第二章

1. 对哪些模 m 以下各同余式成立：

（1） $32 \equiv 11(\mathrm{mod}\, m)$；

（2） $1000 \equiv -1(\mathrm{mod}\, m)$；

（3） $2^8 \equiv 1(\mathrm{mod}\, m)$。

答：（1）$32 \equiv 11(modm) \Rightarrow m|32-11=21$，因此，$m=1,3,7,21$。

（2）$1000 \equiv -1(modm) \Rightarrow m|1000+1=1001$，又$1001=7\times 11\times 13$，所以 $m=1,7,11,13,77,91,143,1001$。

（3） $2^8 \equiv 1(modm) \Rightarrow m|2^8-1=255$，又 $255=3\times 5\times 17$，所以 $m=1,3,5,17,15,51,85,255$。

2. 证明：（1） $a \equiv b(\mathrm{mod}\, m)$ 等价于 $a-b \equiv 0(\mathrm{mod}\, m)$；

（2）若 $a \equiv b(\mathrm{mod}\, m)$， $c \equiv d(\mathrm{mod}\, m)$，则 $a-c \equiv b-d(\mathrm{mod}\, m)$。

从同余式的运算角度来解释这两个结果的意义。

证明：（1）$a \equiv b(modm) \Leftrightarrow m|(a-b) \Leftrightarrow m|(a-b)-0 \Leftrightarrow a-b \equiv 0(modm)$

（2）$a \equiv b(modm), c \equiv d(modm) \Rightarrow m|(a-b), m|(c-d)$，根据整除的性质，有 $m|(a-b)-(c-d)=(a-c)-(b-d) \Rightarrow a-c \equiv b-d(modm)$。从同余式运算的角度来看，（1）表示同余式与方程类似，可以左右移项；（2）同余式满足可加性。

3. 判断以下结论是否成立。对的给出证明，错的给出反例。

（1）若 $a^2 \equiv b^2(\mathrm{mod}\, m)$ 成立，则 $a \equiv b(\mathrm{mod}\, m)$；

（2）若 $a^2 \equiv b^2(\mathrm{mod}\, m)$，则 $a \equiv b(\mathrm{mod}\, m)$ 或 $a \equiv -b(\mathrm{mod}\, m)$ 至少有一个成立；

（3）若 $a \equiv b(\mathrm{mod}\, m)$，则 $a^2 \equiv b^2(\mathrm{mod}\, m^2)$；

（4）若 $a \equiv b(\mathrm{mod}\, 2)$，则 $a^2 \equiv b^2(\mathrm{mod}\, 2^2)$；

（5）设 p 是奇素数， $p \nmid a$。那么， $a^2 \equiv b^2(\mathrm{mod}\, p)$ 成立的充要条件是 $a \equiv b(\mathrm{mod}\, p)$ 或 $a \equiv -b(\mathrm{mod}\, p)$ 有且仅有一个成立；

（6）设 $(a,m)=1$，$k \geq 1$。那么，从 $a^k \equiv b^k(\mathrm{mod}\, m)$， $a^{k+1} \equiv b^{k+1}(\mathrm{mod}\, m)$ 同时成立可推出 $a \equiv b(\mathrm{mod}\, m)$。

答：（1）不成立。例如$4^2 \equiv 5^2(\mathtt{mod}3)$，而$4^2 \neq 5^2(\mathtt{mod}3)$；

（2）不成立。例如$9^2 \equiv 5^2(\mathtt{mod}28)$，而$9 \neq 5(\mathtt{mod}28)$，$9 \neq -5(\mathtt{mod}28)$；

（3）不成立。例如$8 \equiv 5(\mathtt{mod}3)$，而$8^2 \equiv 5^2(\mathtt{mod}3^2)$；

（4）成立。

证明：$a \equiv b(\mathtt{mod}2) \Rightarrow a=2k+b \Rightarrow a^2=4K^2+4kb+b^2 \Rightarrow a^2-b^2=4(k^2+k)$，即$a^2 \equiv b^2(\mathtt{mod}2^2)$。

