

Title	二次ディオファントス方程式の求解アルゴリズムについて
Author(s)	中村, 悠人
Citation	
Issue Date	2024-12
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/19420
Rights	
Description	Supervisor: 小川 瑞史, 先端科学技術研究科, 修士(情報科学)

概要

多項式制約解消は、実数解と整数解の場合に分かれ、SMT ソルバーの背景理論として、それぞれ Nonlinear Real number Arithmetic (NRA)、Nonlinear Integer Arithmetic (NIA) に相当し、その手法と決定可能性は異なる。

多項式制約の実数上の充足可能解は、1930 年前後に Tarski が Quantifier elimination が適用可能であり、決定可能性を示した。しかし、そのアルゴリズムは暗黙的であり、実際にアルゴリズムとして整理されるのは Tarski 自身によって 1951 年になってからであった。

多項式制約の整数解に限る場合を Diophantine 制約とよぶ。Diophantine 方程式の決定可能性は Hilbert の 第十問題として知られ、その否定的解決は Matijasevic により示された。

一方、Grunwald は 1981 年単一の二次 Diophantine 方程式は決定可能であることを示した。その論文は数ページの短いものであるが、実際の内容は、Hasse 原理を含む古典的二次形式の理論、Hensel 補題を含む可換環論・代数群・Lie 環の基礎理論に基づき、背景知識は多岐にわたると同時にアルゴリズムの記述は暗黙的である。

本論文では、Grunwald が提案した単一の二次 Diophantine 方程式の充足可能性の決定アルゴリズムを self-contained に紹介する。その際、数学的命題の証明は基本的に各参考文献にゆずるが、アルゴリズムの記述に必要となる命題、ならびに手続きは余さず記述する。