S-unit equations and the Diophantine problem in abelian-by-cyclic groups

Ruiwen Dong

Magdalen College, University of Oxford, UK

May 2025

Part I: linear equations

Linear equations with extra constraints

Given a system of linear equations:

$$\begin{cases} 4y_1 + 12y_2 + 2z_1 + 3z_2 = 7 \\ 5y_1 + 17y_2 + 9z_1 + 8z_2 = 4 \\ 2y_1 + 21y_2 + 3z_1 + 4z_2 = 6 \end{cases}$$

Linear equations with extra constraints

Given a system of linear equations:

$$\begin{cases} 4y_1 + 12y_2 + 2z_1 + 3z_2 = 7 \\ 5y_1 + 17y_2 + 9z_1 + 8z_2 = 4 \\ 2y_1 + 21y_2 + 3z_1 + 4z_2 = 6 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}$?

Linear equations with extra constraints

Given a system of linear equations:

$$\begin{cases} 4y_1 + 12y_2 + 2z_1 + 3z_2 = 7 \\ 5y_1 + 17y_2 + 9z_1 + 8z_2 = 4 \\ 2y_1 + 21y_2 + 3z_1 + 4z_2 = 6 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}$?

Decidable by **linear algebra** over $\mathbb{Z}$.

Linear equations with extra constraints

Given a system of linear equations:

$$\begin{cases} 4y_1 + 12y_2 + 2z_1 + 3z_2 = 7 \\ 5y_1 + 17y_2 + 9z_1 + 8z_2 = 4 \\ 2y_1 + 21y_2 + 3z_1 + 4z_2 = 6 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}$?

Decidable by **linear algebra** over $\mathbb{Z}$.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}$, $z_1, z_2 \in \mathbb{N}$?

Linear equations with extra constraints

Given a system of linear equations:

$$\begin{cases} 4y_1 + 12y_2 + 2z_1 + 3z_2 = 7 \\ 5y_1 + 17y_2 + 9z_1 + 8z_2 = 4 \\ 2y_1 + 21y_2 + 3z_1 + 4z_2 = 6 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}$?

Decidable by **linear algebra** over $\mathbb{Z}$.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}$, $z_1, z_2 \in \mathbb{N}$?

Decidable by **Integer Programming**.

Linear equations with extra constraints

Given a system of linear equations:

$$\begin{cases} 4y_1 + 12y_2 + 2z_1 + 3z_2 = 7 \\ 5y_1 + 17y_2 + 9z_1 + 8z_2 = 4 \\ 2y_1 + 21y_2 + 3z_1 + 4z_2 = 6 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}$?

Decidable by **linear algebra** over $\mathbb{Z}$.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}$, $z_1, z_2 \in \mathbb{N}$?

Decidable by **Integer Programming**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}$, $z_1, z_2 \in 2^{\mathbb{N}} := \{2^n \mid n \in \mathbb{N}\}$?

Linear equations with extra constraints

Given a system of linear equations:

$$\begin{cases} 4y_1 + 12y_2 + 2z_1 + 3z_2 = 7 \\ 5y_1 + 17y_2 + 9z_1 + 8z_2 = 4 \\ 2y_1 + 21y_2 + 3z_1 + 4z_2 = 6 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}$?

Decidable by **linear algebra** over $\mathbb{Z}$.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}$, $z_1, z_2 \in \mathbb{N}$?

Decidable by **Integer Programming**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}$, $z_1, z_2 \in 2^{\mathbb{N}} := \{2^n \mid n \in \mathbb{N}\}$?

Decidable by a fragment of **Büchi arithmetic**.

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2 z_2 = X^2-X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2 z_2 = X^2-X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}[X]$?

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2 z_2 = X^2 - X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}[X]$?
Decidable by **Gröbner Basis**.

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2z_2 = X^2-X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}[X]$?
Decidable by **Gröbner Basis**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{Z}$?

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2 z_2 = X^2 - X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}[X]$?
Decidable by **Gröbner Basis**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{Z}$?
Decidable by **Gröbner Basis + Variable Elimination**.

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2 z_2 = X^2 - X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}[X]$?
Decidable by **Gröbner Basis**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{Z}$?
Decidable by **Gröbner Basis + Variable Elimination**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{N}[X]$ (polynomials with only positive coefficients)?

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2 z_2 = X^2 - X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}[X]$?
Decidable by **Gröbner Basis**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{Z}$?
Decidable by **Gröbner Basis + Variable Elimination**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{N}[X]$ (polynomials with only positive coefficients)?

Undecidable in general (Narenden 1996).

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2 z_2 = X^2 - X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}[X]$?
Decidable by **Gröbner Basis**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{Z}$?
Decidable by **Gröbner Basis + Variable Elimination**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{N}[X]$ (polynomials with only positive coefficients)?

Undecidable in general (Narenden 1996).
Decidable for **homogeneous** linear equations (Einsiedler 2003).

