1.3 同余式

一.同余和同余类

def 3.1 设$m\in\mathbb{Z}^+$，$a,b\in\mathbb{Z}$.如果$m|a-b$,则称a和b模m同余(或称a模m同余于b),表示成$a\equiv b\pmod m$.

注：a和b模m同余$\Leftrightarrow$ a和b用m去除有相同的余数r $(0\le r<m)$.

特别地，$m|a \Leftrightarrow a\equiv 0\pmod m$

同余是比整除更精细的概念.

当$m=1$时.任意两个整数模m都同余.

以下，设$m\ge 2$

Thm 3.2 设$a,b,c,d\in\mathbb{Z}$，$m\in\mathbb{Z}^+$，则

1) $a\equiv a\pmod m$

2) 若 $a\equiv b\pmod m$，则 $b\equiv a\pmod m$

3) 若 $a\equiv b\pmod m$，$b\equiv c\pmod m$，则 $a\equiv c\pmod m$

4) 若 $a\equiv b$，$c\equiv d\pmod m$，则 $a\pm c\equiv b\pm d\pmod m$

$ac\equiv bd\pmod m$

5) 若 $ac\equiv bc\pmod m$，则 $a\equiv b\pmod{\frac{m}{(c,m)}}$.

特别地，当$(c,m)=1$，$a\equiv b\pmod m$

6) 若$a\equiv b\pmod m$，则对m的每个正因子d，$a\equiv b\pmod d$

7) 对每个正整数d. $a\equiv b\pmod m \Leftrightarrow ad\equiv bd\pmod{md}$

8) 若 $a\equiv b\pmod{m_i}$ $(1\le i\le r)$，则$a\equiv b\pmod{[m_1,m_2,\cdots,m_r]}$

证：1) $a-a=0$　$m|0$　即$m|a-a$　故 $a\equiv a\pmod m$

2) 若 $a\equiv b\pmod m$　即$m|a-b$　$\therefore m|(-1)(a-b)$

即 $m|b-a$　$\therefore b\equiv a\pmod m$

3) 若 $a\equiv b\pmod m$　则 $m|a-b$

若 $b\equiv c\pmod m$　则 $m|b-c$

$\therefore m|(a-b)+(b-c)=a-c$

$\therefore a\equiv c\pmod m$

4) 若 $a\equiv b,\ c\equiv d \pmod m$ 则 $m\mid a-b,\ m\mid c-d$

$\therefore m\mid (a-b)\pm(c-d)=(a\pm c)-(b\pm d)$

$\therefore a\pm c\equiv b\pm d \pmod m$

5) $\because ac\equiv bc \pmod m$

$\therefore m\mid ac-bc=(a-b)c$

$\therefore \frac{m}{(m,c)} \Big| (a-b)\frac{c}{(c,m)}$

又 $\left(\frac{m}{(m,c)},\frac{c}{(m,c)}\right)=1$

$\therefore \frac{m}{(m,c)} \Big| a-b$

即 $a\equiv b \pmod{\frac{m}{(m,c)}}$

特别地，若 $(c,m)=1$，则 $\frac{m}{(c,m)}=m$，则 $a\equiv b \pmod m$

6) $\because a\equiv b \pmod m$ $\therefore m\mid a-b$

对 $\forall d\mid m$ 则 $d\mid a-b$ $\therefore a\equiv b \pmod d$

7) "$\Rightarrow$"

若 $a\equiv b \pmod m$ 则 $m\mid a-b$

$\therefore md\mid d(a-b)$ $\forall d\in \mathbb{Z}^+$

即 $md\mid ad-bd$ $\therefore ad\equiv bd \pmod{md}$

"$\Leftarrow$"

若 $ad\equiv bd \pmod{md}$ 则 $md\mid ad-bd=(a-b)d$

$\therefore m\mid a-b$ $\therefore a\equiv b \pmod m$

8) $a\equiv b \pmod{m_i}$ 则 $m_i\mid a-b$

即 $a-b$ 是 $m_1,m_2,\cdots,m_r$ 的公倍数

$\therefore a-b$ 是 $[m_1,m_2,\cdots,m_r]$ 的倍数

即 $[m_1,m_2,\cdots,m_r]\mid a-b$

$\therefore a\equiv b \pmod{[m_1,m_2,\cdots,m_r]}$

Col 3.3 设 $f(x)$ 是整系数多项式，则对于 $A, B \in \mathbb{Z}$，如果 $A \equiv B \pmod m$，则 $f(A) \equiv f(B) \pmod m$

