初等数论

Charles

2023 年 2 月

目录

1 整除 **1**

1.1 整除与带余除法 1

1.1.1 整除的定义与性质 1

1.1.2 带余除法 2

1.2 最大公因数与辗转相除法 2

1.2.1 最大公因数 2

1.2.2 辗转相除法 3

1.2.3 Bézout 等式 4

1.2.4 最大公因数的性质 4

1.2.5 最小公倍数 6

1.3 不定方程 1: 一次不定方程 7

1.3.1 一元一次不定方程 $ax + by = (a, b)$ 8

1.3.2 一元一次不定方程 $ax + by = c$ 9

1.3.3 多元一次不定方程 10

1.4 素数与算术基本定理 12

1.4.1 素数 12

1.4.2 算术基本定理 13

1.4.3 素数无穷多 14

1.4.4 梅森素数与完全数 15

2 同余 **19**

2.1 同余与同余类 19

2.1.1 同余的概念与性质 19

2.1.2 同余类与同余类环 21

2.2 同余方程 1: 一次同余方程 23

2.2.1 线性同余方程 23

2.2.2 线性同余方程组与中国剩余定理 24

2.3 费马小定理与欧拉公式 . . . 25
2.3.1 费马小定理 . . . 25
2.3.2 欧拉函数 . . . 27
2.3.3 欧拉公式 . . . 30
2.4 同余方程 2: 高次同余方程 . . . 31
2.4.1 模 p 多项式的根数 . . . 31
2.4.2 高次同余方程的解数及解法 . . . 33
2.5 模 m 的幂与根 . . . 35
2.5.1 模 m 的幂与逐次平方法 . . . 35
2.5.2 模 m 的 k 次根 . . . 37
2.6 素性测试与卡米歇尔数 . . . 38
2.6.1 卡米歇尔数 . . . 38
2.6.2 拉宾-米勒测试 . . . 40

3 高次同余方程的进一步研究 42
3.1 平方剩余 . . . 42
3.1.1 模 p 平方剩余 . . . 42
3.1.2 勒让德符号 . . . 44
3.1.3 欧拉准则 . . . 44
3.2 二次互反律 . . . 45
3.2.1 $\left(\frac{-1}{p}\right)$ 与 $\left(\frac{2}{p}\right)$ . . . 45
3.2.2 二次互反律及其应用 . . . 48
3.2.3 二次互反律的证明 . . . 52
3.3 原根与指标 . . . 52
3.3.1 模 p 原根 . . . 52
3.3.2 指标 . . . 52

4 高次不定方程 55
4.1 勾股数 . . . 55
4.1.1 勾股数组 . . . 55
4.1.2 将整数表示成两数平方和 . . . 56
4.2 佩尔方程 . . . 58
4.2.1 三角平方数 . . . 58
4.2.2 佩尔方程 . . . 59

Chapter 1

整除

1.1 整除与带余除法

1.1.1 整除的定义与性质

定义 1.1.1 (整除) 设 a, b 均为整数, $b \neq 0$. 若存在整数 q 使得

$$a = bq,$$

则称 b **整除** a, 记为 $b \mid a$; 且称 b 是 a 的**因数** (factor, divisor), a 是 b 的**倍数** (multiple). 反之, 如果不存在整数 q 使得 $a = bq$, 则称 b 不整除 a, 记为 $b \nmid a$.

从定义中能看出, 任意非零整数 b 整除 0, 因为 $0 = b \cdot 0$.

定理 1.1.2 (整除的性质) (i) $a \mid b \iff -a \mid b \iff a \mid -b \iff |a| \mid |b|$;
(ii) $a \mid b$ 且 $b \mid c \Longrightarrow a \mid c$;
(iii) $a \mid b$ 且 $a \mid c \iff$ 对任意的 $x, y \in \mathbb{Z}$, 有 $a \mid bx + cy$;
一般地, $a \mid b_1, \cdots, a \mid b_k$ 同时成立 $\iff$ 对任意的 $x_1, \cdots, x_k \in \mathbb{Z}$, 有 $a \mid (b_1x_1 + \cdots + b_kx_k)$;
特别地, $a \mid b$ 且 $a \mid c$ 则 $a \mid b \pm c$, $a \mid b + c$ 且 $a \mid b$ 则 $a \mid (b + c) - b = c$;
(iv) 设 $m \neq 0$, 那么 $a \mid b \iff ma \mid mb$;
(v) $a \mid b$ 且 $b \mid a \Longrightarrow b = \pm a$;
(vi) 设 $b \neq 0$, 那么 $a \mid b \Longrightarrow |a| \leqslant |b|$;

证 (i) $b = aq \iff b = (-a)(-q) \iff -b = a(-q) \iff |b| = |a||q|$.
(ii) 由 $b = aq_1$ 和 $c = bq_2$ 可推出 $c = a\,(q_1q_2)$.
(iii) (必要性) 由 $b = aq_1$, $c = aq_2$ 可推出 $bx + cy = a\,(q_1x + q_2y)$;
(充分性) 取 $x = 1, y = 0$ 及 $x = 0, y = 1$ 即可.

(iv) 当 $m \neq 0$ 时,

$$b = aq \Longleftrightarrow mb = (ma)q.$$

(v) 由 $b = aq_1$ 和 $a = bq_2$ 可以推出 $a = a(q_1q_2)$, 由此及 $a \neq 0$ 推出 $q_1q_2 = 1$. 所以 $q_1 = \pm 1$.

(vi) 由 (i) 知, 从 $a \mid b$ 可推出 $|b| = |a||q|$. 由 $b \neq 0$ 知 $|q| \geqslant 1$, 所以 $|a| \leqslant |b|$. □

1.1.2 带余除法

定理 1.1.3 (带余除法, Euclidean division) 若 a, b 均为整数, $b \neq 0$, 则存在整数 q 和 r 使得

$$a = bq + r,\ 0 \leqslant r < |b|, \tag{1.1}$$

且 q 和 r 是唯一的.

注 式 (1.1) 中的 r 称为**余数** (remainder), q 称为**不完全商** (quotient), 也称 a 除以 b 等于 q 余 r, 或 a 模 b 余 r.

证 先设 $b > 0$, 取 $q = \lfloor \frac{a}{b} \rfloor$, 令 $r = a - bq$, 则得 $a = bq + r$. 也可考虑整数序列

$$\cdots,\ -3b,\ -2b,\ -b,\ 0,\ b,\ 2b,\ 3b, \cdots$$

(这些整数将实数轴分割为无限多个长为 b 的小段, 则 a 必落在某小段之中, 设落在 qb 与 $(q+1)b$ 之间). 则必存在整数 q 使

$$qb \leqslant a < (q+1)b.$$

令 $r = a - qb$ (即 a 到小段左端点的距离), 则得到 $a = bq + r$ 且 $0 \leqslant r < b$.

当 $b < 0$ 时, 则 $b' = -b > 0$, 故有 $a = (-b)q' + r$ 且 $0 \leqslant r < (-b)$. 令 $q = -q'$, 则 $a = (-b)(-q) + r = bq + r$ 且 $0 \leqslant r < |b|$.

现证 q 和 r 是唯一的. 假若 $a = bq + r = bq_1 + r_1$. 于是 $b(q - q_1) = r_1 - r$, 故

$$b\,|q - q_1| = |r_1 - r|\,.$$

由于 r 及 r_1 都是小于 b 的正数, 所以上式右边是小于 b 的. 如果 $q \neq q_1$ 则上式左边 $\geqslant b$. 矛盾. 因此 $q = q_1$ 而 $r = r_1$. □

1.2 最大公因数与辗转相除法

1.2.1 最大公因数

定义 1.2.1 (最大公因数) 设 $a_1, a_2, \cdots, a_n$ 是 n ($n \geqslant 2$) 个整数. 若整数 d 是它们之中每一个的因数, 那么 d 称为 $a_1, a_2, \cdots, a_n$ 的一个**公因数** (common divisor). 整数 $a_1, a_2, \cdots, a_n$ 的

公因数中最大的一个叫作**最大公因数** (greatest common divisor, gcd), 记作 $\gcd(a_1, a_2, \cdots, a_n)$ 或 $(a_1, a_2, \cdots, a_n)$.

若 $(a_1, a_2, \cdots, a_n) = 1$, 则称 $a_1, a_2, \cdots, a_n$ **互素** (relatively prime, coprime), 若 a_1, a_2, $\cdots$, a_n 中每两个整数互素, 则称它们**两两互素**.

容易看出, 最大公因数一定是正的且是唯一的; $(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$; $(0, b) = |b|$.

根据定义和整除的性质容易得出, 对任意的整数 x, a_1, a_2 的公因数与 a_1, a_2, a_1x 的公因数 (集合) 相等; a_1, a_2 的公因数与 $a_1, a_2 + a_1x$ 的公因数相等, 因此它们的最大公因数也相等.

定理 1.2.2 (i) 对任意的整数 x, $(a_1, a_2) = (a_1, a_2, a_1x)$, 一般地, $(a_1, \cdots, a_k) = (a_1, \cdots, a_k, a_1x)$;

(ii) 对任意整数 x, $(a_1, a_2) = (a_1, a_2 + a_1x)$, 一般地, $(a_1, a_2, a_3, \cdots, a_k) = (a_1, a_2 + a_1x, a_3, \cdots, a_k)$.

1.2.2 辗转相除法

定理 1.2.3 若 $a = bq + r$, 其中 a, b, r 为整数 (a, b 不全为 0), 则

$$(a, b) = (r, b).$$

证 根据定理 1.2.2 (ii), $(a, b) = (a - bq, b) = (r, b)$. □

定理说明, 余数 r 可做原数 a 的 "替身" 去求最大公因数. 我们又可找 b 的替身 r_1 代替 b, 等等. 如此继续, 就是著名的**辗转相除法** (Euclidean algorithm):

$$\begin{aligned}
&a = bq_0 + r_1, && 0 < r_1 < |b|,\\
&b = r_1q_1 + r_2, && 0 < r_2 < r_1,\\
&r_1 = r_2q_2 + r_3, && 0 < r_3 < r_2,\\
&\cdots\cdots\\
&r_{s-2} = r_{s-1}q_{s-1} + r_s, && 0 < r_s < r_{s-1},\\
&r_{s-1} = r_sq_s && (r_{s+1} = 0).
\end{aligned}$$

其中不完全商 q_i 和余数 r_i 都是逐步唯一确定的 (可记 $b = r_0$, $a = r_{-1}$). 因为非负余数 $r_0, r_1, r_2, \cdots$ 逐步减小, 终会为零, 故可设 $r_{s+1} = 0$, 即 $r_s \mid r_{s-1}$. 从前向后看, 即得最大公因数

$$d = (a, b) = (r_1, b) = (r_1, r_2) = \cdots = (r_{s-1}, r_s) = r_s.$$

1.2.3 Bézout 等式

定理 1.2.4 (Bézout (贝祖) 等式, Bézout's identity) 设两整数 a, b ($b \neq 0$) 的最大公因数 $(a, b) = d$, 则存在整数 u, v 使

$$ua + vb = d.$$

证 从后向前看辗转相除法的式子. 首先有

$$r_s = r_{s-2} - r_{s-1}q_{s-1}.$$

而再前一式为 $r_{s-1} = r_{s-3} - r_{s-2}q_{s-2}$, 以此 r_{s-1} 代入上式, 可知 r_s 是 "r_{s-2} 和 r_{s-3} 的整数倍之和". 再前推一式以 r_{s-2} 代入, 可得 r_s 是 "r_{s-3} 和 r_{s-4} 的整数倍之和". 由此不断上推, 最终可得 r_s 是 "a 与 b 的整数倍之和", 即得 Bézout 等式. □

注 u, v 称为 Bézout 系数, 不是唯一的, 例如 $d = ua + vb = (u - 2b)a + (v + 2a)b$.

推论 1.2.5 两整数 a, b 互素当且仅当存在整数 u, v 使

$$ua + vb = 1.$$

证 若 $ua + vb = 1$, 因 (a, b) 整除 a 与 b, 故整除 $1 = ua + vb$, 从而 $(a, b) = 1$. 反之, 若 $(a, b) = 1$, 则由上定理知 $ua + vb = 1$ 成立. □

推论 1.2.6 整数 c 是两整数 a, b 的公因数当且仅当 c 是 a, b 的最大公因数 (a, b) 的因数, 即 $c \mid a$ 且 $c \mid b$ 当且仅当 $c \mid (a, b)$.

证 根据 Bézout 等式, 存在整数 u, v, 使得 $(a, b) = au + bv$. 故若 $c \mid a$ 且 $c \mid b$, 则 $c \mid au + bv = (a, b)$. 反之, 若 $c \mid (a, b)$, 由于 $(a, b) \mid a$, 故 $c \mid a$, 同理 $c \mid b$. □

注 这一结果刻画了最大公因数的本质属性, "最大" 的含义实际上不是指 "大小", 而是指它一定是任一公因数的倍数, 是公因数在整除意义的 "最大". 这可以作为最大公因数的定义, 但这时它的存在性则需证明. 近世代数中可以用这样的方法在一般的整环上定义最大公因子.

对多个数的情形也有 Bézout 等式.

定理 1.2.7 设 $a_1, \cdots, a_s$ 是 s 个非零整数, 记 $(a_1, \cdots, a_s) = d$, 则存在整数 $u_1, \cdots, u_s$ 使得

$$u_1a_1 + \cdots + u_sa_s = d \text{ (Bézout 等式)}.$$

1.2.4 最大公因数的性质

下面是最大公因数的几个常用定理, 可能它们在中小学就是知道且经常应用的, 这里用 Bézout 等式证明.

定理 1.2.8 (i) 设 $m>0$, 则

$$m\left(b_1,\cdots,b_k\right)=\left(mb_1,\cdots,mb_k\right).$$

即若干个数乘以相同的数 $m(m>0)$ 后的最大公因数等于它们的最大公因数乘以 m.

(ii) 设 $(m,a)=1$, 则有 $(m,ab)=(m,b)$. 即求 m 与另一个数的最大公因数时, 可以把另一个数中与 m 互素的因数去掉.

(iii) 设 $(m,a)=1$, 那么, 若 $m\mid ab$, 则 $m\mid b$. 即若一个数被 m 整除, 则把这个数中与 m 互素的因数去掉后仍被 m 整除.

(iv) (推论) 设 $a_1,a_2,\cdots,a_n$ 及 $b_1,b_2,\cdots,b_m$ 是任意两组整数. 若前一组中任一整数与后一组中任一整数互素, 则 $a_1a_2\cdots a_n$ 与 $b_1b_2\cdots b_m$ 互素.

证 (i) 由 Bézout 等式, 可设

$$\begin{aligned}\left(b_1,\cdots,b_k\right)&=b_1y_1+\cdots+b_ky_k,\\ \left(mb_1,\cdots,mb_k\right)&=\left(mb_1\right)x_1+\cdots+\left(mb_k\right)x_k.\end{aligned}$$

根据这两式, 由 $m\left(b_1,\cdots,b_k\right)\mid mb_j(1\leqslant j\leqslant k)$ 推出

$$m\left(b_1,\cdots,b_k\right)\mid\left(mb_1,\cdots,mb_k\right);$$

由 $\left(mb_1,\cdots,mb_k\right)\mid mb_j(1\leqslant j\leqslant k)$, 推出

$$\left(mb_1,\cdots,mb_k\right)\mid\left(mb_1\right)y_1+\cdots+\left(mb_k\right)y_k=m\left(b_1,\cdots,b_k\right).$$

由以上两式, $m\left(b_1,\cdots,b_k\right)=\left(mb_1,\cdots,mb_k\right)$.

(ii) 由 Bézout 等式, 可设

$$\begin{aligned}(m,b)&=mx_1+bx_2,\\ (m,ab)&=my_1+(ab)y_2.\end{aligned}$$

由 $(m,b)\mid m$, $(m,b)\mid b$ 及第二式就推出 $(m,b)\mid(m,ab)$. 由 $(m,a)=1$ 及 Bézout 等式知, 存在 z_1,z_2, 使得

$$mz_1+az_2=1,$$

因而有

$$\begin{aligned}(m,b)&=\left(mx_1+bx_2\right)\left(mz_1+az_2\right)\\ &=m\left(mx_1z_1+ax_1z_2+bx_2z_1\right)+(ab)\left(x_2z_2\right).\end{aligned}$$

由此及 $(m,ab)\mid m$, $(m,ab)\mid ab$ 就推出 $(m,ab)\mid(m,b)$. 所以 $(m,ab)=(m,b)$.

(iii) 由 Bézout 等式及 $(m,a)=1$ 知存在 z_1,z_2, 使得

$$mz_1+az_2=1,$$

所以有 $m\left(bz_1\right)+(ab)z_2=b$. 由此及 $m\mid ab$ 即得 $m\mid b$.

(iv) 因为 $(a_i, b_j) = 1$, 由 (ii), 有

$$\begin{aligned}(a_1a_2\cdots a_n,\, b_j) &= (a_2a_3\cdots a_n,\, b_j)\\ &= \cdots = (a_n,\, b_j) = 1,\ j = 1, 2, \cdots, m.\end{aligned}$$

再用一次 (ii),

$$\begin{aligned}(a_1a_2\cdots a_n,\, b_1b_2\cdots b_m) &= (a_1a_2\cdots a_n,\, b_2b_3\cdots b_m)\\ &= \cdots = (a_1a_2\cdots a_n,\, b_m) = 1.\end{aligned}$$ □

下面的定理说明求若干个数的最大公因数可以归结为求两个数的最大公因数的情形, 求若干个数的最大公因数, 可以先将这些数任意分组, 分别求出各组数的最大公因数, 然后再求这些最大公因数的最大公因数.

定理 1.2.9 (i) $(a_1, a_2, a_3, \cdots, a_k) = ((a_1, a_2), a_3, \cdots, a_k)$;
(ii) $(a_1, \cdots, a_{k-1}, a_k) = ((a_1, \cdots, a_{k-1}), a_k)$;
(iii) $(a_1, \cdots, a_{k+r}) = ((a_1, \cdots, a_k), (a_{k+1}, \cdots, a_{k+r}))$.

证 (i) 由最大公因数的定义, 左边 $\mid a_i$ $(i = 1, 2, \cdots k)$, 从而是 a_1, a_2 的公因数, 进而整除 (a_1, a_2), 所以左边是 $(a_1, a_2), a_3, \cdots, a_k$ 的公因数, 从而左边 $\mid ((a_1, a_2), a_3, \cdots, a_k) =$ 右边. 反之, 右边整除 $(a_1, a_2), a_3, \cdots, a_k$, 因为右边 $\mid (a_1, a_2)$, 所以右边整除 a_1 和 a_2, 所以右边是 $a_1, a_2, a_3, \cdots, a_k$ 的公因数, 从而右边 $\mid (a_1, a_2, a_3, \cdots, a_k) =$ 左边. 所以左边 = 右边.

类似可证 (ii), (iii). □

1.2.5 最小公倍数

定义 1.2.10 (最小公倍数) 设 $a_1, a_2, \cdots, a_n$ 是 n $(n \geqslant 2)$ 个整数. 若 d 是这 n 个数的倍数, 则 d 就叫作这 n 个数的一个**公倍数** (common multiple). 在 $a_1, a_2, \cdots, a_n$ 的一切公倍数中的最小的正数叫作它们的**最小公倍数** (least common multiple, LCM), 记作 $\mathrm{LCM}\,[a_1, a_2, \cdots, a_n]$ 或 $[a_1, a_2, \cdots, a_n]$.

由于任何正数都不是 0 的倍数, 故讨论整数的最小公倍数时, 一概假定这些整数都不是零.
由定义易得, $[a_1, a_2, \cdots, a_n] = [|a_1|, |a_2|, \cdots, |a_n|]$.
与公因数类似, 公倍数一定是最小公倍数的倍数. 这是最小公倍数的本质属性.

定理 1.2.11 c 是 a_j $(1 \leqslant j \leqslant k)$ 的公倍数 $(a_j \mid c)$ 当且仅当 $[a_1, \cdots, a_k] \mid c$.

