格子基底簡約を利用した合同方程式の求解アルゴリズム

Kazushi Kato

Japan Advanced Institute of Science and Technology

June 17, 2022

$ whoami

- 名前: 加藤和志 (Kato Kazushi)
- 所属: コンピューティング科学領域 藤崎研究室
- 趣味: CTF, 読書 (SF 小説), ヤバいアルゴリズムの調査
- Twitter
  1. @Xornet_Euphoria (よくいる)
  2. @Encrypted_Legna (JAIST 関連の連絡と生存報告)

合同について

- ある正の整数 n で割った余りが同じ 2 つの数を「同じもの」とみなす
- 例えば $4 = 1 \times 3 + 1, 7 = 2 \times 3 + 1$ なので「4 と 7 は 3 を法として合同」
- これを $4 \equiv 7 \mod 3$ のように書く
- 通常の四則演算であれば合同なものはどれを用いても良いので原則として $0 \leq a < n$ を満たす a を用いる
- $2x \equiv 1 \mod 3$ のような方程式も考えることが出来る
  - 解は $3k + 2$ の形をした整数だが、ここでは 2 を解とする

通常の方程式 vs 合同方程式

- 通常の方程式であれば、解の公式で厳密解を、そうでなくてもニュートン法等で数値的な近似解を求められる
- 一方、合同方程式は次のような「特殊な場合」を除いて汎用的な解法が存在していない
  1. 法が素数 p の場合 (以下、p と書いたら素数とする)
  2. 法が素数のべき乗 p^e の場合 (1 が解ける事を利用)
  3. 解が $n^{\deg f}$ より小さい場合 (今回扱う)
- 一応 n 以下の数を総当りすれば解けるが...

現在の暗号技術における数の大きさ

- 現在の RSA 暗号で用いられている数値: 2048bit
- ECDSA で用いられている数値: 256bit
- SHA-512 のハッシュ空間: 512bit
- AES のブロック長: 128bit

ご家庭のパソコンどころか、スパコン等で総当りをしても途方もない年月がかかるレベル

同一解を持つ合同方程式

次の 3 つの多項式は同一解 $x = 3$ を持つ

1. $x^2 + 6x + 12 \equiv 0 \mod 13$
2. $x^2 + 2x - 2 \equiv 0 \mod 13$
3. $x^2 - x - 6 \equiv 0 \mod 13$

実際に代入してみるといずれも 13 の倍数であることがわかる

1. $3^2 + 6 \times 3 + 12 = 39 = 3 \times 13$
2. $3^2 + 2 \times 3 - 2 = 13 = 1 \times 13$
3. $3^2 - 3 - 6 = 0 = 0 \times 13$

同一解を持つ合同方程式

1. $x^2 + 6x + 12 \equiv 0 \mod 13$
2. $x^2 + 2x - 2 \equiv 0 \mod 13$
3. $x^2 - x - 6 \equiv 0 \mod 13$

- 代入した結果は n の倍数になるが、方程式によって異なる
- 特に 3 の場合は 0 になったので法がなくてもそもそも解ける
  - $x^2 - x - 6 = (x+2)(x-3) = 0$ より $x = 3$ は解である

Question

ある方程式から解が同じで法が無いような方程式に持っていけないか?

Howgrave-Graham's Lemma

Theorem (Howgrave-Graham's Lemma[1])

n を法とした多項式 $f(x)$ に対して、ある数 X が存在し、f の根 x_0 について $|x_0| < X$ であるとする。この時、次が成立するなら $f(x_0) = 0$ である。

$$|f(xX)| < \frac{n}{\sqrt{e+1}}$$

ここで多項式 $f(x) = \sum_{i=0}^{e} a_i x^i$ に対するノルム $|f(x)|$ を次で定義した。

$$|f(x)| = \sqrt{\sum_{i=0}^{e} a_i^2}$$

Howgrave-Graham's Lemma

Example

$n = 221, f(x) = x^2 + 31x - 66$、$X = 3$ として $f(x)$ の根で絶対値が X より小さいものを探す。

$X = 3$ より、$f(xX) = 9x^2 + 93x - 66$

$|f(xX)| = \sqrt{81 + 8649 + 4356} = \sqrt{13086} < 115$

一方、$\frac{n}{\sqrt{e+1}} = \frac{221}{\sqrt{3}} > 127$ であるから、$|f(xX)| < \frac{n}{\sqrt{e+1}}$

