A GENERALIZATION OF SELFRIDGE'S QUESTION

Devendra Prasad
Department of Mathematics, IISER-Tirupati, Tirupati, Andhra Pradesh, India
devendraprasad@iisertirupati.ac.in

Received: 6/2/20, Accepted: 6/4/21, Published: 6/14/21

Abstract

Selfridge asked to investigate the pairs (m, n) of natural numbers for which $2^m - 2^n$ divides $x^m - x^n$ for all integers x. This question was answered by different mathematicians independently by showing that there are only finitely many such pairs. In the literature, various generalizations of this question have been studied already. Let R be the ring of integers of a number field $\mathbb{K}$ and $M_n(R)$ be the ring of all $n \times n$ matrices over R. In the current article, we suggest a new kind of generalization to Selfridge's question in the case of $M_n(R)$.

1. Introduction

This article is devoted to a generalization of a question asked by Selfridge. Once he observed that $2^2 - 2$ divides $n^2 - n, 2^{2^2} - 2^2$ divides $n^{2^2} - n^2$ and $2^{2^{2^2}} - 2^{2^2}$ divides $n^{2^{2^2}} - n^{2^2}$ for all $n \in \mathbb{N}$. Motivated by this example, he asked the question: for what pairs of natural numbers m and n does $(2^m - 2^n)$ divide $(x^m - x^n)$ for all integers x? We do not know at what point in time he asked this question, but it was published in the book "Unsolved Problems in Number Theory" by Richard Guy (see [3], problem B47). In 1974, Ruderman posed a similar problem.

Question 1 (Ruderman [8])**.** Suppose that $m > n > 0$ are integers such that $2^m - 2^n$ divides $3^m - 3^n$. Show that $2^m - 2^n$ divides $x^m - x^n$ for all natural numbers x.

This famous question is called 'Ruderman's problem' in the literature and is still open. Selfridge's problem was answered for the first time by Pomerance [9] in 1977 by combining results of Schinzel [12] and Velez [10]. Q. Sun and M. Zhang [13] also answered Selfridge's question. Actually, there are fourteen such pairs which are the solution of Selfridge's question and the set of solutions is

$$S = \{(1,0), (2,1), (3,1), (4,2), (5,1), (5,3), (6,2), (7,3), (8,2), (8,4), (9,3), (14,2),$$
$$(15,3), (16,4)\}.$$

In 2011, Ram Murty and Kumar Murty [5] proved that there are only finitely many m and n for which the hypothesis in Question 1 holds. Hence a positive solution to it will also lead to the answer to Selfridge's question.

Once Selfridge's question is answered thoroughly, a natural question arises: what happens if we replace '2' by '3' or, more generally, by some other integer other than ± 1. Bose [1] considered the question of finding solutions of $b^m - b^n$ dividing $a^m - a^n$ for all non-zero integer a, where m and n are positive integers with $m > n$ and b is an integer satisfying $(b^m - b^n) \neq 0$. He proved that the above congruence has a solution if and only if $b = 2$ and, in this case, solutions are precisely the members of S defined above. Rundle [11] also examined two types of generalizations of Selfridge's problem.

Now, a natural question crops up in our mind: what happens if there are three or more terms in Selfridge's problem? More precisely, what are the tuples $(m_1, \ldots, m_k)$ with positive entries such that for a given polynomial $f(x) = \sum_{i=1}^{k} a_i x^{m_i} \in \mathbb{Z}[x]$ and given integer b, $f(b)$ divides $f(m)$ $\forall$ m $\in \mathbb{Z}$, under reasonable conditions.

The arguments used to answer Selfridge's question were elementary and will not suffice to answer this question as already pointed out by Bose (see [1]). However, the notion of the fixed divisor of a polynomial can be used to get rid of this impasse. We first give a general definition of this notion (see Rajkumar, Reddy and Semwal, [7]).

Definition 1. Let A be a ring and $f(\underline{x}) \in A[\underline{x}]$ be a polynomial in n variables. Given $\underline{S} \subseteq A^n$, the *fixed divisor* of f over $\underline{S}$, denoted by $d(\underline{S}, f)$, is defined as the ideal of A generated by the values taken by f on $\underline{S}$.