证 设 m' 是 a, b 的一个公倍数. 由定义可设

$$m' = ak = bk'.$$

在等式 $ak = bk'$ 两边约去 (a, b), 得

$$\frac{a}{(a,b)}k = \frac{b}{(a,b)}k'.$$

所以 $\dfrac{b}{(a,b)} \mid \dfrac{a}{(a,b)}k$, 由于 $\left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)}\right) = 1$, 故 $\dfrac{b}{(a,b)} \mid k$. 因此存在整数 t 使得 $k = t \cdot \dfrac{b}{(a,b)}$, 故

$$m' = t \cdot \frac{ab}{(a,b)}. \tag{1.2}$$

反过来, 当 t 为任一整数时, $\dfrac{ab}{(a,b)}t$ 为 a, b 的一个公倍数, 故 (1.2) 可以表示 a, b 的一切公倍数. 令 $t = 1$ 即得到最小的正数, 故

$$[a,b] = \frac{ab}{(a,b)},$$
$$m' = t \cdot [a,b],\ t \in \mathbb{Z}.$$ □

推论 1.2.12 (最小公倍数与最大公因数的关系) 设 a, b 是任意两个正整数, 则 a, b 的最小公倍数

$$[a,b] = \frac{ab}{(a,b)}.$$

特别地, 若 $(a,b) = 1$, 则 $[a,b] = a \cdot b$.

与最大公因数类似, 求多个数的最小公倍数也可以通过不断求两个数的最小公倍数实现.

定理 1.2.13 设 $a_1, a_2, \cdots, a_n$ 是 n 个正整数, 令

$$[a_1, a_2] = m_2,\ [m_2, a_3] = m_3,\ \cdots,\ [m_{n-1},\ a_n] = m_n.$$

则

$$[a_1, a_2, \cdots, a_n] = m_n.$$

证 由 m_i 的构造, $m_i \mid m_{i+1}$, $i = 2, 3, \cdots, n-1$, 且 $a_1 \mid m_2$, $a_i \mid m_i$, $i = 2, 3, \cdots, n$, 故 m_n 是 $a_1, a_2, \cdots, a_n$ 的一个公倍数. 反之, 设 m 是 $a_1, a_2, \cdots, a_n$ 的任一公倍数, 则 $a_1 \mid m$, $a_2 \mid m$, 则 m 是 a_1, a_2 的公倍数, 故 $m_2 \mid m$. 又 $a_3 \mid m$, 同理得 $m_3 \mid m$. 依此类推, 最后得 $m_n \mid m$. 因此 $m_n \leqslant |m|$. 故

$$m_n = [a_1, a_2, \cdots, a_n].$$

1.3 不定方程 1: 一次不定方程

不定方程是指未知数只能取整数的整数系数多项式方程. 这里先讨论一次不定方程. 先考虑二元一次不定方程, 所谓二元一次不定方程的一般形式是

$$ax + by = c,$$

其中 a, b, c 是整数.

首先考虑 $c = (a,b)$ 的简单情形.

1.3.1 一元一次不定方程 $ax + by = (a, b)$

由 Bézout 等式我们知道方程 $ax + by = (a, b)$ 是有 (整数) 解的, 定理 1.2.4 的证明过程实际上还给出了一个解的求法. 即利用辗转相除法:

$$\begin{array}{r|l} a = q_1 b + r_1 & r_1 = a - q_1 b \\ & r_2 = b - q_2 r_1 \\ b = q_2 r_1 + r_2 & \quad = b - q_2 (a - q_1 b) \\ & \quad = -q_2 a + (1 + q_1 q_2) b \\ & r_3 = r_1 - q_3 r_2 \\ r_1 = q_3 r_2 + r_3 & \quad = (a - q_1 b) - q_3 (-q_2 a + (1 + q_1 q_2) b) \\ & \quad = (1 + q_2 q_3) a_4 - (q_1 + q_3 + q_1 q_2 q_3) b \\ \cdots & \cdots \end{array}$$

一行行进行, 将陆续得到形如

$$\text{新的余数} = a \text{ 的倍数} + b \text{ 的倍数}$$

的等式. 最终我们得到最后的非零余数, 它等于 (a, b). 这就给出了方程 $ax + by = (a, b)$ 的一个解.

由这个解出发可以求出方程的所有解.

定理 1.3.1 设 a 与 b 是非零整数, $g = (a, b)$. 方程

$$ax + by = g \tag{1.3}$$

总是有一个整数解 (x_0, y_0), 它可由前面叙述的方法得到. 则方程的所有解为

$$\left(x_0 + k \cdot \frac{b}{g}, y_0 - k \cdot \frac{a}{g} \right), k = 0, \pm 1, \pm 2, \cdots . \tag{1.4}$$

证 容易验证 (1.4) 是原方程 (1.3) 的解.

反之, 设 (x_1, y_1) 也是原方程的解. 则

$$ax_1 + by_1 = g = ax_0 + by_0.$$

进而

$$a(x_1 - x_0) = b(y_0 - y_1).$$

两边约去 $g = (a, b)$, 有

$$\frac{a}{g}(x_1 - x_0) = \frac{b}{g}(y_0 - y_1).$$

因此

$$\frac{b}{g} \mid \frac{a}{g}(x_1 - x_0).$$

由于 $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$, 则

$$\frac{b}{g} \mid (x_1 - x_0).$$

即存在整数 k, 使得

$$x_1 - x_0 = k \cdot \frac{b}{g}.$$

所以

$$x_1 = x_0 + k \cdot \frac{b}{g},$$

进而

$$y_1 = y_0 - k \cdot \frac{a}{g}.$$

这就证明了方程 (1.3) 的解都有 (1.4) 的形式. □

注 这里可以类比线性代数中线性方程组的通解理解, "非齐次方程" $ax + by = g$ 的 "通解" $\left(x_0 + k \cdot \frac{b}{g}, y_0 - k \cdot \frac{a}{g}\right)$ 是其 "特解" (x_0, y_0) 加上 "齐次方程" $ax + by = 0$ 的 "通解". 考虑 $ax + by = 0$ 的解, 容易看出 "通解" 有形式

$$\left(x, \ -\frac{a}{b}x\right)$$

由于 y 应该是整数, 所以 x 要是 $\frac{a}{b}$ 的分母 (既约) 的倍数. 而 $\frac{a}{b}$ 约分 (即约去 $(a, b) = g$) 后的分母是 $\frac{b}{g}$, 所以 $x = k \cdot \frac{b}{g}$, $k \in \mathbb{Z}$, 进而 $y = -\frac{a}{b}x = -k \cdot \frac{a}{g}$. 所以 "齐次方程" $ax + by = 0$ 的 "通解" 为

$$\left(k \cdot \frac{b}{g}, \ -k \cdot \frac{a}{g}\right), \ k = 0, \pm 1, \pm 2, \cdots.$$

1.3.2 一元一次不定方程 $ax + by = c$

下面考虑一般形式的二元一次不定方程

$$ax + by = c. \tag{1.5}$$

定理 1.3.2 式 (1.5) 有整数解的充分与必要条件是 $(a, b) \mid c$.

证 若 (1.5) 有一整数解, 设为 x_0, y_0, 则

$$ax_0 + by_0 = c.$$

由于 (a, b) 整除 a 及 b, 因而整除 c, 必要性获证.

反之, 若 $(a, b) \mid c$, 则 $c = c_0(a, b)$, c_0 是整数. 由 Bézout 等式, 存在两个整数 u, v 满足

$$au + bv = (a, b).$$

令 $x_0 = uc_0, y_0 = vc_0$, 即得 $ax_0 + by_0 = c$, 故 (1.5) 式有整数解 x_0, y_0. □

从证明过程中可以看出, 求方程 $ax+by=c$ 的一个解可以从 $ax+by=(a,b)$ 的一个解得到. 具体而言, 设 $ax+by=(a,b)$ 的一个解为 (u,v), 则 $ax+by=c$ 有一个解 $\left(u\cdot\dfrac{c}{(a,b)},\ v\cdot\dfrac{c}{(a,b)}\right)$. 这样就得到了方程 $ax+by=c$ 的一个 "特解", "通解" 的求法与定理 1.3.1 类似.

定理 1.3.3 设二元一次不定方程

$$ax+by=c$$

有一整数解 $x=x_0$, $y=y_0$, 记 $(a,b)=g$, 则方程的所有解为

$$\left(x_0+k\cdot\frac{b}{g},\ y_0-k\cdot\frac{a}{g}\right),\ k=0,\pm1,\pm2,\cdots.$$

证 与定理 1.3.1 的证法相同. □

注 "非齐次方程" $ax+by=c$ 的 "通解" 也是其 "特解" 加上 "齐次方程" $ax+by=0$ 的 "通解" 的形式:

$$(x,y)=(x_0,y_0)+\left(k\cdot\frac{b}{g},\ -k\cdot\frac{a}{g}\right).$$

1.3.3 多元一次不定方程

所谓多元一次不定方程, 就是可以写成下列形式的方程:

$$a_1x_1+a_2x_2+\cdots+a_nx_n=N,$$

其中 $a_1,a_2,\cdots,a_n,N$ 都是整数, $n\geqslant 2$, 不失一般性, 我们可以假定 $a_1,a_2,\cdots,a_n$ 都不等于零.

多元一次不定方程有解的条件与二元的情形类似.

定理 1.3.4 多元一次不定方程 $a_1x_1+a_2x_2+\cdots+a_nx_n=N$ 有整数解的充分必要条件是 $(a_1,a_2,\cdots,a_n)\mid N$.

证 记 $(a_1,a_2,\cdots,a_n)=d$.

(必要性) 若方程有解, 即有 n 个整数 $x_1',x_2',\cdots,x_n'$ 满足等式

$$a_1x_1'+a_2x_2'+\cdots+a_nx_n'=N,$$

则 $d\mid a_1x_1'+a_2x_2'+\cdots+a_nx_n'$, 即 $d\mid N$.

(充分性) 若 $d\mid N$, 用数学归纳法证明方程有解. 当 $n=2$ 时, 方程是二元一次不定方程, 根据上一节的结论, 方程有解. 假定上述条件对 $n-1$ 元一次不定方程是充分的, 下证上述条件对 n 元一次不定方程也是充分的.

令 $d_2=(a_1,a_2)$, 则 $(d_2,a_3,a_4,\cdots,a_n)=d\mid N$. 由归纳假设, 方程

$$d_2t_2+a_3x_3+\cdots+a_nx_n=N$$

有解, 设其一解为 $t_2', x_3', \cdots, x_n'$. 再考虑

$$a_1x_1 + a_2x_2 = d_2t_2'.$$

根据上一节的结论, 上式有解, 设其一解为 x_1', x_2'. 则

$$\begin{aligned} &a_1x_1' + a_2x_2' + a_3x_3' + \cdots + a_nx_n' \\ &= d_2t_2' + a_3x_3' + \cdots + a_nx_n' = N. \end{aligned}$$

故 $x_1', x_2', \cdots, x_n'$ 是原方程的解. □

定理的证明过程还提供出一个求多元一次不定方程的解的方法, 即先顺次求出 $(a_1, a_2) = d_2$, $(d_2, a_3) = d_3$, $\cdots$, $(d_{n-1}, a_n) = d_n$. 若 $d_n \nmid N$, 则方程无解; 若 $d_n \mid N$, 则方程有解, 并将多元一次不定方程转化为二元一次不定方程组

$$\begin{cases} a_1x_1 + a_2x_2 = d_2t_2, \\ d_2t_2 + a_3x_3 = d_3t_3, \\ \cdots\cdots \\ d_{n-2}t_{n-2} + a_{n-1}x_{n-1} = d_{n-1}t_{n-1}, \\ d_{n-1}t_{n-1} + a_nx_n = N. \end{cases}$$

首先求出最后一个方程的一切解, 然后把 t_{n-1} 的每一个值代人倒数第二个方程求出它的一切解, 这样做下去即得出原方程的一切解.

例 1.3.5 求不定方程 $9x + 24y - 5z = 1000$ 的一切解.

解 因 $(9, 24) = 3$, $(3, -5) = 1$, 故方程有解.

先考虑方程

$$3t - 5z = 1000,$$

解得

$$\begin{cases} t = 2000 + 5v, \\ z = 1000 + 3v. \end{cases}$$

再考虑方程

$$9x + 24y = 3t,$$

即 $3x + 8y = t$, 解得

$$\begin{cases} x = 3t - 8u, \\ y = -t + 3u. \end{cases}$$

把 $t = 2000 + 5v$ 代入即得原方程的解

$$\begin{cases} x = 6000 + 15v - 8u, \\ y = -2000 - 5v + 3u, \\ z = 1000 + 3v. \end{cases}$$

1.4 素数与算术基本定理

1.4.1 素数

定义 1.4.1 (素数) 设整数 $p \neq 0, \pm 1$, 显然它总有两个正因数 1 和 p, 若 p 的正因数只有 1 和 p, 则称 p 为**素数** (prime number). 不是素数或 $0, \pm 1$ 的整数称为**合数** (composite number).

注 当 $p \neq 0, \pm 1$ 时, 由于 p 和 $-p$ 必同为素数或合数, 所以, 若没有特别说明, 素数总是指正的.

换句话说, 素数是不可分解的 (即若素数 $p = bc$, 则必然 $b = \pm 1$ 或 $c = \pm 1$). 而合数可分解, 即合数 a 可写为 $a = bc$ (其中 $b, c \neq \pm 1$; 或者说 $b, c \neq \pm a$). 1 既不是素数也不是合数. 小于 100 的正素数为

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$
$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

素数有如下的简单性质.

定理 1.4.2 设 a 是任一大于 1 的整数, 则 a 的除 1 外最小正因数 q 是一素数, 并且当 a 是合数时, $q \leqslant \sqrt{a}$.

证 假定 q 不是素数, 由定义, q 除 1 及本身外还有一正因数 q_1, 因而 $1 < q_1 < q$, $q_1 \mid q$. 由于 $q \mid a$, 所以 $q_1 \mid a$, 这与 q 是 a 的除 1 外的最小正因数矛盾, 故 q 是素数.

当 a 是合数时, 则 $a = a_1 q$, 且 $a_1 > 1$, 否则 a 是素数. 由于 q 是 a 的除 1 外的最小正因数, 所以 $q \leqslant a_1$, $q^2 \leqslant q a_1 = a$, 故 $q \leqslant \sqrt{a}$. □

定理 1.4.3 若 p 是一素数, a 是任一整数, 则或者 $p \mid a$, 或者 p 与 a 互素.

证 因为 $(p, a) \mid p$, $(p, a) > 0$, 由素数的定义, $(p, a) = 1$, 或 $(p, a) = p$. 即 $(p, a) = 1$ 或 $p \mid a$. □

推论 1.4.4 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数, p 是素数. 若 $p \mid a_1 a_2 \cdots a_n$, 则 p 一定能整除某一 a_k.

证 如果 $a_1, a_2, \cdots, a_n$ 都不能被 p 整除, 则由上定理

$$(p, a_i) = 1,\ i = 1, 2, \cdots, n.$$

因此由定理 1.2.8, $(p, a_1a_2\cdots a_n)=1$, 这与 $p \mid a_1a_2\cdots a_n$ 矛盾. □

1.4.2 算术基本定理

定理 1.4.5 (算术基本定理) 任一大于 1 的整数能唯一地表成素数的乘积. 即任一大于 1 的整数

$$a = p_1p_2\cdots p_n,\ p_1 \leqslant p_2 \leqslant \cdots \leqslant p_n, \tag{1.6}$$

其中 $p_1, p_2, \cdots, p_n$ 是素数, 并且若

$$a = q_1q_2\cdots q_m,,\ q_1 \leqslant q_2 \leqslant \cdots \leqslant q_m,$$

其中 $q_1, q_2, \cdots, q_m$ 是素数, 则 $m=n$, $q_i=p_i$, $i=1,2,\cdots,n$.

证 先用数学归纳法证明存在性. 当 $a=2$ 时, (1.6) 式显然成立. 假定对一切小于 a 的正整数 (1.6) 式都成立, 此时若 a 是素数, 则 (1.6) 式对 a 成立; 若 a 是合数, 则有两正整数 bc 满足条件

$$a=bc,\ 1<b<a,\ 1<c<a.$$

由归纳假设

$$b = p_1'p_2'\cdots p_t', c = p_{l+1}'p_{t+2}'\cdots p_n',$$

于是

$$a = p_1'p_2'\cdots p_t'p_{t+1}'\cdots p_n'.$$

将 p_i' 的次序适当调动后即得 (1.6) 式, 故 (1.6) 式对 a 成立. 由归纳法即知对任一大于 1 的正整数, (1.6) 式成立.

下证唯一性. 若 $a = q_1q_2\cdots q_m$, $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_m$, 则

$$p_1p_2\cdots p_n = q_1q_2\cdots q_m.$$

因此 $p_1 \mid q_1q_2\cdots q_m$, $q_1 \mid p_1p_2\cdots p_n$. 故存在 p_k, q_j, 使得 $p_1 \mid q_j$, $q_1 \mid p_k$. 但 q_j, p_k 都是素数, 故 $p_1=q_j$, $q_1=p_k$. 又 $p_k \geqslant p_1$, $q_j \geqslant q_1$, 故

$$p_1 = q_1.$$

进而 $p_2\cdots p_n = q_2\cdots q_m$, 同法可得 $p_2=q_2$. 依此类推, 最后即得 $n=m$, $p_i=q_i$, $i=1,2,\cdots,n$. □

由定理立即得到如下推论.

推论 1.4.6 任一大于 1 的整数 a 能够惟一地写成

$$a = p_1^{\alpha_1}\cdots p_k^{\alpha_k},\ \alpha_i>0,\ i=1,\cdots,k, \tag{1.7}$$

其中 $p_i < p_j$ $(i<j)$.

式 (1.7) 叫做 a 的标准分解式. 为方便有时会添加若干素数的零次幂而把 a 表成下面的形式:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_t},\ \alpha_i \geqslant 0,\ i = 1, 2, \cdots, t.$$

推论 1.4.7 设 a 是一个大于 1 的整数, 且

$$a = p_1^{\alpha_1} p_2^{\alpha_2 \cdots} p_k^{\alpha_k},\ \alpha_i > 0,\ i = 1, 2, \cdots, k,$$

则 a 的正因数 d 可以表成

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},\ \alpha_i \geqslant \beta_i \geqslant 0, i = 1, 2, \cdots, k$$

的形式, 而且当 d 可以表成上述形式时, d 是 a 的正因数.

推论 1.4.8 设 a, b 是任意两个正整数, 且

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \alpha_i \geqslant 0, i = 1, 2, \cdots, k,$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \beta_1 \geqslant 0, i = 1, 2, \cdots, k,$$

则

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k},$$
$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k},$$

其中 $\gamma_i = \min(\alpha_i, \beta_i)$, $\delta_i = \max(\alpha_i, \beta_i)$, $i = 1, 2, \cdots, k$.

算术基本定理说明每个整数 $n \geqslant 2$ 可表示成素数乘积. 给定一个整数 $n \geqslant 2$, 如果 n 不太大, 要将 n 表示成素数乘积, 可以用小于等于于 $\sqrt{n}$ 的每个素数 $2, 3, \cdots$ 试除它. 如果没有求得整除 n 的素数, 则 n 本身是素数. 否则求得的第一个因数是素数 p. 分解得 $n = pm$, 然后对 m 重复这个过程, 最终就可以具体地把 n 分成素数乘积. 但对非常大的数, 这一方法几乎没有可行性.

1.4.3 素数无穷多

定理 1.4.9 存在无穷多个素数.

证 用反证法. 如果正整数中只有有限个素数, 设为 $p_1, p_2, \cdots, p_k$. 令 $N = p_1 p_2 \cdots p_k + 1$, 则 $N > 1$. 如果 N 本身是素数, 则证明已完成; 如果 N 不是素数, 则 N 有一素因数 p. 这里 $p \neq p_i$, $i = 1, 2, \cdots, k$, 否则 $p \mid p_1 p_2 \cdots p_k$, $p \mid N$, 因此 $p \mid 1$, 而与 p 是素数矛盾. 故 p 是上面 k 个素数以外的素数. □

用类似的方法还可以证明

定理 1.4.10 存在无穷多个模 4 余 3 的素数.