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2 z_2 = X^2 - X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}[X]$?
Decidable by **Gröbner Basis**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{Z}$?
Decidable by **Gröbner Basis + Variable Elimination**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{N}[X]$ (polynomials with only positive coefficients)?

Undecidable in general (Narenden 1996).
Decidable for **homogeneous** linear equations (Einsiedler 2003).

Does it have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in X^{\mathbb{N}} := \{X^n \mid n \in \mathbb{N}\}$?

Linear equations with extra constraints

Given a system of linear equations (with coefficients in the ring $\mathbb{Z}[X]$):

$$\begin{cases} (4X+1)y_1 + (X^2-3X+1)y_2 + (2X^3-1)z_1 + 3z_2 = X^3+7 \\ (X^3+2X)y_1 + (X^4+2X^3+1)y_2 + (2X^2+7)z_1 + X^2z_2 = X^2-X \\ (X^2-4)y_1 + (X^2+2X+2)y_2 + (3X^2-5X)z_1 + (X+1)z_2 = X+5 \end{cases}$$

Does this system have solutions $y_1, y_2, z_1, z_2 \in \mathbb{Z}[X]$?
Decidable by **Gröbner Basis**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{Z}$?
Decidable by **Gröbner Basis + Variable Elimination**.

Does this system have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in \mathbb{N}[X]$ (polynomials with only positive coefficients)?

Undecidable in general (Narenden 1996).
Decidable for **homogeneous** linear equations (Einsiedler 2003).

Does it have solutions $y_1, y_2 \in \mathbb{Z}[X]$, $z_1, z_2 \in X^{\mathbb{N}} := \{X^n \mid n \in \mathbb{N}\}$?

Undecidable (D. 2024, **first result of this talk**).

S-unit equations in fields

Definition (S-unit equation in a field)

Let $\mathbb{K}$ be a field. Given a finite subset $S \subseteq \mathbb{K} \setminus \{0\}$, denote by $\langle S \rangle$ the multiplicative subgroup generated by S. Let $m_0, m_1, \ldots, m_K$ in $\mathbb{K}$, an *S-unit equation* is a linear equation of the form

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

where we look for solutions $x_1, \ldots, x_K \in \langle S \rangle$.

Example: the equation $7x - 4y = 2$ where $x, y \in \langle 2, 3 \rangle = 2^{\mathbb{Z}} \cdot 3^{\mathbb{Z}}$.

S-unit equations in fields

Definition (S-unit equation in a field)

Let $\mathbb{K}$ be a field. Given a finite subset $S \subseteq \mathbb{K} \setminus \{0\}$, denote by $\langle S \rangle$ the multiplicative subgroup generated by S. Let $m_0, m_1, \ldots, m_K$ in $\mathbb{K}$, an *S-unit equation* is a linear equation of the form

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

where we look for solutions $x_1, \ldots, x_K \in \langle S \rangle$.

Example: the equation $7x - 4y = 2$ where $x, y \in \langle 2, 3 \rangle = 2^{\mathbb{Z}} \cdot 3^{\mathbb{Z}}$.

Theorem (Subspace theorem, Schmidt 1972)

When $\mathbb{K} = \mathbb{Q}$, an S-unit equation has only a finite number of nondegenerate solutions (solutions with the property that no proper subsum vanishes).

However, the Subspace theorem is **not** effective, so no known algorithm to determine whether a solution exists.

S-unit equations in modules

Let $\mathbb{K}$ be a field (or any commutative ring) and let a set $S = \{s_1, \ldots, s_N\}$ be a set of invertible elements of $\mathbb{K}$.
Then $\mathbb{K}$ is a $\mathbb{Z}[X_1^{\pm}, \ldots, X_N^{\pm}]$-module where each X_i acts as s_i.

S-unit equations in modules

Let $\mathbb{K}$ be a field (or any commutative ring) and let a set $S = \{s_1, \ldots, s_N\}$ be a set of invertible elements of $\mathbb{K}$.
Then $\mathbb{K}$ is a $\mathbb{Z}[X_1^{\pm}, \ldots, X_N^{\pm}]$-module where each X_i acts as s_i.

Definition (S-unit equation in a module)

Let $\mathcal{M}$ be a finitely presented $\mathbb{Z}[X_1^{\pm}, \ldots, X_N^{\pm}]$-module. Let $m_0, m_1, \ldots, m_K$ in $\mathcal{M}$, an *S-unit equation* is a linear equation of the form

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

where we look for **monomial** solutions $x_1, \ldots, x_K \in X_1^{\mathbb{Z}} X_2^{\mathbb{Z}} \cdots X_N^{\mathbb{Z}}$.

S-unit equations in modules

Let $\mathbb{K}$ be a field (or any commutative ring) and let a set $S = \{s_1, \ldots, s_N\}$ be a set of invertible elements of $\mathbb{K}$.

Then $\mathbb{K}$ is a $\mathbb{Z}[X_1^{\pm}, \ldots, X_N^{\pm}]$-module where each X_i acts as s_i.