In the case of $\mathbb{Z}$ or a unique factorization domain (UFD), we manipulate Definition 1 as follows and this definition is more useful than the above definition in this case.

Definition 2. For a polynomial $f(x) \in \mathbb{Z}[x]$, its fixed divisor over $\mathbb{Z}$ is defined as

$$d(\mathbb{Z}, f) = \gcd\{f(a) : a \in \mathbb{Z}\}.$$

Now we paraphrase how this notion is helpful in the study of Selfridge's question. Observe that for a given $a \in \mathbb{Z}\backslash\{\pm 1\}$, $(a^m - a^n)$ divides $(x^m - x^n)$ for all $x \in \mathbb{Z}$ if and only if $(a^m - a^n)$ divides $d(\mathbb{Z}, f_{m,n})$, where $f_{m,n} = x^m - x^n$. Hence, we must have $|a^m - a^n| \leq d(\mathbb{Z}, f_{m,n})$. Now, if we can show that with finitely many exceptions we always have

$$|a^m - a^n| > d(\mathbb{Z}, f_{m,n}),$$

then it will lead to the conclusion that there could be only finitely many pairs, which are the solutions. Vajaitu and Zaharescu [14]) used this argument to generalize Selfridge's question.

In 1999, Vajaitu and Zaharescu [14] generalized Selfridge's question in a number ring and proved the following result.

Theorem 1 (Vajaitu and Zaharescu [14]). *Let R be a number ring of an algebraic number field and let $a_1, a_2, \ldots, a_k$ and b be non-zero elements of R. If b be a non-unit, then there are only finitely many k-tuples $(n_1, n_2, \ldots, n_k) \in \mathbb{N}^k$ satisfying the following simultaneously:*

$$\sum_{i=1}^{k} a_i b^{n_i} \text{ divides } \sum_{i=1}^{k} a_i x_i^{n_i} \quad \text{for all } x \in R$$

and

$$\sum_{i \in S} a_i b^{n_i} \neq 0 \text{ for all } S \subseteq \{1, 2, \ldots, k\}.$$

Vajaitu and Zaharescu also strengthened the conclusion of Theorem 1 for the ring of integers in a specific number field.

Theorem 2 (Vajaitu and Zaharescu [14]). *Let R be the ring of rational integers $\mathbb{Z}$ or the ring of integers in an imaginary quadratic number field and let $a_1, a_2, \ldots, a_k$ and b be non-zero elements of R. Then there are only finitely many elements in R for which there exist k-tuples $(n_1, n_2, \ldots, n_k) \in \mathbb{N}^k$, not all zero, satisfying the following simultaneously:*

$$\sum_{i=1}^{k} a_i b^{n_i} \text{ divides } \sum_{i=1}^{k} a_i x^{n_i} \quad \text{for all } x \in R$$

and

$$\sum_{i \in S} a_i b^{n_i} \neq 0 \text{ for all } S \subseteq \{1, 2, \ldots, k\}.$$

Theorem 1 generalizes Selfridge's question to the case of a number ring. In 2004, Choi and Zaharescu [2] generalized Theorem 1 in the case of n-variables.

Theorem 3 (Choi and Zaharescu [2]). *Let R be the ring of integers in an algebraic number field and let $b_1, b_2, \ldots, b_n$ be non-zero non-unit elements of R. Let $a_{i_1,\ldots,i_n} \in R$, $1 \leq i_1 \leq k_1, \ldots, 1 \leq i_n \leq k_n$, then there are only finitely many n-tuples $(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n) \in \mathbb{N}^{k_1} \times \mathbb{N}^{k_2} \times \cdots \times \mathbb{N}^{k_n}$ satisfying the following simultaneously:*

$$\sum_{i_1=1}^{k_1} \cdots \sum_{i_n=1}^{k_n} a_{i_1,\ldots,i_n} b_1^{m_{1i_1}} \cdots b_n^{m_{ni_n}} \text{ divides } \sum_{i_1=1}^{k_1} \cdots \sum_{i_n=1}^{k_n} a_{i_1,\ldots,i_n} x_1^{m_{1i_1}} \cdots x_n^{m_{ni_n}}$$

for all $\underline{x} \in R^n$ *where* $\mathbf{m}_j = (m_{j1}, \ldots, m_{jk_j})$ *and*

$$\sum_{(i_1,\ldots,i_n) \in S} a_{i_1,\ldots,i_n} b_1^{m_{1i_1}} \cdots b_n^{m_{ni_n}} \neq 0$$

for all non-empty $S \subseteq \{1, 2, \ldots, k_1\} \times \cdots \times \{1, 2, \ldots, k_n\}$.

