SPECTRAL DECOMPOSITION OF MATRICES FOR HIGH SCHOOL STUDENTS

ALBERT WILANSKY, Lehigh University

This topic has developed over a period of seven years in a summer "Junior Research" program sponsored by the National Science Foundation. The participants were high school students, mostly about to be seniors, who were selected on the basis of their mathematical talent. The author was assisted at various times by I. D. Berg, A. K. Snyder, G. A. Stengle, and T. M. Morrisette. (There are obvious reasons for not mentioning the names of the students, even those who made quite good contributions.) The development of the subject may be judged by the early report [10].

Even in the context of mathematics available at this level, several problems have arisen naturally that seem intractable by any standards, and many meaningful research projects were carried out by the students. Some of these will be described below.

Mathematicians will recognize special cases of the spectral theorem (here not restricted to normal matrices) and some properties of field extensions. The final results obtained may be extracted by suitable specialization from those of [3], [6], [7], [8], and [9]; however, the techniques of these articles are quite different from the ones developed here all of which have been successfully presented to (and partially developed by) high school students.

1. Residue rings. We denote by J_n the familiar residue ring mod n. For example, $J_6=\{0, 1, 2, 3, 4, 5\}$. We write $2+3=5$, $4+5=3$ (rather than $4+5\equiv 3 \pmod 6$), $4\times 5=2$ and so on. In J_6 we write $8=2$, $14=2$; for example $3+4=7=1$.

Each J_n is a commutative ring with identity. If $a\cdot b=1$ we say that a and b are *reciprocals*; the Euclidean algorithm shows that a member x of J_n has a reciprocal in J_n if and only if x and n have no common factor larger than 1 in the ordinary arithmetic of the positive integers. In particular, if p is prime, J_p is a field (a commutative ring with identity in which every nonzero member has a reciprocal). We shall make use of Fermat's Theorem to the effect that to each nonzero $a\in J_p$ corresponds a smallest $k>0$ such that $a^k=1$, and $k \mid (p-1)$. (See [2], pp 125, 131.) Any solution of the equation $x^2=x$ is called an *idempotent.*

2. Matrices. We shall be concerned mostly with 2 by 2 matrices with entries in some residue ring J_n. These will be referred to as matrices over J_n, and the collection of all of them will be written $M(J_n)$. As usual

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}+\begin{bmatrix} e & f \\ g & h \end{bmatrix}=\begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix},\ \begin{bmatrix} a & b \\ c & d \end{bmatrix}\cdot\begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

$$=\begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix},\ k\cdot\begin{bmatrix} a & b \\ c & d \end{bmatrix}=\begin{bmatrix} ka & kb \\ kc & kd \end{bmatrix}$$

The search for idempotent matrices motivates an attempt to simplify the square of a matrix. Setting

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}; \Delta = ad - bc \text{ (the } \textit{determinant}\text{)}; t = a + d \text{ (the } \textit{trace}\text{)};$$

we have

$$A^2 = \begin{bmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{bmatrix} = \begin{bmatrix} a^2 + ad - \Delta & bt \\ ct & d^2 + ad - \Delta \end{bmatrix}$$

$$= \begin{bmatrix} at & bt \\ ct & dt \end{bmatrix} - \begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} = tA - \Delta I.$$

The equation $A^2 - tA + \Delta I = 0$ is called the *characteristic equation* of A. An obvious sufficient condition that A be idempotent is $t = 1$ and $\Delta = 0$. This condition is not necessary.

$$\left(\text{Witness } \begin{bmatrix} 3 & 0 \\ 0 & 0 \end{bmatrix} \text{ over } J_6, \text{ not to mention the zero and identity matrices.} \right)$$

THEOREM 1. *Let $A \in M(J_p)$, p prime, $A \neq 0$, $A \neq I$. Then A is idempotent if and only if $t = 1$, $\Delta = 0$.*

We have $A^2 - tA + \Delta I = 0$, so that the condition is obviously sufficient. Conversely, suppose that A is idempotent and that $t \neq 1$. The characteristic equation says $A - tA + \Delta I = 0$; since J is a field this yields $A = [-\Delta/(1-t)]I$ which we abbreviate as $A = \lambda I$. Since A is idempotent, so is λI; that is, $\lambda^2 = \lambda$. Either $\lambda = 0$, or if not, multiplying by $1/\lambda$ yields $\lambda = 1$. Thus either $A = 0$ or I, both excluded. It follows that $t = 1$ after all. Setting $A^2 = A$ and $t = 1$ in the characteristic equation yields $\Delta I = 0$; hence $\Delta = 0$. (It would also be easy to check that $\Delta(A^2) = (\Delta A)^2$; hence Δ is idempotent; hence $\Delta = 0$ or else A has an inverse forcing $A = I$.)

