高速乗算法の設計と実装 (2)

梅谷 武

作成：2001-09-12 更新：2005-04-20

メルセンヌ素数を標数とする 2 次体上の離散フーリエ変換を使った 32bit 算術演算器向け高速乗算法を設計し、Pentium への実装を試みる。
IMS:20010912001; NDC:412.1; keywords:離散 Fourier 変換, メルセンヌ素数, 2 次体;

目　　次

1　メルセンヌ素数を標数とする 2 次体

1.1　有限体上の離散フーリエ変換

「高速乗算法の設計と実装 (1)」(→ [N6]) においては素体 $\mathbf{F}_p$ 上の離散フーリエ変換について考えたが、ここでは一般の有限体上の離散フーリエ変換について考える。

命題 1.1 有限体 $\mathbf{F}_q$ において

$$1 \text{ の原始 } n \text{ 乗根} \zeta_n \in \mathbf{F}_q \Leftrightarrow n | q-1$$

証明　単元群 $(\mathbf{F}_q)^*$ は位数 $q-1$ の巡回群であるから、その生成元 $\zeta \in \mathbf{F}_q$ が存在する。ζ は

$$\zeta^{q-1} = 1, \zeta^k \neq 0 (0 \leqq k < q-1)$$

という性質によって特徴付けられている。一方 1 の原始 n 乗根 ζ_n は、

$$\zeta_n^n = 1, \zeta_n^k \neq 0 (0 \leqq k < n)$$

という性質によって特徴付けられている。$n | q-1$ のとき、もし生成元 $\zeta \in \mathbf{F}_q$ が与えられたならば、

$$\zeta_n = \zeta^{(q-1)/n}$$

とおくことによって一つの 1 の原始 n 乗根が得られる。証明は群論のラグランジュの定理を単元群 $(\mathbf{F}_q)^*$ に適用すればよい。■

1 の原始 n 乗根 ζ_n が存在する場合に条件 3

$$n > k > 0 \rightarrow \sum_{i=0}^{n-1} \zeta_n^{ik} = 0$$

について考える。

$$(\sum_{i=0}^{n-1} \zeta_n^{ik})(1 - \zeta_n^k) = 1 - \zeta_n^{kn} = 0$$

が可換環であるという条件だけで成立するが、ここで $1 \neq \zeta_n^k$ であるから、すべての k について $(1 - \zeta_n^k)$ が単元であるとき条件 3 が満たされることがわかる。体上ではこの条件はつねに満たされる。

定理の形でまとめると次のようになる。

定理 1.2 (有限体上の離散フーリエ変換) 有限体 $\mathbf{F}_q$ において

$$n|q-1 \Leftrightarrow \exists \zeta_n \in \mathbf{F}_q : (n, \mathbf{F}_q, \zeta_n) \text{ は離散フーリエ変換の型}$$

1.2 メルセンヌ素数を標数とする２次体

メルセンヌ素数、すなわち、

$$p = 2^k - 1, k = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, \cdots$$

の形の素数について考える。平方剰余の第 1 補充法則より

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & p \equiv 1 (mod\, 4) \\ -1 & p \equiv 3 (mod\, 4) \end{cases}$$

であるから、-1 は p を法として平方非剰余である。したがって $\mathbf{F}_p$ 上の多項式 $x^2 + 1$ は既約であり、剰余環 $\mathbf{F}_p[x]/(x^2+1)$ は $\mathbf{F}_p$ 上２次の拡大体となる。これはガウスの複素整数 $\mathbf{Z}[i], i^2 = -1$ をイデアル (p) で剰余した $\mathbf{Z}_p[i]$ と体として同型である。$\mathbf{Z}_p[i]$ の元は、

$$a + bi, a, b \in \mathbf{Z}_p$$

と表現することができ、加算と乗算は

$$(a + bi) + (c + di) = (a + c) + (b + d)i,\ a, b, c, d \in \mathbf{Z}_p$$
$$(a + bi)(c + di) = (ac - bd) + (bc + ad)i,\ a, b, c, d \in \mathbf{Z}_p$$

という式で計算することができる。

定理 1.2 により、$\mathbf{Z}_p[i]$ を係数体としたとき、長さ n の離散フーリエ変換が存在するための必要十分条件は、

$$n|2^{k+1}(2^{k-1} - 1)$$

である。

メルセンヌ素数 $M_{31} = 2^{31} - 1$ を法とする剰余演算は、32 ビット算術演算器で効率よく処理することができる。高速乗算法 (2) はこの性質を利用して実装される。離散フーリエ変換の長さ n として

$$n|2^{32}(2^{30} - 1)$$

なるものが使用できるので当面の目的には十分である。

1.3 原始根

$p = M_{31}$ とし、$\mathbf{Z}_p[i]$ 上の離散フーリエ変換を行なうにあたってその原始根を求めなければならない。一般に大きい有限体の原始根を探索することは計算量が多く難しい問題であるが、この場合は、原始根探索プログラムによって比較的簡単に原始根

$$12 + i$$

を発見することができた。

離散フーリエ変換の長さ N としては

$$N = 2^n, 0 < n \leqq 32$$

という形のものを使うことにする。この N は離散フーリエ変換の条件を満たし、さらに原始根 $12 + i$ を使って 1 の原始 N 乗根を

$$(12 + i)^t, t = 2^{32-n}(2^{30} - 1), 0 < n \leqq 32$$

と表現することができる。

2 高速乗算法 (2)

