

FERMAT'S EQUATION OVER 2-BY-2 MATRICES

MAO-TING CHIEN AND JIE MENG

ABSTRACT. We study the solvability of the Fermat's matrix equation in some classes of 2-by-2 matrices. We prove the Fermat's matrix equation has infinitely many solutions in a set of 2-by-2 positive semidefinite integral matrices, and has no nontrivial solutions in some classes including 2-by-2 symmetric rational matrices and stochastic quadratic field matrices.

1. Introduction

Pierre de Fermat mentioned in 1637 that for any integer n greater than 2, no positive integers a, b, c satisfy the equation

$$(1) \quad a^n + b^n = c^n.$$

The Fermat's last theorem had become a conjecture since then. Andrew Wiles [15] confirmed the conjecture is true. Subsequent research has extended the problem of Fermat's last theorem over some number fields (cf. [5,9]). In contrast to the classical Fermat's last theorem in integers, there have been a number of papers on the Fermat's equation in matrices (cf. [6, 11–14]). In particular, the Fermat's equation has been investigated in 2-by-2 integer matrices [3], rational matrices [7], general linear group $GL_2(\mathbb{Z})$ [3] and special linear group $SL_2(\mathbb{Z})$ of 2-by-2 matrices with $\det = 1$ [11].

In this paper, we study the solvability of Fermat's matrix equation

$$(2) \quad A^n + B^n = C^n$$

in some classes of 2-by-2 matrices for $n \geq 4$. We prove the Fermat's matrix equation (2) has infinitely many solutions in a commuting family of 2-by-2 symmetric positive semidefinite integral matrices, and the equation (2) has no nontrivial solutions in some 2-by-2 symmetric rational matrices and m -by- m complex row stochastic matrices with row sums belonging to the quadratic field $\mathbb{Q}(\sqrt{2})$.

Received May 4, 2020; Accepted December 9, 2020.

2010 *Mathematics Subject Classification*. Primary 15A24, 11D41.

Key words and phrases. Fermat's matrix equation, commuting family of matrices, stochastic matrices.

Jie Meng was partially supported by National Research Foundation of Korea (NRF) Grant funded by the Korean Government (MSIP) (NRF-2017R1A5A1015722).

2. Fermat's matrix equation

It is no surprising the Fermat's matrix equation (2) has solutions in positive integral matrices, such as

$$\begin{pmatrix} 2 & 6 \\ 6 & 3 \end{pmatrix}^3 + \begin{pmatrix} 7 & 3 \\ 3 & 3 \end{pmatrix}^3 = \begin{pmatrix} 3 & 6 \\ 6 & 6 \end{pmatrix}^3.$$

The three matrices are symmetric, but not positive semidefinite. Observe that the mutual commutativity is invalid for the three matrices. In the following, we determine a class of commuting family of 2-by-2 matrices.

Lemma 1. *Let \mathbb{K} be a subset of complex numbers and q be a complex number. Then $H(q, \mathbb{K}) = \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in M_2(\mathbb{K}), a - c = bq \right\}$ is a commuting family.*

Proof. Suppose $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ and $\begin{pmatrix} x & y \\ y & z \end{pmatrix}$ are matrices in $H(q, \mathbb{K})$. Then $(a - c)y = b(x - z)$, which implies that the two matrices commute since

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x & y \\ y & z \end{pmatrix} = \begin{pmatrix} ax + by & ay + bz \\ bx + cy & by + cz \end{pmatrix} \text{ and} \\ \begin{pmatrix} x & y \\ y & z \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} = \begin{pmatrix} ax + by & bx + cy \\ ay + bz & by + cz \end{pmatrix}. \quad \square$$

Denote $H^+(q, \mathbb{K})$ the positive definite matrices in $H(q, \mathbb{K})$. We give a subclass of positive definite matrices for which the Fermat's matrix equation (2) has infinitely many solutions when $n = 3$.