（5）成立。

证明：充分性。$a^2\equiv b^2(\mathrm{mod}p)\Rightarrow p|(a^2-b^2)\Rightarrow p|(a-b)(a+b)$，由于$p$是素数，根据定理 1.3.1，有$p|(a-b)$或$p|(a+b)$，即$a\equiv b(\mathrm{mod}\ p)$或$a\equiv -b(\mathrm{mod}\ p)$。若两者同时成立，则有$p|(a+b)+(a-b)=2a$，而$p$是奇素数，所以$p|a$，矛盾。因此$a\equiv b(\mathrm{mod}\ p)$或$a\equiv -b(\mathrm{mod}\ p)$有且仅有一个成立。

必要性。$a\equiv b(\mathrm{mod}\ p)$或$a\equiv -b(\mathrm{mod}\ p)\Rightarrow p|(a-b)$或$p|(a+b)$，显然有$p|(a^2-b^2)$即$a^2\equiv b^2(\mathrm{mod}p)$。

（6）成立。

证明：a^k(a-b) $=(a^{k+1}-b^{k+1})-(a^k-b^k)b$，故m|$a^k$(a-b)

又$(a,m)=1$，知m|(a-b)

即： $a\equiv b(\mathrm{mod}m)$

另证：$a^k\equiv b^k(mod\ m)$，$a^{k+1}\equiv b^{k+1}(\mathrm{mod}\ m)$，$\Rightarrow a^k\cdot a\equiv b^k\cdot b(\mathrm{mod}m)$

$\Rightarrow a^k\cdot a\equiv a^k\cdot b(\mathrm{mod}m)$，又因为$(a,m)=1$，所以

$a^k\cdot a\equiv a^k\cdot b(\mathrm{mod}m)\Rightarrow a\equiv b(\mathrm{mod}m)$.

4. 证明：$70!\equiv 61!\ \ (\mathrm{mod}\ 71)$。

证明：

$$70!\equiv 61!(\mathrm{mod}\ 71)\Leftrightarrow 70\cdot 69\cdots 62\equiv 1(\mathrm{mod}\ 71)\Leftrightarrow (71-1)(71-2)\cdots(71-9)\equiv 1(\mathrm{mod}\ 71)$$
$$\Leftrightarrow -9!\equiv 1(\mathrm{mod}\ 71)\Leftrightarrow -(8*9)(3*4*6)(2*5*7)\equiv 1(\mathrm{mod}\ 71)\Leftrightarrow -70\equiv 1(\mathrm{mod}\ 71)$$

5. （1）求 3 对模 7 的逆；（2）求 13 对模 10 的逆。

答：（1）$3\times 5\equiv 1(\mathrm{mod}7)$，所以 3 对模 7 的逆为 5.

（2）$13\times 7\equiv 1(\mathrm{mod}10)$，所以 13 对模 10 的逆为 7.

6. 设a^{-1}是a对模m的逆。证明：

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

（2）$a^{-1}b^{-1}$是ab对模m的逆，即$(ab)^{-1}\equiv a^{-1}b^{-1}(\mathrm{mod}\ m)$。特别对任意正整数$k$，$(a^k)^{-1}\equiv (a^{-1})^k\ \mathrm{mod}(m)$。

证明：（1）$an\equiv c(\mathrm{mod}m)\Rightarrow m|(an-c)\Rightarrow m|(an-c)a^{-1}$，即$m|aa^{-1}n-a^{-1}c$，又$aa^{-1}\equiv 1(\mathrm{mod}m)\Rightarrow aa^{-1}=km+1$，所以$m|aa^{-1}n-a^{-1}c=kmn+n-a^{-1}c$
$m|n-a^{-1}c$即$n\equiv a^{-1}c(\mathrm{mod}\ m)$。反之，$m|n-a^{-1}c\Rightarrow m|(n-a^{-1}c)a=an-aa^{-1}c$
$\Rightarrow m|(n-a^{-1}c)a=an-aa^{-1}c=an-c-kmc\Rightarrow m|an-c$，即$an\equiv c(\mathrm{mod}\ m)$。

（2）$(ab)(a^{-1}b^{-1})\equiv(aa^{-1})(bb^{-1})\equiv 1(\mathrm{mod}m)$，因此，$a^{-1}b^{-1}$是$ab$对模$m$的逆。

