Serdica
Mathematical Journal
Сердика
Математическо списание

Serdica Math. J. **21** (1995), 19-40

Serdica
Mathematical Journal
Institute of Mathematics
Bulgarian Academy of Sciences

FERMAT'S EQUATION IN MATRICES

Alex Khazanov

Communicated by E. Formanek

Abstract. The Fermat equation is solved in integral two by two matrices of determinant one as well as in finite order integral three by three matrices.

1. Introduction. In [1] L. N. Vaserstein suggested solving some variations on various classical number theory problems in matrices. In particular he suggested Fermat's equation in $\mathrm{SL}_2\mathbf{Z}$ and $\mathrm{GL}_3\mathbf{Z}$, emphasizing exponents n for which solutions exist. We solve this problem for $\mathrm{SL}_2\mathbf{Z}$ and for periodic matrices in $\mathrm{GL}_3\mathbf{Z}$. As a consequence of our characterization of the solutions to these equations, we obtain some new non-trivial symmetries on certain affine varieties; and the question of possible generalizations of these results is raised. Part of our approach involves passing via conjugation from solutions in integral matrices to solutions in simpler (e.g. diagonal) matrices, whose entries are no longer necessarily integral or rational. This raises questions about necessary and sufficient conditions for matrices of one type to be simultaneously transformable by a conjugation into matrices of another type.

2. Statement of results.

A) On equation $x^n + y^n = z^n$ in $\mathrm{SL}_2\mathbf{Z}$, $\mathrm{SL}_3\mathbf{Z}$, $\mathrm{GL}_3\mathbf{Z}$, and $\mathrm{SL}_2\mathbf{Q}$:

1991 *Mathematics Subject Classification:* 11D41,15A24,15A36,14J50.

Key words: matrix equations, Fermat equation, simultaneous similarity, automorphisms on affine varieties.

(i) In $\mathrm{SL}_2\mathbf{Z}$ the equation has solutions if and only if n is not a multiple of 3 or 4;

(ii) In $\mathrm{GL}_3\mathbf{Z}$ or $\mathrm{SL}_3\mathbf{Z}$ periodic solutions exist if and only if n is not a multiple of 3;

(iii) In $\mathrm{GL}_3\mathbf{Z}$ solutions do not exist if n is a multiple of either 21 or 96;

(iv) In $\mathrm{SL}_3\mathbf{Z}$ solutions do not exist if n is a multiple of 48;

(v) For any solution $x^n + y^n = z^n$ in $\mathrm{SL}_2\mathbf{Q}$ there exists a matrix f in $\mathrm{GL}_2\mathbf{Q}$ such that for $x_1 = f^{-1}xf$, $y_1 = f^{-1}yf$, $z_1 = f^{-1}zf$, we have $x_1^n + y_1^n = z_1^n$ and $x_1^n \in \mathrm{SL}_2\mathbf{Z}$, $y_1^n \in \mathrm{SL}_2\mathbf{Z}$, $z_1^n \in \mathrm{SL}_2\mathbf{Z}$, $x_1 \in \mathrm{SL}_2\mathbf{Q}$, $y_1 \in \mathrm{SL}_2\mathbf{Q}$, $z_1 \in \mathrm{SL}_2\mathbf{Q}$;

(vi) For $n = 3$ solutions in $\mathrm{SL}_2\mathbf{Q}$ exist.

B) On related questions of when a set of matrices can be transformed by the same conjugation from one type into another:

(i) If $A_1, \ldots, A_m \in \mathrm{SL}_n\mathbf{Q}$ (respectively $\mathrm{GL}_n\mathbf{Q}$, $\mathbf{M}_n\mathbf{Q}$), then the following conditions are equivalent:

1°) There exists $F \in \mathrm{GL}_n\mathbf{Q}$ such that $F^{-1}A_iF$ are integral matrices for all i;

2°) For any element C in the multiplicative semigroup G, generated by all A_i $(i = 1, \ldots, m)$, $\mathrm{tr}C \in \mathbf{Z}$;

3°) There exists an effectively obtainable integer d such that $dC \in \mathbf{M}_n\mathbf{Z}$ for any $C \in G$ (see 2°);

4°) There exists an effective algorithm for finding $F \in \mathrm{GL}_n\mathbf{Q}$ such that $F^{-1}A_iF \in \mathrm{SL}_n\mathbf{Z}$ (respectively $\mathrm{GL}_n\mathbf{Z}$, $\mathbf{M}_n\mathbf{Z}$) for all i;

(ii) If $A, B \in \mathrm{SL}_2\mathbf{Q}$, then the conditions of (i) are also equivalent to

5°) $\mathrm{tr}A \in \mathbf{Z}$, $\mathrm{tr}B \in \mathbf{Z}$, $\det(A + B) \in \mathbf{Z}$;

(iii) Suppose $A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, $\lambda_i \in K = \mathbf{Q}(\sqrt{D})$, $\lambda_2 = \overline{\lambda}_1$ (hereafter for each $x \in K, \overline{x}$ denotes the K-conjugate of x), $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Then the following conditions are equivalent:

1°) There exists a matrix $F \in \mathrm{GL}_2K$ such that $F^{-1}AF \in \mathrm{SL}_2\mathbf{Q}$, $F^{-1}BF \in \mathrm{SL}_2\mathbf{Q}$;

2°) $\det A = \det B = 1$; $d = \overline{a}$, $\mathrm{N}(a)$ -1 is the norm of an element in K;

(iv) For $\alpha \in \mathbf{Q}$, $m \in \mathbf{Q}$ the following conditions are equivalent:

1°) There exist $A, B \in \mathrm{SL}_2\mathbf{Q}$ such that $\mathrm{tr}A = 2\alpha$, $\mathrm{tr}B = 2m$, $A + B \in \mathrm{SL}_2\mathbf{Q}$;

2°) $(\alpha m + 1/2)^2 - (\alpha^2 - 1)(m^2 - 1)$ is the norm of an element in $\mathbf{Q}(\sqrt{\alpha^2 - 1})$.

(v) Let K is a cyclic extension of $\mathbf{Q}$ of degree n with generating automorphism δ and $A_1, \dots, A_r \in M_m K$. Then the following conditions are equivalent:

1°) There exists a matrix $F \in \mathrm{GL}_m K$ such that $F^{-1} A_i F \in \mathbf{M}_m \mathbf{Q}$ for all i;

2°) There exists $X \in \mathrm{GL}_m K$ such that $X^{-1} A_i X = A_i^\delta$ for all i and $X \cdot X^{\delta^1} \cdots X^{\delta^{n-1}} = I$ (I stands for the identity matrix).

Conditions similar to the ones in (iii) and (iv) exist for higher dimensions as long as the Galois group of K over $\mathbf{Q}$ is cyclic (and even for arbitrary K — see page 39). However, they are much harder to deal with; the only result obtained through them is A)(ii).

C) On symmetries of a certain variety:

(i) On the variety $(2a^3+3a^2+a+1)^2-4w((3a^2+3a+1)^2/3-(3a^2+3a+1)w+w^2) = -3r^2$ over $\mathbf{C}$ there exists a non-trivial symmetry of period 2, that commutes with the aw-plane symmetry and transforms rational points into rational points.

3. Methods used. We use such well known techniques as consideration of trace modulo 32, modulo 9, consideration of groups $\mathrm{SL}_3(\mathbf{Z}/2\mathbf{Z})$, $\mathrm{SL}_2(\mathbf{Z}/3\mathbf{Z})$, and characteristic polynomials of their elements. Besides that, we use the following Field Theory approach. Suppose that $A+B=C$ for 3 matrices $A, B, C \in \mathrm{GL}_k\mathbf{Q}$. Fix the characteristic polynomials of A, B, and C. In an appropriate extension K and by appropriate conjugation, we obtain $A_1 + B_1 = C_1$, where A_1 is diagonal and fixed, with $A = F^{-1}A_1F$, $B = F^{-1}B_1F$, and $C = F^{-1}C_1F$. (This is only valid in the case when the characteristic polynomial of A is separable.) For any automorphism δ of K over $\mathbf{Q}$ we have $A = A^\delta$, $B = B^\delta$, $C = C^\delta$, i.e., for $X = F(F^\delta)^{-1}$, $X^{-1}A_1X = A_1^\delta, X^{-1}B_1X = B_1^\delta$. If δ generates the Galois group of K over $\mathbf{Q}$, these conditions are also sufficient for A, B, and C to be rational. Since A_1 is diagonal, the condition $X^{-1}A_1X = A_1^\delta$ assumes a very convenient form. The condition that A, B and C are n-th powers or that A, B and C are periodic matrices is utilized in the form of its reflections on their characteristic polynomials.