Choi and Zaharescu also generalized Theorem 2 in this setting. We write the statement for the sake of completeness.

Theorem 4 (Choi and Zaharescu [2])**.** *Let R be the ring of rational integers $\mathbb{Z}$ or the ring of integers in an imaginary quadratic number field. Fix n and choose non-zero elements $a_{i_1,\ldots,i_n} \in R$ for all $1 \leq i_1 \leq k_1, \ldots, 1 \leq i_n \leq k_n$. Then there are only finitely many n-tuples $(b_1, b_2, \ldots, b_n)$ with $b_j \in R, j = 1, \ldots, n$, for which there exists $(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n) \in \mathbb{N}^{k_1} \times \mathbb{N}^{k_2} \times \cdots \times \mathbb{N}^{k_n}$ with none of the tuples $(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n)$ having all the components equal to zero, satisfying the following, simultaneously*

$$\sum_{i_1=1}^{k_1} \cdots \sum_{i_n=1}^{k_n} a_{i_1,\ldots,i_n} b_1^{m_{1i_1}} \cdots b_n^{m_{ni_n}} \text{ divides } \sum_{i_1=1}^{k_1} \cdots \sum_{i_n=1}^{k_n} a_{i_1,\ldots,i_n} x_1^{m_{1i_1}} \cdots x_n^{m_{ni_n}}$$

for all $\underline{x} \in R^n$ *where* $\mathbf{m}_j = (m_{j1}, \ldots, m_{jk_j})$ *and*

$$\sum_{(i_1,\ldots,i_n) \in S} a_{i_1,\ldots,i_n} b_1^{m_{1i_1}} \cdots b_n^{m_{ni_n}} \neq 0$$

for all non-empty $S \subseteq \{1, 2, \ldots, k_1\} \times \cdots \times \{1, 2, \ldots, k_n\}$.

In this article, we consider a generalization of Theorem 1, Theorem 2, Theorem 3 and Theorem 4 in the case when the ring under consideration is that of $n \times n$ matrices over a number ring. We denote by $M_n(A)$, the ring of $n \times n$ matrices over the given ring A. We use the notion of the fixed divisor of a polynomial as our main tool in the generalization. In the case of the ring of the matrices over a ring, a reasonable definition of the fixed divisor of a polynomial is suggested by Prasad, Rajkumar and Reddy ([6], Section 7) with suitable justifications.

Definition 3. For a polynomial $f \in M_n(A)[x]$, its *fixed divisor over* $M_n(A)$ (or $d(M_n(A), f)$) is defined as the ideal in A generated by all the entries of $f(C)\ \forall\ C \in M_n(A)$.

Observe that here the fixed divisor is not considered as an ideal of the ring $M_n(A)$ as usual. This definition is helpful in the study of fixed divisors and related topics. For a given matrix $M \in M_n(\mathbb{K})$, where $\mathbb{K}$ is any number field, recall that the norm

$$\|M\| = \left(\sum_{i,j}^{n} |m_{ij}|^2 \right)^{\frac{1}{2}}$$

makes the space $(M_n(\mathbb{K}), \|\cdot\|)$ a Banach algebra. The spectral radius $\rho(M)$ of M is defined as the largest absolute value of its eigenvalues. We suggest the following generalization of Selfridge's question.

Question 2. Let $A_1, A_2, \ldots, A_k, B$ be non-zero matrices in $M_n(R)$ and B satisfy the following

(A.1) The ideal generated by B is not the whole ring.

(A.2) Either $\rho(B^*B) > n$ or $\rho((B^*B)^{-1}) > n$, where B^* is the conjugate transpose of B.

(A.3) $\Sigma_{i\in S} A_i B^{m_i} \neq 0 \ \forall \ S \subseteq \{1, 2, \ldots, k\}$.

