离散数学

（第 3 版）

智能科学与技术学院 2024 级

目录

目录

4.1 素数

设 $a, b \in \mathbb{Z}, b \neq 0$. 若存在整数 c 使 $a = bc$, 则称 a 被 b 整除, 或 b 整除 a, 记作 $b \mid a$. 此时, 又称 a 为 b 的倍数, b 为 a 的因子. 将 b 不整除 a 记作 $b \nmid a$.

4.1 素数

设 $a, b \in \mathbb{Z}, b \neq 0$. 若存在整数 c 使 $a = bc$, 则称 a 被 b 整除, 或 b 整除 a, 记作 $b \mid a$. 此时, 又称 a 为 b 的倍数, b 为 a 的因子. 将 b 不整除 a 记作 $b \nmid a$.

由于正负因子成对出现, 通常只考虑正因子. 显然, 任何大于 1 的正整数都有两个正因子: 1 和它自身, 称作它的平凡因子. 除平凡因子之外的因子称作真因子.

4.1 素数

设 $a, b \in \mathbb{Z}, b \neq 0$. 若存在整数 c 使 $a = bc$, 则称 a 被 b 整除, 或 b 整除 a, 记作 $b \mid a$. 此时, 又称 a 为 b 的倍数, b 为 a 的因子. 将 b 不整除 a 记作 $b \nmid a$.

由于正负因子成对出现, 通常只考虑正因子. 显然, 任何大于 1 的正整数都有两个正因子: 1 和它自身, 称作它的平凡因子. 除平凡因子之外的因子称作真因子.

设 a, b 是两个整数, 且 $b \neq 0$, 则存在唯一的整数 q 和 r, 使得

$$a = qb + r, \text{ 其中} 0 \leqslant r < |b|,$$

这个式子称作带余除法. 记余数 $r = a \mod b$. 显然, $b \mid a \Leftrightarrow a \mod b = 0$.

4.1 素数

设 $a, b \in \mathbb{Z}, b \neq 0$. 若存在整数 c 使 $a = bc$, 则称 a 被 b 整除, 或 b 整除 a, 记作 $b \mid a$. 此时, 又称 a 为 b 的倍数, b 为 a 的因子. 将 b 不整除 a 记作 $b \nmid a$.

由于正负因子成对出现, 通常只考虑正因子. 显然, 任何大于 1 的正整数都有两个正因子: 1 和它自身, 称作它的平凡因子. 除平凡因子之外的因子称作真因子.

设 a, b 是两个整数, 且 $b \neq 0$, 则存在唯一的整数 q 和 r, 使得

$$a = qb + r, \text{ 其中} 0 \leqslant r < |b|,$$

这个式子称作带余除法. 记余数 $r = a \mod b$. 显然, $b \mid a \Leftrightarrow a \mod b = 0$.

命题 1.1.1

1. 若 $a \mid b$ 且 $a \mid c$, 则对任意的整数 m, n, 有 $a \mid mb + nc$.
2. 若 $a \mid b$ 且 $b \mid c$, 则 $a \mid c$.
3. 若 $m \neq 0$, 则 $a \mid b$ 当且仅当 $ma \mid mb$.
4. 若 $a \mid b$ 且 $b \mid a$, 则 $a = \pm b$.
5. 若 $a \mid b$ 且 $b \neq 0$, 则 $|a| \leqslant |b|$.

素数与合数

定义 1.1.1

设 a 是大于 1 的正整数，如果 a 的正因子只有 1 和 a，那么称 a 为素数或质数；否则，称 a 为合数.

素数与合数

定义 1.1.1

设 a 是大于 1 的正整数，如果 a 的正因子只有 1 和 a，那么称 a 为素数或质数；否则，称 a 为合数.

命题 1.1.2

1. 设 p 是素数且 $d \mid p$，若 $d > 1$，则 $d = p$.
2. 设 p 是素数且 $p \mid ab$，则必有 $p \mid a$ 或者 $p \mid b$.
3. 设 a 是大于 1 的整数，则 a 是合数当且仅当存在整数 b, c, 使得 $a = bc$，其中 $1 < b < a, 1 < c < a$.
4. 合数必有素数因子，即设 a 是一个合数，则存在素数 p，使得 $p \mid a$.

算术基本定理

对于命题 1.1.2(2)，更一般地，设 p 是一个素数且 $p \mid a_1 a_2 \cdots a_k$，则必存在 $1 \leqslant i \leqslant k$，使得 $p \mid a_i$. 需要注意的是，当 d 不是素数时，$d \mid ab$ 不一定能推导出 $d \mid a$ 或 $d \mid b$. 例如，$6 \mid 4 \times 9$，当 $6 \nmid 4$ 且 $6 \nmid 9$.

算术基本定理

对于命题 1.1.2(2)，更一般地，设 p 是一个素数且 $p \mid a_1 a_2 \cdots a_k$，则必存在 $1 \leqslant i \leqslant k$，使得 $p \mid a_i$. 需要注意的是，当 d 不是素数时，$d \mid ab$ 不一定能推导出 $d \mid a$ 或 $d \mid b$. 例如，$6 \mid 4 \times 9$，当 $6 \nmid 4$ 且 $6 \nmid 9$.

根据命题 1.1.2(4)，任何大于 1 的整数要么是素数，要么可以分解成素数的乘积. 这样的分解是唯一的，这就是下述算术基本定理，它表明素数是构成整数的“基本元素”.

算术基本定理

对于命题 1.1.2(2)，更一般地，设 p 是一个素数且 $p \mid a_1 a_2 \cdots a_k$，则必存在 $1 \leqslant i \leqslant k$，使得 $p \mid a_i$. 需要注意的是，当 d 不是素数时，$d \mid ab$ 不一定能推导出 $d \mid a$ 或 $d \mid b$. 例如，$6 \mid 4 \times 9$，当 $6 \nmid 4$ 且 $6 \nmid 9$.

根据命题 1.1.2(4)，任何大于 1 的整数要么是素数，要么可以分解成素数的乘积. 这样的分解是唯一的，这就是下述算术基本定理，它表明素数是构成整数的“基本元素”.

定理 1.1.1

设 $a > 1$，则 $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$，其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$r_1, r_2, \cdots, r_k$ 是正整数，并且在不计顺序的情况下，该表示是唯一的.

算术基本定理

对于命题 1.1.2(2)，更一般地，设 p 是一个素数且 $p \mid a_1 a_2 \cdots a_k$，则必存在 $1 \leqslant i \leqslant k$，使得 $p \mid a_i$. 需要注意的是，当 d 不是素数时，$d \mid ab$ 不一定能推导出 $d \mid a$ 或 $d \mid b$. 例如，$6 \mid 4 \times 9$，当 $6 \nmid 4$ 且 $6 \nmid 9$.

根据命题 1.1.2(4)，任何大于 1 的整数要么是素数，要么可以分解成素数的乘积. 这样的分解是唯一的，这就是下述算术基本定理，它表明素数是构成整数的“基本元素”.

定理 1.1.1

设 $a > 1$，则 $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$，其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$r_1, r_2, \cdots, r_k$ 是正整数，并且在不计顺序的情况下，该表示是唯一的.

定理中的表达式称作整数 a 的素因子分解. 下面是几个整数的素因子分解.

$$30 = 2 \times 3 \times 5, \quad 88 = 2^3 \times 11,$$
$$35\ 989 = 17 \times 29 \times 73,$$
$$99\ 099 = 3^2 \times 7 \times 11^2 \times 13, \quad 1\ 024 = 2^{10}.$$

推论 1.1.1

设 $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$，其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$r_1, r_2, \cdots, r_k$ 是正整数，则正整数 d 为 a 的因子的充分必要条件是 $d = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$，其中 $0 \leqslant s_i \leqslant r_i, i = 1, 2, \cdots, k.$

推论 1.1.1

设 $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$，其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$r_1, r_2, \cdots, r_k$ 是正整数，则正整数 d 为 a 的因子的充分必要条件是 $d = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$，其中 $0 \leqslant s_i \leqslant r_i, i = 1, 2, \cdots, k.$

例 1.1.1

1. 99 099 有多少个正因子?
2. 20! 的二进制表示中从最低位数起有多少个连续的 0?

推论 1.1.1

设 $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$，其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$r_1, r_2, \cdots, r_k$ 是正整数，则正整数 d 为 a 的因子的充分必要条件是 $d = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$，其中 $0 \leqslant s_i \leqslant r_i, i = 1, 2, \cdots, k.$

例 1.1.1

1. 99 099 有多少个正因子?
2. 20! 的二进制表示中从最低位数起有多少个连续的 0?

解

(1) 前面已有 $99\ 099 = 3^2 \times 7 \times 11^2 \times 13$. 由定理 1.1.1 的推论，99 099 的正因子的个数为 $3 \times 2 \times 3 \times 2 = 36$.

(2) 只需求 20! 含有多少个因子 2. 不超过 20 含有因子 2 的数(即偶数)有 2, $4 = 2^2$, $6 = 2 \times 3, 8 = 2^3, 10 = 2 \times 5, 12 = 2^2 \times 3, 14 = 2 \times 7$, $16 = 2^4$, $18 = 2 \times 9$, $20 = 2^2 \times 5$. 故 20! 含有 18 个因子 2，从而 20! 的二进制表示中从最低位数起有 18 个连续的 0. □

素数定理

定理 1.1.2

有无穷多个素数.

素数定理

定理 1.1.2

有无穷多个素数.

证明.

用反证法. 假设只有有穷个素数,从小到大依次记为 $p_1, p_2, \cdots, p_n$,令 $m = p_1 p_2 \cdots p_n + 1$. 显然,$p_i \nmid m, 1 \leqslant i \leqslant n$. 因此,要么 m 本身是素数,要么存在大于 p_n 的素数整除 m,矛盾. □

素数定理

定理 1.1.2

有无穷多个素数.

证明.

用反证法. 假设只有有穷个素数,从小到大依次记为 $p_1, p_2, \cdots, p_n$,令 $m = p_1 p_2 \cdots p_n + 1$. 显然,$p_i \nmid m, 1 \leqslant i \leqslant n$. 因此,要么 m 本身是素数,要么存在大于 p_n 的素数整除 m,矛盾. □

记 $\pi(n)$ 为小于或等于 n 的素数个数. 例如,$\pi(0) = \pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$, $\pi(5) = 3$. 关于 $\pi(n)$ 与 $\frac{n}{\ln n}$ 的关系有下述素数定理,定理的证明超出了本书的范围.

素数定理

定理 1.1.2

有无穷多个素数.

证明.

用反证法. 假设只有有穷个素数,从小到大依次记为 $p_1, p_2, \cdots, p_n$,令 $m = p_1 p_2 \cdots p_n + 1$. 显然,$p_i \nmid m, 1 \leqslant i \leqslant n$. 因此,要么 m 本身是素数,要么存在大于 p_n 的素数整除 m,矛盾. □

记 $\pi(n)$ 为小于或等于 n 的素数个数. 例如,$\pi(0) = \pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$, $\pi(5) = 3$. 关于 $\pi(n)$ 与 $\frac{n}{\ln n}$ 的关系有下述素数定理,定理的证明超出了本书的范围.

