不思議な p-進数の国のアリス

- Alice in p-adic wonder numberland -

2016年3月10日　熊本大学
工学部　数理工学科
内藤幸一郎

Part I

p-adic Numberland にいたるまでの研究概要

Part II

p-進解析と耐量子計算機暗号

Part I

(1)1977～1983年頃 （修士、博士課程：東工大）
周期的または概周期的な摂動項をもつ反応拡散方程式系の概周期解の存在や安定解の存在についての解析
（博士論文1983を含む）

(2)1983～1993年頃 （東工大、専修大）
制御項をもつ半線形偏微分方程式系の制御可能性の解析

(3)1993～2015年頃 （1993年6月1日～熊本大学）
- 複数の周期的摂動項をもつ非線形偏微分方程式における準周期的解軌道のフラクタル次元評価
- 準周期的離散軌道の再帰性の評価

Part II 2010年～

- P-進解析とその暗号理論への応用

これまでの研究経過での特徴的なこと:

・約10年程度で大きく研究内容が変わっている;
その理由

→マンネリ化（同じ手法で類似の論文を量産し始める。
　テーマ自体に新鮮味を感じなくなる。）

→新たなテーマへのきっかけとなる「出会い」
　(本、論文、ネット情報、もしくは批判、毒舌など）

→　環境の変化：就職、転勤等

(1)1973～1983　反応拡散方程式系の概周期解の解析
→　(2)1983～1993　半線形偏微分方程式系の制御可能性の解析

＊ J. L. Lions: 偏微分方程式と最適制御 (邦訳), 東京図書 (1973)

(2)1983～1993　半線形偏微分方程式系の制御可能性の解析
→　(3)1993～2015　　準周期的解軌道のフラクタル次元評価

＊ P. Berge, Ch. Vidal, Y. Pomeau：カオスの中の秩序―乱流の理解へ向けて，産業図書(1992)
＊Mitchell M. Waldrop：複雑系―生命現象から政治、経済までを統合する知の革命，新潮社（1996）

- カオスへ至る道筋：
  準周期トーラスの崩壊

- KAM理論：
  準周期トーラスの安定性と
  ディオファンタス条件
  （無理数の有理数近似不良性）

- 複雑系の解析：
  カオス現象に現れるフラクタル構造
  数値解析が主流、 数学理論は？？？

概周期から準周期へ

・概周期関数の定義

$$\forall \varepsilon > 0, \exists\, l_\varepsilon > 0 \text{ such that } \forall a \in \mathbb{R}, \exists \tau \in [a, a + l_\varepsilon]:$$
$$\sup_{t \in \mathbb{R}} |f(t + \tau) - f(t)| \leq \varepsilon.$$

(l_ε: ε-inclusion length, τ: ε-almost period)

・準周期関数の定義

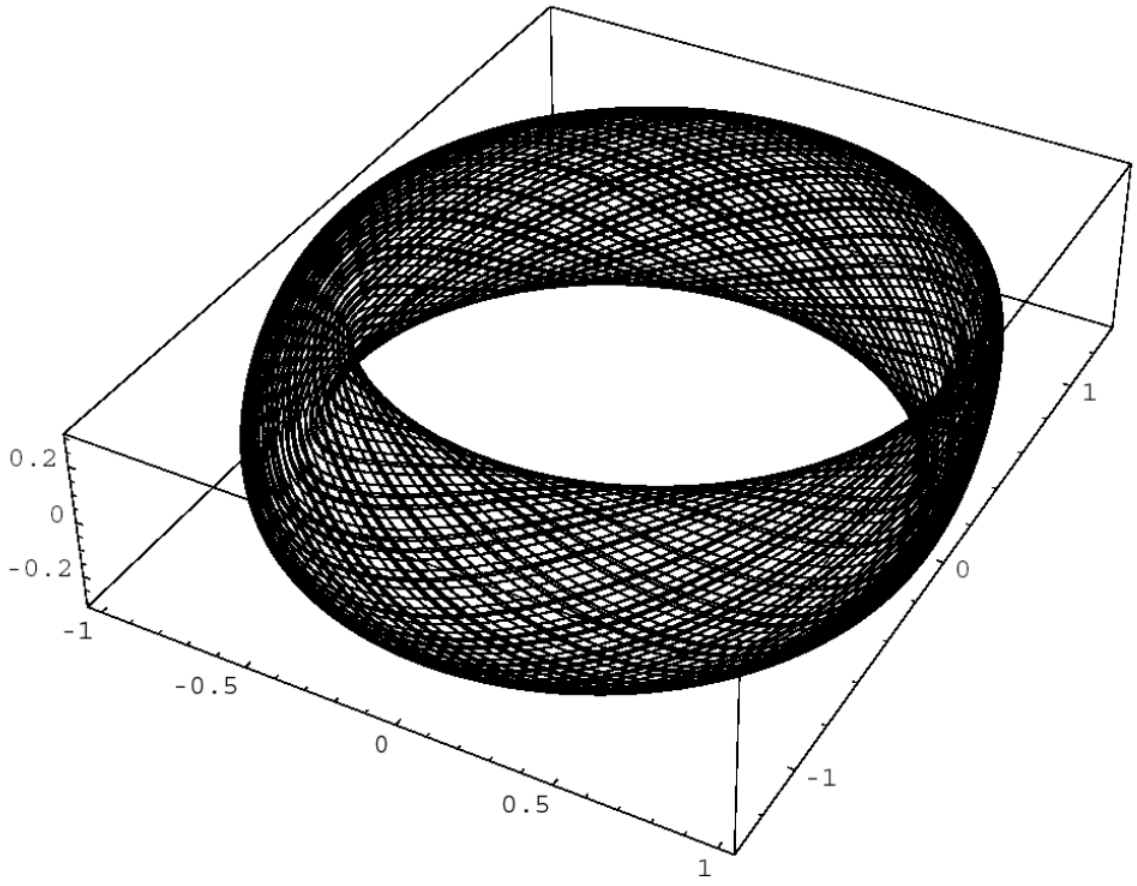
$$g(t, s) = g(t + 1, s) = g(t, s + 1),\ \forall t, s, \in \mathbb{R},\ \tau: \text{ irrational}$$

$$f(t) = g(t, \tau t)$$

準周期トーラス

$$g(t,s) = g_1(t) + g_2(s) = (\cos 2\pi t, \sin 2\pi t, 0) + 0.3(0, \cos 2\pi s, \sin 2\pi s)$$

$f(t) = g_1(t) + g_2(\sqrt{3}t)$ の軌跡



コーカス（堂々巡り）レース：
アリスとドードー鳥

（3） 1993年　～

カオスとフラクタル

・無理数の代数的性質（有理数近似良・不良性）の解析

・準周期的解軌道のフラクタル次元評価

・準周期的離散軌道の再帰性の評価(再帰的次元）

⇒　数論、記号力学系

Continued Fractions, Chaos の検索で：

＊Chaos in numberland:

The secret life of continued fractions (by John D. Barrow)