Theorem 2. *The Fermat's matrix equation (2) has infinitely many solutions in $H^+(\pm 1, \mathbb{N})$ for $n = 3$.*

Proof. Firstly, we find three particular matrices in $H^+(1, \mathbb{N})$ satisfying the Fermat's matrix equation (2):

$$(3) \quad \begin{pmatrix} 7 & 3 \\ 3 & 4 \end{pmatrix}^3 + \begin{pmatrix} 11 & 6 \\ 6 & 5 \end{pmatrix}^3 = \begin{pmatrix} 12 & 6 \\ 6 & 6 \end{pmatrix}^3.$$

Let $\begin{pmatrix} a & b \\ b & a-b \end{pmatrix}$ be an arbitrary matrix in $H^+(1, \mathbb{N})$, which has determinant $a^2 - ab - b^2 > 0$. Direct computations show that

$$\begin{pmatrix} a & b \\ b & a-b \end{pmatrix} \begin{pmatrix} 7 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 7a + 3b & 3a + 4b \\ 3a + 4b & 4a - b \end{pmatrix}$$

which is symmetric and has positive determinant $19(a^2 - ab - b^2)$, and thus belongs to $H^+(1, \mathbb{N})$. Since $H(1, \mathbb{N})$ is a commuting family, it follows that

$$\begin{pmatrix} a & b \\ b & a-b \end{pmatrix}^3 \begin{pmatrix} 7 & 3 \\ 3 & 4 \end{pmatrix}^3 = \left(\begin{pmatrix} a & b \\ b & a-b \end{pmatrix} \begin{pmatrix} 7 & 3 \\ 3 & 4 \end{pmatrix} \right)^3.$$

Similarly,

$$\begin{pmatrix} a & b \\ b & a-b \end{pmatrix} \begin{pmatrix} 11 & 6 \\ 6 & 5 \end{pmatrix} = \begin{pmatrix} 11a + 6b & 6a + 5b \\ 6a + 5b & 5a + b \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \\ b & a-b \end{pmatrix} \begin{pmatrix} 12 & 6 \\ 6 & 6 \end{pmatrix} = \begin{pmatrix} 12a+6b & 6a+6b \\ 6a+6b & 6a \end{pmatrix}$$

which are in $H^+(1, \mathbb{N})$. Multiplying $\begin{pmatrix} a & b \\ b & a-b \end{pmatrix}^3$ to both sides of equation (3), we obtain that

$$\begin{pmatrix} 7a+3b & 3a+4b \\ 3a+4b & 4a-b \end{pmatrix}^3 + \begin{pmatrix} 11a+6b & 6a+5b \\ 6a+5b & 5a+b \end{pmatrix}^3 = \begin{pmatrix} 12a+6b & 6a+6b \\ 6a+6b & 6a \end{pmatrix}^3.$$

Note that $H^+(-1, \mathbb{N}) = \{A = P^T B P : B \in H^+(1, \mathbb{N})\}$, where $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Suppose $A, B, C \in H^+(-1, \mathbb{N})$ satisfy the Fermat's matrix equation $A^3 + B^3 = C^3$. Then,

$$P^T A^3 P + P^T B^3 P = P^T C^3 P,$$

which yields

$$(P^T A P)^3 + (P^T B P)^3 = (P^T C P)^3.$$

Set $X = P^T A P, Y = P^T B P, Z = P^T C P$. Then $X, Y, Z \in H^+(-1, \mathbb{N})$ and $X^3 + Y^3 = Z^3$. \square

Jarvis and Meekin [9] proved that the equation $x^n + y^n = z^n$ with $x, y, z \in \mathbb{Q}(\sqrt{2})$ has no nontrivial solutions, $xyz \neq 0$, when $n \geq 4$, where $\mathbb{Q}(\sqrt{2})$ is the real quadratic field consisting of $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$. The result is helpful for studying of the Fermat's matrix equation (2) which has no nontrivial solutions in some matrix classes.

