Hang Lung Mathematics Awards
Vol. 9 (2021), pp. 3–28 © 2021 HLP, HKUST

ON NON-TORSION SOLUTIONS OF HOMOGENEOUS LINEAR SYSTEMS OVER RINGS

A RESEARCH REPORT SUBMITTED TO THE SCIENTIFIC COMMITTEE OF THE HANG LUNG MATHEMATICS AWARDS

TEAM MEMBER
CHAN TSZ HIN

TEACHER
MR. LEE HO FUNG

SCHOOL
PUI CHING MIDDLE SCHOOL

AUGUST 2021

Abstract. In this paper, we study the existence of non-torsion solutions of a homogeneous linear system over a commutative ring. More precisely, we determine the minimal positive integer n such that any homogeneous systems of m equations with n variables over a given ring R gives a non-torsion solution, i.e. a solution $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ such that at least one coordinate x_i is not a zero-divisor. We proved that over Noetherian rings, a non-trivial lower bound to the minimal number can be guaranteed via the use of primary decomposition. We also consider the number of generators of ideals in R and the localisations of R. For some classes of Noetherian rings, such as principal ideal rings and reduced rings, we show that such minimal number exists.

Contents

1. Introduction

The study of homogeneous systems of linear equations has long been established for its rich applications. A standard problem is to consider how many variables are needed to guarantee that any homogeneous system of m equations gives a non-trivial solution. For instance, consider the case that the system is viewed over a field, i.e. the coefficients and the variables all belong to a given field K. By linear algebra, any homogeneous system of m linear equations has non-trivial solutions if the number of variables is greater than m.

Now, instead of considering linear systems over fields, we would investigate on homogeneous systems of linear equations over a commutative ring R, or more generally an R-module M (readers might refer to Section 2 for definitions needed in this paper). Consider a homogeneous system of linear equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= 0 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots \qquad\quad \vdots& \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0 \end{aligned}$$

with coefficients $a_{ij} \in R$ and variables $x_j \in M$. Equivalently, the above system can be written as the matrix form

$$L\mathbf{x} = \mathbf{0},$$

where $L = (a_{ij})$ is the matrix representing the system, and $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ is the vector representing the solution. One would naturally wonder under a fixed m, when an arbitrary system guarantees a non-trivial solution, i.e. $\mathbf{x} \neq \mathbf{0}$.

In Section 1.1, we provide an answer to the above question. Indeed, following [1], it turns out that the requirement for systems over commutative rings is the same as fields. That is, any homogeneous system of m linear equations over a commutative ring has non-trivial solutions if the number of variables is greater than m.

Related problems also appeared in Mathematical Olympiads. In particular, a problem in the 36th China Mathematical Olympiad concerns on a system of two linear equations modulo k. It asks the minimum number of variables needed to guarantee not only a non-trivial solution, but also a solution $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ that contains a coordinate x_i which is coprime to k. This new condition is equivalent to $x_i + k\mathbb{Z}$ not being a zero-divisor in $\mathbb{Z}/k\mathbb{Z}$. This would be covered in Section 1.2 briefly as it gives a simple example to guide our paths.

Upon further investigation, the additional requirement appears to be a more general notion from abstract algebra − the solution must contain a coordinate which is not a zero-divisor (torsion element) on a ring (resp. module). This is referred in this paper as a **non-torsion solution**. We would then focus on the minimum number of variables needed such that any homogeneous system of m equations guarantees a non-torsion solution. This is the main problem of the paper, and is elaborated in a more detailed manner in Section 1.3.

We would focus on the case that the system is viewed over a ring. As it is intuitively difficult to find the minimum number of variables, we divide the problem into two parts. In Section 3, we tried to construct a system with n variables such that only torsion solutions exist. This shows that the minimum number of variables must be greater than n. In Section 4, we showed that for certain numbers of variables, any homogeneous system would guarantee a non-torsion solution. This gives an upper bound to the minimum number of variables.

In Section 5, we propose possible directions for further investigation. We also discuss the problem over modules.

1.1. **Non-trivial solutions over commutative rings.** Before seeking non-torsion solutions, we would focus on non-trivial solutions first. The following section completely answers when a homogeneous system over a commutative ring R provides non-trivial solutions. The following content is based on [1].

We quote a well-known result on commutative rings.

Proposition 1.1. *Let $R \neq 0$ be a commutative ring and $f : R^n \to R^m$ be a module homomorphism.*

- *If f is injective, then $n \leq m$.*
- *If f is surjective, then $n \geq m$.*

The existence of non-trivial solutions in commutative rings turns out to be similar to fields, as given by the following theorem.

Theorem 1.2. *Let $R \neq 0$ be a commutative ring and $n > m$ be positive integers. Then any homogeneous system of m linear equations with n variables over R has a nontrivial solution.*

Proof. Let L be the matrix representation of the system. Define the module homomorphism $f : R^n \to R^m$ by $\mathbf{x} \mapsto L\mathbf{x}$. By Proposition 1.1, f is not injective because $n > m$. Thus we can pick non-zero $\mathbf{x}_0 \in \ker f$, i.e. there is a non-trivial solution $\mathbf{x}_0$ to the system. □

From now on, we assume **all rings to be commutative, non-zero and with unity**. This would guarantee the existence of non-trivial solutions for any homogeneous system of linear equations with more variables than the number of equations.

1.2. **A problem from CMO.** We then move on to seeking non-torsion solutions. From the 36th China Mathematical Olympiad (CMO) 2021, problem 2 particularly sparks our interest. It states,

Question 1.3 (CMO 2021/2)**.** *Let $k > 1$ be an integer. Find the smallest positive integer n such that for any integers $a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n$, there exists integers $x_1, x_2, \ldots, x_n$ satisfying the following two conditions:*

(i) There exists $i \in \{1, 2, \ldots, n\}$ such that x_i and k are coprime.

(ii) $\displaystyle\sum_{i=1}^{n} a_i x_i \equiv \sum_{i=1}^{n} b_i x_i \equiv 0 \pmod{k}$.

Notice that (ii) means that $(x_1, x_2, \ldots, x_n)$ is a solution to a homogeneous system of two linear equations modulo k. Intuitively, Question 1.3 asks the least number of variables needed so that any homogeneous system guarantees a solution $\mathbf{x}$ such that $\gcd(x_i, k) = 1$ for some index i.

A solution to Question 1.3 can be found in [9], which is included in Appendix A. The solution firstly considers breaking k into its prime factorisation $k = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{\omega(k)}^{\alpha_{\omega(k)}}$ where $\omega(k)$ is the number of distinct prime factors of k. The rest of the proof then relies on the main claim that considering the problem modulo p^α is equivalent to considering it in modulo p. The author proves the claim by listing out cases based on the rank of the matrix representing the system after modulo p. Finally, he uses rank-nullity theorem and combines the results of individual primes using the Chinese Remainder Theorem. The answer to the problem is shown to be $\boxed{2\omega(k) + 1}$.

1.3. **The main problem.** If we view Question 1.3 as a starting point, then the problem itself can be generalised in diverse aspects. It is natural to consider a system of m equations instead of two. In addition, since modules completely inherits the notion of scalar multiplications, we would expect a similar problem in the language of modules.

Definition 1.4. *Let R be a non-zero, commutative ring with unity, M be an R-module and L be the matrix representation of a system of m equations with n variables. A solution $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ with $x_i \in M$ to the system is said to be **non-torsion** if there exists $1 \leq i \leq n$ such that for all $r \in R$, $rx_i = 0$ implies $r = 0$.*

*A solution $\mathbf{x}$ is said to be **torsion** if it is not non-torsion.*

Remark 1.5. *The term "torsion" comes from the notion of torsion elements in a module.*

Definition 1.6. *Let R be a ring, M be an R-module and m be a positive integer. Define a positive integer n to be a **non-torsion number** if any homogeneous system of m equations with n variables guarantees a non-torsion solution. The set of non-torsion numbers is denoted by* $\mathrm{NonTor}_R(M, m)$.

If the base ring R is of no ambiguity, we might omit the subscript and denote the set by $\mathrm{NonTor}(M, m)$.

We can now rigorously state the main problem of the paper.

Question 1.7. *Let R be a ring, M be an R-module and m a positive integer. Find* $\mathrm{NonTor}_R(M, m)$.

As illustrated below, the special case $M = R$ already has fruitful mathematical insights. Thus our major focus is on the special case $M = R$. We are confident that some similar results might be carried over to modules, and is briefly covered in Section 5.2.

Finally, notice that $\mathrm{NonTor}_R(M, m) \neq \mathbb{N}$ since clearly $1 \notin \mathrm{NonTor}_R(M, m)$. This can be seen by choosing a system where all coefficients are 1. The only solution to this system is the trivial solution $(0, 0, \ldots, 0)$, which is torsion.

The following proposition characterises how elements in $\mathrm{NonTor}_R(M, m)$ behave.

Proposition 1.8. *If $n_0 \in \mathrm{NonTor}(M, m)$, then $n \in \mathrm{NonTor}(M, m)$ for any positive integer $n \geq n_0$.*

Proof. Let L be a matrix representation of a system of m equations with n variables. We take the truncated matrix of size $m \times n_0$ formed by the first n_0 columns. This gives a non-torsion solution $\mathbf{x}' = (x_1, \ldots, x_{n_0})$ of this system by assumption, and by taking $\mathbf{x} = (x_1, \ldots, x_{n_0}, 0, \ldots, 0)$ with $n - n_0$ zeroes we obtain a non-torsion solution. □

Thus if $\mathrm{NonTor}(M, m) \neq \emptyset$, it must take the form

$$\mathrm{NonTor}(M, m) = \{n \in \mathbb{N} : n \geq n_0\}$$

where n_0 is a positive integer. In this case, n_0 is defined to be the **minimal non-torsion number**.

In particular, the original CMO problem is equivalent to determining the set $\mathrm{NonTor}_{\mathbb{Z}/k\mathbb{Z}}(\mathbb{Z}/k\mathbb{Z}, 2)$, which is

$$\{n \in \mathbb{N} : n \geq 2\omega(k) + 1\}$$

Remark 1.9. *It is worth mentioning that the minimal element need not exist. Indeed, consider $\mathbb{Z}/k\mathbb{Z}$ as a $\mathbb{Z}$-module. Then all elements in the module is annihilated by k, and thus all solutions must be torsion, i.e.*

$$\mathrm{NonTor}_{\mathbb{Z}}(\mathbb{Z}/k\mathbb{Z}, m) = \emptyset \text{ for all positive integers } m.$$

A simple result can be obtained as a starting point of the investigation by applying Theorem 1.2.

Proposition 1.10. *If R is an integral domain, $\mathrm{NonTor}_R(R, m) = \{n \in \mathbb{N} : n \geq m + 1\}$.*

Proof. There are no non-zero zero-divisors in R, thus all non-trivial solutions are non-torsion. □

1.3.1. *Failure of extension of the original proof.* One might expect that the solution from [9] for Question 1.3 can be extended easily to the case of modules. This is unfortunately not true, based on two reasons.

