二元一次不定方程式　ディオファントス方程式

　教科書では, **互除法**を使うやり方。これが割と面倒くさい。
私は**合同式**を使うやり方で, あるいは**連分数**を使うやり方で不足はなかったので,
生徒が「YouTube でいいやり方があったが, 思い出せないので教えてくれ」と質問にきても,
「やり方を覚えられないような方法なんて, 暗記して何の意味があるの？」で済ましていた。
　前置きが長くなりました。飯高茂さんの本の方法がいいと思われるので紹介しよう。
これからは, 私もこれでいきそう。
私が大学生の頃, 教室のストーブの調子が悪くて中を覗いているときに, 後ろから「ボン！」と人を驚かして面白がっていた人がこの先生でした。
チャメ系な人です。文章にも人柄が出てます。「数学のかんどころ」シリーズは面白いです。
「環論, これはおもしろい（素因数分解と循環小数への応用）」から。

$ax+by=1$ **の解き方**

	1	0	a
$q_1\cdots$①	0	1	b
q_2	$1\cdots$②	$-q_1\cdots$③	$a-q_1\cdot b$

①の q_1 は, a を b で割ったときの商
②③ は, 上の行から下の行を q_1 倍して引いたもの
これを繰り返し,
右下が 1 になったときの,②が x で③が y

右の欄が互除法で, これで解が出てしまうとは！
　証明もベクトルを使って爽快でした。
1・2 行目から作ったベクトル $(1,0,a),(0,1,b)$ は $(a,b,-1)$ と内積が 0。
3 行目からは，実数倍の加減だから，どれも内積 0。
最後の行との内積 $ax+by-1$ も 0 ，つまり，$ax+by=1$
　「繰り返し」という言葉があればプログラミング。
本文中の章末問題を途中を書くプログラムでやってみる。
(5)$a=529,b=728$ に対して $1=ax+by$ を満たす整数 x,y を 1 組求めよ。

```
import numpy
def dhio(a,b):
    l=numpy.array([1,0,a])
    m=numpy.array([0,1,b])
    print(" ",l)
    print(l[2]//m[2],m)
    n=l-(l[2]//m[2])*m
    while n[2]¿0:
        l=m
        m=n
        print(l[2]//m[2],m)
        n=l-(l[2]//m[2])*m
    print("x=",m[0],",y=",m[1])
```

```
dhio(529,728)
[ 1 0 529]
0 [ 0 1 728]
1 [ 1 0 529]
2 [ -1 1 199]
1 [ 3 -2 131]
1 [-4 3 68]
1 [ 7 -5 63]
12 [-11 8 5]
1 [ 139 -101 3]
1 [-150 109 2]
2 [ 289 -210 1]
x= 289 ,y= -210
```

a,b は正の互いに素な整数（自然数）です。
どちらかがマイナスのときは, それに対応する解の方をマイナスにすればいい。
互いに素でないときは, 右下が最大公約数で,
$ax+by=gcd(a,b)$ の解です。なんて便利な。

もっとも，プログラムとしてはもっと楽にできる。
以下 a と b は互いに素として，
Python には Maxima の `inv_mod` に当たる関数がある。`pow(a,-1,b)` : 法 b で a^{-1}
例えば，$ax+by=1$ の解は $ax\equiv 1(\mod b)$ だから，

```
def diof(a,b):
        x=pow(a,-1,b)
        y=(1-a*x)//b
        return(x,y)
```

で，いいわけだ。

中国剰余定理もこれを使うと楽。

m で割ると a 余り， n で割ると b 余る数は，
$mx+ny=1$ の解を $(x,y)=(p,q)$ とすると，
$anq+bmp$ と 法 mn で合同。

例　5 で割ると 3 余り， 9 で割ると 2 余る数を求めよ。
解 1)　$\{3,8,13,18,23,28,33,38,\cdots\}\cap\{2,11,20,29,38,\cdot\}$
5 と 9 の最小公倍数 45 で割ると 38 余る数

解 2）m,n を整数として，$5m+3=9n+2$ つまり $-5m+9n=1$
これを解いて k を整数として $m=-2+9k, n=-1+5k$
$5(-2+9k)+3=-7+45k=38+45(k-1)$ で， 45 で割ると 38 余る数

解 3) $5m+9n=1$ の解を p,q とすると，
$9q\cdot 3+5p\cdot 2(\mod 45)$ が解。というのが中国剰余定理。
何故なら，$5p\equiv 1(\mod 9), 9q\equiv 1(\mod 5)$ だから。

```
def china(m,a,n,b):
        return((a*n*pow(n,-1,m)+b*m*pow(m,-1,n)) % (m*n))
```

帰ってくるのが 38。