第二章 同余

计算证明（注意问题的要求是同余还是余数）

1. (1) 求 7^{2046} 写成十进制数时的个位数；
   (2) 求 2^{1000} 的十进制表示中的末尾两位数字。
2. 计算 555^{555} 被 7 除的余数。
3. 计算以下整数的欧拉函数：
   （1）64 （2） 187
4. 利用费马小定理求解以下题目：
   (1)求数 $a(0 \leqslant a < 73)$，使得 $a \equiv 9^{794}(mod\ 73)$；
   (2)解方程 $x^{86} \equiv 6(mod\ 29)$。
5. 求 $1^5 + 2^5 + 3^5 + ... + 99^5$ 被 4 除的余数。（*能写出两种方法额外给分）
6. 证明如果 a 是整数，且 $(a, 3) = 1$，那么 $a^7 \equiv a(mod\ 63)$。
7. 证明如果 p 是奇素数，则 $1^{p-1} + 2^{p-1} + 3^{p-1} + ... + (p-1)^{p-1} \equiv -1(mod\ p)$。
8. 证明如果 p 是奇素数，则$1^2 * 3^2 * ... * (p-4)^2 * (p-2)^2 \equiv -1^{\frac{p+1}{2}}(mod\ p)$。
9. 解以下问题：
   (1)求 $229^{-1}(mod\ 281)$；
   (2)求 $3169^{-1}(mod\ 3571)$；
   (3)解方程 $105x + 121y = (105, 121)$。
10. 证明如果 p 是素数，且 $0 < k < p$，则 $(p-k)!(k-1)! \equiv (-1)^k(mod\ p)$。
11. *在一个密码体系中，明文 x 被加密成密文 y。密钥生成的过程是选择两个大素数 p 和 q，计算 $n = p * q$ 和 $z = \varphi(n)$，选择一个与 z 互质的数，令其为 d，找到一个 e 使满足 $e * d \equiv 1(mod\ z)$，则公钥是 (e, n)，私钥是 (d, n)。加密过程是 $y = x^e(mod\ n)$。解密过程是 $x = y^d(mod\ n)$。现在为了简化计算，选择 $p = 11, q = 13, e = 7$，明文消息为 $m = 85$，说明使用该加密算法的加密和解密(计算密文并还原)。

编程练习（基于C/C++）

1. 编程实现平方-乘算法，效果如图所示。

```
Calculate a^n(mod m). . .
Please input:
  a=2021
  n=20212023
  m=2023
2021^20212023(mod 2023)=671
```

2. 编程实现扩展的欧几里得算法求逆元，效果如图所示。

```
a=12345
b=65432
gcd(a,b)=1
lcm(a,b)=807758040
a^(-1)=63561(mod 65432)
b^(-1)=353(mod 12345)
```