- The proof uses many special properties of the ring $\mathbb{Z}$. In particular, all elements in $\mathbb{Z}$ have a unique prime factorisation. This also forbids the use of rank-nullity theorem, since we cannot decompose a module into fields or even integral domains.
- Generalising to m equations, the main claim of the solution requires splitting into $m + 1$ cases, which is intuitively difficult and not systematic.

Hence, we need more advanced algebra tools to tackle the problem. The next section would be devoted to some preliminaries of commutative algebra.

2. Notations and Preliminaries

Throughout this paper, a field is denoted by K. Inclusion of sets is denoted by the sign $\subseteq$. We reserve the sign $\subset$ for strict inclusion, i.e. $A \subset B$ means that A is contained in B and is not equal to B.

We will now go through ring and module preliminaries. This is solely for the paper to be self-contained, so the definitions and results below are not in any way exhaustive and complete. Readers may skip this section unless needed and are advised to refer to [2] for a more detailed discussion in commutative algebra.

Definition 2.1. *A **ring** R is a set with two binary operations (addition $+$ and multiplication $\cdot$) such that*

(i) $(R, +)$ is an abelian group.

(ii) Multiplication is associative and distributive over addition.

We only consider rings which are commutative:

(iii) $xy = yx$ for all $x, y \in R$,

and have an identity element, denoted by 1, which is different from 0:

(iv) $x \cdot 1 = 1 \cdot x = x$ for all $x \in R$.

*An **ideal** $\mathfrak{a}$ of a ring R is an additive subgroup of R such that $ra \in \mathfrak{a}$ for all $r \in R$ and $a \in \mathfrak{a}$.*

*The elements of the **quotient ring** $R/\mathfrak{a}$ are the cosets of $\mathfrak{a}$ in R, which has a natural ring structure.*

Some classes of elements of a ring are defined below.

Definition 2.2. *An element $x \in R$ is a **zero-divisor** if there exists $y \neq 0$ in R such that $xy = 0$. A ring with no non-zero zero-divisors is called an **integral domain**.*

*An element $x \in R$ is **nilpotent** if $x^n = 0$ for some positive integer n. The set of all nilpotent elements is denoted by $\mathfrak{N}_R$, the **nilradical** of R.*

For example, $\mathbb{Z}$ and $K[x_1, \ldots, x_n]$ are integral domains. Some classes of ideals are also defined.

Definition 2.3. *An ideal is **principal** if it is generated by a single element $x \in R$, denoted by (x).*

*An ideal $\mathfrak{p} \neq (1)$ is **prime** if $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.*

*An ideal $\mathfrak{m} \neq (1)$ is **maximal** if there is no ideal $\mathfrak{a}$ such that $\mathfrak{m} \subset \mathfrak{a} \subset (1)$ (strict inclusions).*

Equivalently:

$$\mathfrak{p} \text{ is prime } \Leftrightarrow \ R/\mathfrak{p} \text{ is an integral domain;}$$

$$\mathfrak{m} \text{ is maximal } \Leftrightarrow \ R/\mathfrak{m} \text{ is a field.}$$

Hence a maximal ideal is prime but not conversely, in general. The following proposition is frequently used in this paper.

Lemma 2.4. *(**Prime avoidance lemma**)*

(i) Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

(ii) Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal containing $\bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i.

Definition 2.5. *Let $\mathfrak{a}$ be an ideal of a ring R.*

- *The **annihilator** of $\mathfrak{a}$, denoted by $Ann(\mathfrak{a})$, is the set of all elements $x \in R$ such that $xa = 0$ for all $a \in \mathfrak{a}$.*
- *The **radical** of $\mathfrak{a}$, denoted by $r(\mathfrak{a})$, is the set of all elements $x \in R$ such that $x^n \in \mathfrak{a}$ for some $n > 0$.*

Proposition 2.6. *Let R be a ring and $\mathfrak{a}, \mathfrak{b}$ be ideals in R. Then*

(i) if $\mathfrak{a} \subseteq \mathfrak{b}$, then $r(\mathfrak{a}) \subseteq r(\mathfrak{b})$.

(ii) if $\mathfrak{p}$ is a prime ideal, then $r(\mathfrak{p}) = \mathfrak{p}$.

(iii) $r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.

We now introduce concepts related to modules.

Definition 2.7. *Let R be a ring. An R-**module** is an abelian group $(M, +)$ on which "scalar multiplications" from R acts linearly, i.e. for all $r, s \in R$ and $x, y \in M$,*

$$\begin{aligned} r(x+y) &= rx + ry, \\ (r+s)x &= rx + sx, \\ (rs)x &= r(sx), \\ 1x &= x. \end{aligned}$$

*Let M, N be R-modules. A mapping $f : M \to N$ is an R-**module homomorphism** if*

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(rx) &= r \cdot f(x) \end{aligned}$$

for all $r \in R$ and $x, y \in M$. The set of all R-module homomorphisms is denoted $Hom_R(M, N)$, or $Hom(M, N)$ if there is no ambiguity about the ring R.

*A **submodule** M' of M is a subgroup of M which is closed under multiplication by elements of R. The elements of the quotient M/M' are the cosets of M' in M, which has a natural R-module structure.*

For example, R^n is an R-module. In particular R itself is an R-module with ideals as its submodules. On the other hand, if R is a field, then all R-modules are R-vector spaces.

Definition 2.8. *Let R be a ring and M be an R-module. M is said to be generated by $x_1, x_2, \ldots, x_n \in M$ if all elements m of M can be written as a linear combination $m = \sum_{i=1}^n r_i x_i$ where $r_i \in R$. In this case, the elements $x_1, x_2, \ldots, x_n$ are said to be the **generators** of M and we write $M = Rx_1 + Rx_2 + \cdots + Rx_n$. If M has a finite set of generators, then M is said to be **finitely generated**.*

We now state an important concept in our paper.

Definition 2.9. *An R-module M is said to be* ***Noetherian*** *if it satisfies one of the following equivalent conditions:*

(i) Every increasing sequence of submodules $M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ is stationary, i.e. there exists positive integer n such that $M_n = M_{n+1} = \cdots$.
(ii) Every submodule of M is finitely generated.

In particular, a ring R is said to be Noetherian if every increasing sequence of ideals is stationary, or equivalently if every ideal of R is finitely generated.

There is one major fact that requires special attention.

Proposition 2.10. *Let R be a Noetherian ring. If M is a finitely generated R-module, then M is Noetherian.*

This concludes the required commutative algebra preliminaries.

3. Elements not in $\mathrm{NonTor}(R, m)$

The main goal is to identify elements which are in and out of $\mathrm{NonTor}_R(R, m)$. Obviously, this task can be divided into two parts: identifying elements not in $\mathrm{NonTor}_R(R, m)$ and elements in $\mathrm{NonTor}_R(R, m)$. In this section, we focus on the former sub-task.

Question 3.1 (Objective of this section)**.** *Let R be a ring and m be a positive integer. Find elements which are not in* $\mathrm{NonTor}(R, m)$.

In other words, we would try to construct a system of m equations with n variables which gives only torsion solutions, so that $n \notin \mathrm{NonTor}(R, m)$.

Our intuition comes from the solution [9] of the CMO problem.

Example 3.2. *Let $R = \mathbb{Z}/k\mathbb{Z}$ and $m = 2$. Write $k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{\omega(k)}^{\alpha_{\omega(k)}}$ and consider the system represented by*

$$L = \begin{pmatrix} \prod_{i\neq 1} p_i & 0 & \prod_{i\neq 2} p_i & 0 & \cdots & \prod_{i\neq \omega(k)} p_i & 0 \\ 0 & \prod_{i\neq 1} p_i & 0 & \prod_{i\neq 2} p_i & \cdots & 0 & \prod_{i\neq \omega(k)} p_i \end{pmatrix}.$$

Suppose $\mathbf{x} = (x_1, x_2, \ldots, x_{2\omega(k)})$ is a solution. Note that p_i must divide x_{2i-1} and x_{2i}. Thus all solutions are torsion and $2\omega(k) \notin \mathrm{NonTor}(\mathbb{Z}/k\mathbb{Z}, 2)$.

For a general ring R, we would expect the choice of L to have a similar form. This motivates the following proposition, which gives a sufficient condition of an element not belonging to $\mathrm{NonTor}(R, m)$.

Proposition 3.3. *Let R be a ring and m be an integer. Suppose there exist n elements $d_1, d_2, \ldots, d_n \in R$ satisfying*

(i) $\displaystyle\prod_{i=1}^{n} d_i = 0$,
(ii) $\displaystyle\prod_{i\neq j} d_i^2 \neq 0$ *for all* $1 \leq j \leq n$.

Then $mn \notin \mathrm{NonTor}(R, m)$.

Proof. The idea is to construct a system of m equations with mn variables, represented by the matrix L such that all solutions are torsion. We claim that

$$L = \begin{pmatrix} \prod_{k\neq 1} d_k & 0 & \cdots & 0 & \cdots & \prod_{k\neq n} d_k & 0 & \cdots & 0 \\ 0 & \prod_{k\neq 1} d_k & \cdots & 0 & & 0 & \prod_{k\neq n} d_k & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \prod_{k\neq 1} d_k & \cdots & 0 & 0 & \cdots & \prod_{k\neq n} d_k \end{pmatrix}$$

is such a choice. Suppose $\mathbf{x} = (x_1, x_2, \ldots, x_{mn})^T$ is a solution to $L\mathbf{x} = \mathbf{0}$. Then for each $1 \leq i \leq m$, we have

$$\Big(\prod_{k\neq 1} d_k\Big)x_i + \Big(\prod_{k\neq 2} d_k\Big)x_{m+i} + \cdots + \Big(\prod_{k\neq n} d_k\Big)x_{m(n-1)+i} = 0. \tag{1}$$

Fix $1 \leq j \leq n$. Note that all but the j-th term in the sum above belongs to the principal ideal (d_j). By making the j-th term as subject in (1), we see that the j-th term also belongs to (d_j), i.e.

$$\Big(\prod_{k\neq j} d_k\Big)x_{m(j-1)+i} = d_j \cdot y$$

for some $y \in R$. Multiplying $\prod_{k\neq j} d_k$ to both sides, we have

$$\Big(\prod_{k\neq j} d_k\Big)^2 x_{m(j-1)+i} = \Big(\prod_{k=1}^{n} d_k\Big) \cdot y = 0.$$

Hence $x_{m(j-1)+i}$ is a zero-divisor. Since i, j are arbitrary, $x_1, x_2, \ldots, x_{mn}$ are zero-divisors. Thus $\mathbf{x}$ is torsion. □

Let us demonstrate how to utilise Proposition 3.3. The following two examples showcase the fact that some rings might have no non-torsion numbers.