定理 1.1.3

$$\lim_{n \to +\infty} \frac{\pi(n)}{n/\ln n} = 1.$$

素数分布

$\pi(n)$ 描述了素数分布，表 1.1.1 表明 $\frac{n}{\ln n}$ 是 $\pi(n)$ 很好的近似.

表 1.1.1

n	10^3	10^4	10^5	10^6	10^7
$\pi(n)$	168	1 229	9 592	78 498	664 579
$\frac{n}{\ln n}$	145	1 086	8 686	72 382	620 421
$\frac{\pi(n)}{n/\ln n}$	1.159	1.132	1.104	1.085	1.071

检查一个正整数是否是素数称作素数测试. 根据命题 1.1.2 (3), 任给一个正整数 a, 只要对所有的 $1 < b < a$, 检查 $b \mid a$ 是否成立, 就能判断 a 是否是素数. 下述定理可以改进这个算法.

检查一个正整数是否是素数称作 素数测试. 根据命题 1.1.2 (3), 任给一个正整数 a, 只要对所有的 $1 < b < a$, 检查 $b \mid a$ 是否成立, 就能判断 a 是否是素数. 下述定理可以改进这个算法.

定理 1.1.4

若 a 是一个合数, 则 a 必有一个小于等于 $\sqrt{a}$ 的真因子.

检查一个正整数是否是素数称作素数测试. 根据命题 1.1.2 (3), 任给一个正整数 a, 只要对所有的 $1 < b < a$, 检查 $b \mid a$ 是否成立, 就能判断 a 是否是素数. 下述定理可以改进这个算法.

定理 1.1.4

若 a 是一个合数, 则 a 必有一个小于等于 $\sqrt{a}$ 的真因子.

证明.

由命题 1.1.2 3, $a = bc$, 其中 $1 < b < a, 1 < c < a$. 显然, b 和 c 中必有一个小于等于 $\sqrt{a}$. 否则, $bc > (\sqrt{a})^2 = a$, 矛盾. □

检查一个正整数是否是素数称作 *素数测试*. 根据命题 1.1.2 (3), 任给一个正整数 a, 只要对所有的 $1 < b < a$, 检查 $b \mid a$ 是否成立, 就能判断 a 是否是素数. 下述定理可以改进这个算法.

定理 1.1.4

若 a 是一个合数, 则 a 必有一个小于等于 $\sqrt{a}$ 的真因子.

证明.

由命题 1.1.2 3, $a = bc$, 其中 $1 < b < a, 1 < c < a$. 显然, b 和 c 中必有一个小于等于 $\sqrt{a}$. 否则, $bc > (\sqrt{a})^2 = a$, 矛盾. □

推论 1.1.2

若 a 是一个合数, 则 a 必有一个小于等于 $\sqrt{a}$ 的素因子.

检查一个正整数是否是素数称作素数测试. 根据命题 1.1.2 (3), 任给一个正整数 a, 只要对所有的 $1 < b < a$, 检查 $b \mid a$ 是否成立, 就能判断 a 是否是素数. 下述定理可以改进这个算法.

定理 1.1.4

若 a 是一个合数, 则 a 必有一个小于等于 $\sqrt{a}$ 的真因子.

证明.

由命题 1.1.2 3, $a = bc$, 其中 $1 < b < a, 1 < c < a$. 显然, b 和 c 中必有一个小于等于 $\sqrt{a}$. 否则, $bc > (\sqrt{a})^2 = a$, 矛盾. □

推论 1.1.2

若 a 是一个合数, 则 a 必有一个小于等于 $\sqrt{a}$ 的素因子.

证明.

由定理 1.1.4, a 有 $\leq \sqrt{a}$ 的真因子 b. 若 b 是素数, 结论成立; 否则, 由命题1.1.2 (4)和1.1.1(5), b 有素因子 $p < b \leq \sqrt{a}$. 由命题1.1.1(2), p 也是 a 的因子. □

素数测试

例 1.1.2

判断 *127* 和 *133* 是否是素数.

素数测试

例 1.1.2

判断 *127* 和 *133* 是否是素数.

解

$\sqrt{127}, \sqrt{133}$ 都小于 13，根据定理 1.1.2 的推论，只需检查它们是否有小于 13 的素因子. 小于 13 的素数有：$2, 3, 5, 7, 11$. 检查结果如下.

$$2 \nmid 127,\ 3 \nmid 127,\ 5 \nmid 127,\ 7 \nmid 127,\ 11 \nmid 127.$$

结论：127 是素数.

$$2 \nmid 133,\ 3 \nmid 133,\ 5 \nmid 133,\ 7 \mid 133\ (133 = 7 \times 19).$$

结论：133 是合数. □

10 以内的素数是 $2, 3, 5, 7$，用它们除 100 以内大于 10 的数，删去所有能被它们整除的数，剩下的(含 $2, 3, 5, 7$ 在内)就是 100 以内的所有素数. 如下表所示，其中画有 $\backslash, /, -, \times$ 的数分别表示能被 $2, 3, 5, 7$ 整除的数. 最后剩下 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89$ 和 97. 这 25 个数就是 100 以内的全部素数. 再用这 25 个素数除 $100^2 = 10\ 000$ 以内大于 100 的数，删去所有能被它们整除的数，可以得到 10 000 以内的所有素数. 重复这个做法可以得到任意给定的正整数以内的所有素数. 这个方法称作厄拉多塞(Eratosthene)筛法.

①	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

大素数

- 人们一直在寻找更大的素数. 近代已知的最大素数差不多总是形如 2^n-1 的数. 当 n 是合数时, 2^n-1 一定是合数. 设 $n=ab$, 其中 $a>1, b>1$, 有

$$2^{ab}-1=(2^a-1)(2^{a(b-1)}+2^{a(b-2)}+\cdots+\cdots+2^a+1).$$

  当 n 为素数时, $2^2-1=3, 2^3-1=7, 2^5-1=31, 2^7-1=127$ 都是素数, 而 $2^{11}-1=2\ 047=23\times 89$ 是合数. 设 p 为素数, 称形如 2^n-1 的素数为梅森(Mersenne)素数. 到 2023 年共找到 51 个梅森素数, 其中最大的梅森素数是 2018 年 12 月 7 日发现的第 51 个, 即 $2^{82\ 589\ 933}-1$, 这个数达到 $24\ 862\ 048$ 位.

- 2004 年, 印度学者 Agrawal、Kayal 和 Saxena 首次给出了一个确定性的、多项式时间复杂度的、对一般数均适用并且不依赖任何未被证明的猜想的素数测试算法①.

4.2 最大公因数与最小公倍数

设 a 和 b 是两个整数，如果 $d \mid a$ 且 $d \mid b$，那么称 d 为 a 与 b 的公因数，或公约数. 除 0 之外，任何整数只有有限个因子. 因而，两个不全为 0 的整数 a 和 b 只有有限个公因子，其中最大的称作最大公因数，或最大公约数. 记作 $\gcd(a, b)$.

4.2 最大公因数与最小公倍数

设 a 和 b 是两个整数，如果 $d \mid a$ 且 $d \mid b$，那么称 d 为 a 与 b 的公因数，或公约数. 除 0 之外，任何整数只有有限个因子. 因而，两个不全为 0 的整数 a 和 b 只有有限个公因子，其中最大的称作最大公因数，或最大公约数. 记作 $\gcd(a, b)$.

设 a 和 b 是两个非零整数，如果 $a \mid m$ 且 $b \mid m$，那么称 m 为 a 与 b 的公倍数. a 与 b 有无穷多个公倍数，其中最小的正公倍数称作最小公倍数. 记作 $\operatorname{lcm}(a, b)$.

4.2 最大公因数与最小公倍数

设 a 和 b 是两个整数，如果 $d \mid a$ 且 $d \mid b$，那么称 d 为 a 与 b 的公因数，或公约数. 除 0 之外，任何整数只有有限个因子. 因而，两个不全为 0 的整数 a 和 b 只有有限个公因子，其中最大的称作最大公因数，或最大公约数. 记作 $\gcd(a, b)$.

设 a 和 b 是两个非零整数，如果 $a \mid m$ 且 $b \mid m$，那么称 m 为 a 与 b 的公倍数. a 与 b 有无穷多个公倍数，其中最小的正公倍数称作最小公倍数. 记作 $\mathrm{lcm}(a, b)$.

显然，对任意的正整数 a，$\gcd(0, a) = a, \gcd(1, a) = 1, \mathrm{lcm}(1, a) = a$.

4.2 最大公因数与最小公倍数

设 a 和 b 是两个整数，如果 $d \mid a$ 且 $d \mid b$，那么称 d 为 a 与 b 的公因数，或公约数. 除 0 之外，任何整数只有有限个因子. 因而，两个不全为 0 的整数 a 和 b 只有有限个公因子，其中最大的称作最大公因数，或最大公约数. 记作 $\gcd(a, b)$.

设 a 和 b 是两个非零整数，如果 $a \mid m$ 且 $b \mid m$，那么称 m 为 a 与 b 的公倍数. a 与 b 有无穷多个公倍数，其中最小的正公倍数称作最小公倍数. 记作 $\mathrm{lcm}(a, b)$.

显然，对任意的正整数 a，$\gcd(0, a) = a, \gcd(1, a) = 1, \mathrm{lcm}(1, a) = a$.

可以利用整数的素因子分解，求最大公因数和最小公倍数. 设

4.2 最大公因数与最小公倍数

设 a 和 b 是两个整数，如果 $d \mid a$ 且 $d \mid b$，那么称 d 为 a 与 b 的公因数，或公约数. 除 0 之外，任何整数只有有限个因子. 因而，两个不全为 0 的整数 a 和 b 只有有限个公因子，其中最大的称作最大公因数，或最大公约数. 记作 $\gcd(a, b)$.

设 a 和 b 是两个非零整数，如果 $a \mid m$ 且 $b \mid m$，那么称 m 为 a 与 b 的公倍数. a 与 b 有无穷多个公倍数，其中最小的正公倍数称作最小公倍数. 记作 $\mathrm{lcm}(a, b)$.

显然，对任意的正整数 a，$\gcd(0, a) = a, \gcd(1, a) = 1, \mathrm{lcm}(1, a) = a$.

可以利用整数的素因子分解，求最大公因数和最小公倍数. 设

$$a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \quad b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k},$$

其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$r_1, r_2, \cdots, r_k, s_1, s_2, \cdots, s_k$ 是非负整数.

4.2 最大公因数与最小公倍数

设 a 和 b 是两个整数，如果 $d \mid a$ 且 $d \mid b$，那么称 d 为 a 与 b 的公因数，或公约数. 除 0 之外，任何整数只有有限个因子. 因而，两个不全为 0 的整数 a 和 b 只有有限个公因子，其中最大的称作最大公因数，或最大公约数. 记作 $\gcd(a, b)$.

设 a 和 b 是两个非零整数，如果 $a \mid m$ 且 $b \mid m$，那么称 m 为 a 与 b 的公倍数. a 与 b 有无穷多个公倍数，其中最小的正公倍数称作最小公倍数. 记作 $\operatorname{lcm}(a, b)$.

显然，对任意的正整数 a，$\gcd(0, a) = a, \gcd(1, a) = 1, \operatorname{lcm}(1, a) = a$.