证 假设模 4 余 3 的素数只有有限个, 为

$$3, p_1, p_2, \cdots, p_r.$$

考虑数

$$A = 4p_1p_2\cdots p_r + 3.$$

将 A 素因数分解

$$A = q_1q_2\cdots q_s.$$

我们断言素数 $q_1, q_2, \cdots, q_s$ 中至少有一个必是模 4 余 3 的. 若不然, 则 $q_1, q_2, \cdots, q_s$ 都模 4 余 1, 此时其乘积 A 一定模 4 余 1. 但是由定义知 A 显然模 4 余 3. 从而, $q_1, q_2, \cdots, q_s$ 中至少有一个必定模 4 余 3, 设为 q_i. 而由于 q_i 整除 A, 而由 A 的定义显然 $3, p_1, p_2, \cdots, p_r$ 都不整除 A. 因此 q_i 是上面的 r 个模 4 余 3 的素数之外的模 4 余 3 的素数. □

或者

定理 1.4.11 存在无穷多个模 6 余 5 的素数.

证 设 $5, p_1, \ldots, p_r$ 是所有模 6 余 5 的素数. 设 $A = 6p_1p_2\cdots p_r + 5$, 并将 A 素因数分解 $A = q_1q_2\cdots q_s$. 因为 q_i 是素数, 所以它们不能模 6 余 $2, 3, 4$; 又因为 A 模 6 余 5, 所以 A 不能被 2 或 3 整除, 所以 q_i 中也没有 2 或 3. 如果所有 q_i 都模 6 余 1, 则 A 也模 6 余 1. 所以至少有一个 q_i 模 6 余 5, 记为 q. 而由于 q 整除 A, 而由 A 的定义显然 $5, p_1, p_2, \cdots, p_r$ 都不整除 A. 因此 q 是上面的 r 个模 6 余 5 的素数之外的模 6 余 5 的素数. □

一般地, 狄利克雷在 1837 年证明的一条著名定理说明, 在 $(a, m) = 1$ 的假设下总存在无穷多个素数模 m 余 a.

定理 1.4.12 (算术级数的素数狄利克雷定理, Dirichlet's Theorem on Primes in Arithmetic Progressions[1]) 设 a 与 m 是整数, $(a, m) = 1$. 则存在无穷多个素数模 m 余 a.

我们已经证明了 $(a, m) = (3, 4)$ 和 $(6, 5)$ 的狄利克雷定理, 但不能用类似的方式证明所有情形的定理. 例如不能用同样的思想 (用 $A = 5p_1p_2\cdots p_r + 4$) 证明存在无穷多个模 5 余 4 的素数, 这样证明的关键问题是如果素数乘积 $q_1q_2\cdots q_s$ 模 5 余 4, 则其中一个因数模 5 余 4 不一定为真, 例如, 如果两个因数都模 5 余 2, 那么乘积仍将模 5 余 4. 所有 (a, m) 的狄利克雷定理的证明都相当复杂.

1.4.4 梅森素数与完全数

考虑形如 $a^n - 1$ $(n \geqslant 2)$ 的素数. 事实上, 只有 a 等于 2 且 n 是素数时这样的数才可能是素数.

[1] 算术级数是有公差的数列 (即等差数列). 模 m 余 a 的数构成公差为 m 的算术级数, 定理即是说等差数列 $a + m$, $a + 2m$, $a + 3m$, $\cdots$ 中有无限多个素数, 这就解释了定理的名称.

定理 1.4.13 如果对整数 $a \geqslant 2$, $n \geqslant 2$, $a^n - 1$ 是素数, 则 a 必等于 2 且 n 一定是素数.

证 首先, 根据公式

$$x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1\right) \tag{1.8}$$

我们知道 $a^n - 1$ 被 $a - 1$ 整除. 所以若 $a^n - 1$ 是素数, 必然有 $a - 1 = 1$, 即 $a = 2$.

其次, $a = 2$ 时, 若 n 是合数, 设 $n = mk$, 则 $2^n = 2^{mk} = (2^m)^k$. 将 $x = 2^m$ 代入 (1.8) 式得

$$2^n - 1 = (2^m)^k - 1 = (2^m - 1)\left((2^m)^{k-1} + (2^m)^{k-2} + \cdots + (2^m)^2 + (2^m) + 1\right).$$

因此 $2^n - 1$ 是合数. □

形如

$$2^p - 1$$

的素数称为**梅森素数** (Mersenne primes). 前几个梅森素数是

$$2^2 - 1 = 3,\ 2^3 - 1 = 7,\ 2^5 - 1 = 31,\ 2^7 - 1 = 127,\ 2^{13} - 1 = 8191.$$

当然, 并非每个形如 $2^p - 1$ 的数都是素数. 例如

$$2^{11} - 1 = 2047 = 23 \cdot 89,\ 2^{29} - 1 = 536870911 = 233 \cdot 1103 \cdot 2089.$$

截至 2018 年 12 月 21 日, 已发现 51 个梅森素数[1]. 是否存在无穷多个梅森素数的答案尚未知晓.

梅森素数与完全数有着密切的联系. 所有的真因数 (即除了自身以外的正因数) 的和, 恰好等于它本身的数称为**完全数** (perfect number). 对梅森素数 $2^p - 1$, 则 $2^{p-1}(2^p - 1)$ 是完全数.

定理 1.4.14 (欧几里得完全数公式, Euclid's Perfect Number Formula) 如果 $2^p - 1$ 是素数, 则 $2^{p-1}(2^p - 1)$ 是完全数.

证 设 $q = 2^p - 1$, 我们需要验证 $2^{p-1}q$ 是完全数. $2^{p-1}q$ 的真因数是

$$1, 2, 4, \cdots, 2^{p-1} \text{ 与 } q, 2q, 4q, \cdots, 2^{p-2}q.$$

根据等比数列的求和公式,

$$1 + 2 + 4 + \cdots + 2^{p-1} = \frac{2^p - 1}{2 - 1} = 2^p - 1 = q;$$

$$q + 2q + 2^2 q + \cdots + 2^{p-2}q = q\left(1 + 2 + 2^2 + \cdots + 2^{p-2}\right) = q\left(\frac{2^{p-1} - 1}{2 - 1}\right) = q\left(2^{p-1} - 1\right).$$

因此 $2^{p-1}q$ 的所有真因数之和为 $q + q\left(2^{p-1} - 1\right) = 2^{p-1}q$. 因此 $2^{p-1}q$ 是完全数. □

[1] GIMPS Discovers Largest Known Prime Number: 2^82,589,933-1. https://www.mersenne.org/primes/?press=M82589933. Retrieved 2019-01-01.

根据欧几里得完全数公式, 求得一个梅森素数就可以得到一个完全数. 这时一个自然的问题就是欧几里得完全数公式是否表示了所有完全数. 换句话说, 是否每个完全数是 $2^{p-1}(2^p-1)$ (2^p-1 是素数) 的形式? 欧拉证明了欧几里得公式至少给出所有偶完全数.

在证明欧拉的定理之前, 先讨论所需用到的因数和函数 σ, [1] 即

$$\sigma(n)=\sum_{d|n} d\ (d>0).$$

例如

$$\sigma(6)=1+2+3+6=12,$$
$$\sigma(8)=1+2+4+8=15.$$

显然, 一个数 n 是完全数即是 $\sigma(n)=2n$.

我们将逐步得出完全数的公式. 首先, 对素数 p, 其因数仅是 1 与 p, 因此 $\sigma(p)=p+1$. 更一般地, 素数幂 p^k 的因数是 $1,p,p^2,\cdots,p^k$, 所以

$$\sigma\left(p^k\right)=1+p+p^2+\cdots+p^k=\frac{p^{k+1}-1}{p-1}.$$

对一般的数 n, 因为它有素因数分解 $n=p_1^{k_1}\cdot p_2^{k_2}\cdots p_r^{k_r}$, 且事实上根据下面的定理, 如果 $(m,n)=1$, 则 $\sigma(mn)=\sigma(m)\sigma(n)$, 这样我们就可以对每个正整数 n 计算 $\sigma(n)$ 的值了.

定理 1.4.15 如果 $(m,n)=1$, 则

$$\sigma(mn)=\sigma(m)\sigma(n).$$

证 设 $d_1,\ldots,d_r$ 是 m 的因数, $e_1,\ldots,e_s$ 是 n 的因数. 那么 m 和 n 没有公因数意味着 mn 的因数恰好是通过取 d_i 之一和 e_j 之一的乘积获得的. 所以 $\sigma(mn)$ 是所有乘积 d_ie_j 的总和, 即

$$\sigma(mn)=d_1e_1+\cdots+d_re_s=(d_1+\cdots+d_r)(e_1+\cdots+e_s)=\sigma(m)\sigma(n). \qquad \square$$

现在就可以证明欧拉的偶完全数定理了.

定理 1.4.16 (欧拉完全数定理, Euler's Perfect Number Theorem).) 如果 n 是偶完全数, 则 n 形如

$$n=2^{p-1}(2^p-1),$$

其中 2^p-1 是梅森素数.

[1] 事实上这里的 σ 函数是一般的因数函数 (Divisor function) 的特例, 一般的因数函数 $\sigma_z(n)$ 定义为

$$\sigma_z(n)=\sum_{d|n} d^z.$$

$z=0$ 时表示 n 的正因数的数目, $z=1$ 时就是这里的 σ 函数.

证 假设 n 是偶完全数. n 是偶数说明可将它分解成 $n=2^k m$, $k\geqslant 1$ 且 m 是奇数. 下面计算 $\sigma(n)$:

$$\begin{aligned}\sigma(n)&=\sigma\left(2^k m\right) && n=2^k m,\\ &=\sigma\left(2^k\right)\sigma(m) && \left(2^k,m\right)=1,\\ &=\left(2^{k+1}-1\right)\sigma(m) && \text{使用 } p=2 \text{ 时 } \sigma\left(p^k\right) \text{ 的公式.}\end{aligned}$$

由假设 n 是完全数, 这意味着 $\sigma(n)=2n=2^{k+1}m$. 所以

$$2^{k+1}m=\left(2^{k+1}-1\right)\sigma(m).$$

显然 $2^{k+1}-1$ 是奇数, 故由于 $\left(2^{k+1}-1\right)\sigma(m)$ 是 2^{k+1} 的倍数, 所以 2^{k+1} 必整除 $\sigma(m)$. 换句话说, 存在整数 c 使得 $\sigma(m)=2^{k+1}c$. 将其代入前面的等式得

$$2^{k+1}m=\left(2^{k+1}-1\right)\sigma(m)=\left(2^{k+1}-1\right)2^{2^{k+1}}c,$$

从两边消去 2^{k+1} 得 $m=\left(2^{k+1}-1\right)c$. 概括地说, 我们已证明存在整数 c 使得

$$m=\left(2^{k+1}-1\right)c \text{ 且} \sigma(m)=2^{k+1}c.$$

接下来用反证法来证明 $c=1$. 假设 $c>1$, 则 $m=\left(2^{k+1}-1\right)c$ 被不同的数 $1,c,m$ 整除 (n 是偶数说明 $k\geqslant 1$, 所以 c 与 m 不同). 因此

$$\sigma(m)\geqslant 1+c+m=1+c+\left(2^{k+1}-1\right)c=1+2^{k+1}c.$$

然而, 我们还知道 $\sigma(m)=2^{k+1}c$, 所以

$$2^{k+1}c\geqslant 1+2^{k+1}c,$$

矛盾, 所以 c 必等于 1, 即

$$m=\left(2^{k+1}-1\right) \text{ 且} \sigma(m)=2^{k+1}=m+1.$$

显然 $\sigma(m)=m+1$ 意味着 m 的正因数只有 1 和 m, 即 m 是素数. 在根据 m 形如 $2^{k+1}-1$ (前面证明过这样的数是素数必有 $k+1$ 等于某素数 p) 知 m 是梅森素数 2^p-1. □

欧拉完全数定理给出了所有偶完全数的漂亮描述, 但对于奇完全数, 连其是否存在也是至今尚未解决的难题.

Chapter 2

同余

2.1 同余与同余类

2.1.1 同余的概念与性质

定义 2.1.1 (同余) 设 $m, a, b \in \mathbb{Z}$, $m \neq 0$, 如果

$$m \mid (a - b),$$

则称 a 与 b 模 m **同余** (a is congruent to b modulo m), 记为 $a \equiv b \pmod{m}$. 称 m 为**模** (modulus, 复数为 moduli). 符号 "$\equiv$" 称为同余号, 读作 "同余于", 带同余号的表达式称为**同余式** (congruence). 同余式的运算称为 "模算术" (modular arithmetic).

由定义可知, 同余关系有如下各种等价的表述:

$$\begin{aligned} a \equiv b \pmod{m} &\iff a - b = mk \text{ (对某 } k \in \mathbb{Z}) \\ &\iff a = b + mk \text{ (对某 } k \in \mathbb{Z}) \\ &\iff \text{在忽略不计 } m \text{ 的倍数的意义下 } a \text{ 与 } b \text{ 相等} \\ &\iff a \text{ 与 } b \text{ 除以 } m \text{ 的余数相同.} \end{aligned}$$

容易验证, 同余关系是一个等价关系 (equivalent relation), 即满足:
(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 $a \equiv c \pmod{m}$.
容易看出, 模 m 同余的两个数模 m 的因数也同余.

定理 2.1.2 若 $a \equiv b \pmod{m}$, $d \mid m$, 则 $a \equiv b \pmod{d}$.

证 由条件 $a \equiv b \pmod m$ 有 $a = b + mt$, $d \mid m$ 有 $m = kd$, 故 $a = b + d(kt)$, 即 $a \equiv b \pmod d$. □

定理 2.1.3 若 $a \equiv b \pmod m$, 则 $(a, m) = (b, m)$.

证 因为 $a = b + mt$, 故立即有 $(a, m) = (b, m)$. □

同余式可以相加和相乘.

定理 2.1.4 (i) (同余式相加) 若 $a \equiv b \pmod m$, $c \equiv d \pmod m$, 则 $a+c \equiv b+d \pmod m$. 特别地, 若 $a + b \equiv c \pmod m$, 则 $a \equiv c - b \pmod m$; $a + b + k \equiv c + k \pmod m$, $(k \in \mathbb{Z})$.

(ii) (同余式相乘) 若 $a \equiv b \pmod m$, $c \equiv d \pmod m$, 则 $ac \equiv bd \pmod m$. 特别地, 由 $a \equiv b \pmod m$ 可推出 $a^k \equiv b^k \pmod m$ $(\forall k \in \mathbb{Z}^+)$; $ak \equiv bk \pmod m$, $(\forall k \in \mathbb{Z})$.

证 (i) 由定义可设 $a = b + ms$, $c = d + mt$, 因此 $a + c = b + d + m(s + t)$, 即 $a + c \equiv b + d \pmod m$.

(ii) 由定义可设 $a = b + mk$, $c = d + mj$. 二式相乘得 $ac = bd + m(kd + jb + mkj)$, 即 $ac \equiv bd \pmod m$. □

但在模不变的情况下, 同余式两侧约去同一个数并非总是可能的. 即果 $ac \equiv bc \pmod m$, 则 $a \equiv b \pmod m$ 未必成立. 事实上关于同余式的倍数和约化有如下结论.

定理 2.1.5 (i) (同余式的倍数) 若 $a \equiv b \pmod m$, 当且仅当 $ak \equiv bk \pmod{mk}$;[1]

(ii) (同余式的约化) 若 $a \equiv b \pmod m$, 且 $d \mid (a, b)$ (即 d 是 a, b 的公因数, 或 $d \mid a$ 且 $d \mid b$), 则

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{(d, m)}}$$

特别地, 若 d 与 m 互素, 则 $\frac{a}{d} \equiv \frac{b}{d} \pmod m$; 若 $d \mid m$ (即 d 是 a, b, m 的公因数, 或 $d \mid (a, b, m)$), 则 $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

证 (i) 只需注意到 $km \mid (ka - kb) \Longleftrightarrow m \mid a - b$.

(ii) $a \equiv b \pmod m$ 即 $m \mid (a - b)$, 即 $\frac{m}{(d, m)} \mid \frac{a-b}{d}\frac{d}{(d, m)}$, 而 $\frac{m}{(d, m)}$ 与 $\frac{d}{(d, m)}$ 互素, 故

$$\frac{m}{(d, m)} \mid \frac{a - b}{d}.$$

也就是 $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{(d, m)}}$. □

定理 2.1.6 若 $a \equiv b \pmod{m_i}$, $i = 1, 2, \cdots, k$, 当且仅当

$$a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}.$$

[1] 这一结论比定理 2.1.4 (ii) 更强.

证 只需注意到 $m_i \mid a-b$, $i=1,2,\cdots,k$ 当且仅当 $[m_1,m_2,\cdots,m_k] \mid a-b$, 这用素因数分解容易证明. □

2.1.2 同余类与同余类环

我们知道同余关系是一个等价关系, 因此可以按这一关系在 $\mathbb{Z}$ 上划分等价类. 设 m 为固定的非零整数, 按照模 m 同余关系, 将整数集 $\mathbb{Z}$ 分类: 相互同余者分在同一类, 称为模 m 的一个**同余类**或剩余类 (congruence class modulo m). 同余于 a 的同余类 (即 a 所代表的同余类) 记为

$$\overline{a}=a+m\mathbb{Z}=\{a+mk \mid k\in\mathbb{Z}\}.$$

对应的商集称为 $\mathbb{Z}$ 的模 m 同余类集, 记作 $\mathbb{Z}/m\mathbb{Z}$ 或 $\mathbb{Z}_m$,

$$\mathbb{Z}/m\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{m-1}\}.$$

对 $\mathbb{Z}/m\mathbb{Z}$ 的 m 个同余类 $\overline{0},\overline{1},\overline{2},\cdots,\overline{m-1}$, 它们的代表元通常分别取为 $0,1,2,\cdots,m-1$, 这称为模 m 的**最小非负完全剩余系** (complete residue system). 有时也取代表元为 0, ±1, ±2, $\cdots$, $\pm\dfrac{(m-1)}{2}$ (当 m 为奇数); $-\dfrac{m}{2}$, $\cdots$, -1, 0, 1, $\cdots$, $\dfrac{m}{2}-1$ 或 $-\dfrac{m}{2}+1$, $\cdots$, -1, 0, 1, $\cdots$, $\dfrac{m}{2}$ (当 m 为偶数), 称为**绝对 (值) 最小完全剩余系**. 一般地, 在这些同余类的每一个中各取一个代表元得到的集合, 称为模 m 的一个**完全剩余系**, 容易看出, 任意 m 个互不同余的数构成一个模 m 的完全剩余系.

定义 2.1.7 记 $\mathbb{Z}/m\mathbb{Z}=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{m-1}\}$ 为整数模 m 的同余类集, 定义同余类 $\overline{a}$ 和 $\overline{b}$ 的加法和乘法如下:

$$\overline{a}+\overline{b}=\overline{a+b},\ \overline{a}\cdot\overline{b}=\overline{ab}.$$

我们需要验证上面规定的运算与同余类的代表元的选取无关. 设

$$\overline{a}=\overline{a'},\ \overline{b}=\overline{b'},$$

则

$$m\,|a-a',\ m|\,b-b',$$

于是

$$\begin{aligned} m &\mid (a-a')+(b-b')=(a+b)-(a'+b'),\\ m &\mid (a-a')\,b+(b-b')\,a'=(ab)-(a'b'), \end{aligned}$$

从而

$$\overline{a+b}=\overline{a'+b'},\ \overline{ab}=\overline{a'b'}.$$ □

容易验证, 模 m 的同余类集与上述运算 $(\mathbb{Z}/m\mathbb{Z},+,\cdot)$ 构成环. 事实上, $0=\overline{0}$ 为零元; 若 $\alpha=\overline{a}$, 则 $\alpha'=\overline{-a}$ 为其负元; $e=1=\overline{1}$ 即为么元[1]; 且 $\mathbb{Z}/m\mathbb{Z}$ 还是交换环. $\mathbb{Z}/m\mathbb{Z}$ 称为模 m 的

[1] 这里所说的环都是含幺元的.

同余类环 (或模 m 的商环). 同余式的运算就是同余类环上的运算, 环中运算的性质可以直接用到同余式的计算上.

$\mathbb{Z}/m\mathbb{Z}$ 一般关于除法不封闭, 即非零元不一定有逆, 或关于乘法不构成群. 但其部分元素关于同余类的乘法是可以构成群的.

定理 2.1.8 设 m 是大于 1 的正整数, 记

$$U(m) = \{\overline{a} \in \mathbb{Z}/m\mathbb{Z} \mid (a, m) = 1\},$$

则 $U(m)$ 关于同余类的乘法构成群.

