

アルゴリズム論特講 (塩田)

2006年4月20日の課題

課題 拡張版ユークリッドのアルゴリズムを実行する関数を Python で作成し、以下のデータに対して実行せよ。(検算も忘れないこと。)

- (1) $a = 17, b = 31$
- (2) $a = 1234, b = 56789$
- (3) $a = 5 * 100, b = 7 * 70$

規格

- 引数は2つの整数 a, b .
- 関数の戻り値は3つの要素を持つ配列 $[d, x, y]$ で、 $d = \gcd(a, b)$ は a と b の最大公約数、 x, y は $d = ax + by$ を満たす整数。

提出期限：未定 (512号室ポストまで)

雛形

```
#!/bin/env python
#
# hina060420.py

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

# ユークリッドのアルゴリズム
# d = gcd(a,b) = ax+by となる d,x,y を求め、
# 3つの要素を持つ配列 [d,x,y] を戻り値にする
# 戻り値の使い方は main routine の5行目以降を参照

def euclid(a,b):
    if b == 0:
        if a >= 0:
            return [a,1,0]
        else:
            return [-a,-1,0]
    else:
        r0 = a
        r1 = b
        x0 = 1
        x1 = 0
        y0 = 0
        y1 = 1
        while r1 != 0:
            q = r0/r1
```

```

##### ここを埋めよ #####
##### ここを埋めよ #####
##### ここを埋めよ #####
r0 = r1
r1 = r2
x0 = x1
x1 = x2
y0 = y1
y1 = y2
if r0 < 0:
    r0 = -r0
    x0 = -x0
    y0 = -y0
return [r0,x0,y0]

# ここから main routine

print
print 'Euclid のアルゴリズムのテストプログラムです。'
a = input('a = ')
b = input('b = ')
ls = euclid(a,b)
d = ls[0]
x = ls[1]
y = ls[2]
print
print 'd = ',d
print 'x = ',x
print 'y = ',y
print '検算 :'
print '(' ,a,') * (' ,x,') + (' ,b,') * (' ,y,') = ',a*x + b*y

# 実行例
#
# Euclid のアルゴリズムのテストプログラムです。
# a = 5**30
# b = 3**50
#
# d = 1
# x = -89115256441822303775825
# y = 115608417198323432874
# 検算 :
# ( 931322574615478515625 ) * ( -89115256441822303775825 )
# + ( 717897987691852588770249 ) * ( 115608417198323432874 ) = 1

```

C 言語による実装例

```

/* rep02.c */

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

```

```

/* 拡張ユークリッドのアルゴリズム、数列を作る version */
int euclid1(int a, int b, int *x, int *y)
{
    int r[64],xx[64],yy[64],q,n=1;
    r[0] =a;
    r[1] =b;
    xx[0]=1;
    xx[1]=0;
    yy[0]=0;
    yy[1]=1;
    while(r[n]!=0){
        n++;
        q=r[n-2]/r[n-1];
        r[n] =r[n-2] -q*r[n-1];
        xx[n]=xx[n-2]-q*xx[n-1];
        yy[n]=yy[n-2]-q*yy[n-1];
    }
    if(r[n-1]>=0){
        *x=xx[n-1];
        *y=yy[n-1];
        return(r[n-1]);
    }
    else{
        *x=-xx[n-1];
        *y=-yy[n-1];
        return(-r[n-1]);
    }
}

```

```

/* 拡張ユークリッドのアルゴリズム、メモリを節約する version */
int euclid2(int a, int b, int *x, int *y)
{
    int r0=a,r1=b,r2,x0=1,x1=0,x2,y0=0,y1=1,y2,q;
    while(r1!=0){
        q=r0/r1;
        r2=r0-q*r1;
        x2=x0-q*x1;
        y2=y0-q*y1;
        r0=r1;
        r1=r2;
        x0=x1;
        x1=x2;
        y0=y1;
        y1=y2;
    }
    if(r0<0){
        r0=-r0;
        x0=-x0;
        y0=-y0;
    }
    *x=x0;
    *y=y0;
    return(r0);
}