よって $f(x) \equiv 0 \mod n$ の絶対値が $X = 3$ より小さい解は法が無くても解である。

実際、$f(x) = (x-2)(x+33)$ より、$x = 2$ が解。

Howgrave-Graham's Lemma

これらを纏めると

- 合同方程式 $f(x) \equiv 0 \mod n$ は $|f(xX)|$ が小さい時に $|x_0| < X$ である解 x_0 を求められる
- $|f(xX)|$ が小さくなるというのは主に次の 2 つの要因がある
  1. X が小さい
  2. $f(x)$ の係数が小さい
- 1 は $|x_0|$ が小さい、つまり解が小さいことを要求している
- 2 は文字通り

Question

与えられた方程式から 2 を満たす多項式を得られないか?

同一根を持つ多項式

命題 (1)

同一根を持つ 2 つの多項式の加減算も同じ根を持つ

Proof.

$f_1(x), f_2(x)$ が同一根 a を持つとする。
$f(a) \equiv 0 \mod n \Leftrightarrow \exists k \in \mathbb{Z} f(x) = kn$ であるから、
$f_1(a) = k_1 n, f_2(a) = k_2 n$ となる $k_1, k_2 \in \mathbb{Z}$ が存在する。
$f_1(a) \pm f_2(a) = (k_1 \pm k_2)n$ より、$f_1(a) \pm f_2(a) \equiv 0 \mod n$。

□

同一根を持つ多項式

命題 (2)

多項式を整数倍しても同じ根を持つ

Proof.

$f_1(x)$ が根 a を持つとする。
任意の整数 $k \in \mathbb{Z}$ に対して $kf_1(a) = kk_1n$ より、$kf_1(a) \equiv 0 \mod n$ □

Question

多項式に対するこれらの演算を繰り返すことで Howgrave-Graham's Lemma を満たすような多項式を生成出来ないか

解くために必要なもの

1. 与えられた多項式 $f(x)$ と同じ根を持つ別の多項式
2. 多項式の集合から Howgrave-Graham's Lemma を満たすような多項式を作る方法

1 は自明な多項式 N, Nx^i が使える。
2 は多項式の加減算とスカラー倍をベクトルに対応させて行列で表現し、適切な係数を選んで $f(xX)$ のノルムが小さいベクトルを探す。

多項式の集合を行列に変換

高々 m 次整数係数多項式全体の集合を V_m とおくと次のような全単射が得られる。

$$F : V_m \to \mathbb{Z}^{m+1}$$

$$f(x) = \sum_{i=0}^{m} a_i x^i \mapsto (a_0, a_1, \ldots, a_m)$$

面白い事にこの写像は加法とスカラー倍で保存される。

$$F(f(x) + g(x)) = F(f(x)) + F(g(x))$$
$$F(kf(x)) = kF(f(x))$$

ということは多項式の加減算とスカラー倍を行列で代用出来るのでは?

多項式の集合を行列に変換

高々 m 次の整数係数多項式が n 個入っている集合
$S = \{f_i(x) \mid f_i(x) = \sum_{j=0}^{m} a_{i,j}x^j \wedge a_{i,j} \in \mathbb{Z}\}$ に対して、各成分が
$M_{i,j} = a_{i,j}$ であるような次のような $n \times m+1$ 行列 M を考える。

$$M = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,m} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,m} \\ & & \vdots & \\ a_{n-1,0} & a_{n-1,1} & \cdots & a_{n-1,m} \end{pmatrix}$$

S 内の多項式の整数係数線形結合は M を用いて次のようになる。

$$\sum_{i=0}^{n-1} k_i f_i(x) = (k_0, k_1, \ldots, k_{n-1})M$$

多項式の集合を行列に変換

Question

$\sum_{i=0}^{n-1} k_i f_i(x)$ が小さくなるような $(k_0, k_1, \ldots, k_{n-1})$ をどうやって探すか

answer

格子基底簡約を利用する

なお、実際は $f_i(x)$ ではなく、$f_i(xX)$ の線形結合でノルムが短いものを探すが、これについてはアルゴリズムのページで再度説明する。

格子の定義

Definition (格子)