注意：同余式做除法未必成立

即由 $ac \equiv bc \pmod m$ 不一定有 $a \equiv b \pmod m$

只有在 $(c, m) = 1$ 时，才有 $ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod m$

def 3.4 设 m 是固定的正整数，模 m 彼此同余的整数形成的集合叫做一个模 m 的同余类。对于整数 a，a 所在的模 m 同余类表示成 $\bar{a}$。于是

$$\bar{a} = \{n \in \mathbb{Z} : n \equiv a \pmod m\} = \{a + lm : l \in \mathbb{Z}\}$$

因而对于 $a, b \in \mathbb{Z}$，$\bar{a} = \bar{b}$ 当且仅当 $a \equiv b \pmod m$

每个整数 m 总会同余于 $0, 1, 2, \cdots, m-1$ 中一个，因而 $\mathbb{Z}$ 可分析成 m 个彼此不相交的模 m 同余类 $\bar{0}, \bar{1}, \cdots, \overline{m-1}$.

从每个模 m 同余类中取出一个整数作为"代表"，用这种方式找到的 m 个整数 $a_1, a_2, \cdots, a_m$ 叫做是模 m 的一个完全代表系，一般地，m 个整数 $\{a_1, a_2, \cdots a_m\}$ 是模 m 的一个完系，当且仅当它们彼此模 m 不同余（从而它们恰好是 m 个同余类的代表元）

设 a 是与 m 互素的整数，则模 m 同余类 $\bar{a}$ 中每个整数 a' 均与 m 互素，这是整个同余类的性质。这样的同余类叫做模 m 的缩同余类。模 m 的同余类共有 m 个：

$\bar{1}, \bar{2}, \cdots, \overline{m-1}, \bar{m} = \bar{0}$，其中 $\bar{i}$ 是模 m 的缩同余类 $\Leftrightarrow (i, m) = 1$

所以模 m 的缩同余类的个数即是 Euler 函数 $\varphi(m)$。从每个缩同余类取一个"代表"，$\varphi(m)$ 个"代表"组成的集合 $\{a_1, a_2, \cdots, a_{\varphi(m)}\}$ 叫做模 m 的一个缩代表系，简称缩系。一般地，$\varphi(m)$ 个整数 $\{a_1, a_2, \cdots, a_{\varphi(m)}\}$ 是模 m 的一个缩系，当且仅当它们均与模 m 互素并且彼此模 m 不同余.

定理3.5 设m为正整数，$a、b\in\mathbb{Z}$，$(a,m)=1$

1）若$\{c_1,c_2,\cdots,c_m\}$是模m的完系，则

$\{ac_1+b,ac_2+b,\cdots,ac_m+b\}$也是模$m$的完系

2）若$\{r_1,r_2,\cdots,r_{\varphi(m)}\}$是模$m$的缩系，则

$\{ar_1,ar_2,\cdots,ar_{\varphi(m)}\}$也是模$m$的缩系

3）存在$x\in\mathbb{Z}$，使得$ax\equiv b \pmod m$，并且此同余方程的所有整数解为形成m的一个同余类.

证明：1）若$ac_i+b\equiv ac_j+b \pmod m$

则$ac_i\equiv ac_j \pmod m$

又$(a,m)=1$

所以$c_i\equiv c_j \pmod m$ 故$i=j$

所以$ac_1+b,ac_2+b,\cdots,ac_m+b$模$m$彼此不同余

所以$\{ac_1+b,ac_2+b,\cdots,ac_m+b\}$是模$m$的完系

2）$\because\{r_1,r_2,\cdots,r_{\varphi(m)}\}$是模$m$的缩系

$\therefore r_1,r_2,\cdots,r_{\varphi(m)}$模$m$彼此不同余，且$(r_i,m)=1$ $(1\le i\le\varphi(m))$

