a 与 b 模 m 同余 $:\Longleftrightarrow$ a 与 b 被 m 除余数相同

记作 $a\equiv b\pmod m \Leftrightarrow m\mid a-b$

命题1. 若 $a\equiv b\pmod m \Rightarrow m\mid a-b$

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

$\Rightarrow m\mid (a-b)+(c-d)$

$\Downarrow$

$m\mid (a+c)-(b+d)$

$\Leftarrow$

$a+c\equiv b+d\pmod m$

同理 $ac\equiv bd\pmod m$

缺补

$\mathbb{Z}_m := \{\bar 0, \bar 1, \bar 2, \cdots, \overline{m-1}\}$

规定加法 $:\ \bar a+\bar b := \overline{a+b}$

$\bar a = \bar c$, $\bar b = \bar d$, $\overline{a+b} = \overline{c+d}$

$a\equiv c\pmod m$, $b\equiv d\pmod m \Rightarrow a+b\equiv c+d\pmod m$

乘法 $:\ \bar a\cdot\bar b = \overline{ab}$

缺补

零元为 $\bar 0$，负元为 $\overline{-a}$

易验证 $\mathbb{Z}_m$ 成为一个有单位元交换环

称为 模 m 剩余类环

定义1. 设 R 为一有单位元的环，对于 $a\in R$，若有 $b\in R$，

$s.t.\ ab=ba=1$，

则称 a 是 可逆元，把 b 称为 a 的 逆元 a^{-1}

定义2. 若F是有单位元的交换环，并且每一个非零元都是可逆元，
则称F是一个域（field）

定理1. 若P为素数，则 $\mathbb{Z}_p$ 是一个域，

证：$\mathbb{Z}_p$ 为含单位元1的交换环

任取一非零元 $\bar{a}$，其中 $0<a<p$.

则 $p \nmid a \Rightarrow (p,a)=1$

$\exists u, v \in \mathbb{Z}$, s.t. $up+va=1$

在 $\mathbb{Z}_p$ 中 $\bar{1}=\overline{up+va}=\bar{u}\bar{p}+\bar{v}\bar{a}=\bar{v}\bar{a}$

$\therefore \bar{a}$ 为可逆元，$\therefore \mathbb{Z}_p$ 为域

若m是合数，则 $\mathbb{Z}_m$ 不是域

证：$\because m$ 为合数 $\therefore \exists a,b<m$, s.t. $ab=m$

$\therefore \bar{a}\bar{b}=\bar{m}=\bar{0}$

设 $\bar{a}$ 有可逆元 $\bar{c}$

则 $\bar{c}\bar{a}\bar{b}=\bar{1}\bar{b}=\bar{b}=\bar{c}\bar{0}=\bar{0}$ $\therefore b \geq m$，矛盾

$\therefore \bar{a}$ 不存在可逆元 $\therefore \mathbb{Z}_m$ 不是域

定理2. 任一域F，单位元为e，

情形1，$\forall m \in \mathbb{N}^*$，有 $me \neq 0$，称数域特征为0

情形2. 一素数n，有 $ne=0$ $n'e \neq 0$，$(0<n'<n)$ 特征为P

证：设 n不为素数，则 $n=n_1 n_2$，$0<n_i<n$，n_i 为可逆元

$n_1 e \cdot n_2 e = n_1(e(n_2 e)) = n_1(n_2(ee)) = (n_1 n_2)e = ne = 0$

$(n_1e)^{-1}((n_1e)(n_2e)) = (n_1e)^{-1}0 = n_2e \Rightarrow n_2e = 0$ 矛盾

$\therefore n$ 为素数

注：域 F 上一元多项式环 $F[x]$.

当 F 为有限域时 $f = g \not\Leftrightarrow f(x) = g(x)$