アルゴリズム論特講 （塩田）

2006年6月8日の課題

課題

- 関数定義部 crypto060608.py，講義中 3 で述べた方法による原始根計算の雛形プログラム hina060608.py，および原始根の高速計算プログラム prrt.py をダウンロードせよ。
- hina060608.py の位数計算関数 elementorder を完成せよ。
- hina060608.py と prrt.py を、素数の大きさを取り替えて実行し計算時間の違いを実感せよ。

提出期限：未定 （ 512号室ポストまで ）

雛形

```
#!/bin/env python
#
# hina060608.py

from sys import *
from time import *
from math import *
from random import *
from crypto060608 import *    # crypto060608.py はホームページから download せよ

# mod m での a の乗法位数を返す
def elementorder(a, m):
    ##### ここを埋めよ #####

# 素数 p を法とする原始根を返す
def primitiveroot(p):
    g = 1
    while elementorder(g,p) != p-1:
        g = g+1
    return g

##### ここからメインルーチン #####

while 1:
    print
    print '-----'
    k = input('素数 p のビット数を指定してください （ 1 以下で終了 ）: ')
    if k < 2:
        exit(0)
```

```
    print ’素数生成中 ...’
    p = getprimebit(k)
    print ’素数 p          =’,p,’ (’,bitlen(p),’bits )’

    t0 = time()                 # 開始時刻
    g = primitiveroot(p)
    print ’法 p の原始根 g =’,g
    print ’検索時間        =’,time()-t0
```

実行例

```
-----
素数 p のビット数を指定してください ( 1 以下で終了 ) : 10
素数生成中 ...
素数 p          = 919  ( 10 bits )
法 p の原始根 g = 7
検索時間        = 0.00800013542175

-----
素数 p のビット数を指定してください ( 1 以下で終了 ) : 15
素数生成中 ...
素数 p          = 27427  ( 15 bits )
法 p の原始根 g = 5
検索時間        = 0.171000003815

-----
素数 p のビット数を指定してください ( 1 以下で終了 ) : 20
素数生成中 ...
素数 p          = 579947  ( 20 bits )
法 p の原始根 g = 2
検索時間        = 2.10800004005
```

原始根の高速計算プログラム

```
#!/bin/env python
#
# prrt.py
# 2006.6.8
# 大きな素数 p を法とする原始根 g を求める

from sys import *
from math import *
from random import *
from time import *
from crypto060608 import *      # crypto060608.py はホームページから download せよ

##### p-1 が素因数分解しやすい素数 p を作為的に生成 #####

while 1:
    print
    print ’-----’
    k = input(’素数 p のビット数を指定してください ( 10 以下で終了 ) : ’)
    if k < 11:
```

```
    exit(0)
print '素数生成中 ...'
q1 = getprimebit(round(0.8*k))      # 素因子のひとつは大きく
p = 1
while solovaystrassen(p) == 0:
    a = q1
    while bitlen(a) < k:
        a *= (rand(256)+1)
    p = a + 1               # p = q1*(小さな数)+1
print '素数 p          =',p,' (',bitlen(p),'bits )'

##### p-1 の素因子のリストを作成 #####

q = []
x = p-1
r = 2
while r <= 256:
    if x%r == 0:            # x が r で割り切れれば
        q.append(r)         # リストに r を追加
        while x%r == 0:
            x /= r
    r += 1
if x > 1:
    q.append(x)             # 商が残っていればそれも素因子
print 'p-1 の素因子    :',q

##### 法 p の原始根 g を検索 #####

t0 = time()                 # 開始時刻を計測
g = 1                       # 原始根の候補
ok = 0
while ok == 0:
    g += 1
    ok = 1
    for r in q:
        if powermod(g,(p-1)/r,p) == 1:
            ok = 0
            break
print '法 p の原始根 g =',g
print '検索時間        =',time()-t0
```

prrt.py の実行例

```
-----
素数 p のビット数を指定してください ( 10 以下で終了 ) : 20
素数生成中 ...
素数 p          = 1380811  ( 21 bits )
p-1 の素因子    : [2, 3, 5, 46027L]
法 p の原始根 g = 2
検索時間        = 0.00100016593933

-----
```

```
素数 p のビット数を指定してください ( 10 以下で終了 ) : 100
素数生成中 ...
素数 p          = 864336493025724464683244571421  ( 100 bits )
p-1 の素因子    : [2, 3, 5, 13, 17, 23, 944691994038652222750393L]
法 p の原始根 g = 6
検索時間        = 0.0130000114441

-----
素数 p のビット数を指定してください ( 10 以下で終了 ) : 300
素数生成中 ...
素数 p          = 915760805944528895467513149782545099999230153371776584954529504140353336883549150485047296 01  ( 306 bits )
p-1 の素因子    : [2, 3, 5, 11, 13, 43, 47, 53, 109, 211, 1424581243113377791654435546645961036540367992641894648787307659242941 67L]
法 p の原始根 g = 7
検索時間        = 0.147000074387

-----
素数 p のビット数を指定してください ( 10 以下で終了 ) : 500
素数生成中 ...
素数 p          = 359942571104999947171630133452081543758565505742108232514480426934797667478225340487040143820341513919789627742973728451755655698848590393769543302144 1  ( 501 bits )
p-1 の素因子    : [2, 3, 5, 7, 11, 13, 17, 19, 23, 37, 47, 59, 61, 163, 197, 2446787520320813380706925444517197532307399497346178977757672645839745984642559404709855222006695785208548983775398910819L]
法 p の原始根 g = 31
検索時間        = 1.46499991417

-----
素数 p のビット数を指定してください ( 10 以下で終了 ) : 1000
素数生成中 ...
素数 p          = 282926342124473571889401585078579578835136950287802025598336555133162968506700219178599644785515541667589275625205972069626005874185094450180272527401019564409892523171831070429603734684668793727016517015899685293620146026210378962813152502193559920622778934904755271540197443409927865827328000000000001  ( 1002 bits )
p-1 の素因子    : [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 47, 73, 109, 127, 173, 193, 227, 3945334253261905423174033627345392764926779301259965173218107026715604136618901695622875659772243568543234485058606658645531052373961225948151713641529672144042721105283047489033637825132585255151058952776157211677560042197671003259756677757L]
法 p の原始根 g = 37
検索時間        = 10.7180001736
```