2002/1/26 JANT

格子基底縮小とその応用

㈱東芝　研究開発センター

清水 秀夫

内容

- ＬＬＬアルゴリズムの紹介
- 最新の研究動向／成果
  （トピックの紹介）

ＬＬＬアルゴリズムの概要

- 1982年 A.K.Lenstra, H.W.Lenstra,Jr., L.Lovasz
- **格子基底縮小** (lattice basis reduce) **アルゴリズムの一種**
- **格子に含まれる最短ベクトルを求める問題の近似解を求めるアルゴリズム (基底変換アルゴリズム) 。**
- **近似の精度と実行時間 (多項式時間) が証明されている。**
- **現実には理論で示されている結果よりかなりよく動くことが実験により示されている。**
- **基本的なツールであり、暗号分野における様々な応用が示されている。**
- **優秀なフリーソフト**NTL (http://www.shoup.net/NTL/)

“Factoring Polynomials with rational coefficients,” Math.Ann.,261,513-534, 1982

格子(lattice)

定義

$b_1, b_2, \ldots, b_n \in \mathbf{R}^n$が線形独立のとき

$$L = z_1 b_1 + z_2 b_2 + \cdots + z_n b_n, (z_i \in \mathbf{Z})$$

を格子という。$B = \{b_1, b_2, \ldots, b_n\}$を基底という。

性質

- **同じ格子を張る別の基底が無限に存在する**
- **基本行操作した規定も同じ格子を張る**

$$L(B) = L(UB), U \in GL^n$$

- **同じ格子を張る基底の** $d(L) = \left|\det(B)\right|$ **は同じ値を取る。**

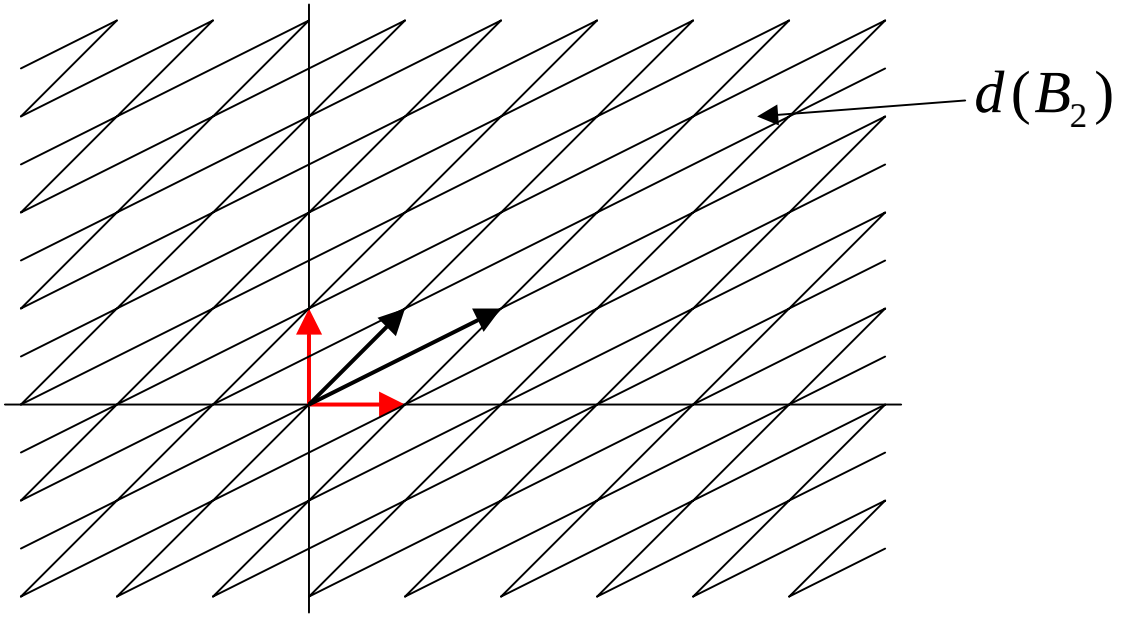
$$L(B) = L(B') \Rightarrow d(B) = d(B')$$

格子の例

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B_2 = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

$$L(B_1) = L(B_2)$$
$$d(B_1) = d(B_2) = 1$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$



格子に関する問題

ＳＶＰ(shortest vector problem)

格子が与えられて（基底ベクトルが与えられて）、
格子に含まれる最短ベクトルを求める問題

$$\lambda_1(L) \le \sqrt{n}\, d(L)^{1/n}$$

ＣＶＰ(closest vector problem)

格子と任意のベクトルx**が与えられて**
格子に含まれるx**に最も近いベクトルを求める問題**

ＳＢＰ(smallest basis problem

格子が与えられて
最も「小さな」基底ベクトルを求める問題
※「小さな」の意味は問題によって変わる

縮小基底

Gram-Schmidt**の直交化過程**

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*$$

$$\mu_{ij} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)}$$

(·,·)は内積

縮小基底(LLL-reduced basis)

$$\left|\mu_{ij}\right| \le \frac{1}{2}, \ 1 \le j < i \le n \qquad (\textbf{条件}1)$$

$$\left\|b_i^*\right\|^2 \ge \left(\frac{3}{4} - \mu_{ii-1}^2\right)\left\|b_{i-1}^*\right\|^2, \ 1 < i \le n \qquad (\textbf{条件}2)$$

縮小基底の性質

$$(1)\forall x \in L, \|b_1\| \le 2^{(n-1)/2}\|x\|$$

$$(2)\forall x_1, x_2, \ldots, x_t \in L, \|b_j\| \le 2^{(n-1)/2} \max\left(\|x_1\|, \|x_2\|, \ldots, \|x_t\|\right)$$

$$\text{for} 1 \le j \le t,\ x_1, x_2, \ldots, x_t \text{は線形独立}$$

$$(3)\|b_1\| \le 2^{(n-1)/4} d(L)^{1/n}$$

$$(4)d(L) \le \prod_{i=1}^{n} \|b_i\| \le 2^{n(n-1)/4} d(L)$$

LLL**アルゴリズム**(Lenstra, Lenstra, Lovasz, 1982)

縮小基底を見出す多項式時間アルゴリズムが存在する

LLLアルゴリズムの概要

入力：$b_1, b_2, \ldots, b_n$
出力：**縮小された** $b_1, b_2, \ldots, b_n$

(1)$b_1, \ldots, b_{k-1}$は条件1と条件2を満足する

(2)b_kを条件1を、満足するように修正する

(3)b_kが条件(2)を満足するなら$k = k + 1$として(1)へ行く
　($k \geq n$なら終了する)

(4)b_kとb_{k-1}を入れ替え、$k = k - 1$として(1)へ行く

- **停止することは証明されている**(LLL 1982)
- **計算量は** $O\left(n^4 \log B\right), B = \max \left\| b_i \right\|^2$