Then, for how many tuples $(m_1, m_2, \ldots, m_k) \in \mathbb{N}^k$, does the ideal generated by $\sum_{i=1}^k A_i B^{m_i}$ contain the ideal generated by $\{\sum_{i=1}^k A_i C^{m_i} : C \in M_n(R)\}$?

We know that each ideal of $M_n(A)$ is of the form $M_n(I)$ for some ideal $I \subseteq A$. Also, for each $I \subseteq A$, $M_n(I)$ is an ideal of $M_n(A)$. For the given ideals I and J of A, the condition $M_n(I) \subseteq M_n(J)$ is equivalent to saying that $I \subseteq J$. For a matrix $M \in M_n(A)$, we denote the ideal generated by all the entries of M in A by I_M. Hence, we have to find the number of tuples $(m_1, m_2, \ldots, m_k) \in \mathbb{N}^k$, for which $I_{f(B)} \supseteq d(M_n(A), f)$ where $f = \sum_{i=1}^k A_i x^{m_i}$.

The structure of the paper is as follows. In Section 2, we give bounds for fixed divisors by combining the arguments of Vajaitu and Zaharescu and fixed divisors. Indeed, our work is motivated by the work of Vajaitu and Zaharescu. In Section 3, we answer Question 2 by proving Theorem 5 and Theorem 6. Finally, in Section 4, we suggest a further generalization of our theorems in the case of several variables when the underlying ring is still $M_n(R)$.

2. Bounds for Fixed Divisors

We fix the notations for the whole paper. Let $\mathbb{N}$ denote the set of natural numbers as usual. For a given tuple $\mathbf{m} = (m_1, m_2, \ldots, m_k) \in \mathbb{N}^k$, m denotes the maximum of m_i where $i = 1, 2, \ldots, k$. The norm of an ideal $I \subseteq R$, where R is a number ring, is denoted by $N(I)$ and is the cardinality of the residue class ring R/I. The norm of an element $a \in R$ is the norm of the ideal generated by the element, which is the same as $\prod_{\sigma\in G} \sigma(a)$, where G is the set of all embeddings from R to $\mathbb{C}$ (see Marcus [4]).

To prove our main theorem, we need several lemmas. With all the notations as in Question 2, we prove the following lemma, in which we consider the case when $\rho(B^*B) > n$. The other case can be handled by considering B^{-1}.

Lemma 1. *Let $\mathbf{m} = (m_1, \ldots, m_k) \in \mathbb{N}^k$ and m be the supremum of the components of $\mathbf{m}$. Under the assumption A.3 above, there exist constants c and d, independent to $\boldsymbol{m}$ such that*

$$\| \sum_{i=1}^{k} A_i B^{m_i} \| \geq c|d|^m.$$

Proof. We claim that $\| \sum_{i=1}^{k} A_i B^{m_i - m} \| \geq c$, for a constant c. Denoting the difference $m - m_i$ by n_i for $i = 1, 2, \ldots, k$, we have to show $\| \sum_{i=1}^{k} A_i B^{-n_i} \| \geq c$. If this is false then there would exist a sequence $(n_{1,r}, n_{2,r}, \ldots, n_{k,r})$ of natural numbers with $\min \{n_{1,r}, n_{2,r}, \ldots, n_{k,r}\} = 0$ for each r, such that when r tends to infinity, $\| \sum_{i=1}^{k} A_i B^{-n_{i,r}} \|$ tends to zero. Let $A \subseteq \{1, 2, \ldots, k\}$ be the largest subset such that for each $r \in A$ there exists a natural number b_r and an infinite sequence M such that $n_{i,r} = b_r$ for each $r \in A$ and $i \in M$. Then, we have the following inequality:

$$\| \sum_{i=1}^{k} A_i B^{-n_{i,r}} \| \leq \| \sum_{i \in A} A_i B^{-b_i} \| + \| \sum_{i \in A^c} A_i B^{-n_{i,r}} \|. \tag{1}$$

Here A^c denotes the complement of A with respect to the set $\{1, 2, \ldots, k\}$. The second term in Equation (1) can be bounded as follows:

$$\| \sum_{i \in A^c} A_i B^{-n_{i,r}} \| \leq \sum_{i \in A^c} \|A_i\| \|B^{-n_{i,r}}\|.$$