Theorem 3. *The Fermat's matrix equation $A^n + B^n = C^n$ has no nontrivial solutions in $H(q, \mathbb{Q})$ for $q = \pm 2, \pm 3, \pm 6$ and $n \geq 4$.*

Proof. Assume $q = 2$. Suppose $A, B, C \in H(2, \mathbb{Q})$ are nontrivial solutions satisfying $A^n + B^n = C^n$ with $n \geq 4$. Let $T = \begin{pmatrix} t_1 & t_2 \\ t_2 & t_3 \end{pmatrix} \in H(2, \mathbb{Q})$, then $t_1 - t_3 = 2t_2$. It is easy to see that the eigenvalues of T are

$$(4) \quad \lambda_{\pm}(T) = \frac{t_1 + t_3 \pm 2t_2\sqrt{2}}{2} \in \mathbb{Q}(\sqrt{2}).$$

By Lemma 1, the family $H(2, \mathbb{Q})$ is commuting. Hence, by [8, Theorem 2.2.3], there exists a unitary matrix U which simultaneously upper triangularizes the matrices A, B, C . The assumption $A^n + B^n = C^n$ implies that

$$(U^* A U)^n + (U^* B U)^n = (U^* C U)^n.$$

Comparing the (1,1) entries on both sides, we have that

$$(5) \quad \lambda_{\epsilon}(A)^n + \lambda_{\xi}(B)^n = \lambda_{\eta}(C)^n,$$

where $\epsilon, \xi, \eta \in \{+, -\}$ according to the choice of the eigenvalues of (4). The eigenvalues, according to (4), are elements of $\mathbb{Q}(\sqrt{2})$, and thus by a result of Jarvis and Meekin [9], one of the eigenvalues should be 0, say $\lambda_{\epsilon}(A)$. From (4), if $A = \begin{pmatrix} a_1 & a_2 \\ a_2 & a_3 \end{pmatrix}$, $a_1 - a_3 = 2a_2$, then $\lambda_{\epsilon}(A) = \frac{a_1 + a_3 \pm 2a_2\sqrt{2}}{2}$. The condition $\lambda_{\epsilon}(A) = 0$ implies that $a_2 = 0$, and thus $a_1 = a_3$ which is nonzero for $A \neq 0$, gives a contradiction. Therefore, the matrix equation has no nontrivial solutions in

$H(2, \mathbb{Q})$ for $n \geq 4$. Apply the same reasoning to prove Theorem 2, we obtain that the Fermat's matrix equation $A^n + B^n = C^n$ has no solution in $H(-2, \mathbb{Q})$ for $n \geq 4$.

Assume $q = \pm 3, \pm 6$. We quote a result due to Freitas and Siksek [5]: The Fermat's equation $x^n + y^n = z^n$ has no nontrivial solutions in $\mathbb{Q}(\sqrt{d})$ for $n \geq 4$ when $3 \leq d \neq 5, 17 \leq 23$ is a square free integer. Let $T = \begin{pmatrix} t_1 & t_2 \\ t_2 & t_3 \end{pmatrix} \in H(q, \mathbb{Q})$. Then $t_1 - t_3 = qt_2$. It is easy to see that the eigenvalues of T are

$$\lambda_{\pm}(T) = \frac{t_1 + t_3 \pm t_2 \sqrt{q^2 + 4}}{2} \in \mathbb{Q}(\sqrt{q^2 + 4}).$$

If $q = \pm 3$, $q^2 + 4 = 13$. Suppose $A^n + B^n = C^n$ has no nontrivial solutions in $H(q, \mathbb{Q})$. Repeating the argument used for $q = \pm 2$, we obtain the equation (5) has a solution in $\mathbb{Q}(\sqrt{13})$, a contradiction. For $q = \pm 6$, in this case, $q^2 + 4 = 40$, and $\mathbb{Q}(\sqrt{40}) = \mathbb{Q}(\sqrt{10})$. The conclusion follows a similar way. \square

For $q = 0$, we have the following result.

Theorem 4. *The Fermat's matrix equation $A^n + B^n = C^n$ has infinitely many solutions in $H(0, \mathbb{Z})$ for all positive integer n .*

Proof. We claim that for arbitrary $a, b \in \mathbb{C}$ and positive integer n ,

$$(6) \quad \begin{pmatrix} a & a \\ a & a \end{pmatrix}^n + \begin{pmatrix} b & -b \\ -b & b \end{pmatrix}^n = \begin{pmatrix} a+b & a-b \\ a-b & a+b \end{pmatrix}^n.$$

Direct computations show that

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix}^n = a^n \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}^n = a^n \begin{pmatrix} 2^{n-1} & 2^{n-1} \\ 2^{n-1} & 2^{n-1} \end{pmatrix}$$

and

$$\begin{pmatrix} b & -b \\ -b & b \end{pmatrix}^n = a^n \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}^n = b^n \begin{pmatrix} 2^{n-1} & -2^{n-1} \\ -2^{n-1} & 2^{n-1} \end{pmatrix}.$$