Example 3.4 (Rings with no non-torsion number)**.** *We provide two examples where* $\mathrm{NonTor}(R, m) = \emptyset$*:*

- *Let* $R = \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \cdots$*. For any positive integer* k*, we define*

$$d_i = (1, \ldots, 1, 0, 1, \ldots, 1, 0, 0, \ldots) \text{ for } 1 \leq i \leq k.$$

  Here, the first k *coordinates are* 1*'s except the* i*-th position, which is zero. All the other coordinates are zeroes. This produces* k *elements that clearly satisfy the two conditions in Proposition 3.3. Thus* $mk \notin \mathrm{NonTor}(R, m)$ *for all* k*. Together with Proposition 1.8,* $\mathrm{NonTor}(R, m) = \emptyset$*.*
- *Let* $R = K[x_1, x_2, \ldots]/(x_1, x_2x_3, x_4x_5x_6x_7, \ldots)$*. Then for each positive integer* k*, we define*

$$d_i = x_{2^k+(i-1)} \text{ for } 1 \leq i \leq 2^k.$$

  Using the same argument, $m \cdot 2^k \notin \mathrm{NonTor}(R, m)$ *for all* k*. Thus*

$$\mathrm{NonTor}(R, m) = \emptyset.$$

However, it is difficult to find suitable d_i's satisfying the conditions in Proposition 3.3 for a general ring R. Indeed, putting $d_i = p_i$ as in Example 3.2, their product is not zero and hence Proposition 3.3 cannot be applied. To resolve this issue, we should choose $d_i = p_i^{\alpha_i}$.

Example 3.5. *Let $R = \mathbb{Z}/k\mathbb{Z}$, $m = 2$ and write $k = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{\omega(k)}^{\alpha_{\omega(k)}}$. Define $d_i = p_i^{\alpha_i}$ for $1 \leq i \leq \omega(k)$. We claim that the two conditions are satisfied:*

(i) $\displaystyle\prod_{i=1}^{\omega(k)} d_i = \prod_{i=1}^{\omega(k)} p_i^{\alpha_i} = k = 0$ *in $\mathbb{Z}/k\mathbb{Z}$,*

(ii) $\displaystyle\prod_{i\neq j} d_i^2 = \prod_{i\neq j} p_i^{2\alpha_i} \neq 0$ *in $\mathbb{Z}/k\mathbb{Z}$ for all $1 \leq j \leq \omega(k)$, since it is not a multiple of p_j.*

Hence, Proposition 3.3 can be applied to show that $2\omega(k) \notin \mathrm{NonTor}(\mathbb{Z}/k\mathbb{Z}, 2)$.

3.1. **Primary decomposition.** From Example 3.5, we should choose d_i's to be prime powers instead of primes. Surprisingly, this fits perfectly with the notion of **primary ideals** in abstract algebra.

The aim of this section is to provide some definitions and results related to primary ideals.

Definition 3.6. *An ideal $\mathfrak{q} \neq (1)$ in a ring R is **primary** if*

$$xy \in \mathfrak{q} \;\Rightarrow\; x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some positive integer } n.$$

Notice that the radical $r(\mathfrak{q})$ (Definition 2.5) of a primary ideal must be prime. In particular, if p is a prime number, (p^α) is a primary ideal in $\mathbb{Z}/k\mathbb{Z}$ with $r((p^\alpha)) = (p)$, which fits into our motivation. We will now introduce a powerful tool to aid us with choosing suitable elements.

Definition 3.7. *A **minimal primary decomposition** of an ideal $\mathfrak{a}$ in R is an expression of $\mathfrak{a}$ as a finite intersection of primary ideals $\mathfrak{q}_1, \mathfrak{q}_2, \dots, \mathfrak{q}_N$, that is,*

$$\mathfrak{a} = \bigcap_{i=1}^{N} \mathfrak{q}_i,$$

such that the $r(\mathfrak{q}_i)$'s are distinct and $\mathfrak{q}_i \not\supseteq \bigcap_{j\neq i} \mathfrak{q}_j$ for all $1 \leq i \leq N$.

In general, such a primary decomposition need not exist. Yet, this is true if we assume the ring to be Noetherian.

Theorem 3.8. *(Lasker-Noether theorem)*
Every ideal in a Noetherian ring has a minimal primary decomposition.

In particular, (0) has a minimal primary decomposition in a Noetherian ring. This allows us to have further definitions based on a minimal primary decomposition of (0).

Definition 3.9. *Let R be a Noetherian ring. Consider a minimal primary decomposition of $(0) = \bigcap_{i=1}^{N} \mathfrak{q}_i$.*

Define $\mathrm{Ass}(R)$[1] $= \{r(\mathfrak{q}_i) : 1 \le i \le N\}$ *to be the set of* ***associated primes*** *of* R. *An associated prime* $\mathfrak{p} \in \mathrm{Ass}(R)$ *is said to be*

- ***minimal*** *if* $\mathfrak{p}' \in \mathrm{Ass}(R)$ *and* $\mathfrak{p}' \subseteq \mathfrak{p}$ *implies* $\mathfrak{p} = \mathfrak{p}'$.
- ***maximal*** *if* $\mathfrak{p}' \in \mathrm{Ass}(R)$ *and* $\mathfrak{p}' \supseteq \mathfrak{p}$ *implies* $\mathfrak{p} = \mathfrak{p}'$.
- ***embedded*** *if it is not minimal.*

Denote $\mathrm{Ass}^\flat(R)$ *and* $\mathrm{Ass}^\sharp(R)$ *to be the set of minimal and maximal associated primes respectively.*

Remark 3.10. *The associated primes are independent of the minimal primary decompositions. Thus it makes sense to define the associated primes of* R. *Also, we would keep away from using the term maximal to avoid confusion with the notation of maximal ideals.*

Example 3.11.

(i) Let $R = \mathbb{Z}/k\mathbb{Z}$. *Take the minimal primary decomposition*

$$(0) = (p_1^{\alpha_1}) \cap (p_2^{\alpha_2}) \cap \ldots \cap (p_{\omega(k)}^{\alpha_{\omega(k)}}),$$

with $\mathrm{Ass}(R) = \{(p_1), (p_2), \ldots, (p_{\omega(k)})\}$ *by taking radicals. As all of the* (p_i)*'s are maximal ideals, there are no embedded associated primes. Hence,* $\mathrm{Ass}^\flat(R) = \mathrm{Ass}^\sharp(R) = \mathrm{Ass}(R)$.

(ii) Let $R = K[x, y]/(x^2y, xy^2)$. *Take the minimal primary decomposition*

$$(0) = (x) \cap (y) \cap (x^2, y^2),$$

with $\mathrm{Ass}(R) = \{(x), (y), (x, y)\}$. *Since* $(x) \subset (x, y)$ *and* $(y) \subset (x, y)$, $\mathrm{Ass}^\flat(R) = \{(x), (y)\}$ *(thus* (x, y) *is embedded) and* $\mathrm{Ass}^\sharp(R) = \{(x, y)\}$.

3.2. **Application of primary decomposition to the problem.** Recall from Proposition 3.3 that we want to choose elements $d_1, d_2, \ldots, d_n$ satisfying

(i) $\prod_{i=1}^{n} d_i = 0$,

(ii) $\prod_{i \ne j} d_i^2 \ne 0$ for all $1 \le j \le n$.

Example 3.5 suggests that d_i should be chosen from primary ideals. In this example, the minimal primary decomposition of (0) is given by

$$(0) = \bigcap_{i=1}^{\omega(k)} \mathfrak{q}_i,$$

with $\mathfrak{q}_i = (p_i^{\alpha_i})$ and $\mathfrak{p}_i = r(\mathfrak{q}_i) = (p_i)$ for $1 \le i \le \omega(k)$.

To ensure that (i) is satisfied, each d_i should be chosen from $\mathfrak{q}_i$ so that their product belongs to the intersection of the $\mathfrak{q}_i$'s, which is (0). On the other hand, each d_i should not belong to $\bigcup_{j \ne i} \mathfrak{p}_j$, ensuring that (ii) is satisfied. For if $\prod_{i \ne j} d_i^2 = 0 \in \mathfrak{p}_j$, then $d_i \in \mathfrak{p}_j$ for some $i \ne j$ by the definition of prime ideal. This contradicts to the choice of d_i. Intuitively, it suggests that each d_i should be chosen from $\mathfrak{q}_i \setminus \bigcup_{j \ne i} \mathfrak{p}_j$ for general rings.

[1]Although this is somewhat "regrettable" [7, p.3], but yes, this is the standard notation.

Tragically, the example below illustrates that $\mathfrak{q}_i \setminus \bigcup_{j\neq i} \mathfrak{p}_j$ may be empty in some cases.

Example 3.12. *Consider $R = K[x,y]/(x^2y, xy^2)$ and the minimal primary decomposition of (0) as in Example 3.11(ii). Denote $\mathfrak{q}_1 = (x)$, $\mathfrak{q}_2 = (y)$ and $\mathfrak{q}_3 = (x^2, y^2)$ as the primary ideals and $\mathfrak{p}_1 = (x)$, $\mathfrak{p}_2 = (y)$ and $\mathfrak{p}_3 = (x,y)$ as the associated primes.*

Then $\mathfrak{q}_1 \setminus (\mathfrak{p}_2 \cup \mathfrak{p}_3) = \emptyset$ because $\mathfrak{q}_1 \subseteq \mathfrak{p}_3$.

It turns out that the set $\mathfrak{q}_i \setminus \bigcup_{j\neq i} \mathfrak{p}_j$ is empty precisely when embedded primes are present. Luckily, we can still pick $d_1 = x^2$ and $d_2 = y^2$ that satisfy the conditions. This accounts to the fact that $d_1 \in \mathfrak{q}_1 \cap \mathfrak{q}_3 \setminus \mathfrak{p}_2$ and $d_2 \in \mathfrak{q}_2 \cap \mathfrak{q}_3 \setminus \mathfrak{p}_1$. Thus the product $d_1 d_2 \in \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \mathfrak{q}_3 = (0)$ and the squares $d_1^2 \notin \mathfrak{p}_2$ and $d_2^2 \notin \mathfrak{p}_1$.

Taking this into consideration, we have a more refined strategy to choose suitable d_i's in Noetherian rings.

Theorem 3.13. *Let R be a Noetherian ring. Then $m|\operatorname{Ass}^\flat(R)| \notin \operatorname{NonTor}(R,m)$.*

Proof. Fix a minimal primary decomposition $(0) = \bigcap_{k=1}^N \mathfrak{q}_k$. Write $\operatorname{Ass}^\flat(R) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ where the $\mathfrak{p}_i$'s are distinct. For each $1 \leq i \leq n$, define $I_i = \{1 \leq k \leq N : \mathfrak{p}_i \subseteq r(\mathfrak{q}_k)\}$. We claim that we can choose

$$d_i \in \bigcap_{k\in I_i} \mathfrak{q}_k \setminus \bigcup_{j\neq i} \mathfrak{p}_j$$

by showing that the set is non-empty.