(時空の特異点の近傍で重力場に現れるカオス現象）

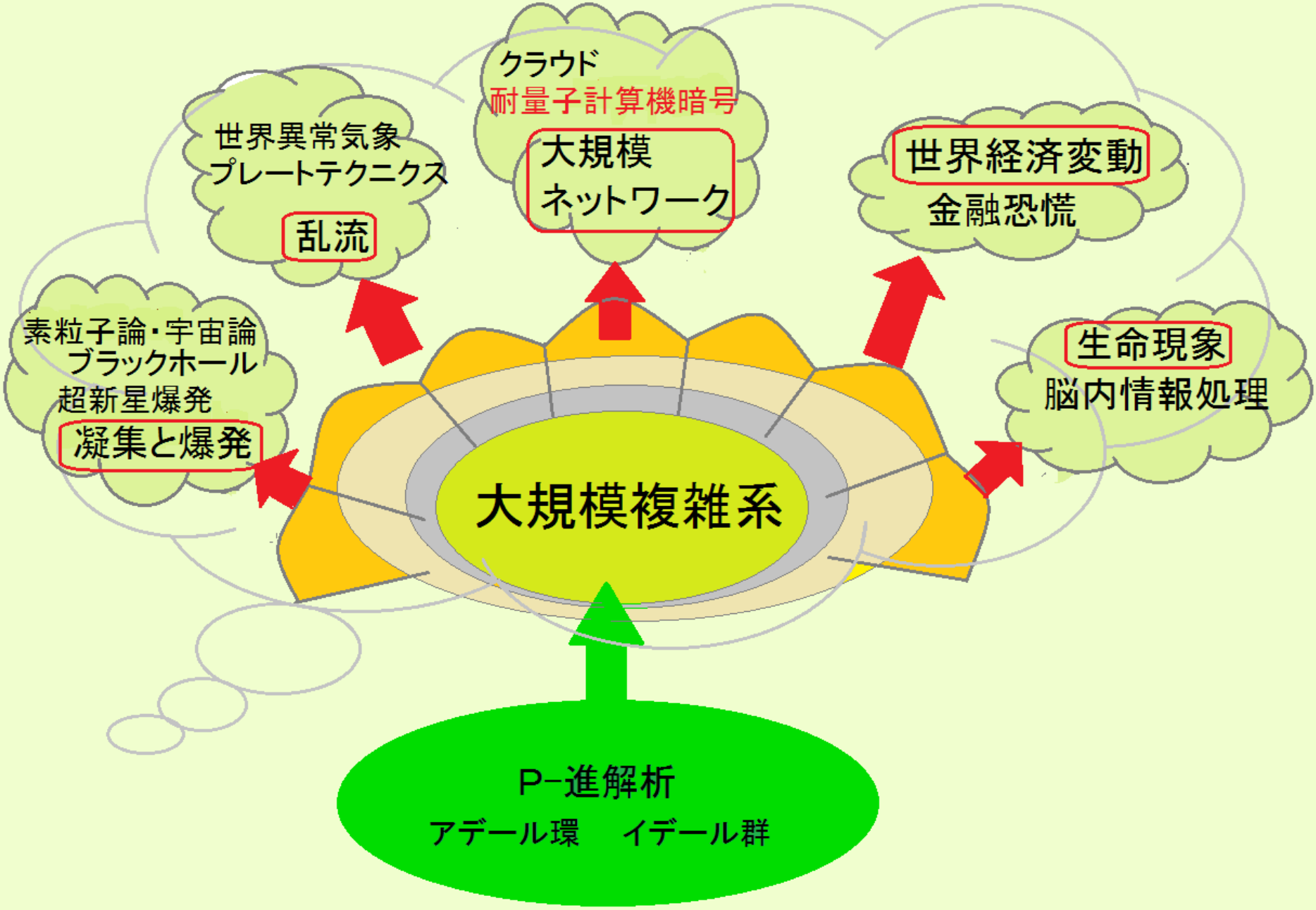
数論＋宇宙論、素粒子論のKey Word：

連分数展開、カオス、フラクタル、超弦理論
量子カオス、リーマン予想、…
→ p-進数

＊p-adic, continued fractions の検索：
「p-Adic Number Theory and Continued Fractions」
の索引： Matthew R. Watkins:
p-adic numbers and adeles - an introduction

⇒P-進数と数理物理；
V.S. Vladimirov, I.V. Volovich, E.I. Zelenov：
p-Adic Analysis and Mathematical Physics
(World Scientific, 1994)

⇒p-進解析：複雑系解析の数学的理論


クラウド
耐量子計算機暗号
大規模
ネットワーク
世界異常気象
プレートテクニクス
乱流
世界経済変動
金融恐慌
素粒子論・宇宙論
ブラックホール
超新星爆発
凝集と爆発
生命現象
脳内情報処理
大規模複雑系
P−進解析
アデール環　イデール群

Part II　p-進解析と耐量子計算機暗号

P-進数について：　SSH（2014）より抜粋

有理数の間に定義される「距離」は 2 種類だけ!!

「Ostrovski の定理」

(i) 絶対値 $|a-b|$

(ii) p-進絶対値: $|a-b|_p$　(p はある素数)

ある素数 p に対して、有理数 a は次のように表わされる；

$$a = \frac{n}{m} \times p^r \quad (m, n, r \text{は整数})$$

ただし、$\frac{n}{m}$ は既約分数で、n, m は p と互いに素。

$a = \frac{n}{m} \times p^r$ と表わされるとき、

a の p-進絶対値は、 $|a|_p = p^{-r}$ で定義される。

例. $|12|_2 = |3 \cdot 2^2|_2 = 2^{-2}$, $\left|\frac{4}{45}\right|_3 = \left|\frac{4}{5} \cdot 3^{-2}\right|_3 = 3^2$

(i) 絶対値 $|a-b|$ の距離で得られる有理数列の極限値が実数で、実数全体の集合を $\mathbb{R}$ で表わし、

(ii) p-進絶対値: $|a-b|_p$ の距離で得られる有理数列の極限値は p-進数と呼ばれ、p-進数全体の集合を $\mathbb{Q}_p$ で表わす。