$\mathbb{R}^m$ の n 本の基底 $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ の整数係数による線形結合で生成される空間 $\Lambda \subset \mathbb{R}^m$ を $\mathbb{R}^m$ の n 次元格子と呼ぶ。

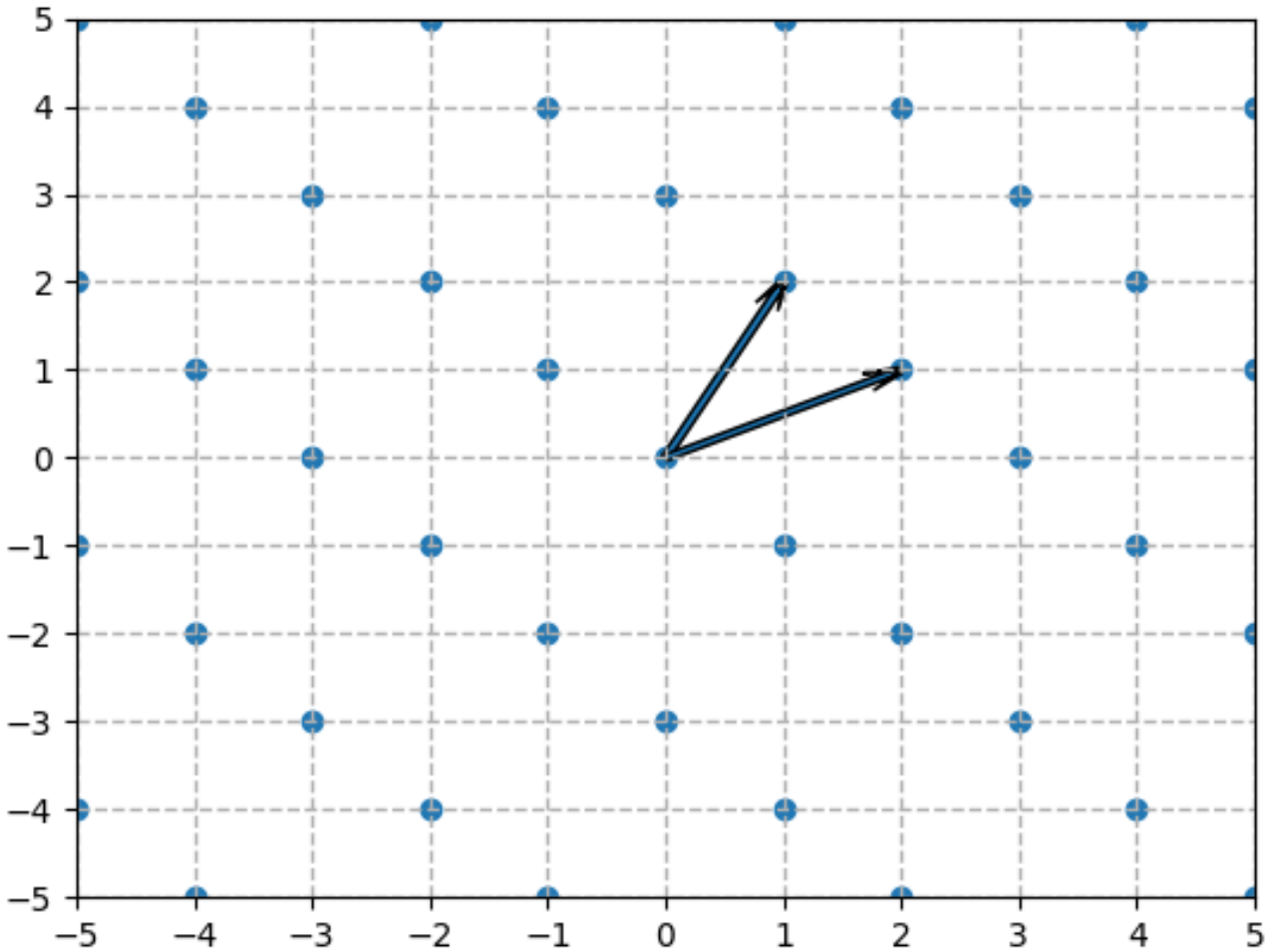
$$\Lambda = \left\{ \sum_{i=1}^{n} a_i \boldsymbol{b}_i \mid a_i \in \mathbb{Z} \right\}$$