On the other hand,

$$\begin{aligned} \begin{pmatrix} a+b & a-b \\ a-b & a+b \end{pmatrix}^n &= \left(\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^{-1} \right)^n \\ &= \begin{pmatrix} \frac{1}{2}((2a)^n + (2b)^n) & \frac{1}{2}((2a)^n - (2b)^n) \\ \frac{1}{2}((2a)^n - (2b)^n) & \frac{1}{2}((2a)^n + (2b)^n) \end{pmatrix}. \end{aligned}$$

This proves the identity (6). \square

Remark. It is explicitly proved in [4] that there exist solutions of the Fermat's matrix equation $A^4 + B^4 = C^4$ in 2-by-2 integral matrices. In addition, it is shown [10] that the Fermat's matrix equation $A^n + B^n = C^n$ has infinitely many solutions in weighted shift integral matrices. Theorem 4 provides a class of positive semidefinite integral matrices which is a subset of $H(0, \mathbb{Z})$ and assures the solvability of Fermat's matrix equation (6).

Vaserstein [14] proved that the Fermat's matrix equation $A^n + B^n = C^n$ in $GL_2(\mathbb{Z})$ with $\det = \pm 1$ has a nontrivial solution if and only if n is not a multiple of 4 or 6. In $SL_2(\mathbb{Z})$, Khazanov [11] proved that the Fermat's matrix equation has a nontrivial solution if and only if n is not a multiple of 3 or 4. When $n = 4$, there is a solution in 2-by-2 invertible matrices, for instance,

$$\begin{pmatrix} 1 & 6 \\ 9 & 4 \end{pmatrix}^4 + \begin{pmatrix} 8 & 6 \\ 1 & 7 \end{pmatrix}^4 = \begin{pmatrix} 5 & 10 \\ 5 & 5 \end{pmatrix}^4.$$

For $n = 4, 6$, we have the following result.

Theorem 5. *The Fermat's matrix equation $A^n + B^n = C^n$ has no nontrivial solutions in $H(q, \mathbb{Q})$ for any integer $q \neq 0$ when $n = 4$ and 6.*

Proof. As indicated in the proof of Theorem 3, the eigenvalues of a matrix in $H(q, \mathbb{Q})$ are elements in $\mathbb{Q}(\sqrt{q^2 + 4})$. Suppose there are matrices $A, B, C \in H(q, \mathbb{Q})$ satisfying $A^4 + B^4 = C^4$. Apply the same technique used in the proof of Theorem 3, it yields

$$(7) \quad \lambda_\epsilon(A)^4 + \lambda_\xi(B)^4 = \lambda_\eta(C)^4,$$

where $\epsilon, \xi, \eta \in \{1, -1\}$ according to the choice of the respective eigenvalues. By a theorem of [1]: The equation $x^4 + y^4 = z^4$ has nontrivial solutions in the field $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer, $d \neq 0, 1$, if and only if $d = -7$. Since $q^2 + 4 \neq -7$ and $q^2 + 4$ is square free for $q \neq 0$, it follows that the equation $x^4 + y^4 = z^4$ has no nontrivial solutions in $\mathbb{Q}(\sqrt{q^2 + 4})$, a contradiction to the fact of (7).

The assertion for $n = 6$ can be followed by using the similar argument to the Fermat's matrix equation $n = 4$, and applying a known result by Aigner [2] that the equation $x^6 + y^6 = z^6$ has no nontrivial solutions in the field $\mathbb{Q}(\sqrt{d})$ if d is a square-free integer, $d \neq 0, 1$. \square

We summarize in Table 1 the solvability of the Fermat's matrix equation $A^n + B^n = C^n$, $A, B, C \in H(q, \mathbb{Q})$, $q \in \mathbb{Z}$.