证 这里只证所有元素有逆. 对任意的 $\overline{a} \in U(m)$, 有 $(a, m) = 1$. 由 Bézout 等式, 存在 $u, v \in \mathbb{Z}$, 使

$$au + mv = 1.$$

因此 $(u, m) = 1$, 所以 $\overline{u} \in U(m)$, 且

$$\begin{aligned}
\overline{a} \cdot \overline{u} &= \overline{au} \\
&= \overline{au + mv} \quad (\text{ 因为 } \overline{m} = \overline{0} \text{ }) \\
&= \overline{1}, \\
\overline{u} \cdot \overline{a} &= \overline{ua} = \overline{au} = \overline{1},
\end{aligned}$$

所以 $\overline{u}$ 为 $\overline{a}$ 的逆元. 从而知, $U(m)$ 的每个元素在 $U(m)$ 中都可逆. □

注 上述证明也给出了求逆的方法: 辗转相除求 Bézout 等式 $au + mv = 1$, 则 $\overline{u}$ 为 $\overline{a}$ 的逆.

事实上, $U(m)$ 是环 $\mathbb{Z}/m\mathbb{Z}$ 中的所有可逆元. 若 $(b, m) = d > 1$, 则 $m = m_1 d$, $b = b_1 d$, 故

$$b \cdot m_1 = b_1 d m_1 = b_1 m \equiv 0 \pmod{m},$$

即 $\overline{b} \cdot \overline{m_1} = \overline{0}$, 故 $\overline{b}$ 是环 $\mathbb{Z}/m\mathbb{Z}$ 的零因子[1]. 进而可知, $\overline{b}$ 不可逆: 假若 $\overline{b}$ 有逆元 $\overline{b}^{-1} \in \mathbb{Z}/m\mathbb{Z}$, 将上式两边同乘 $\overline{b}^{-1}$, 得到 $\overline{m_1} = \overline{0}$, 矛盾.

因此, 群 $(U(m), \cdot)$ 就是环 $\mathbb{Z}/m\mathbb{Z}$ 的**单位群**[2] (group of units), 也称为 $\mathbb{Z}$ 的模 m 单位群, 显然这是一个交换群. 当 p 为素数时,

$$U(p) = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\} = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}.$$

这时 $\mathbb{Z}/p\mathbb{Z}$ 中的非零元均可逆, 从而 $\mathbb{Z}/p\mathbb{Z}$ 为域, 记为

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}.$$

[1] 在交换环中, 零因子 (divisor of zero) 是指 $\alpha \neq 0$ 且 $\beta \neq 0$ 但 $\alpha\beta = 0$ 的 α 和 β.

[2] 环中的可逆元也称为其单位 (unit), 环的单位的集合关于环的乘法构成群, 称为环的单位群.

若 m 不是素数, 则有整数 $1 < b < m$ 使 $(b, m) = d > 1$, 于是 $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ 是零因子, 不可逆. 故此时 $\mathbb{Z}/m\mathbb{Z}$ 不是域.

现在回头看同余式约化性质: 若 $(d, m) = 1$, $d \mid a$, $d \mid b$, 则由 $a \equiv b \pmod{m}$ 可得

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{m}.$$

这是很自然的了, 因为此时 $d \pmod{m}$ 可逆, 当然可约去了 (即 $\overline{a}\overline{d}^{-1} = \overline{b}\overline{d}^{-1}$).

2.2 同余方程 1: 一次同余方程

2.2.1 线性同余方程

线性同余方程即是由如下同余式确定的方程

$$ax \equiv c \pmod{m}. \tag{2.1}$$

容易看出, (2.1) 等价于存在整数 y 使得 $ax - c = my$, 即原方程等价于不定方程

$$ax - my = c.$$

根据前面不定方程的相关结论, 方程有解的充分与必要条件是 $(a, m) \mid c$.

记 $g = (a, m)$, $u = u_0$, $v = v_0$ 是

$$au + mv = g$$

的一个解, 由于 $g \mid c$, 所以可用整数 $\dfrac{c}{g}$ 乘以这个方程得

$$a\frac{cu_0}{g} + m\frac{cv_0}{g} = c.$$

这说明 $x_0 \equiv \dfrac{cu_0}{g} \pmod{m}$ 是 $ax \equiv c \pmod{m}$ 的一个解.

另一方面, 假设 x_1 是 $ax \equiv c \pmod{m}$ 的其他解, 则 $ax_1 \equiv ax_0 \pmod{m}$, 所以 $m \mid ax_1 - ax_0$. 这蕴涵

$$\frac{m}{g} \mid \frac{a(x_1 - x_0)}{g},$$

由于 $\left(\dfrac{m}{g}, \dfrac{a}{g}\right) = 1$, 从而 $\dfrac{m}{g} \mid x_1 - x_0$. 也即存在整数 k 使得

$$x_1 = x_0 + k \cdot \frac{m}{g}.$$

所以方程在模 m 意义下恰好有 g 个不同的解, 这些解通过取 $k = 0, 1, \cdots, g-1$ 而得到. 注意到同余方程 $ax \equiv c \pmod{m}$ 与不定方程 $ax - my = c$ 的解完全相同.

以上分析即是如下定理.

定理 2.2.1 设 a, c 与 m 是整数, $m \geqslant 1$, 且设 $g = (a, m)$.

(i) 如果 $g \nmid c$, 则同余方程 $ax \equiv c \pmod{m}$ 无解;

(ii) 如果 $g \mid c$, 则同余方程 $ax \equiv c \pmod{m}$ 恰好有 g 个不同的解. 要求这些解, 首先求不定方程

$$au + mv = g$$

的一个解 (u_0, v_0), 则 $x_0 = \dfrac{cu_0}{g}$ 是 $ax \equiv c \pmod{m}$ 的一个解, 进而求出所有解为

$$x \equiv x_0 + k \cdot \frac{m}{g} \pmod{m},\ k = 0, 1, 2, \cdots, g-1.$$

注 定理的一个特殊情形是 $(a, m) = 1$. 在这种情形下, 同余方程

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

恰好有一个解. 我们甚至可将解写成分数

$$x \equiv \frac{c}{a} \pmod{m}.$$

事实上, 这里 $\dfrac{1}{a}$ 指 $a \pmod{m}$ 的逆 $a^{-1} \pmod{m}$ (由于 $(a, m) = 1$ 故 $a \pmod{m}$ 可逆), 上式即是 $x \equiv ba^{-1} \pmod{m}$, 或 $\overline{x} = \overline{b}\overline{a}^{-1}$.

2.2.2 线性同余方程组与中国剩余定理

下面考虑同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ \cdots\cdots \\ x \equiv b_k \pmod{m_k} \end{cases} \tag{2.2}$$

的求解.

定理 2.2.2 (中国剩余定理, 孙子定理, Chinese Remainder Theorem) 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数, $m = m_1 m_2 \cdots m_k$, $m = m_i M_i$, $i = 1, 2, \cdots, k$, 则同余方程组 (2.2) 有解

$$x \equiv M_1^{-1} M_1 b_1 + M_2^{-1} M_2 b_2 + \cdots + M_k^{-1} M_k b_k \pmod{m},$$

其中 M_i^{-1} 是 M_i 对模 m_i 的逆 (即 $M_i^{-1} M_i \equiv 1 \pmod{m_i}$), $i = 1, 2, \cdots, k$, 且在模 m 意义下解唯一.

证 由 $(m_i, m_j) = 1$, $i \neq j$ 和 M_i 的构造即得 $(M_i, m_i) = 1$, 故 M_i 对模 m_i 有逆 (求解可通过求同余方程 $M_i y \equiv 1 \pmod{m_i}$), 即存在 M_i^{-1}, 使得

$$M_i^{-1} M_i \equiv 1 \pmod{m_i}.$$

另一方面由 $m = m_i M_i$, 因此 $m_j \mid M_i$, $i \neq j$, 故

$$\sum_{j=1}^{k} M_j^{-1} M_j b_j \equiv M_i^{-1} M_i b_i \equiv b_i \pmod{m_i}$$

即为原方程组的解.

若原方程组有两个解 x_1, x_2, 则

$$x_1 \equiv x_2 \pmod{m_i},\ i = 1, 2, \cdots, k,$$

因 $(m_i, m_j) = 1$, 故 $m = m_1 m_2 \cdots m_k = [m_1, \cdots, m_k]$. 于是 $x_1 \equiv x_2 \pmod{m}$. □

注 这种求法来源于《孙子算经》, 这种求解方法可以列表如下:

除数	余数	最小公倍数	衍数	乘率 (逆)	各总	答数 (解)
m_1	b_1	$m = m_1 m_2 \cdots m_k$	M_1	M_1^{-1}	$M_1 M_1^{-1} b_1$	$x \equiv \sum_{i=1}^{k} M_i M_i^{-1} b_i \pmod{m}$
m_2	b_2		M_2	M_2^{-1}	$M_2 M_2^{-1} b_2$	
$\cdots$	$\cdots$		$\cdots$	$\cdots$	$\cdots$	
m_k	b_k		M_k	M_k^{-1}	$M_k M_k^{-1} b_k$	

定理 2.2.3 若 $b_1, b_2, \cdots, b_k$ 分别遍历模 $m_1, m_2, \cdots, m_k$ 的完全剩余系, 则同余方程组 (2.2) 的解 $x \equiv \sum_{i=1}^{k} M_i M_i^{-1} b_i \pmod{m}$ 遍历模 $m = m_1 m_2 \cdots m_k$ 的完全剩余系.

证 当 $b_1, b_2, \cdots, b_k$ 分别遍历模 $m_1, m_2, \cdots, m_k$ 时, 令 $x_0 = \sum_{i=1}^{k} M_i^{-1} M_i b_i$, 则 x_0 遍历 $m_1 m_2 \cdots m_k$ 个数. 这 m 个数是两两不同余的, 这是因为若

$$\sum_{i=1}^{k} M_i^{-1} M_i b_i' \equiv \sum_{i=1}^{k} M_i^{-1} M_i b_i'' \pmod{m}$$

则 $M_i^{-1} M_i b_i' \equiv M_i^{-1} M_i b_i'' \pmod{m_i}$, $i = 1, 2, \cdots, k$. 即 $b_i' \equiv b_i'' \pmod{m_i}$, $i = 1, 2, \cdots, k$. 但 b_i', b_i'' 是模 m_i 的同一完全剩余系中的二数, 故 $b_i' = b_i''$, $i = 1, 2, \cdots, k$. 所以 x_0 遍历模 m 的完全剩余系. □

2.3 费马小定理与欧拉公式

2.3.1 费马小定理

定理 2.3.1 (费马小定理, Fermat's little theorem) 设 p 为素数, $a \not\equiv 0 \pmod{p}$ (即 $p \nmid a$) (a 为整数), 则

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

(也可叙述为: $a^p \equiv a \pmod{p}$, 对任意整数 a.)

证 对 a 用数学归纳法. $a=1$ 时显然成立. 设 $a^p \equiv a \pmod p$ 成立. 考察

$$(a+1)^p = a^p + \cdots + \mathrm{C}_p^k a^k + \cdots + 1,\ \mathrm{C}_p^k = \frac{p(p-1)\cdots(p-k+1)}{k!},$$

C_p^k 是整数, 是 p 的倍数 (分子的 p 不可能被分母消去, 因 $0<k<p$), 故

$$\begin{aligned}(a+1)^p &\equiv a^p + 0 + \cdots + 0 + \cdots 0 + 1\\ &\equiv a^p + 1 \equiv a+1 \pmod p.\end{aligned}$$ □

我们可使用费马小定理简化计算. 例如, 为计算 $2^{35} \pmod 7$, 可利用 $2^6 \equiv 1 \pmod 7$. 所以把 35 分解为 $35 = 6\cdot 5 + 5$, 计算

$$2^{35} = 2^{6\cdot 5+5} = \left(2^6\right)^5 \cdot 2^5 \equiv 1^5 \cdot 2^5 \equiv 32 \equiv 4 \pmod 7.$$

类似地, 假设要解同余方程 $x^{103} \equiv 4 \pmod{11}$. 肯定有 $x \not\equiv 0 \pmod{11}$, 因此由费马小定理得

$$x^{10} \equiv 1 \pmod{11}.$$

进而 $x^{100} \equiv 1 \pmod{11}$, 两边乘 x^3 得 $x^{103} \equiv x^3 \pmod{11}$. 要解原同余方程, 只需解 $x^3 \equiv 4 \pmod{11}$. 进而得到原方程的解为 $x \equiv 5 \pmod{11}$.

利用费马小定理还可以得到下面的重要定理.

定理 2.3.2 (i) 设 p 为素数, 则 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$ 的元素恰为多项式 $x^p - x$ 的 p 个根, 即

$$x^p - x \equiv x(x-\overline{1})(x-\overline{2})\cdots[x-(\overline{p-1})].$$

或者说, $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{\overline{0}\}$ 恰为 $x^{p-1} - \overline{1}$ 的 $p-1$ 个根:

$$x^{p-1} - \overline{1} \equiv (x-\overline{1})\cdots[x-(\overline{p-1})].$$

(ii) **(威尔逊 (Wilson) 定理)** p 为素数当且仅当

$$(p-1)! \equiv -1 \pmod p.$$

证 (i) 设 $\overline{a} \in \mathbb{F}_p$, 则 $\overline{a^p} = \overline{a}$ (费马小定理), 故 $\overline{a}$ 是 $x^p - x$ 的根. $\overline{a} \in \mathbb{F}_p$ 共 p 个取值, 故 $x^p - x \equiv x(x-\overline{1})(x-\overline{2})\cdots[x-(\overline{p-1})]$.

(ii) 对 $x^{p-1} - \overline{1} \equiv (x-\overline{1})\cdots[x-(\overline{p-1})]$, 令 $x=0$ 则得威尔逊的等式. 反之, 设

$$(p-1)! \equiv -1 \pmod p.$$

则对任意 $d \mid p$ 有 $(p-1)! \equiv -1 \pmod d$. 若 $d < p$ 则此式化为 $0 \equiv -1 \pmod d$ (因为 $d \mid (p-1)!$), 则 $d=1$. 这说明 p 的因数只有 1 和 p, 故 p 为素数. □

对不是素数的 m, $(m-1)! \bmod m$ 也是确定的.

定理 2.3.3 设 m 是合数, 如果 $m=4$, 那么 $(m-1)!\equiv 2 \pmod m$; 如果 $m\geqslant 6$, 那么 $(m-1)!\equiv 0 \pmod m$.

证 设 m 是合数, $m=m_1m_2$. 若 $m_1\neq m_2$, 则由于 m_1 和 m_2 都出现在乘积

$$(m-1)!=1\cdot 2\cdot 3\cdots(m-2)\cdot(m-1)$$

中, 因而 $m=m_1m_2\mid (m-1)!$, 即 $(m-1)!\equiv 0 \pmod m$. 若 $m_1=m_2$, 即 $m=n^2$, 因 m 是合数故 $n\geqslant 2$, $n=2$ 时, $m=4$, $(4-1)!=6\equiv 2 \pmod 4$; $n>2$ 时, $n<2n<n^2=m$, 则 n 和 $2n$ 都出现在乘积

$$(m-1)!=1\cdot 2\cdot 3\cdots(m-2)\cdot(m-1)$$

中, 因而 $m=n\cdot n\mid n\cdot 2n\mid (m-1)!$, 即 $(m-1)!\equiv 0 \pmod m$. □

所以 $(n-1)! \pmod n$ 的值可以用来判断 n 是否是素数: 如果是 -1, 则 n 是素数; 如果是 0 (或 2), 则 n 是合数.

2.3.2 欧拉函数

以 Φ_m 记 "小于 m 且与 m 互素" 的正整数集合, 即

$$\Phi_m=\{a\mid (a,m)=1,\ 1\leqslant a<m\}.$$

我们知道, Φ_m 是 $\mathbb{Z}/m\mathbb{Z}$ 的单位群 $U(m)$ 的代表元集, Φ_m 称为模 m 的**最小正既约剩余系**, 简称既约系. 更一般地, 在 $U(m)$ 中的每个同余类中取一个代表元得到的集合, 称为模 m 的一个**既约 (剩余) 系** (或缩系, reduced residue system), Φ_m 是最常用的既约系. $U(p)$ 与 Φ_m 的元素个数相同, 记为 $\varphi(m)$, 即

$$\varphi(m)=\#\Phi_m=\#\{a\mid (a,m)=1,\ 1\leqslant a<m\}.$$

是 $\mathbb{Z}/m\mathbb{Z}$ 中的可逆元个数. 称 φ 为**欧拉函数** (Euler's totient function). 例如,

$$\varphi(1)=1 \text{ (规定)},\ \varphi(2)=1,\ \varphi(3)=2,\ \varphi(4)=2,\ \varphi(5)=4\cdots.$$

定理 2.3.4 (i) 任意 $\varphi(m)$ 个与 m 互素的且模 m 互不同余的正整数构成模 m 的一个既约剩余系.

(ii) 设 $(u,m)=1$, 则整数集 S 与 $uS=\{us\mid s\in S\}$ 同时是或不是模 m 的一个既约剩余系. 特别知, $u\Phi_m$ 是模 m 的一个既约剩余系.

证 (i) 显然这些整数代表的同余类不同, 都属于 $U(m)$, 且与 $U(m)$ 中同余类个数相同.

(ii) 若 S 是模 m 的一个既约剩余系, 对互异的 $s_1,s_2\in S$, 必然

$$us_1\not\equiv us_2 \pmod m,$$

否则将导致 $s_1=s_2 \pmod m$ (因为 u 与 m 互素), 从而 $s_1=s_2$. 故 uS 是模 m 互不同余的 $\varphi(m)$ 个与 m 互素的正整数, 构成模 m 的一个既约剩余系. 反之, 同理可证. □

定理 2.3.5 设 m,n 为互素正整数, 记 $m\Phi_n+n\Phi_m=\{mx+ny\mid x\in\Phi_n,y\in\Phi_m\}$, 则

$$m\Phi_n+n\Phi_m\equiv\Phi_{mn}\pmod{mn}$$

(即两个集合的元素之间对应同余). 也可叙述为: 当 x,y 分别遍历模 n 和模 m 的既约剩余系时, $mx+ny$ 遍历模 mn 的既约剩余系.

证 因 n 和 y 均与 m 互素, 故 $(mx+ny,m)=(ny,m)=1$. 同理

$$(mx+ny,n)=1.$$

故

$$(mx+ny,mn)=1,$$

所以左边属于右边.

因为 $mx+ny$ 模 m 和模 n 相互都不同余, 所以 $\{mx+ny\}$ 互不同余 $\pmod{mn}$. 任取 $a\in\Phi_{mn}$, 则 a 与 m 互素, 故 a 同余于 $n\Phi_m$ 中某元 $\pmod m$ ($n\Phi_m$ 也是模 m 既约剩余系), 设为 $a\equiv ny\pmod m$, $y\in\Phi_m$. 同理得

$$a\equiv mx\pmod n,\ x\in\Phi_n.$$

故 $a\equiv mx+ny$ 对模 m 和模 n 都成立, 即知 $a\equiv mx+ny\pmod{mn}$. 故右边集合中任一元 a 必同余于左边集合中某元素, 即右边属于左边. □

定理 2.3.6 欧拉函数 $\varphi(m)$ 的取值由以下等式决定:

(i) 当 p 为素数时, $\varphi(p)=p-1$;

(ii) 当 p 为素数时, $\varphi\left(p^k\right)=p^{k-1}(p-1)=p^k-p^{k-1}$;

(iii) $\varphi(mn)=\varphi(m)\varphi(n)$ (m,n 互素); (这被简称为 φ 是积性函数. 因而规定 $\varphi(1)=1$.)

(iv) 若 $p_1,\cdots,p_s$ 两两互素, 则

$$\begin{aligned}\varphi(p_1^{k_1}\cdot p_2^{k_2}\cdots p_r^{k_r})&=(p_1^{k_1}-p_1^{k_1-1})\cdot(p_2^{k_2}-p_2^{k_2-1})\cdots(p_r^{k_r}-p_r^{k_r-1})\\&=p_1^{k_1-1}(p_1-1)\cdots p_r^{k_r-1}(p_r-1)\\&=p_1^{k_1}\cdot p_2^{k_2}\cdots p_r^{k_r}\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).\end{aligned}$$

证 (i) 因为每个整数 $1\leqslant a\leqslant p-1$ 与 m 互素.

