Solving System of Linear Congruence Equations over some Rings by Decompositions of Modules

Mahmood Behboodi[1,3], Shadi Asgari[1], Ali Moradzadeh-Dehkordi[2,3], Amir Hashemi[1,3*];

1. Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, Iran
2. Faculty of Basic Sciences, University of Shahreza, Isfahan, Iran
3. School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran

Received: 20 April 2017 Accepted: 7 Jan. 2018

Extended Abstract

Paper pages (133-152)

In this paper, we deal with solving systems of linear congruences over commutative CF-rings. More precisely, let R be a CF-ring (every finitely generated direct sum of cyclic R-modules has a canonical form) and let $I_1, \dots, I_n$ be n ideals of R. We consider the system of linear congruences :

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{I_1} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 \pmod{I_2} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \qquad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \equiv b_n \pmod{I_n} \end{cases}$$

where $a_{ij}, b_i \in R$ and $I_j \subseteq \bigcap_{i\neq j}(I_i : a_{ij})$ for all $1 \leq i, j \leq n$ and $(I : a) = \{r \in R : ra \in I\}$. We introduce congruence matrices theory techniques and exploit its application to solve the above system. Further, we investigate the application of computer algebra techniques (Gröbner bases) in this context whenever $R = \mathbb{Z}$.

Introduction

The theory of solving systems of linear equations has its origin in the works of the Chinese mathematician Sun Zi. In his book entitled “The mathemetical classic of Sun Zi” published in the third century AD, he introduced the Chinese remainder theorem and exploited it to solve systems of linear congruences. It is worth noting that solving such systems has many applications in different areas including signal processing, cryptography and so on. In this paper, we consider a more general form of systems of linear congruences over CF-rings where the congruence relations are defined on some given ideals. For this purpose, we develop the theory of congruence linear algebra that we employ in this paper to study this general form of linear congruence systems. In this direction, let us give a review of some previous algebraic results about CF-rings on which our approach is based.

Throughout this paper all rings are commutative with unity, and all modules are unital. Following [3], a CF-ring is a ring for which every finitely generated direct sum of cyclic R-modules has a canonical form (a canonical form for an R-module M is a decomposition $M \cong R/I_1 \oplus \cdots \oplus R/I_n$, where $I_1 \subseteq \cdots \subseteq I_n \neq R$). Every CF-ring is a finite direct product of indecomposable CF-rings. The indecomposable CF-rings are precisely the rings R for which the following four conditions are satisfied: (1) R is an arithmetical ring, (2) R has a unique minimal prime ideal P, (3) every ideal contained in P is comparable with every ideal of R, and (4) R/P is an h –local domain (see [3, Theorem 1] for more details).
Let R be a CF-ring and $\beta = (I_1, \ldots, I_n)$ be a sequence of ideals of R. In this paper, we introduce the techniques to solve the linear congruence systems

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 & (\mathrm{mod}\ I_1) \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \equiv b_2 & (\mathrm{mod}\ I_2) \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots & \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \equiv b_n & (\mathrm{mod}\ I_n), \end{cases}$$

where $I_j \subseteq \bigcap_{i \neq j} (I_i : a_{ij})$ for all $1 \leq i, j \leq n$.

In Section 1, we introduce the congruence matrices theory techniques and exploit its application to solve the above system. Further, we investigate the application of computer algebra techniques (Gröbner bases) in this context whenever $R = \mathbb{Z}$.

Congruence linear algebra techniques

Definition 1.1. We define the relation $\approx$ on the set $M_{n\times m}(R)$ of all n×m matrices over the ring R as follows: for $A = (a_{ij})$ and $A' = (a'_{ij})$ in $M_{n\times m}(R)$

$$.A \approx A' \Leftrightarrow a_{ij} - a'_{ij} \in I_i$$

Clearly, $\approx$ is an equivalence relation. An equivalence class of $A = (a_{ij})_{n\times m}$ is denoted by $\left(\left(a_{ij}\right)\right)$. We set $R^{\beta} = \left\{\left(\left(a_i\right)\right)_{n\times 1} \mid 1 \leq i \leq n, a_i \in R\right\}$. Clearly, R^{β} is an R-module with the ordinary addition and the multiplication.

In this section, we introduce and study some congruence matrices theory techniques. To exploit our techniques over the congruence matrix $A = \left(\left(a_{ij}\right)\right)$ (see Definition 1.1), like the ordinary linear algebra, we show that one can define the canonical R-endomorphism $\varphi : R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n \to R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$ associate to A if and only if $I_j \subseteq \bigcap_{i \neq j} (I_i : a_{ij})$ for all $1 \leq i, j \leq n$. Also, the invertibility of the congruence matrix A and its application to solve the above system is discussed. Next, we propose a method based on modular linear algebra techniques to solve a linear system of congruence equations. In doing so, we present a modular Gaussian elimination method for performing Gaussian elimination on the matrices over integers modulo a given integer. Some relevant examples are presented in the full version of the paper.

Gröbner Bases and Congruence Systems

Gröbner bases is an important algorithmic object in computational algebraic geometry. This notion was introduced and an algorithm for its construction was designed in 1965 by

Buchberger in his Ph.D. thesis [2]. Gröbner bases method is a practical tool to solve a wide class of problems in polynomial ideal theory (like ideal membership, equality of ideals and solving polynomial systems) and in many other research areas of science and engineering (like integer programming, computer graphics, digital signal processing, robotics and so on). We refer to [1] for more details on the theory of Gröbner bases and its applications.

In this section, we apply Gröbner bases techniques to solve these systems in the case that $R = \mathbb{Z}$.

Keywords: Linear congruence systems, Modular Gaussian elimination, Gröbner bases.

*Corresponding author: amir.hashemi@cc.iut.ac.ir