LLLアルゴリズムの例

$$B = \begin{pmatrix} 105 & 821 & 404 & 328 \\ 881 & 667 & 644 & 927 \\ 181 & 483 & 87 & 500 \\ 893 & 834 & 732 & 441 \end{pmatrix} \begin{matrix} \|b_1\| = 977.68\cdots \\ \|b_2\| = 1579.59\cdots \\ \|b_3\| = 723.61\cdots \\ \|b_4\| = 1491.07\cdots \end{matrix}$$

$$d(B) = 6918837099$$

$$d(B)^{1/4} = 512.87\cdots$$

$$2^{(4-1)/4} d(B)^{1/4} = 862.54\cdots$$

$$B' = \begin{pmatrix} 88 & -171 & -229 & -314 \\ 269 & 312 & -142 & 186 \\ 76 & -338 & -317 & 172 \\ 519 & -299 & 470 & -73 \end{pmatrix} \begin{matrix} \|b_1'\| = 433.61\cdots \\ \|b_2'\| = 473.77\cdots \\ \|b_3'\| = 500.09\cdots \\ \|b_4'\| = 764.84\cdots \end{matrix}$$

NTLを使ったコーディング例

プログラム

```
#include <NTL/LLL.h>

main()
{
        mat_ZZ b;           整数行列の宣言

        cin >> b;           入力
        LLL_FP(b);          浮動小数点LLL
        cout << b << "¥n";  出力
}
```

※http://www.shoup.net/ntl/
windows/unixのフリーソフト(GPL)
C++, GMP対応

入力ファイル

```
[
 [105 821 404 328]
 [881 667 644 927]
 [181 483  87 500]
 [893 834 732 441]
]
```

出力ファイル

```
[[88 -171 -229 -314]
[269 312 -142 186]
[76 -338 -317 172]
[519 -299 470 -73]
]
```

格子（ＬＬＬ）に関係する研究

格子に関する研究

- **格子に含まれる最短ベクトルの長さの上界／下界**
- Geometries of numbers**と呼ばれる分野の数学**

格子に関する問題（SVP, CVP, SBP）**の計算量に関する研究**

- lattice**暗号**（Ajtai-Dwork**暗号**）

格子基底縮小アルゴリズムの改良に関する研究

- C.P.Schnorr**による一連の研究**
  （Blockwise Korkine-Zolotarev **アルゴリズム**, segment LLL）
- Kannan**のアルゴリズム**

格子基底縮小アルゴリズムの応用（→後半の話題）

- **暗号の解読等**

計算量理論の成果

長い間の未解決問題

- SVPはNP困難。(Ajtai, STOC 1998)
- 近似SVP (大きさf(n)λ$_1$以内のベクトルを見つける)について、近似<$2^{1/2}$もNP困難。(Micciancio, FOCS 1998)
- 近似$(n/O(\log n))^{1/2}$はNP困難ではない。(Goldreich, Goldwasser, STOC 1998)
- SVP (CVP) を多項式近似できるアルゴリズムは知られていない。
- ∞ノルムに関する結果、SVP∞はNP困難 (P. van Emde Boas, 1981)
- Ajtaiの成果。Average caseとworst caseが一致する格子に関する問題 (n^c-SVP) の発見 (1996)

※LLLは近似$=2^{(n-1)/2}$の多項式時間アルゴリズム

Ajtaiの結果のインパクト

n^c-SVPに関してworst caseからaverage caseへの reductionを証明した。

- Pの外のNPでは初めて
- たとえworst caseで困難でもaverage caseで 困難かどうか分からないという問題を解決した。
- 真の証明可能安全性への道を開いた。

Ajtai-Dwork暗号（STOC 1997)

- 理論的な暗号
- 漸近的な結果なのでパラメータが小さい時は解ける （Nguyen, Stern, C98） n≧32 → 公開鍵≧20Mバイト（impractical）

格子基底縮小アルゴリズムの改良

LLL

- **近似精度の改良**
  - $2^{O(n(\log\log n)^2/\log n)}$ Schnorr (1987)
  - **実行時間**$O(2^n)$ Kannan (STOC 1983)
- **速度の向上**
  - serial
    - BKZ Schnorr(1994, C95)
    - segment LLL Schnorr(2002, Calc01)
  - parallel
    - Wetzel (ANTS III 1998)
    - **他**
  - ad hoc
    - **整数版、浮動小数点版、**deep insertion (Cohen)

segment LLL

- C.P.Schnorrら(Calc01)
- **計算量** $O(n^3 \log n)$
- 1000**次元以上にも適用可能**
  (LLL**は**100**次元程度まで**?)
- 1000**次元で**10**時間程度**(800MHz PC)

ＬＬＬの応用

- 暗号への攻撃
  - ナップザック暗号への攻撃
  - lattice暗号への攻撃
  - 他
- 法多項式の求解
  - 一変数、多変数
  - 応用
- 素因数分解への応用
- 代数的整数論
- その他

LLLの応用(その1)

- **多項式の因数分解**(LLL 82)
- **ナップザック暗号に対する低密度攻撃**(Brickell C83)
- Mental Poker(Shamir**他**79)**への攻撃**(Coppersmith C84)
- Low exponent RSA**への攻撃**(Hastad C85, SIAM J.Comp 88)
- **ナップザック暗号に対する低密度攻撃**(Lagarias**他** JACM85)
- ESIGN**への攻撃**(Vallee**他** E88)
- e**乗根近似問題への適用**(Vallee**他** AAEEC-6 88)
- truncated congruence generator**の解読**(Frieze**他** SIAM J.Comp88)
- **有理数暗号**(Isselhorst E89)**への攻撃**(Stern**他** E90)
- modular knapsack(Niemi E90)**への攻撃**(Chee C91,Joux**他** A91)
- **低密度攻撃の改良**(Coster**他** E91)
- Diophantine**近似を使った素因数分解**(Schnorr E91)
- **小林-田村-藤波暗号の解読**(**清水**, **林** 93)
- knapsack hash(Damgard C89)**への攻撃**(Joux E94)
- Number Field Sieve**への応用**(Montgomery Math.Comp.94)

