第３章　Goodのアルゴリズム

３．１　不定方程式

整数$a,b,n\in\mathbb{Z},\ n>0$として，

△ $\mathbb{Z}_n=\{0,1,\cdots,n-1\}$．

△ $n|a$ ⇔ nはaを割り切る．

△ $a\equiv b\ (\mathrm{mod}\,n)$ ⇔ $n|(a-b)$ ⇔ a,bをnで割った余りは等しい．

△ $a=\mathrm{mod}(b,n)$ ⇔ aはbをnで割った余り$(a\equiv b(\mathrm{mod}\,n),\ a\in\mathbb{Z}_n)$．

3.1.0 基本的性質

☆ $a\equiv a'\ (\mathrm{mod}\,n), b\equiv b'\ (\mathrm{mod}\,n)$なら，$a+b\equiv a'+b'\ (\mathrm{mod}\,n), ab\equiv a'b'\ (\mathrm{mod}\,n)$．

（証明）条件より，$a-a', b-b'$はnで割り切れる．ゆえに，$(a+b)-(a'+b')=(a-a')+(b-b')$は$n$で割り切れるので$a+b\equiv a'+b'\ (\mathrm{mod}\,n)$．また，$ab-a'b'=(a-a')b-a'(b-b')$も$n$で割り切れるので$ab\equiv a'b'\ (\mathrm{mod}\,n)$．//

3.1.1 最大公約数

整数a,bの最大公約数$\mathrm{GCD}(a,b)$を求める．

＜ユークリッドの互除法＞

$a_0=a, a_1=b, k=0$

While $a_{k+1}\neq 0$

$k=k+1$

$a_{k-1}=q_k a_k+a_{k+1}$　；a_{k-1}をa_kで割った商q_k，余りa_{k+1}．

end while

☆上のアルゴリズムで，$\mathrm{GCD}(a,b)=a_k$．

（証明）アルゴリズム実行後，次の式が成立している．

$$\begin{aligned} &a_{i-1}=q_i a_i+a_{i+1}\ \ (1\le i\le k)\\ &a_{k+1}=0 \end{aligned} \tag{3.1}$$

特に，$a_{k-1}=q_k a_k$より$\mathrm{GCD}(a_{k-1},a_k)=a_k$．$k\ge 2$なら，$a_k=a_{k-2}-q_{k-1}a_{k-1}$から，

$$\mathrm{GCD}(a_{k-1},a_k)=\mathrm{GCD}(a_{k-1},a_{k-2}-q_{k-1}a_{k-1})=\mathrm{GCD}(a_{k-1},a_{k-2})=\mathrm{GCD}(a_{k-2},a_{k-1}).$$

同様にして，

$$a_k=\mathrm{GCD}(a_{k-1},a_k)=\mathrm{GCD}(a_{k-2},a_{k-1})=\cdots=\mathrm{GCD}(a_0,a_1).\ //$$

3.1.2 不定方程式　$ax\equiv 1\ (\mathrm{mod}\,n), x\in\mathbb{Z}_n$．ただし，$\mathrm{GCD}(a,n)=1$を仮定．

＜拡張ユークリッド互除法＞

(1) $a_0=n, a_1=a$とし，ユークリッド互除法で$a_i\ (0\le i\le k), q_i\ (1\le i\le k)$を求める．

$a_k=\mathrm{GCD}(a,n)=1$となる．

(2) $x_{k-1}=1, x_{k-2}=-q_{k-1}$として，

$$x_{l-1}=-x_l q_l+x_{l+1}\ \ (l=k-2,k-3,\cdots,1) \tag{3.2}$$

(3) $x = \mathrm{mod}(x_0, n)$

☆上のアルゴリズムで，$ax_0 \equiv 1 \pmod{n}$．

（証明）$ax_0 + nx_1 = a_1x_0 + a_0x_1 = 1$を示す．これと$x \equiv x_0 \pmod{n}$より，$ax \equiv ax_0 \equiv 1 \pmod{n}$である．