Recall that for any matrix $M \in M_n(\mathbb{K})$, we have

$$\|M\| \leq \sqrt{n \rho(M^* M)}.$$

Since $\rho(B^* B) > n$, the quantity

$$\|B^{-n_{i,r}}\| \leq \|B^{-1}\|^{n_{i,r}} \leq \left(\sqrt{n \rho((B^* B)^{-1})} \right)^{n_{i,r}}$$

tends to zero as r tends to infinity. We rewrite the left-hand side of Equation (1) as follows:

$$\| \sum_{i \in A} A_i B^{-b_i} + \sum_{i \in A^c} A_i B^{-n_{i,r}} \|,$$

which tends to zero as r tends to infinity. Observe that $\| \sum_{i \in A^c} A_i B^{-n_{i,r}} \|$ also tends to zero as r tends to infinity leading to the conclusion that

$$\| \sum_{i \in A} A_i B^{-b_i} \| \to \ 0.$$

This implies that $\sum_{i \in A} A_i B^{-b_i} = 0$, which is a contradiction to A.3 of the Question 2. Hence, we must have $\| \sum_{i=1}^{k} A_i B^{m_i - m} \| \geq c$.

We know that for any pair of matrices X and Y in $M_n(R)$, we always have

$$\|XY\| \leq \|X\| \|Y\|.$$

Consequently, we get

$$\| \sum_{i=1}^{k} A_i B^{m_i} \| \geq c \|B^{-m}\|^{-1} \geq c \|B^{-1}\|^{-m},$$

which completes the proof. □

For a given matrix $M = [m_{ij}]_{n\times n}$, we define

$$\sigma(M) = [\sigma(m_{ij})]_{n\times n},$$

where σ is an automorphism of $\mathbb{K}$. With this definition in hand, we can prove that $\sigma(\|M\|^2) = \|\sigma(M)\|^2$. In Lemma 1 , we take the product over all the conjugates of $\|f(B)\|$ and get $N(\|f(B)\|^2) \geq c'|d'|^m$, where c' and d' are new constants. It is clear that $\|f(B)\|^2 \in I_{f(B)}$; hence there exists an ideal $J \subseteq R$ such that $I_{f(B)}J = (\|f(B)\|^2)$. Recall that an element's norm in a number ring is the same as the norm of the ideal generated by that element. Hence, $N(I_{f(B)}J) = N(\|f(B)\|^2) = N(I_{f(B)})N(J)$. Now, we prove that $N(J)$ is also bounded above.

Lemma 2. *Let J be the ideal such that $I_{f(B)}J = (\|f(B)\|^2)$. Then there exist constants c' and d' not depending on $\boldsymbol{m}$ such that $N(J) \leq c'|d'|^m$.*

Proof. Applying the norm on both sides of $I_{f(B)}J = (\|f(B)\|^2)$ we get

$$N(I_{f(B)})N(J) = N(\|f(B)\|^2).$$

By the definition of the norm, we have $N(I_{f(B)}) \geq 1$, hence $N(J) \leq N(\|f(B)\|^2)$. Consider, the following inequality:

$$\|f(B)\| = \|\sum_{i=1}^{k} A_i B^{m_i}\| \leq \sum_{i=1}^{k} \|A_i\|\|B\|^{m_i}. \tag{2}$$

Since $\|B\| > 1$, the right-hand side of the above equation is at most $|B|^m \sum_{i=1}^{k} \|A_i\|$, which is of the form $c_1|d_1|^m$. Now, we take $\sigma(f(B))$ in Equation 2 for all automorphisms of $\mathbb{K}$ and then multiply them together. In this way, we get an upper bound of the form $c'|d'|^m$ for $N(\|f(B)\|^2)$. This bound also serves as an upper bound for $N(J)$, completing the proof of the lemma. □

Combining Lemma 1 and Lemma 2 with the observation $N(I_{f(B)}) = \frac{N(\|f(B)\|^2)}{N(J)}$, we get the following proposition.

Proposition 1. *There exist non-zero constants c_1 and d_1 depending on $A_1, A_2, \ldots, A_k, B$ and not depending on $\boldsymbol{m} \in \mathbb{N}^k$, such that $N(I_{f(B)}) \geq c_1|d_1|^m$, where m is the maximum component of $\mathbf{m}$.*

We end this section with the following lemma.

