令 和 6 年 度

生 活 環 境 学 部

第 3 年 次 編 入 学 者 選 抜 学 力 試 験 問 題

小　　論　　文

〔文化情報学科 生活情報通信科学コース〕

令和５年６月１０日（土）

１３：００～１４：３０

注　　　意

１．解答は，別添の解答用紙（２枚同封）を使用し，問題ごとに別の解答用紙を用いること。

２．総ページ数 ―――― ３ページ
　問題ページ ―――― 第２～３ページ
　（第１ページは，下書き用紙）

３．試験終了後，この問題冊子は持ち帰ること。

問題1

下記に示す、プログラミング言語Cで書かれた2つの関数mod_exp1, mod_exp2はどちらも、引数に3つの非負整数b, e, m (ただし$m > 0$とする) を与えて、$b^e \bmod m$を返すものである (ここで$x \bmod m$とは、xをmで割った余りを表す)。

また、mod_exp2_auxは、mod_exp2の中で用いる補助関数で、引数b, e, a, mに対して$(b^e \times a) \bmod m$を返すものである。この関数は、$b' = b^2$とし、e'を$e/2$の整数部としたときに、関係

$$b^e \times a = \begin{cases} (b')^{e'} \times a & e \bmod 2 = 0 \text{ の場合} \\ (b')^{e'} \times ab & e \bmod 2 = 1 \text{ の場合} \end{cases}$$

が成り立つことを繰り返し使って、指数eが0の場合に帰着させることで計算を行っている。

mod_exp1とmod_exp2での、必要となる掛け算の回数の違いについて、特にeが大きい場合を念頭に置いて論ぜよ。

なお、任意の非負整数x, yと任意の正の整数mについて、$xy \bmod m = ((x \bmod m) \times (y \bmod m)) \bmod m$であることは、プログラム中では既知として暗黙に使っており、解答でもこのことは既知としてよい。また、Cで「%」は割り算の余りを計算する演算子である。

```
unsigned int
mod_exp1(unsigned int b, unsigned int e, unsigned int m)
{
        unsigned int i, a = 1;
        b %= m;
        for(i = 0; i < e; i++){
                a *= b;
                a %= m;
        }
        return a;
}

unsigned int
mod_exp2_aux(unsigned int b, unsigned int e, unsigned int a,
             unsigned int m)
{
        b %= m;
        while(e > 0){
                if(e % 2){
                        a *= b;
                        a %= m;
                }
                b *= b;
                b %= m;
                e /= 2;
        }
        return a;
}

unsigned int
mod_exp2(unsigned int b, unsigned int e, unsigned int m)
{
        return mod_exp2_aux(b, e, 1, m);
}
```

問題 2

n 個の実数 $a_1, a_2, \cdots, a_n$ があるとする。1 以上 n 以下の整数をランダムに 1 つ選択したいが、a_i が大きいほど i の選択される確率を大きくしたい、という場合によく用いられるのは

$$i \text{ を選ぶ確率を } \frac{e^{a_i/\tau}}{e^{a_1/\tau} + e^{a_2/\tau} + \cdots + e^{a_n/\tau}} \text{ にする}$$

という手法である (ここで τ はあらかじめ決めておく正の定数である)。

しかし、実際にこの方法を計算機でプログラムとして実装する場合は、$a_1, a_2, \cdots, a_n$ のうち最大のものを a とするとき

$$i \text{ を選ぶ確率を } \frac{e^{(a_i-a)/\tau}}{e^{(a_1-a)/\tau} + e^{(a_2-a)/\tau} + \cdots + e^{(a_n-a)/\tau}} \text{ にする}$$

という実装を行う方がよい。

(問 1)　その理由を説明せよ。

(問 2)　「i を選ぶ確率を $a_i/(a_1 + a_2 + \cdots + a_n)$ にする」という方法が、一般には使えない理由を述べよ。