(ii) p^k 仅有的因数是 p 的幂次, 所以当 a 是 p 的倍数 ($p\mid a$) 时 a 不与 p^k 互素. 所以

$$\varphi\left(p^k\right)=p^k-\#\left\{a\middle|1\leqslant a\leqslant p^k,\,p\mid a\right\}.$$

而 p 的倍数是 p, $2p$, $3p$, $4p$, $\cdots$, $\left(p^{k-1}-2\right)p$, $\left(p^{k-1}-1\right)p$, $p^{k-1}\cdot p$, 共有 p^{k-1} 个, 所以

$$\varphi\left(p^k\right)=p^k-p^{k-1}.$$

(iii) (证法一) $\varphi(mn) = \#\Phi_{mn} = \#(n\Phi_m + m\Phi_n) =^{1} \#(\Phi_m \times \Phi_n) = \varphi(m)\varphi(n)$.

(证法二) 要证 $\varphi(mn) = \varphi(m)\varphi(n)$, 只需证 $\#\Phi_{mn} = \#(\Phi_m \times \Phi_n)$. 作映射

$$\begin{aligned} f: \quad & \Phi_{mn} \to \Phi_m \times \Phi_n \\ & a \bmod mn \mapsto (a \bmod m,\ a \bmod n). \end{aligned}$$

设 $a_1, a_2 \in \Phi_{mn}$, 若 $f(a_1) = f(a_2)$, 即 $a_1 \equiv a_2 \pmod m$ 与 $a_1 \equiv a_2 \pmod n$. 因为 m 与 n 互素, 所以 $a_1 \equiv a_2 \pmod{mn}$, 因此 f 是单射.

对任意 $(b, c) \in \Phi_m \times \Phi_n$, 根据中国剩余定理, 同余方程组

$$\begin{cases} a \equiv b \pmod m \\ a \equiv c \pmod n \end{cases}$$

有解. 即存在 $a \in \Phi_{mn}$ 使得 $f(a) = (b, c)$, 因此 f 是满射.

所以 f 是 $\Phi_{mn} \to \Phi_m \times \Phi_n$ 的双射, 所以 $\#\Phi_{mn} = \#(\Phi_m \times \Phi_n)$.

(iv) 由 (ii), (iii) 显然. □

推论 2.3.7 设 m 有素因数分解 $m = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$, 则

$$\begin{aligned} \varphi(m) &= (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \\ &= p_1^{k_1-1}(p_1 - 1) \cdots p_r^{k_r-1}(p_r - 1) \\ &= m \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)^{2}. \end{aligned}$$

定理 2.3.8 $\sum\limits_{d \mid m} \varphi(d) = m$, 其中 $d > 0$ 是 m 的正因数.

证 (证法一) 考虑 m 个分数: $1/m, 2/m, \cdots, (m-1)/m, m/m$. 将它们皆约化为既约分数. 于是分母均为 m 的因数. 考虑分母为 d 的分数 $*/d$ 全体, 分子取遍与 d 互素而不超过 d 的所有正整数, 故这样的分数共 $\varphi(d)$ 个. 对各 $d \mid m$ 求和, 则得 m.

(证法二) 固定 $d \mid m$, 考虑满足 $(a, m) = d$ 的整数 a 的集合 A_d, 这当且仅当

$$(a/d, m/d) = 1.$$

故满足前式的 a $(1 \leqslant a \leqslant m)$ 是一一对应于满足后式的 $a_1 = a/d$ $(1 \leqslant a_1 \leqslant m/d)$. 而按欧拉 φ 函数的定义知, 后者个数为 $\varphi(m/d)$, 故 $\#A_d = \varphi(m/d)$. 而任意 a $(1 \leqslant a \leqslant m)$ 皆属于某个 A_d (对某个 $d \mid m$). 故

$$m = \sum_{d \mid m} \#A_d = \sum_{d \mid m} \varphi(m/d).$$

[1] 这个等号成立是因为 $\{mx + ny\}$ 互不同余.

[2] 注意计算这个式子只需要知道 m 的所有素因数而不必知道它们的具体幂次.

令 $\delta = m/d$, 则知后者即为 $\sum_{\delta|m} \varphi(\delta)$.

(证法三) 先设 $m = p^e$, 则其因数为 $d = p^k$ $(0 \leqslant k \leqslant e)$, 而 $\varphi\left(p^k\right) = p^k - p^{k-1}$, 故

$$\sum_{d|m} \varphi(d) = \sum_{0\leqslant k\leqslant e} \varphi\left(p^k\right) = 1 + \sum_{1\leqslant k\leqslant e} \left(p^k - p^{k-1}\right) = p^e.$$

再设 $m = p_1^{e_1} \cdots p_s^{e_s}$ 为其因数分解, 则因数 d 可能为

$$p_1^{k_1} \cdots p_s^{k_s} \quad (0 \leqslant k_i \leqslant e_i,\, 1 \leqslant i \leqslant s),$$

故

$$\begin{aligned}\sum_{d|m} \varphi(d) &= \sum_{k_1,\cdots,k_s} \varphi\left(p_1^{k_1} \cdots p_s^{k_s}\right) = \sum_{k_1,\cdots,k_s} \varphi\left(p_1^{k_1}\right) \cdots \varphi\left(p_s^{k_s}\right) \\ &= \sum_{k_1} \varphi\left(p_1^{k_1}\right) \cdots \sum_{k_s} \varphi\left(p_s^{k_s}\right) = p_1^{e_1} \cdots p_s^{e_s} = m.\end{aligned}$$

□

2.3.3 欧拉公式

欧拉公式是费马小定理的推广.

定理 2.3.9 (欧拉公式, Euler's Formula) 设整数 a 与 m 互素, 则

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

其中 φ 是欧拉函数.

证 设 $\Phi_m = \left\{k_1, \cdots, k_{\varphi(m)}\right\}$ 是 "小于 m 且与 m 互素" 的正整数集合. 令

$$a\Phi_m = \left\{ak_1, \cdots, ak_{\varphi(m)}\right\}.$$

由定理 2.3.4, $a\Phi_m$ 与 Φ_m 的元素模 m 同余. 将每个集合的元素各自乘起来, 得到

$$\begin{aligned}ak_1 \cdot ak_2 \cdots ak_{\varphi(m)} &\equiv k_1 \cdot k_2 \cdots k_{\varphi(m)} \pmod{m}, \\ a^{\varphi(m)} &\equiv 1 \pmod{m}.\end{aligned}$$

(因 $k_1, \cdots, k_{\varphi(m)}$ 与 m 互素, 可以约化去.) □

定理 2.3.10 设 $\Phi_m = \{b_1, b_2, \cdots, b_{\varphi(m)}\}$ 是 1 与 m 之间且与 m 互素的整数 (包括 1), $B = b_1b_2b_3 \cdots b_{\varphi(m)}$ 是它们的乘积[1]. 则 $B \equiv \pm 1 \pmod{m}$.

证 因为 $(b_i, m) = 1$, 所以 b_i 模 m 可逆, 即对于每个 b_i 都有一个 b_j (可能等于 b_i) 使得 $b_ib_j \equiv 1 \pmod{m}$. 所以对于每个 b_i, 要么有与 b_i 不同的 b_j 使得 $b_ib_j \equiv 1 \pmod{m}$, 在这种情

[1] 这个乘积出现在了欧拉公式的证明中, 虽然它在证明中用不上, 因为我们直接约去了它.

况下我们可以从乘积 B 中除去 b_i 和 b_j; 要么 $b_i^2 \equiv 1 \pmod{m}$. 因此 B 等于那些满足 $b_i^2 \equiv 1 \pmod{m}$ 的 b_i 的乘积. 我们记 $c_1, c_2, \ldots, c_r$ 为这些特殊的 b_i.

现在考虑同余方程 $c_i x \equiv -1 \pmod{m}$, 因为 $(b_i, m) = 1$, 所以方程只有一个解, 设为 $x \equiv d \pmod{m}$. 对 $c_i d \equiv -1 \pmod{m}$ 的两边平方并使用 $c_i^2 \equiv 1 \pmod{m}$ 的事实, 我们有 $d^2 \equiv 1 \pmod{m}$, 所以 d 必须是 c_j 之一. 而 d 显然不是 c_i, 因为 $c_i^2 \equiv 1$ 而不是 -1. 通过这种方式, 每个 c_i 都与不同的 c_j 配对. 因为乘积 $c_i c_j$ 为 -1, 这意味着 B 是若干个 -1 的乘积, 即 $B \equiv \pm 1 \pmod{m}$. □

2.4 同余方程 2: 高次同余方程

2.4.1 模 p 多项式的根数

我们知道一个 d 次实系数多项式的实根不超过 d 个. 这个结论对同余方程并不一定成立. 例如, 同余方程

$$x^2 + x \equiv 0 \pmod{6}$$

有 4 个模 6 不同的根: $0, 2, 3, 5$. 然而, 对模是素数的同余方程, 这个结论依然成立.

定理 2.4.1 (拉格朗日定理, Lagrange's theorem) 设 p 为素数,

$$f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d$$

是次数为 $d \geqslant 1$ 的整系数多项式, 且 p 不整除 a_0, 则同余方程

$$f(x) \equiv 0 \pmod{p}$$

最多有 d 个模 p 不同余的解.

证 用反证法. 假设至少存在一个首项系数不被 p 整除的整系数多项式 $F(x)$, 使得同余式 $F(x) \equiv 0 \pmod{p}$ 模 p 不同余的根的个数大于 $F(x)$ 的次数. 在所有这样的多项式中选择一个次数最低的, 设为

$$F(x) = A_0 x^d + A_1 x^{d-1} + \cdots + A_d.$$

设

$$r_1, r_2, \cdots, r_{d+1}$$

是同余式 $F(x) \equiv 0 \pmod{p}$ 模 p 不同余的解.

先证明对任意值 r, $F(x) - F(r)$ 是可约的.

$$F(x) - F(r) = A_0 \left(x^d - r^d\right) + A_1 \left(x^{d-1} - r^{d-1}\right) + \cdots + A_{d-1}(x - r).$$

由于

$$x^i - r^i = (x - r)\left(x^{i-1} + x^{i-2} r + \cdots + x r^{i-2} + r^{i-1}\right),$$

因此每项 $x^i - r^i$ 中都有 $x - r$ 这个因式, 提取 $x - r$, 得

$$F(x) - F(r) = (x - r)(\text{某个次数为 } d-1 \text{ 的多项式}),$$

即存在次数为 $d-1$ 的多项式

$$G(x) = B_0 x^{d-1} + B_1 x^{d-2} + \cdots + B_{d-2} x + B_{d-1},$$

使得

$$F(x) = F(r) + (x - r)G(x).$$

特别地, 取 $r = r_1$, 由 $F(r_1) \equiv 0 \pmod{p}$ 得

$$F(x) = (x - r_1)\, G(x) \pmod{p}.$$

我们已经假设 $F(x) \equiv 0 \pmod{p}$ 有 $d+1$ 个互不同余的解 $x = r_1, r_2, \cdots, r_{d+1}$, 让 x 取某个解 r_k $(k \geqslant 2)$ 得

$$0 \equiv F(r_k) = (r_k - r_1)\, G(r_k) \pmod{p}.$$

因为 r_1 与 r_k 模 p 不同余, 由素数整除性质得 $G(r_k) \equiv 0 \pmod{p}$ (注意这里用了 p 是素数这一条件). 现在 $r_2, r_3, \cdots, r_{d+1}$ 都是 $G(x) \equiv 0 \pmod{p}$ 的解, 于是 $G(x)$ 就是一个次数为 $d-1$ 且有 d 个模 p 不同余的解的多项式. 这与 $F(x)$ 是次数最低的这种类型的多项式相矛盾. □

定理 2.4.2 设 p 是素数, 若同余方程

$$x^2 \equiv a \pmod{p},$$

有一个解[1] $x_0 \pmod{p}$, 则方程还有一解 $-x_0 \pmod{p}$, 且方程有且仅有这两个解 $\pm x_0 \pmod{p}$. 特别地, $x^2 \equiv 1 \pmod{p}$ 的解为 $x \equiv \pm 1 \pmod{p}$.

证 $-x_0 \equiv p - x_0 \pmod{p}$, 而

$$(p - x_0)^2 = \left(p^2 - 2px_0 + x_0^2\right) \equiv x_0^2 \equiv a \pmod{p}.$$

再根据拉格朗日定理, 方程至多有两个解, 故方程有且仅有这两个解 $\pm x_0 \pmod{p}$. □

利用这一定理还可以给出威尔逊定理 (定理 2.3.2 (ii)) 充分性的一种更直观的证法.

定理 2.4.3 (威尔逊 (Wilson) 定理) p 为素数当且仅当

$$(p-1)! \equiv -1 \pmod{p}.$$

证′ (充分性) 设 p 是素数, 则所有 $1, 2, \cdots, p-1$ 模 p 可逆, 即对 $a \in \{1, 2, \cdots, p-1\}$, 有 $a^{-1} \in \{1, 2, \cdots, p-1\}$ 使得 $a \cdot a^{-1} \equiv 1 \pmod{p}$. 若 $a \equiv a^{-1} \pmod{p}$, 即 $a^2 \equiv 1 \pmod{p}$, 这时

[1] 对这个方程解的存在性会在平方剩余部分讨论.

$a = 1, p-1$, 所以对余下的数 $2, \cdots, p-2$ 可以两两配对[1]且乘积为 1, 所以可以在乘积 $(p-1)!$ 中除去它们, 所以

$$(p-1)! \equiv 1 \cdot p - 1 \equiv -1 \pmod{p}. \qquad \square$$

下面我们进一步研究一下多项式的根与次数相等的情况.

定理 2.4.4 若 $n \leqslant p$, $\deg f(x) = n$, 则同余方程

$$f(x) \equiv 0 \pmod{p},$$

有 n 个解的充分与必要条件是 $x^p - x$ 除以 $f(x)$ 所得余式 $r(x) \equiv 0 \pmod{p}$ (即一切系数都是 p 的倍数)[2].

证 对 $f(x)$ 作带余除法, 存在 $q(x)$ 及 $r(x)$ 使得

$$x^p - x = f(x)q(x) + r(x), \tag{2.3}$$

且 $\deg r(x) < n$, $\deg q(x) p - n$. 若原方程有 n 个解, 则由费马小定理知这 n 个解都是 $x^p - x \equiv 0 \pmod{p}$ 的解. 因此这 n 个解也是 $r(x) \equiv 0 \pmod{p}$ 的解. 但 $r(x)$ 的次数小于 n, 故 $r(x) \equiv 0 \pmod{p}$. 反之, 若 $r(x) \equiv 0 \pmod{p}$ 则由 (2.3) 及费马小定理知, 对任何整数 x 都有

$$f(x)q(x) \equiv 0 \pmod{p}. \tag{2.4}$$

即 (2.4) 有 p 个不同的解 $(x \equiv 0, 1, \cdots, p-1 \pmod{p})$. 假设 $f(x) \equiv 0 \pmod{p}$ 的解数 $k < n$, 而由于 $\deg q(x) = p - n$ 有 $q(x) \equiv 0 \pmod{p}$ 的解数 $h \leqslant p - n$. 于是 (2.4) 的解数 $\leqslant k + h < p$, 矛盾. $\square$

2.4.2 高次同余方程的解数及解法

定理 2.4.5 若 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数, $m = m_1 m_2 \cdots m_k$, 则同余方程

$$f(x) \equiv 0 \pmod{m} \tag{2.5}$$

与同余方程组

$$f(x) \equiv 0 \pmod{m_i},\ i = 1, 2, \cdots, k \tag{2.6}$$

等价. 并且若用 T_i 表示 $f(x) \equiv 0 \pmod{m_i}$, $i = 1, 2, \cdots, k$, 对模 m_i 的解数, T 表示 $f(x) \equiv 0 \pmod{m}$ 对模 m 的解数, 则

$$T = T_1 T_2 \cdots T_k.$$

[1] 这些数一定是偶数个, 因为 $p = 2$ 时 $1 = p - 1$, 否则 p 为奇数.

[2] 因为 $\mathbb{Z}/p\mathbb{Z}$ 是域, 所以 $\mathbb{Z}/p\mathbb{Z}[x]$ 中的多项式可以作带余除法.

证 先证 (2.5), (2.6) 等价. 设 x_0 是 (2.5) 的解, 则

$$f(x_0) \equiv 0 \pmod{m}.$$

由 $m_i \mid m$ 有

$$f(x_0) \equiv 0 \pmod{m_i},\ i = 1, 2, \cdots, k.$$

反之, 若 x_0 是 (2.6) 的解, 则

$$f(x_0) \equiv 0 \pmod{m_i},\ i = 1, 2, \cdots, k.$$

由 $m_1, m_2, \cdots, m_k$ 两两互素有 $m = m_1 m_2 \cdots m_k = [m_1, m_2, \cdots, m_k]$, 从而

$$f(x_0) \equiv 0 \pmod{m},$$

故 (2.5), (2.6) 等价.

设 $f(x) \equiv 0 \pmod{m_i}$ 的 T_i 个不同解是

$$x \equiv b_{it_i} \pmod{m_i},\ t_i = 1, 2, \cdots, T_i,$$

则 (2.6) 的解即下列诸同余方程组的解:

$$\begin{cases} x \equiv b_{1t_1} \pmod{m_1}, \\ x \equiv b_{2t_2} \pmod{m_2}, \\ \cdots\cdots \\ x \equiv b_{kt_k} \pmod{m_k}, \end{cases} \tag{2.7}$$

其中 $t_i = 1, 2, \cdots, T_i$, $i = 1, 2, \cdots, k$. 所以 (2.5) 的解与 (2.7) 的解相同. 由中国剩余定理知 (2.7) 中每一同余式组对模 m 恰有一解, 故 (2.7) 有对模 m 的 $T_1 T_2 \cdots T_k$ 个解. 又根据定理 2.2.3 可知此 $T_1 T_2 \cdots T_k$ 个解对模 m 两两不同余. 故 (2.5) 对模 m 的解数是

$$T = T_1 T_2 \cdots T_k.$$

□

例 2.4.6 解同余方程

$$f(x) \equiv 0 \pmod{35}, f(x) = x^4 + 2x^3 + 8x + 9.$$

解 原方程与同余方程组

$$\begin{cases} f(x) \equiv 0 \pmod{5} \\ f(x) \equiv 0 \pmod{7} \end{cases}$$

等伶. 容易验证第一个同余方程有两个解:

$$x \equiv 1, 4 \pmod{5},$$

而第二个同余方程有三个解:

$$x \equiv 3, 5, 6 \pmod 7.$$

故原方程有 $2 \cdot 3 = 6$ 个解. 即诸同余方程组

$$\begin{cases} x \equiv b_1 \pmod 5,\ b_1 = 1, 4 \\ x \equiv b_2 \pmod 7,\ b_2 = 3, 5, 6 \end{cases}$$

把 b_1, b_2 的值分别代人解 6 个线性同余方程组即得原方程的全部解:

$$x \equiv 31,\ 26,\ 6,\ 24,\ 19,\ 34 \pmod{35}.$$

2.5 模 m 的幂与根

2.5.1 模 m 的幂与逐次平方法

本节考虑如何计算模 m 下的幂 $a^k \pmod m$. 我们知道这可以用费马小定理 (m 是素数时) 或欧拉公式来简化计算, 但有时在 "简化" 之后仍会十分复杂. 如计算

$$5^{100000000000000} \pmod{12830603}.$$

由于 $12830603 = 3571 \cdot 3593$ 故

$$\varphi(12830603) = \varphi(3571)\varphi(3593) = 3570 \cdot 3592 = 12823440.$$

根据欧拉公式, 可用

$$100000000000000 = 7798219 \cdot 12823440 + 6546640$$

来 "简化" 我们的问题:

$$\begin{aligned} 5^{100000000000000} &= \left(5^{12823440}\right)^{7798219} \cdot 5^{6546640} \\ &\equiv 5^{6546640} \pmod{12830603}. \end{aligned}$$

这仍十分复杂! 这时可以用一种巧妙的方法——逐次平方法.

定理 2.5.1 (逐次平方法计算 $a^k \pmod m$) 1. 将 k 作二进制展开:

$$k = u_0 + u_1 \cdot 2 + u_2 \cdot 2^2 + u_3 \cdot 2^3 + \cdots + u_r \cdot 2^r,$$

其中每个 u_i 是 0 或 1 (即二进制 $u_r u_{r-1} \cdots u_1 u_0$).