帰納法により$a_{l+1}x_l + a_lx_{l+1} = 1 \ (0 \le l \le k-1)$を示す．$l = k-1$のとき，式(3.1), (3.2)より，

$$x_{k-1}a_{k-2} + x_{k-2}a_{k-1} = a_{k-2} - q_{k-1}a_{k-1} = a_k = 1.$$

また，ある$l = i \le k-1$で$a_{i+1}x_i + a_ix_{i+1} = 1$を仮定すると，式(3.1), (3.2)を用いて，

$$a_ix_{i-1} + a_{i-1}x_i = a_i(-x_iq_i + x_{i+1}) + a_{i-1}x_i = (a_{i-1} - a_iq_i)x_i + a_ix_{i+1} = a_{i+1}x_i + a_ix_{i+1} = 1.$$

ゆえに，$l = i-1$でも成立する．ゆえに，$a_{l+1}x_l + a_lx_{l+1} = 1 \ (0 \le l \le k-1)$．//

☆解の一意性：$ax \equiv 1 \pmod{n}, ay \equiv 1 \pmod{n}$かつ$x, y \in \mathbb{Z}_n$なら，$x = y$．

（証明）$x - y \equiv ax(x-y) \equiv x(ax-ay) \equiv 0 \pmod{n}$．また，$x, y \in \mathbb{Z}_n$より，$-n < x - y < n$．よって，$x = y$．//

3.1.3 不定方程式　$ax \equiv b \pmod{n}$の解$x \in \mathbb{Z}_n$を求める．ただし，$\mathrm{GCD}(a, n) = 1$．

＜アルゴリズム 1 ＞

(1) $a\bar{a} \equiv 1 \pmod{n}$を満たす$\bar{a} \in \mathbb{Z}_n$を計算（拡張ユークリッドの互除法）．

(2) $x = \mathrm{mod}(\bar{a}b, n)$.

（$\because ax \equiv a(\bar{a}b) \equiv 1 \cdot b = b \pmod{n}$）

［命題3.1］（解の一意性）$ax \equiv b \pmod{n}, ay \equiv b \pmod{n}$かつ$x, y \in \mathbb{Z}_n$なら，$x = y$．

（証明）$x - y \equiv au(x-y) \equiv u(ax-ay) \equiv 0 \pmod{n}$．これと$-n < x - y < n$より，$x = y$．//

3.1.4 連立不定方程式，多変数不定方程式

$p_1, \cdots, p_m$は互いに素，$n = p_1p_2 \cdots p_m$とする．$n_i = n / p_i \ (1 \le i \le m)$とする．

◎連立不定方程式：$x \equiv b_i \pmod{p_i} \ (1 \le i \le m)$の解$x \in \mathbb{Z}_n$を求める．

＜アルゴリズム2＞

(1) $n_ix_i \equiv b_i \pmod{p_i} \ (1 \le i \le m)$を解く．（アルゴリズム1より，$x_i = \bar{n}_ib_i$）

(2) $x = \mathrm{mod}\left(\sum_{i=1}^{m} n_ix_i, n\right) = \mathrm{mod}\left(\sum_{i=1}^{m} n_i\bar{n}_ib_i, n\right)$.

（$n_j \equiv 0 \pmod{p_j} \ (j \ne i)$ゆえ，$x \equiv \sum_{j=1}^{m} n_jx_j \equiv n_ix_i \equiv b_i \pmod{p_i}$）

［命題3.2］（中国剰余定理：解の存在と一意性）

アルゴリズム2のxは解である．また，$x, y \in \mathbb{Z}_n$が2つの解なら，$x = y$．//

（証明） $n_j \equiv 0 \pmod{p_j}\,(j \neq i)$ ゆえ， $x \equiv \sum_{j=1}^{m} n_j x_j \equiv n_i x_i \equiv b_i \pmod{p_i}\ (1 \leq i \leq m)$．ゆえに， x は解である．

命題3.1より， $x - y \equiv 0 \pmod{p_i}$．すなわち， $p_i \mid (x-y)\ (1 \leq i \leq m)$．ゆえに， $n \mid (x-y)$．これと $-n < x - y < n$ より， $x = y$．//

