Canad. Math. Bull. Vol. **26** (4), 1983

THE EQUATION $X^k + Y^k = Z^k$ IN COMMUTING RATIONAL MATRICES

BY
DAVID E. RUSH

ABSTRACT. Solutions of $X^k + Y^k = Z^k$ in invertible pairwise commuting rational 2×2 matrices are determined for $k = 3, 4, 6, 9$, from the analogous results of A. Aigner for algebraic number fields.

Since so much profitable effort has been spent in trying to prove Fermat's assertion that the equation $X^k + Y^k = Z^k$ is not solvable in the ring of integers for $k \geq 3$, it is natural to vary the question by asking for solutions of this equation in other rings. Some of these variations are surveyed in [11, Lecture XIII]. A relationship between solutions of this equation in rational matrices and solutions of the same equation in algebraic number fields has been indicated in [5] and [11]. In this note we show that this relationship can be tightened enough to give the complete solution of the above equation in pairwise commutative invertible rational 2×2 matrices for $k = 4$, 6, 9, and some partial results for other exponents.

In what follows Q will denote the rational numbers and T an indeterminate. If P is a square matrix then $Q[P]$ denotes $\{g(P) \mid g \in Q[T]\}$. It should be noted that the solvability of $X^k + Y^k = Z^k$ in rational matrices is equivalent to the solvability of the same equation in integral matrices since one can always multiply through by a common denominator of the entries of the matrices involved.

THEOREM. *Let δ be algebraic over Q of degree n with minimal polynomial f, and let P be the companion matrix of f. If α, β, $\gamma \in Q(\delta)$ are nonzero and $\alpha^k + \beta^k = \gamma^k$, then there exist polynomials g, h, $l \in Q[T]$ such that $A = g(P)$, $B = h(P)$, and $C = l(P)$ are nonsingular and $A^k + B^k = C^k$. Conversely, if $A = g(P)$, $B = h(P)$, and $C = l(P) \in Q[P]$ are nonsingular matrices such that $A^k + B^k = C^k$, then $\alpha = g(\delta)$, $\beta = h(\delta)$, and $\gamma = l(\delta)$ are nonzero elements of $Q(\delta)$ satisfying $\alpha^k + \beta^k = \gamma^k$.*

Proof. If α, β, $\gamma \in Q(\delta) - \{0\}$ satisfy $\alpha^k + \beta^k = \gamma^k$, then $\alpha = g(\delta)$, $\beta = h(\delta)$, $\gamma = l(\delta)$ for some g, h, $l \in Q[T]$. If $\delta = \delta_1, \delta_2, \ldots, \delta_n$ are the conjugates of δ, then $\alpha_i = g(\delta_i)$, $\beta_i = h(\delta_i)$, and $\gamma_i = l(\delta_i)$ are the conjugates respectively of α, β,

Received by the editors May 25, 1982.
AMS Subject Classification (1980): Primary 10M20, 15A36 Secondary 12A25, 10J06

γ, and these are nonzero. Let D be the $n \times n$ diagonal matrix with diagonal elements $\delta_1, \delta_2, \ldots, \delta_n$. Then $A_1 = g(D)$, $B_1 = h(D)$ and $C_1 = l(D)$ are nonsingular diagonal matrices such that $A_1^k + B_1^k = C_1^k$. Let S be an $n \times n$ matrix such that $SDS^{-1} = P$ and let $A = SA_1S^{-1}$, $B = SB_1S^{-1}$, and $C = SC_1S^{-1}$. Then $A = g(P)$, $B = h(P)$, and $C = l(P)$ are nonsingular and $A^k + B^k = C^k$.

Conversely, if $A = g(P)$, $B = h(P)$, and $C = l(P) \in Q[P]$ are nonsingular matrices such that $A^k + B^k = C^k$, then let x be an eigenvector of P corresponding to the eigenvalue δ. Then $g(\delta) = \alpha$, $h(\delta) = \beta$, and $l(\delta) = \gamma$ are nonzero eigenvalues of A, B, and C respectively and since $(\alpha^k + \beta^k)x = \gamma^k x$ we have $\alpha^k + \beta^k = \gamma^k$.

REMARKS. (1) If in the above theorem the solution (α, β, γ) to $X^k + Y^k = Z^k$ corresponds to the matrix solution (A, B, C), and $\eta \in Q(\delta)$, then $\eta = r(\delta)$, $r \in Q[T]$, and the solution $(\eta\alpha, \eta\beta, \eta\gamma)$ corresponds to (NA, NB, NC) where $N = r(P)$.