2.1 高速乗算法 (2) の構造

Step 1. 数の P 進表現

基数を $P = 2^{32}$ とし、長さを

$$N = 2^n, 0 < n \leqq 30$$

とする。正の整数 a, b が次のように P 進表現されるものとする。

$$a = a_{N-1}P^{N-1} + \cdots + a_1P + a_0, 0 \leqq a_i < P$$
$$b = b_{N-1}P^{N-1} + \cdots + b_1P + b_0, 0 \leqq b_i < P$$

この積について $0 \leqq ab < P^N$ が成り立つと仮定する。

Step 2. 多項式としての積の計算

$P^K \equiv 1 (\mathrm{mod}\, P^N - 1)$ より、

$$c = ab \equiv \sum_{r=0}^{N-1} \Big(\sum_{s+t \equiv r (mod N)} a_s b_t \Big) P^r (\mathrm{mod}\, P^N - 1)$$

となる。この係数 $c_r = \sum_{s+t \equiv r (mod N)} a_s b_t$ の大きさを評価すると、

$$0 \leqq c_r \leqq N(2^{32} - 1)^2$$

となる。

Step 3. 係数の分解

2 つの不等式

$$N < M_{31} = 2^{31} - 1$$
$$(2^{32} - 1)^2 < T_5 = 2^{32}(2^{32} - 1) + 1$$

より、係数 c_r を

$$0 \leqq c_r < M_{31}T_5$$

によって評価する。係数を M_{31} を法とした場合と T_5 を法とした場合の 2 つに分解する。

$$\begin{aligned} a'_r &\equiv a_r (\mathrm{mod}\, M_{31}) \\ b'_r &\equiv b_r (\mathrm{mod}\, M_{31}) \\ a''_r &\equiv a_r (\mathrm{mod}\, T_5) \\ b''_r &\equiv a_r (\mathrm{mod}\, T_5) \end{aligned}$$

Step 4. **離散フーリエ変換による係数の計算**

c'_r は、$(N, \mathbf{Z}_{M_{31}}[i], \omega), \omega = (12+i)^t, t = 2^{32-n}(2^{30}-1)$ 型の離散 Fourier 変換を利用して次のように計算する。

$$\begin{aligned} F(a')_k &= \sum_{s=0}^{N-1} a'_s \omega^{sk} \quad (in \mathbf{Z}_{M_{31}}[i]) \\ F(b')_k &= \sum_{t=0}^{N-1} b'_t \omega^{tk} \quad (in \mathbf{Z}_{M_{31}}[i]) \\ c'_r &= N^{-1} \sum_{k=0}^{N-1} F(a')_k F(b')_k \omega^{-kr} \quad (in \mathbf{Z}_{M_{31}}[i]) \end{aligned}$$

c''_r は、$(N, \mathbf{F}_{T_5}, \zeta), \zeta = 7^t, t = 2^{32-n}(2^{32}-1)$ 型の離散 Fourier 変換を利用して次のように計算する。

$$\begin{aligned} F(a'')_k &\equiv \sum_{s=0}^{N-1} a''_s \zeta^{sk} \quad (\mathrm{mod}\, T_5) \\ F(b'')_k &\equiv \sum_{t=0}^{N-1} b''_t \zeta^{tk} \quad (\mathrm{mod}\, T_5) \\ c''_r &\equiv N^{-1} \sum_{k=0}^{N-1} F(a'')_k F(b'')_k \zeta^{-kr} \quad (\mathrm{mod}\, T_5) \end{aligned}$$

Step 5. **孫子の剰余定理による連立方程式の解法**

$(M_{31}, T_5) = 1$ であるから、孫子の剰余定理から c_r を、連立合同式

$$\begin{aligned} c_r &\equiv c'_r (\mathrm{mod}\, M_{31}) \\ c_r &\equiv c''_r (\mathrm{mod}\, T_5) \end{aligned}$$

を解くことによって求めることができる。

Step 6. **桁上げ処理**

最後に $c_r, r = 0, \cdots, K-1$ に桁上げ処理を施すことで、$c = ab$ の P 進表現が得られる。

参考文献

計算数論

[N1] 和田 秀男, “コンピュータと素因子分解 改訂版”, 遊星社, 1999

[N2] 和田 秀男, “高速乗算法と素数判定法”, 上智大学数学教室, 1983
[N3] 梅谷 武, 離散 *Fourier* 変換
[N4] 梅谷 武, ストラッセン-ショーンハーゲ法
[N5] Daniel J. Bernstein, *Multidigit multiplication for mathematicians*
[N6] 梅谷 武, 高速乗算法の設計と実装 *(1)*
[N7] I. S. Reed, T. K. Truong, *“The use of finite fields to compute convolution”*, IEEE Trans.IT-21, 208-213, 1975
[N8] I. S. Reed, T. K. Truong, *“Complex integer convolutions over a direct sum of Galois fields”*, IEEE Trans.IT-21, 657-661, 1975

算法

[S1] 野下 浩平, 高岡 忠雄, 町田 元, “基本的算法”, 岩波書店, 1983
[S2] D. E. Knuth(中川 圭介訳), “準数値算法/算術演算”, サイエンス社, 1986
[S3] H. J. Nussbaumer(佐川雅彦他訳), “高速フーリエ変換のアルゴリズム”, 科学技術出版社, 1989
[S4] David H. Bailey, *The computation of π to 29,360,000 decimal digits using Borweins’ quartically convergent algorithm*
[S5] Mikko Tommila, *Number theoretic transforms*

ディジタル信号処理

[D1] 電子情報通信学会, “ディジタル信号処理の基礎”, コロナ社, 1988
[D2] G. A. Jullien, *Number theoretic techniques in digital signal processing*
[D3] G. A. Jullien, *Residue arithmetic with application in digital signal processing*