Lemma 3. *For a polynomial $f = \sum_{i=1}^{k} A_i x^{m_i} \in M_n(R)[x]$, there exist constants c_3, c_4, c_5 and c_6 not depending on $\mathbf{m}$ such that*

$$N(d(M_n(R), f)) \leq c_3 N(a_1)^{c_4} \exp\left(c_5 m^{\frac{c_6}{\log(\log m)}}\right).$$

Proof. Corresponding to the polynomial $f = \sum_{i=1}^{k} A_i x^{m_i} \in M_n(R)[x]$, we construct a new polynomial $g = \sum_{i=0}^{k} a_i x^{m_i} \in R[x]$, in which each a_i is the $(1,1)^{\text{th}}$ (or some fixed position) entry of the matrix A_i for each $0 \leq i \leq k$. Observe that

$$d(M_n(R), f) \supseteq d(R, f) \supseteq d(R, g).$$

Taking the norm, we obtain the following;

$$N(d(M_n(R), f)) \leq N(d(R, f)) \leq N(d(R, g)).$$

Using the fact that $N(d(R,g)) \leq c_3 N(a_1)^{c_4} \exp\left(c_5 m^{\frac{c_6}{\log(\log m)}}\right)$ (see [14], Proposition 2), where c_3, c_4, c_5 and c_6 are constants not depending on $\mathbf{m}$, we conclude that

$$N(d(M_n(R), f)) \leq c_3 N(a_1)^{c_4} \exp\left(c_5 m^{\frac{c_6}{\log(\log m)}}\right),$$

completing the proof of the lemma. □

3. A Generalization of Selfridge's Question in the Case of the Ring of Matrices

We start this section with our main theorem.

Theorem 5. *Let $f = \sum_{i=1}^{k} A_i x^{m_i} \in M_n(R)[x]$ be a polynomial and $B \in M_n(R)$ be a matrix satisfying A.1, A.2 and A.3 of Question 2. Then there are finitely many tuples in $\mathbb{N}^k$, which are solutions to Question 2.*

Proof. We know that $d(M_n(R), f)$ is the ideal in R generated by all the entries of $f(A)$ for all $A \in M_n(R)$. Also, the condition "the ideal generated by $\sum_{i=1}^{k} A_i B^{m_i}$ contains the ideal generated by $\{\sum_{i=1}^{k} A_i C^{m_i} : C \in M_n(R)\}$" is equivalent to "$I_{f(B)}$ contains the ideal in R generated by all the entries of $f(C)$ for all $C \in M_n(R)$". This is equivalent to saying that $d(M_n(R), f) \subseteq I_{f(B)}$. This implies $N(d(M_n(R), f)) \geq N(I_{f(B)})$. Invoking Proposition 1 and Lemma 3, we sandwich $N(d(M_n(R), f))$ as follows:

$$c_1 |d_1|^m \leq N(d(M_n(R), f)) \leq c_3 N(a_1)^{c_4} \exp\left(c_5 m^{\frac{c_6}{\log(\log m)}}\right).$$

Comparing the lower and upper bounds of $N(d(M_n(R), f))$, it follows that m is bounded above and the statement of the theorem holds. □

We strengthen Theorem 5 in the case when R is a special domain. The following theorem is a generalization of Theorem 2.

Theorem 6. *Let R be the ring of rational integers $\mathbb{Z}$ or the ring of integers in an imaginary quadratic number field and let $A_1, A_2, \dots A_k$ be non-zero elements of $M_n(R)$. Then there are only finitely many elements B in $M_n(R)$ for which there exist k-tuples $(m_1, m_2, \dots, m_k) \in \mathbb{N}^k$, not all zero, satisfying the following simultaneously*

(A.1) the ideal generated by $\sum_{i=1}^{k} A_i B^{m_i}$ contains the ideal generated by $\sum_{i=1}^{k} A_i x^{m_i}$ for all $x \in M_n(R)$;

(A.2) $\sum_{i\in S} A_i B^{m_i} \neq 0$ for all $S \subseteq \{1, 2, \dots, k\}$.

