**实验一 密码学数学基础**

**一、实验目的**

1. 掌握最大公因数的计算方法，理解其在密码学中的重要性。

2. 学习扩展欧几里得算法，能够计算乘法逆元。

3. 熟悉模幂运算的方法，了解其在加密和签名算法中的应用。

**二、实验原理**

**1. 最大公因数**

最大公因数（GCD）是两个整数的最大公因数，是数论中一个基本概念。在密码学中，计算GCD用于判断两个数是否互素，有以下三种常见方法：

1) 暴力穷举法

通过列举所有可能的公约数来找到最大公约数。具体操作是依次检查从1到较小数（假设则范围为）的所有整数是否为*x*和*y*的公约数，最终选择最大的公约数。此方法简单直观，但效率较低，适合小整数场景。

2) 更相减损法

基于以下性质：两个整数的最大公约数等于较大数减去较小数后的结果与较小数的最大公约数。递归关系如下：



重复相减直至两数相等，此时的值即为最大公约数。该方法虽然比暴力穷举法更高效，但当两数差值较小时，计算量依然较大。

3) 辗转相除法

又称欧几里得算法，是效率最高的方法，基于以下定理：



即，两个数的最大公约数等于较小数*y*和两数取模结果*x* *mod* *y*的最大公约数。通过不断取模运算，最终当余数为零时，非零的数即为最大公约数。

**2. 扩展的欧几里得算法**

扩展欧几里得算法不仅可以求出两个数的GCD，还可以得到其线性组合形式 ，其中x和y是整数，a和b是输入整数。具体过程如下：

对于或，显然有或。在此情况下，*x*和*y*的值可以直接给出。

对于，算法通过以下步骤来逐步减少问题的规模：

。

其中，*q*是商，*r*是余数。根据欧几里得定理，然后递归地求解，并在递归过程中保存每一层的系数*x*和*y*，最终构造出线性组合的解。

**3. 模幂运算**

模幂运算即计算，是密码学中诸多算法的基础操作。直接计算然后对*n*取模会导致数值过大，计算复杂度高。为了提高效率，通常采用**快速幂算法**，该算法利用二进制分解的性质将指数幂的计算转化为一系列的平方和乘法，从而大大减少计算量。

直接计算的时间复杂度是*O(m)*，而使用快速幂算法，通过二进制分解后，时间复杂度降低为*O(log m)*。这显著提高了大指数计算的效率，尤其在密码学中进行大数计算时尤为重要。

**三、实验内容**

1. 求最大公因数

给定两个整数*a*和*b*，计算其最大公因数。

2. 扩展的欧几里得算法

输入两个整数*a*和*b*，利用扩展欧几里得算法计算其GCD，并输出对应的线性组合系数*x*和*y*。

3. 模幂运算

给定整数*a*，*m*，*n*，使用快速幂算法计算。

**四、实验报告要求**

实验报告正文部分格式及内容如下：

实验目的：给出本次实验所涉及并要求掌握的知识点。

实验内容：给出实验的具体内容。

实验代码：给出实验时所实现的核心代码，展示算法的实现过程。

实验结果：给出实验的实际运行结果，并分析实验结果，验证算法的正确性和效率。

实验总结与心得：总结实验过程，分析实验中出现的问题及解决方法，总结实验的心得体会，并提出实验的改进意见。