Discrete Mathematics

XU Ming (徐 鸣)

Department of Computer Science, East China Normal University

June 10, 2016

Chapter 2 NUMBER THEORY

Outline of §-1 GCDs and LCMs

整除

Definition (整除)

设 $a, b \neq 0$ 为整数.
b 整除 a: 存在整数 q, 使得 $a = b \cdot q$, 记为 $b \mid a$; 否则 $b \nmid a$.
b 是 a 的因数 (约数, 因子, factor), a 是 b 的倍数: $b \mid a$;
b 是 a 的真因数 (proper factor): $b \mid a$ 并且 $|a| > |b|$.

注意零除的问题:

- 任何数不能除以 0;
- 任何整数都是 0 的因数, 但 0 不是任何整数的因数;
- 0 是任何整数的倍数, 但 0 没有倍数.

整除

Definition (整除)

设 $a, b \neq 0$ 为整数.
b 整除 a: 存在整数 q, 使得 $a = b \cdot q$, 记为 $b \mid a$; 否则 $b \nmid a$.
b 是 a 的因数 (约数, 因子, factor), a 是 b 的倍数: $b \mid a$;
b 是 a 的真因数 (proper factor): $b \mid a$ 并且 $|a| > |b|$.

注意零除的问题:

- 任何数不能除以 0;
- 任何整数都是 0 的因数, 但 0 不是任何整数的因数;
- 0 是任何整数的倍数, 但 0 没有倍数.

同余

Definition (同余和同余式)

设 a, b 为整数, m 为非零整数.
a 和 b 模 m 同余 (congruent): $m \mid (a - b)$, 记为同余式 $a \equiv b \mod m$.

显然, 我们有 $a \equiv b \mod m$ 当且仅当 $a \mod m = b \mod m$.

同余

Definition (同余和同余式)

设 a, b 为整数, m 为非零整数.
a 和 b 模 m 同余 (congruent): $m \mid (a - b)$, 记为同余式 $a \equiv b \mod m$.

显然, 我们有 $a \equiv b \mod m$ 当且仅当 $a \mod m = b \mod m$.

同余

Example

$$10 \equiv 4 \mod 3,$$
$$24 \equiv 0 \mod 8.$$

Remark

注意 $\equiv$ 和 $=$ 的区别:
因为 $4 \mod 3 = 7 \mod 3 = 1$, 所以 $7 \equiv 4 \mod 3$.
但 $4 \neq 7$.

同余

Example

$$10 \equiv 4 \mod 3,$$
$$24 \equiv 0 \mod 8.$$

Remark

注意 $\equiv$ 和 $=$ 的区别:
因为 $4 \mod 3 = 7 \mod 3 = 1$, 所以 $7 \equiv 4 \mod 3$.
但 $4 \neq 7$.

同余

Theorem (同余关系是等价关系)

1. 自反性: $a \equiv a \mod m$.
2. 对称性: $a \equiv b \mod m \Leftrightarrow b \equiv a \mod m$.
3. 传递性: $a \equiv b \mod m, b \equiv c \mod m \Rightarrow a \equiv c \mod m$.

同余

Theorem (模算术运算的性质)

1. 若 $a \equiv b \mod m$, $c \equiv d \mod m$, 则 $a \pm c \equiv b \pm d \mod m$.
2. 若 $a \equiv b \mod m$, $c \equiv d \mod m$, 则 $a \cdot c \equiv b \cdot d \mod m$.
3. 若 $a \cdot c \equiv b \cdot c \mod m$, 则 $a \equiv b \mod \frac{m}{(c,m)}$;
   特别地, 当 $(c, m) = 1$ 时, 有 $a \equiv b \mod m$.
   (其中 (c, m) 表示 c 和 m 的最大公因数.)

同余

同余式与通常的等式具有许多相似的性质

Theorem (按模运算)

1. $(x \pm y) \mod m = \big((x \mod m) \pm (y \mod m)\big) \mod m.$
2. $(x \times y) \mod m = \big((x \mod m) \times (y \mod m)\big) \mod m.$

Example

计算 $2^{340} \mod 31$, $3^5 \mod 7$, 和 $2^{340} \mod 11$.