3. Eigenvalues. Let $A \in M(J_n)$ have trace t, determinant Δ. Any solution of the equation $x^2 - tx + \Delta = 0$ is called an *eigenvalue* of A. For example, define $A \in M(J_8)$ by

$$A = \begin{bmatrix} 2 & 1 \\ 5 & 6 \end{bmatrix}.$$

Then $t = 0$, $\Delta = 7$ and the characteristic equation is $A^2 + 7I = 0$. The solutions of the equation $x^2 + 7 = 0$ in J_8 are 1, 3, 5, 7 so A has 4 eigenvalues. Considering that, in J_8, $x^2 + 7 = (x-1)(x-7) = (x-3)(x-5)$, it is reasonable to list the eigenvalues as 1, 7; 3, 5. On the other hand, let

$$B = \begin{bmatrix} 1 & 1 \\ 5 & 7 \end{bmatrix} \in M(J_8).$$

Then B has no eigenvalues, for since $t = 0$, $\Delta = 2$, we are looking for solutions of $x^2 \pm 2 = 0$; but the squares of 0, 1, 2, 3, 4, 5, 6, 7 are 0, 1, 4, 1, 0, 1, 4, 1. Thus $x^2 \neq -2$ for all $x \in J_8$. (Note: $-2 = 6$.)

THEOREM 2. *Let p be a prime and $A \in M(J_p)$. Then A has two, one, or no eigenvalues.*

The upper bound, two, follows from the fact that a quadratic equation over a field can have at most two roots. (See, for example [4], Lemma 5.2.)

THEOREM 3. *Let $A \in M(J_p)$ with p prime, and let α, β be the eigenvalues of A. Then $(A-\alpha I)(A-\beta I)=0$. This holds even if $\alpha=\beta$.*

Since α, β are solutions of $x^2-tx+\Delta=0$ we have $x^2-tx+\Delta=(x-\alpha)(x-\beta)$. Thus $\alpha+\beta=t$, $\alpha\beta=\Delta$ and so $(A-\alpha I)(A-\beta I)=A^2-(\alpha+\beta)A+\alpha\beta I=A^2-tA+\Delta I=0$.

4. Statement of the problem. (The following result may be greatly generalized; see [1].)

THEOREM 4. *Let x be a member of a finite ring. Then there exists a positive integer k such that x^k is idempotent.*

The sequence $\{x, x^2, x^3, \cdots\}$ must have repetition, say $x^r=x^s$, $r>s$. Let $d=r-s$. Choose an integer t with $td>s$ and let $u=td-s$. Then x^{s+u} is idempotent, as we see by the following computation: $x^s=x^{s+d}=x^{s+2d}=\cdots=x^{s+td}$, hence $x^{s+u}=x^{s+td+u}$; but $s+td+u=2(s+u)$.

DEFINITION. *The order of x is the least positive integer k such that x^k is idempotent.*

This generalizes the usual definition which is given for nonzero elements of a field, namely the least positive integer k such that $x^k=1$. We are assured by Theorem 4 that every element of a finite ring has an order. For example, in J_{15}, the order of 3 is 4 since $3^2=9$, $3^3=12$ are not idempotent but $3^4=6$ is since $6\times 6=6$.

COROLLARY. *Every member of $M(J_n)$ has an order.*

For there are only finitely many 2 by 2 matrices over J_n; n^4 of them to be exact.

PROBLEMS. 1. What is the order of a given matrix?

2. What orders are possible for any 2 by 2 matrix over J_n?

In the early stages of this problem, direct computation produced the maximum order 3 for $n=2$, and 8 for $n=3$. Since $M(J_5)$ has 625 matrices, this approach had to be abandoned. There were much excitement and conjecture in the class over the possibilities for the maximum order for $n=5$.