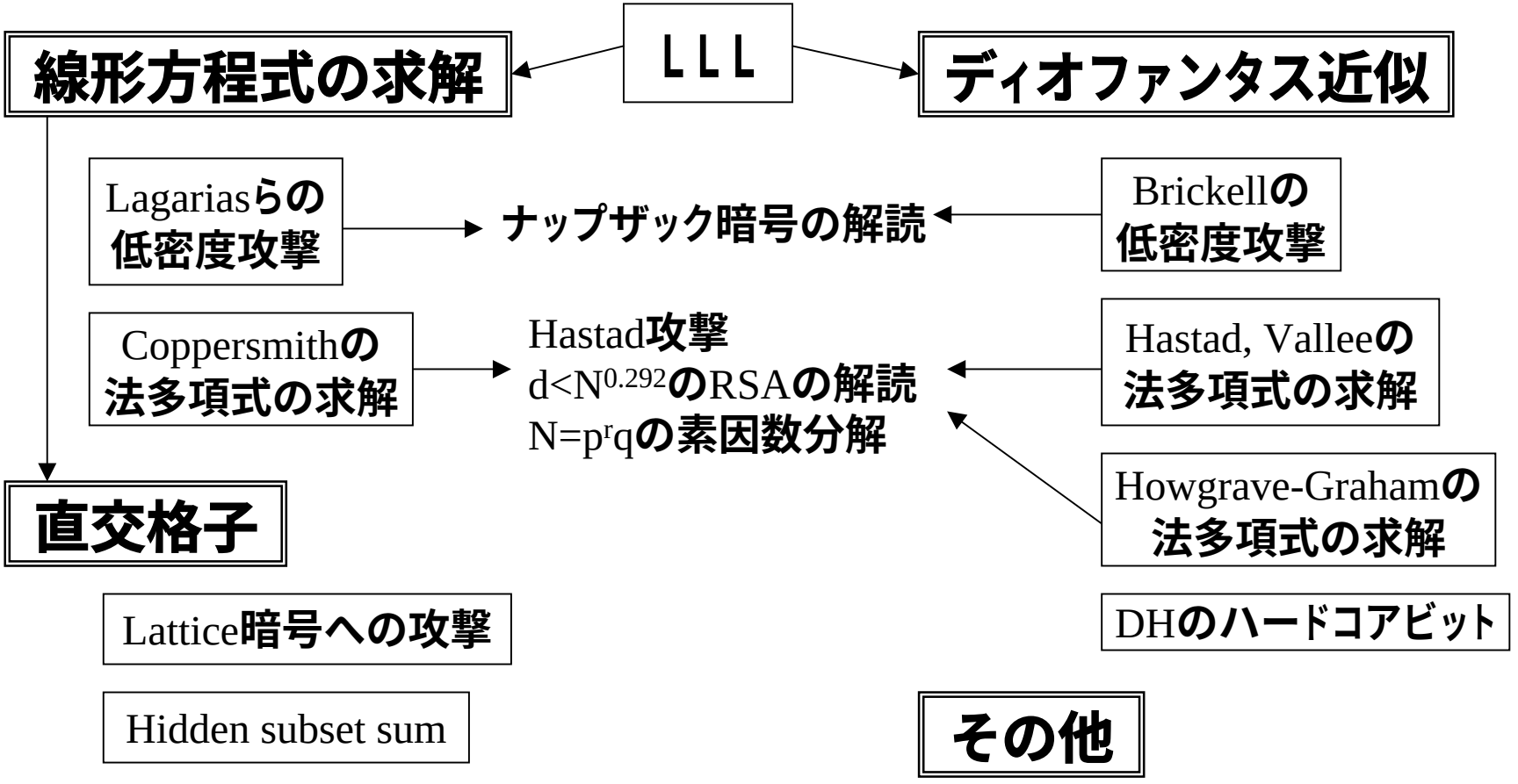
LLLの応用(その2)

- Chor-Rivest暗号(Chor他 IT88)への攻撃(清水, 林 94)
- Chor-Rivest暗号(Chor他 IT88)への攻撃(Schnorr他 E95)
- 1変数法多項式の求解(Coppersmith E96, JC97)
- 多変数法多項式の求解(Coppersmith E96, JC97)
- Diffie-Hellmanのハードコアビット(Boneh他 C96)
- Hastad boundの改良(清水 96)
- 一方向性関数の提案(Buchmann他 C97)
- ISO/IEC9796-3署名への攻撃(Misarsky C97)
- Qu-Vanstone暗号への攻撃(Nguyen他 C97)
- NTRU暗号(Hoffstein他C96)への攻撃(Coppersmith他 E97)
- Coppersmithアルゴリズムの改良(Howgrave-Graham CCS97)
- 超楕円暗号のJacob和を求める(Buhler他 97)
- Number Field Sieveへの応用(Nguyen, ANTS III 98)
- Ajtai-Dwork暗号の解析(Nguyen他 C98)

ＬＬＬの応用（その3）

- **多変数多項式の求解**（Julta E98）
- **伊藤,岡本,満保暗号**（SAC97）**の解読**（Nguyen**他** SAC98）
- $N=p^rq$**の素因数分解**（Boneh**他** C99）
- GGH**暗号**（Goldreich**他**C97）**の解読**（Nguyen C99）
- Hidden subset sum**問題への適用**（Nguyen**他** C99）
- $d<N^{0.292}$**の**RSA**の解読**（Boneh**他** E99）
- **笠原-村上暗号への攻撃**（**清水** ISEC99）
- Noisy Polynomial**の補間**（Bleichenbacher**他** E00）
- **素因数分解への応用**（Boneh STOC00）
- two-third method（Vallee**他** Math.Comp.??）

LLLの応用とテクニック



ナップザック暗号の解読（1）

ナップザック暗号

公開鍵：**整数**$a_1,a_2,\ldots,a_n$
平文：$m_1,\ldots,m_n \in \{0,1\}$
暗号化：$a_1m_1+\cdots+a_nm_n = C$

ナップザック暗号の解読
（公開鍵と暗号文から平文を求める）

整数$a_1,a_2,\ldots,a_n$**と**C**が与えられて**

$$a_1x_1+\cdots+a_nx_n = C$$

を満足する解$x_1,x_2,\ldots,x_n \in \{0,1\}$**を見出す。**

※100～200**次元くらいまで解ける**

ナップザック暗号の解読（2）

- $a_1x_1+\cdots+a_nx_n = C$の解を含む格子を考える
- LLLアルゴリズムで短いベクトルを求める

$b_1 = (1, 0, \ldots, 0, a_1)$
$b_2 = (0, 1, \ldots, 0, a_2)$
$\cdots$
$b_n = (0, 0, \ldots, 1, a_n)$
$b_{n+1} = (0, 0, \ldots, 0, C)$

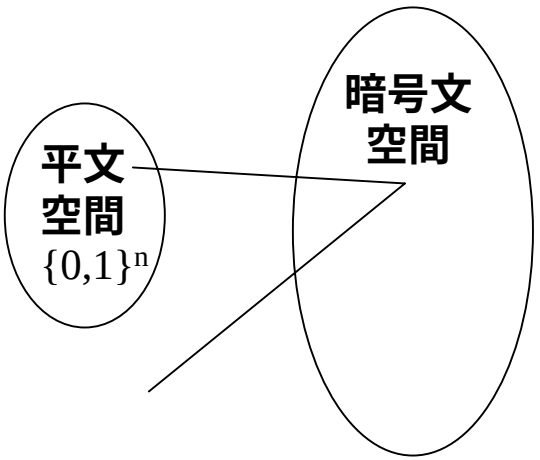
$x_1b_1+\cdots+x_nb_n+x_{n+1}b_{n+1} = (x_1, \ldots, x_n, a_1x_1+\cdots+a_nx_n+x_{n+1}C)$
なので最終要素$= 0$ かつ $x_{n+1} = -1$のとき
$x_1, \ldots, x_n$は$a_1x_1+\cdots+a_nx_n = C$を満足する。

問題となるのは$(x_1, \ldots, x_n) \in \{0, 1\}^n$となるかどうか

ナップザック暗号の解読（3）

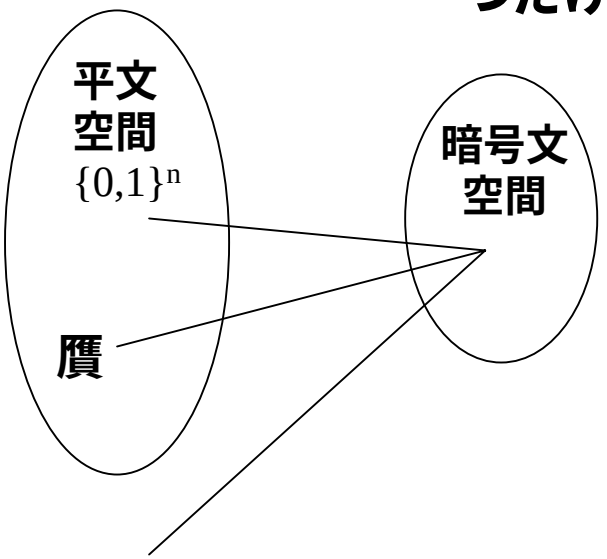
密度 ρ = n / (max a_i)
= **平文空間の広さ／暗号文空間の広さ**