1. $2^{340} = (2^5)^{68}$,
   $2^{340} \mod 31 = (32 \mod 31)^{68} \mod 31 = 1^{68} \mod 31 = 1.$
2. $3^5 = 3 \times 9^2$,
   $3^5 \mod 7 = \big(3 \times (9 \mod 7)^2\big) \mod 7 = (3 \times 4) \mod 7 = 5.$
3. $2^{340} \mod 11 = (2^{10} \mod 11)^{34} \mod 11 = 1^{34} \mod 11 = 1.$

同余

同余式与通常的等式具有许多相似的性质

Theorem (按模运算)

1. $(x \pm y) \mod m = \big((x \mod m) \pm (y \mod m)\big) \mod m.$
2. $(x \times y) \mod m = \big((x \mod m) \times (y \mod m)\big) \mod m.$

Example

计算 $2^{340} \mod 31$, $3^5 \mod 7$, 和 $2^{340} \mod 11$.

1. $2^{340} = (2^5)^{68}$,
   $2^{340} \mod 31 = (32 \mod 31)^{68} \mod 31 = 1^{68} \mod 31 = 1.$
2. $3^5 = 3 \times 9^2$,
   $3^5 \mod 7 = \big(3 \times (9 \mod 7)^2\big) \mod 7 = (3 \times 4) \mod 7 = 5.$
3. $2^{340} \mod 11 = (2^{10} \mod 11)^{34} \mod 11 = 1^{34} \mod 11 = 1.$

最大公因数

Definition (公因数, 最大公因数)

设整数 $a_1, a_2, \ldots, a_n$ $(n \geq 2)$ 不全为零,

- 公因数: 各个数的公共因数;
- 最大公因数 (greatest common divisor, GCD): 最大的公因数, 记为 $(a_1, a_2, \ldots, a_n)$ 或 $\gcd(a_1, a_2, \ldots, a_n)$;
- $a_1, a_2, \ldots, a_n$ 互素(互质) (co-prime): $(a_1, a_2, \ldots, a_n) = 1$.

Remark

最大公因数一定是正整数, 因为若 d 是公因数, 则 $-d$ 也是公因数.

Example

$(24, -28) = 4$, $(24, -28, 0) = 4$, $(0, 0) = ?$.

最大公因数

Definition (公因数, 最大公因数)

设整数 $a_1, a_2, \ldots, a_n$ $(n \geq 2)$ 不全为零,

- 公因数: 各个数的公共因数;
- 最大公因数 (greatest common divisor, GCD): 最大的公因数, 记为 $(a_1, a_2, \ldots, a_n)$ 或 $\gcd(a_1, a_2, \ldots, a_n)$;
- $a_1, a_2, \ldots, a_n$ 互素(互质) (co-prime): $(a_1, a_2, \ldots, a_n) = 1$.

Remark

最大公因数一定是正整数, 因为若 d 是公因数, 则 $-d$ 也是公因数.

Example

$(24, -28) = 4$, $(24, -28, 0) = 4$, $(0, 0) =$?.

最小公倍数

Definition (公倍数, 最小公倍数)

设整数 $a_1, a_2, \ldots, a_n$ $(n \geq 2)$ 不全为零,

- 公倍数: 各个数的公共倍数;
- 最小公倍数 (least common multipler, LCM): 最小的正公倍数, 记为 $[a_1, a_2, \ldots, a_n]$ 或 $\operatorname{lcm}(a_1, a_2, \ldots, a_n)$.

Remark

从定义中, 我们已限定了最小公倍数是正整数.

Example

$[24, -28] = 4 \cdot 6 \cdot 7$, $(24, -28, 0) = ?$, $(0, 0) = ?$.

最小公倍数

Definition (公倍数, 最小公倍数)

设整数 $a_1, a_2, \ldots, a_n$ $(n \geq 2)$ 不全为零,

- 公倍数: 各个数的公共倍数;
- 最小公倍数 (least common multipler, LCM): 最小的正公倍数, 记为 $[a_1, a_2, \ldots, a_n]$ 或 $\operatorname{lcm}(a_1, a_2, \ldots, a_n)$.

Remark

从定义中, 我们已限定了最小公倍数是正整数.

Example

$[24, -28] = 4 \cdot 6 \cdot 7$, $(24, -28, 0) = ?$, $(0, 0) = ?$.

最大与最小

任何公因数都是最大公因数的因数,

任何公倍数都是最小公倍数的倍数.

TIPS: 这两条性质可分别用来定义最大公因数和最小公倍数.

PROBLEM: 如何求最大公因数?—欧几里得算法.

最大与最小

任何公因数都是最大公因数的因数,

任何公倍数都是最小公倍数的倍数.

TIPS: 这两条性质可分别用来定义最大公因数和最小公倍数.

PROBLEM: 如何求最大公因数?—欧几里得算法.