A few computations will illustrate some primitive methods of computing an order. These yield results (eventually) but very little insight. Let

$$A=\begin{bmatrix}1 & 2\\ 2 & 1\end{bmatrix}\in M(J_3);$$

then A is not idempotent ($t=2\neq 1$) but

$$A^2 = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

is idempotent ($t = 4 = 1$, $\Delta = 3 = 0$); hence the order of A is 2. Let

$$B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in M(J_3);$$

then $B, B^2, \cdots B^7$ are not idempotent, but $B^8 = I$, so the order of B is 8. (Notice that if Δ has a reciprocal in J_n and k is the order of A, then $A^k = I$ since ΔA^k is a unit and A^k is idempotent.) Some students listed all 81 two by two matrices over J_3 with their orders. These are 1, 2, 3, 4, 6, 8. Further investigation revealed the curious fact that the matrices of order 4, 8 have no eigenvalues, those of order 3, 6 have one, and those of order 1, 2 have two eigenvalues, with the exception of $0, I$. The staff was unable to "explain" this at first, but subsequent developments, described below, clarified the situation completely, yielding an exact prediction of orders in $M(J_n)$ for all n.

The technique just given may be improved. Let

$$B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in M(J_3).$$

Then $B^2 = B + I$ (the characteristic equation),

$$\begin{aligned} B^3 &= B \cdot B^2 = B(B + I) = B^2 + B = (B + I) + B \\ &= 2B + I, B^4 = B \cdot B^3 = 2B^2 + B = 2(B + I) + B \\ &= 2I, \text{ (since } 3 = 0), B^5 = 2B, B^6 = B^4 \cdot B^2 \\ &= 2I(B + I) = 2B + 2I, B^7 = B^4 \cdot B^3 = 2B^3 \\ &= B + 2I, B^8 = (B^4)^2 = I \end{aligned}$$

Now the traces of B^2, B^5, B^6, B^7 are 0, 2, 0, 2 so they are not idempotent; further $B \neq B^2$, $B^3 \neq B^6$, $B^4 \neq B^8$ so B, B^3, B^4 are not idempotent. Thus the order of B is 8.

5. Resolution of the identity. Consider the three members 6, 10, 15 of J_{30}. They are idempotents, $6 + 10 + 15 = 1$, and $6 \times 10 = 6 \times 15 = 10 \times 15 = 0$.

DEFINITION. *A set* $(a_1, a_2, \cdots, a_n)$ *is called a resolution of the identity if each* a_i *is idempotent and not* 0 *or* 1, $a_1 + a_2 + \cdots + a_n = 1$, *and* $a_i a_j = 0$ *if* $i \neq j$.

An example of a matrix resolution of the identity is

$$A = \begin{bmatrix} 2 & 4 \\ 4 & 2 \end{bmatrix}, B = \begin{bmatrix} 3 & 0 \\ 0 & 0 \end{bmatrix}, C = \begin{bmatrix} 2 & 2 \\ 2 & 5 \end{bmatrix} \text{ over } J_6.$$

(Here $A + B + C = I$.)

THEOREM 5. *In* $M(J_p)$, p *prime, a resolution of the identity has exactly two members.*

This is immediate from Theorem 1 and the fact that the trace of I is 2.

6. Spectral decomposition. There is a certain class of matrices for which computation is very easy, with the result that the orders are easy to obtain. Suppose that (E, F) is a matrix resolution of the identity; that is $E^2=E$, $F^2=F$, $EF=FE=0$, $E+F=I$, and let α, β be members of the ring of entries of E, F. (For example, if E, F are matrices over J_5, then $\alpha, \beta \in J_5$.) Now set

$$A = \alpha E + \beta F. \tag{1}$$

Then $A^2=\alpha^2E^2+\alpha\beta EF+\beta\alpha FE+\beta^2F^2=\alpha^2E+\beta^2F$. Similarly $A^3=\alpha^3E+\beta^3F$ and, by easy induction,

$$A^n = \alpha^n E + \beta^n F, \qquad n = 1, 2, 3, \cdots. \tag{2}$$

Although irrelevant for order questions, it is interesting to ask if equation (2) holds for other n. For example, let us try it for $n=1/2$. If α, β have square roots, say $\alpha^{1/2}$, $\beta^{1/2}$, set $B=\alpha^{1/2}E+\beta^{1/2}F$ and we soon see that $B^2=(\alpha^{1/2})^2E+(\beta^{1/2})^2F=A$, and so indeed B is a square root of A. For $n=0$, equation (2) reads (with reasonable interpretation) $I=E+F$, and this also is true. Similarly equation (2) holds for negative n if we take A^{-1} as the inverse of A.