ρ < 1



ρ > 1

複数の平文のうちの一つだけが真の平文



SVP**オラクルを仮定すると ρ** < 0.6463**まで解ける**（Lagarias**他**）。
CVP**オラクルを仮定すると ρ** < 0.9408**まで解ける**（Coster**他**）。

NTRUへの攻撃(1)

NTRUの特徴

•J.Hoffstein, J.Pipher, J.H.Silverman, 1996

•多項式環上の公開鍵暗号

•暗号化／復号が比較的高速

•現在知られている最も効率的な攻撃は

lattice reduction(Coppersmith,Shamir 1997)

•http://www.ntru.com/ (http://www.ntru.co.jp/)

NTRUへの攻撃(2)

鍵生成　公開情報 $n, p, q \in \mathbf{Z}, h \in \mathbf{Z}_q[x]/x^n - 1$

秘密情報 $f, g \in \mathbf{Z}_p[x]/x^n - 1$

(1) $(p, q) = 1, q > p$

(2) $f^{-1} \bmod p, x^n - 1$と$f^{-1} \bmod q, x^n - 1$が存在する

(3) $h = pf^{-1}g \pmod{q, x^n - 1}$

例　$n = 11, p = 3, q = 32$

$$f = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10} \in \mathbf{Z}_3[x]/x^{11} - 1$$

$$g = -1 + x^2 + x^3 + x^5 - x^8 - x^{10} \in \mathbf{Z}_3[x]/x^{11} - 1$$

$$h = pf^{-1}g = 5 + 9x + 6x^2 + 16x^3 + 4x^4 + 15x^5 + 16x^6 + 22x^7 + 20x^8 + 18x^9 + 30x^{10} \pmod{32, x^{11} - 1}$$

NTRUへの攻撃(3)

暗号化

平文$m \in \mathbf{Z}_p[x]/x^n - 1$

乱数$r \in \mathbf{Z}_q[x]/x^n - 1$

暗号文$e \in r \in \mathbf{Z}_q[x]/x^n - 1$

暗号化$e = m + rh (\mathrm{mod}\, q, x^n - 1)$

例

$$m = -1 + x^3 - x^4 - x^8 + x^9 + x^{10}$$

$$r = -1 + x^2 + x^3 + x^4 - x^5 - x^7$$

$$e = m + rh = 14 + 11x + 26x^2 + 24x^3 + 14x^4 +$$

$$16x^5 + 30x^6 + 7x^7 + 25x^8 + 6x^9 + 19x^{10} (\mathrm{mod}\, 32, x^{11} - 1)$$

NTRUへの攻撃(3)

復号

$$a = fe \pmod{q, x^n - 1}$$

$$b = a \pmod{p}$$

$$c = f^{-1} b \pmod{p, x^n - 1}$$

例

$$e = 14 + 11x + 26x^2 + 24x^3 + 14x^4 + 16x^5 + 30x^6 + 7x^7 + 25x^8 + 6x^9 + 19x^{10}$$

$$a = fe = 3 - 7x - 10x^2 - 11x^3 + 10x^4 + 7x^5 + 6x^6 + 7x^7 + 5x^8 - 3x^9 - 7x^{10}$$

$$b = a \pmod{3} = -x - x^2 + x^3 + x^4 + x^5 + x^7 - x^8 - x^{10}$$

$$c = f^{-1} b \pmod{3, x^{11} - 1} = -1 + x^3 - x^4 - x^8 + x^9 + x^{10}$$

$$a = fe = f(m + rh) = f(m + rpf^{-1} g) = fm + prg \pmod{q, x^n - 1}$$

$$b = a = fm + prg = fm \pmod{p}$$

$$c = f^{-1} b = f^{-1} fm = m \pmod{p, x^n - 1}$$

NTRUへの攻撃(4)

- Coppersmith,Shamir(EC97)
- **公開情報** $n, p, q, h(= pf^{-1}g(\mathrm{mod}\, q, x^n - 1)$ **から等価鍵** f', g'**を求める**
- $p^{-1}hx = \lambda y(\mathrm{mod}\, q, x^n - 1)$ **を満足する格子の短いベクトル** x, y **を**LLL**アルゴリズムで求める**

$$B = \begin{pmatrix} \lambda I & H \\ 0 & qI \end{pmatrix} = \begin{pmatrix} \lambda & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{n-1} \\ 0 & \lambda & \cdots & 0 & h_1 & h_2 & \cdots & h_0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda & h_{n-1} & h_0 & \cdots & h_{n-2} \\ 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{pmatrix}$$

h_iは$p^{-1}h(\mathrm{mod}\, q)$の係数、$\lambda(= \|f\| / \|g\|)$は定数

Howgrave-Graham**アルゴリズム**(1997)

- **法多項式の小さな解** ($< N^{1/d}$) **を求める。**
- Coppersmith**アルゴリズムの改良** (**より小さな基底行列**)
- x_0**を解とする方程式を組み合わせて整数上の多項式を作る。**
- dual lattice(B^{-t})**を**shrink**して基底行列を生成**

$$p(x) = x^2 + ax + b$$

$$p(x)^2 = x^4 + cx^3 + dx^2 + ex + f$$

$$\begin{array}{c} N^2 \\ N^2 \\ N \\ N \\ 1 \\ 1 \end{array} \begin{pmatrix} N^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & N^2X & 0 & 0 & 0 & 0 \\ Nb & NXa & NX^2 & 0 & 0 & 0 \\ 0 & NXb & NX^2a & X^3 & 0 & 0 \\ f & Xe & X^2d & X^3c & X^4 & 0 \\ 0 & Xf & X^2e & X^3d & X^4c & X^5 \end{pmatrix} \begin{array}{c} 1 \\ 1 \\ p(x) \\ xp(x) \\ p(x)^2 \\ xp(x)^2 \end{array}$$

$$\begin{array}{cccccc} 1 & X & X^2 & X^3 & X^4 & X^5 \end{array}$$

X**は定数**

b_1を係数とする多項式r(X)**を解くことにより解を求める。**

Howgrave-Grahamアルゴリズムの例

$p(x) = x^2 + 14x + 19 \equiv 0 \pmod{35}$ を解く。

$(p(x))^2 = x^4 + 28x^3 + 234x^2 + 532x + 361$

$X = 2$

$$\begin{pmatrix} 35^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 35^2 \times 2 & 0 & 0 & 0 & 0 \\ 35\times 19 & 35\times 14\times 2 & 35\times 2^2 & 0 & 0 & 0 \\ 0 & 35\times 19\times 2 & 35\times 14\times 2^2 & 35\times 2^3 & 0 & 0 \\ 361 & 532\times 2 & 234\times 2^2 & 28\times 2^3 & 2^4 & 0 \\ 0 & 361\times 2 & 532\times 2^2 & 234\times 2^3 & 28\times 2^4 & 2^5 \end{pmatrix}$$