有理数列 $\{a_n\}$ について

$$|a_n - \alpha|_p \to 0 \quad (n \to \infty)$$

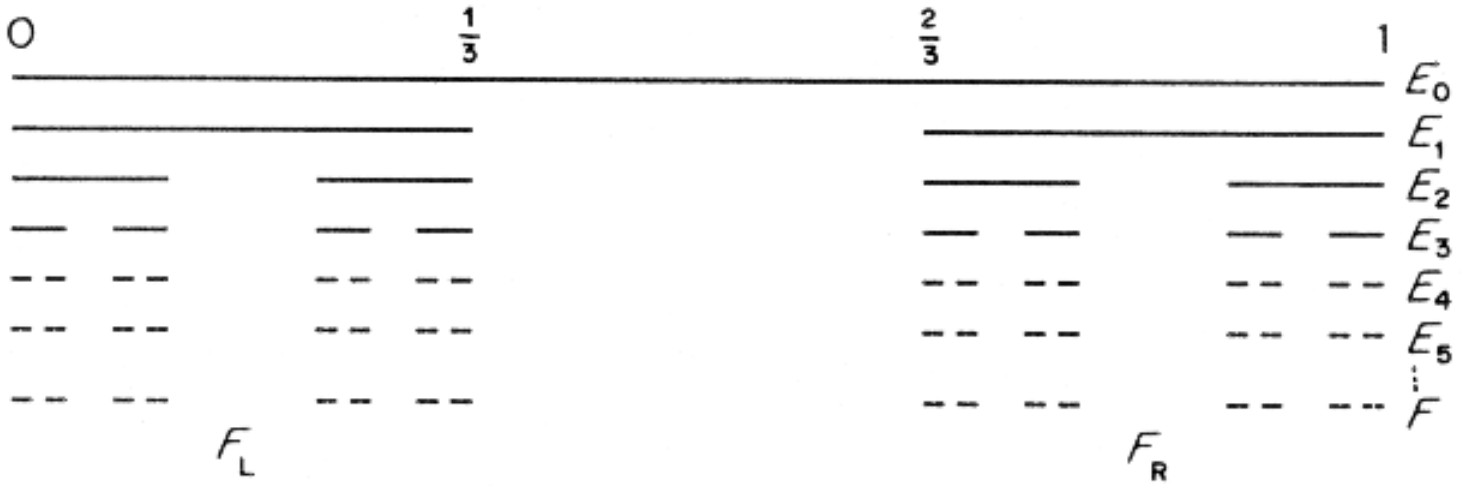
を満たす α が p-進数。

p-進整数の集合 $\mathbb{Z}_p$ は次で定義される。

$$\mathbb{Z}_p = \{z \in \mathbb{Q}_p : \ |z|_p \leq 1\}$$

p-進数の集合 $\mathbb{Q}_p$ は「カントール集合」と似た性質をもつ、
自己相似性をもったフラクタル集合：

カントール集合



非アルキメデス距離と非アルキメデス的性質

絶対値で与えられる距離は次の「三角不等式」を満たす：

$$|a+b| \leq |a| + |b|$$

p-進絶対値で与えられる距離は「強三角不等式」

$$|a+b|_p \leq \max\{|a|_p, |b|_p\}$$

を満たし、この性質を満たす距離は「非アルキメデス距離」、満たさない場合は「アルキメデス距離」と呼ばれる。

「非アルキメデス距離」満たす場合、次の「非アルキメデス的性質」が成り立つ；

a を p-進数とするとき、任意の整数 n に対して

$$|na|_p \leq |a|_p$$

「アルキメデス距離」では、次の「アルキメデス的性質」が成り立つ；

任意の有理数（実数でもよい）の組 $a, b : a \neq 0$ に対して、ある自然数 n を

$$|na| \geq |b|$$

を満たすようにとることができる。

「アルキメデス的性質」：どんなに微小な数量でも繰り返し加えあわせれば幾らでも大きい数量を構成できることが保証されている（限りなく微小な量も計測が可能）。

一方、「非アルキメデス距離」ではその性質は不成立 !!

プランクスケール：$1.616.. \times 10^{-33} m,\ 5.391.. \times 10^{-45}$ 秒の極微小世界では、「アルキメデス的性質」は成立しない !!

格子暗号:

・耐量子計算機暗号の最も有力な候補の一つ
・格子の最短ベクトル問題（SVP)の計算困難性が安全性の根拠
・NTRU暗号：唯一の実用化されている格子暗号
Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman：1996年に発表、
特許取得、2000年にNTRU Cryptosystems社設立

・Merkle-Hellmanナップサック暗号：1976年に発表、
ナップザック問題の計算困難性を利用、
種々の攻撃法が開発され、実用化はまだされてはいないが
現在も改良研究が継続されている。

・Commitment方式付P-進ナップザック暗号を提案(2016年)
P-adic Knapsack Cryptosystem with Commitment Schemes
by Hirohito Inoue(D3), Shoichi Kamada(M2) and K.N.

格子とLLL簡約基底について:

H24年度卒論(北野友里香)スライドより

格子とは

n 次元ユークリッドベクトル空間 $\mathbb{R}^n$ における

線形独立な n 個のベクトル $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}$ の全ての整数結合の集合

$$L(\mathbf{b_1}\mathbf{b_2}\ldots\mathbf{b_n}) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b_i} : x_i \in \mathbb{Z} \right\}$$

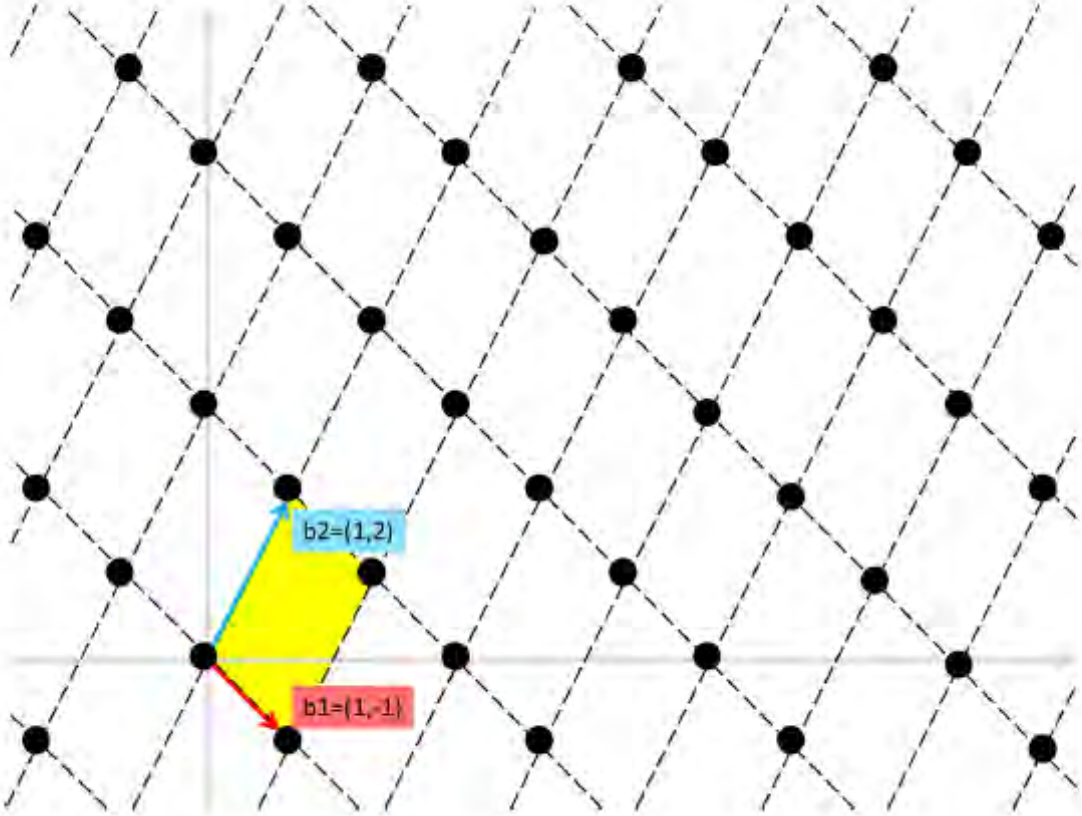
である。

ベクトルの列 $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}$ は「格子基底」と呼ばれ、行列 $\mathbf{B} = (\mathbf{b_1}\mathbf{b_2}\ldots\mathbf{b_n})$

