2 次の DBPS2 による因数分解

2006/09/01　　後 保範
2006/10/22　改訂(複数多項式)

1. 概要

2 次多項式を使用した DBPS(Double Base Polynomial Sieve, 2 重基底多項式篩法)の改訂版(DBPS2, Double Base Polynomial Sieve 2nd, 改訂 2 重基底多項式篩法)である。

N を分解対象数とするとき、 $f_k(x)=A_kx^2+B_kx+C_k$, $f(M_k)\equiv 0 \pmod N$ となる複数個($k=1,2,\cdots,L$)の多項式 $f_k(x)$ と整数 M_k を求める。

次に、一定の範囲の整数 a_k,b_k に対して、下記で s_kx+t_k を計算する。

$$S_kx+T_k=(\alpha_kx+a_k)\cdot(\beta_kx+b_k)-f_k(x)$$
$$S_k=\beta_ka_k+\alpha_kb_k-B_k,\ T_k=a_kb_k-C_k,\ \ A_k=\alpha_k\cdot\beta_k \qquad \text{---- (1)}$$
$$G_k=sign(S_k)\cdot GCD(|S_k|,|T_k|),\ s_k=S_k/G_k,\ t_k=T_k/G_k$$

このとき、s_kx+t_k が同一で G_k が異なるもの及び、s_kx+t_k が α_kx+a_k 又は β_kx+b_k と一致するものを、α_kx+a_k 、β_kx+b_k 及び s_kx+t_k を分解する素数基底の個数以上ふるいで集める。

このふるい処理において、イデアル $\alpha_k\theta+a_k$ 及び $\beta_k\theta+b_k$ が素イデアル基底で分解できるものを使用するのが、DBPS2 の特徴である。それは、素イデアル基底で分解できるものを使用すると、S_kx+T_k もまた素イデアル基底で分解でき、G_k だけ異なり、s_kx+t_k が同じとなるものが多く発生し、ふるいの効率が向上するためである。

DBPS2 は TBPS2 と異なり、素イデアル基底は整数 a_k,b_k の選定にだけ使用し、GNFS(一般数体ふるい法)で行う処理は使用しないで、素数基底(途中で追加あり)だけを使用してふるいをおこなう。

2. 多項式算出

与えられた整数 N に対して、 $f_k(x)=A_kx^2+B_kx+C_k$, $f_k(M_k)\equiv 0 \pmod N$ となる、L 個の 2 次多項式の整数係数 A_k,B_k,C_k 及び整数 M_k を求める。このとき、$A_k\geq 1$ で $A_k+|B_k|+|C_k|$ が小さく、A_k が整数 α_k 及び β_k で分解できるものを採用する。

3. DBPS2 ふるい

p 以下の素数で基本素数基底 P1 を構成する。また各 $f_k(x)$ に対応する素イデアル基底 Q_k(θ は $f_k(\theta)=0$ の根)を求める。このとき、素イデアル基底 Q_k の要素数は素数基底 P1 より大幅に少なくする。各 k 対して基準値 ma_k,mb_k を定め、$|a_k|\leq ma_k,|b_k|\leq mb_k$ と

なる整数a_k, b_kに対して、$\alpha_k M_k + a_k$及び$\beta_k M_k + b_k$が基本素数基底 P1 で分解されるもの及び、イデアル$\alpha_k \theta + a_k$及び$\beta_k \theta + b_k$が素イデアル基底 Qk で分解されるものを求める。このとき、$\alpha_k M_k + a_k$及び$\beta_k M_k + b_k$が基本素数基底 P1 以外の整数で分解されるなら、その整数を追加素数基底 P2 に追加する。P1 と P2 を合わせたものを素数基底 P とする。ここで求めた、$\alpha_k x + a_k$と$\beta_k x + b_k$を乗算して式(1)で$s_k x + t_k$及びG_kを求める。同じ$s_k x + t_k$でG_kが異なるものが 2 回以上発生するか、$s_k x + t_k$が$\alpha_k x + a_k$又は$\beta_k x + b_k$と一致したものを集める。また、基本区間(s_k, t_kが小さいもの)に対しては、$s_k M + t_k$が素数基底 P で分解するふるいを行い、分解されるものを集める。このふるいで集めた$s_k x + t_k$の個数(重複削除後)が素数基底 P の個数を超えればふるいは完了する。

3.1 基本基底

(1) 基本素数基底

p以下の全ての素数及び-1 を基本素数基底 P1 とする。

(2) 素イデアル基底

基本素数基底 P1 に含まれる h 個の素数p_jに対して、$f_k(s_{kj}) \equiv 0 \pmod{p_j}$が成立する$(p_k : s_k)$を全て求め、素イデアル基底(Qk)とする。