↓ LLL

$\mathbf{b}_1 = (\underline{3},\ \underline{8}\times 2,\ \underline{-24}\times 2^2,\ \underline{-8}\times 2^3,\ \underline{-1}\times 2^4,\ \underline{2}\times 2^5)$

$r(x) = 2x^5 - x^4 - 8x^3 - 24x^2 + 8x + 3 = 0$**を解いて** $x = 3$**を求める。**

$d < N^{0.292}$のRSAの解読

$ed \equiv 1 \pmod{L}$

$(p-1, q-1) = 2$とすると$L=(p-1)(q-1)/2=(N-p-q+1)/2$なので

$ed+k\{(N+1)/2 - (p+q)/2\} = 1$

$A= (N+1)/2$

$s =(p+q)/2$

$d=N^{\delta}$

kとsを変数とする不定方程式

$k(A+s) \equiv 1 \pmod{e}$

e　N**とすると**s　$e^{0.5}$, k　e^{δ}

Wiener (IT90) **連分数を使って**$\delta < 0.25$**まで解ける**

Boneh**ら** (C99) ＬＬＬ (Howgrave-Graham) **を使って**$\delta < 0.292$

D.Boneh, G. Durfee, Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$,CRYPTO'99

$N=p^rq$の素因数分解

pに近い値Pを知っていたとする。$t=P-p$とすると

$$(P+t)^r \equiv 0 \pmod{p^r}$$

が成立する。$f(x)=(P+x)^r$とおくとtは$f(x)\equiv 0 \pmod{p^r}$の解になっている。
ただし、p^rは知らないのでp^rの倍数Nを使って$f(x)\equiv 0 \pmod{N}$を解くことで代用する（Howgrave-Grahamアルゴリズム）。

実際にはPの値は知らないので、Pに関する探索を行う。

$r > (\log p)^{1/2}$ のときに既存の方法より速くなる。

その他

•Hidden subset sum problem (C99)
ナップザックでa_iが秘密。x_iとCのペアを元に解読。
•Noisy polynomial reduction (Noisy chinise remainder theorem) (E00)
曲線上に乗らない点（ノイズ）も与えられたときに補間する。
•超楕円曲線
•NFS**への応用**
最終段で代数的数の平方根を求める。

Orthogonal lattice technique

与えられた格子と直交する格子をLLL**で求め、利用するテクニック**

- •Qu-Vanstone**暗号への攻撃**（Nguyen**他** C97）
- •Ajtai-Dwork**暗号の解析**（Nguyen**他** C98）
- **•伊藤,岡本,満保暗号**（SAC97）**の解読**（Nguyen**他** SAC98）
- •Hidden subset sum**問題への適用**（Nguyen**他** C99）
- •GGH**暗号**（Goldreich**他**C97）**の解読**（Nguyen C99）