可以利用整数的素因子分解，求最大公因数和最小公倍数. 设

$$a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}, \quad b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k},$$

其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数，$r_1, r_2, \cdots, r_k, s_1, s_2, \cdots, s_k$ 是非负整数. 则

$$\gcd(a, b) = p_1^{\min(r_1, s_1)} p_2^{\min(r_2, s_2)} \cdots p_k^{\min(r_k, s_k)},$$
$$\operatorname{lcm}(a, b) = p_1^{\max(r_1, s_1)} p_2^{\max(r_2, s_2)} \cdots p_k^{\max(r_k, s_k)}.$$

最大公因数与最小公倍数(续)

定理 1.2.1

1. 若 $a \mid m, b \mid m$, 则 $\operatorname{lcm}(a, b) \mid m$.
2. 若 $d \mid a, d \mid b$, 则 $d \mid \gcd(a, b)$.

最大公因数与最小公倍数(续)

定理 1.2.1

1. 若 $a \mid m, b \mid m$,则 $\operatorname{lcm}(a, b) \mid m$.
2. 若 $d \mid a, d \mid b$,则 $d \mid \gcd(a, b)$.

证明.

(1) 记 $M = \operatorname{lcm}(a, b)$,设 $m = qM + r, 0 \leqslant r < M$.

根据命题 1.1.1 (1),由 $a \mid m, a \mid M$,及 $r = m - qM$,可以得到 $a \mid r$. 同理,有 $b \mid r$. 即,r 是 a 和 b 的公倍数. 根据最小公倍数的定义,必有 $r = 0$. 得证 $M \mid m$.

最大公因数与最小公倍数(续)

定理 1.2.1

1. 若 $a \mid m, b \mid m$,则 $\operatorname{lcm}(a, b) \mid m$.
2. 若 $d \mid a, d \mid b$,则 $d \mid \gcd(a, b)$.

证明.

(1) 记 $M = \operatorname{lcm}(a, b)$,设 $m = qM + r, 0 \leqslant r < M$.

根据命题 1.1.1 (1),由 $a \mid m, a \mid M$,及 $r = m - qM$,可以得到 $a \mid r$. 同理,有 $b \mid r$. 即,r 是 a 和 b 的公倍数. 根据最小公倍数的定义,必有 $r = 0$. 得证 $M \mid m$.

(2) 记 $D = \gcd(a, b)$,令 $m = \operatorname{lcm}(d, D)$. 若 $m = D$,自然有 $d \mid D$,结论成立. 否则 $m > D$,注意到 $d \mid a, D \mid a$,由 (1),得 $m \mid a$. 同理,$m \mid b$. 即 m 是 a 和 b 的公因子,与 D 是 a 和 b 的最大公因数矛盾. □

例 1.2.1

求 168 和 300 的最大公因数和最小公倍数.

例 1.2.1

求 168 和 300 的最大公因数和最小公倍数.

解

对 168 和 300 做素因子分解:

$$168 = 2^3 \times 3 \times 7, \quad 300 = 2^2 \times 3 \times 5^2.$$

可把它们写成

$$168 = 2^3 \times 3^1 \times 5^0 \times 7^1, \quad 300 = 2^2 \times 3^1 \times 5^2 \times 7^0.$$

于是

$$\gcd(168, 300) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12,$$
$$\operatorname{lcm}(168, 300) = 2^3 \times 3^1 \times 5^2 \times 7^1 = 4\ 200.$$

□

辗转相除法

求最大公因数的常用方法是辗转相除法. 它是基于下述定理构造的.

定理 1.2.2

设 $a = qb + r$, 其中 a, b, q, r 都是整数, 则 $\gcd(a, b) = \gcd(b, r)$.

辗转相除法

求最大公因数的常用方法是辗转相除法. 它是基于下述定理构造的.

定理 1.2.2

设 $a = qb + r$, 其中 a, b, q, r 都是整数, 则 $\gcd(a, b) = \gcd(b, r)$.

证明.

只需证 a 和 b 的公因子与 b 和 r 的公因子相同. 设 d 是 a 与 b 的公因子, 即 $d \mid a$ 且 $d \mid b$. 注意到, $r = a - qb$, 由命题1.1.1 1, 有 $d \mid r$. 从而, $d \mid b$ 且 $d \mid r$, 即 d 也是 b 与 r 的公因子. 反之一样, 设 d 是 b 与 r 的公因子, 即 $d \mid b$ 且 $d \mid r$. 注意到, $a = qb + r$, 故有 $d \mid a$. 从而, $d \mid a$ 且 $d \mid b$, 即 d 也是 a 与 b 的公因子. □

设 $a, b \in \mathbb{Z}$, 且 $b \neq 0$, 做带余除法

$$a = q_1 b + r_2, \quad 0 \leqslant r_2 < |b|.$$

设 $a, b \in \mathbb{Z}$, 且 $b \neq 0$, 做带余除法

$$a = q_1 b + r_2, \quad 0 \leqslant r_2 < |b|.$$

若 $r_2 > 0$,再对 b 和 r_2 做带余除法,得

$$b = q_2 r_2 + r_3, \quad 0 \leqslant r_3 < r_2.$$

设 $a, b \in \mathbb{Z}$, 且 $b \neq 0$, 做带余除法

$$a = q_1 b + r_2, \quad 0 \leqslant r_2 < |b|.$$

若 $r_2 > 0$, 再对 b 和 r_2 做带余除法, 得

$$b = q_2 r_2 + r_3, \quad 0 \leqslant r_3 < r_2.$$

重复上述过程. 由于 $|b| > r_2 > r_3 > \cdots \geqslant 0$, 必存在 k 使 $r_{k+1} = 0$. 于是, 有

$$\begin{aligned}
a &= q_1 b + r_2, && 1 \leqslant r_2 < |b|; \\
b &= q_2 r_2 + r_3, && 1 \leqslant r_3 < r_2; \\
r_2 &= q_3 r_3 + r_4, && 1 \leqslant r_4 < r_3; \\
&\vdots \\
r_{k-2} &= q_{k-1} r_{k-1} + r_k, && 1 \leqslant r_k < r_{k-1}; \\
r_{k-1} &= q_k r_k.
\end{aligned} \tag{①}$$

设 $a, b \in \mathbb{Z}$, 且 $b \neq 0$, 做带余除法

$$a = q_1 b + r_2, \quad 0 \leqslant r_2 < |b|.$$

若 $r_2 > 0$, 再对 b 和 r_2 做带余除法, 得

$$b = q_2 r_2 + r_3, \quad 0 \leqslant r_3 < r_2.$$

重复上述过程. 由于 $|b| > r_2 > r_3 > \cdots \geqslant 0$, 必存在 k 使 $r_{k+1} = 0$. 于是, 有

$$\begin{aligned}
a &= q_1 b + r_2, && 1 \leqslant r_2 < |b|; \\
b &= q_2 r_2 + r_3, && 1 \leqslant r_3 < r_2; \\
r_2 &= q_3 r_3 + r_4, && 1 \leqslant r_4 < r_3; \\
&\vdots \\
r_{k-2} &= q_{k-1} r_{k-1} + r_k, && 1 \leqslant r_k < r_{k-1}; \\
r_{k-1} &= q_k r_k.
\end{aligned} \tag{①}$$

根据定理 1.2.2, 有 $\gcd(a, b) = \gcd(b, r_2) = \cdots = \gcd(r_{k-1}, r_k) = r_k$.

这就是辗转相除法, 又称作欧几里得(Euclid)算法.

定理 1.2.3

设 a 和 b 不全为 0, 则存在整数 x 和 y 使得 $\gcd(a, b) = xa + yb$.

定理 1.2.3

设 a 和 b 不全为 0, 则存在整数 x 和 y 使得 $\gcd(a,b) = xa + yb$.

证明.

记 $a = r_0, b = r_1$, ①式可写成

$$r_i = q_{i+1}r_{i+1} + r_{i+2},\ \ i = 0, 1, \cdots, k-2,\ \ r_{k-1} = q_k r_k,$$

其中 $\gcd(a,b) = r_k$. 把上式改写成 $r_i = r_{i-2} - q_{i-1}r_{i-1},\ \ i = 2, 3, \cdots, k$. 从后向前逐个回代, 就可以将 r_k 表示成 a 和 b 的线性组合.

记 $x_{k-1} = 1, y_{k-1} = -q_{k-1}$, 把最后一式写成

$$r_k = x_{k-1}r_{k-2} + y_{k-1}r_{k-1}.$$

一般地, 设 $r_k = x_i r_{i-1} + y_i r_i$, 代入 r_i,

$$r_k = x_i r_{i-1} + y_i(r_{i-2} - q_{i-1}r_{i-1}) = y_i r_{i-2} + (x_i - q_{i-1}y_i)r_{i-1},$$

得 $x_{i-1} = y_i,\ \ y_{i-1} = x_i - q_{i-1}y_i,\ \ i = k-1, k-2, \cdots, 2.$

取 $x = x_1, y = y_1$, 得 $r_k = xa + yb$. □

例 1.2.2

用辗转相除法求 168 与 300 的最大公因子 d,并把 d 表示成 168 和 300 的线性组合,即求整数 x 和 y 使得 $d = 168x + 300y$.

例 1.2.2

用辗转相除法求 168 与 300 的最大公因子 d，并把 d 表示成 168 和 300 的线性组合，即求整数 x 和 y 使得 $d = 168x + 300y$.

解

做辗转相除有

$$\begin{aligned}
300 &= 168 + 132,\\
168 &= 132 + 36,\\
132 &= 3 \times 36 + 24,\\
36 &= 24 + 12,\\
24 &= 2 \times 12,
\end{aligned}$$

得 $\gcd(168, 300) = 12$.

由上面的式子，又有

$$\begin{aligned}
12 &= 36 - 24\\
&= 36 - (132 - 3 \times 36)\\
&= 4 \times 36 - 132\\
&= 4 \times (168 - 132) - 132\\
&= -5 \times 132 + 4 \times 168\\
&= -5 \times (300 - 168) + 4 \times 168\\
&= 9 \times 168 - 5 \times 300.
\end{aligned}$$

取 $x = 9, y = -5$，有 $d = 12 = 168x + 300y$.

定义 1.2.1

如果 $\gcd(a, b) = 1$，那么称 a 和 b *互素*. 如果整数 $a_1, a_2, \cdots, a_n$ 中的任意两个都互素，那么称它们*两两互素*.

定义 1.2.1

如果 $\gcd(a,b)=1$，那么称 a 和 b *互素*. 如果整数 $a_1, a_2, \cdots, a_n$ 中的任意两个都互素，那么称它们*两两互素*.

定理 1.2.4

整数 a 和 b 互素的充分必要条件是存在整数 x 和 y 使得 $xa+yb=1$.

定义 1.2.1

如果 $\gcd(a,b)=1$，那么称 a 和 b *互素*. 如果整数 $a_1,a_2,\cdots,a_n$ 中的任意两个都互素，那么称它们*两两互素*.

定理 1.2.4

整数 a 和 b 互素的充分必要条件是存在整数 x 和 y 使得 $xa+yb=1$.

证明.

必要性可由定理 1.2.3 得到.