Once rational solutions are obtained, the question arises whether they can be transformed into integral matrices by the same conjugation. The question is equivalent to the question of the existence of a complete discrete lattice mapped into itself by the linear mappings corresponding to the given rational matrices. Since we can assume any single rational point (or vector) to be a lattice point, the question is equivalent to existence of d in IIB(i)3°. We treat $\sum_{C\in G} \mathbf{Z}C$ as the limit position of M_i ($i \to \infty$), where

$M_0 = \sum_{s=1}^{m} \mathbf{Z}A_s + \mathbf{Z}I$, and $M_{i+1} = \sum_{X,Y \in M_i} \mathbf{Z}XY$. Condition IIB(i) 2° is obviously necessary for IIB(i) 1° and since the dimension of M_i quickly stabilizes, IIB(i) 2° provides us with a sufficient number of necessary equations for any $C \in G$ to find such d (see IIB(i) 3°) effectively. The sufficiency of IIB(i)2° follows. Since M_i eventually gets sandwiched between 2 modules of the same dimension, only a finite number of "allowed" changes can occur as we pass from M_i to M_{i+1}, starting from a point where the dimension is stabilized. Therefore, we can effectively find out whether the module will be stabilized, or a "forbidden" change will occur (no other alternatives exist). In the first case we will effectively find out what the ultimate module is. In the alternative case we will observe a "forbidden" change (in the sense that $dC \notin \mathbf{M}_m\mathbf{Z}$ for some $C \in M_i$, where d can be found effectively by (iii)). Elementary Group Theory is used to derive IIB(ii).

4. Derivation of Results.

4.1. Characteristic Polynomial of Solutions. For any square matrix G we will denote its characteristic polynomial in t as $p(G)$.

Lemma 1.0. *For any matrices $A, B \in \mathrm{SL}_m\mathbf{Q}$ such that $p(A) = p(B)$ is a separable polynomial, the following conditions are equivalent:*

1) *$\exists C \in \mathrm{SL}_m\mathbf{Q}$ such that $A = C^n$;*

2) *$\exists D \in \mathrm{SL}_m\mathbf{Q}$ such that $B = D^n$.*

Proof. The matrices A and B are conjugate, i.e., $\exists F \in \mathrm{GL}_m K$ such that $B = F^{-1}AF$ for some field $K \supset \mathbf{Q}$. That means that $FB = AF$ and $\det F \neq 0$. The condition $FB = AF$ can be rewritten as system of homogeneous linear equations with rational coefficients. The set Ω of all matrices F which satisfy the condition $FB = AF$ can thus be parameterized linearly, so that rational parameters correspond to rational matrices. If all the rational points in the set Ω lied in the subspace $\{F | \det F = 0\}$ then $\det F$ as a polynomial on the parameters would be identically 0. Then there would not exist any field K such that there is a matrix $F \in \mathbf{M}_m K \bigcap \Omega$ with $\det F \neq 0$. That would be a contradiction. Thus the matrix F can be chosen in $\mathrm{GL}_m\mathbf{Q}$. For any C such that $C^n = A$ we can now set $D = F^{-1}CF \in \mathrm{SL}_m\mathbf{Q}$ and for any D such that $D^n = B$ we can set $C = FDF^{-1} \in \mathrm{SL}_m\mathbf{Q}$ to complete the proof.

a) The case of $\mathrm{SL}_2\mathbf{Z}$

Lemma 1.1. *If $A^3 + B^3 = C^3$ with $A, B, C \in \mathrm{SL}_2(\mathbf{Z}/9\mathbf{Z})$ then*

$$\mathrm{tr}A^3 = \mathrm{tr}B^3 = \mathrm{tr}C^3 = 0.$$

Proof. Let $a = \mathrm{tr}A$, $b = \mathrm{tr}B$, $c = \mathrm{tr}C$. Then $\mathrm{tr}A^3 = a^3 - 3a$, $\mathrm{tr}B^3 = b^3 - 3b$, $\mathrm{tr}C^3 = c^3 - 3c$. In $\mathbf{Z}/9\mathbf{Z}$, $x^3 - 3x$ is 0, -2, and 2 for $x \equiv 0, 1, 2 (\mathrm{mod} 3)$ respectively. Since $\mathrm{tr}A^3 + \mathrm{tr}B^3 = \mathrm{tr}C^3$ we obtain that either $\mathrm{tr}A^3$, $\mathrm{tr}B^3$, or $\mathrm{tr}C^3$ equals 0. Unless $\mathrm{tr}A^3 = \mathrm{tr}B^3 = \mathrm{tr}C^3 = 0$, the equality can be rearranged and values of variables can be redefined so that $\mathrm{tr}A^3 = 0$, $\mathrm{tr}B^3 = 2$, $\mathrm{tr}C^3 = 2$. We must prove that the latter is impossible. We now consider matrices modulo 3. The characteristic polynomials of B and C modulo 3 are $(t-1)^2$. Hence B and C are conjugate to matrices of the form $\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$, whose cube is I. B^3 and C^3 are thus conjugate to I, i.e., $B^3 = C^3 = I$, hence $A^3 = 0$, i.e., $(\det A)^3 = \det A^3 = 0$, hence $\det A = 0$ (modulo 3). This is a contradiction. Therefore, $\mathrm{tr}A^3 = \mathrm{tr}B^3 = \mathrm{tr}C^3 = 0$, q.e.d.

Lemma 1.2 (L.N.Vaserstein). *For $A, B, C \in \mathrm{GL}_2(\mathbf{Z}/8\mathbf{Z})$, $\mathrm{tr}(A^4 + B^4) \neq \mathrm{tr}C^4$.*

Corollary (L.N.Vaserstein). *The equation $x^n + y^n = z^n$ has no solutions in $\mathrm{GL}_2\mathbf{Z}$ if n is a multiple of 4.*

Periodic Matrices in $\mathrm{SL}_2\mathbf{Z}$

Periodic solutions are particularly sought, since they work for infinitely many exponents at once.

Lemma 1.3. *Any periodic matrix A in $\mathrm{SL}_2\mathbf{Z}$ has period m of either 1, 2, 3, 4 or 6. If $m = 1$, $p(A) = (t-1)^2$; if $m = 2$, $p(A) = (t+1)^2$ or $t^2 - 1$; if $m = 3$, $p(A) = t^2 + t + 1$; if $m = 6$, $p(A) = t^2 - t + 1$. For $m > 2$, the converse is also true.*

Proof. The eigenvalues λ_1, λ_2 of A must satisfy $\lambda_1^m = \lambda_2^m = 1$. If $\lambda_1 \neq \lambda_2$ this is also sufficient. If m is minimal, λ_1 and λ_2 have degree $\phi(m)$, hence $\phi(m) \leq 2$. Thus, $m = 1, 2, 3, 4$ or 6, and if $\phi(m) = 2$ $(m = 3, 4, 6)$, $p(A)$ must be the minimal polynomial of $\sqrt[m]{1}$. This completes the proof.

b) The case of $\mathrm{SL}_3\mathbf{Z}$, $\mathrm{GL}_3\mathbf{Z}$

Lemma 1.4. *For $A \in \mathrm{SL}_3(\mathbf{Z}/2\mathbf{Z}) = \mathrm{GL}_3(\mathbf{Z}/2\mathbf{Z})$, $\mathrm{tr}(A^{21}) = 1$.*

Proof. The group $\mathrm{SL}_3(\mathbf{Z}/2\mathbf{Z})$ has $2^3(2^2-1)(2^3-1) = 168$ elements. Therefore, by the Lagrange theorem, $A^{168} = I$ for any $A \in \mathrm{SL}_3(\mathbf{Z}/2\mathbf{Z})$. Note that for $X \in \mathrm{SL}_3(\mathbf{Z}/2\mathbf{Z})$, $\mathrm{tr}(X^2) = \mathrm{tr}X$, since if $p(X) = t^3 - ut^2 + vt - 1$, then $\mathrm{tr}X = u$, $\mathrm{tr}X^2 = u^2 - 2v = u^2 = u$. Thus $\mathrm{tr}A^{21} = \mathrm{tr}A^{42} = \mathrm{tr}A^{84} = \mathrm{tr}A^{168} = \mathrm{tr}I = 1$.

Corollary 1. *For* $A, B, C \in \mathrm{GL}_3\mathbf{Z}$, $\mathrm{tr}(A^{21}+B^{21}) \neq \mathrm{tr}C^{21}$.

Corollary 2. *Equation* $x^n + y^n = z^n$ *has no solutions in* $\mathrm{SL}_3\mathbf{Z}$ *if* n *is a multiple of* 21.

Lemma 1.5. *For* $A \in \mathrm{SL}_3(\mathbf{Z}/32\mathbf{Z})$, $\mathrm{tr}A^{48} \in \{3, -6, 5\}$.