Notation

基底 (行ベクトル) を並べた $n \times m$ 行列 B を考え、その基底が生成する格子を $\mathcal{L}(B)$ とする。
これによって左から係数ベクトル $x := (a_1, \ldots, a_n)$ を掛けることで、任意の $\mathcal{L}(B)$ の要素 $xB \in \mathcal{L}(B)$ を表すことが出来る。

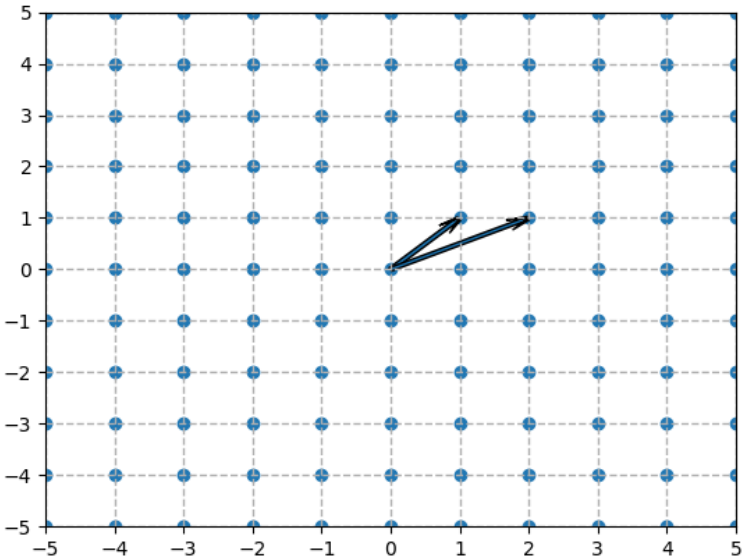
格子の例

次は $(1, 2), (2, 1)$ という基底から生成される格子

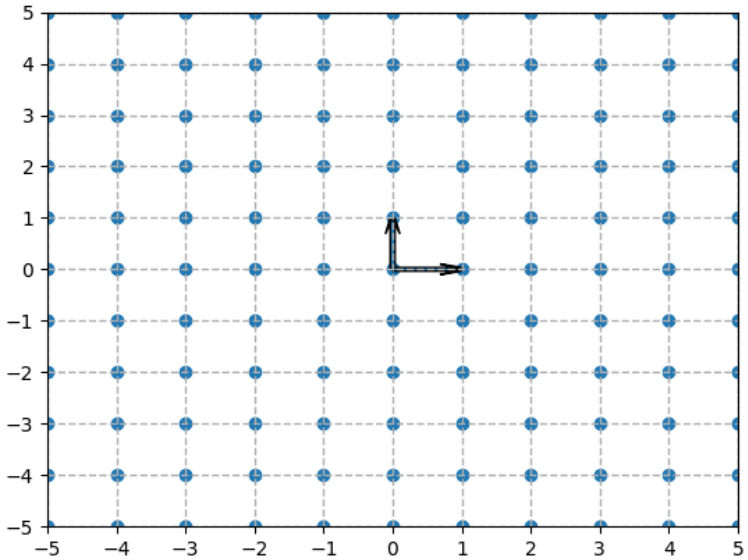


同一の格子を張る基底

次の 2 つは異なる基底だが同一の格子を生成する



基底は $(2, 1), (1, 1)$



基底は $(1, 0), (0, 1)$

格子には「体積」と呼ばれる不変量が存在し、これは $\sqrt{\det(BB^T)}$ である (B が正方行列なら $\det B$)

基底簡約

ある基底を与えた時に、同じ格子を張る別の「都合の良い」基底を与える

1. 基底がある程度直交している
2. 基底の長さが短い

特に 2 に関しては次のような問題の近似解を与える事につながる

Problem (最短ベクトル問題)

与えられた格子中で次のようなベクトルを見つける

- 格子中でノルムが最も小さい非零ベクトル (SVP)
- 最短ベクトルのノルムに γ を掛けたものより短いベクトル (γ-SVP)

LLL 簡約基底

基底簡約には様々なアルゴリズムが存在するが、特に有名なものに次の LLL 簡約基底を与える LLL アルゴリズムがある

Definition (LLL 簡約基底 [2])