2. 使用**逐次平方法** (Method of Successive Squaring) 制作模 m 的 a 的幂次表.

$$\begin{aligned}
a^1 &\equiv A_0 \pmod m\\
a^2 \equiv \left(a^1\right)^2 &\equiv A_0^2 \equiv A_1 \pmod m\\
a^4 \equiv \left(a^2\right)^2 &\equiv A_1^2 \equiv A_2 \pmod m\\
a^8 \equiv \left(a^4\right)^2 &\equiv A_2^2 \equiv A_3 \pmod m\\
&\cdots\cdots\\
a^{2^r} \equiv \left(a^{2^r-1}\right)^2 &\equiv A_{r-1}^2 \equiv A_r \pmod m
\end{aligned}$$

注意要计算表的每一行, 仅需要取前一行最末的数, 平方它然后模 m 取余数.

3. 计算

$$\begin{aligned}
a^k &= a^{u_0+u_1\cdot 2+u_2\cdot 2^2+u_3\cdot 2^3+\cdots+u_r\cdot 2^r} && \text{使用第一步,}\\
&= a^{u_0}\cdot\left(a^2\right)^{u_1}\cdot\left(a^{2^2}\right)^{u_2}\cdots\left(a^{2^r}\right)^{u_r}\\
&\equiv A_0^{u_0}\cdot A_1^{u_1}\cdot A_2^{u_2}\cdots A_r^{u_r} \pmod m && \text{使用第二步的表.}
\end{aligned}$$

注意到所有 u_i 是 0 或 1, 因此这个数实际上是 u_i 等于 1 的那些 A_i 的乘积.

注 将 10 进制数转为 2 进制数可以用短除法, 将余数倒排即得 2 进制数. 如将 13 转为二进制数为 1101:

2	13	1
2	6	0
2	3	1
	1	1

即 $13 = 1\cdot 2^0 + 0\cdot 2^1 + 1\cdot 2^2 + 1\cdot 2^3$.

例 2.5.2 用逐次平方法计算 $7^{327} \pmod{853}$.

解 首先, $327 = 2^8+2^6+2^2+2^1+2^0 = 256+64+4+2+1$. 再制作 7 的模 853 的幂次表:

$$\begin{aligned}
7^1 &\equiv 7 \equiv 7 \pmod{853}\\
7^2 \equiv \left(7^1\right)^2 &\equiv 7^2 \equiv 49 \equiv 49 \pmod{853}\\
7^4 \equiv \left(7^2\right)^2 &\equiv 49^2 \equiv 2401 \equiv 695 \pmod{853}\\
7^8 \equiv \left(7^4\right)^2 &\equiv 695^2 \equiv 483025 \equiv 227 \pmod{853}\\
7^{16} \equiv \left(7^8\right)^2 &\equiv 227^2 \equiv 51529 \equiv 349 \pmod{853}\\
7^{32} \equiv \left(7^{16}\right)^2 &\equiv 349^2 \equiv 121801 \equiv 675 \pmod{853}\\
7^{64} \equiv \left(7^{32}\right)^2 &\equiv 675^2 \equiv 455625 \equiv 123 \pmod{853}\\
7^{128} \equiv \left(7^{64}\right)^2 &\equiv 123^2 \equiv 15129 \equiv 628 \pmod{853}\\
7^{256} \equiv \left(7^{128}\right)^2 &\equiv 628^2 \equiv 394384 \equiv 298 \pmod{853}
\end{aligned}$$

最后计算

$$\begin{aligned} 7^{327} &= 7^{256+64+4+2+1} = 7^{256}\cdot 7^{64}\cdot 7^{4}\cdot 7^{2}\cdot 7^{1}\ [1] \\ &\equiv 298\cdot 123\cdot 695\cdot 49\cdot 7 \pmod{853} \\ &\equiv 828\cdot 695\cdot 49\cdot 7 \pmod{853} \\ &\equiv 538\cdot 49\cdot 7 \pmod{853} \\ &\equiv 772\cdot 7\equiv 286 \pmod{853} \end{aligned}$$

即得到

$$7^{327}\equiv 286 \pmod{853}.$$

2.5.2 模 m 的 k 次根

前一节学习了当 k 与 m 很大时, 如何计算模 m 的 k 次幂. 现在考虑其相反方向, 如何计算模 m 的 k 次根, 即求解同余方程

$$x^k\equiv b \pmod{m}.$$

事实上, 如果已知 $\varphi(m)$ 的值, 则可相当容易地计算 b 模 m 的 k 次根.

定理 2.5.3 (计算模 m 的 k 次根) 设 b,k 与 m 是已知整数, 满足 $(b,m)=1$ 与 $(k,\varphi(m))=1$. 可用下述步聚求解同余方程

$$x^k\equiv b \pmod{m}.$$

1. 计算 $\varphi(m)$.

2. 求解满足 $ku\equiv 1 \pmod{\varphi(m)}$ 的 u [2], 即 u 是 $k \pmod{\varphi(m)}$ 的逆 (因此 $ku=1+\varphi(m)v$).

3. 用逐次平方法计算 $b^u \pmod{m}$. 所得值给出解 x. 这成立是因为

$$\begin{aligned} x^k &= (b^u)^k && \text{将 } x=b^u \text{ 代入 } x^k, \\ &= b^{uk} && \\ &= b^{1+\varphi(m)v} && \text{用第二步,} \\ &= b\cdot\left(b^{\varphi(m)}\right)^v && \\ &\equiv b \pmod{m} && \text{由欧拉公式 } b^{\varphi(m)}\equiv 1 \pmod{m}\ [3]. \end{aligned}$$

例 2.5.4 解同余方程

$$x^{131}\equiv 758 \pmod{1073}.$$

[1] 计算这个乘积时, 可以逐步把两个数相乘并模 853 取余.

[2] 这里就是要求 $(k,\varphi(m))=1$ 的原因.

[3] 这里就是要求 $(b,m)=1$ 的原因.

解 第一步计算 $\varphi(1073)$. 将 1073 素因数分解 $1073 = 29 \cdot 37$, 所以 $\varphi(1073) = \varphi(29) \cdot \varphi(37) = 28 \cdot 36 = 1008$.

下一步解方程 $131u \equiv 1 \pmod{1008}$, 这可通过辗转相除法求解 $131u - 1008v = 1$ 实现, 注意这里需要 u 是正数, 这可以通过将求出的解加 1008 的若干倍实现.

最后, 使用逐次平方法计算 $758^{731} \pmod{1073}$. 得到答案 $x \equiv 905 \pmod{1073}$. 作为验证, 还可用逐次平方法来证明 905^{131} 确实与 758 模 1073 同余.

2.6 素性测试与卡米歇尔数

费马小定理可用于素性测试. 根据费马小定理, 如果 p 是素数, 则对每个整数 a, 有

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

因此若有整数 a 使得 $a^p \not\equiv a \pmod{p}$, 则 p 不是素数. 但反之不成立, 即存在合数 n, 也使得对每个整数 a, 有 $a^n \equiv a \pmod{n}$ 成立, 这样的合数称为卡米歇尔数.

2.6.1 卡米歇尔数

定义 2.6.1 (卡米歇尔数) 对合数 n, 如果对每个整数 a, 都有

$$a^n \equiv a \pmod{n},$$

则这样的的 n 称为**卡米歇尔数** (Carmichael number).

10000 以内的所有卡米歇尔数为:

$$561,\ 1105,\ 1729,\ 2465,\ 2821,\ 6601,\ 8911.$$

定理 2.6.2 (卡米歇尔数的考塞特判别法, Korselt's Criterion for Carmichael Numbers) 设 n 是合数. 则 n 是卡米歇尔数当且仅当它是奇数, 且 n 的每个素因数 p 满足下述两个条件:

(i) $p^2 \nmid n$ (即 p 的素因数的次数都是 1, 或者说卡米歇尔数是不同素数的乘积).

(ii) $p - 1 \mid n - 1$.

证 (充分性) 设 n 是卡米歇尔数. 取 $a = n - 1 \equiv -1 \pmod{n}$, 根据 $a^n \equiv a \pmod{n}$ 得

$$(-1)^n \equiv -1 \pmod{n}.$$

这蕴涵 n 是奇数 (或 $n = 2$, 但 n 是合数故 $n \neq 2$).

设 p 是 n 的一个素因数, p^{e+1} 是整除 n 的 p 的最大幂次. 取 $a = p^e$, 由于 n 是卡米歇尔数有

$$p^{en} \equiv p^e \pmod{n}.$$

即 $n \mid p^{en}-p^e$, 由假设 $p^{e+1} \mid n$, 得 $p^{e+1} \mid p^{en}-p^e$, 即 $p \mid p^{en-e}-1$. 因为 $p>1$, 所以 $en-e=0$, 即 $e=0$. 这就证明了 n 满足 (i).

下面用原根的方法来证明 n 满足 (ii). 我们在后面会证明对每个素数 p, 至少存在一个数 g, 其幂 $g, g^2, g^3, \cdots, g^{p-1}$ 都是模 p 不同余的 (这样的数称为原根). 对 n 的素因数 p, 取 $a=g$ 为模 p 原根. 有 $g^n \equiv g \pmod{n}$ 有 $g^n \equiv g \pmod{p}$. 作带余除法 n 除以 $p-1$, 存在 k, j 使得

$$n=(p-1)k+j.$$

根据费马小定理,

$$g^n=\left(g^{p-1}\right)^k \cdot g^j \equiv g^j \pmod{p},$$

所以

$$g^j \equiv g \pmod{p}.$$

但由于 g 是模 p 原根, 所以数 $1, g, g^2, \ldots, g^{p-2}$ 都是模 p 不同余的, 因此 $j=1$. 这说明

$$n=(p-1)k+1,$$

即 $p-1 \mid n-1$.

(必要性) 设 n 是满足 (i), (ii) 的奇合数. 将 n 素因数分解

$$n=p_1p_2p_3\cdots p_r,$$

由条件 (i) 得 $p_1, p_2, \cdots, p_r$ 是互不相同的素数, 由条件 (ii) 得每个 p_i-1 整除 $n-1$, 即存在 k_i, 使得

$$n-1=(p_i-1)\,k_i,$$

任取一个整数 a, 计算 $a^n \pmod{p_i}$ 的值如下: 首先, 如果 $a \equiv 0 \pmod{p_i}$, 则显然有

$$a^n \equiv 0 \equiv a \pmod{p_i}.$$

否则 $a \not\equiv 0 \pmod{p_i}$, 这时我们可用费马小定理计算

$$\begin{aligned} a^n &= a^{(p_i-1)k_i+1} && \text{因为 } n-1=(p_i-1)\,k_i, \\ &= \left(a^{p_i-1}\right)^{k_i} \cdot a \\ &\equiv 1^{k_i} \cdot a \pmod{p_i} && \text{由费马小定理, } a^{p_i-1} \equiv 1 \pmod{p_i}, \\ &\equiv a \pmod{p_i}. \end{aligned}$$

现在我们已证明对每个 $i=1,2,\cdots,r$, 有

$$a^n \equiv a \pmod{p_i}.$$

因为 p_i 是不同的素数, 所以 $n=p_1p_2p_3\cdots p_r=[p_1, p_2, \cdots, p_r]$, 因此,

$$a^n \equiv a \pmod{n},$$

所以 n 是卡米歇尔数. □

用与上述证明充分性部分 (ii) 相同的方法还可证明 $p-1$ 实际上整除比较小的数 $\frac{n}{p}-1$.

推论 2.6.3 如果 n 是卡米歇尔数, p 是 n 的素因数, 则 $p-1 \mid \frac{n}{p}-1$.

证 令 $m=n/p$, 对 m 作带余除法 $m=(p-1)u+v$. 和上面的证明一样取模 p 原根 g, 用 $g^p \equiv g \pmod p$ 得到

$$\begin{aligned} g^n &= g^{pm} \\ &= (g^p)^{(p-1)u+v} \\ &\equiv g^v \pmod p \quad \text{因为 } g^p \equiv g \pmod p \text{ 及 } g^{p-1} \equiv 1 \pmod p. \end{aligned}$$

与上面证明中相同的论证可用得出 $v=1$ 的结论, 因此 $(n/p)-1=m-1=(p-1)u$. □

推论 2.6.4 不存在仅有两个素因数的卡米歇尔数.

证 假设 n 是卡米歇尔数且 $n=pq$ 只有两个素因数. 根据上推论 $p-1 \mid (n/p)-1$, 所以 $p-1 \mid q-1$. 交换 p 和 q 的角色, 我们发现 $q-1$ 也可以整除 $p-1$. 这意味着 $p=q$, 所以 $n=p^2$, 与 n 是卡米歇尔数矛盾. 这证明不存在只有两个素因数的卡米歇尔数. □

2.6.2 拉宾-米勒测试

卡米歇尔数存在的事实意味着我们需要一个更好的检验合数的办法, 一种方法是拉宾-米勒测试, 它基于下述事实.

定理 2.6.5 (素数的一个性质) 设 p 是奇素数, 记

$$p-1=2^k q,\ q\text{是奇数}.$$

设 a 是不被 p 整除的整数. 则下述两个条件之一成立:

(i) $a^q \equiv 1 \pmod p$.

(ii) 数 $a^q, a^{2q}, a^{2^2 q}, \cdots, a^{2^{k-1}q}$ 之一模 p 余 -1.

证 根据费马小定理 $a^{p-1} \equiv 1 \pmod p$. 这意味着当我们考察数表

$$a^q,\ a^{2q},\ a^{4q}, \cdots,\ a^{2^{k-1}q},\ a^{2^k q}$$

时, 得到表中的最后一个数等于 $1 \pmod p$ (因为 $2^k q$ 等于 $p-1$), 此外, 表中的每个数是前一个数的平方. 因此下述两种可能之一必成立:

(i) 表中的第一个数等于 $1 \pmod p$.

(ii) 表中的一些数不等于 $1 \pmod p$, 但平方后它就等于 $1 \pmod p$. 具有这种特点的数等于 $-1 \pmod p$, 所以在这种情况下, 表包含 $-1 \pmod p$. □

从上面素数的性质出发, 我们得到被称为拉宾-米勒测试的合数试验: 如果 n 是奇数, 且 n 没有定理中描述的素数性质, 则它必是合数; 对 a 的许多不同值, 如果 n 确实具有上面的素数性质, 则 n 可能是素数.

定理 2.6.6 (合数的拉宾-米勒测试, Rabin-Miller Test for Composite Numbers) 设 n 是奇数, 记 $n-1=2^k q$, q 是奇数. 对不被 n 整除的某个 a, 如果下述两个条件都成立, 则 n 是合数:

(i) $a^q \neq 1 \pmod{n}$,

(ii) 对所有 $i=0,1,2,\cdots,k-1$, $a^{2^i q} \neq -1 \pmod{n}$.

对任意选取的 a, 拉宾-米勒测试结论性地证明 n 是合数, 或表明 n 可能是素数. n 的合数性的拉宾-米勒证据是拉宾-米勒测试能成功证明 n 是合数的数 a. 拉宾-米勒测试如此有用的理由归于下述事实: 如果 n 是奇合数, 则 1 与 $n-1$ 之间至少有 75% 的数可作为 n 的拉宾-米勒证据[1]. 换句话说, 每个合数有许多拉宾-米勒证据来说明它的合数性, 所以, 不存在拉宾-米勒测试的任何 "卡米歇尔型数".

[1] K CONRAD. 2011. The Miller-Rabin Test. Encyclopedia of Cryptography and Security. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf.

Chapter 3

高次同余方程的进一步研究

3.1 平方剩余

考虑同余方程 $x^2 \equiv a \pmod{m}$, 我们已经知道 m 是素数 p 时方程要么无解要么恰有两个解, 现在我们考虑它什么时候有解的问题. 一般地, 我们把使 $x^2 \equiv a \pmod{m}$ 有解的 a 称为是模 m 平方剩余.

定义 3.1.1 (平方剩余) 设整数 a 与 m 互素, 若 $x^2 \equiv a \pmod{m}$ 有解, 则称 a 是模 m 的**平方 (二次) 剩余** (quadratic residue, QR), 否则称为**平方 (二次) 非剩余** (quadratic non-residue, NR).

3.1.1 模 p 平方剩余

我们先考虑模素数 p 的平方剩余.

定理 3.1.2 设 p 为一个奇素数, 则模 p 的最小非负完全剩余系中恰有 $\dfrac{p-1}{2}$ 个模 p 的平方剩余, 且恰有 $\dfrac{p-1}{2}$ 个模 p 的平方非剩余. 且 $\dfrac{p-1}{2}$ 个平方剩余分别与序列

$$1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$$

中之一数且仅与一数同余.

证 易知模 p 平方剩余是下面这些数:

$$1^2; 2^2, \cdots, (p-1)^2 \pmod{p}.$$

而由于 $x^2 \equiv a \pmod{m}$ 若有解则有且仅有两个解, 故上面这个序列实际上只有 $\dfrac{p-1}{2}$ 个数 $\pmod{p}$. 现在只需验证 $1^2, 2^2, \cdots, \left(\dfrac{p-1}{2}\right)^2$ 模 p 是两两不同的.

假设 b_1 与 b_2 都是 1 到 $\dfrac{p-1}{2}$ 之间的数, 且满足 $b_1^2 \equiv b_2^2 \pmod{p}$, 这即是说

$$p \mid b_1^2 - b_2^2 = (b_1 - b_2)(b_1 + b_2).$$

然而, $b_1 + b_2$ 是 2 到 $p-1$ 之间的数, 因此不可能被 p 整除. 故 p 必整除 $b_1 - b_2$, 但是 $|b_1 - b_2| < (p-1)/2$, 所以 $b_1 - b_2$ 一定等于 0, 即 $b_1 = b_2$. 这就证明了 $1^2, 2^2, \cdots, \left(\dfrac{p-1}{2}\right)^2$ 模 p 是两两不同的. □

定理 3.1.3 (平方剩余乘法法则) 设 p 为奇素数, 则

(i) 两个模 p 的平方剩余的积是平方剩余;

(ii) 平方剩余与平方非剩余的积是平方非剩余;

(iii) 两个平方非剩余的积是平方剩余,

这三条法则可用符号表示如下:

$$\mathrm{QR} \times \mathrm{QR} = \mathrm{QR},\ \mathrm{QR} \times \mathrm{NR} = \mathrm{NR},\ \mathrm{NR} \times \mathrm{NR} = \mathrm{QR}.$$

证 (i) 假定 a_1, a_2 都是模 p 的 QR, 即存在数 b_1 和 b_2, 使得 $a_1 \equiv b_1^2 \pmod{p}$, $a_2 \equiv b_2^2 \pmod{p}$. 将这两个同余式相乘, 得到 $a_1 a_2 \equiv (b_1 b_2)^2 \pmod{p}$, 此即表明 $a_1 a_2$ 是一个 QR.

(ii) 设 a_1 是一个 QR, $a_1 \equiv b_1^2 \pmod{p}$, 且设 a_2 是一个 NR. 如果 $a_1 a_2$ 是一个 QR, 则存在某个整数 b_3 使得 $a_1 a_2 \equiv b_3^2 \pmod{p}$, 所以有

$$b_3^2 \equiv a_1 a_2 \equiv b_1^2 a_2 \pmod{p}.$$

因为 p 不整除 a_1 且 $a_1 = b_1^2$, 所以 $(b_1, p) = 1$, 因此 $b_1 \pmod{p}$ 可逆. 即存在 c_1 使得 $c_1 b_1 \equiv 1 \pmod{p}$, 两边同乘 c_1^2 得

$$c_1^2 b_3^2 \equiv c_1^2 a_1 a_2 \equiv (c_1 b_1)^2 a_2 \equiv a_2 \pmod{p}.$$

于是 $a_2 \equiv (c_1 b_3)^2 \pmod{p}$ 是一个 QR, 与 a_2 是 NR 矛盾.