Definition (S-unit equation in a module)

Let $\mathcal{M}$ be a finitely presented $\mathbb{Z}[X_1^{\pm}, \ldots, X_N^{\pm}]$-module. Let $m_0, m_1, \ldots, m_K$ in $\mathcal{M}$, an *S-unit equation* is a linear equation of the form

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

where we look for **monomial** solutions $x_1, \ldots, x_K \in X_1^{\mathbb{Z}} X_2^{\mathbb{Z}} \cdots X_N^{\mathbb{Z}}$.

Example: let $a_1 y_1 + \cdots + a_n y_n + b_1 z_1 + \cdots + b_m z_m = c$ be an equation in $\mathbb{Z}[X, X^{-1}]$. We look for solutions $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

S-unit equations in modules

Let $\mathbb{K}$ be a field (or any commutative ring) and let a set $S = \{s_1, \dots, s_N\}$ be a set of invertible elements of $\mathbb{K}$.
Then $\mathbb{K}$ is a $\mathbb{Z}[X_1^{\pm}, \dots, X_N^{\pm}]$-module where each X_i acts as s_i.

Definition (S-unit equation in a module)

Let $\mathcal{M}$ be a finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_N^{\pm}]$-module. Let $m_0, m_1, \dots, m_K$ in $\mathcal{M}$, an *S-unit equation* is a linear equation of the form

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

where we look for **monomial** solutions $x_1, \dots, x_K \in X_1^{\mathbb{Z}} X_2^{\mathbb{Z}} \cdots X_N^{\mathbb{Z}}$.

Example: let $a_1 y_1 + \cdots + a_n y_n + b_1 z_1 + \cdots + b_m z_m = c$ be an equation in $\mathbb{Z}[X, X^{-1}]$. We look for solutions $y_1, \dots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \dots, z_n \in X^{\mathbb{Z}}$.
This is equivalent to the S-unit equation

$$b_1 z_1 + \cdots + b_m z_m = c$$

in the module $\mathbb{Z}[X, X^{-1}] / \langle a_1, \dots, a_n \rangle$.

S-unit equation in $\mathbb{Z}[X^{\pm}]$-modules

Theorem (D. 2024)

It is undecidable whether, given system of linear equations $a_{i1}y_1 + \cdots + a_{in}y_n + b_{i1}z_1 + \cdots + b_{im}z_m = c_i$, $i = 1, \ldots, k$, there are solutions $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

S-unit equation in $\mathbb{Z}[X^{\pm}]$-modules

Theorem (D. 2024)

It is undecidable whether, given system of linear equations $a_{i1}y_1 + \cdots + a_{in}y_n + b_{i1}z_1 + \cdots + b_{im}z_m = c_i$, $i = 1, \ldots, k$, there are solutions $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

Proof (part 1): We embed Hilbert's tenth problem (solving a polynomial equation over integers is undecidable).

S-unit equation in $\mathbb{Z}[X^{\pm}]$-modules

Theorem (D. 2024)

It is undecidable whether, given system of linear equations $a_{i1}y_1 + \cdots + a_{in}y_n + b_{i1}z_1 + \cdots + b_{im}z_m = c_i$, $i = 1, \ldots, k$, *there are solutions* $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

Proof (part 1): We embed Hilbert's tenth problem (solving a polynomial equation over integers is undecidable).

Lemma (Expressing squares)

Suppose $n_1, n_2, n_3 \in \mathbb{Z}$. *We have*

$$(X-1)^3 \mid X^{n_1} + X^{n_2}(1-X) + X^{n_3} + (X-3)$$

if and only if $n_2 = n_1^2$, $n_3 = -n_1$.

Idea: $(X-1)^3 \mid f$ if and only if $f(1) = f'(1) = f''(1) = 0$.

S-unit equation in $\mathbb{Z}[X^{\pm}]$-modules

Theorem (D. 2024)

It is undecidable whether, given system of linear equations $a_{i1}y_1 + \cdots + a_{in}y_n + b_{i1}z_1 + \cdots + b_{im}z_m = c_i$, $i = 1, \ldots, k$, *there are solutions* $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

Proof (part 1): We embed Hilbert's tenth problem (solving a polynomial equation over integers is undecidable).

Lemma (Expressing squares)

Suppose $n_1, n_2, n_3 \in \mathbb{Z}$. *We have*

$$(X-1)^3 \mid X^{n_1} + X^{n_2}(1-X) + X^{n_3} + (X-3)$$

if and only if $n_2 = n_1^2$, $n_3 = -n_1$.

Idea: $(X-1)^3 \mid f$ if and only if $f(1) = f'(1) = f''(1) = 0$.

Note that "$(X-1)^3 \mid f$" can be expressed as "$(X-1)^3 y = f$". Therefore we can express "squaring" of integers.