Proof. For any matrix X we denote by $v(X)$ the coefficient of linear term in the characteristic polynomial of X. We have that $\mathrm{tr}(X^2) = (\mathrm{tr}X)^2 - 2v(X)$, $v(X^2) = (v(X))^2 - 2\mathrm{det}X\mathrm{tr}X = (v(X))^2 - 2\mathrm{tr}X$ (since $\mathrm{det}X = 1$). Note that $\mathrm{tr}X$ and $v(X)$ modulo 2^m determine $\mathrm{tr}X^2$ and $v(X^2)$ modulo 2^{m+1}. Also, $\mathrm{tr}X^3 = (\mathrm{tr}X)^3 - 3\mathrm{tr}Xv(X) + 3\mathrm{det}X = (\mathrm{tr}X)^3 - 3\mathrm{tr}Xv(X) + 3$, $v(X^3) = (v(X))^3 - 3\mathrm{tr}Xv(X)\mathrm{det}X + 3(\mathrm{det}X)^2 = (v(X))^3 - 3\mathrm{tr}Xv(X) + 3$. Therefore, it is impossible that $\mathrm{tr}X^3 \equiv v(X^3) \equiv 0(\mathrm{mod}2)$. Thus, $\mathrm{tr}A^3$ and $v(A^3)$ are not both 0 modulo 2 and we are left with 3 cases for $\mathrm{tr}A^3$ and $v(A^3)$ modulo 2:

Case	$\mathrm{tr}(A^3)$	$V(A^3)$
1	1	1
2	0	1
3	1	0

We now form a table for $\mathrm{tr}A^{3\cdot 2^l}$ and $v(A^{3\cdot 2^l})\mathrm{mod}\ 2^{l+1}$ for $l = 0, \ldots, 4$ in each of the three cases:

Case	Degree	l				
	(tr or v)	**0**	**1**	**2**	**3**	**4**
1	tr	1	-1	3	3	3
	v	1	-1	3	3	3
2	tr	0	0	2	-6	-6
	v	1	1	5	$21 \equiv 5$	$37 \equiv 5$
3	tr	1	1	5	$21 \equiv 5$	$37 \equiv 5$
	v	0	0	2	-6	-6

This completes the proof.

Corollary 1. *For $A, B, C \in \mathrm{SL}_3(\mathbf{Z}/32\mathbf{Z})$, $\mathrm{tr}(A^{48} + B^{48}) \neq \mathrm{tr}C^{48}$.*

Corollary 2. *The equation $x^n + y^n = z^n$ has no solutions in $\mathrm{SL}_3\mathbf{Z}$ if n is a multiple of 48 and no solutions in $\mathrm{GL}_3\mathbf{Z}$ if n is a multiple of 96.*

Corollary 3. *Parts (iii), (iv) of IIA holds (see statement of results).*

Proof. This is Corollary 2 of Lemma 1.4 and Corollary 2 of Lemma 1.5.

Periodic Matrices in $\mathrm{SL}_3\mathbf{Z}$, $\mathrm{GL}_3\mathbf{Z}$

Lemma 1.6. *Any periodic matrix A in $\mathrm{GL}_3\mathbf{Z} \in \mathbf{Z}$ has period $m = 1, 2, 3, 4$ or 6. The characteristic polynomial $p(A)$ is $(t-1)^3$ if $m = 1$, $(t+1)(t \pm 1)(t \pm 1)$ if $m = 2$, $t^3 - 1$ if $m = 3$, $(t^2+1)(t \pm 1)$ if $m = 4$, $(t \pm 1)(t^2 \pm t + 1)$ if $m = 6$. For $m > 2$, the converse is also true.*

The proof is completely similar to the proof of Lemma 1.3.

Corollary 1. *The equation $x^n + y^n = z^n$ has no periodic solutions if n is a multiple of 3.*

Proof. If x is periodic then x^n is periodic and if n is a multiple of 3, according to Lemma 1.6, x^n has period of either 1, 2, or 4. The same applies to y^n and z^n. Since $\mathrm{tr}A^2 \equiv \mathrm{tr}A (\mathrm{mod}\ 2)$ (see proof of Lemma 1.4), we obtain

$$\mathrm{tr}x^n \equiv \mathrm{tr}(x^n)^2 \equiv \mathrm{tr}(x^n)^4 \equiv \mathrm{tr}I \equiv 1 (\mathrm{mod} 2).$$

Similarly, $\mathrm{tr}y^n \equiv 1 (\mathrm{mod}\ 2)$, $\mathrm{tr}z^n \equiv 1 (\mathrm{mod}\ 2)$, hence $\mathrm{tr}(x^n + y^n) \not\equiv \mathrm{tr}z^n (\mathrm{mod}\ 2)$, and $x^n + y^n \neq z^n$, q.e.d.

Corollary 2. *If $A + B = C$ and $p(A) = p(B) = p(C) = t^3 - 1$, then the equation $x^n + y^n = z^n$ has periodic solutions in $\mathrm{SL}_3\mathbf{Z}$ for any n that is not a multiple of 3.*

Proof. By Lemma 1.6, $A^3 = B^3 = C^3 = I$. Thus for $n \equiv 1 (\mathrm{mod}\ 3)$, $A^n + B^n = A + B = C = C^n$. For $n \equiv 2 (\mathrm{mod}\ 3)$, assume $x = A^{-1}$, $y = B^{-1}$, $z = C^{-1}$ and obtain: $x^n + y^n = A^{-n} + B^{-n} = A + B = C = C^{-n} = z^n$, q.e.d.

4.2. Solutions in non rational entry matrices, one of which is diagonal. Here we do not deal with solutions of $x^n + y^n = z^n$ itself. Instead, we consider solutions of the equation $A + B = C$ with certain restrictions on their characteristic polynomials.

a. The case of $\mathrm{SL}_2\mathbf{K}$

Lemma 2.1. *Suppose* $A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, $\lambda_i \in K = \mathbf{Q}(\sqrt{D})$, $\lambda_2 = \overline{\lambda}_1$, $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$*;* $\det A = \det B = 1$, $\mathrm{tr} A = 2\alpha \in \mathbf{Q}$, $\mathrm{tr} B = 2m \in \mathbf{Q}$*;* $D = \alpha^2 - 1$*;* $a = m_1 + n\sqrt{D}$, m_1, $n \in \mathbf{Q}$*;* $\lambda_1 = \alpha + \sqrt{D}$*. Then the following conditions* 1° *and* 2° *are equivalent if* $\sqrt{D} \notin \mathbf{Q}$ *((*1°*) follows from (*2°*) in any case):*

1°) $\det(A+B) = 1$*;*

2°) $m_1 = m$, $n = (\alpha m + 1/2)/D$.

If $K = \mathbf{Q}(\sqrt{D}) \neq \mathbf{Q}$, *then* 2° *can also be rewritten as* $d = \overline{a}$, $n = (\alpha m + 1/2)/D$.

Proof. $1^\circ \Rightarrow 2^\circ$. (assuming $\sqrt{D} \notin \mathbf{Q}$). We rewrite $\det A = \det B = \det(A + B) = 1$ as

(1) $\lambda_1\lambda_2 = 1$; $\lambda_2 = \alpha - \sqrt{D}$;

(2) $ad - bc = 1$;

(3) $(a + \lambda_1)(d + \lambda_2) - bc = 1$;

(4) (subtract (1) and (2) from (3)) $a\lambda_2 + d\lambda_1 = -1$.

Since $\lambda_2 = \overline{\lambda}_1$, we obtain: $a\lambda_2 + \overline{a}\lambda_1 \in \mathbf{Q}$, hence $(\overline{a} - d)\lambda_1 = (a\lambda_2 + \overline{a}\lambda_1) - (a\lambda_2 + d\lambda_1) = a\lambda_2 + \overline{a}\lambda_1 + 1 \in \mathbf{Q}$. Since $\overline{a} - d = a + \overline{a} - (a + d) = a + \overline{a} - \mathrm{tr} B \in \mathbf{Q}$, we obtain: either $\overline{a} - d = 0$ or $\lambda_1 = ((\overline{a} - d)\lambda_1)/(\overline{a} - d) \in \mathbf{Q}$. Since $\sqrt{D} = \lambda_1 - \alpha$ and $\sqrt{D} \notin \mathbf{Q}$, we obtain that $\lambda_1 \notin \mathbf{Q}$, hence $\overline{a} - d = 0$ and $d = \overline{a}$. Hence, $2m = a + d = a + \overline{a} = 2m_1$, i.e., $m = m_1$. Now rewrite (4) as

(5) $a\lambda_2 + \overline{a}\lambda_2 = -1$.

Substitute $\lambda_2 = \alpha - \sqrt{D}$, $a = m + n\sqrt{D}$ to obtain: $2\alpha m - 2nD = -1$, hence $n = (2\alpha m + 1)/2D = (\alpha m + 1/2)/D$, q.e.d.