(iii) 设 a 是一个 NR, 根据定理 2.3.4

$$\{a, 2a, \cdots, (p-1)a\} \equiv \{1, 2, \cdots, p-1\} \pmod{p}.$$

特别地, 这些数中包括 $\dfrac{p-1}{2}$ 个 QR 和 $\dfrac{p-1}{2}$ 个 NR. 由 (ii), 每次将 a 乘一个 QR 便得到一个 NR, 故 $\dfrac{p-1}{2}$ 个积

$$a \times \mathrm{QR}$$

已经给出了 $\dfrac{p-1}{2}$ 个 NR, 这已经 "用完了" 所有得 NR. 因此 a 乘 NR 只能等于一个 QR. □

3.1.2 勒让德符号

勒让德 (Legendre) 观察到 QR 与 NR 的乘法性质同 $+1$ 与 -1 的性质类似, 于是他引人了下面非常有用的符号.

定义 3.1.4 设 p 为奇素数, **勒让德符号**定义如下:

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若 } a \text{ 平方剩余} \pmod p,\\ -1, & \text{若 } a \text{ 是平方非剩余} \pmod p,\\ 0, & \text{若 } a\equiv 0 \pmod p.\end{cases}$$

由定义易得, 若 $a\equiv a_1 \pmod p$, 则

$$\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right).$$

这说明要计算 $\left(\frac{a}{p}\right)$ 的值可以用 $a \bmod p=a_1$, $0\leqslant a_1<p$ 去代替 a 以简化计算.

利用勒让德符号, 平方剩余的乘法法则可用一个公式表出.

定理 3.1.5 (平方剩余乘法法则) 设 p 为奇素数, 则

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right).$$

由此我们可以得到

$$\left(\frac{a_1a_2\cdots a_n}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right).$$

特别地,

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right),\ p\nmid b.$$

这说明如果 a 是合数那么计算 $\left(\frac{a}{p}\right)$ 时可把 a 对 p 的勒让德符号表成 a 的因数对 p 的勒让德符号的乘积; 且在计算过程中可以去掉符号上方不被 p 整除 (模 p 不为 0) 的任何平方因数.

3.1.3 欧拉准则

虽然我们已经研究了一些平方剩余的性质, 我们到现在为止还没有有关平方剩余的具体计算方式. 下面的欧拉准则提供了判断平方剩余的充要条件.

定理 3.1.6 (欧拉准则) 设 p 为奇素数, 则

$$\left(\frac{a}{p}\right)\equiv a^{(p-1)/2} \pmod p.$$

证 首先假设 $\left(\frac{a}{p}\right)=1$ (即 a 是一个平方剩余), 设 $a\equiv b^2 \pmod p$. 则由费马小定理可知

$$a^{(p-1)/2}\equiv \left(b^2\right)^{(p-1)/2}=b^{p-1}\equiv 1=\left(\frac{a}{p}\right) \pmod p.$$

下面考虑同余方程

$$x^{(p-1)/2}-1\equiv 0 \pmod p.$$

上一段的证明即是说每个平方剩余都是这个同余方程的解, 并且由于恰有 $\frac{p-1}{2}$ 个平方剩余, 且这个多项式同余方程至多有 $\frac{p-1}{2}$ 个不同的解, 因此

$$\left\{x^{(p-1)/2}-1\equiv 0 \pmod p \text{ 的解}\right\}=\{\text{模 } p \text{ 的平方剩余}\}.$$

再设 $\left(\frac{a}{p}\right)=-1$ (即 a 是一个平方非剩余). 由费马小定理可知 $a^{p-1}\equiv 1 \pmod p$, 所以

$$0\equiv a^{p-1}-1\equiv \left(a^{(p-1)/2}-1\right)\left(a^{(p-1)/2}+1\right) \pmod p.$$

第一个因子 $\left(a^{(p-1)/2}-1\right)$ 模 p 不等于零, 因为我们已经证明 $x^{(p-1)/2}-1\equiv 0 \pmod p$ 的解都是平方剩余. 因此, 第二个因子 $\left(a^{(p-1)/2}+1\right)$ 必模 p 为零. 从而

$$a^{(p-1)/2}\equiv -1=\left(\frac{a}{p}\right) \pmod p.$$

最后 $\left(\frac{a}{p}\right)=0$ 时, $a=0$,

$$a^{(p-1)/2}\equiv 0=\left(\frac{a}{p}\right) \pmod p. \qquad \square$$

3.2 二次互反律

3.2.1 $\left(\frac{-1}{p}\right)$ 与 $\left(\frac{2}{p}\right)$

在前一节中, 对各种素数 p, 我们讨论了模 p 的平方剩余和平方非剩余. 现在我们给定 a, 看看对哪些素数 p, a 是 QR.

首先考虑 $a=-1$. 利用欧拉准则很容易确定哪些素数以 -1 为平方剩余.

定理 3.2.1 (二次互反律——第 I 部分) 设 p 为奇素数, 则

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & \text{当 } p\equiv 1 \pmod 4 \text{ 时;}\\ -1, & \text{当 } p\equiv 3 \pmod 4 \text{ 时.}\end{cases}$$

即 $p\equiv 1 \pmod 4$ 时 -1 是模 p 的平方剩余, $p\equiv 3 \pmod 4$ 时 -1 是模 p 的平方非剩余.

证 根据欧拉准则, $\left(\dfrac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$. 所以 $\left(\dfrac{-1}{p}\right) = 1 \iff \dfrac{p-1}{2}$ 为偶数 $\iff \dfrac{p-1}{2} = 2k \iff p = 4k+1 \iff p \equiv 1 \pmod{4}$; $\left(\dfrac{-1}{p}\right) = -1 \iff \dfrac{p-1}{2}$ 为奇数 $\iff \dfrac{p-1}{2} = 2k+1 \iff p = 4k+3 \iff p \equiv 3 \pmod{4}$. □

我们可以利用这一定理来回答曾经遗留的问题. 我们曾证明存在无穷多个模 4 余 3 和模 6 余 5 的素数, 现在我们可以证明存在无穷多个模 4 余 1 的素数.

定理 3.2.2 存在无穷多个模 4 余 1 的素数.

证 如果只有有限个模 4 余 1 的素数 $p_1, p_2, \cdots, p_r$.

考虑数

$$A = (2p_1p_2\cdots p_r)^2 + 1.$$

将 A 素因数分解

$$A = q_1q_2\cdots q_s.$$

显然, $q_1, q_2, \cdots, q_s$ 不在我们原来的素数中, 因为每个 p_i 都不整除 A. 因此, 只需证明至少有一个 q_i 是模 4 余 1 的, 事实上每个 q_i 都是模 4 余 1 的.

首先注意到 A 是奇数, 所以每个 q_i 都是奇数. 其次, 每个 q_i 整除 A, 因此

$$(2p_1p_2\cdots p_r)^2 + 1 = A \equiv 0 \pmod{q_i}.$$

这意味着 $x = 2p_1p_2\cdots p_r$ 是同余方程

$$x^2 \equiv -1 \pmod{q_i}$$

的解, 因此 -1 是模 q_i 的平方剩余. 由二次互反律知 $q_i \equiv 1 \pmod{4}$. □

现在考虑 $a = 2$ 的情形, 我们希望寻找使得 2 为模 p 的平方剩余的那些素数 p 的简单特征. 这件事很难类似上面用欧拉准则完成, 因为似乎并没有简单的方法去计算 $2^{(p-1)/2} \pmod{p}$.

定理 3.2.3 (高斯 (Gauss) 引理) 设奇素数 $p \nmid a$, ν 是 $\{a, 2a, \cdots, a(p-1)/2\}$ 的模 p 绝对最小剩余 (即模 p 到 $\left[-\dfrac{p-1}{2}, \dfrac{p-1}{2}\right]$ 中) 中的负数个数, 则

$$\left(\frac{a}{p}\right) = (-1)^{\nu}.$$

证 记

$$\{a, 2a, \cdots, a(p-1)/2\} \equiv \left\{s_1(-1)^{\alpha_1}, s_2(-1)^{\alpha_2}, \cdots, s_{(p-1)/2}(-1)^{\alpha_{(p-1)/2}}\right\} \pmod{p}, \quad (3.1)$$

其中 $0 < s_k \leqslant (p-1)/2$, ak 的模 p 绝对最小剩余为 $\pm s_k$. 我们断言 $s_k \neq s_j$ $(1 \leqslant k \neq j \leqslant (p-1)/2)$. 事实上, 若 $s_k = s_j$, 即 $ak \equiv \pm aj \pmod{p}$, 则 $k \mp j \equiv 0 \pmod{p}$, 即 $k \equiv j \pmod{p}$

或 $k+j\equiv 0 \pmod p$, 又由于 $1\leqslant k,j\leqslant (p-1)/2$ 且 $k\neq j$, 则前者意味着 $k=j$, 而后者是不可能的. 这说明

$$\left\{s_1,s_2,\cdots,s_{(p-1)/2}\right\}=\{1,2,\cdots,(p-1)/2\}.$$

对 (3.1) 式, 两边求其元素乘积得

$$a^{(p-1)/2}\cdot[(p-1)/2]!\equiv(-1)^{\nu}s_1\cdots s_{(p-1)/2}=(-1)^{\nu}[(p-1)/2]! \pmod p,$$

$$(-1)^{\nu}\equiv a^{(p-1)/2}\equiv\left(\frac{a}{p}\right) \pmod p. \qquad \square$$

例如, $p=11$ 时, $(p-1)/2=5$. 对 $a=2$, 求 $\{2,2\cdot 2,3\cdot 2,4\cdot 2,5\cdot 2\}$ 的最小绝对剩余为 $\{2,4,-5,-3,-1\}$, 故 $\nu=3$, $\left(\dfrac{2}{11}\right)=-1$. 而对 $a=3$, $\{3,2\cdot 3,3\cdot 3,4\cdot 3,5\cdot 3\}$ 的最小绝对剩余得 $\{3,-5,-2,1,4\}$, 故 $\nu=2$, $\left(\dfrac{3}{11}\right)=1$, 事实上, $5^2\equiv 3 \pmod{11}$.

定理 3.2.4 (二次互反律——第 II 部分) 设 p 为奇素数, 则

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}=\begin{cases}1, & \text{若 } p\equiv\pm 1 \pmod 8,\\ -1, & \text{若 } p\equiv\pm 3 \pmod 8.\end{cases}$$

即当 p 模 8 余 1 或 7 时, 2 是模 p 的平方剩余; 当 p 模 8 余 3 或 5 时, 2 是模 p 的平方非剩余.

证 用高斯引理, $\left(\dfrac{2}{p}\right)=(-1)^{\nu}$, 现 ν 恰为 $\left\{2\cdot 1,2\cdot 2,\cdots,2\cdot\dfrac{p-1}{2}\right\}$ 中大于 $\dfrac{p-1}{2}$ 的个数. 而对 $k=1,2,\cdots,\dfrac{p-1}{2}$,

$$\frac{p-1}{2}<2\cdot k\leqslant 2\cdot\frac{p-1}{2}\Longleftrightarrow\frac{p-1}{4}<k\leqslant\frac{p-1}{2}\Longleftrightarrow\rho<k\leqslant\frac{p-1}{2},$$

其中 ρ 为 $\dfrac{p-1}{4}$ 的整数部分. 故 $\nu=\dfrac{p-1}{2}-\rho$. 当 $p=8k+1,8k+3,8k+5,8k+7$ 时, 依次有

$$\frac{p-1}{2}=4k,4k+1,4k+2,4k+3,$$

而这时对应的 $\rho=2k,2k,2k+1,2k+1$, 故

$$\nu=\frac{p-1}{2}-\rho=2k,2k+1,2k+1,2k+2.$$

由高斯引理知依次有 $\left(\dfrac{2}{p}\right)=(-1)^{\nu}=1,-1,-1,1.$ $\square$

用这一定理可以证明存在无穷多个模 8 余 7 和模 8 余 1 的素数.

定理 3.2.5 存在无穷多个模 8 余 7 的素数.

证 如果只存在有限个模 8 余 7 (即 -1) 的素数 $p_1,\cdots,p_r$. 考虑数

$$A=(p_1\cdots p_r)^2-2.$$

则 $p=(p_1p_2\cdots p_r)^2-2\equiv(-1)^{2r}-2\equiv 1^r-2\equiv -1 \pmod 8$. 进而 A 是奇数, 将 A 素因数分解

$$A=q_1q_2\cdots q_s.$$

则所有 q_i 都是奇素数, 且有 $(p_1p_2\cdots p_r)^2\equiv 2 \pmod{q_i}$, 即 -1 是模 q 的平方剩余, 则 $q_i\equiv\pm 1 \pmod 8$. 若所有 q_i 都模 8 余 1, 则 $A=q_1q_2\cdots q_s$ 模 8 余 1, 但 A 模 8 余 -1, 矛盾. 则必存在 q_j 模 8 余 -1 (即 7). 而显然 q_j 不在最初的 $p_1,p_2,\cdots,p_r$ 中. □

定理 3.2.6 存在无穷多个模 4 余 1 的素数.

证 如果只存在有限个模 8 余 1 的素数 $p_1,p_2,\cdots,p_r$.

考虑数

$$A=(2p_1p_2\cdots p_r)^4+1,$$

将 A 素因数分解

$$A=q_1q_2\cdots q_s.$$

注意到 A 是奇数, 故 q_i 都是奇素数.

记 $X=2p_1p_2\cdots p_r$. 由于 $q_i\mid X^4+1$, 则 -1 是 q_i 的平方剩余, 即 $q_i\equiv 1 \pmod 4$. 另一方面 $X^4+1\equiv 0 \pmod{q_i}\iff X^4+2X^2+1\equiv 2X^2 \pmod p$. 即 $2X^2$ 是模 q_i 的平方剩余, 进而 2 是模 q_i 的平方剩余, 故 $q_i\equiv\pm 1 \pmod 8$. 综上可得 $q_i\equiv 1 \pmod 8$.

而显然 q_i 不在最初的 $p_1,p_2,\cdots p_r$ 中. □

3.2.2 二次互反律及其应用

上一节我们讨论了 $\left(\dfrac{-1}{p}\right)$ 与 $\left(\dfrac{2}{p}\right)$, 现在我们要解决的是一般的 a 值的勒让德符号 $\left(\dfrac{a}{p}\right)$ 的计算问题.

一般地, 如果想对任意的 a 计算 $\left(\dfrac{a}{p}\right)$, 可以先将 a 素因数分解

$$a=q_1q_2\cdots q_r$$

(某些 q_i 可以相同). 由平方剩余乘法法则可得

$$\left(\frac{a}{p}\right)=\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_r}{p}\right).$$

这就意味着: 如果知道如何对素数 q 计算 $\left(\dfrac{q}{p}\right)$, 就能对任意的 a 计算 $\left(\dfrac{a}{p}\right)$.

定理 3.2.7 (二次互反律, law of quadratic reciprocity) 设 p,q 为奇素数, 则

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)(-1)^{(p-1)/2\cdot(q-1)/2} \text{ (即 } p,q \text{ 之一模 4 余 1 时, 取正号)},$$

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2} \text{ (即 } p \text{ 模 4 余 1 时, 取正号)},$$

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8} \text{ (即 } p \text{ 模 8 余 } \pm 1 \text{ 时, 取正号)}.$$

我们已经证明了二次互反律对于 $\left(\frac{-1}{p}\right)$ 和 $\left(\frac{2}{p}\right)$ 的情形, 完整证明在下一节给出.

二次互反律是计算 $\left(\frac{a}{p}\right)$ 的有用的工具. 例如

$$\begin{aligned}
\left(\frac{14}{137}\right) &= \left(\frac{2}{137}\right)\left(\frac{7}{137}\right) && \text{平方剩余乘法法则,}\\
&= \left(\frac{7}{137}\right) && 137 \equiv 1 \pmod 8 \Longrightarrow \left(\frac{2}{137}\right) = 1,\\
&= \left(\frac{137}{7}\right) && \text{用二次互反律, } 137 \equiv 1 \pmod 4,\\
&= \left(\frac{4}{7}\right) && 137 \bmod 7 = 4\\
&= 1 && 4 = 2^2 \text{ 是平方数.}
\end{aligned}$$

因此, 14 是模 137 的平方剩余. 事实上, $39^2 \equiv 14 \pmod{137}$ 及 $98^2 \equiv 14 \pmod{137}$. 在计算过程中, 勒让德符号可能会多次 "翻转", 如

$$\begin{aligned}
\left(\frac{55}{179}\right) &= \left(\frac{5}{179}\right)\left(\frac{11}{179}\right)\\
&= \left(\frac{179}{5}\right) \times (-1) \times \left(\frac{179}{11}\right) && \text{因为 } 5 \equiv 1 \pmod 4 \text{ 且 } 11 \equiv 179 \equiv 3 \pmod 4,\\
&= \left(\frac{4}{5}\right) \times (-1) \times \left(\frac{3}{11}\right) && \text{因为 } 179 \bmod 5 = 4 \text{ 且 } 179 \bmod 11 = 3,\\
&= 1 \times (-1) \times \left(\frac{3}{11}\right) && \text{因为 } 4 = 2^2 \text{ 是平方数,}\\
&= 1 \times (-1) \times (-1) \times \left(\frac{11}{3}\right) && \text{因为 } 3 \equiv 11 \equiv 3 \pmod 4,\\
&= 1 \times (-1) \times (-1) \times \left(\frac{2}{3}\right) && \text{因为 } 11 \bmod 3 = 2,\\
&= 1 \times (-1) \times (-1) \times (-1) && \text{因为 } 3 \equiv 3 \pmod 8 \text{ 故 } \left(\frac{2}{3}\right) = -1,\\
&= -1.
\end{aligned}$$

因此, 55 是模 179 的平方非剩余.

计算 $\left(\frac{a}{p}\right)$ 的最困难之处不是二次互反律的使用, 而是在使用二次互反律之前, 必须对 a 因式分解. 对非常大的 a, 这可能是难以完成的. 因此我们希望对一般的奇数 a, 能直接 "翻转" $\left(\frac{a}{p}\right)$ 而不必考虑 a 是否是素数. 事实上这是可行的.

定义 3.2.8 (雅可比 (Jacobi) 符号) 设 $b = p_1 p_2 \cdots p_t$ 为正奇数, p_i $(i = 1, \cdots, t)$ 为奇素数 (不必互异), 对任意整数 a, **雅可比符号**定义为

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1 p_2 \cdots p_t}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_t}\right).$$

注 需要注意的是, $\left(\frac{a}{b}\right)=1$ 并不意味着 a 为模 b 的平方剩余, 例如

$$\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=1,$$

但 2 并非模 15 的平方剩余. 但若 a 为模 b 的平方剩余, 则必定

$$\left(\frac{a}{b}\right)=\left(\frac{x^2}{b}\right)=\left(\frac{x}{b}\right)^2=1.$$

雅可比符号保有了勒让德符号的许多性质, 有多种用途, 特别便于计算. 根据定义容易得到

定理 3.2.9 雅可比符号有如下性质:
(i) $\left(\frac{a_1a_2}{b}\right)=\left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$;
(ii) $\left(\frac{a}{b_1b_2}\right)=\left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$;
(iii) 若 $a_1\equiv a_2 \pmod b$, 则 $\left(\frac{a_1}{b}\right)=\left(\frac{a_2}{b}\right)$.

更重要的是, 对雅可比符号也有类似二次互反律的结论成立.

定理 3.2.10 (广义二次互反律) 设 a,b 为正奇数, 则

$$\left(\frac{a}{b}\right)=\left(\frac{b}{a}\right)(-1)^{(a-1)/2\cdot(b-1)/2} \text{ (即 } a,b \text{ 之一模 4 余 1 时取正号)},$$
$$\left(\frac{-1}{b}\right)=(-1)^{(b-1)/2} \text{ (即 } b \text{ 模 4 余 1 时取正号)},$$
$$\left(\frac{2}{b}\right)=(-1)^{(b^2-1)/2} \text{ (即 } b \text{ 模 8 余 } \pm1 \text{ 时取正号)}.$$

证 二次互反律说明, 定理对 a,b 为奇素数情形成立. 雅可比符号的性质说明, 雅可比符号 $\left(\frac{a}{b}\right)$ 对奇数 a,b 都是完全积性函数 ($f(x)$ 是完全积性函数是指: $f(xy)=f(x)f(y)$ 对任意 x,y 成立; $f(x)$ 是积性是指: $f(xy)=f(x)f(y)$ 对互素整数 x,y 成立). 下述引理说明, $(-1)^{(b-1)/2}$ 与 $(-1)^{(b^2-1)/8}$ 对奇数 b 是完全积性函数. 故定理中涉及的函数都是积性的, 故对一般奇数 a,b 成立. □

引理 3.2.11 设 $s_1,\cdots,s_r$ 为奇数, 则
(1) $\frac{s_1\cdots s_r-1}{2}\equiv\frac{s_1-1}{2}+\cdots+\frac{s_r-1}{2} \pmod 2$;
(2) $\frac{s_1^2\cdots s_r^2-1}{8}\equiv\frac{s_1^2-1}{8}+\cdots+\frac{s_r^2-1}{8} \pmod 2$.