S-unit equation in $\mathbb{Z}[X^{\pm}]$-modules

Theorem (D. 2024)

It is undecidable whether, given system of linear equations $a_{i1}y_1 + \cdots + a_{in}y_n + b_{i1}z_1 + \cdots + b_{im}z_m = c_i$, $i = 1, \ldots, k$, *there are solutions* $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

Proof (part 2):

S-unit equation in $\mathbb{Z}[X^{\pm}]$-modules

Theorem (D. 2024)

It is undecidable whether, given system of linear equations $a_{i1}y_1 + \cdots + a_{in}y_n + b_{i1}z_1 + \cdots + b_{im}z_m = c_i$, $i = 1, \ldots, k$, there are solutions $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

Proof (part 2):

Lemma (Expressing sums)

Suppose $n_1, n_2, n_3 \in \mathbb{Z}$. We have

$$(X-1)^2 \mid X^{n_1} + X^{n_2} - X^{n_3} - 1$$

if and only if $n_3 = n_1 + n_2$.

Idea: $(X-1)^2 \mid f$ if and only if $f(1) = f'(1) = 0$.

Therefore linear equations with monomial constraints can express "summing" of integers.

S-unit equation in $\mathbb{Z}[X^{\pm}]$-modules

Theorem (D. 2024)

It is undecidable whether, given system of linear equations $a_{i1}y_1 + \cdots + a_{in}y_n + b_{i1}z_1 + \cdots + b_{im}z_m = c_i$, $i = 1, \ldots, k$, there are solutions $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

Proof (part 3): We embed Hilbert's tenth problem (solving a polynomial equation over integers is undecidable).

Theorem (D. 2024)

It is undecidable whether, given system of linear equations $a_{i1}y_1 + \cdots + a_{in}y_n + b_{i1}z_1 + \cdots + b_{im}z_m = c_i$, $i = 1, \ldots, k$, *there are solutions* $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

Proof (part 3): We embed Hilbert's tenth problem (solving a polynomial equation over integers is undecidable).

Linear equations with monomial constraints can express "squaring" and "summing" of integers. Note that "product" of integers and be expressed by "squaring" and "summing": $xy = \Big((x+y)^2 - x^2 - y^2\Big)/2$.

S-unit equation in $\mathbb{Z}[X^{\pm}]$-modules

Theorem (D. 2024)

It is undecidable whether, given system of linear equations $a_{i1}y_1 + \cdots + a_{in}y_n + b_{i1}z_1 + \cdots + b_{im}z_m = c_i$, $i = 1, \ldots, k$, there are solutions $y_1, \ldots, y_n \in \mathbb{Z}[X, X^{-1}]$, $z_1, \ldots, z_n \in X^{\mathbb{Z}}$.

Proof (part 3): We embed Hilbert's tenth problem (solving a polynomial equation over integers is undecidable).

Linear equations with monomial constraints can express "squaring" and "summing" of integers. Note that "product" of integers and be expressed by "squaring" and "summing": $xy = \Big((x+y)^2 - x^2 - y^2\Big)/2$.

Therefore linear equations with monomial constraints can express any polynomial equation over integers, therefore undecidable.

Q.E.D

Part II: Diophantine problem

Let G be an (infinite) group. Let $g_1, g_2, g_3, g_4 \in G$. Consider the following problems:

Applications to group theory: Equations over groups

Let G be an (infinite) group. Let $g_1, g_2, g_3, g_4 \in G$. Consider the following problems:

(Conjugacy Problem): Is there $x \in G$ such that $x g_1 x^{-1} = g_2$?

Applications to group theory: Equations over groups

Let G be an (infinite) group. Let $g_1, g_2, g_3, g_4 \in G$. Consider the following problems:

(Conjugacy Problem): Is there $x \in G$ such that $xg_1x^{-1} = g_2$?

(Simultaneous Conjugacy): Is there $x \in G$ such that $xg_1x^{-1} = g_2$ and $xg_3x^{-1} = g_4$?

Applications to group theory: Equations over groups

Let G be an (infinite) group. Let $g_1, g_2, g_3, g_4 \in G$. Consider the following problems:

(Conjugacy Problem): Is there $x \in G$ such that $xg_1x^{-1} = g_2$?

(Simultaneous Conjugacy): Is there $x \in G$ such that $xg_1x^{-1} = g_2$ and $xg_3x^{-1} = g_4$?

(Finding Square Root): Is there $x \in G$ such that $x^2 = g_1$?

Applications to group theory: Equations over groups

Let G be an (infinite) group. Let $g_1, g_2, g_3, g_4 \in G$. Consider the following problems:

(Conjugacy Problem): Is there $x \in G$ such that $xg_1x^{-1} = g_2$?

(Simultaneous Conjugacy): Is there $x \in G$ such that $xg_1x^{-1} = g_2$ and $xg_3x^{-1} = g_4$?

(Finding Square Root): Is there $x \in G$ such that $x^2 = g_1$?

(???): Are there $x, y \in G$ such that $xy^2g_1x^{-1} = g_2yg_3$ and $yxyg_2x^{-1} = xyg_1xg_4$?

Applications to group theory: Equations over groups

Let G be an (infinite) group. Let $g_1, g_2, g_3, g_4 \in G$. Consider the following problems:

(Conjugacy Problem): Is there $x \in G$ such that $xg_1x^{-1} = g_2$?

