アルゴリズム論特講 （塩田）

2006 年 4 月 27 日の課題

課題 以下の規格に基づいて法演算を行う Python の関数を作成し、数当て手品プログラムを完成せよ。

規格

- 法 m の剰余系の数は $0, 1, \cdots, m-1$ として表現する。
- `mod(a,m)`
  整数 a を法 m の数に直した値を返す。($a < 0$ の場合も $0, 1, \cdots, m-1$ の範囲の剰余に取り直す。)
- `modadd(a,b,m)`
  返り値は $a + b$ `mod` m
- `modsub(a,b,m)`
  返り値は $a - b$ `mod` m
- `modmul(a,b,m)`
  返り値は $a \times b$ `mod` m

提出期限：未定 （ 512 号室ポストまで ）

雛形

```
#!/bin/env python
# 一行目は python プログラムとして実行するためのおまじない
# hina060427.py
#
# 最初の実行の前に chmod +x を忘れずに

from math import *    # 数学関数を使うためのまじない

# a を法 m の数に取り直す
def mod(a,m):
        x = a % m
        if x < 0:
                x = x + m
        return x

# 法 m での a+b
def modadd(a,b,m):
        ##### ここを埋めよ #####

# 法 m での a-b
def modsub(a,b,m):
```

```
        ##### ここを埋めよ #####

# 法 m での a*b
def modmul(a,b,m):
        ##### ここを埋めよ #####

# ここから main

print '2 桁の好きな数字を思い浮かべてください。'
a = input('その数を 3 で割った余りはいくつですか。')
b = input('その数を 5 で割った余りはいくつですか。')
c = input('その数を 7 で割った余りはいくつですか。')
x = modmul(70,a,105)
y = modmul(21,b,105)
z = modmul(15,c,105)
ans = modadd(modadd(x,y,105),z,105)
print 'それは ',ans,' ですね。'

# 実行例:
#
# 2 桁の好きな数字を思い浮かべてください。
# その数を 3 で割った余りはいくつですか。1
# その数を 5 で割った余りはいくつですか。2
# その数を 7 で割った余りはいくつですか。2
# それは  37  ですね。
```

C 言語による実装例

```
/* rep03.c */

#include<stdio.h>
#include<stdlib.h>

/* a を法 m の数に取り直す */
int mod(int a, int m)
{
        int b=a%m;
        return b<0 ? b+m : b;
}

/* 法 m での a+b */
int modadd(int a, int b, int m)
{
        return mod(a+b,m);
}

/* 法 m での a-b */
int modsub(int a, int b, int m)
{
        return mod(a-b,m);
}
```

```
/* 法 m での a*b */
int modmul(int a, int b, int m)
{
        return mod(a*b,m);
}

main()
{
        int a,b,c,x,y,z,ans;
        printf("2 桁の好きな数字を思い浮かべてください。\n");
        printf("その数を 3 で割った余りはいくつですか。");
        scanf("%d",&a);
        printf("その数を 5 で割った余りはいくつですか。");
        scanf("%d",&b);
        printf("その数を 7 で割った余りはいくつですか。");
        scanf("%d",&c);
        x = modmul(70,a,105);
        y = modmul(21,b,105);
        z = modmul(15,c,105);
        ans = modadd(modadd(x,y,105),z,105);
        printf("それは %d ですね。\n",ans);
}

/* 実行例:

2 桁の好きな数字を思い浮かべてください。
その数を 3 で割った余りはいくつですか。1
その数を 5 で割った余りはいくつですか。2
その数を 7 で割った余りはいくつですか。2
それは 37 ですね。

*/
```

法 2 における演算表

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

法 3 における演算表

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

法 4 における演算表

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

法 5 における演算表

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

法 6 における演算表

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1