整数的整除性

Division in the Integers

刘铎

liuduo@bjtu.edu.cn

整数的整除性

- 定理

（**带余除法**）设 n 和 m 都是整数且$n\neq0$，则可以唯一地将 m 写为 $m = q\cdot n + r$，其中 q 和 r 是整数，且 $0 \le r < |n|$。q 称作**商（quotient）**，r 称作**余数（remainder）**，记作 $r = m \bmod n$。

整数的整除性

- 例：
  - $-29 = (-6)\cdot 5+1$
  - $143 = 11\cdot 13+0$
  - $915 = 11\cdot 78+57$

整数的整除性

- 若余数 $r=0$，则称 m **能被** n **整除**（m **is dividable by** n），或 n **整除** m（n **divides** m），记作 $n|m$。
- 此时，称 m 是 n 的一个**倍数(multiple)**，称 n 是 m 的一个**约数**或**因子（divisor）**。
- 若 $n|m$，则存在整数 q 使得 $m=q\cdot n$，且有 $n\leq|m|$。

整数的整除性

- 例
  - $3|12$
  - $3|(-15)$
  - 12 的所有因子是 $\{\pm1, \pm2, \pm3, \pm6, \pm12\}$

整数的整除性

- 定理

  假设 a, b, c 是整数，$a \neq 0$，则

  (a) 若 $a|b$ 且 $a|c$，则对于任意的整数 x, y，有 $a|(xb+yc)$；

  (b) 若 $b \neq 0$，$a|b$ 且 $b|c$，则 $a|c$；

  (c) 若 $b \neq 0$，$a|b$ 且 $b|a$，则 $a = \pm b$。

整数的整除性

- 证明

若 $a|b$ 且 $a|c$，则对于任意的整数 x, y，有 $a|(xb+yc)$

  - 若 $a|b$ 且 $a|c$，则存在整数 k_1 及 k_2 使得 $b = k_1a$ 及 $c = k_2a$
  - 于是 $xb+yc = xk_1a+yk_2a = (xk_1+yk_2)a$
  - 即 $a|(xb+yc)$

整数的整除性

- 定理

  对于任意正整数 a，有 $a|a$ 及 $1|a$。

整数的整除性

- 若大于 **1** 的整数 ***p*** 的所有正因子只有 ***p*** 和 **1**，则称其为**质数**或**素数**（**prime**）；否则称其为**合数**（**composite number**）。
- 例
  - 2, 3, 5, 7, 11, 13, 17, 19都是素数
  - 而4, 6, 8, 9, 10, 12, 15, 16, 18都是合数

整数的整除性

- 定理

  有无穷多个素数。

- 证明.（反证法）
  - 假设只有有穷多个素数，设为$p_1,p_2,\ldots,p_n$
  - 令 $m=p_1p_2\ldots p_n+1$，显然有 $p_i \nmid m$，$1 \le i \le n$
  - 因此要么 m 本身是素数，要么存在大于 p_n 的素数整除 m，与假设产生矛盾。

整数的整除性

- 定 理 （**算 术 基 本 定 理 ， arithmetic fundamental theorem**）

  设正整数 $n>1$，则 n 可唯一地表示为，

$$p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$$

其中 $p_1<p_2<,\ldots,<p_s$ 是 s 个相异的素数，指数 k_i 都是正整数。此定理又称作**唯一析因定理**（**unique factorization theorem**）。该表达式称作整数 n 的**素因子分解**。

- 例
  - $12=2^2\cdot3^1$, $15=3^1\cdot5^1$

整数的整除性

- 设 a 和 b 是两个不全为 0 的整数，若整数 d 满足 $d|a$ 且 $d|b$，则称 d 是 a, b 的**公因子（common divisor）**
- 所有公因子中最大的称作 a 与 b 的**最大公因子（greatest common divisor）**，记作 **GCD(a, b)**
- 若整数 a 和 b 的最大公因子为1，则称 a 与 b **互素（relatively prime）**

整数的整除性

- 设 a 和 b 是两个不全为 0 的整数，若整数 m 满足 $a|m$ 且 $b|m$，则称 m 是 a, b 的**公倍数（common multiple）**
- 所有公倍数中最小的正整数称作a与b的**最小公倍数（least common multiple）**，记作 **LCM(a, b)**

整数的整除性

- 对任意的正整数 a 有
  - GCD(0, a)=a
  - GCD(1, a)=1
  - LCM(1, a)=a
- 例
  - GCD(12, 15)=3
  - LCM(12, 15)=60
  - 8和15互素
  - 12和15不互素
  - 6、11、35两两互素

整数的整除性

- 若 $a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ 且 $b = p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}$

  则 $\mathbf{GCD}(a,b) = p_1^{\min(k_1,l_1)} p_2^{\min(k_2,l_2)} \cdots p_s^{\min(k_s,l_s)}$

- 例
  - $12=2^2 \cdot 3=2^2 \cdot 3^1 \cdot 5^0$
  - $15=3 \cdot 5=2^0 \cdot 3^1 \cdot 5^1$
  - $GCD(12,15)=3=2^0 \cdot 3^1 \cdot 5^0$

整数的整除性

- 若 $a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ 且 $b = p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}$

  则 $\mathbf{LCM}(a,b) = p_1^{\max(k_1,l_1)} p_2^{\max(k_2,l_2)} \cdots p_s^{\max(k_s,l_s)}$

- 例
  - $12=2^2 \cdot 3^1 \cdot 5^0$, $15=2^0 \cdot 3^1 \cdot 5^1$
  - $\mathrm{LCM}(12,15)=60=2^2 \cdot 3^1 \cdot 5^1$
  - $\mathrm{GCD}(a, b) \cdot \mathrm{LCM}(a, b)=a \cdot b$

整数的整除性

- 推论

  设a, b是正整数，则

  $\mathbf{GCD}(a, b)\cdot\mathbf{LCM}(a, b) = a\cdot b$。

整数的不同进位制表示

- $6798=6\cdot10^3+7\cdot10^2+9\cdot10^1+8\cdot10^0$
- b - 进制表示
  - $b=16$
  - $1A8E=1\cdot16^3+10\cdot16^2+8\cdot16^1+14\cdot16^0$

End