$2^\circ \Rightarrow 1^\circ$. We have: $\det(A + B) = (\lambda_1 + a)(\lambda_2 + d) - bc = \lambda_1\lambda_2 + ad - bc + \lambda_1 d + \lambda_2 a = \det A + \det B + (\alpha + \sqrt{D})(m - n\sqrt{D}) + (\alpha - \sqrt{D})(m + n\sqrt{D}) = 2 + 2\alpha m - 2nD = 1$. (We used $\lambda_2 = 2\alpha - \lambda_1 = \alpha - \sqrt{D}$ and $d = 2m - a = m - n\sqrt{D}$).

b. The case of $\mathrm{SL}_3 K$

Our aim for the SL_3-case is to satisfy the condition for Corollary 2 of Lemma 1.6.

Lemma 2.2. *Let* $\rho = (-1 + \sqrt{-3})/2 = \sqrt[3]{1}$ *and* $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in \mathbf{M}_3\mathbf{Q}(\rho)$.

Let $\Lambda = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \rho & 0 \\ 0 & 0 & \rho^2 \end{pmatrix}$, $u = bd$, $v = cg$, $w = fh$, $p = bfg$, $q = cdh$. *Then the following conditions* 1° *and* 2° *are equivalent:*

1°) $p(A) = p(A + \Lambda) = t^3 - 1$*;*

2°) (a) $e = a\rho$, $i = a\rho^2$,

(b) $u + v + w = 0$,

(c) $u\rho^2 + v\rho + w = 3a^2 + 3a + 1$

(d) $p + q = 2a^3 + 3a^2 + a + 1$

Proof. (1°) is immediately equivalent to the system of equations:

(1) $a + e + i = 0$;

(2) $ae + ai + ei - bd - cg - fh = 0$;

(3) $(a + 1)(e + \rho) + (a + 1)(i + \rho^2) + (e + \rho)(i + \rho^2) - bd - cg - fh = 0$;

(4) $aei - afh + bfg - bdi + cdh - ceg = 1$;

(5) $(a + 1)(e + \rho)(i + \rho^2) - (a + 1)fh + bfg - bd(i + \rho^2) + cdh - c(e + \rho)g = 1$.

We subtract (2) from (3) to obtain (use $\rho^2 + \rho + 1 = 0$):

(6) $a + a\rho^2 + e + e\rho + i + i\rho = 0$;

(7) $a + e\rho + i\rho^2 = 0$.

(1) and (7) can be considered as system of linear equations for e and i whose only solution is $e = a\rho$, $i = a\rho^2$. Thus, (a) follows from 1°.

Now $ae + ai + ei = a^2(\rho^2 + \rho + 1) = 0$, hence (2) implies $bd + cg + fh = 0$, or equivalently (b) $u + v + w = 0$.

We subtract (4) from (5) to obtain, (taking into account (a)) that $3a^2 + 3a + 1 - fh - bd\rho^2 - cg\rho = 0$, from which (c) follows.

Finally, (4) can be rewritten as (d), taking into account (a) and (c).

The converse may be obtained by following derivation backwards.

4.3. Transformation into solutions over Q.

Lemma 3.1 (Hilbert's Theorem #90 for Matrices). *Let K be a cyclic extension of* $\mathbf{Q}$ *of degree n with generating automorphism δ and $X \in \mathrm{GL}_m K$. Then the following conditions are equivalent:*

1°*)* $XX^{\delta^1} \ldots X^{\delta^{n-1}} = I$*;*

2°*)* $\exists F \in \mathrm{GL}_m K$ *such that* $X = F(F^\delta)^{-1}$

Proof. Despite the absence of the commutative property for matrix multiplication, the classical approach works here.

1° follows from 2° trivially, since

$$F(F^{\delta})^{-1}(F(F^{\delta})^{-1})^{\delta}\ldots(F(F^{\delta})^{-1})^{\delta^{n-1}} =$$

$$= F(F^{\delta})^{-1}F^{\delta}(F^{\delta^2})^{-1}\ldots F^{\delta^{n-1}}(F^{\delta^n})^{-1} = F(F^{\delta^n})^{-1} = FF^{-1} = I.$$

Suppose now that 1°) holds. In our exponential notation $Y^{\delta}Y^{\tau} = Y^{\delta+\tau}(\delta+\tau$ and $\tau+\delta$ may be different). For any $\theta \in K$ we set

$$F(\theta) = \sum_{k=0}^{n-1} X^{1+\delta+\delta^2+\ldots+\delta^{k-1}}\theta^{\delta^k}.$$

Note that for all $\theta \in K$,

$$X(F(\theta))^{\delta} = X(\sum_{k=0}^{n-1} X^{\delta+\delta^2+\ldots+\delta^k}\theta^{\delta^{k+1}}) = \sum_{k=0}^{n-2} X^{1+\delta+\delta^2+\ldots+\delta^k}\theta^{\delta^{k+1}} + X^{1+\delta+\delta^2+\ldots+\delta^n}\theta^{\delta^n} =$$

$$= \sum_{k=1}^{n-1} X^{1+\delta+\delta^2+\ldots+\delta^{k-1}}\theta^{\delta^k} + I\theta^{id} = \sum_{k=0}^{n-1} X^{1+\delta+\delta^2+\ldots+\delta^{k-1}}\theta^{\delta^k} = F(\theta).$$

Our goal is to find $\theta \in K$ such that $F(\theta) \in \mathrm{GL}_m K$, so that $X = F(\theta)((F(\theta))^{\delta})^{-1}$. Let $d(\theta) = \det(F(\theta))$. We can write out $d(\theta)$ as a linear combination of characters and the coefficient at $n \cdot id$ will be equal to $\det I = 1$. By Artin's Theorem on the linear independence of characters we obtain that $d(\theta) \not\equiv 0$, hence $\exists \theta \in K$ such that $d(\theta) \neq 0$ and $\det F(\theta) \neq 0$. We let $F = F(\theta)$ to complete the proof.

Theorem 3.1 (B(v) in the statement of results). *Let K and δ be the same as in Lemma 3.1 and $A_1, \ldots, A_r \in \mathbf{M}_m K$. Then the following conditions are equivalent:*

1°) *There exists $F \in \mathrm{GL}_m K$ such that $F^{-1}A_iF \in \mathbf{M}_m\mathbf{Q}$ for all i.*

2°) *There exists $X \in \mathrm{GL}_m K$ such that $X^{-1}A_iX = A_i^{\delta}$ for all i and $X \cdot X^{\delta^1} \cdots X^{\delta^{n-1}} = I$.*

Proof. By Lemma 3.1, condition 2° is equivalent to the existence of $F \in \mathrm{GL}_m K$ such that

$$(F(F^{\delta})^{-1})^{-1}A_iF(F^{\delta})^{-1} = A_i^{\delta}$$

for all i, or equivalently

$$F^{-1}A_iF = (F^{\delta})^{-1}A_i^{\delta}F^{\delta}$$

for all i, or equivalently 1°, since δ generates the Galois group of K over $\mathbf{Q}$.

a. The case of 2 by 2 matrices

Theorem 3.2 (Theorem IIB)(iii) in the statement of results.) *Suppose*

$$A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \ \lambda_i \in K = \mathbf{Q}(\sqrt{D}), \ \lambda_2 = \overline{\lambda}_1, \ B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then the following conditions are equivalent:

1°) *There exists a matrix* $F \in \mathrm{GL}_2 K$ *such that* $F^{-1}AF \in \mathrm{SL}_2\mathbf{Q}$, $F^{-1}BF \in \mathrm{SL}_2\mathbf{Q}$;

2°) $\det A = \det B = 1$; $d = \overline{a}$, $N(a) - 1$ *is the norm of an element in* K.

Proof. We rewrite 1°) according to Theorem 3.1. Note that $A^\delta = \overline{A} = \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}$ and $X^{-1}AX = \overline{A}$ can be rewritten as

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} X = X \begin{pmatrix} \lambda_2 & 0 \\ 0 & \lambda_1 \end{pmatrix}.$$

Thus, if $X = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ then $e = h = 0$. Since

$$X\overline{X} = \begin{pmatrix} 0 & f \\ g & 0 \end{pmatrix} \begin{pmatrix} 0 & \overline{f} \\ \overline{g} & 0 \end{pmatrix} = \begin{pmatrix} f\overline{g} & 0 \\ 0 & \overline{f}g \end{pmatrix},$$

$X\overline{X} = I$ is equivalent to $f\overline{g} = 1$. Finally, $X^{-1}BX = \overline{B}$ can be rewritten as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & f \\ g & 0 \end{pmatrix} = \begin{pmatrix} 0 & f \\ g & 0 \end{pmatrix} \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix},$$

i.e., as system of equations:

(1) $bg = f\overline{c}$;
(2) $af = f\overline{d}$;
(3) $dg = g\overline{a}$;
(4) $cf = g\overline{b}$.

