第二章 同余

1. 同余定义及基本性质

2. 剩余系

3. 欧拉函数与麦比乌斯函数

4. 一次同余方程

5. 中国剩余定理

6. 模为素数的高次同余方程

7. 模为合数的高次同余方程

前面一章讨论整除性和素数是利用因数来讨论的, 讨论的对象只是个别整数, 而整数有无穷多个, 如何全面地考虑全体整数呢?

前面一章讨论整除性和素数是利用因数来讨论的, 讨论的对象只是个别整数, 而整数有无穷多个, 如何全面地考虑全体整数呢?

如果用一个固定的数来除所有整数, 根据余数我们可以把全体整数进行分类, 余数相同的分在同一类. 因为任何固定数作为除数只能产生有限多个不同的余数, 所以按照这种方式, 我们可以把无穷多个整数分成有限多个类.

前面一章讨论整除性和素数是利用因数来讨论的, 讨论的对象只是个别整数, 而整数有无穷多个, 如何全面地考虑全体整数呢?

如果用一个固定的数来除所有整数, 根据余数我们可以把全体整数进行分类, 余数相同的分在同一类. 因为任何固定数作为除数只能产生有限多个不同的余数, 所以按照这种方式, 我们可以把无穷多个整数分成有限多个类.

进而我们将研究同一类的数有哪些性质, 不同类的数之间又有哪些关系, 这样我们就可以达到研究所有整数的目的.

本章我们介绍同余的基本理论.

同余概念最早出现在高斯 1801 年出版的名著 $\ll$ 算术研究 $\gg$ 中, 在日常生活中也经常碰到. 例如 10 月 1 日是星期四, 那么 10 月 8 日, 15 日, 22 日, 29 日都是星期四, 这是因为 1, 8, 15, 22, 29 这些数用 7 除有相同的余数.

同余概念最早出现在高斯 1801 年出版的名著 ≪ 算术研究 ≫ 中, 在日常生活中也经常碰到. 例如 10 月 1 日是星期四, 那么 10 月 8 日, 15 日, 22 日, 29 日都是星期四, 这是因为 1, 8, 15, 22, 29 这些数用 7 除有相同的余数.

定义 1.1. 设 $a, b \in \mathbb{Z}$, m 是一个正整数, 如果用 m 分别去除 a 和 b 所得的余数相同, 我们就称 a 和 b 关于模 m **同余**, 用符号 $a \equiv b \pmod{m}$ 表示; 如果余数不同, 我们就说 a 和 b 关于模 m **不同余**, 用符号 $a \not\equiv b \pmod{m}$ 表示.

同余概念最早出现在高斯 1801 年出版的名著 ≪ 算术研究 ≫ 中, 在日常生活中也经常碰到. 例如 10 月 1 日是星期四, 那么 10 月 8 日, 15 日, 22 日, 29 日都是星期四, 这是因为 1, 8, 15, 22, 29 这些数用 7 除有相同的余数.

定义 1.1. 设 $a, b \in \mathbb{Z}$, m 是一个正整数, 如果用 m 分别去除 a 和 b 所得的余数相同, 我们就称 a 和 b 关于模 m **同余**, 用符号 $a \equiv b \pmod{m}$ 表示; 如果余数不同, 我们就说 a 和 b 关于模 m **不同余**, 用符号 $a \not\equiv b \pmod{m}$ 表示.

例如, $2009 \equiv 1949 \pmod{10}$, $2009 \not\equiv 1949 \pmod{50}$.

在上面的定义中, 我们要求模 m 是正整数, 这是因为模为负整数的情形与模为正整数的情形完全一致, 即 $a \equiv b \pmod{m}$ 当且仅当 $a \equiv b \pmod{-m}$, 因此, 方便起见我们只考虑模为正整数的情况.

在上面的定义中, 我们要求模 m 是正整数, 这是因为模为负整数的情形与模为正整数的情形完全一致, 即 $a \equiv b \pmod{m}$ 当且仅当 $a \equiv b \pmod{-m}$, 因此, 方便起见我们只考虑模为正整数的情况.

假如 $a \equiv b \pmod{m}$, 那么存在 $t \in \mathbb{Z}$ 使得 $a = b + mt$.

在上面的定义中, 我们要求模 m 是正整数, 这是因为模为负整数的情形与模为正整数的情形完全一致, 即 $a \equiv b \pmod{m}$ 当且仅当 $a \equiv b \pmod{-m}$, 因此, 方便起见我们只考虑模为正整数的情况.

假如 $a \equiv b \pmod{m}$, 那么存在 $t \in \mathbb{Z}$ 使得 $a = b + mt$.

显然, 如果 a 和 b 关于模 m 同余, 那么 $m|a-b$; 否则有 $m \nmid (a-b)$. 因此 $a \equiv b \pmod{m}$ 的充要条件是 $m|a-b$. 关于模 1, 任意两个整数 a, b 都同余, 即 $a \equiv b \pmod{1}$. 关于模 2, 奇数与奇数同余, 偶数与偶数同余, 奇数与偶数不同余.

同余与通常的相等类似, 也是 $\mathbb{Z}$ 上的等价关系, 即:

命题 1.1. 设 $a, b, c \in \mathbb{Z}$, m 是任意正整数, 则模 m 同余是 $\mathbb{Z}$ 上的等价关系, 即下列性质成立.

