数论基础知识

主讲人：邓哲也

整除性和约数

- 整除是数论中的一个中心概念。
- 记号 d | a 意味着对某个整数 k，有 a = kd。
- 0 可被任何整数整除。
- 如果 d | a 我们称 a 是 d 的倍数，d 是 a 的约数。
- 一个整数 a 的约数最小为 1， 最大为 |a|。
- 例如：12 的约数有 1，2，3，4，6，12.

素数和合数

对于某个整数 $a > 1$，如果它仅有平凡约数 1 和 a，则称 a 为素数（或质数）

前 10 个素数：2，3，5，11，13，17，19，23，29，31

不是素数的整数 $a > 1$ 称为合数。

例如，因为 $2 \mid 10$，所以 10 是合数。

整数 1 既不是素数也不是合数。

除法定理

对任意整数 a 和任意正整数 n， 存在唯一的整数 q 和 r，

满足 0 <= r < n，并且 a = qn + r.

值 q = [a / n] 称为除法的商

值 r = a mod n 称为除法的余数。

n | a 当且仅当 a mod n = 0。

模 n 等价类

包含整数 a 的模 n 等价类为：$[a]_n = \{a + kn : k \epsilon Z\}$

例如，$[3]_7 = \{\ldots, -11, -4, 3, 10, 17, \ldots\}$

$b \epsilon [a]_n$ 等同于b = a (mod n)

-1 = n - 1 (mod n)

公约数与最大公约数

如果 d 是 a 的约数并且也是 b 的约数，则 d 是 a 与 b 的公约数。
例如，12 的约数是 1，2，3，4，6，12，因此 8 与 12 的公约数为 1，2，4。
1 是任意两个整数的公约数。
公约数的重要性质为：
d | a 且 d | b 蕴含着 d | (a + b) 且 d | (a - b)
更一般的，对任意整数 x 和 y，有
d | a 且 d | b 蕴含着 d | (ax + by)

公约数与最大公约数

两个不同时为 0 的整数 a 与 b 的最大公约数表示成 gcd(a, b)。

例如 gcd(12, 8) = 4，gcd(5, 9) = 1, gcd(0, 4) = 4.

定义 gcd(0, 0) = 0

gcd 函数的基本性质：

- gcd(a, b) = gcd(b, a)
- gcd(a, b) = gcd(-a, b)
- gcd(a, b) = gcd(|a|, |b|)
- gcd(a, 0) = |a|
- gcd(a, ka) = |a|

gcd 的其他性质

如果 a 和 b 是不都为 0 的任意整数，则 gcd(a, b) 是 a 与 b 的线性组合集合 {ax + by: x, y ∈ Z} 中的最小正元素。

gcd 的其他性质

证明：设s是a与b的线性组合集中的最小正元素，并且对某个 $x, y \in z$, 有$s = ax + by$.设$q = \{a / s\}$。则式（3.8）说明a mod s=a-qs=a-q(ax+by)=a(1-qx)+b(-qy)。因此，a mod s也是a与b的一种线性组合。但由于a mod s<s，所以有a mod s=0,因为s是满足这样的线性组合的最小整数。因此有 $s|a$ ，并且类似可推得 $s|b$ 。因此，s是a与b的公约数，所以 $\gcd(a, b) \geq s$。因为 $\gcd(a, b)$能同时被a与b整除，并且s是a与b的一个线性组合，所以可知 $\gcd(a, b)|s$ 但由 $\gcd(a, b)|s$ 和s>0,可知$\gcd(a, b) \leq s$ 。将上面已证明的 $\gcd(a, b) \geq s$ 与 $\gcd(a, b) \leq s$ 结合起来，得到$\gcd(a, b)$ =s，因此证得s是a与b的最大公约数。

gcd 的其他性质

- 对于任意整数 a 和 b，如果 d | a 并且 d | b，则 d | gcd(a, b)

- 对所有正整数 n，a 和 b，如果 n | ab 且 gcd(a, n)=1，则 n | b

互质数

如果两个整数 a 和 b 仅有公因数 1，即如果 gcd(a, b) = 1，则 a 与 b 称为互质数。

例如，5 和 9 是互质数。

对任意整数 p，a 和 b，如果 gcd(a, p) = gcd(b, p) = 1，则 gcd(ab, p) = 1

互质数

证明：由定理31.2可知，存在整数x, y, x′ ， y′， 满足

ax+py=1,

bx′+py′=1

把上面两个等式两边相乘，整理得

ab(x x′)+p(ybx′+y′ax+pyy′)=1

因为1是ab与p的一个正线性组合，所以运用定理3就可以证明所需结论。

唯一的因子分解

对所有素数 p 和所有整数 a，b，如果 p | ab，则 p | a 或 p | b.

唯一质因子分解定理：合数 a 仅能以一种方式，写成如下的乘积形式：

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

其中 p_i 为素数，$p_1 < p_2 < \cdots < p_r$，且 e_i 为正整数。

例如 6000 可以唯一分解为 2^4 * 3 * 5^3.

下节课再见