Since $f\overline{g} = 1$, (2) and (3) are both equivalent to $d = \overline{a}$. (1) and (4) can be rewritten as $N(g) = g\overline{g} = gf^{-1} = c(\overline{b})^{-1} = \overline{c}b^{-1} = N(c)(bc)^{-1}$. Thus 1°) implies $d = \overline{a}$ and $N(a) - 1 = ad - 1 = bc = N(cg^{-1})$, that is 1°) implies 2°). Conversely, 2°) implies (2) and (3) and the existence of $s \in K$ such that $N(s) = N(a) - 1$. We let $g = cs^{-1}$,

$f = (\overline{g})^{-1}$ to obtain $X = \begin{pmatrix} 0 & f \\ g & 0 \end{pmatrix}$ which satisfies the necessary conditions. Condition $\det A = \det B = 1$ assures that the resulting conjugates in $\mathbf{M}_2\mathbf{Q}$ in fact lie in $\mathrm{SL}_2\mathbf{Q}$.

Corollary 1. (Theorem IIB)(iv) in the statement of results). *For $\alpha \in \mathbf{Q}$, $m \in \mathbf{Q}$ the following conditions are equivalent:*

1°) *There exist A, B in $\mathrm{SL}_2\mathbf{Q}$ such that $\mathrm{tr}A = 2\alpha$, $\mathrm{tr}B = 2m$, $A + B \in \mathrm{SL}_2\mathbf{Q}$;*

2°) $(\alpha m + 1/2)^2 - (\alpha^2 - 1)(m^2 - 1)$ *is the norm of an element in $\mathbf{Q}(\sqrt{\alpha^2 - 1})$.*

Proof. If $\alpha = \pm 1$, both conditions hold for any m. (Indeed, if $\alpha m \neq -1/2$, we can set

$$A = \begin{pmatrix} \alpha & \alpha \\ 0 & \alpha \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1/(2m+\alpha) \\ 2m+\alpha & 2m \end{pmatrix};$$

if $\alpha m = -1/2$ we can set

$$A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -\alpha \\ \alpha & -\alpha \end{pmatrix},$$

thus showing 1°); 2°) holds since $(\alpha m + 1/2)^2 - (\alpha^2 - 1)(m^2 - 1) = (\alpha m + 1/2)^2$.)

1° ⇒ 2°. If $\alpha \neq \pm 1$, A is conjugate to $A_1 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, where $\lambda_1 = \alpha + \sqrt{D}$, $\lambda_2 = \alpha - \sqrt{D}$, $D = \alpha^2 - 1$. The conjugate B_1 to B under the same conjugation can be written as $B_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbf{Q}(\sqrt{D})$, i.e., $a = m_1 + n\sqrt{D}$ for some rational m_1, n. We have $\det A_1 = \det A = 1$, $\det B_1 = \det B = 1$ and $\det(A_1 + B_1) = \det(A+B) = 1$. Now A_1 and B_1 satisfy condition 1° of Theorem 3.2 and condition 1° of Lemma 2.1. If $\sqrt{D} \in \mathbf{Q}$, condition 2° is obviously satisfied. If $\sqrt{D} \notin \mathbf{Q}$ by Lemma 2.1 we obtain $m = m_1$. Also, $n = (\alpha m + 1/2)/D$. Thus,

$$N(a) - 1 = m^2 - n^2 D - 1 = m^2 - 1 - \frac{(\alpha m + 1/2)^2}{(\alpha^2 - 1)^2} \cdot (\alpha^2 - 1) =$$

$$= (\frac{1}{1 - \alpha^2}) \cdot ((\alpha m + 1/2)^2 - (\alpha^2 - 1)(m^2 - 1)).$$

By Theorem 3.2, $N(a) - 1$ is the norm of an element in $K = \mathbf{Q}(\sqrt{\alpha^2 - 1})$. Also,

$$(\alpha m + 1/2)^2 - (\alpha^2 - 1)(m^2 - 1) = (1 - \alpha^2)(N(a) - 1) = N(\sqrt{\alpha^2 - 1})(N(a) - 1)$$

from which 2° follows.

2° ⇒ 1°. Conversely, we can consider $A_1 = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, $\lambda_1 = \alpha + \sqrt{D}$, $\lambda_2 = \alpha - \sqrt{D}$, $D = \alpha^2 - 1$; $B_1 = \begin{pmatrix} m + n\sqrt{D} & b \\ 1 & m - n\sqrt{D} \end{pmatrix}$, where $n = (\alpha m + 1/2)/D$, $b = m^2 - 1 - n^2 D$. A_1 and B_1 satisfy conditions 2° of Lemma 2.1 and 2° of Theorem 3.2. Thus by Theorem 3.2, $\exists F \in \mathrm{GL}_2\mathbf{Q}(\sqrt{D})$ such that $F^{-1}A_1F \in \mathrm{SL}_2\mathbf{Q}$ and $F^{-1}B_1F \in \mathrm{SL}_2\mathbf{Q}$. By Lemma 2.1, $A_1 + B_1 \in \mathrm{SL}_2\mathbf{Q}(\sqrt{D})$, hence $F^{-1}A_1F + F^{-1}B_1F = F^{-1}(A_1 + B_1)F \in \mathrm{SL}_2\mathbf{Q}$. We let $A = F^{-1}A_1F$, $B = F^{-1}B_1F$ to complete the proof.

Corollary 2. *Suppose, α, $m \in \mathbf{Q}$; 2α, $2m \in \mathbf{Z}$, $2\alpha \equiv 2m \equiv 0 (\mathrm{mod}\ 9)$. Then there do not exist $A, B \in \mathrm{SL}_2\mathbf{Q}$ such that $\mathrm{tr}A = 2\alpha$, $\mathrm{tr}B = 2m$, and $A + B \in \mathrm{SL}_2\mathbf{Q}$.*

Proof. Assume otherwise. By Corollary 1, that would imply

(1) $(\alpha m + 1/2)^2 - (\alpha^2 - 1)(m^2 - 1) = x^2 - (\alpha^2 - 1)y^2$.

with $x, y \in \mathbf{Q}$. Let $d = \mathrm{l.c.d.}(x, y)$. (1) can be rewritten as

(2) $d^2((2\alpha \cdot 2m + 2)^2 - ((2\alpha)^2 - 4)((2m)^2 - 4)) = (4xd)^2 - ((2\alpha)^2 - 4)(2yd)^2$, $xd, yd \in \mathbf{Z}$.

Now $(2\alpha \cdot 2m + 2)^2 - ((2\alpha)^2 - 4)((2m)^2 - 4) \equiv 2^2 - (-4)(-4) \equiv -12 \equiv 6 (\mathrm{mod}\ 9)$. Therefore,

$$(4xd)^2 + (2yd)^2 \equiv (4xd)^2 - ((2\alpha)^2 - 4)(2yd)^2 \equiv$$
$$\equiv d^2((2\alpha \cdot 2m + 2)^2 - ((2\alpha)^2 - 4)((2m)^2 - 4)) \equiv 0 (\mathrm{mod}\ 3).$$

That implies $4xd \equiv 2yd \equiv 0 (\mathrm{mod}\ 3)$, hence the right side in (2) is 0 modulo 9. Since the factor besides d^2 in the left side of (2) is congruent to 6 modulo 9, we conclude that $d \equiv 0 (\mathrm{mod}\ 3)$. That contradicts $d = \mathrm{l.c.d.}(x, y)$, and completes the proof.

Corollary 3. *The equation $x^n + y^n = z^n$ has no solution in $\mathrm{SL}_2\mathbf{Z}$ if n is a multiple of 3.*

Proof. It is sufficient to prove it for $n = 3$. By Lemma 1.1, $\mathrm{tr}x^3 \equiv \mathrm{tr}y^3 \equiv \mathrm{tr}z^3 \equiv 0 (\mathrm{mod}\ 9)$ for any solution (x, y, z). By Corollary 2 under these conditions $z^3 = x^3 + y^3 \notin \mathrm{SL}_2\mathbf{Q}$, which is a contradiction.

Corollary 4.(Theorem IIA)(i) in the statement of results). *The equation $x^n + y^n = z^n$ has solutions in $\mathrm{SL}_2\mathbf{Z}$ if and only if n is not a multiple of either 3 or 4.*

Proof. The "only if" part follows immediately from the corollary of Lemma 1.2 and Corollary 3 of Theorem 3.2. The solutions for the "if" part can be found by carefully looking at [1]. However, we shall demonstrate how the above theorem and lemmas of Section 1 produce the solutions.

