課題番号：GR087
助成額：20百万円

グリーン・イノベーション

理工系

平成23年2月10日
～平成26年3月31日

高次元p進ディオファントス近似と整数格子クリプトシステム

平田 典子（河野典子） 日本大学理工学部 教授
Noriko Hirata-Kohno

専門分野
数論と暗号の基本原理

キーワード
数論／数論幾何学／群論／暗号系／アルゴリズム理論／ディオファントス近似／格子

WEBページ
http://trout.math.cst.nihon-u.ac.jp/~hirata/Next.html

研究背景

離散対数などの暗号の基礎原理は、理論的には解けるが膨大な時間を要する数学の問題の計算困難性によって「暗号を容易に破られないように守る」という発想に負うている。しかし早く計算できる方法が数学的に見つかってしまえば、その暗号原理は危険になってしまうため、新しい暗号の数学原理の創成が必要であった。

研究目的の特色

高次元p進ディオファントス近似不等式とは、楕円曲線のS整数点の決定のために不可欠な不等式である。その証明に成功し、最良評価不等式の予想を完全解決した論文を完成した。これを用いて、楕円曲線のS整数格子決定アルゴリズムを作り、暗号の新しい基礎原理を求めた論文を出版した。暗号の新しい数学原理が示された。

実績

代表論文：Noriko Hirata-Kohno and Attila Petho, On a key exchange protocol based on Diophantine equations, Infocommunications Journal, ISSN 2061-2079, Vol. 5, (2013), No. 3, 17--21.
一般雑誌：雑誌「工学教育：事例紹介」（2013年5月号）61巻, No. 3, 113-115.
雑誌「数学セミナー『素朴で奥深い整数の世界』」(2013年7月号）52巻, no. 7, 32--36.

研究成果

高次元p進ディオファントス近似

長い間その確立が待たれていたp進楕円対数一次結合のディオファントス近似不等式を完成した。「極めて新規性に富む絶対的な数学の結果」である。1998年出版London Mathematical Society Student Texts, 41巻, N. P. Smart著の本（Cambridge 大学出版）の207-210ページに、この不等式の欠落とそれによる障害が明記されており、解決が望まれていた問題であった。

TABLE 1. The upper bound for N_p in each case of p.

N_p	$\leqq$	A_p	$\times$	10^{n_p}
N_3	$\leqq$	3.338213	$\times$	10^{123}
N_5	$\leqq$	4.964138	$\times$	10^{122}
N_{1009}	$\leqq$	4.501887	$\times$	10^{137}
N_∞	$\leqq$	1.647738	$\times$	10^{149}

The bound for $\{3, 5, 1009, \infty\}$-integral solutions to $E : y^2 = x^3 - 20932x - 330140$.

楕円曲線のS整数上界

楕円曲線のS整数格子決定アルゴリズム

高次元p進ディオファントス近似不等式が未解決であったために計算例がなかった楕円曲線のS整数格子を決定するアルゴリズムを構築し、これを用いて楕円曲線 y*y=x*x*x-20932*x-330140 と3,5,1009および無限素点から成る素点の集合Sに対してS整数を決定した(T. Kovacsと共著、左図表は点の上界)。

Concrete example. Set $m = 4, n = 3$ and choose the polynomials as follows.

$$
\begin{aligned}
f &= c_1x_1^2 + c_2x_2^3 + c_3x_3^3 + c_4x_4^7 + c_5;\\
c_1 &= 10044396160689962515669775888965258647,\\
c_2 &= -34981051230118512018117948645199447959092\\
c_3 &= 36379686253405252442775297079115999387383647\\
&\quad 1062704444171396361954364,\\
c_4 &= -70754124560273954620402107149399581088175120\\
&\quad 207422399264982424 01,\\
c_5 &= -98765432345678987654321654320567896543210567,\\
g &= 3x_1 + 5x_2^2 + 7x_1x_2 + 93x_3^3 + 753x_4,\\
H &= ((g + 734367)^3 + 537769)^5 + 56478587.
\end{aligned}
$$

暗号数理モデル

暗号の新しい基礎原理

曲線の定義方程式fを単射変換した方程式gと元の方程式fの整数点との対応に基づいた暗号原理を構築して投稿し、出版された(A. Pethosと共著、右図表)。暗号数理モデルを明示化した。

2030年の応用展開

今まで用いられて来た暗号原理とは異なる斬新な基礎理論を提唱することは、暗号を安全に保つための根幹を支える基礎研究として不可欠である。現在の素因数分解および離散対数暗号とは全く異なる独創的な暗号原理を提案し、数理モデルを構成することによって、容易に破られない暗号の確立に貢献することが期待される。