OURSTORYBEGINS

Chapter 2 作业.

1. 证明：(1) $a\equiv b \pmod m$ 当且仅当 $a-b\equiv 0 \pmod m$.

证明：$\Rightarrow$ ∵ mod 具有自反性：$b\equiv b \pmod m$

据定理 2.1.3：$a\equiv b \pmod m$ ①，$b\equiv b \pmod m$ ②，① − ②：$a-b\equiv 0 \pmod m$

$\Leftarrow$：$a-b\equiv 0 \pmod m$ ①，$b\equiv b \pmod m$ ②，① + ②：$a\equiv b \pmod m$. ∴得证.

(2) 若 $a\equiv b \pmod m$，$c\equiv d \pmod m$，则 $a-c\equiv b-d \pmod m$

证明：$a\equiv b \pmod m \Rightarrow m \mid a-b$

$c\equiv d \pmod m \Rightarrow m\mid c-d$

∴ $m \mid (a-b)-(c-d) \Rightarrow m \mid (a-c)-(b-d) \Rightarrow a-c\equiv b-d \pmod m$

∴得证.

意义：在同余运算下左右两边可以进行移项。

2. 证明：$70!\equiv 61! \pmod{71}$

证明：∵ $61!$ 与 71 互素，要证 $70!\equiv 61! \pmod{71}$，只需证 $\frac{70!}{61!}\equiv 1 \pmod{71}$

又 ∵ $\frac{70!}{61!} = 70\times 69\times\cdots\times 62 \equiv (-1)\times(-2)\times\cdots\times(-9) = -9! \equiv 1 \pmod{71}$

∴得证.

3. 设 a^{-1} 是 a 对于模 m 的逆. 证明：

(1) $an\equiv c \pmod m$ 成立的充要条件是 $n\equiv a^{-1}c \pmod m$.

证明：$\Rightarrow$ ∵ a^{-1} 是 a 对模 m 的逆，即 $a\cdot a^{-1}\equiv 1 \pmod m$

对 $an\equiv c \pmod m$ 两边同乘 a^{-1}：$a^{-1}\cdot a\cdot n\equiv c\cdot a^{-1} \pmod m$

即 $a^{-1}\equiv a^{-1} \pmod m$ $\Rightarrow n\equiv a^{-1}c \pmod m$

$\Leftarrow$：对 $n\equiv a^{-1}c \pmod m$ 两边同乘 a：$a\cdot n\equiv a\cdot a^{-1}\cdot c \pmod m$

即 $a\equiv a \pmod m$. $\Rightarrow a\cdot n\equiv c \pmod m$ ∴得证

(2) $a^{-1}b^{-1}$ 是 ab 对于模 m 的逆，即 $(ab)^{-1}\equiv a^{-1}b^{-1} \pmod m$，特别对 $\forall Z^{*}, k$

$(a^{k})^{-1}\equiv (a^{-1})^{k} \pmod m$.

OURSTORYBEGINS

证明：$\because a^{-1}$是a对模m的逆 $\Rightarrow \gcd(a,m)=1$ $\therefore \gcd(ab,m)=1$

$\because a^{-1}b^{-1}$是ab对模m的逆 $\Rightarrow (ab)\cdot(a^{-1}b^{-1})\equiv 1 \pmod m$

又$\because \gcd(ab,m)=1$ $\therefore (a^{-1}b^{-1})\equiv (ab)^{-1} \pmod m$

即 $(ab)^{-1}\equiv a^{-1}b^{-1} \pmod m$ $\therefore$得证.

设a^k逆元为t，a逆元为s.

$\therefore a^k\cdot t\equiv 1 \pmod m$ $a\cdot s\equiv 1 \pmod m$

$\Rightarrow t\equiv (a^k)^{-1} \pmod m$ $\Rightarrow s\equiv a^{-1} \pmod m \Rightarrow s^k\equiv (a^{-1})^k \equiv (a^k)^{-1} \pmod m$

即 $t\equiv s^k \pmod m$

$\Rightarrow (a^k)^{-1}\equiv (a^{-1})^k \pmod m$ $\therefore$得证.

4. (1) 写出模9的一个完全剩余系，它的每个数是奇数.

$\{9,1,11,3,13,5,15,7,17\}$.

(2) 写出模9的一个完全剩余系，它的每个数是偶数.

$\{18,10,2,12,4,14,6,16,8\}$.

(3) (1)或(2)中的要求对模10的完全剩余系能实现吗？

不能.

5. 具体写出模$m=16,17,18$的最小非负既约剩余系、绝对最小既约剩余系，并算出欧拉函数$\varphi(16)$. $\varphi(17)$. $\varphi(18)$.

解：$m=16$，最小非负：$\{1,3,5,7,9,11,13,15\}$，绝对最小：$\{-7,-5,-3,-1,1,3,5,7\}$.

$m=17$，…… $\{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$

绝对 $\{-8,-7,-6,-5,-4,-3,-2,-1,1,2,3,4,5,6,7,8\}$.

$m=18$. 最小非负：$\{1,5,7,11,13,17\}$.

绝对：$\{-7,-5,-1,1,5,7\}$

$\varphi(16)=8$. $\varphi(17)=16$, $\varphi(18)=6$.

6. 设 $m>2$，证明：

(1) 模 m 的一组既约剩余系的所有元素之和对模 m 必同余于 0.

(2) 模 m 的最小正既约剩余系各数之和等于 $m\varphi(m)/2$，对 $m=2$ 也成立.

证明：令 $A=\{a_1, a_2, \ldots, a_{\varphi(m)}\}$，共 $\varphi(m)=m-1$ 个.

$\because a_i\in A$，则 $\gcd(a_i,m)=\gcd(-a_i,m)=1$，$\gcd(m-a_i,m)=\gcd(a_i,m)=$

$\therefore (m-a_i)\in A$，令 $a_j=m-a_i$，则 $a_i\neq a_j$，否则 $2a_i=m$，矛盾

这时 $a_i+a_j=m$. 所以 A 中的元素是成对出现的，且每一对元素之和为 m

因此 $a_1+a_2+\cdots+a_{\varphi(m)}=\frac{\varphi(m)}{2}\cdot m$

$\Rightarrow$ (2) 得证.

下证 (1)：明显地，一般的既约剩余系和最小正既约剩余系在同一类里的数相差 m 的一个倍数.

又 $\because$ 非负正的元素之和 $=\frac{\varphi(m)}{2}\cdot m$ 是 m 的倍数

$\therefore$ 可得 模 m 的一组既约剩余系的所有元素之和对 m 必同余于 0.

$\Rightarrow$ (1) 得证.