(2) The above theorem can clearly be extended to other equations than $X^k + Y^k = Z^k$ (e.g. the related equation $X^k + Y^k + Z^k = 0$), as well as other fields than Q.

(3) Since the companion matrix is nonderogatory [6, p. 237], the condition in the above theorem that $A \in Q[P]$ is equivalent to the condition that $AP = PA$ [10, p. 107].

For those exponents k for which Fermat's last theorem holds we have:

COROLLARY. *If $m \in Z$ is not a square, then the equation $X^k + Y^k = Z^k$ has a nontrivial solution in $Q(\sqrt{m})$ if and only if it is solvable in pairwise commutative nonsingular 2×2 rational matrices A, B, and C at least one of which has an eigenvalue in $Q(\sqrt{m}) - Q$.*

Proof. If $\alpha, \beta, \gamma \in Q(\sqrt{m}) - \{0\}$ satisfy $\alpha^k + \beta^k = \gamma^k$, then the proof of the above theorem gives nonsingular A, B, $C \in Q[P]$ with $A^k + B^k = C^k$ where $P = \begin{bmatrix} 0 & m \\ 1 & 0 \end{bmatrix}$ is the companion matrix of $f = X^2 - m$, and α, β, γ are eigenvalues of A, B, and C respectively.

Conversely, if A, B, and C are nonsingular, pairwise commutative, rational 2×2 matrices such that $A^k + B^k = C^k$, and say A has an eigenvalue $\alpha \in Q(\sqrt{m}) - Q$. Then $Q(\alpha) = Q(\sqrt{m})$ and A is nonderogatory. Thus $B = h(A)$ and $C = l(A)$ for some h, $l \in Q[T]$ [10, p. 107]. Then as in the above theorem $g(\alpha) = \beta$ and $l(\alpha) = \gamma$ are eigenvalues of B and C respectively and $\alpha^k + \beta^k = \gamma^k$.

Examples: In our examples the emphasis will be on the 2×2 case. For if one has solutions to the equation $X^k + Y^k = Z^k$ in "small" matrices, then one can always get solutions in bigger matrices by putting copies of the given solutions down the main diagonals. Also, it is easier to find solutions to $X^k + Y^k = Z^k$ in

https://doi.org/10.4153/CMB-1983-067-1 Published online by Cambridge University Press

algebraic number fields of degree n when $n \geq k$, as in the following example:

(1) Applying the theorem to the simple example $1^k + 1^k = (\sqrt[k]{2})^k$ yields the example $I^k + I^k = P^k$ where P is the companion matrix of $f = X^k - 2$.

For the remaining examples A, B, and C will denote pairwise commutative, nonsingular, rational 2×2 matrices.

(2) If 6 or 9 divides k, then $A^k + B^k \neq C^k$ since the equations $X^6 + Y^6 = Z^6$ and $X^9 + Y^9 = Z^9$ have only trivial solutions in quadratic number fields [2].

(3) If $A^4 + B^4 = C^4$ then by the above corollary we have $\alpha^4 + \beta^4 = \gamma^4$ for some eigenvalues of A, B and C respectively, and we may assume $\alpha \notin Q$, the other cases being similar. Again by the corollary we get that $\beta, \gamma \in Q(\alpha)$ and by [1] or [11, p. 278], there exists $\eta \in Q(\alpha) = Q(\sqrt{-7})$ such that $(\eta\alpha, \eta\beta, \eta\gamma) = (\pm(1+\sqrt{-7}), \pm(1-\sqrt{-7}), \pm 2)$ (with arbitrary signs). Then, letting $\eta = g(\alpha)$, $g \in Q[T]$ and $D = g(A)$ we get

$$(DA, DB, DC) = \left(\pm\begin{bmatrix} 1 & -7 \\ 1 & 1 \end{bmatrix}, \pm\begin{bmatrix} 1 & 7 \\ -1 & 1 \end{bmatrix}, \pm\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}\right)$$

An analogous result holds for the equation $X^4 + Y^4 + Z^4 = 0$ [using 8, p. 267].