We shall also derive that equation $x^3+y^3=z^3$ has solutions in $\mathrm{SL}_2\mathbf{Q}$ (result IIA)(vi)).

To find solutions in $\mathrm{SL}_2\mathbf{Q}$ we need to find α and m satisfying the conditions of Corollary 1 of Theorem 3.2, such that α, m and $\alpha+m$ are not equal to 1 and $A, B, C \in \mathrm{SL}_2\mathbf{Q}$ such that $\mathrm{tr}A^n = 2\alpha$, $\mathrm{tr}B^n = 2m$, and $\mathrm{tr}C^n = 2(\alpha+m)$. We can then apply Lemma 1.0 to obtain the solutions of the equation. For $x \in \mathrm{SL}_2\mathbf{Q}$, $\mathrm{tr}x^3 = (\mathrm{tr}x)^3 - 3\mathrm{tr}x$. If $\mathrm{tr}x = 0$, then, $\mathrm{tr}x^3 = 0$. If we could find $a \in \mathbf{Q}$ such that $\alpha = 0$ and $m = (a^3-3a)/2$ satisfy the conditions of Corollary 1 of Theorem 3.2, we would prove the existence of solutions of $x^3+y^3=z^3$ in $\mathrm{SL}_2\mathbf{Q}$. For $\alpha=0$, $(\alpha m+1/2)^2-(\alpha^2-1)(m^2-1) = m^2-3/4$. For $a=4$, $m=26$, $(\alpha m+1/2)^2-(\alpha^2-1)(m^2-1) = 26^2-3/4 = N(51/2+5\sqrt{-1})$. Thus, solutions of the equation exist. One such solution is

$$x = \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} \dfrac{3}{5} & \dfrac{3}{5} \\ \dfrac{26}{15} & \dfrac{17}{5} \end{pmatrix},$$

$$z^3 = \begin{pmatrix} 6 & 11 \\ 25 & 46 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} + \begin{pmatrix} 5 & 9 \\ 26 & 47 \end{pmatrix} = x^3+y^3$$

(z can be obtained from y by Lemma 1.0).

To find periodic solutions of $x^n+y^n=z^n$ for $n \equiv \pm 2 (\mathrm{mod}\ 12)$ we set $\alpha(x^2) = -1/2$, $m(y^2) = -1/2$ (see Lemma 1.3). Following the procedure of Corollary 1 of Theorem 3.2, Lemma 3.1, etc., we obtain:

$$x = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \; y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \; z = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}$$

($n \equiv 2(\mathrm{mod}12)$). Take their inverse for $n \equiv -2(\mathrm{mod}\ 12)$.

To find periodic solutions for odd n not divisible by 3, we use $\alpha(x) = -1/2$, $m(y) = -1/2$ (Lemma 1.3) to obtain the solution:

$$x = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \; y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \; z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

($n \equiv 1(\mathrm{mod}\ 6)$). Take their inverse for $n \equiv 5(\mathrm{mod}\ 6)$.

b. The case of 3 by 3 matrices

Theorem 3.3. *Let* $\rho = (-1+\sqrt{-3})/2 = \sqrt[3]{1}$ *and* $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in$

$\mathbf{M}_3\mathbf{Q}(\rho)$. *Let* $\Lambda = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \rho & 0 \\ 0 & 0 & \rho^2 \end{pmatrix}$, $u = bd$, $v = cg$, $w = fh$, $p = bfg$, $q = cdh$. *Then the following conditions* 1° *and* 2° *are equivalent:*

1°) *a)* $p(A) = p(A + \Lambda) = t^3 - 1$;

b) $\exists F \in \mathrm{GL}_3\mathbf{Q}(\rho)$ *such that* $F^{-1}AF \in \mathrm{SL}_3\mathbf{Q}$, $F^{-1}\Lambda F \in \mathrm{SL}_3\mathbf{Q}$;

2°) *(a)* $e = a\rho$, $i = a\rho^2$,

(b) $u + v + w = 0$,

(c) $u\rho^2 + v\rho + w = 3a^2 + 3a + 1$,

(d) $p + q = 2a^3 + 3a^2 + a + 1$;

(e) $a, w \in \mathbf{Q}$; $q = \overline{p}$.

Proof. By Lemma 2.2, the combination of parts ((a), (b), (c), (d)) of condition 2° is equivalent to part (a) of condition 1°. We must prove that this combination (or equivalently part (a) of 1°) provided, part (e) of condition 2° should be equivalent to part (b) of condition 1°. We use Theorem 3.1. Since, $\overline{\Lambda} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \rho^2 & 0 \\ 0 & 0 & \rho \end{pmatrix}$, condition $X^{-1}\Lambda X = \overline{\Lambda}$ can be rewritten as

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \rho & 0 \\ 0 & 0 & \rho^2 \end{pmatrix} X = X \begin{pmatrix} 1 & 0 & 0 \\ 0 & \rho^2 & 0 \\ 0 & 0 & \rho \end{pmatrix}$$

to imply that X is of the form $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & 0 & \beta \\ 0 & \gamma & 0 \end{pmatrix}$. Condition $X\overline{X} = I$ can be rewritten as $N(\alpha) = 1$, $\beta\overline{\gamma} = 1$. Condition $X^{-1}AX = \overline{A}$ can be rewritten as $AX = X\overline{A}$, i.e.,

$$\begin{pmatrix} a\alpha & c\gamma & b\beta \\ d\alpha & f\gamma & e\beta \\ g\alpha & i\gamma & h\beta \end{pmatrix} = \begin{pmatrix} \alpha\overline{a} & \alpha\overline{b} & \alpha\overline{c} \\ \beta\overline{g} & \beta\overline{h} & \beta\overline{i} \\ \gamma\overline{d} & \gamma\overline{e} & \gamma\overline{f} \end{pmatrix}$$

which is equivalent to the following system of equations:

(1) $\alpha a = \alpha\overline{a}$;

(2) $c\gamma = \alpha\overline{b}$;

(3) $b\beta = \alpha\overline{c}$;

(4) $\beta\overline{g} = d\alpha$;

(5) $\beta\overline{h} = f\gamma$;

(6) $\beta\overline{i} = e\beta$;

(7) $\gamma\overline{d} = g\alpha$;

(8) $\gamma\overline{e} = i\gamma$;

(9) $h\beta = \gamma\overline{f}$.

We now derive 2° from 1°. Assuming 1°, we also prove that $u \neq 0$, $v \neq 0$, $w \neq 0$.

1° $\Rightarrow$ 2°. (1) implies $a = \overline{a}$, i.e., $a \in \mathbf{Q}$, since $\alpha \neq 0$ as $N(\alpha) = 1$. (4) implies $b\beta\overline{g} = bd\alpha$, and (3) implies $b\beta\overline{g} = \alpha\overline{cg}$. Thus, together (3) and (4) imply $bd\alpha = b\beta\overline{g} = \alpha\overline{cg}$, and since $\alpha \neq 0$, that implies: $bd = \overline{cg}$, i.e., $u = \overline{v}$. By (2°)(b) we have: $w = -(u+v) = -(\overline{v}+v) \in \mathbf{Q}$. If $w = 0$, then either $f = 0$ or $h = 0$, hence by (9) since as $\beta\overline{\gamma} = 1$, $\beta \neq 0$, $\gamma \neq 0$, we would obtain that $f = h = 0$. That would mean $p = q = 0$, hence by 2°(d), $2a^3 + 3a^2 + a + 1 = 0$ which is impossible for $a \in \mathbf{Q}$. Thus, $w \neq 0$. Since $u = \overline{v}$ and $u + v = -w$ that also implies $u \neq 0$, $v \neq 0$. Condition (5) implies:

$$N(\beta h) = \beta\overline{h\beta}h = f\gamma\overline{\beta}h = fh = w = pq/uv = pq/N(u).$$

Since $u \neq 0$, by (3), $\beta = \alpha\overline{c}b^{-1}$, hence

$$N(\beta h) = N(\alpha\overline{c}h/b) = N(ch/b) = N(q/u) = N(q)/N(u).$$

Since $pq = uvw \neq 0$, we have $q \neq 0$, hence $pq/N(u) = N(\beta h) = N(q)/N(u)$ implies: $pq = N(q)$ implies $p = \overline{q}$. Thus, 2°(e) follows from 1° which completes the proof.

Conversely, 2° implies 1°. To prove this we are to prove that under (2°), $\exists\alpha$, β, γ, such that $N(\alpha) = 1$, $\beta\overline{\gamma} = 1$, and conditions (1)–(9) hold.

