提出日: 2015/06/08

数理システム工学特論レポート 第7回

氏名: 市野 晴之
学籍番号: 281567038

1. 第1回レポートのp'(16bitの乱数)とp(p'より大きい素数)について、$(p')^{-1} \bmod p$ を求めよ。

第1回レポートの問2のプログラムに拡張ユークリッドの互除法とそれを用いた乗法逆元を求める機能を実装した。以下にプログラムの実行結果を示す。またプログラムは別紙1を参照。

```
MacBook-Pro-2:report07-mse Haru$ python3 ex1.py
p' =  42789
p =  42793
p'^-1 mod p =  10698
```

2. 拡張ユークリッドの互除法について、数学的帰納法を用いて、$a_i = a_r x_i + a_1 y_i$ を示せ。

問より、

$$a_i = a_r x_i + a_1 y_i \ldots(1)$$

i=0,1を(1)式に代入

$$a_0 = a_0 x_0 + a_1 y_i = a_0 \times 1 + a_1 \times 0 = a_0 \ldots(2)$$
$$a_1 = a_1 x_0 + a_1 y_i = a_0 \times 0 + a_1 \times 1 = a_1 \ldots(3)$$

次に、i=k、k-1のときに(1)式が成り立つと仮定すると

$$a_{k-1} = a_0 x_{k-1} + a_1 y_{k-1} \ldots(4)$$
$$a_k = a_1 x_k + a_1 y_k \ldots(5)$$

i=k+1の場合を、(4),(5)式を用いて拡張ユークリッドの互除法を適用する

$$\begin{aligned} a_{k=1} &= a_0 x_{k+1} + a_1 y_{k+1} \\ &= a_0(x_{k-1} - q_{k+1} x_i) + a_1(y_{k-1} - q_{k-1} y_k) \\ &= (a_0 x_{k-1} - a_1 y_{k-1}) - q_{k+1}(a_0 x_k - a_1 y_k) \\ &= a_{k-1} - q_{k+1} a_k \end{aligned}$$

従って、(1)式は成り立つ。