If a matrix A has a representation in the form (1), with $\alpha \neq \beta$, and with E, F a resolution of the identity, we say that A has a *spectral decomposition.* (If we allowed $\alpha=\beta$ we would have $A=\alpha(E+F)=\alpha I$, a trivial case.)

THEOREM 6. *Let $A \in M(J_p)$, p prime, and suppose that A has a spectral decomposition (1). Then α, β are the eigenvalues of A, and α, β, E, F are uniquely determined by A.*

From (1) it follows that $EA=AE=\alpha E$ since $EF=0$. Also $EA^2=(EA)A=\alpha EA=\alpha^2E$. Thus if we multiply the characteristic equation $A^2-tA+\Delta I=0$ by E we obtain $\alpha^2E-t\alpha E+\Delta E=0$. Since $E\neq 0$ this yields $\alpha^2-t\alpha+\Delta=0$, and so α is an eigenvalue. (This argument works even if $\alpha=\beta$.) Similarly β is an eigenvalue. This shows that α, β are uniquely determined (using Theorem 2). To see that E and, similarly, F, are uniquely determined by (1), replace F by $I-E$ obtaining $A=(\alpha-\beta)E+\beta I$. Thus

$$E = \frac{A - \beta I}{\alpha - \beta} \tag{3}$$

$$F = \frac{\alpha I - A}{\alpha - \beta} \tag{4}$$

7. Solution of the problem for spectrally decomposed matrices over J_p. Let p be a prime and suppose that $A \in M(J_p)$ has a spectral decomposition as in equation (1) with $\alpha \neq \beta$. If $\alpha=0$, then $\beta\neq 0$; let k be the order of β. Fermat's Theorem shows that $k \mid (p-1)$. We have $A^r=\beta^rF$ for all r; thus $A^k=F$ and the order of A is k. Any divisor of $p-1$ can be obtained in this way as an order for $A \in M(J_p)$. Next suppose $\alpha\neq 0$ and $\beta\neq 0$. Let u and v be the orders of α and β respectively. Then the order of A is m, the least common multiple of α and β for we have $A^m=\alpha^mE+\beta^mF=E+F=I$ is idempotent, while if A^r is idempotent,

we have $A^r = A^{2r}$; thus by Theorem 6, $\alpha^r = \alpha^{2r}$, $\beta^r = \beta^{2r}$ and so r is a multiple of both u and v. Once again we find that the order of A is a factor of $p-1$.

8. Solution of the problem for matrices with two eigenvalues over J_p, p prime. This is accomplished by the pleasant device of showing that every such matrix has a spectral decomposition. Let α, β be its eigenvalues and define E, F by formulas (3), (4). Then $EF = 0$ by Theorem 3; $E+F = I$ is a trivial computation, $E^2 = E(I-F) = E-EF = E$, and, similarly, $F^2 = F$. Thus (E, F) is a resolution of the identity. Finally, it is easy to compute that $\alpha E + \beta F = A$. This shows that A has a spectral decomposition and reduces the problem to that solved in Section 7.

9. Solution of the problem for matrices with repeated eigenvalues over J_p, p prime. We invent a type of spectral decomposition. Let α be the only eigenvalue of $A \in M(J_p)$. By Theorem 3, $(A-\alpha I)^2 = 0$ so if we set $N = A - \alpha I$ we shall have

$$A = \alpha I + N, \quad \text{with} \quad N^2 = 0. \tag{5}$$

The point of this decomposition is that we obtain $A^2 = \alpha^2 I + 2\alpha N$, since $N^2 = 0$; $A^3 = \alpha^3 I + 3\alpha^2 N$, and, in general,

$$A^r = \alpha^r I + r\alpha^{r-1} N. \tag{6}$$

THEOREM 7. *Let $A \in M(J_p)$, p prime and suppose that $A = \alpha I + N$ with $N^2 = 0$, $\alpha \neq 0$. Then A is idempotent if and only if $\alpha = 1$ and $N = 0$.*

If $A = A^2$, then $\alpha I + N = \alpha^2 I + 2\alpha N$; hence $(\alpha - \alpha^2) I = (2\alpha - 1) N$. Squaring both sides yields $(\alpha - \alpha^2)^2 = 0$; hence $\alpha = \alpha^2$ and so $\alpha = 1$. The same equation then yields $N = 0$.