Condition ($w, a \in \mathbf{Q}$) together with conditions (b) and (c) imply: $v = \overline{u}$. Also if either $u = 0$, $v = 0$, or $w = 0$, then either $p = 0$ or $q = 0$ hence since $q = \overline{p}$, we obtain $p = q = 0$ which is a contradiction under (d). Thus, $u \neq 0$, $v \neq 0$, $w \neq 0$, hence b, d, c, g, f, h, p, $q \neq 0$. We now set arbitrarily $\alpha \in \mathbf{Q}(\rho)$ so that $N(\alpha) = 1$, and then set β according to (3): $\beta = (\alpha\overline{c}/b) \neq 0$. We set $\gamma = 1/\overline{\beta}$. Now we are to prove that conditions (1)–(9) are satisfied.

(1) holds since $a = \overline{a}$ as $a \in \mathbf{Q}$;

(2) holds as $c\gamma = c/\overline{\beta} = c\overline{b}/(\overline{\alpha}c) = \alpha\overline{b}$;

(3) holds by definition of β;

(4) holds since $\beta\overline{g} = \alpha\overline{cg}/b = \alpha\overline{v}/b = \alpha u/b = \alpha d$;

(5) holds since

$$\beta\overline{h} = N(\beta h)/(\overline{\beta}h) = \gamma N(\beta h)/h = f\gamma N(\beta h)/w = (f\gamma/w)N(h\alpha\overline{c}/b) =$$

$$= (f\gamma/w)N(hc/b) = (f\gamma/w)N(q/u) = (f\gamma/w)q\overline{q}/(u\overline{u}) = (f\gamma/w)qp/(uv) =$$

$$= (f\gamma/w)w = f\gamma;$$

(6) holds since $\beta\overline{i} = \beta e$, as $a \in \mathbf{Q}$, $e = a\rho$, $i = a\rho^2$;

(7) holds since $\gamma\overline{d} = \overline{b}\alpha\overline{d}/c = \alpha\overline{bd}/c = \alpha\overline{u}/c = \alpha v/c = \alpha g$;

(8) holds since $\gamma\overline{e} = \gamma i$, since $\overline{e} = i$ (see(6));

(9) holds since $h\beta = (h/\overline{h})\overline{h}\beta = (h/\overline{h})f\gamma = (fh/\overline{fh})(\overline{f}/f)f\gamma = (w/\overline{w})(\overline{f}/f)f\gamma = (\overline{f}/f)f\gamma = \overline{f}\gamma$.

This completes the proof.

Corollary 1. *Any and all solutions of equation $x + y = z$ in $\mathrm{SL}_3\mathbf{Q}$, such that $p(x) = p(y) = p(z) = t^3 - 1$ can be obtained by the following procedure:*

(1) *Take an arbitrary solution (a, w, r) in $\mathbf{Q}$ of the following equation:*

$$(2a^3 + 3a^2 + a + 1)^2 - 4w((3a^2 + 3a + 1)^2/3 - (3a^2 + 3a + 1)w + w^2) = -3r^2;$$

Set $s = r(\rho - \rho^2)$.

(2) *Set* $p = ((2a^3 + 3a^2 + a + 1)^2 + s)/2,$

$q = ((2a^3 + 3a^2 + a + 1)^2 - s)/2;$

$u = m + n\rho$, $v = m + n\rho^2$, *where*

$m = (3a^2 + 3a + 1 - 3w)/3,$

$n = (6a^2 + 6a + 2 - 3w)/3;$

(3) *Select arbitrary b and c : $b \neq 0$, $c \neq 0$. Set $d = u/b$, $e = a\rho$, $g = v/c$, $f = p/(bg)$, $h = w/f$, $i = a\rho^2$; Set*

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}, \quad \Lambda = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \rho & 0 \\ 0 & 0 & \rho^2 \end{pmatrix}.$$

(4) *Select an arbitrary $\alpha \in \mathbf{Q}(\rho)$ such that $N(\alpha) = 1$. Set $\gamma = \overline{b}\alpha c^{-1}$, $\beta = \overline{\gamma}^{-1}$. Set* $X = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & 0 & \beta \\ 0 & \gamma & 0 \end{pmatrix}$.

(5) *Select any F such that $X = F(\overline{F})^{-1}$. One such F can always be chosen by Lemma 3.1. All such F form an open subspace of the linear $\mathbf{Q}$-space determined by linear equations for entries' components (in the form $k + l\rho$) of F (which correspond*

to the matrix equation $X\overline{F} = F$). The open subspace is determined by an additional condition: $\det F \neq 0$. *Set $x = F^{-1}\Lambda F$, $y = F^{-1}AF$, $z = F^{-1}(A + \Lambda)F$.*

Then (x, y, z) is a solution.

Remark 1. The conjugation classes of obtained solutions are in one to one correspondence with solutions (a, w, r) of the equation in step 1.

Remark 2. To obtain all solutions it is sufficient to attribute certain fixed values to b and c in step 3 and in step 4 instead of selecting b, c and α arbitrarily. For example, all solutions could be obtained if we set $b = c = 1$, $\alpha = 1$.

Remark 3. The permutation of x and y leads to a symmetry of period 2 on the variety of the rational solutions of the equations in step 1. It commutes with the aw-plane symmetry $(a, w, r) \mapsto (a, w, -r)$, which corresponds to the transpose operation for matrices. Therefore, in conjunction with the aw -plane symmetry it does not bring about an infinite number of solutions, provided one solution is obtained.

Proof of Corollary 1. Since the polynomial $t^3 - 1$ is separable any solution (x, y, z) can be obtained by conjugation of a solution in the form $(\Lambda, A, \Lambda + A)$ and the conjugation is by a matrix in $\mathrm{GL}_3\mathbf{Q}(\rho)$. Thus, Theorem 3.3 can be applied.

The equation in (1) follows from $p, q \in \mathbf{Q}(\rho)$, $q = \overline{p}$, 2°(d) of Theorem 3.3, and $pq = uvw$, in which v and u can be expressed through a and w due to linear equations 2°((b),(c)). This also explains step 2. Step 3 is self explanatory by definition of u, v, w, p and q. (w, u and v defined in steps 1 and 2 are neither 0). Step 4 is determined by the proof of 2° $\Rightarrow$ 1° of Theorem 3.3. Step 5 is due to the proof of Theorem 3.1 and the proof of Lemma 3.1.

Corollary 2. *The equation $x + y = z$ has solutions in* $\mathrm{SL}_3\mathbf{Q}$ *with $p(x) = p(y) = p(z) = t^3 - 1$.*

Proof. By Corollary 1, it is sufficient to find solutions of the equation in the step (1) of the procedure. One such solution is $a = 0$, $w = 1$, $r = -1/3$.

Since our goal is to find (or to prove the existence of) solutions in $\mathrm{SL}_3\mathbf{Z}$, we shall follow the procedure of Corollary 1 to find solution in $\mathrm{SL}_3\mathbf{Q}$ explicitly to see if we can use conjugation to transform it into a solution in $\mathrm{SL}_3\mathbf{Z}$.

(1) $a = 0$, $w = 1$, $r = 1/3$; $s = 1/3(\rho - \rho^2)$;

(2) $p = (1 + s)/2$, $q = (1 - s)/2$, i.e., $p = 2/3 + (1/3)\rho$, $q = 1/3 - (1/3)\rho$; $u = -2/3 - (1/3)\rho$, $v = -2/3 - (1/3)\rho^2$;

(3) Set $b = 1$, $c = 1$, $d = -2/3 - (1/3)\rho$, $e = 0$, $f = \rho^2$, $g = -2/3 - (1/3)\rho^2$, $h = \rho$, $i = 0$. Set

$$A = \begin{pmatrix} 0 & 1 & 1 \\ \dfrac{-2-\rho}{3} & 0 & \rho^2 \\ \dfrac{-2-\rho^2}{3} & \rho & 0 \end{pmatrix}, \ \Lambda = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \rho & 0 \\ 0 & 0 & \rho^2 \end{pmatrix}.$$

(4) $\alpha = 1$, $\beta = 1$, $\gamma = 1$. $X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

(5) $F(\theta) = \theta I + \overline{\theta} X = \begin{pmatrix} \theta + \overline{\theta} & 0 & 0 \\ 0 & \theta & \overline{\theta} \\ 0 & \overline{\theta} & \theta \end{pmatrix}$. Set $\theta = -\rho$. We obtain

$$F = F(-\rho) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\rho & -\rho^2 \\ 0 & -\rho^2 & -\rho \end{pmatrix}, \quad x = F^{-1}\Lambda F = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix},$$

$$y = F^{-1}AF = \begin{pmatrix} 0 & 1 & 1 \\ \dfrac{-1}{3} & 1 & -1 \\ \dfrac{-2}{3} & 0 & -1 \end{pmatrix}, \quad z = x + y = \begin{pmatrix} 1 & 1 & 1 \\ \dfrac{-1}{3} & 1 & -2 \\ \dfrac{-2}{3} & 1 & -2 \end{pmatrix}.$$