充分性. 设 $xa+yb=1, x,y\in\mathbb{Z}$, 设 $d>0$ 是 a 和 b 的公因子，由命题 1.1.1(1)，$d\mid xa+yb$，即 $d\mid 1$. 再由命题 1.1.1(5)，必有 $d=1$，得证 a 和 b 互素. □

定义 1.2.1

如果 $\gcd(a,b)=1$，那么称 a 和 b *互素*. 如果整数 $a_1,a_2,\cdots,a_n$ 中的任意两个都互素，那么称它们*两两互素*.

定理 1.2.4

整数 a 和 b 互素的充分必要条件是存在整数 x 和 y 使得 $xa+yb=1$.

证明.

必要性可由定理 1.2.3 得到.

充分性. 设 $xa+yb=1, x,y\in\mathbb{Z}$, 设 $d>0$ 是 a 和 b 的公因子，由命题 1.1.1(1)，$d\mid xa+yb$，即 $d\mid 1$. 再由命题 1.1.1(5)，必有 $d=1$，得证 a 和 b 互素. □

例 1.2.3

设 $a\mid c, b\mid c$，且 a 与 b 互素，则 $ab\mid c$.

定义 1.2.1

如果 $\gcd(a,b)=1$，那么称 a 和 b *互素*. 如果整数 $a_1,a_2,\cdots,a_n$ 中的任意两个都互素，那么称它们*两两互素*.

定理 1.2.4

整数 a 和 b 互素的充分必要条件是存在整数 x 和 y 使得 $xa+yb=1$.

证明.

必要性可由定理 1.2.3 得到.

充分性. 设 $xa+yb=1, x,y\in\mathbb{Z}$, 设 $d>0$ 是 a 和 b 的公因子，由命题 1.1.1(1)，$d\mid xa+yb$，即 $d\mid 1$. 再由命题 1.1.1(5)，必有 $d=1$，得证 a 和 b 互素. □

例 1.2.3

设 $a\mid c, b\mid c$，且 a 与 b 互素，则 $ab\mid c$.

证明.

根据定理 1.2.4，$\exists x,y\in\mathbb{Z}$，使 $xa+yb=1$. 于是得 $cxa+cyb=c$. 又由 $a\mid xa$ 和 $b\mid c$，可得 $ab\mid cxa$. 同理，$ab\mid cyb$. 于是，有 $ab\mid cxa+cyb$，即 $ab\mid c$. □

4.3 同余

在第 2.6 节，作为等价关系的实例，我们介绍了同余关系. 本节我们进一步讨论同余的性质及同余类上的运算.

定义 1.3.1

设 m 是正整数，a 和 b 是整数. 若 $m \mid a-b$，则称 a 模 m 同余于 b，或 a 与 b 模 m 同余，记作 $a \equiv b \pmod{m}$. 若 a 与 b 模 m 不同余，则记作 $a \not\equiv b \pmod{m}$.

4.3 同余

在第 2.6 节，作为等价关系的实例，我们介绍了同余关系. 本节我们进一步讨论同余的性质及同余类上的运算.

定义 1.3.1

设 m 是正整数，a 和 b 是整数. 若 $m \mid a-b$，则称 a 模 m 同余于 b，或 a 与 b 模 m 同余，记作 $a \equiv b \pmod{m}$. 若 a 与 b 模 m 不同余，则记作 $a \not\equiv b \pmod{m}$.

注 1.3.1

不难验证，下述两条都是 a 与 b 模 m 同余的充分必要条件.

1. a 和 b 分别除以 m 的余数相同，即 $a \bmod m = b \bmod m$.
2. $a = b + km$，其中 k 是整数.

例如，$20 \equiv 2 \pmod{6}, 18 \equiv 0 \pmod{6}, 15 \equiv -3 \pmod{6}$,
$14 \not\equiv 21 \pmod{6}$.

命题 1.3.1

同余关系是等价关系，即同余关系具有：

1. **自反性**：$a \equiv a \pmod{m}$.
2. **对称性**：若 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$.
3. **传递性**：若 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$，则 $a \equiv c \pmod{m}$.

由传递性，常把 $a_1 \equiv a_2 \pmod{m}, a_2 \equiv a_3 \pmod{m}, \cdots, a_{k-1} \equiv a_k \pmod{m}$ 缩写成 $a_1 \equiv a_2 \equiv \cdots \equiv a_k \pmod{m}$.

命题 1.3.1

同余关系是等价关系，即同余关系具有：

1. 自反性：$a \equiv a \pmod{m}$.
2. 对称性：若 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$.
3. 传递性：若 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$，则 $a \equiv c \pmod{m}$.

由传递性，常把 $a_1 \equiv a_2 \pmod{m}$, $a_2 \equiv a_3 \pmod{m}$, $\cdots$, $a_{k-1} \equiv a_k \pmod{m}$ 缩写成 $a_1 \equiv a_2 \equiv \cdots \equiv a_k \pmod{m}$.

命题 1.3.2

1. 若 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$，则 $a \pm c \equiv b \pm d \pmod{m}$, $ac \equiv bd \pmod{m}$, $a^k \equiv b^k \pmod{m}$, 其中 k 是非负整数.
2. 设 $d \geqslant 1, d \mid m$，若 $a \equiv b \pmod{m}$，则 $a \equiv b \pmod{d}$.
3. 设 $d \geqslant 1$，则 $a \equiv b \pmod{m}$ 当且仅当 $da \equiv db \pmod{dm}$.
4. 设 c 与 m 互素，则 $a \equiv b \pmod{m}$ 当且仅当 $ca \equiv cb \pmod{m}$.

整数 a 在模 m 同余关系下的等价类记作 $[a]_m$，称作 a 的模 m 等价类．在不会引起混淆的情况下，可以略去下标 m，简记作 $[a]$，有时也会直接记作 a．把整数集 $\mathbb{Z}$ 在模 m 同余关系下的商集记作 $\mathbb{Z}_m$．根据命题1.3.2(1)，可以在 $\mathbb{Z}_m$ 上定义加法和乘法如下：对任意的整数 a, b，

$$[a] \oplus [b] = [a + b], \quad [a] \otimes [b] = [ab].$$

整数 a 在模 m 同余关系下的等价类记作 $[a]_m$，称作 a 的模 m 等价类. 在不会引起混淆的情况下，可以略去下标 m，简记作 $[a]$，有时也会直接记作 a. 把整数集 $\mathbb{Z}$ 在模 m 同余关系下的商集记作 $\mathbb{Z}_m$. 根据命题1.3.2(1)，可以在 $\mathbb{Z}_m$ 上定义加法和乘法如下：对任意的整数 a, b，

$$[a] \oplus [b] = [a+b], \quad [a] \otimes [b] = [ab].$$

例 1.3.1

写出 $\mathbb{Z}_5$ 的全部元素以及 $\mathbb{Z}_5$ 上的加法表和乘法表.

解

$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$，其中 $[i] = \{5k + i | k \in \mathbb{Z}\}, i = 0, 1, 2, 3, 4.$

$\oplus$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\otimes$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

同余的应用

例 1.3.2

3^{455} 的个位数是多少?

同余的应用

例 1.3.2

3^{455} 的个位数是多少?

解

设 3^{455} 的个位数为 x, 则有 $3^{455} \equiv x \pmod{10}$. 由 $3^4 \equiv 1 \pmod{10}$ 和命题1.3.21, 有

$$3^{455} = 3^{4\times 113+3} \equiv 3^3 \equiv 7 \pmod{10}.$$

故 3^{455} 的个位数是 7. □

日期的星期数

例 1.3.3

如何计算 y 年 m 月 d 日是星期几?

为方便起见,用 $0,1,\cdots,6$ 分别表示周日,周一,$\cdots$,周六,称作星期数. 整百年的年份,即 $100C$ 的年份称作世纪年,C 称作该世纪年的世纪数.

闰年规则:除世纪年外,每 4 年一个闰年,年数能被 4 整除的年为闰年. 平年一年有 365 天,其中 2 月有 28 天;闰年有 366 天,其中 2 月有 29 天.

由于 2 月有 28 天或 29 天,为计算方便,从 3 月 1 日开始算起,或者说,把 3 月看作第 1 个月,把 12 月看作第 10 个月,下一年的 1 月是第 11 个月,2 月是第 12 个月. 于是,y 年 m 月 d 日现在变成 Y 年 M 月 d 日,其中

$$M=(m-3)\bmod 12+1,\ Y=y-\lfloor M/11\rfloor.$$

由于 $365\equiv 1\ (\mathrm{mod}\,7)$,所以 3 月 1 日的星期数每过一个平年加 1,每过一个闰年还要多加一个 1(都是在模 7 下运算). 设 1600 年 3 月 1 日的星期数为 w_{1600},y 年 3 月 1 日(Y 年 1 月 1 日)的星期数为 w_Y. 设 $y=Y=100C+X$,从 1600 年到 Y 年要经过 $100C+X-1600$ 年,星期数应加

$$100C+X-1600\equiv 2C+X+3\ (\mathrm{mod}\,7).$$

例1.3.3(续)

因为每 4 年一个闰年,故有

$$\lfloor (100C + X - 1600)/4 \rfloor = 25C + \lfloor X/4 \rfloor - 400$$

个闰年. 考虑到世纪年,应从这个数中减去 $C - 16$,再加 $\lfloor (C-16)/4 \rfloor = \lfloor C/4 \rfloor - 4$. 因此,

$$\begin{aligned} w_Y &\equiv w_{1600} + (2C + X + 3) + (25C + \lfloor X/4 \rfloor - 400) - (C - 16) + (\lfloor C/4 \rfloor - 4) \\ &\equiv w_{1600} - 2C + X + \lfloor X/4 \rfloor + \lfloor C/4 \rfloor \pmod 7. \end{aligned}$$

已知 2004 年 3 月 1 日是星期一,代入上式,有

$$\begin{aligned} 1 &\equiv w_{1600} - 2 \times 20 + 4 + \lfloor 4/4 \rfloor + \lfloor 20/4 \rfloor \\ &\equiv w_{1600} + 5 \pmod 7, \end{aligned}$$

得 $w_{1600} = 3$,即 1600 年 3 月 1 日是星期三. 于是,得到

$$w_Y \equiv 3 - 2C + X + \lfloor X/4 \rfloor + \lfloor C/4 \rfloor \pmod 7. \qquad ①$$

例1.3.3(续)

接下来计算从当年 3 月 1 日到每个月 1 号的天数. 除每个月加 30 天外, 由于 3、5、7、8、10、12、1 月有 31 天, 应另外加的天数 z 如下表所示.

M	1	2	3	4	5	6	7	8	9	10	11	12
z	0	1	1	2	2	3	4	4	5	5	6	7

z 可以表示成

$$
\begin{aligned}
z &= \begin{cases} \lfloor M/2 \rfloor, & 1 \leqslant M \leqslant 6, \\ \lfloor (M+1)/2 \rfloor, & 7 \leqslant M \leqslant 11, \\ \lfloor (M+1)/2 \rfloor + 1, & M = 12, \end{cases} \\
&= \lfloor (M + \lfloor M/7 \rfloor)/2 \rfloor + \lfloor M/12 \rfloor .
\end{aligned}
$$

因此, M 月 d 日的星期数应在 w_Y 上加

$$
\begin{aligned}
& 30(M-1) + \lfloor (M + \lfloor M/7 \rfloor)/2 \rfloor + \lfloor M/12 \rfloor + d - 1 \\
\equiv\ & 2M + \lfloor (M + \lfloor M/7 \rfloor)/2 \rfloor + \lfloor M/12 \rfloor + d - 3 \pmod 7 .
\end{aligned} \tag{②}
$$

例1.3.3(续)

最后,将 ①,② 两式合并,得到 y 年 m 月 d 日星期数的计算公式:

$$w \equiv X + \lfloor X/4 \rfloor + \lfloor C/4 \rfloor - 2C + 2M + \lfloor (M + \lfloor M/7 \rfloor)/2 \rfloor + \lfloor M/12 \rfloor + d \pmod 7,$$

其中 $M = (m-3) \mod 12 + 1$, $Y = y - \lfloor M/11 \rfloor = 100C + X$.