Suppose on a contrary that $\bigcap_{k\in I_i} \mathfrak{q}_k \subseteq \bigcup_{j\neq i} \mathfrak{p}_j$. Apply prime avoidance lemma (Proposition 2.4(i)) once, we have $\bigcap_{k\in I_i} \mathfrak{q}_k \subseteq \mathfrak{p}_j$ for some $j \neq i$. Apply prime avoidance lemma (Proposition 2.4(ii)) again, we have $\mathfrak{q}_k \subseteq \mathfrak{p}_j$ for some $k \in I_i$, and thus $r(\mathfrak{q}_k) \subseteq r(\mathfrak{p}_j) = \mathfrak{p}_j$ by Proposition 2.6. Since $k \in I_i$, $\mathfrak{p}_i \subseteq r(\mathfrak{q}_k)$, and hence $\mathfrak{p}_i \subseteq \mathfrak{p}_j$. Minimality of $\mathfrak{p}_j$ gives $\mathfrak{p}_i = \mathfrak{p}_j$ but they have to be distinct. Contradiction arises and the claim follows.

It remains to check that conditions (i) and (ii) in Proposition 3.3 are satisfied by the choice of such d_i's.

For (i), we show that $\prod d_i \in \mathfrak{q}_k$ for all $1 \leq k \leq N$. Note that the associated prime $r(\mathfrak{q}_k)$ must contain some minimal associated prime, so $r(\mathfrak{q}_k) \supseteq \mathfrak{p}_i$ for some $1 \leq i \leq n$. In particular, $k \in I_i$ and hence

$$d_i \in \bigcap_{j\in I_i} \mathfrak{q}_j \subseteq \mathfrak{q}_k.$$

For (ii), suppose on a contrary that $\prod_{i\neq j} d_i^2 = 0 \in \mathfrak{p}_j$ for some $1 \leq j \leq n$. By the definition of prime ideals we have $d_i \in \mathfrak{p}_j$ for some $i \neq j$, which contradicts to the choice of d_i.

Hence $mn \notin \operatorname{NonTor}(R,m)$ by Proposition 3.3. □

This implies that for a large class of rings we might find elements out of $\operatorname{NonTor}(R,m)$. More precisely, if we know the number of minimal associated primes of a ring, we immediately obtain a lower bound of the minimal non-torsion number. We illustrate the application of Theorem 3.13 with the following two examples.

Example 3.14. *Consider the same rings as in Example 3.11.*

(i) If $R = \mathbb{Z}/k\mathbb{Z}$*, then* $|\operatorname{Ass}^\flat(R)| = \omega(k)$*. Thus* $m\omega(k) \notin \operatorname{NonTor}(R, m)$ *for all positive integers* m*.*

(ii) If $R = K[x, y]/(x^2y, xy^2)$*, then* $|\operatorname{Ass}^\flat(R)| = 2$*. Thus* $2m \notin \operatorname{NonTor}(R, m)$ *for all positive integers* m*.*

4. Elements in $\operatorname{NonTor}(R, m)$

The results in Section 3 is not enough to identify all numbers which are in $\operatorname{NonTor}(R, m)$; they only implies that some numbers are not in the set. In this section, we try to find elements that belong to $\operatorname{NonTor}(R, m)$. However, as we will see in the following section, showing the non-emptiness of $\operatorname{NonTor}(R, m)$ is already a very difficult task. Let us restate the problem with the focus in this section:

Question 4.1 (Objective of this section)**.** *Let* R *be a ring and* m *be a positive integer. Find elements which are in* $\operatorname{NonTor}(R, m)$*.*

In other words, we need to show that every homogeneous system of m equations with n variables guarantees a non-torsion solution $\mathbf{x} = (x_1, \ldots, x_n)$ so that $n \in \operatorname{NonTor}(R, m)$. Notice that a solution $\mathbf{x}$ is non-torsion if and only if x_i is not a zero-divisor of R for some $1 \leq i \leq n$.

As mentioned in Section 1.3.1, the solution from [9] of the CMO problem cannot be easily generalised. We cannot obtain any intuition from the solution. Consequently, alternative approaches applicable to general rings are developed in the following subsections.

4.1. Reducing the problem.

In this subsection, a sufficient condition for $n \in \operatorname{NonTor}(R, m)$ is given. To achieve this, we deduce equivalent formulations of the problem. Observe that homogeneous systems of m equations with n variables have a one-to-one correspondence to R-module homomorphisms from R^n to R^m. This gives the following result.

Proposition 4.2. *Let* R *be a ring with* D *as the set of zero-divisors and* m, n *be positive integers. Then* $n \in \operatorname{NonTor}(R, m)$ *if and only if* $\ker \phi \not\subseteq D^n$ *for all* $\phi \in Hom_R(R^n, R^m)$*.*

Proof. ($\Rightarrow$) Let $\phi \in \operatorname{Hom}(R^n, R^m)$ be given. For $1 \leq i \leq n$, let

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in R^n$$

with 1 at the i-th position. Consider the system of m equations with n variables represented by

$$L = \begin{pmatrix} | & | & & | \\ \phi(e_1) & \phi(e_2) & \cdots & \phi(e_n) \\ | & | & & | \end{pmatrix}.$$

Since $n \in \operatorname{NonTor}(R, m)$, there is a non-torsion solution $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Notice that $\mathbf{x} \in \ker \phi$ because

$$\mathbf{0} = L\mathbf{x} = \sum_{i=1}^{n} x_i \phi(e_i) = \phi\left(\sum_{i=1}^{n} x_i e_i\right) = \phi(\mathbf{x}).$$

Yet $\mathbf{x} \notin D^n$ as $x_i \notin D$ for some $1 \leq i \leq n$.

($\Leftarrow$) Let L be the matrix representing a system of m equations with n variables. Consider the module homomorphism $\phi \in \mathrm{Hom}(R^n, R^m)$ defined by $\mathbf{x} \mapsto L\mathbf{x}$. By assumption, there is an element in $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \ker\phi$ which is not in D^n, i.e. there is a coordinate $x_i \notin D$. This implies $\mathbf{x}$ is non-torsion. □

The set of zero-divisors D may not be an ideal. Its lack of structure forbids us to discuss whether the solution set is a subset of D^n. However, in light of the use of primary decomposition in the previous section, we recall a result from commutative algebra:

Proposition 4.3. *Let R be a Noetherian ring with D as the set of zero-divisors. Then*

$$D = \bigcup_{\mathfrak{p} \in \mathrm{Ass}^\sharp(R)} \mathfrak{p}.$$

We introduce the following notation for simplicity.

Definition 4.4. *Let R be a ring and $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ be ideals in R. Denote*

$$\mathfrak{a}_1 \times \mathfrak{a}_2 \times \cdots \times \mathfrak{a}_n = \{(a_1, a_2, \ldots, a_n) \in R^n : a_i \in \mathfrak{a}_i, 1 \leq i \leq n\}$$

as a submodule of R^n. In particular, $\mathfrak{a} \times \mathfrak{a} \times \cdots \times \mathfrak{a}$ with n $\mathfrak{a}$'s is denoted by $\mathfrak{a}^{(n)}$.

With the aid of Proposition 4.3, the formulation in Proposition 4.2 can be further simplified.

Theorem 4.5. *Let R be a Noetherian ring and m, n be positive integers. Then $n \in \mathrm{NonTor}(R, m)$ if and only if for all $\phi \in Hom(R^n, R^m)$ and $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n \in \mathrm{Ass}^\sharp(R)$, $\ker\phi \not\subseteq \mathfrak{p}_1 \times \mathfrak{p}_2 \times \cdots \times \mathfrak{p}_n$.*

Remark 4.6. *Note that the $\mathfrak{p}_i$'s need not be distinct.*

Proof. Denote D as the set of zero-divisior of R.

($\Rightarrow$) Let $\phi \in \mathrm{Hom}(R^n, R^m)$. By Proposition 4.2, $\ker\phi \not\subseteq D^n$. Proposition 4.3 implies that $\mathfrak{p}_1 \times \mathfrak{p}_2 \times \cdots \times \mathfrak{p}_n \subseteq D^n$. Hence $\ker\phi \not\subseteq \mathfrak{p}_1 \times \mathfrak{p}_2 \times \cdots \times \mathfrak{p}_n$.

($\Leftarrow$) In view of Proposition 4.2, it suffices to show that $\ker\phi \not\subseteq D^n$ for all $\phi \in \mathrm{Hom}(R^n, R^m)$. Suppose on a contrary that $\ker\phi \subseteq D^n$ for some $\phi \in \mathrm{Hom}(R^n, R^m)$.

For each $1 \leq i \leq n$, consider the projection map $\pi_i : R^n \to R$ defined by $(x_1, x_2, \ldots, x_n) \mapsto x_i$. Note that $\pi_i(\ker\phi)$ is an ideal in R. Since $\ker\phi \subseteq D^n$, we have $\pi_i(\ker\phi) \subseteq D$. By Proposition 4.3 and prime avoidance lemma (Proposition 2.4(i)), we have $\pi_i(\ker\phi) \subseteq \mathfrak{p}_i$ for some $\mathfrak{p}_i \in \mathrm{Ass}^\sharp(R)$. Hence

$$\ker\phi \subseteq \pi_1(\ker\phi) \times \pi_2(\ker\phi) \times \cdots \times \pi_n(\ker\phi) \subseteq \mathfrak{p}_1 \times \mathfrak{p}_2 \times \cdots \times \mathfrak{p}_n.$$

This contradicts to the assumption. □

Theorem 4.5 tells us that if $n \notin \mathrm{NonTor}(R, m)$, then there exist a module homomorphism $\phi \in \mathrm{Hom}(R^n, R^m)$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathrm{Ass}^\sharp(R)$ such that $\ker\phi \subseteq \mathfrak{p}_1 \times \cdots \times \mathfrak{p}_n$. We wonder when would such a homomorphism ϕ exists if the $\mathfrak{p}_i$'s are fixed. The following theorem characterises the existence of ϕ by a condition related to submodules of R^m.

Theorem 4.7. *Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ be ideals in a ring R and m be a positive integer. The followings are equivalent:*

(i) There exists $\phi \in Hom(R^n, R^m)$ such that $\ker\phi \subseteq \mathfrak{p}_1 \times \mathfrak{p}_2 \times \cdots \times \mathfrak{p}_n$.
(ii) There exists a surjective module homomorphism from a submodule M of R^m to $(R/\mathfrak{p}_1) \times \cdots \times (R/\mathfrak{p}_n)$.

