

```
1  /*****
2                                     Masazumi Kurihara    2009/03/25/
3      ファイル名 BadicExpansion.c
4
5      1. 10進数をB進数に変換し、その結果をファイルへ書き込むプログラム
6      2. ファイルからB進数を読み込み、10進数に変換し、画面に表示するプログラム
7
8      補足 1. 与えられた正整数 a, b, N に対し、 $a^b \equiv c \pmod{N}$  を計算する。
9              次に、計算結果 c を B 進数に変換し、その結果を指定したファイルへ
10             書き込む(出力する)。
11
12      2. 上記の B 進展開されたデータをファイルから読み込み、10進数に変換し、
13      画面に表示する(出力する)。
14
15      ただし、B=256とする。また、N の値は、 $2^8 \leq N \leq 2^{16} - 1$  を満たすものとする。
16      つまり、N は1バイトで表現できる整数より大きく、かつ、2バイト以内で表現できる
17      整数であるものとする。
18
19      10進数 c を B 進数 B1, B0 に展開する。c, B1, B0 の関係は以下の通り：
20
21       $c = (256 \times B1) + B0$ 
22
23      *****/
24
25 #include <stdio.h>
26
27 long N;
28 long e;
29 long d;
30 int B=256;
31
32 /*  $a^b \equiv c \pmod{N}$  を計算する関数 cal */
33 long cal( long a, long b )
34 {
35     int i;
36     long tmp;
37
38     tmp=a;
39     for ( i=1; i<b; i++){ /* b-1 回の乗算を実行する */
40         tmp = tmp*a % N; /* 毎回、モッドをとるように計算する */
41     }
42     return tmp; /* 計算結果を返す */
43 }
44
45 /* 入力された値 N が  $2^8 \leq N \leq 2^{16} - 1$  を満たすかをチェックする関数 */
46 check(long a)
47 {
48     if ( 0xff < a && a <= 0xffff ){
49         return 1;
50     }
51     else{
52         printf("\n");
53         printf(" Warning!! N = %ld is less than  $2^8$  or N = %ld is greater than
54                or equal to  $2^{16}$ .\n", a,a);
55         printf(" Warning!! N must be greater than or equal to  $2^8$  and
56                N must be less than  $2^{16}$  .\n", a);
57         printf("\n");
58         return -1;
59     }
60 }
61
62 /* 10進数をB進数に変換し、その結果をファイルへ書き込む関数 */
63 encode()
64 {
65     FILE *fopen(), *fpw;
66     char namew[20];
67     long c;
68     int B0, B1;
69
70     printf(" 10進数からB進数への変換をします。ただし、B=256 とする.\n");
71     printf(" 与えられた3個の正整数 a, b, N に対し、 $a^b \equiv c \pmod{N}$  を計算します.\n");
72     printf(" ただし、N は  $2^8 \leq N < 2^{16} - 1$  を満たす整数とする.\n");
73     printf(" a, b, N の値を 67 5 323 のように空白をはさんで入力して下さい。 : ");
74     scanf( "%d %d %d", &e, &d, &N );
75
76     if ( e>=1 && d>=1){ /* 入力された値 e, d が 正整数であるかをチェック */
77         if(check(N) == 1){ /* 入力された値 N が 正しいかを 関数 check にチェックさせる */
78
79             printf(" 出力file名を指定して下さい。 : ");
80             scanf("%s",namew); /* 書き出しファイル名の指定 */
81             printf("\n");
82
```

```
83         if((fpw=fopen(namew,"w")) == NULL) exit(-1); /* 書き出しファイルをオープンする */
84
85         c=cal(e,d);
86         printf(" 計算結果 %d^%d = %d (mod %d) \n", e, d, c, N );
87         /* c は2バイト以内で表現できる整数 */
88         B0 = c%B; /* c をB進法で2バイトに分割. その下位の桁の係数B0 */
89         B1 = (c - B0)/B; /* 上位の桁の係数 B1 */
90         printf(" B進数展開の結果 (B1,B0) = (%d, %d) such that
91             c = (B1 x 256) + B0 = (%d x 256) + %d = %d \n", B1,B0, B1,B0, c);
92         printf("\n");
93
94         fputc(B0,fpw); /* 下位の桁の係数 B0 をファイルに書き出す */
95         fputc(B1,fpw); /* 続いて, 上位の桁の係数 B1 をファイルに書き出す */
96
97         fclose(fpw); /* 書き出しファイルをクローズする */
98
99         printf(" 10進数 c=%d をB進数展開した (B1,B0)=(%d,%d) を指定file %s への