(Simultaneous Conjugacy): Is there $x \in G$ such that $xg_1x^{-1} = g_2$ and $xg_3x^{-1} = g_4$?

(Finding Square Root): Is there $x \in G$ such that $x^2 = g_1$?

(???): Are there $x, y \in G$ such that $xy^2g_1x^{-1} = g_2yg_3$ and $yxyg_2x^{-1} = xyg_1xg_4$?

Definition (Diophantine problem in groups)

Solving a system of equations over a group G is the following problem. Let $\mathcal{X} = \{x_1, \dots, x_n\}$ be an alphabet and $\mathcal{X}^{-1} := \{x_1^{-1}, \dots, x_n^{-1}\}$.
Input: words $w_1, \dots, w_t$ over the alphabet $\mathcal{X} \cup \mathcal{X}^{-1} \cup G$.
Question: whether there exist $h_1, \dots, h_n \in G$, such that each w_i evaluates to the neutral element when we replace each x_j with h_j.

Diophantine problem in groups: classic results

Theorem (Makanin 1977)

Solving a system of equations over a **free monoid** *(i.e.* **word equations***) is decidable.*

Diophantine problem in groups: classic results

Theorem (Makanin 1977)

Solving a system of equations over a **free monoid** *(i.e.* **word equations***) is decidable.*

Theorem (Makanin 1983)

Solving a system of equations over a **free group** *is decidable.*

Diophantine problem in groups: classic results

Theorem (Makanin 1977)

Solving a system of equations over a **free monoid** *(i.e.* **word equations***) is decidable.*

Theorem (Makanin 1983)

Solving a system of equations over a **free group** *is decidable.*

Theorem (Dahmani, Guirardel 2010)

Solving a system of equations over a **hyberbolic group** *is decidable.*

Diophantine problem in groups: classic results

Theorem (Makanin 1977)

Solving a system of equations over a **free monoid** *(i.e.* **word equations***) is decidable.*

Theorem (Makanin 1983)

Solving a system of equations over a **free group** *is decidable.*

Theorem (Dahmani, Guirardel 2010)

Solving a system of equations over a **hyberbolic group** *is decidable.*

Theorem (folklore)

Solving a system of equations over an **abelian group** *is decidable.*

Diophantine problem in groups: classic results

Theorem (Makanin 1977)

Solving a system of equations over a **free monoid** *(i.e.* **word equations***) is decidable.*

Theorem (Makanin 1983)

Solving a system of equations over a **free group** *is decidable.*

Theorem (Dahmani, Guirardel 2010)

Solving a system of equations over a **hyberbolic group** *is decidable.*

Theorem (folklore)

Solving a system of equations over an **abelian group** *is decidable.*

Theorem (Romankov 1979, Duchin, Liang, Shapiro 2015)

Solving a system of equations over **free metabelian groups** *and over* **free nilpotent groups** *is undecidable.*

Equations over groups: abelian-by-cyclic groups

Motivation: find other groups where Diophantine problem is decidable.

Equations over groups: abelian-by-cyclic groups

Motivation: find other groups where Diophantine problem is decidable.

Hopeful candidates: **abelian-by-cyclic** groups.

Definition

A group G is called **abelian-by-cyclic** if it admits an normal subgroup A, such that A is abelian and $G/A \cong \mathbb{Z}$.

Equations over groups: abelian-by-cyclic groups

Motivation: find other groups where Diophantine problem is decidable.

Hopeful candidates: **abelian-by-cyclic** groups.

Definition

A group G is called **abelian-by-cyclic** if it admits an normal subgroup A, such that A is abelian and $G/A \cong \mathbb{Z}$.

Remark: if A is abelian and G/A is finite then G is **virtually abelian**, and solving a system of equations over G is decidable.

Equations over groups: abelian-by-cyclic groups

Motivation: find other groups where Diophantine problem is decidable.

Hopeful candidates: **abelian-by-cyclic** groups.

Definition

A group G is called **abelian-by-cyclic** if it admits an normal subgroup A, such that A is abelian and $G/A \cong \mathbb{Z}$.

Remark: if A is abelian and G/A is finite then G is **virtually abelian**, and solving a system of equations over G is decidable.

Examples of abelian-by-cyclic groups:

Baumslag-Solitar group: $\mathrm{BS}(1,2) \coloneqq \left\{ \begin{pmatrix} 2^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{Z}[1/2], b \in \mathbb{Z} \right\}$

Equations over groups: abelian-by-cyclic groups

Motivation: find other groups where Diophantine problem is decidable.

Hopeful candidates: **abelian-by-cyclic** groups.

Definition

A group G is called **abelian-by-cyclic** if it admits an normal subgroup A, such that A is abelian and $G/A \cong \mathbb{Z}$.

Remark: if A is abelian and G/A is finite then G is **virtually abelian**, and solving a system of equations over G is decidable.