その他

代数的整数論関連の応用

- 超楕円暗号のJacob和を求める（Buhler他 97）
- NFSの最終段での代数的整数の平方根を求める
- 最小多項式を求める

素因数分解

計算量のboundが証明されている素因数分解アルゴリズムで最速：$L^{2/3}$。

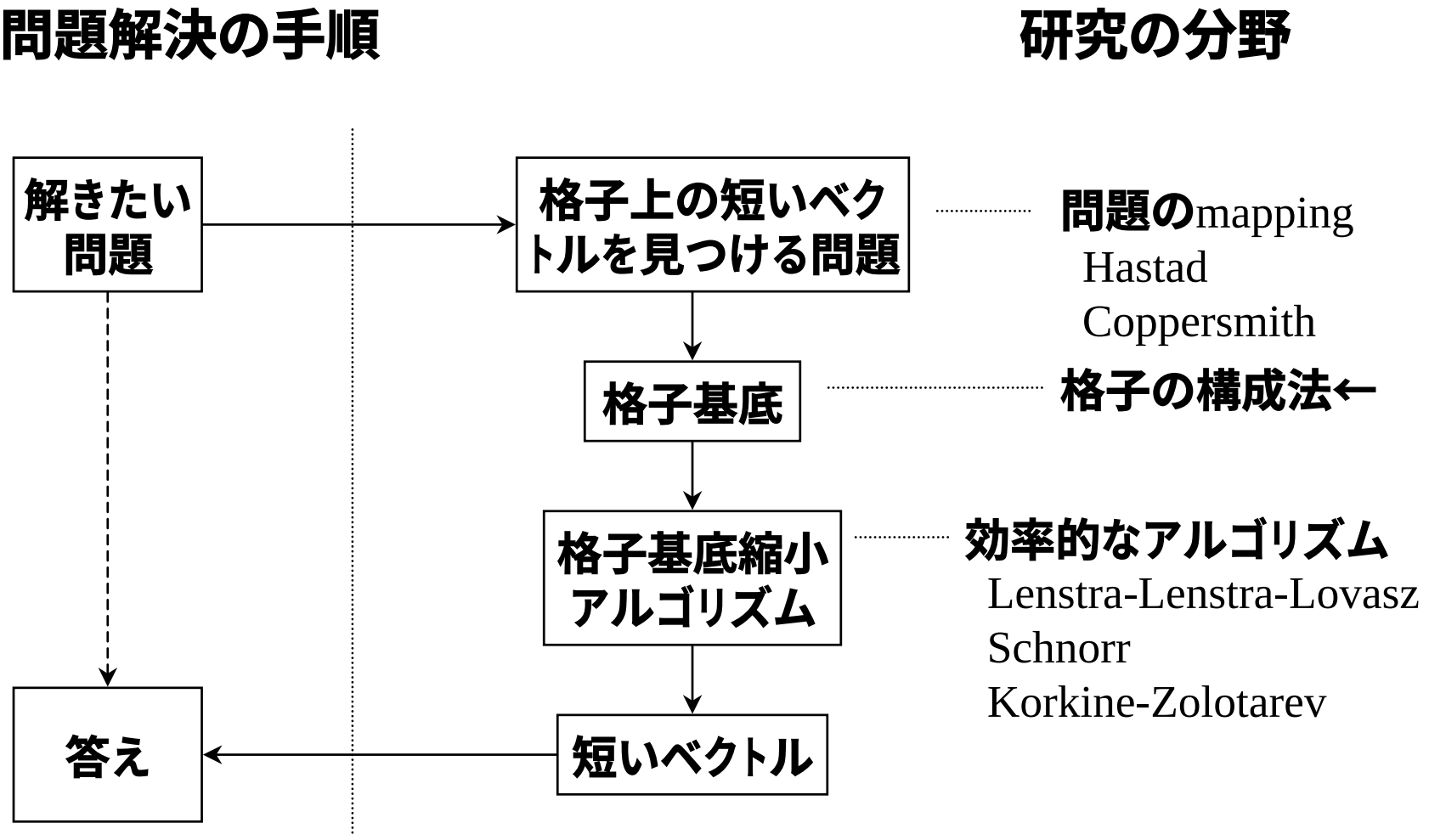
two-third method（Vallee他 Math.Comp.??）

まとめ

- ＬＬＬアルゴリズムの概要
  近似精度と実行時間が証明されている
- 最近の研究動向
  ユニークな研究が増えている。

フリーのLLL(C++) GMP対応 www.shoup.net/NTL/

LLLを使った問題解決のフレームワーク



格子基底の性質

- 同じ格子を張る別の格子基底が無限に存在する。
- 基本行操作した基底も同じ格子を張る
  →ユニモジュラ変換をしても同じ格子を張る。

$$L(B) = L(UB),\ U \in GL^n$$

- 同じ格子を張る基底の$d(\cdot)$は同じ値を取る。

$$L(B) = L(B') \rightarrow d(B) = d(B')$$

基本行操作
- ある行に-1を掛ける
- ある行の整数倍を別の行に加える。
- 行の交換

例

$$B = \begin{pmatrix} 1 & 0 & 0 & -11977006 \\ 0 & 1 & 0 & -11140073 \\ 0 & 0 & 1 & 12780049 \\ 0 & 0 & 0 & 1899061 \end{pmatrix} \quad B' = \begin{pmatrix} 7 & 11 & 16 & 0 \\ 30 & -12 & -3 & 28 \\ -4 & -36 & 20 & 1 \\ -31 & 20 & -3 & 41 \end{pmatrix} \quad U = \begin{pmatrix} 7 & 11 & 16 & 1 \\ 30 & -12 & -3 & 139 \\ -4 & -36 & 20 & -371 \\ -31 & 20 & -3 & -58 \end{pmatrix}$$

$B' = UB$

$L(B) = L(B')$

$\det(B) = 1899061,\ \det(B') = -1899061,\ \det(U) = -1$

格子基底縮小問題

たくさんある基底の中から、基底ベクトルのユークリッドノルムが短い基底を見つけ出す。

定義は?

例

$$B = \begin{pmatrix} 1 & 0 & 0 & -11977006 \\ 0 & 1 & 0 & -11140073 \\ 0 & 0 & 1 & 12780049 \\ 0 & 0 & 0 & 1899061 \end{pmatrix} \qquad \begin{aligned} |\mathbf{b}_1| &= 119977006 \\ |\mathbf{b}_2| &= 11140073 \\ |\mathbf{b}_3| &= 12780049 \\ |\mathbf{b}_4| &= 1899061 \end{aligned}$$

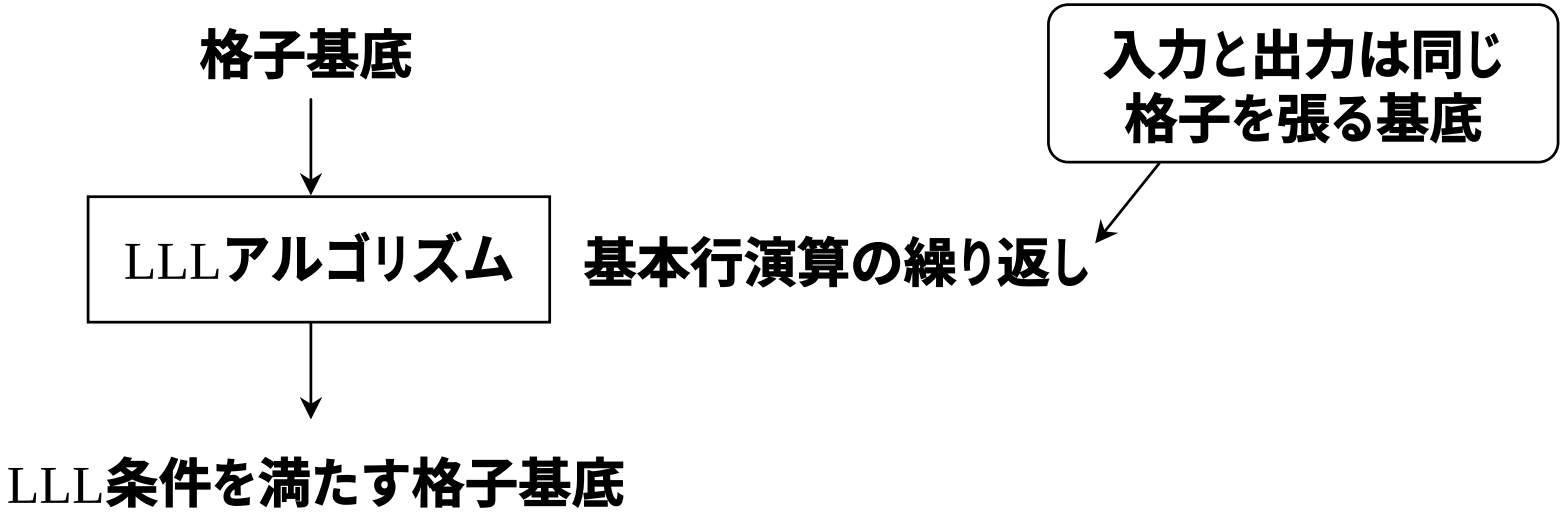
格子基底縮小

$$B' = \begin{pmatrix} 7 & 11 & 16 & 0 \\ 30 & -12 & -3 & 28 \\ -4 & -36 & 20 & 1 \\ -31 & 20 & -3 & 41 \end{pmatrix} \qquad \begin{aligned} |\mathbf{b'}_1| &= 20.64 \\ |\mathbf{b'}_2| &= 42.86 \\ |\mathbf{b'}_3| &= 41.39 \\ |\mathbf{b'}_4| &= 55.24 \end{aligned}$$

実際にLLLアルゴリズムで縮小してみた例 $d(B)^{1/4}$ 37.12

LLLアルゴリズム

格子基底を入力して、基本行操作を繰り返してLLL条件を満足する格子基底を出力する多項式時間アルゴリズム



LLLアルゴリズムの計算量

算術演算で数えて $O(n^4 \log B)$ $(B = \max\{B_{ij}\})$

LLL条件

条件1 $|\mu_{ij}| \le \frac{1}{2} \qquad 1 \le j < i \le n$

条件2 $|\mathbf{b}_i^* + \mu_{ii-1}\mathbf{b}_{i-1}^*|^2 \ge \frac{3}{4}|\mathbf{b}_{i-1}^*|^2 \qquad 1 < i \le n$

ここではb^*とかμの定義は省略する

LLL条件から色々なことが証明できる

- b_1の長さとd(L)の関係

$$|\mathbf{b}_1| \le 2^{(n-1)/4} d(L)^{1/n}$$

- b_1の長さと最短ベクトル∈Lの長さの関係

$$\forall \mathbf{x} \neq 0 \in L \qquad |\mathbf{b}_1|^2 \le 2^{n-1}|\mathbf{x}|^2$$

LLLアルゴリズムの出力を$\{b_1, b_2, \ldots, b_n\}$としている

- b_jの長さとt番目に短いベクトル∈Lの長さの関係

$$\forall \mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_t \qquad |\mathbf{b}_j|^2 \le 2^{n-1} \max\{|\mathbf{x}_1|^2, |\mathbf{x}_2|^2, \ldots, |\mathbf{x}_t|^2\} \qquad \text{for } j=1,\ldots,t$$

⋮

LLLの応用

同時ディオファンタス近似

基本型1 (**横型**)

