2×2 Matrices with both eigenvalues in $\mathbb{Z}/p\mathbb{Z}$

Michael P. Knapp
Mathematical Sciences Department
Loyola College
4501 North Charles Street
Baltimore, MD 21210-2699
mpknapp@loyola.edu

Suppose that p is a prime number. In a recent article [1] in this MAGAZINE, Gregor Olšavský counted the number of 2×2 matrices with entries in the field $\mathbb{Z}/p\mathbb{Z}$ which 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 which 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 $\mathcal{F}_p$. Moreover, 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

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

where we interpret dividing by 2 to mean multiplying by the inverse and square roots are interpreted modulo p. Clearly, $\mathrm{Char}(A)$ has both roots in $\mathcal{F}_p$ if and only if $(a-d)^2+4bc$ 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

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

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.

References

[1] G. Olšavský, The Number of 2 by 2 Matrices over $\mathbb{Z}/p\mathbb{Z}$ with Eigenvalues in the Same Field, *Math Magazine*, **76** (2003), 314–317.