例如,中华人民共和国成立日为 1949 年 10 月 1 日,

$C = 19, X = 49, M = 8, d = 1$,

$$\begin{aligned} w &\equiv 49 + \lfloor 49/4 \rfloor + \lfloor 19/4 \rfloor - 2 \times 19 + 2 \times 8 + \lfloor (8 + \lfloor 8/7 \rfloor)/2 \rfloor + \lfloor 8/12 \rfloor + 1 \\ &\equiv 6 \pmod 7 \end{aligned}$$

是星期六.

1945 年 8 月 15 日,日本正式宣布无条件投降,这里

$C = 19, X = 45, M = 6, d = 15$,

$$\begin{aligned} w &\equiv 45 + \lfloor 45/4 \rfloor + \lfloor 19/4 \rfloor - 2 \times 19 + 2 \times 6 + \lfloor (6 + \lfloor 6/7 \rfloor)/2 \rfloor) + \lfloor 6/12 \rfloor + 15 \\ &\equiv 3 \pmod 7 \end{aligned}$$

是星期三.

4.4 一次同余方程

设 $m > 0$, 方程

$$ax \equiv c \pmod{m} \tag{1.4.1}$$

称作 一次同余方程 , 使方程 (1.4.1) 成立的整数称作方程的 解 .

4.4 一次同余方程

设 $m > 0$, 方程

$$ax \equiv c \pmod{m} \tag{1.4.1}$$

称作 一次同余方程 , 使方程 (1.4.1) 成立的整数称作方程的 解 .

定理 1.4.1

方程 (1.4.1) 有解的充分必要条件是 $\gcd(a, m) \mid c$.

4.4 一次同余方程

设 $m > 0$, 方程

$$ax \equiv c \pmod{m} \tag{1.4.1}$$

称作 一次同余方程 , 使方程 (1.4.1) 成立的整数称作方程的 解 .

定理 1.4.1

方程 (1.4.1) 有解的充分必要条件是 $\gcd(a, m) \mid c$.

证明.

充分性. 记 $d = \gcd(a, m), a = da_1, m = dm_1, c = dc_1$, 其中 a_1 与 m_1 互素. 由定理 1.2.4, 存在 x_1 和 y_1 使得 $a_1x_1 + m_1y_1 = 1$. 令 $x = c_1x_1, y = c_1y_1$, 得 $a_1x + m_1y = c_1$. 等式两边同乘以 d, 得 $ax + my = c$. 所以, $ax \equiv c \pmod{m}$, 即 x 是方程 (1.4.1) 的解.

4.4 一次同余方程

设 $m > 0$, 方程

$$ax \equiv c \pmod{m} \tag{1.4.1}$$

称作 一次同余方程 , 使方程 (1.4.1) 成立的整数称作方程的 解 .

定理 1.4.1

方程 (1.4.1) 有解的充分必要条件是 $\gcd(a, m) \mid c$.

证明.

充分性. 记 $d = \gcd(a, m), a = da_1, m = dm_1, c = dc_1$, 其中 a_1 与 m_1 互素. 由定理 1.2.4, 存在 x_1 和 y_1 使得 $a_1x_1 + m_1y_1 = 1$. 令 $x = c_1x_1, y = c_1y_1$, 得 $a_1x + m_1y = c_1$. 等式两边同乘以 d, 得 $ax + my = c$. 所以, $ax \equiv c \pmod{m}$, 即 x 是方程 (1.4.1) 的解.

必要性. 设 x 是方程的解, 则存在 y 使得 $ax + my = c$. 由命题1.1.1 (1), 有 $d \mid c$. □

解一次同余方程

设 x_0 是方程 (1.4.1) 的解，不难验证所有与 x_0 模 m 同余的数都是方程 (1.4.1) 的解，从而 (1.4.1) 的解可以写成 $x \equiv x_0 \pmod{m}$. 于是，只需对模 m 的每一个等价类取一个代表，验证是否使方程成立，就能找到方程的所有解.

解一次同余方程

设 x_0 是方程 (1.4.1) 的解，不难验证所有与 x_0 模 m 同余的数都是方程 (1.4.1) 的解，从而 (1.4.1) 的解可以写成 $x \equiv x_0 \pmod{m}$. 于是，只需对模 m 的每一个等价类取一个代表，验证是否使方程成立，就能找到方程的所有解.

例 1.4.1

解一次同余方程 $8x \equiv 4 \pmod{6}$.

解一次同余方程

设 x_0 是方程 (1.4.1) 的解，不难验证所有与 x_0 模 m 同余的数都是方程 (1.4.1) 的解，从而 (1.4.1) 的解可以写成 $x \equiv x_0 \pmod{m}$. 于是，只需对模 m 的每一个等价类取一个代表，验证是否使方程成立，就能找到方程的所有解.

例 1.4.1

解一次同余方程 $8x \equiv 4 \pmod{6}$.

解

$\gcd(8,6) = 2, 2 \mid 4$，由定理 1.4.1，方程有解. 取模 6 等价类的代表 $x = -2, -1, 0, 1, 2, 3$，计算结果如下.

$$
\begin{aligned}
8 \times (-2) \equiv 8 \times 1 \equiv 2 \pmod{6}, \\
8 \times (-1) \equiv 8 \times 2 \equiv 4 \pmod{6}, \\
8 \times 0 \equiv 8 \times 3 \equiv 0 \pmod{6}.
\end{aligned}
$$

得方程的解 $x \equiv -1, 2 \pmod{6}$，方程的最小正整数解是 2. □

定义 1.4.1

如果 $ab \equiv 1 \pmod{m}$**,那么称** b **为** a **的** 模 m 逆 **,记作** $a^{-1} \pmod{m}$ **或** a^{-1}.

定义 1.4.1

如果 $ab \equiv 1 \pmod{m}$，那么称 b 为 a 的模 m 逆，记作 $a^{-1} \pmod{m}$ 或 a^{-1}.

根据定义，a 的模 m 逆就是方程

$$ax \equiv 1 \pmod{m} \tag{1.4.2}$$

的解.

定义 1.4.1

如果 $ab \equiv 1 \pmod{m}$，那么称 b 为 a 的模 m 逆，记作 $a^{-1} \pmod{m}$ 或 a^{-1}.

根据定义，a 的模 m 逆就是方程

$$ax \equiv 1 \pmod{m} \tag{1.4.2}$$

的解.

定理 1.4.2

1. a 的模 m 逆存在的充分必要条件是 a 与 m 互素.
2. 设 a 与 m 互素，则在模 m 下 a 的模 m 逆是唯一的，即 a 的任意两个模 m 逆都模 m 同余.

定义 1.4.1

如果 $ab \equiv 1 \pmod{m}$，那么称 b 为 a 的模 m 逆，记作 $a^{-1} \pmod{m}$ 或 a^{-1}.

根据定义，a 的模 m 逆就是方程

$$ax \equiv 1 \pmod{m} \tag{1.4.2}$$

的解.

定理 1.4.2

1. a 的模 m 逆存在的充分必要条件是 a 与 m 互素.
2. 设 a 与 m 互素，则在模 m 下 a 的模 m 逆是唯一的，即 a 的任意两个模 m 逆都模 m 同余.

证明.

(1) 这是定理 1.4.1 的直接推论.

(2) 设 b_1 和 b_2 是 a 的两个模 m 逆，即 $ab_1 \equiv 1 \pmod{m}$, $ab_2 \equiv 1 \pmod{m}$. 由命题1.3.2(1)，得 $a(b_1 - b_2) \equiv 0 \pmod{m}$. 而 a 与 m 互素，由命题1.3.2(4)，$b_1 - b_2 \equiv 0 \pmod{m}$，得证 $b_1 \equiv b_2 \pmod{m}$. □

例 1.4.2

求 5 模 7 的逆.

例 1.4.2

求 *5* 模 *7* 的逆.

解

5 与 7 互素,故 5 模 7 的逆存在.

方法 1. 直接观察或心算. 当 a 和 m 都比较小时,这是行得通的,而且比较快捷. 这里,$3 \times 5 - 2 \times 7 = 1$,得 $5^{-1} \equiv 3 \pmod 7$.

例 1.4.2

求 5 模 7 的逆.

解

5 与 7 互素,故 5 模 7 的逆存在.

方法 1. 直接观察或心算. 当 a 和 m 都比较小时,这是行得通的,而且比较快捷. 这里,$3 \times 5 - 2 \times 7 = 1$,得 $5^{-1} \equiv 3 \pmod 7$.

方法 2. 采用例 1.4.1 中的方法解同余方程 (1.4.2). 将 $x = -3, -2, -1, 0, 1, 2, 3$ 计算 $5x \mod 7$,得到 $5^{-1} \equiv 3 \pmod 7$.

例 1.4.2

求 5 模 7 的逆.

解

5 与 7 互素,故 5 模 7 的逆存在.

方法 1. 直接观察或心算. 当 a 和 m 都比较小时,这是行得通的,而且比较快捷. 这里,$3 \times 5 - 2 \times 7 = 1$,得 $5^{-1} \equiv 3 \pmod 7$.

方法 2. 采用例 1.4.1 中的方法解同余方程 (1.4.2). 将 $x = -3, -2, -1, 0, 1, 2, 3$ 计算 $5x \mod 7$,得到 $5^{-1} \equiv 3 \pmod 7$.

方法 3. 做辗转相除,求得整数 b, k 使得 $ab + km = 1$,则 b 是 a 的模 m 逆. 计算如下.

$$7 = 5 + 2,\ 5 = 2 \times 2 + 1.$$

回代,

$$1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 5) = 3 \times 5 - 2 \times 7,$$

得 $5^{-1} \equiv 3 \pmod 7$. □

4.5 欧拉定理和费马小定理

欧拉函数 ϕ 是数论中的一个重要函数，定义如下：设 n 是正整数，$\phi(n)$ 表示 $\{1, 2, \cdots, n\}$ 中与 n 互素的元素个数.

4.5 欧拉定理和费马小定理

欧拉函数 ϕ 是数论中的一个重要函数，定义如下：设 n 是正整数，$\phi(n)$ 表示 $\{1, 2, \cdots, n\}$ 中与 n 互素的元素个数.

例如，$\phi(1) = \phi(2) = 1, \phi(3) = \phi(4) = 2$. 显然，当 n 为素数时 $\phi(n) = n - 1$；当 n 为合数时，$\phi(n) < n - 1$.

4.5 欧拉定理和费马小定理

欧拉函数 ϕ 是数论中的一个重要函数，定义如下：设 n 是正整数，$\phi(n)$ 表示 $\{1, 2, \cdots, n\}$ 中与 n 互素的元素个数.