带余除法

Theorem (带余除法)

设 $a, b \neq 0$ 为整数.
存在整数 q 和 r, 使得

$$a = b \cdot q + r \quad (0 \leq r < b);$$

并且 q 和 r 由 a 和 b 唯一决定.

一些术语:
在上式中, 若 $r = 0$, 则称 q 是 a 被 b 除的完全商 (quotient);
否则 ($r \neq 0$), q 是不完全商 (partial quotient), r 是余数 (remainder).

QUIZ: 证明 b 整除 a 当且仅当 a 被 b 除的余数为零.

带余除法

Theorem (带余除法)

设 $a, b \neq 0$ 为整数.
存在整数 q 和 r, 使得

$$a = b \cdot q + r \quad (0 \leq r < b);$$

并且 q 和 r 由 a 和 b 唯一决定.

一些术语:
在上式中, 若 $r = 0$, 则称 q 是 a 被 b 除的完全商 (quotient);
否则 ($r \neq 0$), q 是不完全商 (partial quotient), r 是余数 (remainder).

QUIZ: 证明 b 整除 a 当且仅当 a 被 b 除的余数为零.

带余除法

Theorem (带余除法)

设 $a, b \neq 0$ 为整数.
存在整数 q 和 r, 使得

$$a = b \cdot q + r \quad (0 \leq r < b);$$

并且 q 和 r 由 a 和 b 唯一决定.

一些术语:
在上式中, 若 $r = 0$, 则称 q 是 a 被 b 除的完全商 (quotient);
否则 ($r \neq 0$), q 是不完全商 (partial quotient), r 是余数 (remainder).

QUIZ: 证明 b 整除 a 当且仅当 a 被 b 除的余数为零.

带余除法

Example

1. $\frac{255}{15} = 17$, 即 $255 = 15 \times 17 + 0$.
   所以, $15 \mid 255$, 255 被 15 除的完全商是 17, 余数是 0.
2. $\frac{418}{15} = 27.8666\cdots$, 即 $418 = 15 \times 27 + 13$.
   所以, $15 \nmid 418$, 418 被 15 除的不完全商是 27, 余数是 13.
3. $\frac{-81}{15} = -5.4$, 即 $-81 = 15 \times (-6) + 9$.
   所以, $15 \nmid -81$, -81 被15除的不完全商是-6, 余数是 9.

欧几里德算法

欧几里德算法的依据:
设 $a, b \in \mathbb{Z}$ 不全为零, 则有 $a = b \cdot q + c \Rightarrow (a, b) = (b, c)$.

Algorithm 1 Euclidean Algorithm

Require: $a, b \in \mathbb{Z}$ satisfying $a \geq b \geq 0$.
Ensure: (a, b).

```
while b > 0 do
    c ← a mod b.
    a ← b and b ← c.
end while
return a.
```

The algorithm is terminating, because in each loop b is **ranking** by at least 1 and the **invariant** $b \geq 0$ should be preserved.

欧几里德算法

欧几里德算法的依据:
设 $a, b \in \mathbb{Z}$ 不全为零, 则有 $a = b \cdot q + c \Rightarrow (a, b) = (b, c)$.

Algorithm 2 Euclidean Algorithm

Require: $a, b \in \mathbb{Z}$ satisfying $a \geq b \geq 0$.
Ensure: (a, b).

```
while b > 0 do
    c ← a mod b.
    a ← b and b ← c.
end while
return a.
```

The algorithm is terminating, because in each loop b is **ranking** by at least 1 and the **invariant** $b \geq 0$ should be preserved.

欧几里德算法

欧几里德算法

反复进行带余除法, 直到某次余数为 0.

$$
\begin{aligned}
b\text{除}a &: a = b \cdot q_0 + r_0, \quad 0 < r_0 < |b| \\
r_0\text{除}a &: b = r_0 \cdot q_1 + r_1, \quad 0 < r_1 < r_0 \\
r_1\text{除}r_0 &: r_0 = r_1 \cdot q_2 + r_2, \quad 0 < r_2 < r_1 \\
&\cdots \\
r_{n-1}\text{除}r_{n-2} &: r_{n-2} = r_{n-1} \cdot q_n + r_n, \quad 0 < r_n < r_{n-1} \\
r_n\text{除}r_{n-1} &: r_{n-1} = r_n \cdot q_{n+1}
\end{aligned}
$$

$$
(a, b) = (b, r_0) = (r_0, r_1) = \ldots = (r_{n-1}, r_n) = r_n, \quad (r_0 > r_1 \cdots > r_n > 0).
$$