と表し、格子を $L(\mathbf{B})$ と書く。

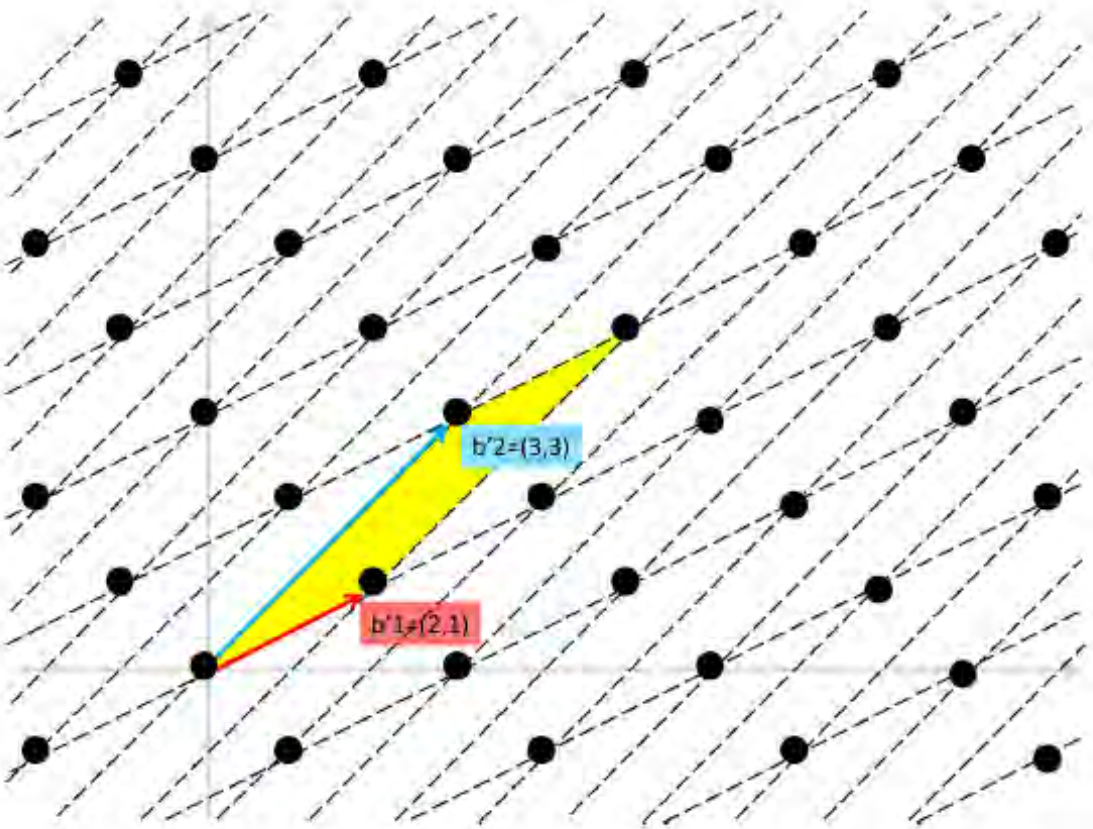
例 1 (2 次元における例)

$$L(\mathbf{B_1}) = L((\mathbf{b_1}\mathbf{b_2})) = L(\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix})$$



例 2

$$L(\mathbf{B_2}) = L((\mathbf{b'_1 b'_2})) = L(\begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \end{pmatrix})$$



最短ベクトル問題：SVP（shortest vector problem)

最短ベクトル問題とは、任意の格子 $\Lambda = L(\mathbf{B})$ の原点から非零格子点 $\mathbf{x}$ を結ぶベクトルのうち、最も長さの短いベクトルを見出す問題である。
ここでベクトルの長さは次のユークリッドノルムによる。

$$\|\mathbf{x}\| = \sqrt{\sum_{i=1}^{n} x_i^2}, \quad \mathbf{x} = (x_1 x_2 \ldots x_n).$$

最短ベクトルのノルムの値を $\lambda_1 = \min\{\|\mathbf{x}\| : \mathbf{x} \in L(\mathbf{B})\}$ とする。
最短ベクトルと一次独立なベクトルの中で、長さが最小なベクトルの値を λ_2 とする。高次元での最短ベクトル λ_1 を見出す多項式時間アルゴリズムは今日まで知られていない.

LLL格子簡約アルゴリズム

LLL 格子簡約アルゴリズムとは、n 次元格子の SVP を近似的に解くためのアルゴリズムで、任意に与えられた基底 $\mathbf{B}$ から δ でパラメータづけされた簡約基底を求めるアルゴリズムである。

1 次元でのユークリッドアルゴリズム（ユークリッドの互除法）の拡張
⇒ 2 次元での一般化ガウスアルゴリズム

ナップザック暗号

ナップザック暗号

公開鍵: $(a_1, a_2, \ldots, a_n)$, $a_i \in \mathbb{N}, i = 1, \ldots, n$

平文: $(x_1, x_2, \ldots, x_n)$, $x_i \in \{0, 1\}, i = 1, \ldots, n$

暗号文: $t = a_1x_1 + a_2x_2 + \ldots + a_nx_n$

ナップザック暗号の解読

公開鍵 $(a_1, a_2, \ldots, a_n)$ と暗号文 t が与えられたとき

$a_1x_1 + a_2x_2 + \ldots + a_nx_n = t$

を満足する解 $(x_1, x_2, \ldots, x_n)$ を見出す

公開鍵 $\{a_i\}$, $1 \leq i \leq n$ が **超増加列** のときナップザック暗号は簡単に解読される。超増加列は各数がそれまでの整数の和よりも大きい数列、

$$a_i > \sum_{k=1}^{i-1} a_k$$

を満たす数列 $\{a_i\}$ のことである。超増加列のときの解読法を以下に示す。

$t = a_1x_1 + a_2x_2 + \ldots + a_nx_n$

(1) $t > a_1 + \cdots + a_{n-1} \Rightarrow x_n = 1$

$t \leq a_1 + \cdots + a_{n-1} \Rightarrow x_n = 0$

(2) $t := t - a_nx_n > a_1 + \cdots + a_{n-2} \Rightarrow x_{n-1} = 1$

$t := t - a_nx_n \leq a_1 + \cdots + a_{n-2} \Rightarrow x_{n-1} = 0$

(3) 以下順に同じ操作を繰り返すことにより、$(x_1, \ldots, x_n)$ を得る。

そこで、超増加列 $\{a_i\}$ を超増加でない数列 $\{b_i\}$ に変換する。

$\{a_i\}, M, W \in \mathbb{N}$ を秘密鍵、次で定義される $\{b_i\}$ を公開鍵とする：

$$b_i \equiv W a_i \pmod{M}$$

但し、$M > a_1 + \cdots + a_n$, $\gcd(M, W) = 1$ とする。

暗号文は $C = b_1 x_1 + b_2 x_2 + \ldots + b_n x_n$ で与えられる。

暗号の受信者は M, W を使って $\{b_i\}$ から $\{a_i\}$ を次のように復元する。

$$\begin{aligned} C &= b_1 x_1 + b_2 x_2 + \ldots + b_n x_n \\ W^{-1} C &\equiv W^{-1} b_1 x_1 + W^{-1} b_2 x_2 + \ldots + W^{-1} b_n x_n \pmod{M} \\ &= a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = t \end{aligned}$$

$\{a_i\}$ は超増加列なのですぐに解読出来る。

LLL 攻撃

しかし超増加でない数列 $\{b_i\}$ を公開鍵としたナップザック暗号も、$n = 100 \sim 200$ くらいまでだと公開鍵 $\{b_i\}$ と暗号文 C だけで LLL アルゴリズムによって解読出来てしまう。LLL アルゴリズムを用いた解読法を以下に示す。

(1) 公開鍵 $\{b_i\}$ と暗号文 C を含む $(n+1) \times (n+1)$ 行列 $\mathbf{B}$ により、格子 $L(\mathbf{B})$ を考える。

$$\mathbf{B} = \begin{pmatrix} \mathbf{b}_1 & \mathbf{b}_2 & \cdots & \mathbf{b}_n & \mathbf{b}_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & & 1 & 0 \\ b_1 & b_2 & & b_n & -C \end{pmatrix}$$