［例］（105算）3で割って余り1，5で割って余り2，7で割って余り3となる最小の非負整数は？

$p_1 = 3, p_2 = 5, p_3 = 7$ は互いに素で， $n = p_1 p_2 p_3 = 3 \cdot 5 \cdot 7 = 105$．したがって，問題は連立不定方程式 $x \equiv b_1 = 1 \pmod{p_1}, x \equiv b_2 = 2 \pmod{p_2}, x \equiv b_3 = 3 \pmod{p_3}$ の最小非負整数解 x を求めることにある．

命題3.2より， $0 \leq x < n$ を満たす解が唯一つある．それがこの方程式を満たす最小の非負整数解であることは明らか．

さて， $n_1 = n / p_1 = 35, n_2 = n / p_2 = 21, n_3 = n / p_3 = 15$ と置くと，

$$n_1 2 \equiv 1 \pmod{p_1}, n_2 1 \equiv 1 \pmod{p_2}, n_3 1 \equiv 1 \pmod{p_3}$$

より， $\bar{n}_1 = 2, \bar{n}_2 = \bar{n}_3 = 1$．ゆえに，アルゴリズム2より，

$$\begin{aligned} x &= \mathrm{mod}(n_1 \bar{n}_1 b_1 + n_2 \bar{n}_2 b_2 + n_3 \bar{n}_3 b_3, n) \\ &= \mathrm{mod}(70 b_1 + 21 b_2 + 15 b_3, n). \end{aligned}$$

元の問題では，

$$x = \mathrm{mod}(70 + 42 + 45, 105) = 52$$

が解となる．//

◎ m 変数不定方程式 $\sum_{i=1}^{m} n_i x_i \equiv b \pmod{n}, x_i \in \mathbb{Z}_{p_i} (1 \leq i \leq m)$

＜アルゴリズム3＞

(1) $n_i x_i \equiv b \pmod{p_i}\,(1 \leq i \leq m)$ を解く．（アルゴリズム1より， $x_i = \mathrm{mod}(\bar{n}_i b, p_i)$）

（ $p_i \mid n_j\ (j \neq i)$ ゆえ， $s = \sum_{j=1}^{m} n_j x_j \equiv n_i x_i \equiv b \pmod{p_i}$．ゆえに， $p_i \mid (s-b)\ (1 \leq i \leq m)$．すなわち， $n \mid (s-b)$）

［命題3.3］（解の一意性）

$\sum_{i=1}^{m} n_i x_i \equiv \sum_{i=1}^{m} n_i y_i \equiv b \pmod{n}, x_i, y_i \in \mathbb{Z}_{p_i}\ (1 \leq i \leq m)$ なら， $x_i = y_i\ (1 \leq i \leq m)$．

（証明） $p_i \mid n_j\ (j \neq i), p_i \mid n$ ゆえ， $n_i x_i \equiv \sum_{i=1}^{m} n_i x_i \equiv b \pmod{p_i}$．同じく $n_i y_i \equiv b \pmod{p_i}$．ゆえに，命題3.1より $x_i = y_i$．//

３．２　Goodのアルゴリズムと計算量

p_1, p_2 は互いに素，$n = p_1 p_2$ とする．$n_1 = n / p_1 = p_2, n_2 = n / p_2 = p_1$ とする．さらに，$\bar{n}_1 n_1 \equiv 1 \pmod{p_1}, \bar{n}_2 n_2 \equiv 1 \pmod{p_2}$ で $\bar{n}_1, \bar{n}_2$ を定める．p_1, p_2 が互いに素でなければならないことは，Goodのアルゴリズムの，Cooley-Tukeyのアルゴリズムにはない，制約である．

3.2.1 データの順序づけ

△ 出力写像：$\varphi : \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \to \mathbb{Z}_n$

$\boldsymbol{k} = (k_1, k_2) \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}$ に対し，$\varphi(\boldsymbol{k}) = \mathrm{mod}\left(n_1 k_1 + n_2 k_2, n\right)$．

［命題3.4］φ は全単射．

（証明）$\left|\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}\right| = p_1 p_2 = n = \left|\mathbb{Z}_n\right|$．また，命題3.3より任意の $k \in \mathbb{Z}_n$ に対し，

$$\sum_{i=1}^{2} n_i k_i \equiv k \pmod{n}, k_i \in \mathbb{Z}_{p_i} \ (i = 1,2)$$