$\because(a,m)=1$

$\therefore ar_1,ar_2,\cdots,ar_{\varphi(m)}$模$m$彼此不同余

且$(ar_i,m)=1$ $(1\le i\le\varphi(m))$

故$\{ar_1,ar_2,\cdots,ar_{\varphi(m)}\}$也是模$m$的缩系

3）任取模m的一个完系$\{c_1,c_2,\cdots,c_m\}$

由1）知，$\{ac_1-b,ac_2-b,\cdots,ac_m-b\}$也是模$m$的完系

$\exists i$，使得$ac_i-b\equiv 0 \pmod m$

即$x=c_i$是同余方程$ax\equiv b \pmod m$的一个解

另一方面，若$x=c$是$ax\equiv b \pmod m$的解

则$ac\equiv b\equiv ac_i \pmod m$ $\therefore c\equiv c_i \pmod m$

$\therefore c\in\overline{c_i}$ $\therefore ax\equiv b \pmod m$的全部解形成模$m$的一个同余类$\overline{c_i}$

由该定理知：当$(a,m)=1$时，同余方程$ax\equiv b \pmod m$必有整数解，并且若c是一个解，则全部解形成模m的一个同余类$\overline{c}$，表示成$x\equiv c \pmod m$.

但若m和a均很大时，寻求一个解不容易，下例示范如何将a逐渐缩小.

例1. 解一次同余方程 $24x\equiv 7 \pmod{59}$

解：$24x\equiv 7 \pmod{59}$

$\Leftrightarrow 24x\equiv 7+59\equiv 66 \pmod{59}$

$\Leftrightarrow 4x\equiv 11 \pmod{59}$ $\quad ((6,59)=1)$

$\Leftrightarrow 4x\equiv 11-59\equiv -48 \pmod{59}$

$\Leftrightarrow x\equiv -12 \pmod{59}$ $\quad ((4,59)=1)$

从而得到方程的全部解 $x\equiv 47 \pmod{59}$

方程也可写成：$x\equiv \frac{7}{24}\equiv\frac{7+59}{24}\equiv\frac{66}{24}\equiv\frac{11}{4}\equiv\frac{11-59}{4}\equiv\frac{-48}{4}\equiv -12$

$\equiv -12+59\equiv 47 \pmod{59}$

需注意：分子和分母的最大公因子一定要和模数互素，此时分数可以约分.

例2. $60x-14y=18$ 即 $30x-7y=9$

模7后得同余方程：$30x\equiv 9 \pmod 7$

$\therefore x\equiv\frac{9}{30}\overset{(3,7)=1}{\equiv}\frac{3}{10}\equiv\frac{3+7}{10}\overset{(10,7)=1}{\equiv}1 \pmod 7$

$\therefore x=1+7t$，$t\in\mathbb{Z}$，代入原方程得：$60(1+7t)-14y=18$

$14y=60+60\times 7t-18=42+60\times 7t$

$\therefore y=3+30t$

$\therefore 60x-14y=18$ 的全部整数解为

$(x,y)=(1+7t,3+30t)\ (t\in\mathbb{Z})$

二. 模m同余类环 $\mathbb{Z}_m$

固定一个正整数m，则模m有m个同余类 $\overline{a_1},\overline{a_2},\cdots,\overline{a_m}$，其中 $\{a_1,a_2,\cdots,a_m\}$ 是模m的一个完系. 现将每个模m的同余类看成是一个元素，那么m个元素 $\overline{a_1},\overline{a_2},\cdots,\overline{a_m}$ 形成一个新集合，表示成 $\mathbb{Z}_m$，叫做模m的同余类集合.

$\mathbb{Z}_m$中共有m个元素：$\mathbb{Z}_m=\{\bar{0},\bar{1},\cdots,\overline{m-1}\}$，对于$a,b\in\mathbb{Z}$，$\bar{a}$和$\bar{b}$是$\mathbb{Z}_m$中同一个元素当且仅当$a\equiv b\pmod m$.

在$\mathbb{Z}_m$中以自然方式引入加、减、乘运算，也就是同余类的运算.

1）对于$\bar{a},\bar{b}$，定义$\bar{a}$与$\bar{b}$的和为$a+b$所属的同余类，即$\bar{a}+\bar{b}\overset{d}{=}\overline{a+b}$

若取$\bar{a}$和$\bar{b}$中的代表元a'和b'，即$a'\equiv a\pmod m$，$b'\equiv b\pmod m$

则$\bar{a}=\overline{a'}$，$\bar{b}=\overline{b'}$，则定义的$\overline{a'+b'}$与$\overline{a+b}$一致.