(2) LLL アルゴリズムで格子 $L(\mathbf{B})$ の簡約基底 $\tilde{\mathbf{B}}$ を求める。

$\tilde{\mathbf{B}} = \begin{pmatrix} \tilde{\mathbf{b}}_1 & \tilde{\mathbf{b}}_2 & \dots & \tilde{\mathbf{b}}_n & \tilde{\mathbf{b}}_{n+1} \end{pmatrix}$ とする。

$\tilde{\mathbf{b}}_i = (\tilde{b}_1, \dots, \tilde{b}_{n+1})^t$, $\tilde{b}_k \in \{0,1\}$, $1 \le k \le n+1$ のとき、

$\tilde{\mathbf{b}}_i$ は最短ベクトルとなり、求める平文 $\tilde{\mathbf{b}}_i = (x_1, x_2, \dots, x_n, 0)$ である。

P-進ナップザック暗号：

2015 年暗号と情報セキュリティシンポジウム　講演スライドより

（発表者：井上裕仁）

強三角不等式や二等辺三角形法則などの p-進数の持つ特異な性質を利用したナップザック暗号方式を提案する。

p-進整数列 $\{a_1, a_2, \ldots, a_n\}$ が次の条件を満たすとき、p-進減少列であるという。

$$|a_1|_p > |a_2|_p > \cdots > |a_n|_p.$$

鍵生成

ボブは秘密鍵として p-進減少列となる n 個の p-進整数 $\{\eta_1, \ldots, \eta_n\}$ を選ぶ:

$$|\eta_1|_p > |\eta_2|_p > \cdots > |\eta_n|_p$$

さらに、$|\eta_n|_p > p^{-m}$ を満たす十分大きい整数 m に対して $\eta = (\eta_{1,m}, \ldots, \eta_{n,m}) \in \mathbb{Z}^n$ とおく。

ただし、各 $\eta_{i,m}$ は η_i の m 次近似であり、η の p-進展開 $\eta_i = \sum_{i=0}^{\infty} c_i p^i$ に対し、$\eta_{i,m} = \sum_{i=0}^{m-1} c_i p^i$ で与えられる。

秘密鍵

- p：素数
- m：近似度数
- $\eta = (\eta_{1,m}, \ldots, \eta_{n,m}) \in \mathbb{Z}^n$：$p$-進減少列
- q: $q > np^m$ を満たす十分大きい素数
- r：$\gcd(p, r) = 1$ を満たすランダムな整数
- s：q を法とする r の逆元

公開鍵

- $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$：$\beta_i = r\eta_{i,m} \pmod q$ で与えられる整数

暗号化

平文 $\mathbf{x} = (x_1, \ldots, x_n) \in \{0, 1\}^n$ に対し、アリスは暗号文 C を次のように計算しボブに送る。

$$C := \mathbf{x} \cdot \beta = \sum_{i=1}^{n} x_i \beta_i.$$

復号

ボブは暗号文 C を受け取り、C' を以下のように計算する。以下、表記を簡略化するため $\eta_{i,m}$ を η_i で表す。

$$C' \equiv Cs \equiv \sum_{i=1}^{n} x_i \eta_i \pmod{q}.$$

復号化では強三角不等式: $|x+y|_p \leq \max\{|x|_p, |y|_p\}$

と、それから導かれる次の二等辺三角形法則が利用される。

$$|x|_p \neq |y|_p \Longrightarrow |x+y|_p = \max\{|x|_p, |y|_p\}$$

η の p-進減少性と p-進絶対値における強三角不等式を利用して、通常の超増加性を持つ数列の場合と同様に以下のステップを行うことで、平文が得られる。

1st-step もし $|C'|_p = |\eta_1|_p$ ならば $x_1 = 1$ とし、そうでなければ $x_1 = 0$ とする。

2nd-step もし $|C' - x_1\eta_1|_p = |\eta_2|_p$ ならば $x_2 = 1$ とし、そうでなければ $x_2 = 0$ とする。

$\vdots$

nth-step もし $|C' - (x_1\eta_1 + \cdots + x_{n-1}\eta_{n-1})|_p = |\eta_n|_p$ ならば $x_n = 1$ とし、そうでなければ $x_n = 0$ とする。

上記の n 個のステップにより、ボブはアリスからのメッセージを正しく復号することができる。

p-進ナップザック暗号の利点

- Shamir(1982) の攻撃に対する耐性；
  超増加数列の代わりに p-進減少列を利用する。
- Lagarias 等の低密度攻撃 (1985) に対する耐性；
  密度 $d = \dfrac{n}{\log_2 p^m}$ に対して p, m の各値の調整による高密度化を利用する。
- 安全性の増大のため p, m も秘密鍵として利用可能。

P-adic Knapsack Cryptosystem with Commitment Schemes - Alice in p-adic wonder numberland –

"Simultaneous approximation problems of p-adic numbers and p-adic knapsack cryptosystems: Alice in p-adic numberland",

by Hirohito Inoue, Shoichi Kamada, Koichiro Naito,

p-Adic Numbers, Ultrametric Analysis and Applications, vol. 8 (2016) 掲載予定より

多次元 p-進近似格子と多重有理近似問題(SAP)

n を自然数とし、$\Xi = \{\xi_1, \xi_2, \ldots, \xi_n\}$ を p-進整数 n 個の組とする。
自然数 m に対し、p-進近似格子 Γ_m を次のように定義する。

$$\Gamma_m = \{(a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1} : |a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \leq p^{-m}\}.$$

この近似格子におけるベクトルの最小ノルム値 $\lambda_1^{(\infty)}(\Gamma_m)$ をディリクレの原理を用いることで次のように評価することができる。

$\mathbb{Q}$ 上で線形独立かつ無理数である n 個の p-進整数の組 $\Xi = \{\xi_1, \ldots, \xi_n\}$ と自然数 m に対し、

$$0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \leq p^{-m}, \quad (*)$$

$$\max_{0 \leq i \leq n} |a_{i,m}| \leq p^{\frac{m}{n+1}}$$

を満たす整数解 $(a_{0,m}, a_{1,m}, \ldots, a_{n,m}) \in \mathbb{Z}^{n+1}$ が存在する。このとき

$$\lambda_1^{(\infty)}(\Gamma_m) \leq p^{\frac{m}{n+1}} = \det(\Gamma_m)^{\frac{1}{n+1}},$$

が成立する。

$(*)$ を満たす整数解 $(a_{0,m}, a_{1,m}, \ldots, a_{n,m})$ を SAP 解という。

次に、LLLアルゴリズムを用いることにより、
数値的に求めたSAP解のノルムを評価する:

p-進整数 ξ_i が次の p-進展開

$$\xi_i = \sum_{k=0}^{\infty} x_{i,k} p^k, \ x_{i,k} \in \{0, 1, \ldots, p-1\}$$

を持つとき、 ξ_i の m 次近似 $\xi_{i,m}$ を

$$\xi_{i,m} = \sum_{k=0}^{m-1} x_{i,k} p^k$$

で定義する。

以下のようなベクトル $b_{0,m}, b_{1,m}, \ldots, b_{n,m} \in \mathbb{Z}^{n+1}$ を考える。

$$
\begin{aligned}
b_{0,m} &= (p^m, 0, \ldots, 0)^t, \\
b_{1,m} &= (\xi_{1,m}, -1, 0, \ldots, 0)^t, \\
b_{2,m} &= (\xi_{2,m}, 0, -1, 0, \ldots, 0)^t, \\
&\vdots \\
b_{n,m} &= (\xi_{n,m}, 0, \ldots, 0, -1)^t.
\end{aligned}
$$

$$
|\xi_{k,m} - \xi_k|_p \leq p^{-m}
$$

が成り立つので、任意の $k \in \{0, 1, \ldots, n\}$ に対して
$b_{k,m} \in \Gamma_m$ となり、一次独立性より格子 Γ_m の基底ベクトルとなる。