```

```

}

/* 拡張ユークリッドのアルゴリズム、再帰呼出しを用いる version */
int euclid3(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=euclid3(b,r,&x0,&y0);
        *x=y0;
        *y=x0-q*y0;
        return(d0);
    }
}

main()
{
    int a,b,d,x,y;
    printf("input a and b:\n");
    printf("a = ");
    scanf("%d",&a);
    printf("b = ");
    scanf("%d",&b);

    printf("\n");
    printf("euclid1 :\n");
    d=euclid1(a,b,&x,&y);
    printf("gcd(%d,%d) = %d = (%d)*(%d)+(%d)*(%d)\n",a,b,d,a,x,b,y);
    printf("check : ");
    printf("(%d)*(%d)+(%d)*(%d) = %d\n",a,x,b,y,a*x+b*y);

    printf("\n");
    printf("euclid2 :\n");
    d=euclid2(a,b,&x,&y);
    printf("gcd(%d,%d) = %d = (%d)*(%d)+(%d)*(%d)\n",a,b,d,a,x,b,y);
    printf("check : ");
    printf("(%d)*(%d)+(%d)*(%d) = %d\n",a,x,b,y,a*x+b*y);

    printf("\n");
    printf("euclid3 :\n");

```

```

    d=euclid3(a,b,&x,&y);
    printf("gcd(%d,%d) = %d = (%d)*(%d)+(%d)*(%d)\n",a,b,d,a,x,b,y);
    printf("check : ");
    printf("(%d)*(%d)+(%d)*(%d) = %d\n",a,x,b,y,a*x+b*y);
}

/* 実行例

input a and b:
a = 12345
b = 6789

euclid1 :
gcd(12345,6789) = 3 = (12345)*(-903)+(6789)*(1642)
check : (12345)*(-903)+(6789)*(1642) = 3

euclid2 :
gcd(12345,6789) = 3 = (12345)*(-903)+(6789)*(1642)
check : (12345)*(-903)+(6789)*(1642) = 3

euclid3 :
gcd(12345,6789) = 3 = (12345)*(-903)+(6789)*(1642)
check : (12345)*(-903)+(6789)*(1642) = 3

*/

```

C 言語版の関数 euclid1 のトレース

$a = 61, b = 39$ のとき

n	q	r_n	x_n	y_n
0		61	1	0
1		39	0	1
2	$1 = \lfloor \frac{61}{39} \rfloor$	$22 = 61 - 1 \times 39$	$1 = 1 - 1 \times 0$	$-1 = 0 - 1 \times 1$
3	$1 = \lfloor \frac{39}{22} \rfloor$	$17 = 39 - 1 \times 22$	$-1 = 0 - 1 \times 1$	$2 = 1 - 1 \times (-1)$
4	$1 = \lfloor \frac{22}{17} \rfloor$	$5 = 22 - 1 \times 17$	$2 = 1 - 1 \times (-1)$	$-3 = -1 - 1 \times 2$
5	$3 = \lfloor \frac{17}{5} \rfloor$	$2 = 17 - 3 \times 5$	$-7 = -1 - 3 \times 2$	$11 = 2 - 3 \times (-3)$
6	$2 = \lfloor \frac{5}{2} \rfloor$	$1 = 5 - 2 \times 2$	$16 = 2 - 2 \times (-7)$	$-25 = -3 - 2 \times 11$
7	$2 = \lfloor \frac{2}{1} \rfloor$	$0 = 2 - 2 \times 1$		

$$\gcd(61, 39) = 1 = 61 \times 16 + 39 \times (-25)$$

ペットボトル問題 500ml 入りの大きなペットボトルと 350ml 入りの小さいペットボトルを 1 本ずつ使って 100ml を測れ。