Examples of abelian-by-cyclic groups:

Baumslag-Solitar group: $\mathrm{BS}(1,2) := \left\{ \begin{pmatrix} 2^b & f \\ 0 & 1 \end{pmatrix} \middle| f \in \mathbb{Z}[1/2], b \in \mathbb{Z} \right\}$

Lamplighter group: $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \middle| f \in \mathbb{F}_2[X^{\pm}], b \in \mathbb{Z} \right\}$

Equations over groups: abelian-by-cyclic groups

Motivation: find other groups where Diophantine problem is decidable.

Hopeful candidates: **abelian-by-cyclic** groups.

Definition

A group G is called **abelian-by-cyclic** if it admits an normal subgroup A, such that A is abelian and $G/A \cong \mathbb{Z}$.

Remark: if A is abelian and G/A is finite then G is **virtually abelian**, and solving a system of equations over G is decidable.

Examples of abelian-by-cyclic groups:

Baumslag-Solitar group: $\mathrm{BS}(1,2) := \left\{ \begin{pmatrix} 2^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{Z}[1/2], b \in \mathbb{Z} \right\}$

Lamplighter group: $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{F}_2[X^{\pm}], b \in \mathbb{Z} \right\}$

Wreath product: $\mathbb{Z} \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{Z}[X^{\pm}], b \in \mathbb{Z} \right\}$

Equations over groups: abelian-by-cyclic groups

Examples of abelian-by-cyclic groups, where solving equations might be decidable:

Baumslag-Solitar group: $\mathrm{BS}(1,2) := \left\{ \begin{pmatrix} 2^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{Z}[1/2], b \in \mathbb{Z} \right\}$

Lamplighter group: $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{F}_2[X^{\pm}], b \in \mathbb{Z} \right\}$

Wreath product: $\mathbb{Z} \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{Z}[X^{\pm}], b \in \mathbb{Z} \right\}$

Equations over groups: abelian-by-cyclic groups

Examples of abelian-by-cyclic groups, where solving equations might be decidable:

Baumslag-Solitar group: $\mathrm{BS}(1,2) := \left\{ \begin{pmatrix} 2^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{Z}[1/2], b \in \mathbb{Z} \right\}$

Lamplighter group: $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{F}_2[X^{\pm}], b \in \mathbb{Z} \right\}$

Wreath product: $\mathbb{Z} \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \;\middle|\; f \in \mathbb{Z}[X^{\pm}], b \in \mathbb{Z} \right\}$

Open problem (Kharlampovich, López, Myasnikov 2020): is solving systems of equations in these groups decidable?

Equations over groups: abelian-by-cyclic groups

Examples of abelian-by-cyclic groups, where solving equations might be decidable:

Baumslag-Solitar group: $\mathrm{BS}(1,2) := \left\{ \begin{pmatrix} 2^b & f \\ 0 & 1 \end{pmatrix} \middle| \, f \in \mathbb{Z}[1/2], b \in \mathbb{Z} \right\}$

Lamplighter group: $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \middle| \, f \in \mathbb{F}_2[X^{\pm}], b \in \mathbb{Z} \right\}$

Wreath product: $\mathbb{Z} \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \middle| \, f \in \mathbb{Z}[X^{\pm}], b \in \mathbb{Z} \right\}$

Open problem (Kharlampovich, López, Myasnikov 2020): is solving systems of equations in these groups decidable?

Theorem (D. 2024)

Solving a system of equations over $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

Equations over groups: abelian-by-cyclic groups

Examples of abelian-by-cyclic groups, where solving equations might be decidable:

Baumslag-Solitar group: $\mathrm{BS}(1,2) := \left\{ \begin{pmatrix} 2^b & f \\ 0 & 1 \end{pmatrix} \,\middle|\, f \in \mathbb{Z}[1/2], b \in \mathbb{Z} \right\}$

Lamplighter group: $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \,\middle|\, f \in \mathbb{F}_2[X^\pm], b \in \mathbb{Z} \right\}$

Wreath product: $\mathbb{Z} \wr \mathbb{Z} := \left\{ \begin{pmatrix} X^b & f \\ 0 & 1 \end{pmatrix} \,\middle|\, f \in \mathbb{Z}[X^\pm], b \in \mathbb{Z} \right\}$

Open problem (Kharlampovich, López, Myasnikov 2020): is solving systems of equations in these groups decidable?

Theorem (D. 2024)

Solving a system of equations over $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

Proof idea: embed S-unit equations in certain $\mathbb{Z}[X, X^{-1}]$-modules.

System of equations over $\mathbb{Z} \wr \mathbb{Z}$

Theorem (D. 2024)

Solving a system of equations over $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

Proof idea: express "sum" and "multiply by monomial".

