# 整除性与约数

如果存在某个整数k，a=kd，那么满足我们就说d|a（读作d整除a），如果d|a，那么-d|a，d|-a。如果a>0且d|a,则称a是d的倍数。如果d>0则称d是a的约数约数。

任何正整数a均可被平凡1和自身a整除，整数a的非平凡约数（即非1非a的可以被a整除的数）均称为a的约数。

# 素数与合数

- 如果一个整数a>1且只能被平凡约数1和他自身整除，则这个数是素数。如果一个整数a>1且不是素数，则称为合数，1既不是素数也不是合数。同样，整数0和所有负整数也既不是素数也不是合数。

# 除法定理，余模和等模

- 除法定理
- 对于任何整数a和任何正整数n，存在唯一的整数q和r，满足0<=r<n且a = qn+r,称q=a/n为除法的商，值r=a%n为除法的余数。
- 根据整数摸n的余数，我们可以将整数集合划分成n个等价类。整数a的模n等价类为[a]n = {a+kn:k属于z}。例如，[3]7 = {...-11. -4, 3, 10...}

$$-1 \equiv n-1 \pmod{n}$$

很多算法利用了等模的思想，例如hash

# 公约数

- 如果d是a的约数并且d也是b的约数，则称d是a与b的公约数
- 一条重要定理:

d|a且d|b蕴含着d|(a+b)且d|(a-b)

证明：a = kd，　b = id，　a+b = (k+i)d, a-b = (k-i)d,显然满足d|(k+i)d,d|(k-i)d。

由上面证明可推论出对任意整数x和y

d|a并且d|b蕴含d|(ax+by) (做x-1，和y-1步上面证明即可)

如果a|b那么|a|<= |b|或b=0(即b为a的整数倍)

a|b且b|a蕴含着a = ±b

# 最大公约数与模线性方程的关系

- 两个不同时为零的整数a和b的公约数中最大的称其为最大公约数，记做gcd(a,b)。
- gcd函数的一些基本性质

gcd(a,b) = gcd(b,a)= gcd(-a,b)=gcd(|a|, |b|)

gcd(a, 0) = |a|

gcd(a,ka) = |a|

定理：如果任意整数a和b都不为0，则gcd(a,b)是线性组合集{ax+by：x，y∈Z}中的最小正元素。