Proof. ((i) $\Rightarrow$ (ii)) Let M be the image of ϕ. We claim that $\psi : M \to (R/\mathfrak{p}_1) \times \cdots \times (R/\mathfrak{p}_n)$ given by

$$\psi(\phi(x_1, x_2, \ldots, x_n)) = (x_1 + \mathfrak{p}_1, x_2 + \mathfrak{p}_2, \ldots, x_n + \mathfrak{p}_n)$$

is the required surjective module homomorphism. Notice that surjectivity of ψ is immediate. To see that it is well-defined, let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ and $\phi(\mathbf{x}) = \phi(\mathbf{y})$. Then $\mathbf{x} - \mathbf{y} \in \ker\phi \subseteq \mathfrak{p}_1 \times \mathfrak{p}_2 \times \cdots \times \mathfrak{p}_n$. It follows that $x_i - y_i \in \mathfrak{p}_i$ for all $1 \leq i \leq n$.

((ii) $\Rightarrow$ (i)) Let $\psi : M \to (R/\mathfrak{p}_1) \times \cdots \times (R/\mathfrak{p}_n)$ be the surjective homomorphism. For each $1 \leq i \leq n$, surjectivity implies that there exist $m_i \in R^m$ such that $\psi(m_i) = (\mathfrak{p}_1, \ldots, \mathfrak{p}_{i-1}, 1 + \mathfrak{p}_i, \mathfrak{p}_{i+1}, \ldots, \mathfrak{p}_n)$.

Define the module homomorphism $\phi : R^n \to R^m$ by

$$\phi(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} x_i m_i.$$

If $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \ker\phi$, then $\sum x_i m_i = 0$. Taking ψ on both sides,

$$\mathbf{0} = \psi(0) = \psi\left(\sum_{i=1}^{n} x_i m_i\right) = \sum_{i=1}^{n} x_i \psi(m_i) = (x_1 + \mathfrak{p}_1, x_2 + \mathfrak{p}_2, \ldots, x_n + \mathfrak{p}_n).$$

Hence $x_i \in \mathfrak{p}_i$ for all $1 \leq i \leq n$ and so $\mathbf{x} \in \mathfrak{p}_1 \times \mathfrak{p}_2 \times \cdots \times \mathfrak{p}_n$. □

It would be nice if we can consider the associated primes in $\mathrm{Ass}^\sharp(R)$ individually. By letting $\mathfrak{p}_1 = \mathfrak{p}_2 = \cdots = \mathfrak{p}_n = \mathfrak{p}$ in Theorem 4.7, we introduce the following definition.

Definition 4.8. *Let $\mathfrak{p}$ be an ideal in R and m be a positive integer. Define $\mathrm{NonTor}^{\mathfrak{p}}(R, m)$ to be the set of positive integers n such that one of the following equivalent conditions is satisfied:*

(i) $\ker\phi \not\subseteq \mathfrak{p}^{(n)}$ for all $\phi \in Hom(R^n, R^m)$.
(ii) for any submodule M of R^m, there are no surjective homomorphism from M to $(R/\mathfrak{p})^n$.

Remark 4.9. *Similar to Proposition 1.8, if $n_0 \in \mathrm{NonTor}^{\mathfrak{p}}(R, m)$, then $n \in \mathrm{NonTor}^{\mathfrak{p}}(R, m)$ for any integer $n \geq n_0$.*

The following theorem is the main theorem of this subsection. It gives a sufficient condition for the existence of a non-torsion number.

Theorem 4.10. *Let R be a Noetherian ring. For each $\mathfrak{p} \in \mathrm{Ass}^\sharp(R)$, suppose $n_{\mathfrak{p}} \in \mathrm{NonTor}^{\mathfrak{p}}(R, m)$. Then*

$$n := 1 + \sum_{\mathfrak{p} \in \mathrm{Ass}^\sharp(R)} (n_{\mathfrak{p}} - 1) \in \mathrm{NonTor}(R, m).$$

Proof. We prove the theorem by contradiction. Suppose not, then by Theorem 4.5 and Theorem 4.7, there exist $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \mathrm{Ass}^\sharp(R)$, a submodule M of R^m, and a sujective module homomorphism

$$\psi : M \twoheadrightarrow (R/\mathfrak{p}_1) \times \cdots \times (R/\mathfrak{p}_n).$$

For each $\mathfrak{p} \in \mathrm{Ass}^\sharp(R)$, define $I_\mathfrak{p} = \{1 \leq i \leq n : \mathfrak{p}_i = \mathfrak{p}\}$. Notice that a surjective homomorphism

$$(R/\mathfrak{p}_1) \times \cdots \times (R/\mathfrak{p}_n) \twoheadrightarrow (R/\mathfrak{p})^{|I_\mathfrak{p}|}$$

can be constructed by projecting the i-th component if $i \in I_\mathfrak{p}$. Composing with ψ, we have

$$M \twoheadrightarrow (R/\mathfrak{p}_1) \times \cdots \times (R/\mathfrak{p}_n) \twoheadrightarrow (R/\mathfrak{p})^{|I_\mathfrak{p}|}.$$

Since $n_\mathfrak{p} \in \mathrm{NonTor}^\mathfrak{p}(R, m)$, we must have $|I_\mathfrak{p}| \leq n_\mathfrak{p} - 1$. Notice that $I_\mathfrak{p}$ partitions $\{1, 2, \dots, n\}$. It follows that

$$n = 1 + \sum_{\mathfrak{p} \in \mathrm{Ass}^\sharp(R)} (n_\mathfrak{p} - 1) \geq 1 + \sum_{\mathfrak{p} \in \mathrm{Ass}^\sharp(R)} |I_\mathfrak{p}| = 1 + n.$$

This is absurd. □

4.2. **Elements in** $\mathrm{NonTor}^\mathfrak{p}(R, m)$**.** Theorem 4.10 tells us that $\mathrm{NonTor}(R, m)$ is non-empty if $\mathrm{NonTor}^\mathfrak{p}(R, m)$ is non-empty for all $\mathfrak{p} \in \mathrm{Ass}^\sharp(R)$. The problem becomes finding elements in $\mathrm{NonTor}^\mathfrak{p}(R, m)$ for each $\mathfrak{p} \in \mathrm{Ass}^\sharp(R)$.

In this subsection, we adopt two approaches to show the existence of elements in $\mathrm{NonTor}^\mathfrak{p}(R, m)$ for classes of Noetherian rings R. One concerns the number of generators (Definition 2.8) of submodules in R^m and one concerns localisation of rings.

4.2.1. *Number of generators.* Notice that if an R-module M is generated by k elements $x_1, \dots, x_k \in M$, a surjective module homomorphism from R^k to M via $(r_1, \dots, r_k) \mapsto r_1x_1 + \cdots + r_kx_k$ can be constructed. Together with Definition 4.8(ii), we come up with the following observation:

Theorem 4.11. *Let R be a ring and m be a positive integer. If any submodule of R^m can be generated by k elements, then $k + 1 \in \mathrm{NonTor}^\mathfrak{p}(R, m)$ for any ideal $\mathfrak{p}$.*

Proof. We prove the theorem by contradiction. Suppose there exists an ideal $\mathfrak{p}$ in R, a submodule M of R^m and a surjective module homomorphism

$$M \twoheadrightarrow (R/\mathfrak{p})^{k+1}.$$

Let $x_1, \dots, x_k$ generate M and consider the surjective module homomorphism $(r_1, \dots, r_k) \mapsto \sum r_ix_i$. Composing the two homomorphisms give the surjective module homomorphism $\varphi : R^k \twoheadrightarrow (R/\mathfrak{p})^{k+1}$.

We claim that $\mathfrak{p}^{(k)} \subseteq \ker\varphi$. To see this, suppose $(p_1, p_2, \dots, p_k) \in \mathfrak{p}^{(k)}$ and write $e_i = (0, \dots, 0, 1, 0, \dots, 0) \in R^k$ where the 1 is in the i-th position for $1 \leq i \leq k$. Then

$$\varphi(p_1, p_2, \dots, p_k) = \varphi\left(\sum_{i=1}^k p_ie_i\right) = \sum_{i=1}^k p_i\varphi(e_i) = \mathbf{0}.$$

The claim follows. By first isomorphism theorem, we have a surjection

$$(R/\mathfrak{p})^k \cong R^k/\mathfrak{p}^{(k)} \twoheadrightarrow R^k/\ker\varphi \cong \operatorname{im}\varphi = (R/\mathfrak{p})^{k+1}.$$

Since $\mathfrak{p} \subseteq \operatorname{Ann}((R/\mathfrak{p})^k)$, we can regard ([2, p.19]) the above R-module homomorphism as an $R/\mathfrak{p}$-module homomorphism. Applying Proposition 1.1 to the commutative ring $R/\mathfrak{p}$ implies that $k \geq k+1$, which is absurd. □

Conditions on the ring R should be imposed so that the assumption of Theorem 4.11 is satisfied. The following lemma is inspired by [3].

Lemma 4.12. *Let R be a ring and M be an R-module. Suppose all ideals in R can be generated by g elements. Then if M is generated by m elements, any submodule of M can be generated by mg elements.*

Proof (Altered from [3]*).* We prove by induction on m. For $m = 1$, $M = Rx$ for some $x \in M$. Let N be a submodule of M and note that $N = \mathfrak{a}x$ where $\mathfrak{a} = \{a \in R : ax \in N\}$ is an ideal of R. By assumption, $\mathfrak{a}$ is generated by g element and so is N.

For the inductive step, let $M = Rx_1 + Rx_2 + \cdots + Rx_{m+1}$ for some $x_1, x_2, \ldots, x_{m+1} \in M$. Consider the submodule $M_1 = Rx_2 + \cdots + Rx_{m+1}$ of M. Suppose N is a submodule of M and define the submodule $N_1 = N \cap M_1$ of M_1. By the inductive hypothesis, N_1 can be generated by mg elements. Write $y_1, y_2, \ldots, y_{mg} \in N_1$ be the generators of N_1.

By second isomorphism theorem, N/N_1 is isomorphic to $(N+M_1)/M_1$, which is a submodule of M/M_1. Note that M/M_1 is generated the element $x_1 + M_1$. From the result for $m = 1$, N/N_1 can be generated by g elements, say $z_1+N_1, z_2+N_1, \ldots, z_g+N_1$ where $z_1, z_2, \ldots, z_g \in N$. We claim that $y_1, y_2, \ldots, y_{mg}, z_1, \ldots, z_g \in N$ generate N. Indeed, if $x \in N$, then $x \in x + N_1 = \sum r_i z_i + N_1$ for some choice of r_i's since $z_i + N_1$ generates N/N_1. Thus $x = \sum r_i z_i + \sum s_j y_j$ since y_j generates N_1. Hence, N is generated by $mg + g = (m+1)g$ elements. □

Combining Theorem 4.11 and Lemma 4.12, a simplified condition on Noetherian rings R with non-empty $\operatorname{NonTor}(R, m)$ is found.