1. 基底の任意の GSO 係数 $\mu_{i,j}$ に対して $|\mu_{i,j}| \leq \frac{1}{2}$
2. 簡約パラメータ δ に対して $\delta\|\boldsymbol{b}_{k-1}^*\| \leq \|\pi_{k-1}(\boldsymbol{b}_k)\|$ を満たす
   - 簡約パラメータ δ は $\frac{1}{4} < \delta < 1$
   - $\delta\|\boldsymbol{b}_{k-1}^*\|^2 \leq \mu_{k,k-1}^2\|\boldsymbol{b}_{k-1}^*\|^2 + \|\boldsymbol{b}_k^*\|^2$ と同値

ここで $\boldsymbol{b}_k^*$ は $\boldsymbol{b}_k$ の GSO ベクトル、π_k は $\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k-1} \rangle_{\mathbb{R}}$ への直交射影

(今回の本筋には関係ないので定義の提示のみに留めます)

LLL 簡約基底の性質

$\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ が格子 L の LLL 簡約基底 (簡約パラメータは δ) だとすると次が成り立つ。

- $\|\boldsymbol{b}_1\| \leq \alpha^{\frac{n-1}{4}} \mathrm{vol}(L)^{\frac{1}{n}}$
  - $\alpha := \frac{4}{4\delta - 1}$
  - $\mathrm{vol}(L)$ は格子の体積
- L の別の基底から $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ を出力する多項式時間のアルゴリズム (LLL アルゴリズム) が存在する
  - LLL アルゴリズムで出てきた基底の内、1 つは ↑ の性質を満たしている
  - つまり、格子中のそれなりに短いベクトルが得られる

多項式への応用

多項式から作った行列を簡約して出てきたベクトルを多項式に変換すれば、解が同じでノルムが小さいものが得られる

Coppersmith's Theorem

Theorem (Coppersmith's Theorem[1])

法が n の m 次モニック合同多項式 $f(x)$ の根 x_0 が $|x_0| \leq n^{\frac{1}{m}-\frac{1}{\epsilon}}$ を満たすなら多項式時間で求めることが出来る。

note

- モニック多項式は最大次数の係数が 1 の多項式
- 今回示す方法ではここまで求解範囲は広くない

Coppersmith's Attack

法 n のモニック m 次多項式 $f(x)$ から、次のような $m+1$ 本の多項式 $g_i(x)$ を用意する

- $g_0(x) := n$
- $g_1(x) := nx$
- $\vdots$
- $g_{m-1}(x) := nx^{m-1}$
- $g_m(x) := f(x)$

$g_i(xX)$ という多項式の集合で線形結合すると多項式 $h(xX)$ が生成されるので $g_i(xX)$ で行列を作って簡約すれば、$h(xX)$ が小さくなる。
(なお、$h(x)$ は $f(x)$ と同じ根を持つが、紙面の都合上証明はカット)

Coppersmith's Attack

先程の多項式の集合 $\{g_i(xX) \mid i \in \mathbb{Z} \wedge 0 \leq i \leq m\}$ から行列を作り、それを基底とした次のような格子を簡約する

$$\begin{pmatrix} n & & & & & \\ & nX & & & & \\ & & nX^2 & & & \\ & & & \ddots & & \\ & & & & nX^{m-1} & \\ a_0 & a_1X & a_2X^2 & \dots & a_{m-1}X^{m-1} & X^m \end{pmatrix}$$

出てきた基底から多項式 $h(xX)$ を構成し、$h(x)$ が法無しでも根を持てば、それが解になる

RSA 暗号への攻撃

- RSA 暗号 (公開鍵は n, e) の暗号化は平文 a に対して $a^e \mod n$
- e が小さくてかつ $a = a_0 + x$ のように部分的に分かっているとする (a_0 が既知)
- この場合、c を暗号文として $c = a^e \equiv (a_0 + x)^e \mod n$ という方程式を Coppersmith's Attack で解けば a がわかる
- 例えばテンプレートやマジックナンバー等で先頭がいつも同じ平文であればこの攻撃が有効 (Stereotype Message Attack)