$a'\equiv a\pmod m$　$b'\equiv b\pmod m$　$a'+b'\equiv a+b\pmod m$

从而$\overline{a'+b'}=\overline{a+b}$

说明同余类的加法定义与代表元的选取无关，即有加法定义是合理的.

2）$\bar{a}-\bar{b}\overset{d}{=}\overline{a-b}$　$\bar{a}\cdot\bar{b}=\overline{ab}$

$\mathbb{Z}_m$上定义了加、减、乘运算，并且满足结合律，交换律和分配律

从而$\mathbb{Z}_m$是（交换）环，$\mathbb{Z}_m$叫模m的同余类环.

整数环$\mathbb{Z}$中的1有性质：$1\cdot a=a$

同余类环$\mathbb{Z}_m$中元素$\bar{1}$有类似的性质：$\bar{1}\cdot\bar{a}=\bar{a}$

整数环$\mathbb{Z}$中乘法可逆元素只有±1，故$\mathbb{Z}$中除法不一定可以进行.

在同余类环$\mathbb{Z}_m$中，元素$\bar{a}$乘法可逆，是指$\exists\bar{b}$，使得$\bar{a}\cdot\bar{b}=\bar{1}$，相当于$ab\equiv1\pmod m$，即同余方程$ax\equiv1\pmod m$有整数解，这等价于$(a,m)=1$，即$\bar{a}$是模$m$的缩同余系，因而环$\mathbb{Z}_m$中乘法可逆元素共有$\varphi(m)$个.

在复数集合$\mathbb{C}$，实数集合$\mathbb{R}$和有理数集合$\mathbb{Q}$中，0不是乘法可逆的，而非零的数都是乘法可逆的，从而在这些集合中有四则运算，只是0不能为除数，这样的代数结构叫做域.（整数环$\mathbb{Z}$不是域.）

对同余类环$\mathbb{Z}_m$，$\bar{0}$也不是乘法可逆的. 当m为素数p时，如果$\bar{a}\neq\bar{0}$，即$a\not\equiv0\pmod p$，则$(a,p)=1$，从而$\bar{a}$是乘法可逆元素.

逆表示成$(\bar{a})^{-1}$，

例如：当$p=5$时，$(\bar{1})^{-1}=\bar{1}$，$(\bar{2})^{-1}=\bar{3}$，$(\bar{3})^{-1}=\bar{2}$

$(\bar{4})^{-1}=\bar{4}$

即$\mathbb{Z}_p$中每个非零元素$\bar{a}$（$\bar{a}\neq\bar{0}$）均可逆，从而$\mathbb{Z}_p$中可进行四则运算，从而$\mathbb{Z}_p$是域，它由有限个元素（p个元素）组成的域，叫做有限域.

当 m 不是素数时，$m=ab$，$a,b\in\mathbb{Z}$，$a,b\in\mathbb{Z}$，$2\le a,b\le m-1$，因而 $\bar{a}\ne\bar{0}$，$\bar{b}\ne\bar{0}$，但 $\bar{a}\cdot\bar{b}=\bar{m}=\bar{0}$，此时 $\bar{a}$ 与 $\bar{b}$ 在 $\mathbb{Z}_m$ 中不可逆，因为它们都不是模 m 的缩同余类（$(a,m)=a>1$，$(b,m)=b>1$）。所以当 m 不是素数时，$\mathbb{Z}_m$ 不是域。

$\mathbb{Z}_m^*$ 表示同余类环 $\mathbb{Z}_m$ 中乘法可逆元素组成的集合，它只有 $\varphi(m)$ 个元素。当 $m=p$ 为素数时，$\mathbb{Z}_p^*$ 就是除了 $\bar{0}$ 以外的 $p-1$ 个元素，由于 $\mathbb{Z}_m^*$ 中元素的可逆，所以在 $\mathbb{Z}_m^*$ 中有乘法的逆运算——除法，确切地说：

1）若 $\bar{a},\bar{b}\in\mathbb{Z}_m^*$（即 $(a,m)=(b,m)=1$，则 $\bar{a}\cdot\bar{b}=\overline{ab}\in\mathbb{Z}_m^*$

