高速乗算法の設計と実装 (3)

梅谷 武

作成：2001-09-20 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。高速乗算法 (2) においては係数を分解したが、高速乗算法 (3) は係数を分解しないで計算する。
IMS:20010920001; NDC:412.1; keywords:離散 Fourier 変換, メルセンヌ素数, 2 次体;

目　　次

1　高速乗算法 (3)

1.1　高速乗算法 (3) の構造

Step 1. 数の P 進表現

基数を $P = 2^{32}$ とし、長さを

$$N = 2^n, 0 < n \leqq 25$$

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 $c_r = \sum_{s+t \equiv r(modN)} a_s b_t$ の大きさを評価すると、

$$0 \leqq c_r \leqq N(2^{32} - 1)^2 < 2^{89} - 1$$

となる。

Step 3. **離散フーリエ変換による係数の計算**

c_r は、$(N, \mathbf{Z}_{M_{89}}[i], \zeta), \zeta = (6+i)^t, t = 2^{90-n}(2^{88}-1)$ 型の離散 Fourier 変換を利用して次のように計算する。

$$F(a)_k = \sum_{s=0}^{N-1} a_s \zeta^{sk} \quad (in \mathbf{Z}_{M_{89}}[i])$$

$$F(b)_k = \sum_{t=0}^{N-1} b_t \zeta^{tk} \quad (in \mathbf{Z}_{M_{89}}[i])$$

$$c_r = N^{-1} \sum_{k=0}^{N-1} F(a)_k F(b)_k \zeta^{-kr} \quad (in \mathbf{Z}_{M_{89}}[i])$$

Step 4. **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

[N9] 梅谷 武, 高速乗算法の設計と実装 *(2)*

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*