素イデアル基底 Qk は$\alpha_k x + a_k$及び$\beta_k x + b_k$の選定にだけ使用する。

イデアル$c\theta + d$が素イデアル$(p_j : s_{kj})$で分解されるとは、$N(c\theta + d)$がp_jで分解されることである。ここで、$N_k(c\theta + d)$は下記で定義する。

$$N_k(c\theta + d) = c^2 \mid f_k(-d/c) \mid = \mid A_k d^2 - B_k cd + C_k c^2 \mid$$

3.2 $\alpha_k x + a_k, \beta_k x + b_k$の選定と追加基底

各$k(k = 1,2,\cdots,L)$に対して下記処理を行う。

$\mid a_k \mid \leq m a_k, \mid b_k \mid \leq m b_k$となる整数$a_k, b_k$で$\alpha_k x + a_k, \beta_k x + b_k$に対して下記の処理を行う。また、これだけで、必要なふるい結果が得られない場合は、Lの値を増加して同様な処理を行う。以下、$\alpha_k x + a_k$について示すが、$\beta_k + b_k$も同様である。項番(1)は総ての k に対して、P1 で一度行い、再度 P=P1+P2 として再度行う。

(1) $\alpha_k M_k + a_k$が素数基底 P で分解されたら$\alpha_k M_k + a_k$を採用する。

(2) $\alpha_k \theta + a_k$の素イデアル基底 Qk による分解

$N_k(\alpha_k \theta + a_k) = \mid A_k a_k^2 - B_k \alpha_k a_k + C_k \alpha_k^2 \mid$が素イデアル基底 Qk で完全分解されるかのチェックを行う。分解されたら$\alpha_k \theta + a_k$は採用し、(3)の処理を行う。

(3) $\alpha_k M_k + a_k$の基本素数基底 P1 による分解

$\alpha_k M_k + a_k$を素数基底 P1 で分解する。

もし、P1 だけでは分解されなければ、新しい因数uを P2 に追加する。

3.3 DBPS2 によるふるい

(1) $G_k, s_k x+t_k$ の算出

選定した、$\alpha_k x+a_k$ 及び $\beta_k x+b_k$ から下記で $s_k x+t_k$ 及び G_k を求める。

求める順序は $S_k = 0,\pm1,\pm2,\cdots$ の順に行う。

$$S_k x+T_k = (\alpha_k x+a_k)\cdot(\beta_k x+b_k) - f_k(x)$$

$$S_k = \beta_k a_k + \alpha_k b_k - B_k,\ T_k = a_k b_k - C_k,\ A_k = \alpha_k \cdot \beta_k$$

$$G_k = sign(S_k)\cdot GCD(|S_k|,|T_k|),\ s_k = S_k / G_k,\ t_k = T_k / G_k$$

$\alpha_k x+a_k, \beta_k x+b_k$ 及び $s_k x+t_k$ と G_k を合わせて 1 データとして、記録する。

このとき、$G_1 = GCD(\alpha_k, |a_k|), G_2 = GCD(\beta_k, |b_k|)$ を求め、

$$\alpha_k = \alpha_k / G_1,\ a_k = a_k / G_1,\ \beta_k = \beta_k / G_2,\ b_k = b_k / G_2$$

と変更し、G_1, G_2 も一緒に記憶する。

(2) $s_k x_k + t_k, G_k$ でのソート

記憶したデータを s_k, t_k, G_k の上昇順にソートする。

3.4 重複データ削除

(1) $G_k, s_k x+t_k$ が共に同じデータ

採択データで $G_k, s_k x+t_k$ が共に一致するデータは、2 件目以降を削除する。

(2) 2 個のデータの右辺及び左辺が一致するデータ

$s_k x+t_k$ が $\alpha_k x+a_k$ 及び $\beta_k x+b_k$ に一致したもので、下記の様に右辺と左辺が一致し、他のデータと同一になるときは、2 つめのデータを削除する。

$$G_{j1}\cdot(\alpha_k x+a_{k1})\cdot(\beta_k x+b_{k1}) = G_{k1}\cdot(\alpha_k x+a_{k2}) = G_{k1}\cdot(s_{k1} x+t_{k1})$$

×) $G_{j2}\cdot(\alpha_k x+a_{k2})\cdot(\beta_k x+b_{k2}) = G_{k2}\cdot(\beta_k x+b_{k1}) = G_{k2}\cdot(s_{k2} x+t_{k2})$ ⇐ 削除

$$G_{j1}\cdot G_{j2}\cdot(\alpha_k x+a_{k1})\cdot(\beta_k x+b_{k2}) = G_{k1}\cdot G_{k2}$$