Now if A has the form (5) with $\alpha \neq 0$, suppose that the order of α is k, and that of A is m. Applying Theorem 7 to (6) yields $\alpha^m = 1$, $m\alpha^{m-1} = 0$. The first equation says m is a multiple of k; the second becomes $m = 0$ after multiplying by α and thus m is a multiple of p. Conversely, if m is a multiple of k and p, (6) yields $A^m = I$; thus m is the least common multiple of p and k. Since k may be any divisor of $p-1$ we have all kp with $k \mid (p-1)$ as the orders of matrices with only one eigenvalue (repeated eigenvalues, an eigenvalue of multiplicity 2).

For $M(J_3)$, $k = 1$ or 2, and so 3, 6 are the orders of matrices with one eigenvalue.

10. Quadratic extensions. The case of a matrix with no eigenvalues requires some completely new techniques. We were lucky enough to recognize this in an unrelated area which had been studied for its own merits for a few summers. Let p be a prime and let g be a quadratic polynomial with leading coefficient 1 and with no root in J_p. For example, $g(v) = v^2 - 2$ has no root in J_3. Let $J_{p,g}$ be the set of all first degree polynomials in an indeterminate v, coefficients in J_p; thus the members of $J_{p,g}$ are expressions $a+bv$ with a, $b \in J_p$. Addition is defined by $(a+bv)+(c+dv) = a+c+(b+d)v$, and multiplication by ordinary multiplication over J_p but with $g(v)$ taken to be 0. For example, let $g(v) = v^2 - 2$ and operate in $J_{3,g}$. Then $(2+v)(1+2v) = 2+5v+2v^2 = 2+2v+2v^2$ (since $5 = 2$ in J_3) $= 2+2v+2(v^2-2)+4 = 2v$ since $v^2 - 2 = 0$, and $2+4 = 0$. (Algebraists will recognize this

as a simple extension of the field J_p by a root of g. See [2], p. 367.) In this computation we came upon $2+2v+2v^2$; a more systematic procedure for seeing that this is $2v$ is to divide it by v^2-2 using ordinary long division (in J_p) and keep only the remainder, $2v$. This is analogous to obtaining $7=2$ in J_5, either by writing $7=5+2=0+2=2$ or by dividing 7 by 5 and keeping only the remainder 2. (This procedure can be applied to any ring. Taking $g(v)=v^2+1$ and defining R_g as the set of all $a+bv$, a, b real, we see that R_g is the complex numbers. For example $v^2=-1$ since $v^2=v^2+1-1=0-1=-1$.) Notice that $J_p \subset J_{p,g}$ since $a=a+0\cdot v$.

LEMMA 8. *$J_{p,g}$ is a field.*

The only nontrivial part of this result is that $a+bv$ has a reciprocal if $a+bv\neq 0$ (i.e., $a\neq 0$ or $b\neq 0$). If $b=0$, $a+bv$ has $1/a$ as its reciprocal. Now suppose $b\neq 0$. Suppose that $g(v)=v^2+sv+t$; let $z=bv+bs-a$, and let $w=(a+bv)z$. Then $w=abv+abs-a^2+b^2v^2+b^2sv-abv=b^2(v^2+sv)+abs-a^2=-b^2t+abs-a^2=-b^2(\lambda^2+s\lambda+t)$ where $\lambda=-a/b$. Thus $w=-b^2g(\lambda)\neq 0$ by our hypothesis about g. Moreover $w\in J_p$. It follows that $(a+bv)\cdot(z/w)=1$. (For more insight on this proof, see [2], corollary, p. 369.)

LEMMA 9. *Let p be a prime, $p\neq 2$, and n a nonsquare in J_p. Let $g(v)=v^2-n$. Then every member of J_p has a square root in $J_{p,g}$.*

Every square in J_p has a square root in J_p. Next let m be a nonsquare in J_p. Then $(m/n)^{(p-1)/2}=(-1)/(-1)=1$ and so m/n is a square in J_p. (See [5], p. 38, Theorem 17.4.) Say $m/n=r^2$. Then $(rv)^2=r^2v^2=r^2n=m$.