このベクトルを並べた行列 $B_m = (b_{0,m} b_{1,m} \dots b_{n,m})$ を考える。

$$B_m = \begin{pmatrix} p^m & \xi_{1,m} & \xi_{2,m} & \cdots & \xi_{n,m} \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -1 \end{pmatrix}.$$

行列 B_m の行列式の絶対値は $|\det(B_m)| = p^m$ である。

行列 B_m に対し、$\delta \in (1/4, 1)$ における LLL アルゴリズムを用いると簡約基底が得られ、これを $\{b_0, b_1, \dots, b_n\}$ とする。$B = (b_0\, b_1\, \dots\, b_n)$ とおく。

LLL 理論から導かれた不等式

$$\|b_0\|_2 \leq \sqrt{n}\ |\det(B)|^{\frac{1}{n}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n-1}$$

から、B の第一ベクトルに対して、次の評価が得られる。

$$\begin{aligned}
\|b_0\|_2 &\leq \sqrt{n+1}\ |\det(B)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n} \\
&= \sqrt{n+1}\ |\det(B_m)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n} \\
&= \sqrt{n+1}\ p^{\frac{m}{n+1}} \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n}.
\end{aligned}$$

一方、LLL アルゴリズムを用いた数値実験では、
n の値が小さいとき (∼60) には

$$\|b_0\|_\infty \leq p^{\frac{m}{n+1}}$$

が成立することが確かめられている。

p-adic numberland の導入

オープンソースソフトウエア Sage 上に暗号系を実装するため、
計算書式をもつp-進数の集合や関数を導入する:

素数 p, precision M (Sage 上で p-進数を表すときの精度)
に対して, $\mathbb{Z}_p^{(M)}$ を次の書式を持つ p-進整数 ξ の集合とする;

$$\xi = a_0 + a_1 p + a_2 p^2 + \cdots + a_{M-1} p^{M-1} + O(p^M)$$

素数 p, 近似度数 m, p-進整数 $\xi = \sum_{k=0}^{\infty} a_k p^k$ の三つ組み (p, m, ξ) に対して、有理整数値関数 $\mathrm{To\_int}(p, m, \xi)$ を次式で定義する；

$$\mathrm{To\_int}(p, m, \xi) = \sum_{k=0}^{m-1} a_k p^k := \xi_m \in \mathbb{Z}.$$

素数 p, 有理整数 $z = \sum_{k=0}^{l} b_k p^k$ の組 (p, z) に対し、p-進整数値関数 $\mathrm{To\_pad}(p, z)$ を次式で定義する；

$$\mathrm{To\_pad}(p, z) = \sum_{k=0}^{M-1} b_k p^k + O(p^M) \in \mathbb{Z}_p^{(M)},$$

ただし、 $b_k = 0$, $k \geq l + 1$ とする。

このとき、変換 $\mathrm{To\_int}(p, m, \xi), \mathrm{To\_pad}(p, z)$ が定義されている p-進数の集合 $\mathbb{Z}_p^{(M)}$ を、

$$\text{a } p\text{-adic numberland } \{p, m, M\}$$

と呼ぶ。

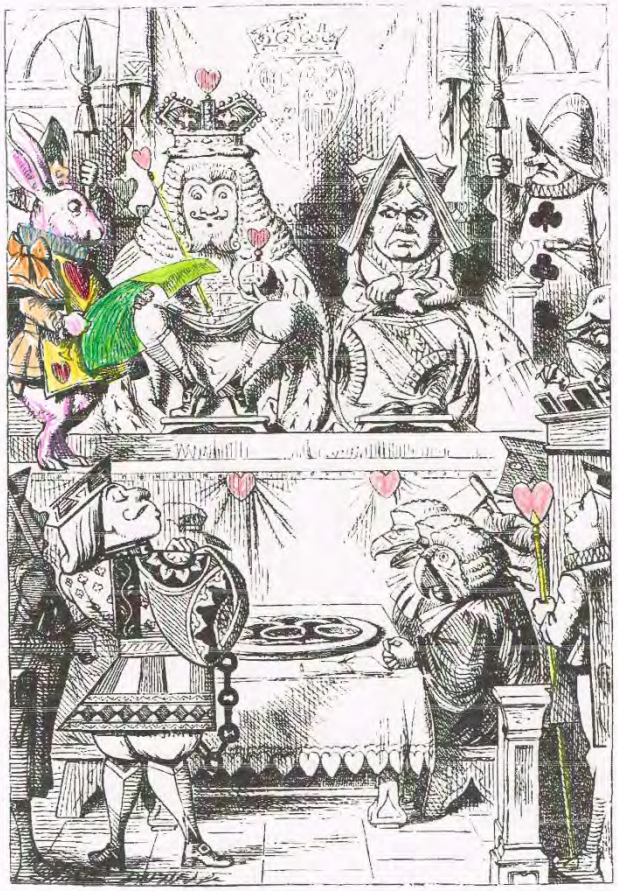
この暗号系では、

アリスには p-adic numberland $\{p_0, m_0, M_0\}$,

Bob（白ウサギ）には p-adic numberland $\{p, m, M\}$

を準備し、以降簡単のため、$M = M_0$ とする。

アリスの p-adic numberland $\{p_0, m_0, M\}$



Bob（白ウサギ）の p-adic numberland $\{p, m, M\}$

鍵生成

ボブは秘密鍵として次を満たす n 個の p-進整数 $\{\eta_1, \ldots, \eta_n\}$ を選ぶ；

$$|\eta_1|_p > |\eta_2|_p > \cdots > |\eta_n|_p$$

このとき、十分大きい整数 m に対して、$|\eta_n|_p > p^{-m}$ を満たすとする。
さらに、$\eta = (\eta_{1,m}, \ldots, \eta_{n,m}) \in \mathbb{Z}^n$ とおく。

ここで、各 $\eta_{i,m}$ は η_i の m 次近似：$\eta_i = \sum_{i=0}^{\infty} c_i p^i$ に対し、

$$\eta_{i,m} = \mathrm{To\_int}(p, m, \eta_i) = \sum_{i=0}^{m-1} c_i p^i$$

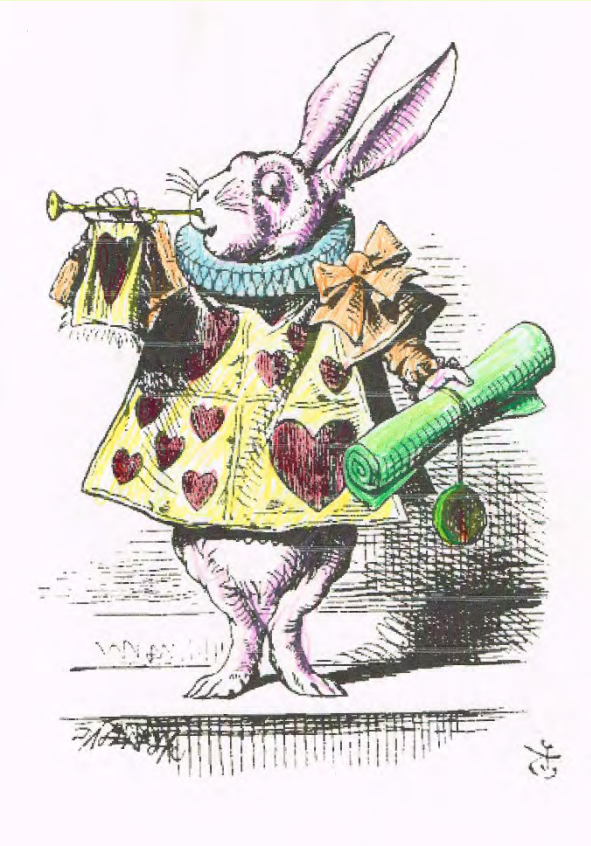
Bob の秘密鍵

- p : 素数
- m : 近似度数
- $\eta = (\eta_{1,m}, \ldots, \eta_{n,m}) \in \mathbb{Z}^n$: p-進減少列
- q : $q > np^m$ を満たす素数
- r : $\gcd(p, r) = 1$, $q < rp^m$ を満たすランダムな整数
- s : q を法とする r の逆元

