模运算与同余

模运算

目的是求两个数相除的余数；在模运算中给定两个数a和b（b不等于0），模运算的结果是a除以b后得到的余数，通常表示为a mod b或a % b

如：11除以2的余数是1，所以11 mod 2或11 % 2的结果是1

同余

概念

两个整数a和b除以同一个正整数m，得到的余数相等，则称a和b对模m同余

定义

如果a和b都是整数，对于一个固定的整数m，当$m|(a-b)$时，我们说a，b对模m同余，记作a≡b(mod m)

如：$29 \equiv 2(mod\ 9)$、$93 \equiv -7(mod\ 50)$

由于$29-2=27=3\times 9$，所以有$29 \equiv 2(mod\ 9)$

由于$93-(-7)=27=2\times 50$，所以有$93 \equiv -7(mod\ 50)$

引理1

如果a,b,c都是整数，m是一个正整数，则当

$a \equiv b(mod\ m)$

$b \equiv c(mod\ m)$

都成立时，我们有a≡c(mod m)

如：$3 \equiv 5(mod\ 2)$、$5 \equiv 7(mod\ 2)$，那么$3 \equiv 7(mod\ 2)$

引理2

如果a,b,c,d都是整数，而m是一个正整数，则当

$a \equiv b(mod\ m)$

$c \equiv d(mod\ m)$

都成立时，我们有

a+c≡b+d(mod m)

a-c≡b-d(mod m)

axc≡bxd(mod m)

如：$22 \equiv 26(mod\ 4)$、$9 \equiv 13(mod\ 4)$，那么 $22+9 \equiv 26+13(mod\ 4)$、$22-9 \equiv 26-13(mod\ 4)$、$22 \times 9 \equiv 26 \times 13(mod\ 4)$

引理3

如果a, b, c都是整数，m是一个正整数，则当

$a \equiv b(mod\ m)$

成立时，我们有ac≡bc(mod m)

如：$3 \equiv 5(mod\ 2)$，那么$3 \times 7 \equiv 5 \times 7(mod\ 2)$

引理4

如果a, b都是整数，而m，n都是正整数，则当

$a \equiv b(mod\ m)$

成立时，我们有$a^n \equiv b^n(mod\ m)$

如：$3 \equiv 5(mod\ 2)$，那么$3^3 \equiv 5^3(mod\ 2)$

引理5

如果$a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$都是整数，$m, n$都是正整数，则当

$a_1 \equiv b_1(mod\ m)$

$a_2 \equiv b_2(mod\ m)$

...

$a_n \equiv b_n(mod\ m)$

都成立时，我们有

$a_1+a_2+\ldots+a_n \equiv b_1+b_2+\ldots+b_n(mod\ m)$

如：

$5 \equiv 8(mod\ 3)$

$11 \equiv 14(mod\ 3)$

$17 \equiv 23(mod\ 3)$

那么$5+11+17 \equiv 8+14+23(mod\ 3)$

5874192能否被9整除？

$5874192 = 5 \times 10^6 + 8 \times 10^5 + 7 \times 10^4 + 4 \times 10^3 + 10^2 + 9 \times 10 + 2$

我们知道$10 \equiv 1(mod\ 9)$

由引理4，我们知道$10^n \equiv 1^n(mod\ 9)$，即$10^n \equiv 1(mod\ 9)$

由引理3，我们知道$5 \times 10^6 = 5(mod 9)$、$8 \times 10^5 = 8(mod 9)$、$7 \times 10^4 = 7(mod 9)$、$4 \times 10^3 = 4(mod 9)$、$10^2 = 1(mod 9)$、$9 \times 10 = 9(mod 9)$

由引理5，我们知道
$5 \times 10^6 + 8 \times 10^5 + 7 \times 10^4 + 4 \times 10^3 + 10^2 + 9 \times 10 + 2 \equiv 5 + 8 + 7 + 4 + 1 + 9 + 2(mod\ 9)$

即$5874192 \equiv 5 + 8 + 7 + 4 + 1 + 9 + 2(mod\ 9)$

由于$5 + 8 + 7 + 4 + 1 + 9 + 2 = 36$，能被9整除，所以5874192能被9整除

性质

- 和的余数等于余数的和

  即对于正整数a，b和n，按照模运算的定义，我们可以表示：

  $a \equiv r_a(mod\ n)$，其中r_a是a除以n的余数，即：

  $a = q_a \times n + r_a$，其中q_a是商，$0 \le r_a < n$。

  类似地，对于另一个整数b，我们有：

  $b \equiv r_b(mod\ n)$，即$b = q_b \times n + r_b$

  $a + b = (q_a \times n + r_a) + (q_b \times n + r_b) = (q_a + q_b) \times n + (r_a + r_b)$

  因此，$a + b$除n后的余数，应该是$r_a + r_b$除n后的余数，即：

  $(a + b) mod\ n = (r_a + r_b) mod\ n$

- 积的余数等于余数的积

  假设有一个正整数 n，然后考虑两个整数 a 和 b。按照模运算的定义，我们可以表示：

  $a \equiv r_a(mod\ n)$，其中r_a是a除以n的余数，即：

  $a = q_a \times n + r_a$

  同理，对于整数 b，我们有：

  $b \equiv r_b(mod\ n)$，即$b = q_b \times n + r_b$

  $a \times b = (q_a \times n + r_a) \times (q_b \times n + r_b)$

  展开后得到：

  $a \times b = q_a \times q_b \times n^2 + q_a \times r_b \times n + q_b \times r_a \times n + r_a \times r_b$

  从中可以看出，前面几项都包含 n 的倍数，所以这些项在模 n 时余数为 0。因此，以上表达式模 n 的结果主要由最后一项$r_a \times r_b$决定：

  $(a \times b)\ mod\ n = r_a \times r_b\ mod\ n$