在特定的场合下，我们非常关心当一个整数除以另一个正整数时所得的余数。比如，从现在开始再过 70 个小时是几点，又比如再过 15 年是中国农历的哪一年。因为经常对余数感兴趣，我们引入了 mod 符号来表示取余运算。其中的一种特殊情况也引起了我们的注意：两个整数除以正整数 m 时具有同样的余数。由此引出定义 1：

定义 1：如果 a 和 b 为整数，m 是正整数，则当 m 整除 a-b 时，称 a 模 m 同余 b。记作

$a \equiv b(\mathrm{mod}\ m)$，也被称为同余式，m 是模(modulus)。如果 a 和 b 不是模 m 同余的，则写成

$a \not\equiv b(\mathrm{mod}\ m)$。

取余运算和同余式之间的关系有如下定理：

定理 1：令 a 和 b 为整数，并令 m 为正整数。则$a \equiv b(\mathrm{mod}\ m)$当且仅当$a\ \mathrm{mod}\ m = b\ \mathrm{mod}\ m$。

处理同余关系有一个很有用的方法。

定理 2：令 m 为正整数，整数 a 和 b 是模 m 同余的当且仅当存在整数 k 使得$a = b + km$。

同余类：所有和 a 模 m 同余的整数集合称为 a 模 m 的同余类。

加法和乘法是保同余的。

定理 3：令 m 为正整数。如果$a \equiv b(\mathrm{mod}\ m)$，$c \equiv d(\mathrm{mod}\ m)$，则

$$a + c \equiv b + d(\mathrm{mod}\ m) \text{ 并且 } ac \equiv bd(\mathrm{mod}\ m) \tag{1}$$

证：

因为$a \equiv b(\mathrm{mod}\ m)$，$c \equiv d(\mathrm{mod}\ m)$，由上述定理 2 可知$a = b + km$，$c = d + tm$。于是

$$a + c = b + d + (k + t)m \tag{2}$$

$$ac = bd + (bt + kd + ktm)m \tag{3}$$

由定理 2 可知：

$$a + c \equiv b + d(\mathrm{mod}\ m) \text{ 及 } ac \equiv bd(\mathrm{mod}\ m) \tag{4}$$

下述推论给出了利用每个整数的 **mod m** 函数值找出两个整数的和与积的该函数的值。

推论 2：令 m 是正整数，a 和 b 是整数。则：

$$(a + b)\,\mathbf{mod}\ m = \big((a\ \mathbf{mod}\ m) + (b\ \mathbf{mod}\ m)\big)\,\mathbf{mod}\ m \tag{5}$$

并且

$$ab\ \mathbf{mod}\ m = \big((a\ \mathbf{mod}\ m)(b\ \mathbf{mod}\ m)\big)\,\mathbf{mod}\ m \tag{6}$$

实例：

求$(99^2\ mod\ 32)^2\ mod\ 15$。

解：$(99^2\ mod\ 32)^2\ mod\ 15 = (99\ mod\ 32 * 99\ mod\ 32)^2 mod\ 15 = 81\ mod\ 15 = 6$

在Z_m，即小于 m 的非负整数的集合$\{0,1,2,3, \cdots, m-1\}$上定义运算$+_m$和$\cdot_m$，其运算如下：

$$a +_m b = (a+b) mod\ m \tag{7}$$

模 m 算术满足的性质如下：

封闭性：如果 a 和 b 属于Z_m，则$a +_m b$和$a \cdot_m b$也属于Z_m。

结合律：如果 a、b 和 c 属于Z_m，则$(a +_m b) +_m c = a +_m (b +_m c)$和$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$。

交换律：如果 a 和 b 属于Z_m，则$a +_m b = b +_m a$和$a \cdot_m b = b \cdot_m a$。

加法逆元：如果$a \neq 0$属于Z_m，则$m-a$是 a 的模 m 的加法逆元，而 0 是其自身的加法逆元，则$a +_m (m-a) = 0$ 且 $0 +_m 0 = 0$。

分配率：如果 a、b 和 c 属于Z_m，则$a \cdot_m (b+c) = (a \cdot_m b) +_m (a \cdot_m c)$和$(a +_m b) \cdot_m c = (a \cdot_m c) + (b \cdot_m c)$。

带有模 m 加法和乘法运算的Z_m满足上述所列条件，所以Z_m连同模加法被称为一个**交换群**，而Z_m连同模加法和模乘法被称为一个**交换环**。