LEMMA 10. *With p, g as in Lemma 9 every quadratic equation over J_p has a solution in $J_{p,g}$.*

Let the quadratic equation be $ax^2+bx+c=0$, $a\neq 0$. This has the solution $x=(-b+(b^2-4ac)^{1/2})/2a$ and Lemma 9 assures us that b^2-4ac has a square root in $J_{p,g}$.

THEOREM 11. *With p, g as in Lemma 9, every matrix A in $M(J_p)$ has an eigenvalue in $J_{p,g}$. If A has no eigenvalue in J_p, or if A has at least one eigenvalue in $J_{p,g}$ which is not in J_p, then A has exactly 2 (distinct) eigenvalues in $J_{p,g}$.*

Consider the equation $x^2-tx+\Delta=0$. As in Lemma 10, this has solutions $x=(t+D^{1/2})/2$ where $D=t^2-4\Delta$. This is resolved into cases similar to standard discussions of quadratics. If $D=0$, A has only one eigenvalue $t/2$; if D is a nonzero square in J_p, A has 2 eigenvalues in J_p; and if D is a nonsquare, A has 2 eigenvalues in $J_{p,g}$ which are not in J_p. These eigenvalues are not equal since $D^{1/2}$ will have two values u and $-u$ where $u^2=D$, and $u=-u$ would force $D=0$.

THEOREM 12. *Let $A\in M(J_p)$ have eigenvalues α, β in $J_{p,g}$. Then A has a spectral decomposition* (1).

The proof is exactly the same as that in Section 8. Now the matrices E, F have coefficients in $J_{p,g}$.

11. Solution of the problem for all $A \in M(J_p)$, p prime, $p \neq 2$.

The only case not yet treated is that in which A has no eigenvalues in J_p. Choose a nonsquare n in J_p, (there surely exists one since the map $x \to x^2$ is 2 to 1), and let $g(v) = v^2 - n$. Then $A = \alpha E + \beta F$ as in Theorem 12. Now $J_{p,g}$ is a field with p^2 members. It follows that for each nonzero $h \in J_{p,g}$, $h^{p^2-1} = 1$. (One proof runs thus. Let $F = (0, a_1, a_2, \cdots, a_m)$ be a finite field, and $h \in F$, $h \neq 0$. The map $a_i \to ha_i$ is a permutation of F; hence $(ha_1)(ha_2) \cdots (ha_m) = a_1 a_2 \cdots a_m$. Thus $h^m = 1$.) By the usual argument, the order of h is a divisor of $p^2 - 1$. The order of A is the least common multiple of the orders of α and β and thus can be no larger than $p^2 - 1$. That it can actually be as large as $p^2 - 1$ follows from the existence in $J_{p,g}$ of an element z of order $p^2 - 1$. (This is a special case of a theorem given in [4], p. 317, Theorem 7.B.) Then any matrix with z as an eigenvalue will have order $p^2 - 1$. To construct such a matrix we write $z = a + bv$ and find that $z^2 = a^2 + 2abv + b^2v^2 = a^2 + 2a(z - a) + b^2n = c + 2az$ where $c = b^2n - a^2$. Thus $z^2 - 2az - c = 0$. Let A be a matrix with trace $2a$ and determinant $-c$. Then the characteristic equation of A is $A^2 - 2aA - cI = 0$ and so z is an eigenvalue of A.

We may also put a lower bound on the order of A; namely, it can be no less than $p + 1$. The reason for this is that if k is a divisor of $p - 1$, the equation $x^k = 1$ has k solutions in J_p and can have no more in $J_{p,g}$. Thus, since the eigenvalues of A are not in J_p, they can satisfy no such equation so their order is a divisor of $p^2 - 1$ which is more than $p - 1$.

12. Summary for $M(J_p)$, p prime. If A has two eigenvalues in J_p, the possible orders of A are the divisors of $p - 1$. If A has one eigenvalue, the possible orders are kp where k is a divisor of $p - 1$. If A has no eigenvalues, the possible orders are divisors of $p^2 - 1$ which are at least $p + 1$.