を満たす k_1, k_2 の組が唯一つ存在する．//

△ 入力写像：$\psi : \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \to \mathbb{Z}_n$

$\boldsymbol{l} = (l_1, l_2) \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}$ に対し，$\psi(\boldsymbol{l}) = \mathrm{mod}\left(n_1 \bar{n}_1 l_1 + n_2 \bar{n}_2 l_2, n\right)$．

［命題3.5］ψ は全単射．

（証明）$\left|\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}\right| = p_1 p_2 = n = \left|\mathbb{Z}_n\right|$．また，任意の $l \in \mathbb{Z}_n$ に対し，

$$n_1 \bar{l}_1 + n_2 \bar{l}_2 \equiv l \pmod{n}, \ \bar{l}_i \in \mathbb{Z}_{p_i} \ (i = 1,2)$$

が解ける．さらに，$l_i = \mathrm{mod}(n_i \bar{l}_i, p_i) \in \mathbf{Z}_{p_i}$ とすれば，

$$\psi(l_1, l_2) \equiv n_1 \bar{n}_1 l_1 + n_2 \bar{n}_2 l_2 = n_1 \bar{n}_1 (n_1 \bar{l}_1) + n_2 \bar{n}_2 (n_2 \bar{l}_2) \pmod{n},$$
$$l \equiv n_1 \bar{l}_1 + n_2 \bar{l}_2 \pmod{n}$$

ゆえ，

$$\psi(l_1, l_2) \equiv n_1 \bar{n}_1 n_1 \bar{l}_1 + n_2 \bar{n}_2 n_2 \bar{l}_2 \equiv 1 n_1 \bar{l}_1 + 0 \equiv n_1 \bar{l}_1 + n_2 \bar{l}_2 \equiv l \pmod{p_1}.$$

同じく，$\psi(l_1, l_2) \equiv l \pmod{p_2}$．ゆえに，$\psi(l_1, l_2) \equiv l \pmod{n}$．これと，$\psi(l_1, l_2), l \in \mathbb{Z}_n$ より，$\psi(l_1, l_2) = l$．//

［命題3.6］任意の $\boldsymbol{k} = (k_1, k_2), \boldsymbol{l} = (l_1, l_2) \in \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2}$ について，

$$\varphi(\boldsymbol{k}) \psi(\boldsymbol{l}) \equiv k_1 l_1 n_1 + k_2 l_2 n_2 \pmod{n}.$$

（証明）$n_1 p_1 = n$．また，$n_1 \bar{n}_1 \equiv 1 \pmod{p_1}$ より $p_1 \left| (n_1 \bar{n}_1 - 1) \right.$．ゆえに，$n \left| n_1 (n_1 \bar{n}_1 - 1) = n_1^2 \bar{n}_1 - n_1 \right.$．したがって，$n_1^2 \bar{n}_1 \equiv n_1 \pmod{n}$．同じく，$n_2^2 \bar{n}_2 \equiv n_2 \pmod{n}$．また，$n_1 n_2 = p_2 p_1 = n$．よって，

$$\begin{aligned}\varphi(\boldsymbol{k})\psi(\boldsymbol{l}) &\equiv \left(n_1k_1+n_2k_2\right)\left(n_1\bar{n}_1l_1+n_2\bar{n}_2l_1\right) \equiv n_1^2\bar{n}_1k_1l_1+n_1n_2\bar{n}_2k_1l_2+n_1n_2\bar{n}_1k_2l_1+n_2^2\bar{n}_2k_2l_2 \\ &\equiv k_1l_1n_1+k_2l_2n_2 \pmod n\end{aligned} \tag{3.2}$$

である．//

３．３ アルゴリズム

命題3.5より，$\boldsymbol{l}=(l_1,l_2)$ が $\mathbb{Z}_{p_1}\times\mathbb{Z}_{p_2}$ 内をくまなく動くと，$l=\psi(\boldsymbol{l})$ は $\mathbb{Z}_n$ 内をくまなく動く．ゆえに，n 項DFT

$$\begin{aligned}&\boldsymbol{c}=W_n\boldsymbol{f},\\ &c_k=\sum_{l=0}^{n-1}\omega_n{}^{kl}f_l \quad (0\le k<n)\end{aligned}$$

