第2章 同余

计算证明

1.计算欧拉函数 $\varphi(n)$：（1）$n=24$ (2) $n=360$

2. 计算：（1）$7^{2023}(mod\,9)$ （2）$666^{666}(mod\,21)$

3. 求解：（1）$x^{86}\equiv 6(mod\,29)$ （2）$x^{21}\equiv 6(mod\,7)$

4. 求模11的一个完全剩余系 $\{r_1,r_2,\cdots,r_i,\cdots,r_{11}\}$ 满足 $\forall i,\ r_i\equiv 1(mod\,3)$.

5. 求 $\sum\limits_{i=1}^{2023} i^{2021}(mod\,4)$.

6.求105，121的最大公因子、最小公倍数以及相互模的逆元.（无过程不给分）

7. 在某个密码系统中采用参数为 (7,3) 的仿射变换进行加密，即对于明文x被加密成密文y，满足 $y=7x+3(mod\,26)$. 已知该系统只采用26个小写拉丁字母传递消息，加密时对字母串的每一个字母进行上述仿射变换加密，且有如下对应关系：$a\leftrightarrow 0, b\leftrightarrow 1,\cdots,z\leftrightarrow 25$ 。如对消息 "ac" 加密，$'a'(x=0)\overset{7\times 0+3\equiv 3(mod\,26)}{\Longrightarrow}\ 'd'(y=3)$，$'c'(x=2)\overset{7\times 2+3\equiv 17(mod\,26)}{\Longrightarrow}\ 'r'(y=17)$，密文为"dr". 现在截获到该密码系统传递的密文为"hcxufqvn"，请解密.

8. 求证对 $n\in\mathbb{Z}$，有 $42\mid(n^7-n)$.

9. 证明若p为素数，且$0<k<p$，则有$(p-k)!\cdot(k-1)!\equiv(-1)^k(mod\,p)$.

10. 若p为素数，n为整数，证明：$p\nmid n$当且仅当 $\varphi(pn)=(p-1)\varphi(n)$.

11. *（选做）证明正整数 n 和 $n+2$ 是一对孪生素数当且仅当 $4((n-1)!+1)+n\equiv 0(mod\,n(n+2)),\ n\neq 1$.

编程练习（基于C/C++）

1. 编程实现平方-乘算法，效果如图所示.

```
Microsoft Visual Studio 调试控制台
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.

```
Microsoft Visual Studio 调试控制台
a=12345
b=65432
gcd(a,b)=1
lcm(a,b)=807758040
a^(-1)=63561(mod 65432)
b^(-1)=353(mod 12345)
```