

第 4 次编程练习报告

姓名：曹瑜 学号：2212794 班级：密码科学与技术

一、编程练习 1——求解最小原根并构造指数表

➤ 源码部分：

```
#include <iostream>
#include<vector>
#include<iomanip>
using namespace std;

// 求解欧拉函数
int oula(int n) {
    int result = n;
    for (int i = 2; i * i <= n; ++i) {
        if (n % i == 0) {
            while (n % i == 0) {
                n /= i;
            }
            result -= result / i;
        }
    }
    if (n > 1) {
        result -= result / n;
    }
    return result;
}

//判断是否为原根
bool isPrimitiveRoot(int a, int n) {
    int p = oula(n);
    int result = 1;
    for (int j = 0; j < p-1; ++j) {
        result = (result * a) % n;
        if (result == 1) {
            return false;
        }
    }
    return true;
}
```

```

// 从2开始找最小原根
int findPrimitiveRoot(int n) {
    for (int a = 2; a < n; ++a) {
        if (isPrimitiveRoot(a, n)) {
            return a;
        }
    }
    return -1;
}

// 构造指数表
vector<vector<int>> constructExponentTable(int n, int primitiveRoot) {
    vector<vector<int>> exponentTable(n / 10 + 1, vector<int>(10, -1));
    for (int p = 0; p < n; p++) {
        int result = 1;
        for (int i = 0; i < 10; i++) {
            result = (result * primitiveRoot) % n; // 使用模运算防止结果溢出
        }
        int row = result / 10;
        int col = result % 10;
        if (exponentTable[row][col] == -1) {
            exponentTable[row][col] = p;
        }
    }
    return exponentTable;
}

// 输出指数表
void printExponentTable(int n, const vector<vector<int>>& exponentTable) {
    cout << setw(8) << " ";
    for (int i = 0; i < 10; i++) {
        cout << setw(8) << i;
    }
    cout << endl;
    for (int i = 0; i <= n / 10; i++) {
        cout << setw(8) << i;
        for (int j = 0; j < 10; j++) {
            if (exponentTable[i][j] == -1) {
                cout << setw(8) << "-";
            }
            else {
                cout << setw(8) << exponentTable[i][j];
            }
        }
    }
}

```

```

        cout << endl;
    }
}

int main()
{
    int n;
    cout << "Please input n(n>0): ";
    cin>>n;

    int g= findPrimitiveRoot(n);
    cout << "The main primitive root of 103: g="<<g<<endl;
    cout << "The ind_table of 103 based on g=" << g << " is:" << endl;
    vector<vector<int>> exponentTable = constructExponentTable(n, g);
    printExponentTable(n, exponentTable);
}

```

➤ **说明部分：**//主要说明实现的一些基本原理等

求解原根部分：从 $g=2$ 开始依次判断是否为原根，原根判断函数中，先求解 n 的欧拉函数 p ，然后验证 g 的 $0-p-1$ 次幂模 n 是否为 1，根据最小原根定义，值为 1 则一定不是最小原根，从而返回 false

构造指数表部分：先接收 n 和最小原根 g ，然后创建二维向量，行数为 $(n/10+1)$ ，列数为 10，然后依次求解 g 的 $0-p-1$ 幂次模 n 运算的结果，存储在对应位置，最后返回指数表；

据题意，打印指数表时表中值为-1 的部分打印为 “-”；

➤ 运行示例：//截图

```
Microsoft Visual Studio 调试控制台
Please input n(n>0): 103
The main primitive root of 103: g=5
The ind_table of 103 based on g=5 is:
    0      1      2      3      4      5      6      7      8      9
0      -      0     44     39     88     1     83     4     30     78
1     45     61     25     72     48    40     74     70     20     80
2     89     43      3     24     69     2     14     15     92     86
3     84     57     16    100     12     5     64     93     22      9
4     31     50     87     77     47    79     68     85     11      8
5     46     7      58     97     59    62     34     17     28     98
6     26     36    101     82     60    73     42     13     56     63
7     49     67      6     33     35    41     66     65     53     18
8     75     54     94     38     29    71     19     23     91     99
9     21     76     10     96     27    81     55     32     52     37
10    90     95     51      -      -      -      -      -      -
F:\试运行1\指数表\x64\Debug\指数表.exe (进程 14940) 已退出, 代码为 0。
按任意键关闭此窗口. . .
```

```
Microsoft Visual Studio 调试控制台
Please input n(n>0): 169
The main primitive root of 103: g=2
The ind_table of 103 based on g=2 is:
    0      1      2      3      4      5      6      7      8      9
0      -      0      1     124     2      9    125    107     3     92
1     10    103    126      -    108    133     4    146     93     65
2     11     75    104    130    127     18      -     60    109     40
3    134     21      5     71    147    116     94    151     66      -
4     12     85     76    122    105    101    131     63    128     58
5     19    114      -    120     61    112    110     33     41     35
6    135    140     22     43      6      -     72     37    148     98
7    117    137     95     51    152    142     67     54      -     24
8     13     28     86     45     77    155    123      8    106     91
9    102      -    132    145     64     74    129     17     59     39
10     20     70    115    150      -     84    121    100     62     57
11    113    119    111     32     34    139     42      -     36     97
12    136    50    141     53     23     27     44    154      7     90
13      -    144     73     16     38     69    149     83     99     56
14    118     31    138      -     96     49     52     26    153     89
15    143     15     68     82     55     30      -     48     25     88
16     14     81     29     47     87     80     46     79     78      -
F:\试运行1\指数表\x64\Debug\指数表.exe (进程 19300) 已退出, 代码为 0。
按任意键关闭此窗口. . .
```

➤ 其他：//用于回答可能预留的问题