Corollary 4.13. *Let R be a Noetherian ring and m be a positive integer. Suppose all ideals in R can be generated by g elements. Then $mg|\operatorname{Ass}^\sharp(R)| + 1 \in \operatorname{NonTor}(R, m)$.*

Proof. Notice that R^m can be generated by m elements. Applying Lemma 4.12 with $M = R^m$, all submodules of R^m can be generated by mg elements. By Theorem 4.11, $mg + 1 \in \operatorname{NonTor}^{\mathfrak{p}}(R, m)$ for any $\mathfrak{p} \in \operatorname{Ass}^\sharp(R)$. Theorem 4.10 then implies the desired result. □

Note that if R is a principal ideal ring (i.e. a ring where all ideals are principal), then $g = 1$ in Corollary 4.13. This gives the following special case:

Example 4.14. *Let R be a principal ideal ring and m be an integer. By Corollary 4.13, $m|\operatorname{Ass}^\sharp(R)| + 1 \in \operatorname{NonTor}(R, m)$. In other words, combining the result with Theorem 3.13,*

$$m|\operatorname{Ass}^\flat(R)| < \min \operatorname{NonTor}(R, m) \leq m|\operatorname{Ass}^\sharp(R)| + 1.$$

In particular, this completely solves the CMO problem, generalised to m equations. Since $R = \mathbb{Z}/k\mathbb{Z}$ is a principal ideal ring, we have $m\omega(k) + 1 \in \mathrm{NonTor}(R, m)$. On the other hand, we have $m\omega(k) \notin \mathrm{NonTor}(R, m)$ by Example 3.14(i). Thus

$$\mathrm{NonTor}(\mathbb{Z}/k\mathbb{Z}, m) = \{n \in \mathbb{N} : n \geq m\omega(k) + 1\}.$$

Remark 4.15. *We note here that Corollary 4.13 actually implies a non-trivial result as a by-product. Namely, it implies that if ideals in R can be generated by g elements, then*

$$g \geq \frac{|\operatorname{Ass}^\flat(R)|}{|\operatorname{Ass}^\sharp(R)|}.$$

4.2.2. *Localisation.* From Definition 4.8(i), $n \in \mathrm{NonTor}^{\mathfrak{p}}(R, m)$ if and only if any system of m equations with n variables has a solution $\mathbf{x}$ such that one of the coordinates is out of $\mathfrak{p}$. As a naive guess, one might be tempted to consider projecting the system to the integral domain $R/\mathfrak{p}$.

This is unfortunately not applicable since we cannot guarantee a solution after lifting back to R. The issue is explained by the following example.

Example 4.16. *Let $R = \mathbb{Z}/9\mathbb{Z}$ and $m = 2$. Consider the associated prime $\mathfrak{p} = (3)$ and the system represented by $L = \begin{pmatrix} 2 & 6 & 3 \\ 4 & 1 & 2 \end{pmatrix}$. By projecting the entries onto the ring $R/\mathfrak{p} \cong \mathbb{Z}/3\mathbb{Z}$, we obtain a new system represented by*

$$L' = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 1 & 2 \end{pmatrix}.$$

It has a non-trivial solution $\mathbf{x}' = (0, 1, 1)$. Yet by directly pulling $\mathbf{x}'$ back to $\mathbf{x}$ in R, we see that

$$L\mathbf{x} = \begin{pmatrix} 2 & 6 & 3 \\ 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \neq \mathbf{0}$$

As a result, $\mathbf{x}$ is no longer a solution to the original system.

In fact, any pull back of a solution $\mathbf{x}'$ from $R/\mathfrak{p}$ to $\mathbf{x}$ in R can only guarantee that $L\mathbf{x} \in \mathfrak{p}^{(m)}$. It turns out that we have to consider the localisation of R at $\mathfrak{p}$ instead.

Definition 4.17. *Let $\mathfrak{p}$ be a prime ideal in a ring R. Define the **localisation** of R at $\mathfrak{p}$, denoted by $R_{\mathfrak{p}}$, to be the ring consisting of equivalence classes a/s where $a \in R$ and $s \in R \setminus \mathfrak{p}$ with respect to the relation*

$$a/s \equiv b/t \Leftrightarrow (at - bs)u = 0 \ \text{ for some } u \in R \setminus \mathfrak{p}.$$

Addition and multiplication in $R_{\mathfrak{p}}$ are given by $a/s + b/t = (at + bs)/st$ and $a/s \cdot b/t = ab/st$. In this case, $R_{\mathfrak{p}}$ is a local ring with a unique maximal ideal denoted by $\mathfrak{p}R_{\mathfrak{p}} = \{a/s : a \in \mathfrak{p}, s \in R \setminus \mathfrak{p}\}$.

Remark 4.18. *Notice that the ring operations in $R_{\mathfrak{p}}$ is similar to the usual operations done on fractions.*

The problem on determining $\mathrm{NonTor}^{\mathfrak{p}}(R, m)$ turns out to be equivalent to that after taking localisation.

Theorem 4.19. *Let $\mathfrak{p}$ be a prime ideal in the ring R and m be a positive integer. Then* $\mathrm{NonTor}^{\mathfrak{p}}(R,m) = \mathrm{NonTor}^{\mathfrak{p}R_{\mathfrak{p}}}(R_{\mathfrak{p}},m)$.

Proof. By Definition 4.8(i), it suffices to show that there exists $\phi \in \mathrm{Hom}_R(R^n,R^m)$ such that $\ker\phi \subseteq \mathfrak{p}^{(n)}$ if and only if there exists $\phi_{\mathfrak{p}} \in \mathrm{Hom}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}^n,R_{\mathfrak{p}}^m)$ such that $\ker\phi_{\mathfrak{p}} \subseteq \mathfrak{p}R_{\mathfrak{p}}^{(n)}$.

($\Rightarrow$) Suppose that $\phi \in \mathrm{Hom}_R(R^n,R^m)$ is represented by (a_{ij}) where $a_{ij} \in R$. i.e.,

$$\phi(x_1,\ldots,x_n) = \Big(\sum a_{1j}x_j,\ldots,\sum a_{mj}x_j\Big).$$

Take $\phi_{\mathfrak{p}} \in \mathrm{Hom}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}^n,R_{\mathfrak{p}}^m)$ be represented by $(a_{ij}/1)$. Suppose

$$\phi_{\mathfrak{p}}(x_1/s_1,\ldots,x_n/s_n) = 0,$$

then for all $1 \le i \le m$,

$$\sum_{j=1}^{n} \frac{a_{ij}}{1}\frac{x_j}{s_j} = 0 \implies u\sum_{j=1}^{n} a_{ij}\Big(\prod_{k\neq j} s_k\Big)x_j = 0, \text{ for some } u \notin \mathfrak{p}.$$

Therefore $(us_2s_3\cdots s_nx_1, us_1s_3\cdots s_nx_2,\ldots,us_1s_2\cdots s_{n-1}x_n) \in \ker\phi \subseteq \mathfrak{p}^{(n)}$. As $s_i \notin \mathfrak{p}$ and $u \notin \mathfrak{p}$, we have $x_i \in \mathfrak{p}$. Hence $x_i/s_i \in \mathfrak{p}R_{\mathfrak{p}}$ for all $1 \le i \le n$.

($\Leftarrow$) Suppose that $\phi_{\mathfrak{p}} \in \mathrm{Hom}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}^n,R_{\mathfrak{p}}^m)$ is represented by (a_{ij}/s_{ij}). Take $\phi \in \mathrm{Hom}_R(R^n,R^m)$ be represented by $(a_{ij}\cdot\prod_{k\neq j}s_{ik})$. Suppose $\phi(x_1,\ldots,x_n) = 0$, then for all $1 \le i \le m$,

$$\sum_{j=1}^{n} a_{ij}\Big(\prod_{k\neq j} s_{ik}\Big)x_j = 0 \implies \sum_{j=1}^{n} \frac{a_{ij}}{s_{ij}}\frac{x_j}{1} = 0.$$

Therefore $(x_1/1,\ldots,x_n/1) \in \ker\phi_{\mathfrak{p}} \subseteq \mathfrak{p}R_{\mathfrak{p}}^{(n)}$. Hence $x_i \in \mathfrak{p}$ for all $1 \le i \le n$. □

From the previous subsection, it is suggested that $\mathrm{NonTor}^{\mathfrak{p}R_{\mathfrak{p}}}(R_{\mathfrak{p}},m)$ is highly correlated to the number of generators of ideals in $R_{\mathfrak{p}}$. It turns out that generators of ideals in local rings have been studied frequently. The following captures some of the related results.

Definition 4.20. *Let R be a ring. Define the* ***length*** *of a chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ as the number of strict inclusions, n.*

The ***Krull dimension*** *of R, denoted by $\dim(R)$, is defined as the supremum of the lengths over all chains of prime ideals in R.*

For a prime ideal $\mathfrak{p}$ in R, the ***height*** *of $\mathfrak{p}$, denoted by $\mathrm{ht}(\mathfrak{p})$, is defined as the supremum of the lengths over all chains of prime ideals taking the form $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$.*

We quote a well-known result concerning generators of ideals in local rings.

Theorem 4.21. *Let R be a local ring with $\dim R \le 1$. Then there is a positive integer g such that all ideals in R can be generated by g elements.*

Note that $\dim(R_{\mathfrak{p}}) = \mathrm{ht}(\mathfrak{p})$ ([5, p.30]). Utilising this fact and Theorem 4.21, we can impose a condition on Noetherian rings so that non-torsion numbers exist.

Theorem 4.22. *Let R be a Noetherian ring and m be a positive integer. If $\mathrm{ht}(\mathfrak{p}) \leq 1$ for all $\mathfrak{p} \in \mathrm{Ass}^\sharp(R)$, then $\mathrm{NonTor}(R, m)$ is non-empty.*

Proof. Since $\mathrm{ht}(\mathfrak{p}) = \dim R_\mathfrak{p}$, by Theorem 4.21 we know there is a non-negative integer g such that all ideals in $R_\mathfrak{p}$ can be generated by g elements. Hence by Lemma 4.12 any submodules of $(R_\mathfrak{p})^m$ can be generated by mg elements. Now notice that $R_\mathfrak{p}$ is Noetherian. Thus by Theorem 4.11, $mg+1 \in \mathrm{NonTor}^{\mathfrak{p}R_\mathfrak{p}}(R_\mathfrak{p}, m)$. This implies that $mg+1 \in \mathrm{NonTor}^{\mathfrak{p}}(R, m)$ by Theorem 4.19. The result is followed by Theorem 4.10. □

As a corollary, we have the following result.

Corollary 4.23. *Let R be a Noetherian ring with no embedded associated primes. Then $\mathrm{NonTor}(R, m)$ is non-empty.*

Proof. By [2, Proposition 4.6], the minimal associated primes will not contain any other prime ideals in R. Hence their heights must be 0. Since there are no embedded primes, $\mathrm{Ass}^\sharp(R) = \mathrm{Ass}^\flat(R)$ and $\mathrm{ht}(\mathfrak{p}) = 0$ for all $\mathfrak{p} \in \mathrm{Ass}^\sharp(R)$. Thus $\mathrm{NonTor}(R, m)$ is non-empty by Theorem 4.22. □

However, Theorem 4.22 is more powerful, in the sense that even if the ring has embedded primes, we can still guarantee a non-torsion number in some cases. Example 4.25 illustrates this intuition. Yet it relies on the following well-known theorem, which is quite useful in computation.