7. （1）写出剩余类$3\mathrm{mod}17$中不超过100的正整数；

（2）写出剩余类$6\mathrm{mod}15$中绝对值不超过 90 的整数。

答：（1）3,20,37,54,71,88；（2）6,21,36,51,66,81。

8. （1）写出模 9 的一个完全剩余系，它的每个数是奇数；

（2）写出模 9 的一个完全剩余系，它的每个数是偶数；

解：（1）{0,1,2,3,4,5,6,7,8}为模 9 的一个完全剩余系，若要是其全为奇数，可令所有的偶数加 9，即{9,1,11,3,13,5,15,7,17}，重新排序为{1,3,5,7,9,11,13,15,17}

（2）{0,1,2,3,4,5,6,7,8}为模 9 的一个完全剩余系，若要是其全为偶数，可所有的奇数加 9，即{0,10,2,12,4,14,6,16,8}，重新排序为{0,2,4,6,8,10,12,14,16}

（3）（1）或（2）中的要求对模 10 的完全剩余系能实现吗？

9. （1）把剩余类$1\bmod 5$写成模 15 的剩余类之并；

（2）把剩余类$6\bmod 10$写成模 120 的剩余类之并；

（3）把剩余类$6\bmod 10$写成模 80 的剩余类之并。

答：（1）$[1]_5=\{x|x=5k+1,k\in Z\}=[1]_{15}\cup[6]_{15}\cup[11]_{15}$；

（2）$[6]_{10}=\{x|x=10k+6,k\in Z\}=[6]_{120}\cup[16]_{120}\cup[26]_{120}\cup[36]_{120}\cup[46]_{120}\cup[56]_{120}\cup[66]_{120}\cup[76]_{120}\cup[86]_{120}\cup[96]_{120}\cup[106]_{120}\cup[116]_{120}$。

（3）$[6]_{10}=\{x|x=10k+6,k\in Z\}=[6]_{80}\cup[16]_{80}\cup[26]_{80}\cup[36]_{80}\cup[46]_{80}\cup[56]_{80}\cup[66]_{80}\cup[76]_{80}$。

10. 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$\varphi(16),\varphi(17),\varphi(18)$。

答：以 16 为例，其余略。

最小非负既约剩余系$\{1,3,5,7,9,11,13,15\}$

绝对最小既约剩余系$\{-7,-5,-3,-1,1,3,5,7\}$

$\varphi(16)=2^4-2^3=8$。

11. 设$m\geq 3$。证明：

（1）模m的一组既约剩余系的所有元素之和对模m必同余于零；

（2）模m的最小正既约剩余系的各数之和等于$m\varphi(m)/2$。这结论对$m=2$也成立。

证明：（1）取模 m 的绝对最小既约剩余系，k 为该剩余系中一个整数。由于 k 与 m 互素，则-k 同样与 m 互素，所以在模 m 的绝对最小既约剩余系中 k 和-k 成对出现，因此模m的一组既约剩余系的所有元素之和对模m必同余于零。

（2）在模 m 的最小非负既约剩余系中，元素 k 和 m-k 成对出现，因此各数之和为$k_1+m-k_1+\cdots+k_{\varphi(m)}+m-k_{\varphi(m)}$=$\mathrm{m}\varphi(m)/2$。当 m=2 时，$m\varphi(m)/2=1$也成立。

12. 列出$\mathbb{Z}_{13},\mathbb{Z}_{14}$中的加法表与乘法表。

略。

13. 设$(a,b)=1, c\neq 0$。证明：一定存在整数n使得$(a+bn,c)=1$。

14. 设p是一个素数，证明：对于任意正整数，具有$a^p\equiv a(\mathtt{mod} p)$。

证明：若a与p互素，则根据欧拉定理有$a^{\varphi(p)}\equiv 1(\mathtt{mod} p)$，即有$a^p\equiv a(\mathtt{mod} p)$。

若a与p不互素，则有$p|a$，因而有$p|a^p-a$，即有$a^p\equiv a(\mathtt{mod} p)$。