(4) The exponent 3 case is especially interesting because of the complexity of the question of solvability of the Fermat cubic in quadratic number fields. The results on this question are mostly due to A. Aigner and are summarized in [11, pp. 279–286]. For instance it holds that any non-trivial solution of the Fermat cubic in $Q(\sqrt{m})$ is equivalent to (that is a $Q(\sqrt{m})$ multiple of) one of the form $(a + b\sqrt{m})^3 + (a - b\sqrt{m})^3 = c^3$, $a, b, c \in Q$, and if one such solution exists in $Q(\sqrt{m})$ there are infinitely many non-equivalent ones. Further, although the solvability of the Fermat cubic in $Q(\sqrt{m})$ is known for many integers m, the complete set of those m for which this equation is solvable has not been determined. The above corollary yields for nonzero rationals a, b, c, that $(a + b\sqrt{m})^3 + (a - b\sqrt{m})^3 = c^3$ if and only if

$$\begin{bmatrix} a & bm \\ b & a \end{bmatrix}^3 + \begin{bmatrix} a & -bm \\ -b & a \end{bmatrix}^3 = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}^3$$

and this gives all solutions if we identify solutions which are similar or multiples by a matrix D which is rational and commutes with A, B, and C. Some specific examples are $(m, a, b, c) = (-2, 2, 1, -2), (-2, -4374, 1935, 3078), (85, 1, 1, 8)$, and many other examples can be obtained from [11, pp. 280–289] and the references given there.

(5) The primitive 3rd root of unity $\zeta = \dfrac{-1 - \sqrt{-3}}{2}$ has minimal polynomial $X^2 + X + 1$. Thus $(\zeta^2)^k + \zeta^k = (-1)^k$ whenever $(k, 6) = 1$, and so we get

$$\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}^k + \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}^k = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}^k.$$

https://doi.org/10.4153/CMB-1983-067-1 Published online by Cambridge University Press

whenever $(k, 6) = 1$. This was observed in [5], which along with [11, Lecture XIII] was the motivation for this note.

The above cases appear to be the only exponents k for which the solvability of $X^k + Y^k = Z^k$ in pairwise commutative nonsingular 2×2 rational matrices is known. Of course solutions in non-commutative matrices are more readily found. For example, it was pointed out in [9] that for k odd

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}^k + \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix}^k = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^k.$$

Although many more examples are known for these exponents [3], [11, p. 277], the solvability of $X^k + Y^k = Z^k$ in nonsingular 2×2 rational matrices does not seem to be known for any other exponent $k \geq 6$.

References

1. A. Aigner, *Über die Möglichkeit von* $X^4 + Y^4 = Z^4$ *in quadratischen Körpern*, Jahresber, d. Deutschen Math. Verein. **43** (1934), 226–229.

2. A. Aigner, *Die Unmöglichkeit von* $X^6 + y^6 = Z^6$ *and* $X^9 + y^9 = Z^9$ *in quadratischen Körpern*, Monatsh. F. Math., **61** (1957), 147–150.

3. I. A. Barnett and H. M. Weitkamp, *The equation* $X^n + Y^n + Z^n = 0$ *in rational binary matrices*, An. Str. Univ. "Al, I. Cuza", Sect. 1, (NS) **7** (1961), 1–64.

4. E. D. Bolker, *Solutions of* $A^k + B^k = C^k$ *in* $n \times n$ *integral matrices*, Amer. Math. Monthly, **75** (1968), 759–760.

5. J. L. Brenner and J. de Pillis, *Fermat's equation* $A^P + B^P = C^P$ *for matrices of integers*, Math. Mag., **45** (1972), 12–15.

6. C. G. Cullen, *Matrices and Linear Transformations*, Addison-Wesley, Reading, Mass. 1972.

7. R. Z. Domiaty, *Solutions of* $X^4 + Y^4 = Z^4$ *in* 2×2 *integral matrices*, Amer. Math. Monthly, **73** (1966), p. 631.

8. E. Fogels, *Über die Möglichkeit einiger diophantischer Gleichung* 3 *and* 4 *Grades in quadratischen Körpern*. Comm. Math. Helv. **10** (1938), 263–269.

9. P. M. Gibson, *Solutions of* $A^k + B^k = C^k$ *in nonsingular integral matrices*, Math. Mag. **43** (1970), 275–276.

10. N. Jacobson, *Lectures in Abstract Algebra*, vol II, Van Nostrand Reinhold, New York, 1953.

11. P. Ribenboim, 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, New York. Heidelberg-Berlin, 1979.

University of California
Riverside, California 92521