例如，$\phi(1) = \phi(2) = 1, \phi(3) = \phi(4) = 2$. 显然，当 n 为素数时 $\phi(n) = n - 1$；当 n 为合数时，$\phi(n) < n - 1$.

例 1.5.1

给定正整数 $n, n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 为 n 的素因子分解式，求欧拉函数的值 $\phi(n)$.

4.5 欧拉定理和费马小定理

欧拉函数 ϕ 是数论中的一个重要函数，定义如下：设 n 是正整数，$\phi(n)$ 表示 $\{1, 2, \cdots, n\}$ 中与 n 互素的元素个数.

例如，$\phi(1) = \phi(2) = 1, \phi(3) = \phi(4) = 2$. 显然，当 n 为素数时 $\phi(n) = n - 1$；当 n 为合数时，$\phi(n) < n - 1$.

例 1.5.1

给定正整数 $n, n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 为 n 的素因子分解式，求欧拉函数的值 $\phi(n)$.

解

我们利用包含排斥原理(定理??)给出欧拉函数的计算公式. 对于给定的正整数 n 及其素因子分解式 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

令 $A_i = \{x | 1 \leqslant x \leqslant n$且 p_i 整除 $x\}$, 那么 $\phi(n) = |\bar{A}_1 \cap \bar{A}_2 \cap \cdots \bar{A}_k|$.

例1.5.1(续)

下面计算定理??中等式右边的各项.

$$|A_i| = \frac{n}{p_i}, i = 1, 2, \cdots, k,$$

$$|A_i \cap A_j| = \frac{n}{p_i p_j}, 1 \leqslant i < j \leqslant n,$$

$$\cdots$$

根据包含排斥原理,

$$\begin{aligned}\phi(n) &= |\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_k| \\ &= n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k}\right) + \left(\frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \cdots + \frac{n}{p_{k-1} p_k}\right) \\ &\quad - \cdots + (-1)^k \frac{n}{p_1 p_2 \cdots p_k} \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).\end{aligned}$$

例1.5.1(续)

下面计算定理??中等式右边的各项.

$$|A_i| = \frac{n}{p_i}, i = 1, 2, \cdots, k,$$

$$|A_i \cap A_j| = \frac{n}{p_i p_j}, 1 \leqslant i < j \leqslant n,$$

$$\cdots$$

根据包含排斥原理,

$$\begin{aligned}\phi(n) &= |\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_k| \\ &= n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots + \frac{n}{p_k}\right) + \left(\frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \cdots + \frac{n}{p_{k-1} p_k}\right) \\ &\quad - \cdots + (-1)^k \frac{n}{p_1 p_2 \cdots p_k} \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

例如, $60 = 2^2 \cdot 3 \cdot 5$, 有

$\phi(60) = 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 60 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 16.$

欧拉定理

定理 1.5.1

设 a 与 n 互素，则 $a^{\phi(n)} \equiv 1 \pmod{n}$.

欧拉定理

定理 1.5.1

设 a 与 n 互素，则 $a^{\phi(n)} \equiv 1 \pmod{n}$.

证明.

设 $r_1, r_2, \cdots, r_{\phi(n)}$ 是 $\{1, 2, \cdots, n\}$ 中与 n 互素的 $\phi(n)$ 个数. 由于 a 与 n 互素，对每一个 $1 \leqslant i \leqslant \phi(n)$, ar_i 也与 n 互素，故存在 $1 \leqslant \tau(i) \leqslant \phi(n)$ 使得 $ar_i \equiv r_{\tau(i)} \pmod{n}$. τ 是 $\{1, 2, \cdots, \phi(n)\}$ 上的一个映射. 要证 τ 是一个单射，即当 $i \neq j$ 时，$\tau(i) \neq \tau(j)$.

由定理 1.4.2，a 的模 n 逆 a^{-1} 存在. 显然，a^{-1} 也与 n 互素. 当 $i \neq j$ 时，假设 $\tau(i) = \tau(j)$，则有 $ar_i \equiv ar_j \pmod{n}$. 由命题1.3.2(4)，两边同乘 a^{-1} ，得 $r_i \equiv r_j \pmod{n}$，矛盾. 得证 τ 是 $\{1, 2, \cdots, \phi(n)\}$ 上的单射，当然它也是 $\{1, 2, \cdots, \phi(n)\}$ 上的双射. 从而，有

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} ar_i \equiv \prod_{i=1}^{\phi(n)} r_i \pmod{n}.$$

而 $\prod_{i=1}^{\phi(n)} r_i$ 与 n 互素，故 $a^{\phi(n)} \equiv 1 \pmod{n}$. □

费马小定理

当 p 为素数时，$\phi(p) = p - 1$. 于是，得到下述定理.

定理 1.5.2

设 p 是素数，a 与 p 互素，则

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.5.1}$$

定理的另一种形式是，设 p 是素数，则对任意的整数 a，

$$a^{p} \equiv a \pmod{p}. \tag{1.5.2}$$

费马小定理

当 p 为素数时，$\phi(p) = p - 1$. 于是，得到下述定理.

定理 1.5.2

设 p 是素数，a 与 p 互素，则

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.5.1}$$

定理的另一种形式是，设 p 是素数，则对任意的整数 a，

$$a^{p} \equiv a \pmod{p}. \tag{1.5.2}$$

当 a 与 p 互素时，由命题1.3.2(4)知，式 (1.5.1) 与式 (1.5.2) 等价. 当 a 与 p 不互素时，必有 $p \mid a$，从而 $a \equiv 0 \pmod{p}$，式 (1.5.2) 自然成立.

费马小定理

当 p 为素数时，$\phi(p) = p - 1$. 于是，得到下述定理.

定理 1.5.2

设 p 是素数，a 与 p 互素，则

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.5.1}$$

定理的另一种形式是，设 p 是素数，则对任意的整数 a，

$$a^{p} \equiv a \pmod{p}. \tag{1.5.2}$$

当 a 与 p 互素时，由命题1.3.2(4)知，式 (1.5.1) 与式 (1.5.2) 等价. 当 a 与 p 不互素时，必有 $p \mid a$，从而 $a \equiv 0 \pmod{p}$，式 (1.5.2) 自然成立.

费马小定理提供了一种不用因子分解就能确认一个数是合数的新途径. 例如，考虑 9(假设不知道它是合数)，取 $a = 2$，计算

$$2^{9-1} \equiv 4 \pmod{9}.$$

由费马小定理，可以断定 9 是合数. 但是，这里没有提供对 9 如何进行因子分解的任何信息.

4.6 均匀伪随机数的产生方法

最基本的伪随机数是服从 $(0,1)$ 上均匀分布的伪随机数，服从其他分布的伪随机数可以利用 $(0,1)$ 上均匀分布的伪随机数产生.

4.6 均匀伪随机数的产生方法

最基本的伪随机数是服从 $(0,1)$ 上均匀分布的伪随机数，服从其他分布的伪随机数可以利用 $(0,1)$ 上均匀分布的伪随机数产生.

最常用的产生 $(0,1)$ 上均匀分布伪随机数的方法是 线性同余法 .

选择 4 个非负整数：模数 m、乘数 a、常数 c 和种子数 x_0，其中 $2 \leqslant a < m$, $0 \leqslant c < m$, $0 \leqslant x_0 < m$，按照下述递推公式产生伪随机数序列：

$$x_n = (ax_{n-1} + c) \mod m, \quad n = 1, 2, \cdots. \tag{1.6.1}$$

4.6 均匀伪随机数的产生方法

最基本的伪随机数是服从 $(0,1)$ 上均匀分布的伪随机数，服从其他分布的伪随机数可以利用 $(0,1)$ 上均匀分布的伪随机数产生.

最常用的产生 $(0,1)$ 上均匀分布伪随机数的方法是 线性同余法 .

选择 4 个非负整数：模数 m、乘数 a、常数 c 和种子数 x_0，其中 $2 \leqslant a < m$, $0 \leqslant c < m$, $0 \leqslant x_0 < m$，按照下述递推公式产生伪随机数序列：

$$x_n = (ax_{n-1} + c) \mod m, \quad n = 1, 2, \cdots. \tag{1.6.1}$$

为了得到 $(0,1)$ 上均匀分布伪随机数，取

$$u_n = x_n/m, \quad n = 1, 2, \cdots. \tag{1.6.2}$$

4.6 均匀伪随机数的产生方法

最基本的伪随机数是服从 $(0,1)$ 上均匀分布的伪随机数，服从其他分布的伪随机数可以利用 $(0,1)$ 上均匀分布的伪随机数产生.

最常用的产生 $(0,1)$ 上均匀分布伪随机数的方法是 线性同余法 .

选择 4 个非负整数：模数 m、乘数 a、常数 c 和种子数 x_0，其中 $2 \leqslant a < m$, $0 \leqslant c < m$, $0 \leqslant x_0 < m$，按照下述递推公式产生伪随机数序列：

$$x_n = (ax_{n-1} + c) \mod m, \quad n = 1, 2, \cdots. \tag{1.6.1}$$

为了得到 $(0,1)$ 上均匀分布伪随机数，取

$$u_n = x_n/m, \quad n = 1, 2, \cdots. \tag{1.6.2}$$

种子数 x_0 在计算时随机给出，其他 3 个参数 m, a 和 c 是固定不变的，它们的取值决定了所产生的伪随机数的质量.

均匀伪随机数的产生方法(续)

式 (1.6.1) 至多能产生 m 个不同的数,因此得到的序列一定会出现循环,即存在正整数 n_0 和 l,使得所有的 $n \geqslant n_0$ 都有 $x_{n+l} = x_n$. 使得上式成立的最小正整数 l 称作该序列的周期.

均匀伪随机数的产生方法(续)

式 (1.6.1) 至多能产生 m 个不同的数,因此得到的序列一定会出现循环,即存在正整数 n_0 和 l,使得所有的 $n \geqslant n_0$ 都有 $x_{n+l} = x_n$. 使得上式成立的最小正整数 l 称作该序列的周期.

例如,取 $m = 8, a = 3, c = 1, x_0 = 2$,由式 (1.6.1) 得到 $7, 6, 3, 2, 7, 6, \cdots$. 这个序列的周期等于 4.

若保持 $m = 8, c = 1, x_0 = 2$ 不变,把 a 改为 $a = 5$,则得到 $3, 0, 1, 6, 7, 4, 5, 2, 3, 0, 1, \cdots$,周期为 8.

显然,伪随机数序列的周期越长越好.

均匀伪随机数的产生方法(续)

式 (1.6.1) 至多能产生 m 个不同的数,因此得到的序列一定会出现循环,即存在正整数 n_0 和 l,使得所有的 $n \geqslant n_0$ 都有 $x_{n+l} = x_n$. 使得上式成立的最小正整数 l 称作该序列的周期.

例如,取 $m = 8, a = 3, c = 1, x_0 = 2$,由式 (1.6.1) 得到 $7, 6, 3, 2, 7, 6, \cdots$. 这个序列的周期等于 4.

若保持 $m = 8, c = 1, x_0 = 2$ 不变,把 a 改为 $a = 5$,则得到 $3, 0, 1, 6, 7, 4, 5, 2, 3, 0, 1, \cdots$,周期为 8.