求解可能範囲

- 上記の格子の体積は $n^m X^{\frac{m(m+1)}{2}}$ であるから、LLL アルゴリズムを用いるとノルムが $N^{\frac{m}{m+1}} X^{\frac{m}{2}}$ 以下のベクトルが現れる
- Howgrave-Graham's Lemma を満たすには $N^{\frac{m}{m+1}} X^{\frac{m}{2}} \leq \frac{N}{\sqrt{m+1}}$ でなくてはならない
- ここから X の範囲を計算すると $X < \frac{1}{\sqrt{m+1}}^{\frac{2}{m}} N^{\frac{2}{m(m+1)}}$
- あまり広い範囲では無いが、実はこれは広げることが可能

求解範囲を広げる

- 先程の簡約に使った多項式は高々 m 次だが、これと「法 n」を大きくすればもっと良い結果が得られる
- 具体的な例として n^2 を法とすると $N^2, xN^2, Nf(x), f(x)^2$ なんかは n^2 を法として同一根を持つ
- 一般的には $g_{i,j}(x) := n^{k-i}x^j f(x)^i$ として法が n^k である $j + ei$ 次の多項式を $m(k+1)$ 個集めて簡約する

素因数分解への応用

- $N = pq$ として p, q は未知だが、それを法とした多項式を得ている場合を考える
- Coppersmith's Attack において px^i のようなものの代わりに Nx^i で代用可能 (但し求解可能な範囲は狭くなる)
- p の上位ビットがある程度わかっているなら、それを a として $a + x = p \equiv 0 \mod p$ が成り立つ
- p の代わりに N を掛ける Coppersmith's Attack で解ける (最適化した攻撃なら半分のビットがわかっていれば良い)

More Reading

提案論文 [3] やそれの関連論文がお世辞にもわかりやすいとは言えないため、下記の Survey や資料、記事を紹介する

- Alexander May の博士論文 [4] が Coppersmith's Attack 関連のトピックを網羅しており、これを読めば良い
- 日本語の資料だと [5] が非常にわかりやすい
- [6] は暗号理論の入門書でありながら最終章でこの攻撃を扱っている
- 手前味噌だが今回の発表は以前書いた [7] をベースにしているのでぜひこちらも
- 格子とその簡約についてより詳しく知りたい場合は [8] が非常に詳しい

Reference I

[1] Nick Howgrave-Graham.
Finding small roots of univariate modular equations revisited, pp. 131–142.
10 2006.

[2] Arjen Lenstra, H. Lenstra, and LovÃ¡sz LÃ¡szlÃ³.
Factoring polynomials with rational coefficients.
Mathematische Annalen, Vol. 261, , 12 1982.

[3] Don Coppersmith.
Finding a small root of a univariate modular equation.
In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, pp. 155–165, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[4] Alexander May.
New RSA vulnerabilities using lattice reduction methods.
PhD thesis, University of Paderborn, 2003.

[5] Shiho Midorikawa.
katagaitai workshop winter - elliptic-shiho's labs.
`http://elliptic-shiho.github.io/slide/katagaitai_winter_2018.pdf`, 2018.

[6] 黒澤馨.
現代暗号への招待.
サイエンス社, 2010.

Reference II

[7] Xornet.
Coppersmith's attack を再実装する.
https://project-euphoria.dev/blog/30-rebuild-coppersmith/, 2022.

[8] 青野良範, 安田雅哉.
格子暗号解読のための数学的基礎.
近代科学社, 2019.

素因数分解と合同方程式

- 素因数分解が出来れば解くことが出来る
  - 具体的には各素因数 (とそのべき乗)$p_i^{e_i}$ を法として解く
  - 中国人剰余定理を用いて、その解を $\bmod n$ へ「持ち上げる」
- しかし素因数分解の時間計算量は非常に大きい
- 逆に言えばこの困難性を暗号で利用できる

モニック多項式への変換

- 方程式 $f(x) \equiv 0 \mod n$ に対してある整数 a を両辺に掛けると $af(x) \equiv 0 \mod n$ となる
- よって、$f(x)$ の最高次係数を a_m とおくと、$a_m b \equiv 1 \mod n$ となる b を掛ければ、$f(x)$ と同一根を持つモニック多項式 $bf(x)$ が得られる
- このような b が存在する a_m の条件は $\gcd(a_m, n) = 1$
- RSA 暗号の場合、$n = pq$ と同じ約数を持つ確率はおよそ $\frac{2p}{n}$ で、これは n が大きければ非常に小さいので無視出来る