欧几里德算法

Example

求 435 和 377 的最大公因数, 并表示为 435 和 377 的线性组合

(1) 进行辗转相除法

$$\begin{aligned} 433 &= 1 \cdot 377 + 58 \\ 377 &= 6 \cdot 58 + 29 \\ 58 &= 2 \cdot 29 + 0 \end{aligned}$$

$$\begin{aligned} (435, 377) &= (377, 58) \\ &= (58, 29) \\ &= 29 \end{aligned}$$

(2) 把辗转相除的过程倒推回去

$$\begin{aligned} 29 &= 377 - 6 \cdot 58 \\ &= 377 - 6 \cdot (435 - 1 \cdot 377) \\ &= 7 \cdot 377 - 6 \cdot 435 \end{aligned}$$

欧几里德算法

Example

求 435 和 377 的最大公因数, 并表示为 435 和 377 的线性组合

(1) 进行辗转相除法

$$
\begin{aligned}
433 &= 1 \cdot 377 + 58 \\
377 &= 6 \cdot 58 + 29 \\
58 &= 2 \cdot 29 + 0 \\
(435, 377) &= (377, 58) \\
&= (58, 29) \\
&= 29
\end{aligned}
$$

(2) 把辗转相除的过程倒推回去

$$
\begin{aligned}
29 &= 377 - 6 \cdot 58 \\
&= 377 - 6 \cdot (435 - 1 \cdot 377) \\
&= 7 \cdot 377 - 6 \cdot 435
\end{aligned}
$$

欧几里德算法

Example

求 435 和 377 的最大公因数, 并表示为 435 和 377 的线性组合

(1) 进行辗转相除法

$$
\begin{aligned}
433 &= 1 \cdot 377 + 58 \\
377 &= 6 \cdot 58 + 29 \\
58 &= 2 \cdot 29 + 0 \\
(435, 377) &= (377, 58) \\
&= (58, 29) \\
&= 29
\end{aligned}
$$

(2) 把辗转相除的过程倒推回去

$$
\begin{aligned}
29 &= 377 - 6 \cdot 58 \\
&= 377 - 6 \cdot (435 - 1 \cdot 377) \\
&= 7 \cdot 377 - 6 \cdot 435
\end{aligned}
$$

扩展的欧几里德算法

扩展的欧几里德算法

$a, b \in \mathbb{Z}$, 不全为零, 在欧几里德算法完成后, 可以通过回代求出整数 s, 和 t, 使得

$$(a, b) = s \cdot a + t \cdot b.$$

Example

$a, b, c \in \mathbb{Z}$, $c \mid a \cdot b$, $(c, a) = 1$, 证明: $c \mid b$.

扩展的欧几里德算法

扩展的欧几里德算法

$a, b \in \mathbb{Z}$, 不全为零, 在欧几里德算法完成后, 可以通过回代求出整数 s, 和 t, 使得

$$(a, b) = s \cdot a + t \cdot b.$$

Example

$a, b, c \in \mathbb{Z}$, $c \mid a \cdot b$, $(c, a) = 1$, 证明: $c \mid b$.

最大公因数的基本性质

设整数 $a_1, a_2, \ldots, a_n\ (n \geq 2)$ 不全为零,

1. $a_i \neq 0 \Rightarrow (0, a_i) = a_i$.
2. $(a_1, a_2, \ldots, a_n) = (|a_1|, |a_2|, \ldots, |a_n|)$.
3. 任意变换各整数的位置, $(a_1, a_2, \ldots, a_n)$ 的值保持不变.
4. $a_1, a_2, \ldots, a_n$ 的公因数是 $(a_1, a_2, \ldots, a_n)$ 的因数.
5. $(a_1, a_2, \ldots, a_n) = ((a_1, a_2), \ldots, a_n)$.
6. 对于任意的 $m \in \mathbb{N}$, $(m \cdot a_1, m \cdot a_2, \ldots, m \cdot a_n) = m \cdot (a_1, a_2, \ldots, a_n)$.
7. 对于任意的 $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, $(a_1, a_2, \ldots, a_n) = (a_1 + a_i \cdot x_1, a_2 + a_i \cdot x_2, \ldots, a_{i-1} + a_i \cdot x_{i-1}, a_i, a_{i+1} + a_i \cdot x_{i+1}, a_{i+2} + a_i \cdot x_{i+2}, \ldots, a_n + a_i \cdot x_n)$.
8. 存在 $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, 使得 $(a_1, a_2, \ldots, a_n) = a_1 \cdot x_1 + a_2 \cdot x_2 + \ldots + a_n \cdot x_n$.