显然,伪随机数序列的周期越长越好.

此外,若取 $a = 0$ 和 $a = 1$,则分别得到序列

$c, c, c, \cdots$ 和 $x_0 + c, x_0 + 2c, x_0 + 3c, \cdots$.

这 2 个序列根本无随机性可言,因而总限定 $a \geqslant 2$.

均匀伪随机数的产生方法(续)

式 (1.6.1) 至多能产生 m 个不同的数,因此得到的序列一定会出现循环,即存在正整数 n_0 和 l,使得所有的 $n \geqslant n_0$ 都有 $x_{n+l} = x_n$. 使得上式成立的最小正整数 l 称作该序列的周期.

例如,取 $m = 8, a = 3, c = 1, x_0 = 2$,由式 (1.6.1) 得到 $7, 6, 3, 2, 7, 6, \cdots$. 这个序列的周期等于 4.

若保持 $m = 8, c = 1, x_0 = 2$ 不变,把 a 改为 $a = 5$,则得到 $3, 0, 1, 6, 7, 4, 5, 2, 3, 0, 1, \cdots$,周期为 8.

显然,伪随机数序列的周期越长越好.

此外,若取 $a = 0$ 和 $a = 1$,则分别得到序列

$c, c, c, \cdots$ 和 $x_0 + c, x_0 + 2c, x_0 + 3c, \cdots$.

这 2 个序列根本无随机性可言,因而总限定 $a \geqslant 2$.

实际上,采用不同的参数得到的伪随机数序列的随机性是不同的,因此要想得到满意的伪随机数,必须选取一组好的参数 m, a 和 c.

取 $c = 0$, 式 (1.6.1) 简化为

$$x_n = ax_{n-1} \mod m, \quad n = 1, 2, \cdots, \tag{1.6.3}$$

称作乘同余法. 采用乘同余法时, 显然不能取 $x_0 = 0$.

取 $c = 0$, 式 (1.6.1) 简化为

$$x_n = ax_{n-1} \mod m, \quad n = 1, 2, \cdots, \tag{1.6.3}$$

称作乘同余法. 采用乘同余法时, 显然不能取 $x_0 = 0$.

取 $m = 2^{31} - 1, a = 7^5$ 的乘同余法是最常用的均匀伪随机数发生器, 它的周期是 $2^{31} - 2$. 取种子数 $x_0 = 1$, 得到伪随机数如下.

x_n	u_n
16 807	0.000 007 826
282 475 249	0.131 537 788
1 622 650 073	0.755 605 322
984 943 658	0.458 650 131
1 144 108 930	0.532 767 237
470 211 272	0.218 959 186
101 027 544	0.047 044 616
1 457 850 878	0.678 864 716
⋮	⋮

4.7 RSA 公钥密码

早在公元前，罗马皇帝恺撒(J. Caesar)就已经使用密码传递作战命令. 他的加密方法是把每个字母按照字母表的顺序向后移动 3 位，最后 3 个字母依次变成前 3 个字母. 例如，“take action at middle night”，经过加密变成“wdnhdfwlrqdwplqqohqljkw”(忽略掉空格).

4.7 RSA 公钥密码

早在公元前，罗马皇帝恺撒(J. Caesar)就已经使用密码传递作战命令. 他的加密方法是把每个字母按照字母表的顺序向后移动 3 位，最后 3 个字母依次变成前 3 个字母. 例如，“take action at middle night”，经过加密变成“wdnhdfwlrqdwplqqohqljkw”(忽略掉空格).

所谓 密码，简单地说就是一组含有参数 k 的变换 E. 信息 m 通过变换 E 得到 $c = E(m)$. 原始信息 m 称作 明文，经过变换得到的信息 c 称作 密文. 从明文得到密文的过程称作 加密，变换 E 称作 加密算法，参数 k 称作 密钥. 同一个加密算法，可以取不同密钥，给出不同的加密结果.

4.7 RSA 公钥密码

凯撒的加密算法是把字母按照字母表的顺序循环移动 k 位，用数字 0–25 分别表示 26 个字母，这个算法可表示成 $E(i) = (i + k) \mod 26, \quad i = 0, 1, \cdots, 25,$ 其中密钥 k 是任意的整数. 例如，“take action at middle night”数字化后为

$$19\ 0\ 10\ 4\ 0\ 2\ 19\ 8\ 14\ 13\ 0\ 19\ 12\ 8\ 3\ 3\ 11\ 4\ 13\ 8\ 6\ 7\ 19$$

4.7 RSA 公钥密码

凯撒的加密算法是把字母按照字母表的顺序循环移动 k 位，用数字 0–25 分别表示 26 个字母，这个算法可表示成 $E(i) = (i + k) \mod 26, \quad i = 0, 1, \cdots, 25,$ 其中密钥 k 是任意的整数. 例如，“take action at middle night”数字化后为

$$19\ 0\ 10\ 4\ 0\ 2\ 19\ 8\ 14\ 13\ 0\ 19\ 12\ 8\ 3\ 3\ 11\ 4\ 13\ 8\ 6\ 7\ 19$$

取 $k = 3$，加密后得到密文

$$22\ 3\ 13\ 7\ 3\ 5\ 22\ 11\ 17\ 16\ 3\ 22\ 15\ 11\ 6\ 6\ 14\ 7\ 16\ 11\ 9\ 10\ 22$$

4.7 RSA 公钥密码

凯撒的加密算法是把字母按照字母表的顺序循环移动 k 位，用数字 0–25 分别表示 26 个字母，这个算法可表示成 $E(i) = (i + k) \mod 26, \quad i = 0, 1, \cdots, 25,$ 其中密钥 k 是任意的整数. 例如，“take action at middle night”数字化后为

$$19\ 0\ 10\ 4\ 0\ 2\ 19\ 8\ 14\ 13\ 0\ 19\ 12\ 8\ 3\ 3\ 11\ 4\ 13\ 8\ 6\ 7\ 19$$

取 $k = 3$，加密后得到密文

$$22\ 3\ 13\ 7\ 3\ 5\ 22\ 11\ 17\ 16\ 3\ 22\ 15\ 11\ 6\ 6\ 14\ 7\ 16\ 11\ 9\ 10\ 22$$

从密文 c 恢复明文 m 的过程称作 解密 . 解密算法 D 是加密算法 E 的逆运算. 解密算法也含有参数，称作解密算法的 密钥 . 凯撒密码的解密算法是

$$D(i) = (i - k) \mod 26, \quad i = 0, 1, \cdots, 25.$$

它的解密算法的密钥与加密算法的密钥相同.

密码要求加密算法 E 是容易计算的. 只要知道密钥,解密算法 D 的计算也是容易的. 关键之处是,如果不知道密钥,就不可能(至少是很难)从密文 c 恢复明文 m. 恺撒密码的加密算法太简单. 如果有足够长的密文,通过统计各个字母以及字母之间关联出现的频率就可以破解出密钥,因此恺撒密码是不安全的.

密码要求加密算法 E 是容易计算的. 只要知道密钥,解密算法 D 的计算也是容易的. 关键之处是,如果不知道密钥,就不可能(至少是很难)从密文 c 恢复明文 m. 恺撒密码的加密算法太简单. 如果有足够长的密文,通过统计各个字母以及字母之间关联出现的频率就可以破解出密钥,因此恺撒密码是不安全的.

这种类型的稍微复杂一点的加密算法是

$$E(i) = (ai + b) \mod 26, \quad i = 0, 1, \cdots, 25,$$

其中 $a, b \in \mathbb{Z}$. 为了保证 E 是双射,a 应满足一定的条件(见习题 4.48).

密码要求加密算法 E 是容易计算的. 只要知道密钥,解密算法 D 的计算也是容易的. 关键之处是,如果不知道密钥,就不可能(至少是很难)从密文 c 恢复明文 m. 恺撒密码的加密算法太简单. 如果有足够长的密文,通过统计各个字母以及字母之间关联出现的频率就可以破解出密钥,因此恺撒密码是不安全的.
这种类型的稍微复杂一点的加密算法是

$$E(i) = (ai + b) \mod 26, \quad i = 0, 1, \cdots, 25,$$

其中 $a, b \in \mathbb{Z}$. 为了保证 E 是双射,a 应满足一定的条件(见习题 4.48).
用一个字母代替另一个字母的密码很容易被分析字母频率的方法破译. 更复杂一些的加密算法是用一段字母代替另一段字母. 例如,维吉利亚(Vigenere)密码先把明文分成若干段,每一段有 n 个数字,密钥 $k = k_1 k_2 \cdots k_n$,加密算法

$$E(m_1 m_2 \cdots m_n) = c_1 c_2 \cdots c_n,$$

其中 $c_i = (m_i + k_i) \mod 26, m_i = 0, 1, \cdots, 25, i = 1, 2, \cdots, n.$

密码要求加密算法 E 是容易计算的. 只要知道密钥,解密算法 D 的计算也是容易的. 关键之处是,如果不知道密钥,就不可能(至少是很难)从密文 c 恢复明文 m. 恺撒密码的加密算法太简单. 如果有足够长的密文,通过统计各个字母以及字母之间关联出现的频率就可以破解出密钥,因此恺撒密码是不安全的.
这种类型的稍微复杂一点的加密算法是

$$E(i) = (ai + b) \mod 26, \quad i = 0, 1, \cdots, 25,$$

其中 $a, b \in \mathbb{Z}$. 为了保证 E 是双射,a 应满足一定的条件(见习题 4.48).
用一个字母代替另一个字母的密码很容易被分析字母频率的方法破译. 更复杂一些的加密算法是用一段字母代替另一段字母. 例如,维吉利亚(Vigenere)密码先把明文分成若干段,每一段有 n 个数字,密钥 $k = k_1 k_2 \cdots k_n$,加密算法

$$E(m_1 m_2 \cdots m_n) = c_1 c_2 \cdots c_n,$$

其中 $c_i = (m_i + k_i) \mod 26, m_i = 0, 1, \cdots, 25, i = 1, 2, \cdots, n.$
传统密码的密钥是对称的,只要知道加密密钥就能推算出解密密钥. 通信双方分别持有加密密钥和解密密钥,密钥对外是绝对保密的,必须通过秘密渠道传送. 这种密码称作私钥密码.

公钥密码思想

随着计算机网络的迅速发展，私钥密码已不能适应计算机网络通信的保密需要.

- 私钥密码的密钥不能用网络传送. 为了确保安全，应定期更新密钥，密钥的传送需要使用另外的秘密渠道，极不方便.
- 一对密钥只能供一对通信的双方使用，而不能多方共用. 假设某人要与 n 个用户进行保密通信，就需要保存 n 个加密密钥和 n 个解密密钥. n 个用户之间进行保密通信需要 $\binom{n}{2}$ 对密钥.

公钥密码思想

随着计算机网络的迅速发展，私钥密码已不能适应计算机网络通信的保密需要.

- 私钥密码的密钥不能用网络传送. 为了确保安全，应定期更新密钥，密钥的传送需要使用另外的秘密渠道，极不方便.
- 一对密钥只能供一对通信的双方使用，而不能多方共用. 假设某人要与 n 个用户进行保密通信，就需要保存 n 个加密密钥和 n 个解密密钥. n 个用户之间进行保密通信需要 $\binom{n}{2}$ 对密钥.

