

数论概论学习小结 by Igwza

第5章 整除性与最大公因数

定理 5.1 (欧几里得算法)

要计算两个整数 a 与 b 的最大公因数，先令 $r_{-1}=a$ 且 $r_0=b$ 然后计算相继的商和余数 $r_{i-1}=q_{i+1} \cdot r_i + r_{i+1}$ ($i = 0, 1, 2, \dots$) 直到某余数 r_{n+1} 为 0。最后的非零余数 r_n 就是 a 与 b 的最大公因数。

第6章 线性方程与最大公因数

定理 6.1 (线性方程定理)

设 a 与 b 是非零整数 $g = \gcd(a, b)$ 。方程 $ax + by = g$ 总是有一个整数解 (x_1, y_1) 它可由前面叙述的欧几里得算法得到。则方程的每一个解可由 $(x_1 + k \cdot \frac{b}{g}, y_1 - k \cdot \frac{a}{g})$ 得到，其中 k 可为任意整数。

第7章 因数分解与算术基本定理

断言 7.1

令 p 是素数，假设 p 整除乘积 ab ，则 p 整除 a 或 p 整除 b (或者 p 既整除 a 也整除 b)

定理 7.2 (素数整除性质)

假设素数 p 整除乘积 $a_1 a_2 \dots a_r$ ，则 p 整除 a_1, a_2, \dots, a_r 中至少一个因数

定理 7.3 (算术基本定理)

每个整数 $n \geq 2$ 可唯一分解成素数乘积 $n = p_1 p_2 \dots p_r$

第8章 同余式

如果 m 整除 $a-b$ ，我们就说 a 与 b 模 m 同余并记之为 $a \equiv b \pmod{m}$ 数 m 叫做同余式的模。具有相同模的同余式在许多方面表现得很像通常的等式。如果 $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$ 则 $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$, $a_1 a_2 \equiv b_1 b_2 \pmod{m}$ 提醒：用数除同余式并非总是可能的。换句话说，如果 $a \equiv b \pmod{m}$

$a \not\equiv b \pmod{m}$, 则 $a \equiv b \pmod{m}$ 未必成立. 然而, 如果 $\gcd(c, m) = 1$, 则可从同余式 $ac \equiv bc \pmod{m}$ 两边消去 c .

定理 8.1 (线性同余式定理)

设 a , c 与 m 是整数, $m \geq 1$, 且设 $g = \gcd(a, m)$. (a) 如果 $g \nmid c$, 则同余式 $ax \equiv c \pmod{m}$ 没有解 (b) 如果 $g \mid c$, 则同余式 $ax \equiv c \pmod{m}$ 恰好有 g 个不同的解. 要求这些解, 首先求线性方程 $au + mv = g$ 的一个解 (u_0, v_0) (第6章叙述了解这个方程的方法). 则 $x_0 = cu_0/g$ 是 $ax \equiv c \pmod{m}$ 的解, 不同余解的完全集由 $x \equiv x_0 + k \cdot \frac{m}{g}$, $k = 0, 1, 2, \dots, g-1$ 给出.

From: https://wiki.cvbbacm.com/ - CVBB ACM Team

Permanent link: https://wiki.cvbbacm.com/doku.php?id=2020-2021:teams:legal_string:%E6%95%B0%E8%AE%BA%E6%A6%82%E8%AE%BA%E5%AD%A6%E4%B9%A0%E5%B0%8F%E7%BB%93_lgwza&rev=1593785529
Last update: 2020/07/03 22:12