Bobの公開鍵

$$\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n:$$

$$\beta_i \equiv r\eta_{i,m} \pmod{q}$$



Aliceの鍵生成

アリスは公開鍵 $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ から一つ： β_{k_0} を選択し、そのべき乗列を作る：

$$\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n) \in \mathbb{Z}^n, \quad \gamma_i = \beta_{k_0}^i, \ i = 1, \ldots, n.$$

次に、それらを p-進数に変換し（$\{p_0, m_0, M\}$ で）：

$$\xi_i = \mathrm{To\_pad}(p_0, \gamma_i), \quad i = 1, \ldots, n,$$

その m_0-近似 $\xi_{m_0} = (\xi_{1,m_0}, \cdots, \xi_{n,m_0})$:

$$\xi_{i,m_0} = \mathrm{To\_int}(p_0, m_0, \xi_i) \in \mathbb{Z}, \quad i = 1, \ldots, n$$

を作成する。

$\xi_{m_0} = (\xi_{1,m_0}, \cdots, \xi_{n,m_0})$ により定義される多次元近似格子を、適宜分割し（各次元が 60 以下）、LLL アルゴリズムにより各格子における SAP 解を求め、結合した解 $(a_0, a_1, ..., a_n) \in \mathbb{Z}^n$ を秘密鍵とする。強三角不等式より

$$|\sum_{i=0}^{n} a_i \xi_{i,m_0}|_{p_0} \leq p_0^{-m_0}, \quad \max_i |a_i| \leq K$$

（$\xi_0 = \xi_{0,m_0} = 1$ としている）が成立する。

$\{a_i\}$ をランダムに分割し、

$$a_i = \sigma_i + \rho_i, \ \sigma_i, \rho_i \in \mathbb{Z} : \ |\sigma_i|, |\rho_i| \leq K, \quad i = 0, 1, ..., n.$$

$\{\sigma_i\}$ をアリスの秘密鍵、
$\{\rho_i\}$ をアリスの認証鍵 (verification or opening key) とする。

暗号化

メッセージ文 $\mathrm{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$ に対し、アリスは暗号文 C を作成する：

$$C = \sum_{i=0}^{n} \sigma_i \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i.$$

1st stage:

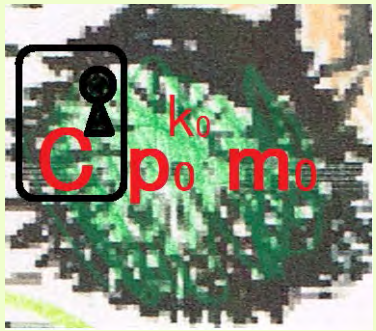
アリスは通信文 $(C, p_0, m_0.k_0)$ を Bob に送る。
Bob は不等式条件 $q < p_0^{m_0}$ をチェックし、

もし、満たされていれば； 数値 0 をアリスに返す。
満たされていなければ、 次の非零整数値 d：

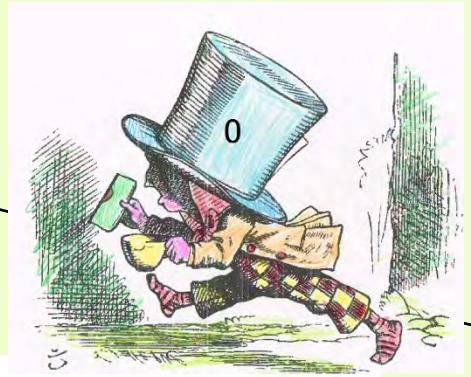
$$d = \min\{d' \in \mathbb{Z}_{>0} : q < p_0^{m_0+d'}\}$$

を返す。

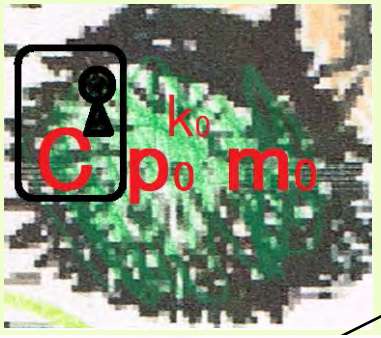
$(C, p_0, m_0.k_0)$



0



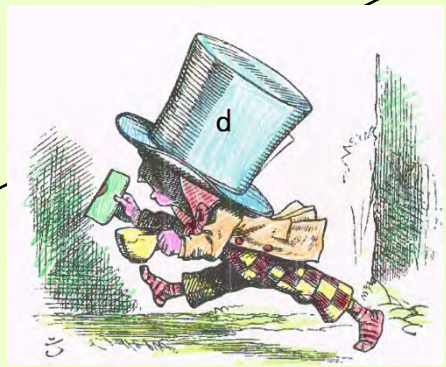
$(C, p_0, m_0.k_0)$



$q < p_0^{m_0}$

$q \geq p_0^{m_0}$

d



$$d = \min\{d' \in \mathbb{Z}_{>0} : q < p_0^{m_0+d'}\}$$

2nd stage:

アリスは 0 を受けた時は、認証鍵（開封鍵）$\{\rho_i\}$ を Bob に送る。

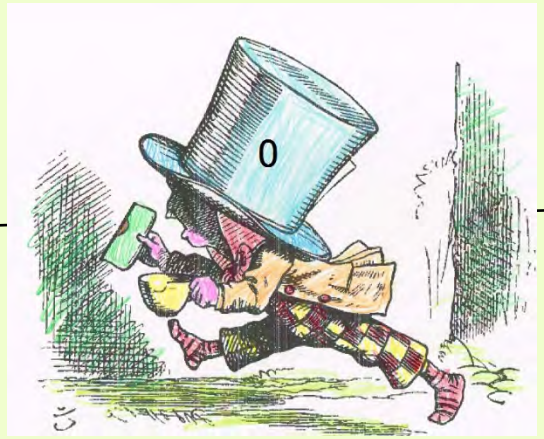
$d(>0)$ を受けた時は、次式を満たす小さな整数の組

$$(c_0, d_0) \in \mathbb{Z}^2_{\geq 0}: \ p_0^{m_0+d} < (p_0+c_0)^{m_0+d_0}, \ \ p_0+c_0 : \text{prime}$$

