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；9

   (2) 求 2^{1000} 的十进制表示中的末尾两位数字。76
2. 计算 555^{555} 被 7 除的余数。1
3. 计算以下整数的欧拉函数：

   （1）64　32

   （2）187　160
4. 利用费马小定理求解以下题目：

   (1)求数 $a(0 \leqslant a < 73)$，使得 $a \equiv 9^{794}(mod\,73)$；8

   (2)解方程 $x^{86} \equiv 6(mod\,29)$。　$x \equiv 8或21(mod\,29)$
5. 求 $1^5 + 2^5 + 3^5 + \ldots + 99^5$ 被 4 除的余数。（*能写出两种方法额外给分）　0
6. 证明如果 a 是整数，且 $(a,3)=1$，那么 $a^7 \equiv a(mod\,63)$。

> $\varphi(9)=6,(a,3)=1$
> 则 $(a,9)=1$
> 所以 $a^6 \equiv 1(mod\,9)$
> 所以 $a^7 \equiv a(mod\,9)$，且 $a^7 \equiv a(mod\,7)$
> 所以 $7|a^7-a$，$9|a^7-a$
> 所以 $63|a^7-a$
> 那么 $a^7 \equiv a(mod\,63)$
> 证毕。

7. 证明如果 p 是奇素数，则 $1^{p-1}+2^{p-1}+3^{p-1}+\ldots+(p-1)^{p-1} \equiv -1(mod\,p)$。

> $\varphi(p)=p-1$
> $a^{\varphi(p)} \equiv 1(mod\,p)$
> $a^{p-1} \equiv 1(mod\,p)$
> $1^{p-1}+2^{p-1}+3^{p-1}+\ldots+(p-1)^{p-1} \equiv (p-1)(mod\,p) \equiv -1(mod\,p)$
> 证毕。

8. 证明如果 p 是奇素数，则$1^2 * 3^2 * \ldots * (p-4)^2 * (p-2)^2 \equiv -1^{\frac{p+1}{2}}(mod\,p)$。

> $1^2 \equiv (-1)*1*(p-1)(mod\,p)$
> $3^2 \equiv (-1)*3*(p-3)(mod\,p)$

> ....
> 所以 原式 $\equiv (-1)^{\frac{p-1}{2}} * (p-1)!(mod\, p) \equiv (-1)^{\frac{p+1}{2}}(mod\, p)$
> 证毕。

9. 解以下问题：
   (1)求 $229^{-1}(mod\, 281)$； 27
   (2)求 $3169^{-1}(mod\, 3571)$； 2887
   (3)解方程 $105x + 121y = (105, 121)$。 $x = -53, y = 46$
10. 证明如果 p 是素数，且 $0 < k < p$，则 $(p-k)!(k-1)! \equiv (-1)^k(mod\, p)$。

$(k-1)! \equiv (-p+k-1)(-p+k-2)\cdots(-p+1) \equiv (-1)^{k-1}[p-(k-1)][p-(k-2)]\cdots(p-1) \quad (mod\, p)$

$(p-k)! \cdot (k-1)! \equiv (-1)^{k-1}(p-k)![p-(k-1)][p-(k-2)]\cdots(p-1) \equiv (-1)^{k-1}(p-1)! \quad (mod\, p)$

由威尔逊定理得$(p-1)! \equiv -1\ (mod\, p)$，则$(p-k)! \cdot (k-1)! \equiv (-1)^k(mod\, p)$.

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)。

```
密钥计算:
n=p*q=11*13=143
z= (p-1) * (q-1) =10*12=120
e*d=1(mod z)
7 * d(mod 120)=1  -------d=103

加密运算示例:
公钥:(e,n)=(7,143)
密文:c=p^e (mod n)=123


解密运算示例:
密钥:(d,n)=(103,143)
明文: P=c^d (mod n)=85
```