Theorem 4.24 ([8], Krull's principal ideal theorem)**.** *Let R be a Noetherian ring and (x) be a principal ideal in R. Then the minimal primes of (x) have height at most 1, i.e. if $(x) \subseteq \mathfrak{p}$ and no other prime $\mathfrak{q}$ satisfy $(x) \subseteq \mathfrak{q} \subset \mathfrak{p}$, then $\mathrm{ht}(\mathfrak{p}) \leq 1$.*

As promised, we now give the following familiar example in which Theorem 4.22 can be applied to rings that were not solved before.

Example 4.25. *Consider $R = K[x, y]/(x^2y, xy^2)$ as in Example 3.11 with $\mathrm{Ass}^\sharp(R) = \{(x, y)\}$. We show that $\mathrm{ht}((x, y)) = 1$, so that $\mathrm{NonTor}(R, m)$ is non-empty for any positive integer m.*

Claim. *$r((x + y)) = (x, y)$.*

Proof. If $p \in r((x + y))$, then $p^n \in (x + y)$ for some positive integer n. If p has a constant term then so does p^n, which violates $p^n \in (x + y)$. Thus p has no constant and must be in (x, y).

Conversely, let $p \in (x, y)$, which has no constant term. Notice that for integer $n \geq 3$,

$$x(x+y)^{n-1} = x^n + (n-1)x^{n-1}y + \frac{(n-1)(n-2)}{2}x^{n-2}y^2 + \cdots + xy^{n-1}$$

which is equal to x^n after modulo (x^2y, xy^2). Since $x(x+y)^{n-1} \in (x+y)$, $x^n \in (x+y)$ and $y^n \in (x + y)$ by symmetry. Thus by taking p^3, all terms must have degree at least 3, so every term must be a multiple of x^3, x^2y, xy^2 or y^3. Thus $p^3 \in (x + y)$ which implies $p \in r((x + y))$. □

Now suppose $(x+y) \subseteq \mathfrak{q} \subset (x,y)$ *for some prime* $\mathfrak{q}$. *By Proposition 2.6,* $(x,y) \subseteq \mathfrak{q} \subset (x,y)$ *since* (x,y) *is prime. Contradiction and so* (x,y) *is a minimal element of all prime ideals which contain* $(x+y)$. *Hence Theorem 4.24 applies and* (x,y) *has height at most* 1, *as required.*

4.3. **A special case: reduced Noetherian rings.** The rest of this section is dedicated to a special class of rings which we have not covered above.

Definition 4.26. *A ring* R *is said to be* ***reduced*** *if it has no non-zero nilpotent elements.*

In this section, we will focus on the class of **reduced Noetherian rings**.

Proposition 4.27. *Let* R *be a reduced Noetherian ring. Then* R *has no embedded associated prime.*

Proof. By the reduced condition, the only nilpotent element is 0, i.e. $(0) = r(0)$. Let $(0) = \bigcap \mathfrak{q}_i$ be a minimal primary decomposition. Notice that the number of associated primes n is fixed. Yet by Proposition 2.6,

$$(0) = \bigcap \mathfrak{q}_i = \bigcap r(\mathfrak{q}_i) = \bigcap \mathfrak{p}_i$$

gives another primary decomposition of (0) by taking radicals. If there are embedded associated primes, say $\mathfrak{p}_2 \subset \mathfrak{p}_1$, then there is a primary decomposition with $n-1$ components. Contradiction to the minimality of n. □

We now focus on the elements which are in $\mathrm{NonTor}(R,m)$, where R is a reduced Noetherian ring. To proceed, we rely on a characterisation for the localisation to be a field.

Proposition 4.28. *Let* R *be a reduced Noetherian ring. Then* $R_{\mathfrak{p}}$ *is a field for all* $\mathfrak{p} \in \mathrm{Ass}(R)$.

Proof. By Proposition 4.27, $\mathfrak{p} \in \mathrm{Ass}^{\flat}(R)$. Suppose $\mathfrak{q}'$ is a prime ideal in $R_{\mathfrak{p}}$. By [2, Proposition 3.11], the prime ideals in $R_{\mathfrak{p}}$ are in one-to-one correspondence with the prime ideals of R in $\mathfrak{p}$. This implies that $\mathfrak{q}'$ corresponds to a prime ideal $\mathfrak{q} \subseteq \mathfrak{p}$ in R. Yet by the minimality of $\mathfrak{p}$, we have $\mathfrak{q} = \mathfrak{p}$. Thus there is only one prime ideal $\mathfrak{p}$ in $R_{\mathfrak{p}}$.

Now, consider the nilradical of $R_{\mathfrak{p}}$, which is just $\mathfrak{p}$ by [2, Proposition 1.8] as there is only one prime ideal. However, since R has no nilpotent elements, $\mathfrak{N}_{R_{\mathfrak{p}}} = (0)$ by [2, Corollary 3.12], i.e. (0) is the only prime ideal in $R_{\mathfrak{p}}$. Thus the maximal ideal in $R_{\mathfrak{p}}$ is (0), and so $R_{\mathfrak{p}}$ is a field. □

This solves the entire problem for the class of reduced Noetherian rings:

Corollary 4.29. *Let* R *be a reduced Noetherian ring and* m *be a positive integer. Then*

$$\mathrm{NonTor}(R,m) = \{n \in \mathbb{N} : n \geq m|\operatorname{Ass}(R)| + 1\}.$$

Proof. We already know $m|\operatorname{Ass}(R)| \notin \mathrm{NonTor}(R,m)$ by Proposition 4.27 and Theorem 3.13. Now by Proposition 4.28, $R_{\mathfrak{p}}$ is a field, and thus $m+1 \in \mathrm{NonTor}(R_{\mathfrak{p}},m) =$

$\operatorname{NonTor}^{\mathfrak{p}R_{\mathfrak{p}}}(R_{\mathfrak{p}}, m)$ for all $\mathfrak{p} \in \operatorname{Ass}(R)$. By Theorem 4.19, $m+1 \in \operatorname{NonTor}^{\mathfrak{p}}(R, m)$. Thus

$$\sum_{i=1}^{|\operatorname{Ass}(R)|} (m+1-1)+1 = m|\operatorname{Ass}(R)|+1$$

is a non-torsion number by Theorem 4.10, which implies the result. □

5. Further Investigation

The potential of the problem is not limited to rings. Even in the case of Noetherian rings, we have not fully found $\operatorname{NonTor}(R, m)$. Some possible further investigation on this problem is suggested in this section.

5.1. Conjectures on $\operatorname{NonTor}(R, m)$.

Of all results we achieved, the focus is solely on Noetherian rings. Based on the intuition from Section 4, we propose the following conjecture.

Conjecture 5.1. *Let R be a Noetherian ring with finite Krull dimension and m be a positive integer. Then $\operatorname{NonTor}(R, m)$ is non-empty.*

Remark 5.2. *We specify R to be finite-dimensional since we believe there are rings which are Noetherian with infinite Krull dimension such that $\operatorname{NonTor}(R, m) = \emptyset$. For instance, take $R = K[x_1, x_2, \ldots]$ and prime ideals $\mathfrak{p}_i = (x_{2^{i-1}}, x_{2^{i-1}+1}, \ldots, x_{2^i-1})$ for positive integers i. Let S be the multiplicative subset*

$$S = \bigcap_{i=1}^{\infty} R \setminus \mathfrak{p}_i.$$

Consider the ring $A = S^{-1}R$, which is Noetherian by [11]*. We suggest that $A/(x_1/1, x_2x_3/1, x_4x_5x_6x_7/1, \ldots)$ or similar quotients might be an infinite dimensional Noetherian ring with $\operatorname{NonTor}(R, m) = \emptyset$. We do not know how to verify this due to the complicated structure of this ring, so we leave this for further investigations.*

On the other hand, we hope to discuss the case of non-Noetherian rings. By Example 3.4, there are non-Noetherian rings R with $\operatorname{NonTor}(R, m) = \emptyset$. However, we do not expect all non-Noetherian rings to have empty $\operatorname{NonTor}(R, m)$. It is hence natural to characterise what rings R would have empty $\operatorname{NonTor}(R, m)$.

Question 5.3. *Let R be a ring and m be a positive integer. What does $\operatorname{NonTor}(R, m) = \emptyset$ tell about the ring R?*

5.2. $\operatorname{NonTor}_R(M, m)$ for R-module M.

We believe that our investigation in Section 3 and 4 can be carried to modules. Recall that a solution in a module being non-torsion means that one of its coordinates is not a torsion element of the module.

Definition 5.4. *Let R be a ring and M be an R-module. An element $x \in M$ is called a **torsion element of** M if there exists non-zero $r \in R$ such that $rx = 0$. The set of all torsion elements is denoted by $T(M)$.*

Similar to the case of the set of zero-divisors in a ring, $T(M)$ is not a submodule of M. Yet in the case that R is an integral domain, $T(M)$ forms a submodule of M, called the **torsion submodule of** M.

Unlike the case of rings, it is possible that $T(M) = M$ (in this case M is called a **torsion module**). It turns out that in the two extreme cases $T(M) = M$ and $T(M) = 0$, we can find their respective minimal non-torsion number quite easily.

Proposition 5.5. *Let M be an R-module and m be a positive integer. If $T(M) = M$, then* $\mathrm{NonTor}_R(M, m) = \emptyset$.

Proof. All elements are torsion in M, and thus no non-torsion solution exists for any system. □

Proposition 5.6. *Let M be a Noetherian R-module and m be a positive integer. If $T(M) = 0$, then* $\mathrm{NonTor}_R(M, m) = \{n \in \mathbb{N} : n \geq m + 1\}$.

Proof. Firstly, note that $m \notin \mathrm{NonTor}_R(M, m)$ by considering the system represented by the identity matrix. To show $m + 1 \in \mathrm{NonTor}_R(M, m)$, it suffices to prove that for all $\phi \in \mathrm{Hom}_R(M^{m+1}, M^m)$, $\ker \phi \not\subseteq T(M)^n$, i.e. $\ker \phi \neq \mathbf{0}$.

Suppose $\ker \phi = \mathbf{0}$. By first isomorphism theorem, we have the injective map

$$M^{m+1} \cong M^{m+1}/\ker \phi \cong \mathrm{im}\ \phi \hookrightarrow M^m,$$

which is impossible by [1, Lemma 1.36] since M^m is Noetherian. □

Some properties of the set of zero-divisors can be carried over to $T(M)$. For example, we have the following analogy to Proposition 4.3.