Proof. The numbers $m_1, \dots, m_k$ must be distinct; otherwise, there is a possibility of violation of the second condition of the theorem. Hence, we assume that $m_1 > m_2 > \cdots > m_k$. The value of the Vandermonde matrix

$$\begin{vmatrix} 1 & 2^{m_1} & 2^{2m_1} & \dots & 2^{(k-1)m_1} \\ 1 & 2^{m_2} & 2^{2m_2} & \dots & 2^{(k-1)m_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{m_k} & 2^{2m_k} & \dots & 2^{(k-1)m_k} \end{vmatrix}$$

cannot be zero. Consequently, the matrices

$$f(2^j I) = \sum_{i=1}^{k} A_i (2^j I)^{m_i}, \text{ where } I \text{ is the identity matrix and } 0 \leq j \leq k-1,$$

cannot be the zero matrix for all $0 \leq j \leq k-1$, as this would imply that a combination of the columns of the above Vandermonde matrix is zero. Now we have

$$\|f(2^j I)\| \leq \sum_{i=1}^{k} \|A_i\| n^{\frac{m_i}{2}} 2^{(k-1)m_i} < 2^{(k-1)m_1} n^{\frac{m_1}{2}} \sum_{i=1}^{k} \|A_i\|. \tag{3}$$

If $\|B\| \geq \frac{2\sum_{i=2}^{k} \|A_i\|}{\|A_1\|}$, then we have

$$\|\sum_{i=2}^{k} A_i B^{m_i}\| \leq \sum_{i=2}^{k} \|A_i\| \|B\|^{m_i} \leq \frac{\|A_1\| \|B\|^{m_1}}{2},$$

which implies

$$\frac{\|A_1\| \|B\|^{m_1}}{2} \leq \|f(B)\|. \tag{4}$$

The condition $f(B) \supseteq f(2^j I)$ implies $\|f(B)\| \leq \|f(2^j I)\|$, for the ring under consideration. If $\|B\|$ is large enough, then the lower bound in Equation (4) is greater than the upper bound in Equation (3), which is a contradiction. Since only finitely many elements in $M_n(R)$ can have a given norm; hence our proof is done. □

We end this section with the following question.

Question 3. Can we find the tuples explicitly which are the answer to Question 2?

4. Generalization to Several Variables

We can extend Theorem 5 and Theorem 6 to the multivariate case by induction on the number of variables to get a generalization of Theorem 3 and Theorem 4. Here we state the results formally for the sake of completeness and omit the proofs.

For given tuples $\mathbf{m}, \mathbf{n} \in \mathbb{N}^k$, $\mathbf{m} \leq \mathbf{n}$ means each entry of the tuple $\mathbf{m}$ is less than or equal to the corresponding entry of the tuple $\mathbf{n}$. Also, we denote the tuple $(1, 1, \ldots, 1) \in \mathbb{N}^r$ by $\mathbf{1}$.

Theorem 7. *Let $f(\underline{x}) = \sum_{\mathbf{i}=\mathbf{1}}^{\mathbf{k}} A_{\mathbf{i}} x_1^{m_{1i_1}} x_2^{m_{2i_2}} \cdots x_r^{m_{ri_r}} \in M_n(R)[\underline{x}]$ be a polynomial in r variables and $B_1, B_2, \ldots, B_r$ be matrices satisfying the following:*

(A.1) The ideal generated by B_i is not the whole ring for all $i = 1, 2, \ldots, r$.

(A.2) Either $\rho(B_i^* B_i) > n$ or $\rho((B_i^* B_i)^{-1}) > n$ for all $i = 1, 2, \ldots, r$.

(A.3) $\Sigma_{\mathbf{i} \in S} A_{\mathbf{i}} B_1^{m_{1i_1}} B_2^{m_{2i_2}} \cdots B_r^{m_{ri_r}} \neq 0$, for any non-empty set S of $\{1, 2, \ldots, k_1\} \times \cdots \times \{1, 2, \ldots, k_r\}$,

Then, there are only finitely many tuples $(\mathbf{m}_1, \mathbf{m}_2 \ldots, \mathbf{m}_r) \in \mathbb{N}^{k_1} \times \mathbb{N}^{k_2} \times \ldots \times \mathbb{N}^{k_r}$ where $\mathbf{m}_j = (m_{j1}, m_{j2}, \ldots, m_{jk_j})$ such that the ideal generated by $f(B_1, B_2, \ldots, B_r)$ contains the ideal generated by $\{f(A_1, A_2, \ldots, A_r) \ \forall \ (A_1, A_2, \ldots, A_r) \in M_n(R)^r\}$.