$\mathbf{a} = (a_1, a_2, \ldots, a_n)$, Nが与えられて、
$\mathbf{b} = \alpha\mathbf{a} \bmod N = (\alpha a_1 \bmod N, \alpha a_2 \bmod N, \ldots, \alpha a_n \bmod N)$
とする。$|\mathbf{b}|$が小さくなるようなαを求める。

$$B = \begin{pmatrix} \varepsilon & a_1 & a_2 & \cdots & a_n \\ 0 & N & 0 & \cdots & 0 \\ 0 & 0 & N & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & N \end{pmatrix} = \begin{pmatrix} \varepsilon & \mathbf{a} \\ 0 & N\mathbf{I} \end{pmatrix}$$

ここのところが横に
並んでいるので横型

(n+1)**次元格子基底**B**の張る格子**L(B)**を考える**
(**ε は小さな定数**)

ε の大きさには何か理論があったはず(^^;

基本型1 (**続き**)

L(B)**を書き下してみる** $\forall \alpha, k_1, k_2, \ldots, k_n \in \mathbf{Z}$

$$
\begin{array}{llllll}
 & (\varepsilon & a_1 & a_2 & \cdots & a_n) \times \alpha \\
 & (0 & N & 0 & \cdots & 0) \times k_1 \\
 & (0 & 0 & N & \cdots & 0) \times k_2 \\
 & & & \vdots & & \vdots \\
+ & (0 & 0 & 0 & \cdots & N) \times k_n \\
\hline
 & (\alpha\varepsilon, \alpha a_1 + k_1 N, \alpha a_2 + k_2 N, \ldots, \alpha a_n + k_n N) &&&&
\end{array}
$$

$$
\begin{aligned}
L(B) &= (\alpha\varepsilon, \alpha a_1 + k_1 N, \alpha a_2 + k_2 N, \ldots, \alpha a_n + k_n N) \\
&= (\alpha\varepsilon, \alpha a_1 \bmod N, \alpha a_2 \bmod N, \ldots, \alpha a_n \bmod N)
\end{aligned}
$$

B**を**LLL**に入力し、出力**B'**に対して** **α**=B'$_{11}$／ **ε** **として** **α** **を求める。**

$$|\mathbf{b}_1| \le 2^{n/4} d(B)^{1/(n+1)} = 2^{n/4} (N^n \varepsilon)^{1/(n+1)}$$

例　**a** = (122, 133, 58, 203), N=209**について**|**α a** mod N|**が小さくなるαを見つける** (|**a**|　277.8)。

$$B = \begin{pmatrix} 1 & 122 & 133 & 58 & 203 \\ 0 & 259 & 0 & 0 & 0 \\ 0 & 0 & 259 & 0 & 0 \\ 0 & 0 & 0 & 259 & 0 \\ 0 & 0 & 0 & 0 & 259 \end{pmatrix}$$

簡単のためにε=1でも求まる例題を選んでいる

LLL

α

実際の長さ

$$B' = \begin{pmatrix} -4 & 30 & -14 & 27 & -35 \\ 23 & -43 & -49 & 39 & 7 \\ -13 & -32 & 84 & 23 & -49 \\ 45 & 51 & 28 & 20 & 70 \\ 70 & -7 & -14 & -84 & -35 \end{pmatrix} \begin{matrix} |\mathbf{b}_1| & 55.4 & (55.2) \\ |\mathbf{b}_2| & 79.7 & (76.3) \\ |\mathbf{b}_3| & 105.7 & (104.9) \\ |\mathbf{b}_4| & 103.5 & (93.2) \\ |\mathbf{b}_5| & 115.9 & (92.3) \end{matrix}$$

α=-4**のとき、**(122**α** mod N, 133**α** mod N, 58**α** mod N, 203**α** mod N)
= (30, -14, 27, -35)**で長さは**55.2。

基本型2 (縦型)

$\mathbf{a} = (a_1, a_2, \ldots, a_n), C, N$が与えられて、
$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \equiv C \pmod{n}$を満足する
$\mathbf{x} = (x_1, x_2, \ldots, x_n)$を求める

ここのところが縦に並んでいるので縦型

$$B = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & a_1 \\ 0 & 1 & \cdots & 0 & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & a_n \\ 0 & 0 & \cdots & 0 & 1 & C \\ 0 & 0 & \cdots & 0 & 0 & N \end{pmatrix} = \begin{pmatrix} \mathbf{I} & 0 & {}^t\mathbf{a} \\ 0 & 1 & C \\ 0 & 0 & N \end{pmatrix}$$

(n+2)**次元格子基底**B**の張る格子**L(B)**を考える**

基本型2 (続き)

L(B)**を書き下してみる。** $\forall x_1, x_2, \ldots, x_n, t, k \in \mathbf{Z}$

$$
\begin{array}{lccccccc}
 & (1 & 0 & \cdots & 0 & 0 & a_1) & \times x_1 \\
 & (0 & 1 & \cdots & 0 & 0 & a_2) & \times x_2 \\
 & & & \vdots & & & & \vdots \\
 & (0 & 0 & \cdots & 1 & 0 & a_n) & \times x_n \\
 & (0 & 0 & \cdots & 0 & 1 & C) & \times t \\
+ & (0 & 0 & \cdots & 0 & 0 & N) & \times k \\
\hline
 & \multicolumn{7}{l}{(x_1, x_2, \ldots, x_n, t, a_1x_1 + \cdots + a_nx_n + tC + kN)} \\
 & \multicolumn{7}{l}{= (x_1, x_2, \ldots, x_n, t, (a_1x_1 + \cdots + a_nx_n + tC) \bmod N)}
\end{array}
$$

縦型は直接解が求まる

B**をLLL**に入力する。b_1=(・・・,-1,0)**という形なら**
$\mathbf{b}_1$**の最初の**n**個の要素が解。**

$|\mathbf{b}_1| \le 2^{(n+1)/4} d(B)^{1/(n+2)} = 2^{(n+1)/4} N^{1/(n+2)}$ **を満足する解が存在するなら**

解が求まる。

例　$12345x_1+13333x_2+10058x_3 \equiv 1033 \pmod{15432}$**の小さな解を求める**

$$B=\begin{pmatrix}1&0&0&0&12345\\0&1&0&0&13333\\0&0&1&0&10058\\0&0&0&1&1033\\0&0&0&0&15432\end{pmatrix}$$

↓ LLL

$$B'=\begin{pmatrix}-2&-3&5&-1&0\\5&0&0&0&-3\\3&-3&-4&-3&1\\0&2&4&-5&5\\4&-5&1&7&4\end{pmatrix}$$

$\mathbf{b}_1$は(・・・,-1,0)という形になっている

(・・・,t,0)という形なら tの逆元を掛けて解を求める

$\mathbf{b}_1$=(-2, -3, 5, -1, 0)**なので**x_1=-2, x_2=-3, x_3=5。

検算:12345*(-2)+13333*(-3)+10058*5≡ 1033 (mod 15432)

$|\mathbf{b}_1|$　6.25≦$d(B)^{1/n}$ =$15432^{1/5}$　6.88

デコレーション(加速法)

解が求まる可能性を高めるための技法

・拡大(重み付け)