TABLE 1. Solvability of $A^n + B^n = C^n$ in $H(q, \mathbb{Q})$

q	n	nontrivial solutions
0	≥ 3	∞ (Theorem 4)
± 1	3	∞ (Theorem 2)
$\pm 2, \pm 3, \pm 6$	≥ 4	\emptyset (Theorem 3)
$\neq 0$	4, 6	\emptyset (Theorem 5)

Although our discussion, so far, is restricted to 2-by-2 matrices, we may relax our results to higher dimensions of matrices. One typical generalization is given as follows.

For any positive integer m , denote

$$H_{2m}(q, \mathbb{K}) = \left\{ \left(\begin{array}{ccc} T_{11} & \cdots & T_{1m} \\ \vdots & \ddots & \vdots \\ T_{m1} & \cdots & T_{mm} \end{array} \right) \in M_{2m}(\mathbb{K}), T_{ij} \in H(q, \mathbb{K}), i, j = 1, \dots, m \right\}.$$

Theorem 6. *The Fermat's matrix equation (2) has infinitely many solutions in $H_{2m}(\pm 1, \mathbb{N})$ for $n = 3$.*

Proof. We prove the case for $H_{2m}(1, \mathbb{N})$, and it can be proved analogously for the case $H_{2m}(-1, \mathbb{N})$. Clearly, $H_{2m}(q, \mathbb{K})$ is a commuting family. By Theorem 2, there are matrices $A, B, C \in H(1, \mathbb{N})$ satisfying $A^3 + B^3 = C^3$. Let $\hat{A}, \hat{B}, \hat{C} \in M_{2m}(\mathbb{N})$ be three block diagonal matrices with block diagonals being A, B and C , respectively. Then, we have $\hat{A}^3 + \hat{B}^3 = \hat{C}^3$. Let $T = (T_{ij}) \in H_{2m}(1, \mathbb{N})$. Since T_{ij} commutes with A, B and C for $i, j = 1, \dots, m$, it follows that T commutes with \hat{A}, \hat{B} and \hat{C} , and thus

$$(T\hat{A})^3 + (T\hat{B})^3 = (T\hat{C})^3,$$

where $T\hat{A}, T\hat{B}, T\hat{C} \in H_{2m}(1, \mathbb{N})$. □

Finally, we give another matrix class for which the Fermat's matrix equation has no solutions.

Theorem 7. *The Fermat's matrix equation $A^n + B^n = C^n$, $n \geq 4$, has no nontrivial solutions in the class of $m \times m$ complex row stochastic matrices with nonzero row sums belonging to the quadratic field $\mathbb{Q}(\sqrt{2})$.*

Proof. Let $\mathcal{C} = \{A = (a_{ij}) \in M_m(\mathbb{C}) : \sum_{j=1}^m a_{ij} = r(A) \in \mathbb{Q}(\sqrt{2}), i = 1, 2, \dots, m\}$. Then the class \mathcal{C} has a common eigenvector $u_1 = \frac{1}{\sqrt{m}}(1, 1, \dots, 1)^T \in \mathbb{C}^m$ corresponding to the eigenvalue r_A for every $A \in \mathcal{C}$. Extend the vector u_1 to an orthonormal basis u_1, u_2, \dots, u_m for \mathbb{C}^m , and denote the unitary matrix $U = [u_1 \ u_2 \ \cdots \ u_m]$, we obtain that, for $A \in \mathcal{C}$,

$$U^*AU = \left[\begin{array}{c|ccc} r(A) & t_{12} & t_{13} & \cdots & t_{1k} \\ \hline 0 & & & & \\ 0 & & A_1 & & \\ \vdots & & & & \\ 0 & & & & \end{array} \right].$$

As a consequence, we have

$$A^n = U \left[\begin{array}{c|ccc} r(A)^n & \tilde{t}_{12} & \tilde{t}_{13} & \cdots & \tilde{t}_{1k} \\ \hline 0 & & & & \\ 0 & & \tilde{A}_1 & & \\ \vdots & & & & \\ 0 & & & & \end{array} \right] U^*.$$

Hence, if $A, B, C \in \mathcal{C}$ satisfy the matrix equation $A^n + B^n = C^n$, $n \geq 4$, then

$$r(A)^n + r(B)^n = r(C)^n, \quad n \geq 4$$

which, by [9], should not have nontrivial solutions $\mathbb{Q}(\sqrt{2})$, and leads to a contradiction. \square

We have the following immediate consequence.

