アルゴリズム論特論　(塩田)

2016 年 5 月 30 日

問題 フェルマ・テストあるいはミラー・ラビン・テストを用いて

$$10^{50} < p < 10^{50} + 1000$$

の範囲の素数 p を全て求めよ。

反復 2 乗法

入力：x, e, n
出力：$x^e \ \% \ n$

```
y = 1
while e > 0:
    if e % 2 == 1:
        y = ( y * x ) % n
    x = ( x * x ) % n
    e /= 2
return y
```

フェルマ・テスト

入力：p
出力：p が素数か否か

充分沢山の乱数 b ($1 < b < p$) に対して

$$\gcd(b, p) = 1 \quad \text{かつ} \quad b^{p-1} \% p = 1$$

が成り立てば return TRUE
else return FALSE

ミラー・ラビン・テスト

入力：p
出力：p が素数か否か

充分沢山の乱数 b ($1 < b < p$) に対して

$$b^{p-1} \% p, \quad b^{\frac{p-1}{2}} \% p, \quad b^{\frac{p-1}{4}} \% p, \quad b^{\frac{p-1}{8}} \% p, \ \cdots$$

の中で最初に $\not\equiv 1$ となるものが $\equiv -1$ ならば return TRUE
else return FALSE