第二讲　剩余系

例1. 解一：利用剩余系，存在 $a,2a,3a,\cdots,na$ 共 n 个数，若存在 $1\le i\le j\le n$ 使得 $ia\equiv ja\pmod n$，则 $n\mid(ja-ia)\therefore n\mid(j-i)a$，又 $\because(a,n)=1$，$\therefore i\mid(j-i)$．但 $1\le j-a\le n-1$，这与 $n\mid(j-i)$ 矛盾，故而模 n 两两互不同余，从而构成模 n 的完系，故存在 x 使得 $ax\equiv b\pmod n$．

解二：利用不定方程，由 $(a,n)=1$，故而存在整数 x,y 使得 $ax+ny=1$，$\therefore a(bx)+n(by)=b$，$\therefore a(bx)\equiv b\pmod n$

例2. 当 $n=19$ 时，若有非负整数 (x,y) 使得 $5x+6y=19$，两边模 5 得 $y\equiv 4\pmod 5$．

从而 $y\ge 4$，$x=\dfrac{19-6y}{5}\le\dfrac{19-6\times4}{5}=-1$，这与 x 为非负整数矛盾，故此时方程无非负整数解．

当 $n>19$ 时，$5x=n-6y$，因为 $6\times0,6\times1,6\times2,6\times3,6\times4$ 构成模 5 的完系，所以存在 $0\le y\le4$ 使得 $5\mid n-6y$，此时 $x=\dfrac{n-6y}{5}>\dfrac{19-6\times4}{5}=-1$，且 $x=\dfrac{n-6y}{5}\in\mathbb{Z}$，故 $x\in\mathbb{N}$，从而方程存在非负整数解．

综上所述，使得方程 $5x+6y=n$ 无非负整数解的 n 最大为 19．

例3. （1）解一：令 $a_i=i\ (i=1,2,\cdots,n)$，则 $a_i+i=2i(i=1,2,\cdots,n)$，若存在 $1\le i<j\le n$，使得 $2i\equiv2j\pmod n$，则 $n\mid2(i-j)$，$n\mid(i-j)$，这不可能，故而 $a_i+i=2i(i=1,2,\cdots,n)$ 互不同余，为完系．

解二：直接利用例 1 的结论，若存在模 n 的完全系，且 $(2,n)=1$，则 2 乘该完系得到的同样是完系．

（2）若存在，则 $a_1+a_2+\cdots+a_n\equiv(a_1+1)+(a_2+2)+\cdots+(a_n+n)\pmod n$，从而 $n\mid\dfrac{n(n+1)}{2}$，矛盾．

例4. 注意 1、2、…、m 是模 m 的完系，2、4、……、2m 也是模 m 的完系

故 $1^n+2^n+3^n+\cdots+m^n\equiv2^n+4^n+6^n+\cdots+(2m)^n\equiv2^n(1^n+2^n+3^n+\cdots+m^n)\pmod m$

于是 $(2^n-1)(1^n+2^n+3^n+\cdots+m^n)$ 是 m 的倍数，故 $1^n+2^n+3^n+\cdots+m^n$ 是 m 的倍数．

例5. 即需要证明（1）当 p 为合数时，不能满足 $(p-1)!\equiv -1(\mathrm{mod}\ p)$，（2）当 p 为质数时，$(p-1)!\equiv -1(\mathrm{mod}\ p)$.

（1）当 p 为合数时，存在 $1<m\le n<p$ 使得 $p=mn$．若 $m\neq n$ 则 $(p-1)!$ 中含因子 m,n，故 $(p-1)!\equiv 0(\mathrm{mod}\ p)$，若 $m=n$，则 $p=m^2$，当 $m\ge 3$ 时，$(p-1)!$ 中含有因子 m，$2m$，$(p-1)!\equiv 0(\mathrm{mod}\ p)$，当 $m=2$ 时，$p=4$，$3!\equiv 2(\mathrm{mod}\ 4)$，故而 $(p-1)!\equiv\begin{cases}0(p\neq 4)\\2(p=4)\end{cases}$.

（2）当 p 为质数时，$1,2,\cdots,p$ 组成模 p 的完系，对任意 $1\le a\le p-1$，存在唯一的 $b\in\{1,2,\cdots,p-1\}$，使得 $ab\equiv 1(\mathrm{mod}\ p)$，若 $a=b$，则 $a^2\equiv 1(\mathrm{mod}\ p)$，$a^2-1=(a+1)(a-1)$ 为 p 的倍数，即 $a=p-1$ 或者 $a=1$.

若 $a\neq b$，则 $a\in\{2,3\ldots p-2\}$，故 2,3```p-2 可以两两配对，每对相乘后模 p 余 1.

.

例6. 解一：利用剩余系，因 $(a,p)=1$，a，$2a$，$3a$，…，pa 组成 p 的完系.

$(p-1)!=1\cdot 2\cdots(p-1)\equiv a\cdot 2a\cdots(p-1)a=(p-1)!\cdot a^{p-1}(\mathrm{mod}\ p)$，又因 $((p-1)!,p)=1$，从而 $a^{p-1}\equiv 1(\mathrm{mod}\ p)$.

解二：$(a+1)^p-a^p=\sum_{i=0}^{p-1}C_p^i a^i\equiv 1(\mathrm{mod}\ p)$，可得 $a^p\equiv a(\mathrm{mod}\ p)$.

例7. （1）$\varphi(9)+\varphi(10)+\varphi(11)+\varphi(12)=6+4+10+4=24$

（2）①$1\sim p^k$ 中，p 的倍数有 p^{k-1} 个，故 $\varphi(p^k)=p^k-p^{k-1}=(p-1)p^{k-1}$.

②利用容斥原理知，$\varphi(n)=n-\sum_i\frac{n}{p_i}+\sum_{i\neq j}\frac{n}{p_ip_j}-\cdots+(-1)^k\frac{n}{p_1p_2\cdots p_k}=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)n$.

由此可知 $(m,n)=1$ 时，$\varphi(mn)=\varphi(m)\varphi(n)$，积性函数