3.5 採択データ選定

(1) $S_k = 0$ で T_k が素数基底 P で分解されるもの。

このデータを区分 1 とする。

(2) 基本区間($s_k \le SL_k, |t| \le TL_k$)で $s_k M_k + t_k$ が素数基底 P で分解されるもの。

このデータも区分 1 とする。

(3) $\alpha_k x+a_k, \beta_k x+b_k$ と一致するデータ

$s_k x+t_k$ が $\alpha_k x+a_k$ 及び $\beta_k x+b_k$ に一致したもの。

このデータを区分 3 とする。

(4) 同じ $s_k x+t_k$ で G_k が異なるデータ

$s_k x+t_k$ が $\alpha_k x+a_k$ 及び $\beta_k x+b_k$ と一致せず、同じ $s_k x+t_k$ が 2 個以上あり、G_k が異なるもの。更に、$s_k M_k+t_k$ は基本区間外か又は、基本区間内だが素数基底 P で分解できないものとする。このデータを区分 2 とする。

3.6 行列作成

得られたデータの個数を nd とするとき、$nd \geq np+h, (h \approx 10\text{進桁数})$ なら行列作成を行う。この条件を満たさないなら、3.2 節に戻り、 L を増加して処理を続ける。

(1) 素数基底 P に 1 から np までの番号をつける。

(2) 行列作成（区分 1 及び 3 のデータ）

$$(\alpha_k x+a_k)\cdot(\beta_k x+b_k)=G_k\cdot(s_k x+t_k)$$

の式で、左辺の x を M_k で置き換えた $\alpha_k M_k+a_k$ 及び $\beta_k M_k+b_k$ を素数基底 P で分解(既に分解済み)し、その指数ベキを素数基底の番号の位置に正の符号を付けて入れる。一方、右辺の G_k 及び $s_k M_k+t_k$ を素数基底 P で分解(既に分解済み)し、その指数ベキを素数基底の番号の位置に負の符号を付けて入れる。

(3) 行列作成（区分 2 のデータ）

G_k が異なり、$s_k x+t_k$ が一致するもので作成する。h 個の同一な $s_k x+t_k$ から h-1 個の行列要素を作成する。j 個目と j+1 個目(j=1,2,…,h-1)から下記の様に作成する。

j 個目の左辺の $(\alpha_k M_k+a_k)\cdot(\beta_k M_k+b_k)$ 及び(j+1)個目の右辺の G_k を素数基底で分解し、その指数ベキを素数基底の番号の位置に正の符号を付けて入れる。また、(j+1)個目の左辺の $(\alpha_k M_k+a_k)\cdot(\beta_k M_k+b_k)$ 及び j 個目の右辺の G_k を素数基底で分解し、その指数ベキを素数基底の番号の位置に負の符号を付けて入れる。

4. 従属行の計算

(1) 行列の次元の縮小

3.6 節で作成した行列で、素数基底 P に対応するベキ指数の絶対値の合計が 1 以下となるものは、素数基底 P から除く。即ち、行列の行は削除後の素数基底 P に対応させ、列は除かれた素数基底に対応するべき指数が 1 つでも 0 以外がある行(データ)を取り除く。

(2) 0-1 行列の作成

項番(1)で作成した行列の要素に対して、(mod 2) を実施して 0 及び 1 だけの要素の 0-1 行列に変換する。この行列を A とする。

(3) 定義方式による従属行の計算

行列 A のサイズを $n\times np, (n>m)$ とする。行列 E を $n\times n$ の単位行列とする。

行列 A の左に行列 I を置き、 $n\times(np+n)$ の行列を作成する。この行列をガウスの消去法で行列 A の部分を完全に消去し、行列 A の部分が完全にゼロになった行以下の I の部分に従属行が現れる。

(4) 高速な従属行の計算

疎行列のまま、0-1 行列のガウス消去法を実施する。

詳細は 0-1 疎行列の直接解法を参照。

5. 因数分解

因数分解は 4 章で求めた、従属行の単位に行う。

(1) $\alpha^2 \equiv \beta^2 \pmod N$ の作成

素数基底 P の要素を $p_1, p_2, \cdots, p_{np}$ とする。このとき、従属行の各 p_k のベキを計算し、正の指数ベキは左辺に、負の指数ベキは右辺に纏めると下記のようになる。

$$\prod_{k=1}^{np}(p_k^{l_k})^2 \equiv \prod_{k=1}^{np}(p_k^{r_k})^2 \pmod N,\ \ 2l_k : p_k\text{の正の指数ベキ},\ 2r_k : p_k\text{の負の指数べき}$$

従って、左辺が α^2 に右辺が β^2 になる。

(2) 因数分解

$\alpha \equiv \beta \pmod N$ の場合は自明解となり因数分解できないが、それ以外なら

$N_1 = GCD(\alpha+\beta, N),\ N_2 = GCD(|\alpha-\beta|, N)$ とすると $N = N_1 \cdot N_2$ と分解される。