で，$k=\varphi(\boldsymbol{k})$ として，

$$c_{\varphi(\boldsymbol{k})}=\sum_{l_1=0}^{p_1-1}\sum_{l_2=0}^{p_2-1}\omega_n{}^{\varphi(\boldsymbol{k})\psi(\boldsymbol{l})}f_{\psi(\boldsymbol{l})}\,. \tag{3.3}$$

さて，一般に $i\equiv j\pmod n$ なら $\omega_n{}^i=\omega_n{}^j$ だから，命題3.6より，

$$\omega_n^{\varphi(\boldsymbol{k})\psi(\boldsymbol{l})}=\omega_n^{k_1l_1n_1+k_2l_2n_2}=\omega_{p_1}^{k_1l_1}\omega_{p_2}^{k_2l_2}\,.$$

したがって，

$$c_{\varphi(\boldsymbol{k})}=\sum_{l_1=0}^{p_1-1}\omega_{p_1}^{k_1l_1}\sum_{l_2=0}^{p_2-1}\omega_{p_2}^{k_2l_2}f_{\psi(\boldsymbol{l})}\quad\left(\boldsymbol{k}=(k_1,k_2)\in\mathbb{Z}_{p_1}\times\mathbb{Z}_{p_2}\right). \tag{3.4}$$

係数 $c_{\varphi(k_1,k_2)}$ $(0\le k_1<p_1,0\le k_2<p_2)$ は，以下のようにして計算できる．

◎基本アルゴリズム

(1) 内DFT（$p_1\times\mathrm{DFT}_{p_2}$）：$0\le l_1<p_1$ について

$$\hat{f}_{l_1,k_2}=\sum_{l_2=0}^{p_2-1}\omega_{p_2}^{k_2l_2}f_{\psi(l_1,l_2)}\left(0\le k_2<p_2\right). \tag{3.5}$$

(2) 外DFT（$p_2\times\mathrm{DFT}_{p_1}$）：$0\le k_2<p_2$ について

$$c_{\varphi(\boldsymbol{k})}=\sum_{l_1=0}^{p_1-1}\omega_{p_1}^{k_1l_1}\hat{f}_{l_1,k_2}\quad\left(0\le k_1<p_1\right). \tag{3.6}$$

◎計算量

計算量は内DFTと外DFTの計算量の和となる．Cooley-Tukeyのアルゴリズムと比較して，「回転」が不要であることが特徴である．

p_1 あるいは p_2 が互いに素な因子に分解できるときは，式(3.6), (3.5)に基本アルゴリズムを再帰的に用いることができる．これが，Goodのアルゴリズムである．計算量は次の定理．

［定理3.7］項数 $n=p_1p_2\cdots p_m$ の因子 $p_1,\cdots,p_m$ は互いに素とする．DFT_p の乗算数を $\mu(p)$，加算数を $\alpha(p)$ とすると，DFT_n に対するGoodのアルゴリズムの乗算数は

$$\mu(n) = n\sum_{i=1}^{m}\frac{\mu(p_i)}{p_i}, \tag{3.8}$$

加算数は

$$\alpha(n) = n\sum_{i=1}^{m}\frac{\alpha(p_i)}{p_i} \tag{3.9}$$

である．

（証明）乗算数(3.8)を m に関する帰納法で証明する． $m=1, n=p_1$ のときは自明である．ある $m \geq 1$ で成立したとすると， $n = p_1 p_2 \cdots p_m p_{m+1} = n' p_{m+1}$ について，帰納法の仮定

$$\mu(n') = n'\sum_{i=1}^{m}\frac{\mu(p_i)}{p_i}$$

と基本アルゴリズムより，

$$\mu(n) = p_{m+1}\mu(n') + n'\mu(p_{m+1}) = p_{m+1}n'\sum_{i=1}^{m}\frac{\mu(p_i)}{p_i} + n\frac{\mu(p_{m+1})}{p_{m+1}} = n\sum_{i=1}^{m+1}\frac{\mu(p_i)}{p_i}$$

となる．ゆえに，任意の $m \geq 2$ で(3.8)が成立する．

加算数も同様である．//