Likewise, we can make an analogue of the Theorem 6 as follows.

Theorem 8. *Let R be the ring of rational integers $\mathbb{Z}$ or the ring of integers in an imaginary quadratic number field and let $\{A_{\mathbf{i}} : \mathbf{0} \leq \mathbf{i} \leq \mathbf{k}\}$ and $\{B_i : 1 \leq i \leq k\}$ be non-zero elements of $M_n(R)$. Then there are only finitely many elements $\{B_i : 1 \leq i \leq k\}$ in $M_n(R)$ for which there exist tuples $(\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_r) \in \mathbb{N}^{k_1} \times \mathbb{N}^{k_2} \times \ldots \times \mathbb{N}^{k_r}$, not all zero, satisfying the following simultaneously*

(A.1) $\Sigma_{\mathbf{i} \in S} A_{\mathbf{i}} B_1^{m_{1i_1}} B_2^{m_{2i_2}} \ldots B_r^{m_{ri_r}} \neq 0$, for any non-empty set S of $\{1, 2, \ldots, k_1\} \times \cdots \times \{1, 2, \ldots, k_r\}$,

(A.2) the ideal generated by $f(B_1, B_2, \ldots, B_r)$ contains the ideal generated by $\{f(A_1, A_2, \ldots, A_r) \ \forall \ (A_1, A_2, \ldots, A_r) \in M_n(R)^r\}$.

Acknowledgments We thank Dr. Krishnan Rajkumar, Dr. A. Satyanarayana Reddy and Saurav Vikash Chatterjee for their valuable suggestions.

References

[1] A. Bose, *Investigations on some exponential congruences*, Master's thesis, University of Lethbridge, Canada, 2016.

[2] G. Choi and A. Zaharescu, A class of exponential congruences in several variables, *J. Korean Math. Soc.* **41** (2004), 717-735.

[3] R. K. Guy, *Unsolved Problems in Number Theory*, Problem Books in Mathematics, Springer-Verlag, New York, second edition, 1994.

[4] D. A. Marcus, *Number Fields*, Springer-Verlag, New York-Heidelberg, Universitext, 1977.

[5] M. R. Murty and V. K. Murty, On a problem of Ruderman, *Amer. Math. Monthly* **118** (2011), 644-650.

[6] D. Prasad, K. Rajkumar, and A. S. Reddy, A survey on fixed divisors, *Confluentes Math.* **11** (2019), 29-52.

[7] K. Rajkumar, A. S. Reddy and D. P. Semwal, Fixed divisor of a multivariate polynomial and generalized factorials in several variables, *J. Korean Math. Soc.* **55** (2018), 1305-1320.

[8] H. Ruderman, D. Gale, C. R. Glassey, G. Tsintsifas, D. Shelupsky, and R. Brooks, Problems and solutions: elementary problems: E2468-E2473, *Amer. Math. Monthly* **81** (1974), 405-406.

[9] H. Ruderman and C. Pomerance, Problems and solutions: solutions of elementary problems: E2468, *Amer. Math. Monthly* **84** (1977), 59-60.

[10] H. Ruderman and W. Y. Velez. Problems and solutions: solutions of elementary problems: E2468, *Amer. Math. Monthly* **83** (1976), 288–289.

[11] R. J. Rundle, *Generalization of Ruderman's Problem to Imaginary Quadratic Fields*, PhD thesis, Queen's University, Canada, 2012.

[12] A. Schinzel, On primitive prime factors of $a^n - b^n$, *Proc. Cambridge Philos. Soc.* **58** (1962), 555-562.

[13] Q. Sun and M. Z. Zhang, Pairs where $2^a - 2^b$ divides $n^a - n^b$ for all n, *Proc. Amer. Math. Soc.* **93** (1985), 218-220.

[14] M. Vâjâitu and A. Zaharescu, A finiteness theorem for a class of exponential congruences, *Proc. Amer. Math. Soc.* **127** (1999), 2225-2232.