4.4. Transformation into solutions over the integers

Theorem 4.1 (result B(i) in Section II above). *If* $A_1, \dots, A_m \in \mathrm{SL}_n\mathbf{Q}$ *(respectively* $\mathrm{GL}_n\mathbf{Q}$, $\mathbf{M}_n\mathbf{Q}$*), then the following conditions are equivalent:*

1°) *There exists* $F \in \mathrm{GL}_n\mathbf{Q}$ *such that* $F^{-1}A_iF$ *are integral matrices for all* i*;*

2°) *For any element* C *in the multiplicative semigroup* G*, generated by all* A_i *(*$i = 1, \dots, m$*),* $\mathrm{tr}C \in \mathbf{Z}$*;*

3°) *There exists an effectively obtainable integer* d*, such that* $dC \in \mathbf{M}_n\mathbf{Z}$ *for any* $C \in G$ *(see 2°);*

4°) *There exists an effective algorithm for finding* $F \in \mathrm{GL}_n\mathbf{Q}$ *such that* $F^{-1}A_iF \in \mathrm{SL}_n\mathbf{Z}$ *(respectively* $\mathrm{GL}_n\mathbf{Z}$, $\mathbf{M}_n\mathbf{Z}$*) for all* i*.*

Proof.

Proof of the implication 1° ⇒ 2° is trivial.

1° ⇔ existence of d in 3°.

1° is equivalent to the existence of a complete discrete lattice mapped into itself by the linear mappings corresponding to the given rational matrices. Since we can assume any single rational point (or vector) to be a lattice point, the question is equivalent to existence of d in 3°.

2° ⇒ 3°.

Let $M_\infty = \sum\limits_{C\in G} \mathbf{Z}C$. We treat it as the limit position of M_i $(i \to \infty)$, where $M_0 = \sum\limits_{s=1}^{m} \mathbf{Z}A_s + \mathbf{Z}I$, and $M_{i+1} = \sum\limits_{X,Y\in M_i} \mathbf{Z}XY$. Since the dimension of M_i quickly stabilizes, 2° provides us with a sufficient number of equations for any $C \in G$ to find such d (see 3°) effectively.

3° ⇒ 4°.

By 3°, M_i eventually gets sandwiched between 2 modules of the same dimension, hence only finite number of "allowed" changes can occur as we pass from M_i to M_{i+1} starting from a point where the dimension is stabilized. Therefore, we can effectively find out whether the module will be stabilized, or a "forbidden" change will occur (no other alternatives exist). In the first case we will effectively find out what the ultimate module is. In the alternative case we will observe a "forbidden" change (in terms of the effectively found d). It is clear from the proof of equivalence of 1° and existence of d in 3° how the ultimate module M provides us with desired F.

4° ⇒ 1°. The proof is trivial.

Corollary 1. *If $A, B \in \mathrm{SL}_2\mathbf{Q}$, then the following conditions are equivalent:*

1°) *There exists $F \in \mathrm{GL}_2\mathbf{Q}$ such that $F^{-1}AF$, $F^{-1}BF \in \mathrm{SL}_2\mathbf{Z}$;*

2°) $\mathrm{tr}A \in \mathbf{Z}$, $\mathrm{tr}B \in \mathbf{Z}$, $\det(A + B) \in \mathbf{Z}$.

Proof. As $\det(A+B) = \det A + \det B + (\mathrm{tr}A)(\mathrm{tr}B) - \mathrm{tr}(AB)$ condition $\det(A+B) \in \mathbf{Z}$ in 2° can (equivalently) be replaced by the condition $\mathrm{tr}(AB) \in \mathbf{Z}$. 2° thus implies that A, B and AB each satisfy some monic equation of degree 2 with integer coefficients. Therefore, any $C \in G$ (see Theorem), which has AA, BB or $ABAB$ in its representation as the product of A^s and B^s, can be represented as the sum of elements of G which are the products of a lesser number of A^s and B^s. Therefore, to derive condition 2° of the theorem, it is sufficient to prove that traces of the following matrices are integers: A, B, AB, BA, ABA, BAB, $BABA$. This follows immediately from the fact that traces of A, B and AB are integers and so are traces of their inverse, as their determinants equal 1. Thus, by the theorem, 1° follows from 2°. The converse is obvious.

Corollary 2. *For any solution $x^n + y^n = z^n$ in $\mathrm{SL}_2\mathbf{Q}$ there exists a matrix f in $\mathrm{GL}_2\mathbf{Q}$ such that for $x_1 = f^{-1}xf$, $y_1 = f^{-1}yf$, $z_1 = f^{-1}zf$, we have $x_1^n + y_1^n = z_1^n$ and $x_1^n \in \mathrm{SL}_2\mathbf{Z}$, $y_1^n \in \mathrm{SL}_2\mathbf{Z}$, $z_1^n \in \mathrm{SL}_2\mathbf{Z}$, $x_1 \in \mathrm{SL}_2\mathbf{Q}$, $y_1 \in \mathrm{SL}_2\mathbf{Q}$, $z_1 \in \mathrm{SL}_2\mathbf{Q}$.*

Proof. This is immediate from Corollary 1.

Corollary 3. *Equation $x^n + y^n = z^n$ has periodic solutions in $\mathrm{SL}_3\mathbf{Z}$ for any n not divisible by 3.*

Proof. We start with the solution

$$x_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}, \quad y_0 = \begin{pmatrix} 0 & 1 & 1 \\ \frac{-1}{3} & 1 & -1 \\ \frac{-2}{3} & 0 & -1 \end{pmatrix}, \quad z_0 = \begin{pmatrix} 1 & 1 & 1 \\ \frac{-1}{3} & 1 & -2 \\ \frac{-2}{3} & 1 & -2 \end{pmatrix}$$

($n \equiv 1 \bmod 3$) in $\mathrm{SL}_3\mathbf{Q}$ derived in Corollary 2 of Theorem 3.3. By following the algorithm of 4° in Theorem 4.1, we obtain $F = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & -1 \\ 0 & 0 & 1 \end{pmatrix}$, which leads to the solution in $\mathrm{SL}_3\mathbf{Z}$:

$$x = F^{-1}x_0F = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 3 & -2 \end{pmatrix}, \quad y = F^{-1}y_0F = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 1 & -1 \\ -2 & 0 & -1 \end{pmatrix},$$

$$z = x + y = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 2 & -2 \\ -2 & 3 & -3 \end{pmatrix}.$$

5. Related open questions. Still unsolved is $x^3 + y^3 = z^3$ in $\mathrm{SL}_3\mathbf{Z}$ and $\mathrm{GL}_3\mathbf{Z}$ as well as in $\mathrm{SL}_3\mathbf{Q}$. The problem has to do with ranges of norms but in much more complex form than in conditions II(iii) 2° and II(iv)2°, especially when we have to deal with non-cyclic extension. In this case the Theory of Galois cohomologies should substitute Hilbert's Theorem #90. How about solutions in $\mathrm{SL}_m\mathbf{Z}$ for larger m? From this paper it follows that periodic solutions exist for all exponents for which solutions exist in $\mathrm{SL}_2\mathbf{Z}$.

In Remark 3 to Corollary 1 of Theorem 3.3 (p. 36), we mentioned a new symmetry on a certain algebraic variety over $\mathbf{Q}$. Plenty of others can be derived from the connection between certain equations in matrices and certain equations in various fields. How can they be used together with classical Number Theory and Algebraic Geometry approaches to find complete set of symmetries on these varieties or to obtain infinite families of solutions from one?

Invariant spaces (i.e. the spaces mapped into themselves under certain linear mappings) might be used to resolve the question regarding the existence of conjugation, transforming the given set of non-rational matrices into rational matrices. Although initial vector or point now matters this approach might still lead to conditions different from those described above and dealing with norms. How might they be compared with each other to obtain further insights and results?

For matrices of the order greater than 2, is it possible to find an effective limit m such that consideration of products of up to m matrices A_i is sufficient in IIB(i) 2°? ($m = 2$ works for 2 matrices 2 by 2.) Can we find other convenient ways to utilize the integral origin of the matrices in irrational case?

What other methods can be used to handle the original and related questions? Can we to some extent apply modified approaches from Analytic Number Theory and Complex Analysis despite the absence of the commutative property? Can we consider our matrices as linear mappings or embeddings with some special properties on the bases of other structures introduced into the linear spaces, e.g. metrics?

REFERENCES

[1] L. N. Vaserstein. Non Commutative Number Theory. *Contemp. Math.*, **83**, (1989), Amer. Math. Soc., 445-449.

679 Ocean PKWY Apt 6a
Brooklyn NY 11230
USA.

Received June 20, 1994