13. Solution of the problem in $M(J_n)$, n squarefree. It may be noticed that in J_{15}, each member is uniquely determined by its values in J_3, J_5. For example $12 \in J_{15}$, and in J_3, $12 = 0$; in J_5, $12 = 2$. No other member of J_{15} leads to these two values, 0 and 2 in J_3, J_5, respectively. Thus we write $15 \equiv (0, 2)$. This leads to a one-to-one correspondence between J_{15} and $J_3 \oplus J_5$, where the latter symbol stands for all pairs (x, y), $x \in J_3$, $y \in J_5$. It is soon recognized that this correspondence is actually an isomorphism, that is, that addition and multiplication correspond. As an example, $12 \in J_{15}$ corresponds to 0 in J_3, 2 in J_5; 8 in J_{15} corresponds to 2 in J_3, 3 in J_5. Write $12 = (0, 2)$; $8 = (2, 3)$. Then $12 + 8 = (0 + 2, 2 + 3) = (2, 0) = 5$ and $12 \times 8 = (0 \times 2, 2 \times 3) = (0, 1) = 6$. A general result of this form is that if m and n are relatively prime, J_{mn} is isomorphic with $J_m \oplus J_n$, under the map $k \to (\alpha, \beta)$ where α and β are the forms taken by k in J_m and J_n respectively. (α is the remainder when k is divided by m.) Now if m and n are primes, and $x \in J_{mn}$ is idempotent, $x = (\alpha, \beta)$, then α and β are idempotents in the fields J_m and J_n respectively. Thus α and β are 0 or 1. Hence J_{mn} has 4 idempotents. Let $A \in M(J_{mn})$; then

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} (\alpha_1, \alpha_2) & (\beta_1, \beta_2) \\ (\gamma_1, \gamma_2) & (\delta_1, \delta_2) \end{bmatrix}$$

which we may write in the form

$$A = B \oplus C \text{ with } B = \begin{bmatrix} \alpha_1 & \beta_1 \\ r_1 & \delta_1 \end{bmatrix} \in M(J_m),$$

and C equal to a similar expression. Clearly $A^k = B^k \oplus C^k$ and so the order of A is the least common multiple of the orders of B and C.

We omit the discussion of $M(J_n)$ where n has repeated prime factors because this theory is not yet in a satisfactory state.

14. An intractable problem. List all the matrices in $M(J_n)$ and opposite each, write its order. Let $s(n)$ be the sum of all these orders. Thus $s(n) = \sum u \cdot v$ where u is the number of matrices of order v. Then $s(2) = 26$, $s(3) = 272$, $s(5) = 4370$. What is $s(n)$ for other values of n?

15. Addendum. We have just learned that the spectral decomposition (5) may also be found in J. H. M. Wedderburn, Lectures on Matrices, Volume 17 of the American Mathematical Society Colloquium Publications. See pages 26, 27. See also J. H. Hodges, Amer. Math. Monthly, 73 (1966) 277–278.

I thank Professor G. E. Raynor for helpful discussions.

References

1. A. A. Bennett, Problem #3133, Amer. Math. Monthly, 73(1966) 89.
2. G. Birkhoff and S. MacLane, A Survey of Modern Algebra, 3rd ed., Macmillan, New York, 1965.
3. A. S. Davis, The Euler-Fermat Theorem for matrices, Duke Math. J., 18(1951) 613–617.
4. I. N. Herstein, Topics in Algebra, Blaisdell, Waltham, 1964.
5. C. C. MacDuffee, An Introduction to Abstract Algebra, Wiley, New York, 1950.
6. J. B. Marshall, On the extension of Fermat's Theorem to matrices of order n, Proc. Edinburgh Math. Soc., (2) 6 (1939) 85–91.
7. M. W. Maxfield, The order of a matrix under multiplication (mod m), Duke Math. J., 18 (1951) 619–621.
8. M. W. and J. E. Maxfield, The number of matrices belonging to a given integer, Notices of the American Math. Soc., 6 (1959) 288.
9. I. Niven, Fermat's Theorem for matrices, Duke Math. J., 15 (1948) 823–826.
10. A. Wilansky, A research program for gifted secondary school students, The Mathematics Teacher, 54 (1961) 250–254.

LINE OF FLIGHT FROM SHOCK RECORDINGS

WALTER P. REID, U. S. Naval Ordnance Laboratory, Silver Spring, Maryland

Assume that a missile is traveling with constant speed in a straight line, and that it generates a shock wave that is conical, except perhaps in the neighborhood of the nose of the missile. Some devices record the times t at which the shock reaches them. In this paper equations will be developed for the speed and