System of equations over $\mathbb{Z} \wr \mathbb{Z}$

Theorem (D. 2024)

Solving a system of equations over $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

Proof idea: express "sum" and "multiply by monomial".
(1) Expressing "multiple by monomial". Let $f, g \in \mathbb{Z}[X, X^{-1}]$. Then $\exists n,\ f = g \cdot X^n$ iff

$$\exists x \in \mathbb{Z} \wr \mathbb{Z}, \quad x \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} x^{-1} = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}$$

System of equations over $\mathbb{Z} \wr \mathbb{Z}$

Theorem (D. 2024)

Solving a system of equations over $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

Proof idea: express "sum" and "multiply by monomial".
(1) Expressing "multiple by monomial". Let $f, g \in \mathbb{Z}[X, X^{-1}]$. Then $\exists n,\ f = g \cdot X^n$ iff

$$\exists x \in \mathbb{Z} \wr \mathbb{Z},\ \ x \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} x^{-1} = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}$$

(2) Expressing "divisibility by $(X-1)^k$". Define $[x, y] = xyx^{-1}y^{-1}$. Then $(X-1) \mid f$ iff

$$\exists x, y \in \mathbb{Z} \wr \mathbb{Z},\ \ [x, y] = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}.$$

System of equations over $\mathbb{Z} \wr \mathbb{Z}$

Theorem (D. 2024)

Solving a system of equations over $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

Proof idea: express "sum" and "multiply by monomial".
(1) Expressing "multiple by monomial". Let $f, g \in \mathbb{Z}[X, X^{-1}]$. Then $\exists n,\ f = g \cdot X^n$ iff

$$\exists x \in \mathbb{Z} \wr \mathbb{Z},\ \ x \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} x^{-1} = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}$$

(2) Expressing "divisibility by $(X-1)^k$". Define $[x, y] = xyx^{-1}y^{-1}$. Then $(X-1) \mid f$ iff

$$\exists x, y \in \mathbb{Z} \wr \mathbb{Z},\ \ [x, y] = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}.$$

Define $[[x, y], z] = [x, y]z[x, y]^{-1}z^{-1}$. Then $(X-1)^2 \mid f$ iff

$$\exists x, y, z \in \mathbb{Z} \wr \mathbb{Z},\ \ [[x, y], z] = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}.$$

System of equations over $\mathbb{Z} \wr \mathbb{Z}$

Theorem (D. 2024)

Solving a system of equations over $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

Proof idea: express "sum" and "multiply by monomial".

(1) Expressing "multiple by monomial". Let $f, g \in \mathbb{Z}[X, X^{-1}]$. Then $\exists n,\ f = g \cdot X^n$ iff

$$\exists x \in \mathbb{Z} \wr \mathbb{Z}, \ \ x \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix} x^{-1} = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}$$

(2) Expressing "divisibility by $(X-1)^k$". Define $[x, y] = xyx^{-1}y^{-1}$. Then $(X-1) \mid f$ iff

$$\exists x, y \in \mathbb{Z} \wr \mathbb{Z}, \ \ [x, y] = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}.$$

Define $[[x, y], z] = [x, y]z[x, y]^{-1}z^{-1}$. Then $(X-1)^2 \mid f$ iff

$$\exists x, y, z \in \mathbb{Z} \wr \mathbb{Z}, \ \ [[x, y], z] = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}.$$

(3) Undecidability. Use addition, multiplication by monomial, and divisibility by $(X-1)^k$, $k = 1, 2, 3$.

Part III: open problems

S-unit equations in fields of positive characteristic

Theorem (Subspace theorem, Schmidt 1972)

An S-unit equation over $\mathbb{Q}$ has only a finite number of nondegenerate solutions (solutions with the property that no proper subsum vanishes).

But no known algorithm can determine whether a solution exists.

S-unit equations in fields of positive characteristic

Theorem (Subspace theorem, Schmidt 1972)

An S-unit equation over $\mathbb{Q}$ has only a finite number of nondegenerate solutions (solutions with the property that no proper subsum vanishes).

But no known algorithm can determine whether a solution exists.

Theorem (Derkson, Masser 2012)

Let $\mathbb{K}$ be a field of characteristic $p > 0$. The solution set of a given S-unit equation over $\mathbb{K}$ can be effectively written as a p-normal set.

For example, the equation

$$(X+1)^z - X^z = 1$$

in $\mathbb{F}_2(X)$ has the solution set $z \in \{2^n \mid n \in \mathbb{N}\}$.
There is an algorithm that determines whether a solution exists.

S-unit equations in $(\mathbb{Z}/T\mathbb{Z})[X_1^{\pm}, \ldots, X_N^{\pm}]$-modules

We can again generalize S-unit equations from fields to modules.

Theorem (D. 2024)

Let p be a prime and $\mathcal{M}$ be a finitely presented $\mathbb{F}_p[X_1^{\pm}, \ldots, X_N^{\pm}]$-module. Then the solution set of an S-unit equation

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

$x_1, \ldots, x_K \in X_1^{\mathbb{Z}} X_2^{\mathbb{Z}} \cdots X_N^{\mathbb{Z}}$, *is effectively p-normal.*

S-unit equations in $(\mathbb{Z}/T\mathbb{Z})[X_1^{\pm}, \ldots, X_N^{\pm}]$-modules

We can again generalize S-unit equations from fields to modules.