迪菲(W. Diffie)和赫尔曼(M. Hellman)于 1976 年提出了公钥密码的思想. 这种密码的密钥是非对称的，也就是说，不能从加密密钥推算出解密密钥，因而加密密钥不需要保密，可以公开，而只需保守解密密钥的秘密.
甲将他的加密密钥公布，任何想与甲通信的人都可以使用这个加密密钥将要传送的信息(明文)加密成密文发送给甲. 只有甲自己知道解密密钥，能够把密文还原为明文. 任何第三方即使截获到密文也不可能知道密文所传送的信息.

RSA 公钥密码

RSA 公钥密码是李维斯特(R. Rivest)、萨莫尔(A. Shamir)和阿德曼(L. Adleman)于 1978 年提出的,也是目前使用最广泛的公钥密码算法.
它的基础是欧拉定理(定理 1.5.1),它的安全性依赖于大数因子分解的困难性.

RSA 公钥密码

RSA 公钥密码是李维斯特(R. Rivest)、萨莫尔(A. Shamir)和阿德曼(L. Adleman)于 1978 年提出的,也是目前使用最广泛的公钥密码算法.

它的基础是欧拉定理(定理 1.5.1),它的安全性依赖于大数因子分解的困难性.

取两个不相等的大素数 p 和 q,记 $n = pq$,由例 1.5.1知, $\phi(n) = (p-1)(q-1)$.

选择正整数 w, w 与 $\phi(n)$ 互素,设 d 是 w 的模 $\phi(n)$ 逆,即 $dw \equiv 1 \pmod{\phi(n)}$.

RSA 公钥密码

RSA 公钥密码是李维斯特(R. Rivest)、萨莫尔(A. Shamir)和阿德曼(L. Adleman)于 1978 年提出的,也是目前使用最广泛的公钥密码算法.

它的基础是欧拉定理(定理 1.5.1),它的安全性依赖于大数因子分解的困难性.

取两个不相等的大素数 p 和 q,记 $n = pq$,由例 1.5.1知, $\phi(n) = (p-1)(q-1)$.

选择正整数 w, w 与 $\phi(n)$ 互素,设 d 是 w 的模 $\phi(n)$ 逆,即 $dw \equiv 1 \pmod{\phi(n)}$.

RSA 密码算法如下:首先将明文数字化,然后把明文分成若干段,每一个明文段的值均小于 n. 对每一个明文段 m,

加密算法 $\quad c = E(m) = m^w \mod n$,

解密算法 $\quad D(c) = c^d \mod n$,

其中加密密钥 w 和 n 是公开的,p、q、$\phi(n)$ 和 d 是保密的.

下面证明解密算法是正确的，即 $m = c^d \mod n$.

由于 $m < n$，故只需证明 $c^d \equiv m \pmod{n}$，亦即 $m^{dw} \equiv m \pmod{n}$. 因为 $dw \equiv 1 \pmod{\phi(n)}$，所以存在整数 k 使得 $dw = k\phi(n) + 1$. 分两种情形讨论如下.

下面证明解密算法是正确的，即 $m = c^d \mod n$.

由于 $m < n$，故只需证明 $c^d \equiv m \pmod n$，亦即 $m^{dw} \equiv m \pmod n$. 因为 $dw \equiv 1 \pmod{\phi(n)}$，所以存在整数 k 使得 $dw = k\phi(n) + 1$. 分两种情形讨论如下.

(1) m 与 n 互素. 由欧拉定理 $m^{\phi(n)} \equiv 1 \pmod n$ 即可得到 $m^{dw} \equiv m^{k\phi(n)+1} \equiv m \pmod n$.

下面证明解密算法是正确的，即 $m = c^d \mod n$.

由于 $m < n$，故只需证明 $c^d \equiv m \pmod n$，亦即 $m^{dw} \equiv m \pmod n$. 因为 $dw \equiv 1 \pmod{\phi(n)}$，所以存在整数 k 使得 $dw = k\phi(n) + 1$. 分两种情形讨论如下.

(1) m 与 n 互素. 由欧拉定理 $m^{\phi(n)} \equiv 1 \pmod n$ 即可得到 $m^{dw} \equiv m^{k\phi(n)+1} \equiv m \pmod n$.

(2) m 与 n 不互素. 由于 $m < n, n = pq, p$ 和 q 是素数且 $p \neq q$，故 m 必含 p 和 q 中的一个为因子，且只含其中的一个为因子. 不妨设 $m = cp$ 且 $q \nmid m$. 由费马小定理有 $m^{q-1} \equiv 1 \pmod q$. 于是，

$$m^{k\phi(n)} \equiv m^{k(p-1)(q-1)} \equiv 1^{k(p-1)} \equiv 1 \pmod q.$$

从而存在整数 h 使得 $m^{k\phi(n)} = hq + 1$. 两边同乘以 m，并注意到 $m = cp$，得

$$m^{k\phi(n)+1} = hcpq + m = hcn + m.$$

得证 $m^{k\phi(n)+1} \equiv m \pmod n$, 即

$$m^{dw} \equiv m \pmod n.$$

模幂乘运算

RSA 公钥密码的加密算法和解密算法都要做模幂乘运算 $a^b \mod n$.

模幂乘运算

RSA 公钥密码的加密算法和解密算法都要做模幂乘运算 $a^b \mod n$.

设 b 的二进制表示为 $b_{r-1} \cdots b_1 b_0$，即

$$b = b_0 + b_1 \times 2 + \cdots + b_{r-1} \times 2^{r-1}.$$

模幂乘运算

RSA 公钥密码的加密算法和解密算法都要做模幂乘运算 $a^b \mod n$.

设 b 的二进制表示为 $b_{r-1} \cdots b_1 b_0$，即

$$b = b_0 + b_1 \times 2 + \cdots + b_{r-1} \times 2^{r-1}.$$

于是，

$$a^b \equiv a^{b_0} \times (a^2)^{b_1} \times \cdots \times (a^{2^{r-1}})^{b_{r-1}} \pmod{n}.$$

模幂乘运算

RSA 公钥密码的加密算法和解密算法都要做模幂乘运算 $a^b \mod n$.

设 b 的二进制表示为 $b_{r-1}\cdots b_1 b_0$, 即

$$b = b_0 + b_1 \times 2 + \cdots + b_{r-1} \times 2^{r-1}.$$

于是,

$$a^b \equiv a^{b_0} \times (a^2)^{b_1} \times \cdots \times (a^{2^{r-1}})^{b_{r-1}} \pmod{n}.$$

令 $A_0 = a, A_i \equiv (A_{i-1})^2 \pmod{n}, i = 1, 2, \cdots, r-1$, 则有

$$a^b \equiv A_0^{b_0} \times A_1^{b_1} \times \cdots \times A_{r-1}^{b_{r-1}} \pmod{n},$$

这里

$$A_i^{b_i} = \begin{cases} A_1, & \text{若 } b_i = 1, \\ 1, & \text{若 } b_i = 0, \end{cases} \quad i = 0, 1, \cdots, r-1.$$

例 1.8.1

取 $p = 43, q = 59, n = 43 \times 59 = 2\ 537, \phi(n) = 42 \times 58 = 2\ 436, w = 13.$

a, *b*, $\cdots$, *z* **依次用** 00, 01, $\cdots$, 25 **表示, 各占** 2 **位.**

设明文段 $m = 2\ 106$, **即** *vg.* **密文** $c = 2\ 106^{13} \bmod 2\ 537.$

计算如下: *13* **的二进制表示为** *1101*, **即** $13 = 1 + 2^2 + 2^3.$

$$
\begin{aligned}
&A_0 = 2\ 106 \equiv -431 \pmod{2\ 537},\\
&A_1 \equiv (-431)^2 \equiv 560 \pmod{2\ 537},\\
&A_2 \equiv 560^2 \equiv -988 \pmod{2\ 537},\\
&A_3 \equiv (-988)^2 \equiv -601 \pmod{2\ 537},\\
&2\ 106^{13} \equiv (-431) \times (-988) \times (-601) \equiv 2\ 321 \pmod{2\ 537},
\end{aligned}
$$

得密文 $c = 2\ 321.$

例1.8.1(续)

又设收到密文 0981，**要把它恢复成明文. 计算** $13^{-1} \equiv 937 \pmod{2\ 436}$，**得** $d = 937$. **明文** $m' = 981^{937} \mod 2\ 537$. **计算如下**：

937 **的二进制表示为** 1110101001，**即** $937 = 1 + 2^3 + 2^5 + 2^7 + 2^8 + 2^9$.

$$A_0 = 981,\ A_1 \equiv 981^2 \equiv 838 \pmod{2\ 537},\ A_2 \equiv 838^2 \equiv -505 \pmod{2\ 537},$$
$$A_3 \equiv (-505)^2 \equiv 1\ 325 \pmod{2\ 537}, A_4 \equiv 1\ 325^2 \equiv 21 \pmod{2\ 537},$$
$$A_5 \equiv 21^2 \equiv 441 \pmod{2\ 537}, A_6 \equiv 441^2 \equiv -868 \pmod{2\ 537},$$
$$A_7 \equiv (-868)^2 \equiv -65 \pmod{2\ 537}, A_8 \equiv (-65)^2 \equiv -849 \pmod{2\ 537},$$
$$A_9 \equiv (-849)^2 \equiv 293 \pmod{2\ 537},$$
$$981^{937} \equiv 981 \times 1\ 325 \times 441 \times (-65) \times (-849) \times 293 \equiv 704 \pmod{2\ 537},$$

得明文 $m' = 0704$，**即** he. □

例1.8.1(续)

又设收到密文 0981，要把它恢复成明文. 计算 $13^{-1} \equiv 937 \pmod{2\ 436}$，得 $d = 937$. 明文 $m' = 981^{937} \mod 2\ 537$. 计算如下：

937 的二进制表示为 1110101001，即 $937 = 1 + 2^3 + 2^5 + 2^7 + 2^8 + 2^9$.

$$A_0 = 981,\ A_1 \equiv 981^2 \equiv 838 \pmod{2\ 537},\ A_2 \equiv 838^2 \equiv -505 \pmod{2\ 537},$$
$$A_3 \equiv (-505)^2 \equiv 1\ 325 \pmod{2\ 537}, A_4 \equiv 1\ 325^2 \equiv 21 \pmod{2\ 537},$$
$$A_5 \equiv 21^2 \equiv 441 \pmod{2\ 537}, A_6 \equiv 441^2 \equiv -868 \pmod{2\ 537},$$
$$A_7 \equiv (-868)^2 \equiv -65 \pmod{2\ 537}, A_8 \equiv (-65)^2 \equiv -849 \pmod{2\ 537},$$
$$A_9 \equiv (-849)^2 \equiv 293 \pmod{2\ 537},$$
$$981^{937} \equiv 981 \times 1\ 325 \times 441 \times (-65) \times (-849) \times 293 \equiv 704 \pmod{2\ 537},$$

得明文 $m' = 0704$，即 he. □

RSA 公钥密码的安全性依赖于大整数分解的困难性. 如果已知分解式 $n = pq$，那么容易计算出 w 的模 $\phi(n) = (p-1)(q-1)$ 逆 d. 现在还没有在不知道分解式 $n = pq$ 的情况下解密的方法.