain a perfect square modulo p, and each one of these is a unique multiple of $4b$. Thus for each of the $p - 1$ nonzero values of b, we see that there are $(p + 1)/2$ values of c such that $(a - d)^2 + 4bc$ is a perfect square in $\mathcal{F}_p$. So the total number of matrices with entries in $\mathcal{F}_p$, both eigenvalues in $\mathcal{F}_p$, and $b \not\equiv 0$ is $(p^2)(p - 1)(p + 1)/2$. Therefore the total number of matrices (with any value of b) having entries in $\mathcal{F}_p$ and both eigenvalues in

$\mathcal{F}_p$ 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.