1.2.ex 整除与同余

整除和同余是数论中的概念，主要研究整数之间的某种等价关系。但在弹幕制作中很少只讨论整数，因此本教程的整除和同余不局限于整数。

$i)$ 整除

首先给出整除的定义：

> 设 a, b 是任意两个数，其中 $b \neq 0$。如果存在整数 q 使得
>
> $$a = q \cdot b$$
>
> 就称 a 被 b 整除，并把 b 叫做 a 的 **因数**，把 a 叫做 b 的 **倍数**。否则，就称 a 不能被 b 整除。

根据定义有：

1. 0 是任何非零数的倍数。
2. 1 是任何整数的因数。
3. 任何非零数是其自身的因数，也是其自身的倍数。

整除具有传递性，即：

> 设 $a,\ b \neq 0,\ c \neq 0$ 为三个数，若 b 被 a 整除，c 被 b 整除，则 c 被 a 整除。

在线性组合中，整除的性质保持不变，即：

> 设 $b \neq 0$。若 $a_1, a_2, \ldots, a_n$ 都被 b 整除，则对任意 n 个整数 $s_1, s_2, \ldots, s_n$，$s_1 a_1 + s_2 a_2 + \cdots + s_n a_n$ 被 b 整除。

$ii)$ 带余数除法

不是任意两个非零数之间都有整除关系，所以我们引入带余数除法。

> 设 a, b 是两个数，其中 $b > 0$，则存在唯一一组 q, r 使得
>
> $$a = q \cdot b + r, \quad q \text{ 为整数}, \ 0 \leq r < b$$
>
> 我们将 q 称为 a 被 b 除所得的 **不完全商**，r 称为 a 被 b 除所得的 **余数**。

实际运用带余数除法时，可以根据需要将余数取成其他形式。

> 设 a, b 是两个数，其中 $b > 0$，则对任意数 c，存在唯一一组 q, r 使得
>
> $$a = q \cdot b + r, \quad q \text{ 为整数}, \ c \le r < b + c$$

在实际应用中，常采用以下两种形式的余数：

1. 最小非负余数：$0 \le r < b$
2. 绝对值最小余数：$-\frac{b}{2} \le r < \frac{b}{2}$ 或 $-\frac{b}{2} < r \le \frac{b}{2}$

$iii)$ 同余

> 给定 $m > 0$，对两个数 a, b，以下几种说法是等价的：
>
> 1. a, b 模 m 同余；
> 2. a, b 被 m 除所得余数相等；
> 3. $a - b$ 被 m 整除；
> 4. 存在整数 k，使得 $a = k \cdot m + b$。
>
> 我们将 a, b 模 m 同余记作
>
> $$a \equiv b \ (mod\, m)$$

根据先前介绍的整除的性质，可以得到同余的一些性质。

> 对 $m > 0$ 和任意 a，有
>
> $$a \equiv a + m \ (mod\, m)$$

> 对 $m > 0$ 和任意正整数 d，若 $a \equiv b \ (mod\, d \cdot m)$，则
>
> $$a \equiv b \ (mod\, m)$$

> 对 $m > 0$，若 $a_1 \equiv a_2 \ (mod\, m)$，$b_1 \equiv b_2 \ (mod\, m)$，则
>
> $$a_1 + b_1 \equiv a_2 + b_2 \ (mod\, m)$$

> 对 $m > 0$ 和任意 $d > 0$，若 $a \equiv b \ (mod\, m)$，则
>
> $$d \cdot a \equiv d \cdot b \ (mod\, d \cdot m)$$

注意，由 $a \equiv b \ (mod\, m)$ 不能得到 $d \cdot a \equiv d \cdot b \ (mod\, m)$。该推导只在 d 为整数时成立。

$iv)$ 整除与同余 in LuaSTG

`lua` 通过取余数运算符 `%` 和向下取整函数 `math.floor` 完成整除和同余的相关计算，其中 `math.floor(x)` 给出 **不大于 x 的最大整数**。

> 在如下带余数除法的定义中，余数 r 对应取余运算 `a % b`，不完全商对应取整运算 `math.floor(a / b)`。
>
> $$a = q \cdot b + r, \quad q \text{ 为整数}, \; 0 \le r < b$$

> a 被 b 整除等价于 a 被 b 除的余数为 0，因此可以用 `a % b == 0` 判定。类似地，$a \equiv b \; (mod \; m)$ 可以用 `a % m == b % m` 或 `(a - b) % m == 0` 判定。
>
> `Tips:` 小心浮点误差。

对于其他形式的带余数除法，`lua` 的对应表示会略复杂一些。

> 设 a, b 是两个数，其中 $b > 0$，则对任意数 c，存在唯一一组 q, r 使得
>
> $$a = q \cdot b + r, \quad q \text{ 为整数}, \; c \le r < b + c$$
>
> 设 $r' = r - c$，则有 $a - c = q \cdot b + r'$，$0 \le r' < b$。
>
> 所以式中不完全商 q 对应 `math.floor((a - c) / b)`，余数 r 对应 `(a - c) % b + c`。