Theorem 8. *The Fermat's matrix equation $A^n + B^n = C^n$ has no nontrivial solutions in the circulant matrices with entries from $\mathbb{Q}(\sqrt{2})$ and nonzero row sum for $n \geq 4$.*

Remark. It is obvious that matrices in $H(0, \mathbb{N})$ are circulant with nonzero row sum. In contrast with Theorem 4, the Fermat's matrix equation $A^n + B^n = C^n$, according to Theorem 8, has no nontrivial solutions in $H(0, \mathbb{N})$ for $n \geq 4$.

References

- [1] A. Aigner, *Über die Möglichkeit von $x^4 + y^4 = z^4$ in quadratischen Körpern*, Jber. Deutsch. Math.-Verein **43** (1934), 226–229.
- [2] ———, *Die Unmöglichkeit von $x^6 + y^6 = z^6$ und $x^9 + y^9 = z^9$ in quadratischen Körpern*, Monatsh. Math. **61** (1957), 147–150. <https://doi.org/10.1007/BF01641485>
- [3] Z. Cao and A. Grytczuk, *Fermat's type equations in the set of 2×2 integral matrices*, Tsukuba J. Math. **22** (1998), no. 3, 637–643. <https://doi.org/10.21099/tkbjm/1496163669>
- [4] R. Z. Domiaty, *Solutions of $x^4 + y^4 = z^4$ in 2×2 integral matrices*, Amer. Math. Monthly **73** (1966), 631. <https://doi.org/10.2307/2314801>
- [5] N. Freitas and S. Siksek, *Fermat's last theorem over some small real quadratic fields*, Algebra Number Theory **9** (2015), no. 4, 875–895. <https://doi.org/10.2140/ant.2015.9.875>
- [6] A. Grytczuk, *On Fermat's equation in the set of integral 2×2 matrices*, Period. Math. Hungar. **30** (1995), no. 1, 67–72. <https://doi.org/10.1007/BF01876927>
- [7] A. Grytczuk and I. Kurzydło, *Note on the matrix Fermat's equation*, Notes Num. Theory Disc. Math. **17** (2011), 4–11.
- [8] R. A. Horn and C. R. Johnson, *Matrix Analysis*, second edition, Cambridge University Press, Cambridge, 2013.
- [9] F. Jarvis and P. Meekin, *The Fermat equation over $\mathbb{Q}(\sqrt{2})$* , J. Number Theory **109** (2004), no. 1, 182–196. <https://doi.org/10.1016/j.jnt.2004.06.006>
- [10] I. Kaddoura and H. Katbi, *A matrix analog to last Fermat's theorem and Beal's conjecture*, 22th LAAS International Science Conference, Lebanon, 2016.
- [11] A. Khazanov, *Fermat's equation in matrices*, Serdica Math. J. **21** (1995), no. 1, 19–40.
- [12] M. Le and C. Li, *On Fermat's equation in integral 2×2 matrices*, Period. Math. Hungar. **31** (1995), no. 3, 219–222. <https://doi.org/10.1007/BF01882197>
- [13] H. Qin, *Fermat's problem and Goldbach's problem over $M_n \mathbf{Z}$* , Linear Algebra Appl. **236** (1996), 131–135. [https://doi.org/10.1016/0024-3795\(94\)00137-5](https://doi.org/10.1016/0024-3795(94)00137-5)
- [14] L. N. Vaserstein, *Noncommutative number theory*, in Algebraic K-theory and algebraic number theory (Honolulu, HI, 1987), 445–449, Contemp. Math., 83, Amer. Math. Soc., Providence, RI, 1989. <https://doi.org/10.1090/conm/083/991989>
- [15] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. <https://doi.org/10.2307/2118559>

MAO-TING CHIEN
DEPARTMENT OF MATHEMATICS
SOOCHOW UNIVERSITY
TAIPEI 11102, TAIWAN
Email address: `mtchien@scu.edu.tw`

JIE MENG
FINANCE-FISHERY-MANUFACTURE INDUSTRIAL MATHEMATICS CENTER ON BIG DATA
PUSAN NATIONAL UNIVERSITY
BUSAN 46241, KOREA
Email address: `mengjie@pusan.ac.kr`