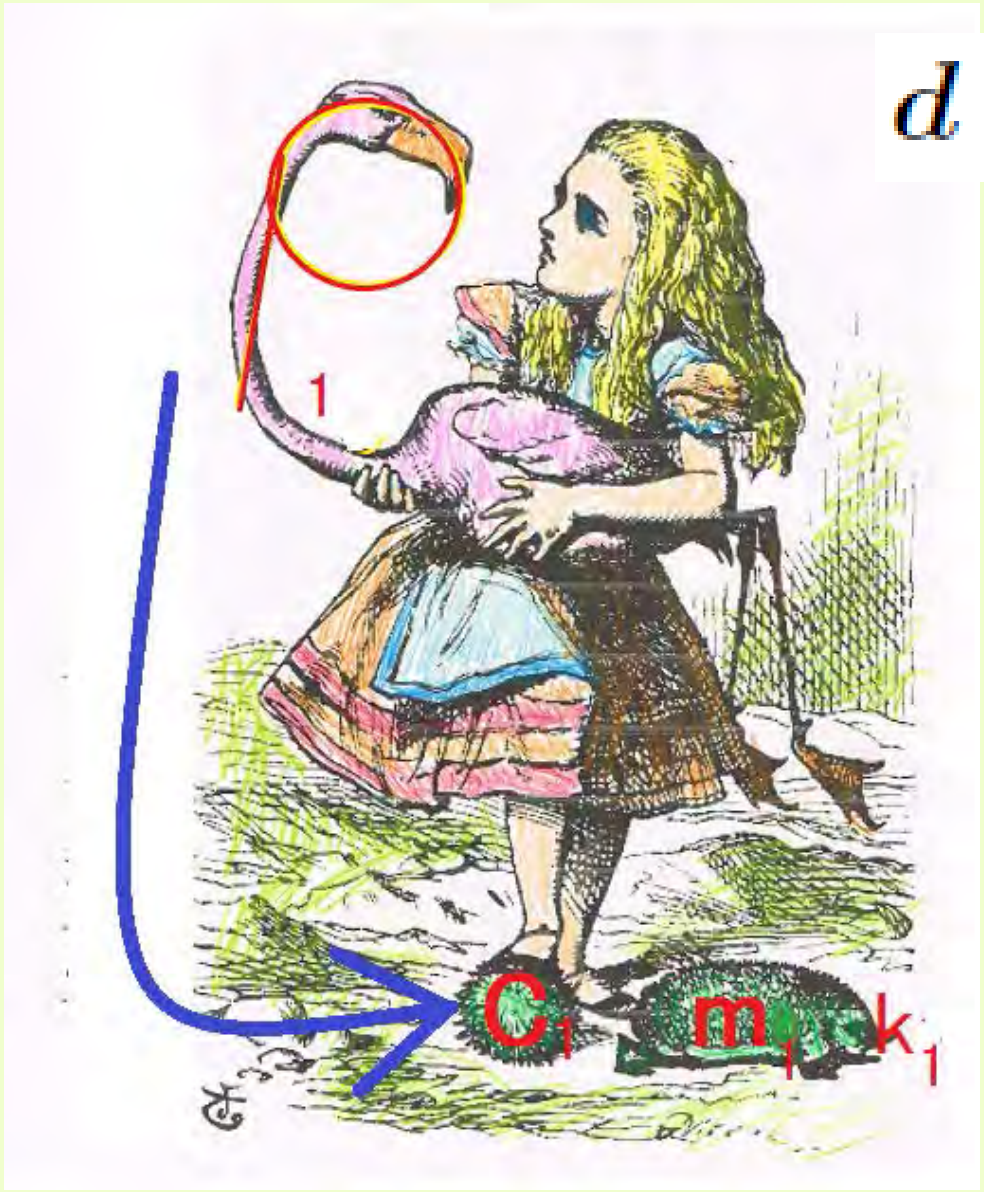
を選び、$p_1 = p_0 + c_0$, $m_1 = m_0 + d_0$ とし、
暗号文 C_1 を新たな p-adic numberland $\{p_1, m_1, M\}$ で再構成し、
通信文 (C_1, p_1, m_1, k_1) を Bob へ送る。

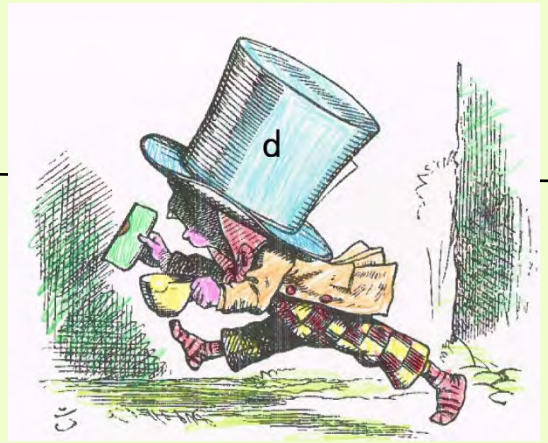
3rd stage:

アリスは 0 を受けた後、新たな p-adic numberland $\{p_1, m_1, M\}$ で作成した認証鍵（開封鍵）$\{\rho'_i\}$ を Bob に送る。



$\{\rho_i\}$





(C_1, p_1, m_1, k_1)

3rd stage

$\{\rho_i'\}$

復号化

アリスが 2nd stage で 0 を受け、$\{\rho_i\}$ を Bob に送った場合；

アリスの開封鍵 $p_0, m_0, k_0, \{\rho_i\}$ を利用して、
Bob は p-adic numberland $\{p_0, m_0, M\}$ で、
ξ_{i,m_0} を変換 To_int and To_pad で作成する：

$$\xi_i = \text{To\_pad}(p_0, \beta^i_{k_0}) \in \mathbb{Z}_p, \quad i = 1, .., n$$

さらに、

$$\xi_{i,m_0} = \text{To\_int}(p_0, m_0, \xi_i) \in \mathbb{Z}, \quad i = 1, .., n.$$

Bob は次の C' を計算する：

$$C' := C + \sum_{i=0}^{n} \rho_i \xi_{i,m_0} = \sum_{i=0}^{n} a_i \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i.$$

$\bmod p_0^{m_0}$ をとり、次の C'' を計算する：

$$C'' := \sum_{i=1}^{n} x_i \beta_i \equiv C' \pmod{p_0^{m_0}}.$$

Bob の秘密鍵 s により、 次の C''' を計算する：

$$C''' := \sum_{i=1}^{n} x_i \eta_i \equiv sC'' \pmod{q},$$

ここでは、$q < p_0^{m_0}$ の関係を利用。

C''' より、Bob はアリスのメッセージを先に紹介した p-進ナップザック暗号の場合と同様にして、step-by-step 方式で復号できる。

1st-step:
If $|C'''_p|_p = |\eta_1|_p$, then $x_1 = 1$, otherwise $x_1 = 0$.

2nd-step:
If $|C'''_p - x_1\eta_1|_p = |\eta_2|_p$, then $x_2 = 1$, otherwise $x_2 = 0$.

$\vdots$

nth-step:
If $|C'''_p - (x_1\eta_1 + \cdots + x_{n-1}\eta_{n-1})|_p = |\eta_n|_p$, then $x_n = 1$, otherwise $x_n = 0$.

以上の n ステップで、Bob はアリスのメッセージ x を復号する。


Good luck!
Alice

今後の課題

耐量子計算機暗号理論の分野で現在最も注目を集めている研究はネットワーク･クラウドに代表される多送信者-多受信者間における暗号通信の安全性の解析である。

このため、p-進数体の積空間であるアデール環やイデール群上の p-adic numberland の構成と暗号解析が重要な研究課題となると予想している。

←――― こんなことが起こらないように！

長い間大変お世話になりました。特に、この10年間、数理工学科の運営にご尽力いただいた全教員,職員の皆様方の暖かいご支援に
心より感謝申し上げます。