（$(ab,m)=1$）从而 $\mathbb{Z}_m^*$ 中元素的乘积仍为 $\mathbb{Z}_m^*$ 中元素

2）若 $\bar{a}\in\mathbb{Z}_m^*$，则 $\bar{a}$ 在 $\mathbb{Z}_m^*$ 中可逆，即有 $\bar{b}\in\mathbb{Z}_m^*$，使得 $\bar{a}\cdot\bar{b}=\bar{1}$

（若 $\bar{b}$ 为 $\bar{a}$ 的逆，则 $\bar{a}$ 也是 $\bar{b}$ 的逆）

一般地，若集合 G 上定义了一个运算 $*$ 且满足以下条件：

A）结合律：$(a*b)*c=a*(b*c)$

B）具有"幺元素" e，即对每个 $a\in G$，$e*a=a*e=a$

C）每个 $a\in G$，都有逆元素 b，即 $a*b=b*a=e$

则 G 叫做群。如果运算 $*$ 还满足交换律：$a*b=b*a$，则 G 叫做交换群。

从同余类引申出近世代数研究的三个基本代数结构（群，环，域）的具体例子：

同余类环 $\mathbb{Z}_m$　乘法群 $\mathbb{Z}_m^*$　和 有限域 $\mathbb{Z}_p$。

从而关于整除和同余的许多结果，可以转述成这些数学结构中的语言，比如：

A）若 $ac\equiv bc \pmod m$，$(m,c)=1$，则 $a\equiv b \pmod m$

对于环 $\mathbb{Z}_m$ 中的元素 $\alpha=\bar{a}$，$\beta=\bar{b}$ 和 $\gamma=\bar{c}$，若 $\alpha\gamma=\beta\gamma$，而 γ 为逆元，则 $\alpha=\beta$（消去律）

B）设 p 为素数，$a,b\in\mathbb{Z}$，若 $p\mid ab$，则 $p\mid a$ or $p\mid b$

在有限域 $\mathbb{Z}_p$ 中，若 $\alpha,\beta\in\mathbb{Z}_p$，$\alpha\beta=\bar{0}$，则 $\alpha=\bar{0}$ or $\beta=\bar{0}$

C）若 $\{c_1,c_2,\cdots,c_m\}$ 是模 m 的完系，$a,b\in\mathbb{Z}$，$(a,m)=1$，则 $\{ac_1+b,\cdots,ac_m+b\}$ 也是模 m 的完系。

若$\gamma_1,\gamma_2,\cdots,\gamma_m$是环$\mathbb{Z}_m$的全部元素，$\alpha,\beta\in\mathbb{Z}$，而$\alpha$是$\mathbb{Z}_m$中可逆元，则$\alpha\gamma_1+\beta,\alpha\gamma_2+\beta,\cdots,\alpha\gamma_m+\beta$也是$\mathbb{Z}_m$的全部元素

D) 若$\{\gamma_1,\gamma_2,\cdots,\gamma_{\varphi(m)}\}$是模$m$的缩系，$(a,m)=1$，则

$\{a\gamma_1,a\gamma_2,\cdots,a\gamma_{\varphi(m)}\}$是模$m$的缩系.

若$\mathbb{Z}_m^*=\{\gamma_1,\gamma_2,\cdots,\gamma_{\varphi(m)}\}$，则对$\forall\alpha\in\mathbb{Z}_m^*$，$\mathbb{Z}_m^*=\{\alpha\gamma_1,\cdots,\alpha\gamma_{\varphi(m)}\}$

威尔逊(Wilson)定理:

若p为素数，则$(p-1)!\equiv(-1)(\mathrm{mod}\ p)$.

证：当$p=2$时，$(2-1)!=1\equiv-1\ (\mathrm{mod}\ 2)$

当p为奇素数时，定理相当于要证：有限域$\mathbb{Z}_p$中所有非零元的乘积为$\bar{-1}$.

$\mathbb{Z}_p$中每个非零元素α都可逆，即有$\alpha^{-1}\in\mathbb{Z}_p$，使得$\alpha\alpha^{-1}=\bar{1}$.

$\because\alpha^{-1}$的逆元素为α，故$\mathbb{Z}_p$中每对互逆元素的乘积为$\bar{1}$.