证 (1) 注意到 $\frac{s-1}{2}\equiv 0,1 \pmod 2$ 分别当 $s\equiv 1,-1 \pmod 4$. 设 $s_1,\cdots,s_r \pmod 4$ 中同余于 -1 的有 t 个 (其余同余于 1). 则

$$\text{左边}\equiv t\equiv\text{右边} \pmod 2.$$

(2) 注意到当 $s \equiv \pm 1$ 或 $\pm 3 \pmod 8$ 时, 分别有 $s^2 \equiv 1$ 或 $9 \pmod{16}$. 设 $s_1, \cdots, s_r \pmod 8$ 中同余于 ± 3 的有 t 个 (其余同余于 ± 1). 则

$$\text{左边} \equiv t \equiv \text{右边} \pmod 2. \qquad \square$$

注 需要注意的是, 我们只允许对正奇数 a 翻转 $\left(\frac{a}{b}\right)$. 如果 a 是偶数, 则必须先分解出 $\left(\frac{2}{b}\right)$ 的幂; 如果 a 是负的, 则必须分解出 $\left(\frac{-1}{b}\right)$.

现在再看二次同余方程

$$x^2 \equiv a \pmod p$$

(p 为奇素数), 我们可以利用二次互反律等方法判断其是否有解. 即 $\left(\frac{a}{p}\right) = 1$ 时有解. 事实上, 当 p 模 4 余 3 和模 8 余 5 时, 我们还可以得到解的具体形式.

定理 3.2.12 设 p 为奇素数, $\left(\frac{a}{p}\right) = 1$, 即 $a^{(p-1)/2} \equiv 1 \pmod p$. 则

(i) 若 $p \equiv 3 \pmod 4$, 则 $x = a^{(p+1)/4}$ 是 $x^2 \equiv a \pmod p$ 的一个解;

(ii) 若 $p \equiv 5 \pmod 8$, 则 $x = a^{(p+3)/8}$ 或 $x = 2a \cdot (4a)^{(p-5)/8}$ 中之一是 $x^2 \equiv a \pmod p$ 的一个解.

证 (i) 若 $p \equiv 3 \pmod 4$. 由 $a^{(p-1)/2} \equiv 1 \pmod p$, 故

$$a^{(p+1)/2} \equiv a \pmod p,$$
$$\left(a^{(p+1)/4}\right)^2 \equiv a \pmod p.$$

故 $x \equiv a^{(p+1)/4}$ 为同余方程 $x^2 \equiv a \pmod p$ 的解.

(ii) 若 $p \equiv 5 \pmod 8$. 由 $a^{(p-1)/2} \equiv 1 \pmod p$, 可得

$$a^{(p-1)/4} \equiv \pm 1 \pmod p,$$
$$\left(a^{(p+3)/8}\right)^2 \equiv a^{(p+3)/4} \equiv \pm a \pmod p$$

(用到 $p \equiv 5 \pmod 8$). 如果值为正的, 则 $x = a^{(p+3)/8}$ 是 $x^2 \equiv a \pmod p$ 的解.

如果值是负的, 则

$$\left(2a \cdot (4a)^{(p-5)/8}\right)^2 = 4a^2 \cdot (4a)^{(p-5)/4} = a \cdot 2^{(p-1)/2} \cdot a^{(p-1)/4}.$$

由假设 $a^{(p-1)/4} \equiv -1 \pmod p$. 另一方面, 因为 $p \equiv 5 \pmod 8$, 由二次互反律知 2 是模 p 的平方非剩余, 所以由欧拉准则 $2^{(p-1)/2} \equiv -1 \pmod p$. 所以

$$\left(2a \cdot (4a)^{(p-5)/8}\right)^2 \equiv a \cdot (-1) \cdot (-1) \equiv a \pmod p,$$

所以 $x = 2a \cdot (4a)^{(p-5)/8}$ 是 $x^2 \equiv a \pmod p$ 的解. $\square$

3.2.3 二次互反律的证明

To do.

3.3 原根与指标

3.3.1 模 p 原根

定义 3.3.1 (次数) 设 a 与素数 p 互素, a 模 p 的**次数** (或**阶**) 指

$$e_p(a) = \left(\text{使得 } a^e \equiv 1 \pmod p \text{ 的最小指数 } e \geqslant 1\right).$$

由定义, $e_p(a)$ 就是 $\overline{a}$ 作为群 $U(p)$ 的元素的阶, 因而 $e_p(a)$ 整除 $U(p)$ 的阶 $p-1$.

定理 3.3.2 设 a 是不被素数 p 整除的整数, 假设 $a^n \equiv 1 \pmod p$, 则次数 $e_p(a)$ 整除 n. 特别地, 次数 $e_p(a)$ 总整除 $p-1$.

定义 3.3.3 具有最高次数 $e_p(g) = p-1$ 的数 g 称为模 p 的**原根**. 也就是这时 $U(p)$ 为循环群, $\overline{g}$ 为其生成元.

定理 3.3.4 (原根定理) 每个素数 p 都有原根. 更精确地, 有恰好 $\varphi(p-1)$ 个模 p 的原根.

3.3.2 指标

定义 3.3.5 因为 $U(p) = \langle\overline{g}\rangle$, 所以对任何 $1 \leqslant a < p$, 我们可选择幂

$$g,\ g^2,\ g^3,\ g^4,\ \cdots,\ g^{p-3},\ g^{p-2},\ g^{p-1}$$

中恰好一个与 a 模 p 同余. 相应的指数被称为以 g 为底的 a 模 p 的**指标**. 假设 p 与 g 已给定, 则记指标为 $I(a)$.

由定义容易看出指标满足如下的法则.

定理 3.3.6 (指标的性质) 指标满足下述性质:
(i) $I(ab) \equiv I(a) + I(b) \pmod{p-1}$; (乘积法则)
(ii) $I\left(a^k\right) \equiv kI(a) \pmod{p-1}$. (幂法则)

这里需要注意模是 $p-1$ 而不是 p.

指标可以用来简化计算和解同余方程. 这里以 2 为底模 37 的指标为例, 先给出以 2 为底模 37 的指标表.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$I(a)$	36	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7	17
a	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$I(a)$	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8	19	18

例 3.3.7 例如要计算 $23 \cdot 19 \pmod{37}$, 可以先计算

$$I(23 \cdot 19) \equiv I(23) + I(19) \equiv 15 + 35 \equiv 50 \equiv 14 \pmod{36}.$$

观察表求得 $I(30) = 14$, 从而得到 $23 \cdot 19 \equiv 30 \pmod{37}$.

再例如,

$$I\left(29^{14}\right) \equiv 14 \cdot I(29) \equiv 14 \cdot 21 \equiv 294 \equiv 6 \pmod{36}.$$

由表得 $I(27) = 6$, 从而 $29^{14} = 27 \pmod{37}$.

指标不但对直接计算有用, 而且是解同余方程的有效工具.

例 3.3.8 考虑同余方程

$$19x \equiv 23 \pmod{37}.$$

如果 x 是解, 则 $I(19x) = I(23)$ 的指标. 使用乘积法则再借助指标表, 我们可计算

$$\begin{aligned} I(19x) &= I(23) \\ I(19) + I(x) &\equiv I(23) \pmod{36} \\ 35 + I(x) &\equiv 15 \pmod{36} \\ I(x) &\equiv -20 \equiv 16 \pmod{36}. \end{aligned}$$

因此, 解的指标是 $I(x) = 16$, 再查表可求得 $x \equiv 9 \pmod{37}$.

例 3.3.9 考虑同余方程

$$3x^{30} \equiv 4 \pmod{37}$$

的所有解.

由取两边的指标开始, 使用乘积法则与幂法则.

$$\begin{aligned} I\left(3x^{30}\right) &= I(4) \\ I(3) + 30I(x) &\equiv I(4) \pmod{36} \\ 26 + 30I(x) &\equiv 2 \pmod{36} \\ 30I(x) &\equiv -24 \equiv 12 \pmod{36}. \end{aligned}$$

这就将原方程转化为了 $30I(x) \equiv 12 \pmod{36}$. 由于 $(30, 36) = 6$ 整除 12, 所以有 6 个解. 求得

$$30I(x) \equiv 12 \pmod{36}$$

的解为

$$I(x) \equiv 4, 10, 16, 22, 28, 34 \pmod{36}.$$

最后, 由指标表得到 x 的对应值

$$\begin{aligned} I(16)=4, \quad I(25)=10, \quad I(9)=16, \\ I(21)=22, \quad I(12)=28, \quad I(28)=34. \end{aligned}$$

因此, 同余方程 $3x^{30} \equiv 4 \pmod{37}$ 有 6 个解, 为

$$x \equiv 16, 25, 9, 21, 12, 28 \pmod{37}.$$

Chapter 4

高次不定方程

4.1 勾股数

4.1.1 勾股数组

不定方程

$$X^2 + Y^2 = Z^2$$

称为勾股数方程, 其正整数解 $(X, Y, Z) = (a, b, c)$ 称为**勾股数组** (Pythagorean triple). 由勾股定理可知, 每个勾股数组构成一个整 (数) 边 (长) 直角三角形的三条边.

若解 a, b, c 使 $abc = 0$, 则称为平凡解. 只需讨论非平凡解. 显然可设解均为正整数. (a, b, c) 为解当且仅当 (ka, kb, kc) 为解 (k 为整数), 它们称为成比例的解. 在一组成比例的解中, 有唯一的正整数解 (a, b, c) 使得最大公因子 $(a, b, c) = 1$. 这样的解称为本原 (primitive) 解, 或**本原勾股数组**. 因此, 只需求本原解即可得到全部解.

若 (a, b, c) 为本原勾股数组, 则

$$a^2 + b^2 \equiv c^2.$$

考虑模 4 同余, 因任意 $k^2 \equiv 0$ 或 $1 \pmod 4$, 故只有两种可能: $1 + 0 \equiv 1$, 或 $0 + 1 \equiv 1 \pmod 4$. 即 a, b 必是一奇一偶. 故可设 a 为奇数, b 为偶数, c 为奇数 (必要时将 a, b 名称互换), 而且 a, b, c 必是两两互素的, 因为, 假若素数 $(a, b) > 1$, 则有素因数 p, 则由 $a^2 + b^2 = c^2$ 知 $p \,|\, c^2, p \,|\, c$, 从而 $p \mid (a, b, c)$, 矛盾.

定理 4.1.1 (勾股数组定理) 每个本原勾股数组 (a, b, c) (其中 a 为奇数, b 为偶数) 都可从如下公式得出:

$$a = st,\ b = \frac{s^2 - t^2}{2},\ c = \frac{s^2 + t^2}{2},$$

其中 $s > t \geqslant 1$ 是任意互素的奇数. 反之, 对任意正整数 $s > t$, 上述 (a, b, c) 是勾股数组; 且 (a, b, c) 为本原勾股数组当且仅当 $s > t$ 为互素正奇数.

4.1.2 将整数表示成两数平方和

高斯整数

考虑一类特殊的复数, 称为高斯 (Gauss) 整数:

$$m+n\mathrm{i}\ (\text{其中 } m,n\in\mathbb{Z} \text{ 是整数}),$$

其全体记为 $\mathbb{Z}[\mathrm{i}]$, 是一个唯一分解整环. 定义高斯整数 $\alpha=m+n\mathrm{i}$ 的**范数**

$$N(\alpha)=m^2+n^2.$$

范数是积性函数, 即对任意高斯整数 α_1,α_2 有

$$N\left(\alpha_1\alpha_2\right)=N\left(\alpha_1\right)N\left(\alpha_2\right).$$

引理 4.1.2 如果两个数都能表成两平方数之和, 则它们的乘积也能表成两平方数之和.

证 因 "二平方和" 等价于 "高斯整数的范数". 故上述命题化为: 高斯整数之积仍为高斯整数. 这是显然的. 事实上, 记 $\alpha=a+b\mathrm{i}$, $\beta=c+d\mathrm{i}$ 为高斯整数, 则

$$\alpha\beta=(ac-bd)+(ad+bc)\mathrm{i}$$

仍为高斯整数. 取范数得

$$N(\alpha)\cdot N(\beta)=N(\alpha\beta),$$
$$\left(a^2+b^2\right)\left(c^2+d^2\right)=(ac-bd)^2+(ad+bc)^2.$$

将素数表示成两数平方和

先看素数 p 能否表为两数平方和. $p=2$ 显然可以, 对奇素数 p, 若

$$p=a^2+b^2,$$

则 a,b 一奇一偶, 故 $p=a^2+b^2\equiv 1\pmod 4$. 也就是说, 只有模 4 余 1 的素数 p 才可能表为两数平方和. 事实上反之也成立.

定理 4.1.3 设 p 是素数, 则 p 是两个平方数之和的充要条件是

$$p\equiv 1\pmod 4\ (\text{或 } p=2).$$

证 假设 $p\equiv 1\pmod 4$, 我们要将 p 表成两平方数之和, 我们使用费马著名的递降法.

我们先将 p 的某个倍数表成两个平方数之和. 例如, 由二次互反律知 $x^2\equiv -1\pmod p$ 有一解, 设为 $x=A$, 则 A^2+1^2 是 p 的倍数. 因此, 我们从

$$A^2+B^2=Mp$$

开始, 其中 A, B, M 为整数. 如果 $M = 1$, 则证明已完成. 因此, 我们假设 $M \geqslant 2$.

我们希望用 A, B, M 发现新的整数 a, b 和 m 使得

$$a^2 + b^2 = mp \text{ 且 } m \leqslant M - 1.$$

如果 $m = 1$, 则证明完成. 如果 $m \geqslant 2$, 则对 a, b, m 可再次使用费马递降程序来找到 p 的更小的倍数, 使其能表成两个平方数之和. 不断重复此过程, 我们最终得到 p 本身能表成两个平方数之和.

其中的递降程序如下: 首先

$$A^2 + B^2 = Mp,\ M < p,$$

将 A, B 模 M 到绝对最小剩余, 即选取数 u, v, 使得 $u \equiv A \pmod{M}$, $v \equiv B \pmod{M}$, $-\frac{1}{2}M \leqslant u, v \leqslant \frac{1}{2}M$. 观察到

$$u^2 + v^2 = A^2 + B^2 \equiv 0 \pmod{M},$$

即

$$u^2 + v^2 = Mr$$

其中 $1 \leqslant r < M$. 与 $A^2 + B^2 = Mp$ 相乘可得

$$\left(u^2 + v^2\right)\left(A^2 + B^2\right) = M^2 rp.$$

将左边平方和的乘积表成平方和

$$(uA + vB)^2 + (vA - uB)^2 = M^2 rp.$$

两边除以 M 得

$$\left(\frac{uA + vB}{M}\right)^2 + \left(\frac{vA - uB}{M}\right)^2 = rp.$$

由此得到能表成两平方数之和的 p 的更小倍数. □

将正整数表示成两数平方和

因为两平方数之和的乘积还是两平方数之和, 故将 m 表成两平方数之和可以将 m 素因数分解 $m = p_1 p_2 \cdots p_r$, 再将每个素数 p_i 表成两个平方数之和, 最后反复使用这一性质将 m 表成两个平方数之和.

定理 4.1.4 设 m 是正整数.

(a) 将 m 分解为

$$m = p_1 p_2 \cdots p_r M^2,$$

其中 $p_1, p_2, \cdots, p_r$ 是互不相同的素因子, 则 m 可表成两个平方数之和的充要条件是每个 p_i 或为 2 或为模 4 余 1.

(b) m 能表成两平方数之和 $m = a^2 + b^2$ 且 $(a, b) = 1$, 当且仅当以下两个条件之一成立:

(i) m 是奇数且 m 的每个素因子都模 4 余 1 (**推论:** c 是一个本原勾股数组斜边当且仅当 c 是模 4 余 1 的素数的乘积.);

(ii) m 是偶数, $m/2$ 是奇数且 $m/2$ 的每个素因子都模 4 余 1.

4.2 佩尔方程

4.2.1 三角平方数

一个平方数 n^2 可排列成 $n \times n$ 的正方形. 类似地, 一个三角数是指可排列成三角形的数. 第 m 个三角数是

$$1 + 2 + 3 + \cdots + m = \frac{m(m+1)}{2}.$$

同时是三角数的平方数称为 "三角平方数". 三角数具有形式 $m(m+1)/2$, 平方数具有形式 n^2, 所以三角平方数对应方程

$$n^2 = \frac{m(m+1)}{2}$$

的正整数解 n, m. 将上式两边同乘 8, 并做一点代数运算可得这提示我们作代换

$$8n^2 = 4m^2 + 4m = (2m+1)^2 - 1.$$

做代换

$$x = 2m + 1,\ y = 2n,$$

得到方程

$$2y^2 = x^2 - 1,$$

整理得

$$x^2 - 2y^2 = 1.$$

由这个方程的解可得到三角平方数

$$m = \frac{x-1}{2},\ n = \frac{y}{2}.$$

通过试验, 我们得到一组解 $(x, y) = (3, 2)$.

定理 4.2.1 (三角平方数定理) (i) 方程

$$x^2 - 2y^2 = 1$$

的每个正整数解都可通过将 $3 + 2\sqrt{2}$ 乘方得到, 即解 (x_k, y_k) 可以通过展开下式得到:

$$x_k + y_k\sqrt{2} = (3 + 2\sqrt{2})^k,\ k = 1, 2, 3, \cdots.$$

(ii) 每个三角平方数 $n^2 = \dfrac{1}{2}m(m+1)$ 由

$$m = \frac{x_k - 1}{2},\ n = \frac{y_k}{2},\ k = 1, 2, 3, \cdots$$

给出, 其中 (x_k, y_k) 是由 (i) 得到的解.

4.2.2 佩尔方程

我们给出了方程

$$x^2 - 2y^2 = 1$$

的正整数解 x, y 的完美描述. 这个方程是佩尔 (Pell) 方程的特例. **佩尔方程**是指具有形式

$$x^2 - Dy^2 = 1$$

的方程, 其中 D 是一个固定的正整数并且不是完全平方数 (容易验证 $D < 0$ 或 D 是完全平方数时方程只有平凡解 $(\pm 1, 0)$).

定理 4.2.2 (佩尔方程定理) 设 D 是一个正整数且不是完全平方数, 则佩尔方程

$$x^2 - Dy^2 = 1$$

总有正整数解. 如果 (x_1, y_1) 是使 x_1 最小的解, 则每个解 (x_k, y_k) 可通过取幂得到:

$$x_k + y_k\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)^k,\ k = 1, 2, 3, \cdots$$

对不定方程

$$x^2 - Dy^2 = M,$$

如果 $M \neq 1$, 则方程不一定有解. 证明方程无解可以考虑模 D 或模 M, 即若方程有解, 则

$$x^2 \equiv M \pmod{D},$$
$$x^2 \equiv Dy^2 \pmod{M},$$

如果上面的方程无解, 原方程一定无解, 但不能用这一方法证明有解.

索引

Bézout 等式, 4
倍数, 1
本原勾股数组, 55
不完全商, 2

次数, 52

带余除法, 2
单位群, 22

范数, 56

公倍数, 6
公因数, 2
勾股数组, 55

合数, 12
互素, 3

既约 (剩余) 系, 27
阶, 52
绝对 (值) 最小完全剩余系, 21

卡米歇尔数, 38

勒让德符号, 44
两两互素, 3

梅森素数, 16
模, 19

辗转相除法, 3

欧拉函数, 27

佩尔方程, 59
平方 (二次) 非剩余, 42
平方 (二次) 剩余, 42

素数, 12
算术基本定理, 13

同余, 19
同余类, 21
同余类环, 22
同余式, 19

完全剩余系, 21
完全数, 16

雅可比符号, 49
因数, 1
余数, 2
原根, 52

整除, 1
指标, 52
逐次平方法, 36
最大公因数, 3
最小非负完全剩余系, 21
最小公倍数, 6
最小正既约剩余系, 27