Theorem (D. 2024)

Let p be a prime and $\mathcal{M}$ be a finitely presented $\mathbb{F}_p[X_1^{\pm}, \ldots, X_N^{\pm}]$-module. Then the solution set of an S-unit equation

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

$x_1, \ldots, x_K \in X_1^{\mathbb{Z}} X_2^{\mathbb{Z}} \cdots X_N^{\mathbb{Z}}$, *is effectively p-normal.*

We can push even further:

Theorem (D., Shafrir 2025)

Let $T = p^a q^b$ be a number with at most two prime divisors, and $\mathcal{M}$ be a finitely presented $(\mathbb{Z}/T\mathbb{Z})[X_1^{\pm}, \ldots, X_N^{\pm}]$-module. It is decidable whether an S-unit equation

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

$x_1, \ldots, x_K \in X_1^{\mathbb{Z}} X_2^{\mathbb{Z}} \cdots X_N^{\mathbb{Z}}$, *admits a solution.*

S-unit equations in $(\mathbb{Z}/T\mathbb{Z})[X_1^{\pm}, \ldots, X_N^{\pm}]$-modules

Theorem (D., Shafrir 2025)

Let $T = p^a q^b r^c$ be a number with three distinct prime divisors, and $\mathcal{M}$ be a finitely presented $(\mathbb{Z}/T\mathbb{Z})[X_1^{\pm}, \ldots, X_N^{\pm}]$-module. Then deciding whether an S-unit equation

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

$x_1, \ldots, x_K \in X_1^{\mathbb{Z}} X_2^{\mathbb{Z}} \cdots X_N^{\mathbb{Z}}$, admits a solution is Turing-equivalent to the following open problem in number theory:

(Linear-exponential Diophantine equation over three primes.)

Given a system of linear equations over $\mathbb{Z}$, where certain variables are restricted to $p^{\mathbb{N}}, q^{\mathbb{N}}, r^{\mathbb{N}}$, decide whether it admits a solution.

S-unit equations in $(\mathbb{Z}/T\mathbb{Z})[X_1^{\pm}, \ldots, X_N^{\pm}]$-modules

Theorem (D., Shafrir 2025)

Let $T = p^a q^b r^c$ be a number with three distinct prime divisors, and $\mathcal{M}$ be a finitely presented $(\mathbb{Z}/T\mathbb{Z})[X_1^{\pm}, \ldots, X_N^{\pm}]$-module. Then deciding whether an S-unit equation

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

$x_1, \ldots, x_K \in X_1^{\mathbb{Z}} X_2^{\mathbb{Z}} \cdots X_N^{\mathbb{Z}}$, admits a solution is Turing-equivalent to the following open problem in number theory:
(Linear-exponential Diophantine equation over three primes.)
Given a system of linear equations over $\mathbb{Z}$, where certain variables are restricted to $p^{\mathbb{N}}, q^{\mathbb{N}}, r^{\mathbb{N}}$, decide whether it admits a solution.

Example: it is unknown how to find all $(a, b, c) \in \mathbb{N}^3$ such that

$$3^a + 5^b - 7^c = 1.$$

S-unit equations in $(\mathbb{Z}/T\mathbb{Z})[X_1^{\pm}, \ldots, X_N^{\pm}]$-modules

Theorem (D., Shafrir 2025)

Let $T = p^a q^b r^c$ be a number with three distinct prime divisors, and $\mathcal{M}$ be a finitely presented $(\mathbb{Z}/T\mathbb{Z})[X_1^{\pm}, \ldots, X_N^{\pm}]$-module. Then deciding whether an S-unit equation

$$x_1 m_1 + \cdots + x_K m_K = m_0,$$

$x_1, \ldots, x_K \in X_1^{\mathbb{Z}} X_2^{\mathbb{Z}} \cdots X_N^{\mathbb{Z}}$, admits a solution is Turing-equivalent to the following open problem in number theory:
(Linear-exponential Diophantine equation over three primes.)
Given a system of linear equations over $\mathbb{Z}$, where certain variables are restricted to $p^{\mathbb{N}}, q^{\mathbb{N}}, r^{\mathbb{N}}$, decide whether it admits a solution.

Example: it is unknown how to find all $(a, b, c) \in \mathbb{N}^3$ such that

$$3^a + 5^b - 7^c = 1.$$

The same problem over two primes is decidable (Karimov et al. 2025).

Group theory application

Corollary (D. 2025)

Submonoid Membership is decidable in $(\mathbb{Z}/T\mathbb{Z}) \wr \mathbb{Z}^N$*, where* T *has at most two prime divisors.*

Group theory application

Corollary (D. 2025)

Submonoid Membership is decidable in $(\mathbb{Z}/T\mathbb{Z}) \wr \mathbb{Z}^N$, where T has at most two prime divisors.

To encode difficult problems, we need Krull dimension $N \geq 2$. Correspondingly, to show undecidability of Diophantine problem this way, we need $\mathrm{rk}(G/[G,G]) \geq 2$. So $\mathbb{Z} \wr \mathbb{Z}$ but not $(\mathbb{Z}/2) \wr \mathbb{Z}$.