基底行列の列に重み付けすることで出力を制御する

$$B = \begin{pmatrix} & \lambda a_1 & \\ & \lambda a_2 & \\ \cdots & \vdots & \cdots \\ & \lambda a_n & \end{pmatrix}$$

$$L(B) = (\cdots, \lambda X, \cdots)$$

現実的にはデコレーションしないと解が求まらないことが多い

・平行移動

あるベクトルδに近いベクトルを求める。

$$\begin{pmatrix} B & 0 \\ \delta & 1 \end{pmatrix}$$

右下の1は重み付けする方が性能がよい

あらかじめ解の近似値が分かっている場合や、正の解のみを求めたいときに使う。

例　$12345x_1+13333x_2+10058x_3 \equiv 14996 \pmod{15432}$**を解く**

重み付けをしないと解けない例

$$B=\begin{pmatrix}1&0&0&0&12345\lambda_2\\0&1&0&0&13333\lambda_2\\0&0&1&0&10058\lambda_2\\0&0&0&\lambda_1&14996\lambda_2\\0&0&0&0&15432\lambda_2\end{pmatrix}$$

$\lambda_1=\lambda_2=1$

$$B'=\begin{pmatrix}0&5&1&-1&-1\\5&0&0&0&-3\\-2&0&-5&5&0\\-1&-1&4&-2&-6\\1&1&7&8&4\end{pmatrix}$$

失敗

$\lambda_1=\lambda_2=30$

$$B'=\begin{pmatrix}-3&5&17&0&0\\-18&14&2&0&0\\-6&-11&2&0&-30\\6&16&-1&-30&0\\17&17&-5&30&0\end{pmatrix}$$

成功

(・・・,-λ_1,0)**という形になっている**

実はこれも解

検算:12345*6+13333*16-10058≡14996 (mod 15432)

縦型の変形

$$a_1x_1 + a_2x_2 + a_3x_3 \equiv c(\mathrm{mod}\ N) \longrightarrow x_1 \equiv a_1^{-1}(-a_2x_2 - a_3x_3 + c) \bmod N$$

$$B = \begin{pmatrix} N & 0 & 0 & 0 \\ \beta a_2 & 1 & 0 & 0 \\ \beta a_3 & 0 & 1 & 0 \\ \beta c & 0 & 0 & 1 \end{pmatrix}$$

$$\beta = a_1^{-1} \bmod N$$

$$\forall x_2, x_3, t \in \mathbf{Z}$$

$$L(B) = (\beta(a_2x_2 + a_3x_3 + tc) \bmod N, x_2, x_3, t)$$

- 別の基底行列でも同じことができる。
- 次元数が少ないほどよい。

Hastad**アルゴリズム**(1988)

d次のモニックなモジュラ方程式$p(x) \equiv 0 \pmod N$**の解**$x_0 < N^{2/d(d+1)}$**を求めるアルゴリズム**($p(x) = p_d x^d + p_{d-1} x^{d-1} + \cdots + p_2 x^2 + p_1 x + p_0$)

$$x_0 < X$$

$$B = \begin{pmatrix} \varepsilon & X^d p_d & X^{d-1} p_{d-1} & \cdots & X p_1 & p_0 \\ 0 & X^d N & 0 & \cdots & 0 & 0 \\ 0 & 0 & X^{d-1} N & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & XN & 0 \\ 0 & 0 & 0 & \cdots & 0 & N \end{pmatrix}$$

重み付き横型

係数をモジュラ変換して、整数上でも成立する方程式に変換する

$$p(x_0) \equiv 0 \pmod n \xrightarrow{\text{モジュラ変換}} p'(x_0) = 0$$

Hastadアルゴリズムの例

$p(x) = x^2 + 1233x + 805 \equiv 0 \pmod{1399}$ **を解く**

$\varepsilon = 1, X = 10$

$$B = \begin{pmatrix} 1 & X^2 & 1233X & 805 \\ 0 & X^2 N & 0 & 0 \\ 0 & 0 & XN & 0 \\ 0 & 0 & 0 & N \end{pmatrix}$$

↓ LLL

α

$$\begin{pmatrix} 8 & 8X^2 & 71X & -555 \\ 8 & 8X^2 & 71X & 844 \\ -9 & -9X^2 & 95X & -250 \\ -N & 0 & 0 & 0 \end{pmatrix}$$

$8x^2+71x-555=0$**を解いて**$x=5$**が答え**

Coppersmithアルゴリズム(1996)

d次のモニックなモジュラ方程式$p(x) \equiv 0 \pmod N$**の解**$x_0 < N^{1/d}$**を求めるアルゴリズム**

$$x_0 < X$$

$$B = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & p_0 \\ 0 & X^{-1} & \cdots & 0 & 0 & p_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & X^{-(d-1)} & 0 & p_{d-1} \\ 0 & 0 & \cdots & 0 & X^{-d} & p_d \\ 0 & 0 & \cdots & 0 & 0 & N \end{pmatrix}$$

↓

$$\sum_{i=0}^{d} p_i z_i \equiv 0 (\mathrm{mod}\, n), z_i \approx X^i$$

↓

z_iに関する制約が弱すぎる(重みをつけただけな)ので$(1, x_0, x_0^2, \ldots, x_0^{d-1}, x_0^d)$のような解は求まらない。

スタート：Bからx_0が求まるかもしれない

↓

駄目

↓

p(x)以外にx_0を解に持つ方程式を連立させて、解が求まる可能性を高める。

↓

$xp(x)$, $x^2p(x)$,...**とか、**
$p(x)^2$,$xp(x)^2$,$x^2p(x)^2$,...**とか、**
$p(x)^3$, $xp(x)^3$,...

Coppersmithアルゴリズム

$$B = \begin{pmatrix} \mathbf{X} & {}^{t}p & {}^{t}xp & {}^{t}p^{2} & {}^{t}xp^{2} \\ \hline & N & 0 & 0 & 0 \\ & 0 & N & 0 & 0 \\ 0 & 0 & 0 & N^{2} & 0 \\ & 0 & 0 & 0 & N^{2} \end{pmatrix}$$

$$p(x) = x^{2} + ax + b$$

$$p(x)^{2} = x^{4} + cx^{3} + dx^{2} + ex + f$$

$$= \begin{array}{c|cccccc|cccc} & & & & & & & \mathrm{p} & \mathrm{xp} & \mathrm{p}^{2} & \mathrm{xp}^{2} \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & b & 0 & f & 0 \\ 0 & X^{-1} & 0 & 0 & 0 & 0 & a & b & e & f \\ 0 & 0 & X^{-2} & 0 & 0 & 0 & 1 & a & d & e \\ 0 & 0 & 0 & X^{-3} & 0 & 0 & 0 & 1 & c & d \\ 0 & 0 & 0 & 0 & X^{-4} & 0 & 0 & 0 & 1 & c \\ 0 & 0 & 0 & 0 & 0 & X^{-5} & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & N & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & N & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & N^{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & N^{2} \end{array}$$

(・・・,0,0,0,0)が解候補

縦型の応用

(・・・,0,0,0,0)が解候補

LLLのまとめ

- 格子と格子基底の紹介
- 格子基底縮小(LLL)の紹介
- 応用 ー 基本形(縦型と横型)
- モジュラ方程式の解を求める

↓

中身をあまり知らなくてもツールとして使える!!