アルゴリズム論特講 （塩田）

2006年5月18日の課題

課題

- 雛形プログラム hina0605018.py をダウンロードせよ。(前回の関数定義部 crypto060511.py も必要。)
- 関数 euclid を利用して、連立合同式

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

  の解 x を計算する関数 chinese（中国剰余アルゴリズム）を完成せよ。
- 法のビット数を取り替えて実行し、動作確認せよ。

提出期限：未定 （ 512号室ポストまで ）

雛形

```
#!/bin/env python
#
# hina060518.py

from sys import *
from math import *
from random import *
from crypto060511 import *    # crypto060511.py を引用

# 連立合同式 x = a ( mod m ), x = b ( mod n ) の解 x を返す関数
def chinese(a,b,m,n):
    e = euclid(m,n)
    d = e[0]
    if d != 1:
        print '法が互いに素ではありません。'
        exit()
    else:
        return ##### ここを埋めよ #####

m = 0
n = 0
print
k = input('法のビット数を入力してください ')
while(gcd(m,n) != 1):
    m = randbit(k)  # kビットの乱数
    n = randbit(k)  # kビットの乱数

a = rand(m)
b = rand(n)
x = chinese(a,b,m,n)
print
print '連立合同式'
print '  x = %d ( mod %d )' % (a,m)
```

```
print '  x = %d ( mod %d )' % (b,n)
print 'の解は'
print '  x = %d ( mod %d )' % (x,m*n)

a0 = mod(x,m)
b0 = mod(x,n)
print
print '検算：'
print '  x mod %d = %d' % (m,a0)
print '  x mod %d = %d' % (n,b0)
if a0 != a or b0 != b:
    print 'エラーです'
```

実行例

```
法のビット数を入力してください 50

連立合同式
  x = 147451837639729 ( mod 705952127566285 )
  x = 544613511631085 ( mod 1116941726320193 )
の解は
  x = 561200806384284030757564729539 ( mod 788507388063299476889741493005 )

検算：
  x mod 705952127566285 = 147451837639729
  x mod 1116941726320193 = 544613511631085
```

C 言語による実装例

```
/* rep05.c
gcc rep05.c -o rep05 -lm
*/

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

int mod(int a, int m)
{
        int b=a%m;
        return b<0 ?  b+m: b;
}

int gcd(int a, int b)
{
  return b==0 ? abs(a): gcd(b,a%b);
}

int euclid(int a, int b, int *x, int *y)
{
        int q,r,d0,x0,y0;
        if(b==0){
                if(a>=0){
                        *x=1;
                        *y=0;
                        return(a);
```

```
                }
                else{
                        *x=-1;
                        *y=0;
                        return(-a);
                }
        }
        else{
                q=a/b;
                r=a-q*b;
                d0=euclid(b,r,&x0,&y0);
                *x=y0;
                *y=x0-q*y0;
                return(d0);
        }
}

int chinese(int a, int b, int m, int n)
{
        int d,u,v,x;
        d=euclid(m,n,&u,&v);
        if(d!=1){
                printf("法が互いに素ではありません。\n");
                exit(1);
        }
        else
                return mod(a*n*v+b*m*u,m*n);
}

main()
{
        int a,b,m=0,n=0,x;

        srand(time(NULL));        // 乱数の初期化
        while(gcd(m,n)!=1){
                m=rand() % 500;
                n=rand() % 500;
        }
        a=rand() % m;
        b=rand() % n;
        x=chinese(a,b,m,n);
        printf("\n");
        printf("連立合同式\n");
        printf("  x = %5d ( mod %5d )\n",a,m);
        printf("  x = %5d ( mod %5d )\n",b,n);
        printf("の解は\n");
        printf("  x = %5d ( mod %5d )\n\n",x,m*n);
        printf("検算：\n");
        printf("  %5d mod %3d = %3d\n",x,m,mod(x,m));
        printf("  %5d mod %3d = %3d\n",x,n,mod(x,n));
}
```