100             書き込み終了. \n", c,B1,B0,namew);
101     }
102 }
103 else{
104     printf("\n");
105     printf("もう一度, やり直してください. \n");
106 }
107 }
108
109 /* ファイルからB進数を読み込み, 10進数に変換し, 画面に表示する関数 */
110 decode()
111 {
112     FILE *fopen(), *fpr;
113     char namer[20];
114     int c, cc;
115     int B0,B1;
116
117     printf(" B進数から10進数への変換をします. \n");
118     printf(" B進数が書かれたfile名を指定して下さい. : ");
119     scanf("%s",namer); /* 読み込みファイル名の指定 */
120     printf("\n");
121
122     if((fpr=fopen(namer,"r")) == NULL) exit(-1); /* 読み込みファイルをオープンする */
123
124     while((cc=fgetc(fpr)) != EOF){ /* B進数の下位桁の係数 B0 を先に読み込む */
125         /* (ファイルの終り(EOF)まで読み込みを続ける) */
126
127         B0 = cc; /* 下位桁の係数 B0 */
128         B1=fgetc(fpr); /* 上位桁の係数 B1 の読み込み */
129
130         c=B1*B+B0; /* 10進数に変換し, その結果を変数 c に代入 */
131
132         /* 上記の計算結果 c を画面に出力 */
133         printf(" 10進数への変換結果 c = (B1 x 256) + B0 = (%d x 256) + %d = %d \n", B1,B0,c);
134         printf("\n");
135     }
136
137     fclose(fpr); /* 読み込みファイルをクローズする */
138
139     printf(" 指定file %s から読み込んだB進数 (B1,B0)=(%d,%d) を10進数 c=%d へ変換し,
140         画面表示終了. \n", namer, B1,B0,c );
141 }
142
143 main()
144 {
145     int sel;
146
147     printf(" 10進数からB進数への変換, または, その逆変換の計算をします. \n");
148     printf(" どちらの変換をするか数字 1 or 2 で選んで下さい. 1. 10進数からB進数へ,
149         2. B進数から10進数へ. \n");
150     printf(" 1 または 2 の数字を入力して下さい : ");
151     scanf("%d",&sel);
152     printf("\n");
153
154     if(sel == 1){ /* 選択肢 1 が選択された場合, 関数 encode を実行 */
155         encode();
156     }
157     else{
158         if(sel == 2){ /* 選択肢 2 が選択された場合, 関数 decode を実行 */
159             decode();
160         }
161         else{ /* 選択肢 1 と 2 以外が選択された場合, 警告のメッセージを画面表示する */
162             printf(" 選択番号 1 or 2 を選択して下さい \n");
163         }
164     }
165 }
```

```
165 }
166
167 /*****
168 コンパイル
169
170 lit46: gcc -o badic BadicExpansion.c
171
172 実行方法および動作について
173
174 lit46: badic
175     1 0 進数から B 進数への変換, または, その逆変換の計算をします。
176     どちらの変換をするか数字 1 or 2 で選んで下さい。1. 1 0 進数から B 進数へ, 2. B 進数から 1 0 進数へ
177
178     1 または 2 の数字を入力して下さい : 1
179
180     1 0 進数から B 進数への変換をします。ただし, B=256 とする。
181     与えられた3個の正整数 a, b, N に対し,  $a^b = c \pmod{N}$  を計算します。
182     ただし, N は  $2^8 \leq N < 2^{16} - 1$  を満たす整数とする。
183     a, b, N の値を 67 5 323 のように空白をはさんで入力して下さい。: 67 5 323
184     出力file名を指定して下さい。 : goo
185
186     計算結果  $67^5 = 288 \pmod{323}$ 
187     B 進数展開の結果  $(B1, B0) = (1, 32)$  such that  $c = (B1 \times 256) + B0 = (1 \times 256) + 32 = 288$ 
188
189     1 0 進数 c=288 を B 進数展開した  $(B1, B0)=(1, 32)$  を指定file goo への書き込み終了。
190 lit46: badic
191     1 0 進数から B 進数への変換, または, その逆変換の計算をします。
192     どちらの変換をするか数字 1 or 2 で選んで下さい。1. 1 0 進数から B 進数へ, 2. B 進数から 1 0 進数へ
193
194     1 または 2 の数字を入力して下さい : 2
195
196     B 進数から 1 0 進数への変換をします。
197     B 進数が書かれたfile名を指定して下さい。 : goo
198
199     1 0 進数への変換結果  $c = (B1 \times 256) + B0 = (1 \times 256) + 32 = 288$ 
200
201     指定file goo から読み込んだ B 進数  $(B1, B0)=(1, 32)$  を 1 0 進数 c=288 へ変換し, 画面表示終了。
202 lit46:
203 *****/
```