アルゴリズム論特論　(塩田)

2009 年 7 月 16 日の課題

課題　PH.py（Pohlig-Hellman 法のサンプルプログラム）を改造して

```
p = 11343517943838792118103430281769874200996833345282626821243704685913913357694611156711845883353317650917294901842300066082511325536378997309440000000001

g = 37

y = 91871433944915327476833473744860148748664295871376571795172326957201590352166555266146984403840158605353823941372219759551697688561256847487059520948 59
```

の場合の、法 p，底 g に対する y の離散対数 $x = \log_g(y)$ を求めよ。

提出期限：7 月 30 日（木）　（ 512 号室ポストまで ）

サンプルプログラム

http://lupus.is.kochi-u.ac.jp/~shiota/mc09/ 配下に以下のプログラム・サンプルデータがある。

- 関数定義部　（サンプルプログラムで import ）
  crypto.py
- Pohlig-Hellman 法（$p-1$ の素因数が全て小さいときに有効）
  PH.py