若$\alpha=\alpha^{-1}$，则$\alpha^2=\bar{1}$，即$0=\alpha^2-\bar{1}=(\alpha-\bar{1})(\alpha+\bar{1})$

$\therefore\alpha-\bar{1}=0$ or $\alpha+\bar{1}=0$ 即$\alpha=\bar{1}$或$\alpha=\bar{-1}$

$\because$域$\mathbb{Z}_p$中$p-1$个非零元素除了$\bar{1}$和$\bar{-1}$之外，其他元素是一些互逆的元素时，每对乘积为$\bar{1}$

$\therefore\mathbb{Z}_p$中的所有非零元素的积为$\bar{1}\cdot\bar{-1}=\bar{-1}$ 即$(p-1)!\equiv-1\ (\mathrm{mod}\ p)$

三、Euler-Fermat定理

Thm 3.6 (Euler定理) 设$m\in\mathbb{Z}^+$，$(a,m)=1$，则$a^{\varphi(m)}\equiv1(\mathrm{mod}\ m)$.

特别地，若$m=p$为素数，$(a,p)=1$，则$a^{p-1}\equiv1\ (\mathrm{mod}\ p)$ (费马小定理)

证：设$\mathbb{Z}_m^*=\{\alpha_1,\alpha_2,\cdots,\alpha_{\varphi(m)}\}$，由$(a,m)=1$可知$\alpha=\bar{a}\in\mathbb{Z}_m^*$

$\therefore\mathbb{Z}_m^*=\{\alpha\alpha_1,\alpha\alpha_2,\cdots,\alpha\alpha_{\varphi(m)}\}$

从而在乘法群$\mathbb{Z}_m^*$中，$\alpha_1\alpha_2\cdots\alpha_{\varphi(m)}=(\alpha\alpha_1)(\alpha\alpha_2)\cdots(\alpha\alpha_{\varphi(m)})$

$=\alpha^{\varphi(m)}\alpha_1\alpha_2\cdots\alpha_{\varphi(m)}$

由消去律可知：$\alpha^{\varphi(m)}=\bar{1}$ 即$a^{\varphi(m)}\equiv1\ (\mathrm{mod}\ m)$

注：1) Fermat小定理 也可说成 对$\forall a\in\mathbb{Z}$，$a^p\equiv a\ (\mathrm{mod}\ p)$.

$\because$当$p\nmid a$时，$a^{p-1}\equiv1\ (\mathrm{mod}\ p)$ 从而$a^p\equiv a\ (\mathrm{mod}\ p)$

而当$p\mid a$时，同余式两边均$\equiv0\ (\mathrm{mod}\ p)$

故有限域$\mathbb{Z}_p$中p个元素均是由方程$x^p-x=0$的解.

2) 当$(a,m)=1$时 $\alpha=\bar{a}$是环$\mathbb{Z}_m$中可逆元素. Euler定理给出求逆的一种方法:

由$\alpha^{\varphi(m)}=\bar{1}$可知$\alpha^{-1}=\alpha^{\varphi(m)-1}$, 即当$(a,m)=1$时, 同余方程 $ax\equiv 1 \pmod m$ 的解为 $x=a^{\varphi(m)-1}$, 所以同余方程 $ax\equiv b \pmod m$ 的解 $x\equiv ba^{-1}\equiv ba^{\varphi(m)-1} \pmod m$

例: 对$m=17$, $\varphi(17)=16$, 同余方程$7x\equiv 3 \pmod{17}$的解为

$x\equiv 3\cdot 7^{15} \pmod{17}$ 由于

$7^2=49\equiv -2 \quad 7^4\equiv 4 \quad 7^8\equiv 16\equiv -1 \pmod{17}$

$\therefore x\equiv 3\cdot 7^{8+4+2+1}\equiv 3\cdot(-1)\cdot 4\cdot(-2)\cdot 7\equiv 24\cdot 7\equiv 7\cdot 7$

$\equiv 49\equiv 15 \pmod{17}$

Thm 3.7 设p为素数, $\alpha,\beta\in\mathbb{Z}_p$, 则$(\alpha+\beta)^p=\alpha^p+\beta^p$.

换句话, 对$\forall a$和b, $(a+b)^p\equiv a^p+b^p \pmod p$)

证: 由注1): $(\alpha+\beta)^p\equiv \alpha+\beta \equiv \alpha^p+\beta^p \pmod p$)

(即 $(a+b)^p\equiv(a+b)\equiv a^p+b^p \pmod p$))