Proposition 5.7. *Let M be an R-module with $T(M) \neq M$. Then $T(M)$ is a union of prime submodules.*

Here, a submodule P of M is called a **prime submodule** if for $r \in R$ and $m \in M$, $rm \in P$ implies $m \in P$ or $r \in \{x \in R : xM \subseteq P\}$.

We suspect that analogical results to, for instance Theorem 3.13 and Theorem 4.22 can be deduced. In addition, special cases such as M being a free R-module, as well as M being a finitely generated module over a PID can be investigated.

6. Conclusion

In this paper, we proposed the problem of finding the minimum integer n such that every homogeneous system of m equations with n variables over a given ring has a non-torsion solution. The results are summarised as follows.

As shown in the introductory section, the case of integral domains is immediate with the help of [1]. By Proposition 1.10, the set of non-torsion numbers is given by $\mathrm{NonTor}(R, m) = \{x \in \mathbb{N} : x \geq m + 1\}$. Then, the problem from CMO asked for the non-torsion numbers in $\mathbb{Z}/k\mathbb{Z}$ when $m = 2$. We have $\mathrm{NonTor}(\mathbb{Z}/k\mathbb{Z}, 2) = \{x \in \mathbb{N} : x \geq 2\omega(k) + 1\}$ as given in the solution by [9].

We then moved on to the generalised problem over rings. We divided the problem into two sub-tasks; one concerns the elements not in $\mathrm{NonTor}(R, m)$ and the other one concerns those that are in $\mathrm{NonTor}(R, m)$. They are covered in Section 3 and 4 respectively.

In Section 3, we made use of the notion of primary decomposition to show that $m|\operatorname{Ass}^{\flat}(R)| \notin \operatorname{NonTor}(R,m)$ for Noetherian rings R. This is proved by giving a construction and the use of prime avoidance lemma in Theorem 3.13.

In Section 4, we gave equivalent formulations of the problem, which allowed us to consider individual associated primes instead of the whole set of zero-divisors at once by Theorem 4.10. This motivated the definition of $\operatorname{NonTor}^{\mathfrak{p}}(R,m)$. We then approached the sub-problem of finding elements in $\operatorname{NonTor}^{\mathfrak{p}}(R,m)$ by considering the number of generators of ideals and the localisation of R at $\mathfrak{p}$. They gave rich results on the non-emptiness of $\operatorname{NonTor}^{\mathfrak{p}}(R,m)$ and hence $\operatorname{NonTor}(R,m)$.

Combining the results in the two sections, Corollary 4.13 showed that if all ideals in R can be generated by g elements, then $mg|\operatorname{Ass}^{\sharp}(R)|+1 \in \operatorname{NonTor}(R,m)$. In particular, we solved the CMO problem with m equations. We also showed in Theorem 4.22 that if R is a Noetherian ring such that the heights of all associated primes are at most one, then $\operatorname{NonTor}(R,m)$ is non-empty. At last, for the case where R is a reduced Noetherian ring, we gave a complete solution to the problem: $\operatorname{NonTor}(R,m) = \{x \in \mathbb{N} : x \geq m|\operatorname{Ass}(R)|+1\}$.

Appendix A. Proof of the CMO Problem

The following solution to Question 1.3 is adopted from [9]. Note that since the solution is posted on a forum, it might contains unclear explanations, gaps and informal wordings within the proof. We choose not to fix these details to maintain as much original ideas from the author as possible. The only amendments are of its format.

The problem is restated here.

Question A.1 (CMO 2021/2)**.** *[1.3] Let $m > 1$ be an integer. Find the smallest positive integer n, such that for any integers $a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n$ there exists integers $x_1, x_2, \ldots, x_n$ satisfying the following two conditions:*

(i) There exists $i \in \{1, 2, \ldots, n\}$ such that x_i and m are coprime.

(ii) $\displaystyle\sum_{i=1}^{n} a_i x_i \equiv \sum_{i=1}^{n} b_i x_i \equiv 0 \pmod{m}$.

Solution to Question 1.3. The answer is $2\omega(m)+1$, where $\omega(m)$ is the number of distinct primes dividing m. We say that the integer n is m-friendly if it satisfies the conditions.

Construction for $2\omega(m)$

Write $m = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$ and $\omega(m) = t$. For every $s = 1, \ldots, t$, let p_s divide all of the a_i and b_i's except for a_{2s-1} and b_{2s}. Then x_{2s-1} and x_{2s} must both be divisible by p_s, so none of the x_i's are coprime to m.

Proof for $2\omega(m)+1$

We first prove the following claim:

Claim A.2. *For a prime p and a positive integer k, n is p-friendly iff n is p^k-friendly.*

Proof. The reverse implication is obviously true, so we will prove the forward direction. We want to show that n is p^k-friendly, so say that we are given $c_1, \ldots, c_n$ and $d_1, \ldots, d_n$.

Induct on k, and we split into four cases:

Case 1: The vectors $c = (c_1, \ldots, c_n)$ and $d = (d_1, \ldots, d_n)$ are linearly independent in $\mathbb{F}_p^n$. By inductive hypothesis, we assume that

$$\sum_i c_i x_i \equiv ap^{k-1} \pmod{p^k}, \quad \sum_i d_i x_i \equiv bp^{k-1} \pmod{p^k}.$$

Because of our assumption, the matrix

$$\begin{bmatrix} c_1 & c_2 & \ldots & c_n \\ d_1 & d_2 & \ldots & d_n \end{bmatrix}$$

has rank 2, and the vectors (c_i, d_i) span the space $\mathbb{F}_p^2$. Thus, we can also find $y_1, \ldots, y_n$ with $\sum_i a_i y_i \equiv a \pmod{p}$ and $\sum_i b_i y_i \equiv b \pmod{p}$. We can then just take $x_i' = x_i - y_i p^{k-1}$, and

$$\sum_i c_i x_i' \equiv ap^{k-1} - ap^{k-1} = 0 \pmod{p^k}, \quad \sum_i d_i x_i' \equiv bp^{k-1} - bp^{k-1} = 0 \pmod{p^k}.$$

Case 2: The vectors c and d are both zero mod p. Notice that we can just divide all c_i and d_i by p to reduce to the inductive hypothesis.

Case 3: c is the zero vector, and d is not all zero. Suppose that entry d_1 is not zero mod p, then by inductive hypothesis, there exist x_i such that

$$\sum_i (c_i/p) x_i \equiv \sum_i d_i x_i \equiv 0 \pmod{p^{k-1}}.$$

We can then just modify x_1 by a suitable multiple of p^{k-1}.

Case 4: c and d are both nonzero, and $d = \lambda c$ for some nonzero element $\lambda \in \mathbb{F}_p$. In this case, suppose $d_i = \lambda c_i + p\ell_i$. We know that there exist x_i (not all divisible by p) such that

$$\sum_i c_i x_i \equiv \sum_i \ell_i x_i \equiv 0 \pmod{p^{k-1}}$$

Also, let $\sum_i c_i x_i \equiv ap^{k-1} \pmod{p^k}$, and we choose y_i such that $\sum_i c_i y_i \equiv a \pmod{p}$ (this is possible since there exists a nonzero c_i). Let $x_i' = x_i - y_i p^{k-1}$. Then

$$\sum_i c_i x_i' \equiv 0 \pmod{p^k}$$

and

$$\sum_i d_i x_i' = \sum_i (\lambda c_i + p\ell_i) x_i' = \lambda \sum_i c_i x_i' + p \sum_i \ell_i x_i' \equiv 0 \pmod{p^k}.$$

Having listed all cases, the claim has been proven. □

Back to the original problem. We take the equations mod p^k for each $p^k \mid\mid m$, and by the claim above this is equivalent to just taking mod p. The matrix

$$M = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

is a linear map from $\mathbb{F}_p^{2t+1}$ to $\mathbb{F}_p^2$, so its kernel has dimension at least $2t-1$, which implies that at most 2 entries have to be zero. Because there are $t = \omega(m)$ primes dividing m, at most $2t$ entries don't work, so there exists an entry that could be coprime to m (we used CRT here). □

Acknowledgements

I hereby show my sincere gratitude to Mr. Mark Lau Tin Wai and Mr. Ernest Fan Yan Lam for continuous advice and collaborations; without their help, this paper would not be even close to how it is now. I am also especially thankful to my supervising teacher, Mr. Lee Ho Fung for supporting me when writing this paper.

References

[1] T. Y. Lam (1999). *'Lectures on Rings and Modules'* Springer, pp. 9-16.
[2] M. F. Atiyah, I. G. MacDonald (1969). *'Introduction to Commutative Algebra'* CRC Press.
[3] O. Zariski, P. Samuel (1958). *'Commutative Algebra'* D. Van Nostrand Company, pp. 246-247.
[4] J. D. Sally (1978). *'Numbers of generators of ideals in local rings'* Marcel Dekker, Inc., p. 51.
[5] H. Matsumura (1980). *'Commutative Ring Theory'* Cambridge University Press, pp. 30-31.
[6] D. D. Anderson, Sangmin Chun (2014). *'The Set of Torsion Elements of a Module'* Communications in Algebra, 42:4, 1835-1843
[7] R. B. Ash *'A Course in Commutative Algebra'* unpublished, Ch. 1
`https://faculty.math.illinois.edu/~r-ash/ComAlg/ComAlg1.pdf`
[8] M. Hochster *'Dimension theory and systems of parameters'* unpublished, p. 1.
`http://www.math.lsa.umich.edu/~hochster/615W10/supDim.pdf`
[9] Idio-logy (Nov 25 2020). *'m divides linear sum of sequences'* Art of Problem Solving.
`https://artofproblemsolving.com/community/c6h2353705p19100643`
[10] Mec, Alex Becker (May 28 2012). *'When the localization of a ring is a field'* Mathematics StackExchange. `https://math.stackexchange.com/questions/150892/when-the-localization-of-a-ring-is-a-field`
[11] Stack Project. *'A Noetherian ring of infinite dimension'* Section 108.15.
`https://stacks.math.columbia.edu/tag/02JC`

REVIEWERS' COMMENTS

This paper was reviewed by three experts on representation theory and algebraic geometry. All three reviewers were highly impressed by the quality and depth of this paper, and by the fact that the author was just a high school student. The problem investigated by the paper was well-motivated by a 2021 Chinese Mathematical Olympiad (CMO) problem. The author rephrased and generalized that CMO problem about solving a system of two linear equations in $\mathbb{Z}/k\mathbb{Z}$ into a problem in commutative algebra: finding a set NonTor(M,m), which is the positive integers that any homogeneous system of m equations with n variables on the R-module M guarantees a non-torsion solution.

Reviewers found that the author displayed an excellent command of commutative algebra techniques at the level of a very advanced undergraduate or even early graduate student, and he demonstrated his mathematical maturity of using, for instance, primary decomposition in Noetherian ring, to break down the problem into easier components.