素因数分解计算法

设正整数 $a_1, a_2, \ldots, a_n$ 有素因数分解:

$$\begin{aligned} a_1 &= p_1^{\alpha_{11}} \cdot p_2^{\alpha_{12}} \cdot \cdots \cdot p_k^{\alpha_{1k}} \\ a_2 &= p_1^{\alpha_{21}} \cdot p_2^{\alpha_{22}} \cdot \cdots \cdot p_k^{\alpha_{2k}} \\ &\cdots \\ a_n &= p_1^{\alpha_{n1}} \cdot p_2^{\alpha_{n2}} \cdot \cdots \cdot p_k^{\alpha_{nk}}, \end{aligned}$$

则有:

$$\begin{aligned} (a_1, a_2, \ldots, a_n) &= p_1^{\alpha_1} \cdot p_2^{\delta_2} \cdot \cdots \cdot p_k^{\delta_k} \\ [a_1, a_2, \ldots, a_n] &= p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \cdots \cdot p_k^{\gamma_k}, \end{aligned}$$

其中 $\delta_i = \min(\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni})$, $\gamma_i = \max(\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni})$.

最大公因数的基本性质

Example

非零整数 $a_1, a_2, \ldots, a_n$, $n \geq 2$,
证明: $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$.

Example

整数 $a_1, a_2, \ldots, a_n$, $(n \geq 2)$, 不全为零,
证明: $(a_1, a_2, \ldots, a_n) = d \Rightarrow (\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}) = 1$.

最大公因数的基本性质

Example

非零整数 $a_1, a_2, \ldots, a_n$, $n \geq 2$,
证明: $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$.

Example

整数 $a_1, a_2, \ldots, a_n$, $(n \geq 2)$, 不全为零,
证明: $(a_1, a_2, \ldots, a_n) = d \Rightarrow (\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}) = 1$.

最大公因数的基本性质

Example

$n \in \mathbb{N}$, 证明: $(n-1, n^2+n+4) \mid 6$.

Example

$0, 1, \ldots, 10$ 中的哪些数可表示为 $12m + 20n$ 的形式, 其中 m 和 n 是整数?

最大公因数的基本性质

Example

$n \in \mathbb{N}$, 证明: $(n-1, n^2+n+4) \mid 6$.

Example

$0, 1, \ldots, 10$ 中的哪些数可表示为 $12m + 20n$ 的形式, 其中 m 和 n 是整数?

最小公倍数的基本性质

设整数 $a_1, a_2, \ldots, a_n\ (n \geq 2)$ 不全为零,

1. $[a_1, a_2, \ldots, a_n] = [|a_1|, |a_2|, \ldots, |a_n|]$.
2. 任意变换各整数的位置, $[a_1, a_2, \ldots, a_n]$ 的值保持不变.
3. $a_1, a_2, \ldots, a_n$ 的公倍因数是 $[a_1, a_2, \ldots, a_n]$ 的倍数.
4. $[a_1, a_2, \ldots, a_n] = [[a_1, a_2], \ldots, a_n]$.
5. 对于任意的 $m \in \mathbb{N}$, $[m \cdot a_1, m \cdot a_2, \ldots, m \cdot a_n] = m \cdot [a_1, a_2, \ldots, a_n]$.
6. $(a_1, a_2) \cdot [a_1, a_2] = |a_1 \cdot a_2|$.
   (可否推广到 n 个数的情况?)

Hint: 可由最大公倍数的素因数分解计算法得到.

最小公倍数的基本性质

设整数 $a_1, a_2, \ldots, a_n\ (n \geq 2)$ 不全为零,

1. $[a_1, a_2, \ldots, a_n] = [|a_1|, |a_2|, \ldots, |a_n|]$.
2. 任意变换各整数的位置, $[a_1, a_2, \ldots, a_n]$ 的值保持不变.
3. $a_1, a_2, \ldots, a_n$ 的公倍因数是 $[a_1, a_2, \ldots, a_n]$ 的倍数.
4. $[a_1, a_2, \ldots, a_n] = [[a_1, a_2], \ldots, a_n]$.
5. 对于任意的 $m \in \mathbb{N}$, $[m \cdot a_1, m \cdot a_2, \ldots, m \cdot a_n] = m \cdot [a_1, a_2, \ldots, a_n]$.
6. $(a_1, a_2) \cdot [a_1, a_2] = |a_1 \cdot a_2|$.
   (可否推广到 n 个数的情况?)

Hint: 可由最大公倍数的素因数分解计算法得到.

Homework

1. PP. 32–33: Exercises *2,4,7,11.