(1) $a \equiv a \pmod{m}$. (自反性)

同余与通常的相等类似, 也是 $\mathbb{Z}$ 上的等价关系, 即:

命题 1.1. 设 $a, b, c \in \mathbb{Z}$, m 是任意正整数, 则模 m 同余是 $\mathbb{Z}$ 上的等价关系, 即下列性质成立.

(1) $a \equiv a \pmod{m}$. (自反性)
(2) 如果 $a \equiv b \pmod{m}$, 那么 $b \equiv a \pmod{m}$. (对称性)

同余与通常的相等类似, 也是 $\mathbb{Z}$ 上的等价关系, 即:

命题 1.1. 设 $a, b, c \in \mathbb{Z}$, m 是任意正整数, 则模 m 同余是 $\mathbb{Z}$ 上的等价关系, 即下列性质成立.

(1) $a \equiv a \pmod{m}$. (自反性)
(2) 如果 $a \equiv b \pmod{m}$, 那么 $b \equiv a \pmod{m}$. (对称性)
(3) 如果 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 那么 $a \equiv c \pmod{m}$. (传递性)

同余与通常的相等类似, 也是 $\mathbb{Z}$ 上的等价关系, 即:

命题 1.1. 设 $a, b, c \in \mathbb{Z}$, m 是任意正整数, 则模 m 同余是 $\mathbb{Z}$ 上的等价关系, 即下列性质成立.

(1) $a \equiv a \pmod{m}$. (自反性)
(2) 如果 $a \equiv b \pmod{m}$, 那么 $b \equiv a \pmod{m}$. (对称性)
(3) 如果 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 那么 $a \equiv c \pmod{m}$. (传递性)

同余与通常的相等类似, 也是 $\mathbb{Z}$ 上的等价关系, 即:

命题 1.1. 设 $a, b, c \in \mathbb{Z}$, m 是任意正整数, 则模 m 同余是 $\mathbb{Z}$ 上的等价关系, 即下列性质成立.

(1) $a \equiv a \pmod{m}$. (自反性)
(2) 如果 $a \equiv b \pmod{m}$, 那么 $b \equiv a \pmod{m}$. (对称性)
(3) 如果 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 那么 $a \equiv c \pmod{m}$. (传递性)

证明: 直接由定义即得. □

假设 $a \equiv 3 \pmod{17}$, $b \equiv 4 \pmod{17}$, 那么是否有类似等式的性质能得到 $a + b \equiv 7 \pmod{17}$, $a - b \equiv -1 \pmod{17}$, $ab \equiv 12 \pmod{17}$ 呢?

同余与通常的相等类似, 也是 $\mathbb{Z}$ 上的等价关系, 即:

命题 1.1. 设 $a, b, c \in \mathbb{Z}$, m 是任意正整数, 则模 m 同余是 $\mathbb{Z}$ 上的等价关系, 即下列性质成立.

(1) $a \equiv a \pmod{m}$. (自反性)
(2) 如果 $a \equiv b \pmod{m}$, 那么 $b \equiv a \pmod{m}$. (对称性)
(3) 如果 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 那么 $a \equiv c \pmod{m}$. (传递性)

证明: 直接由定义即得. □

假设 $a \equiv 3 \pmod{17}$, $b \equiv 4 \pmod{17}$, 那么是否有类似等式的性质能得到 $a + b \equiv 7 \pmod{17}$, $a - b \equiv -1 \pmod{17}$, $ab \equiv 12 \pmod{17}$ 呢?

答案是肯定的.

下面的定理给出同余的基本算术性质, 这样我们可以不必像上面那样将整数表示成商和余数来研究同余了.

定理 1.1. 设 $a, b, c, d \in \mathbb{Z}$, m 是任意正整数.

(1) 如果 $a \equiv b \pmod{m}$, 那么 $ac \equiv bc \pmod{m}$.

下面的定理给出同余的基本算术性质, 这样我们可以不必像上面那样将整数表示成商和余数来研究同余了.

定理 1.1. 设 $a, b, c, d \in \mathbb{Z}$, m 是任意正整数.

(1) 如果 $a \equiv b \pmod{m}$, 那么 $ac \equiv bc \pmod{m}$.

(2) 如果 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, 那么 $a + c \equiv b + d \pmod{m}$.

下面的定理给出同余的基本算术性质, 这样我们可以不必像上面那样将整数表示成商和余数来研究同余了.

定理 1.1. 设 $a, b, c, d \in \mathbb{Z}$, m 是任意正整数.

(1) 如果 $a \equiv b \pmod{m}$, 那么 $ac \equiv bc \pmod{m}$.

(2) 如果 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, 那么 $a + c \equiv b + d \pmod{m}$.

(3) 如果 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, 那么 $ac \equiv bd \pmod{m}$.

下面的定理给出同余的基本算术性质, 这样我们可以不必像上面那样将整数表示成商和余数来研究同余了.

定理 1.1. 设 $a, b, c, d \in \mathbb{Z}$, m 是任意正整数.

(1) 如果 $a \equiv b \pmod{m}$, 那么 $ac \equiv bc \pmod{m}$.

(2) 如果 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, 那么 $a + c \equiv b + d \pmod{m}$.

(3) 如果 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, 那么 $ac \equiv bd \pmod{m}$.

(4) 如果 $a \equiv b \pmod{m}$, 那么对任意正整数 n 有 $a^n \equiv b^n \pmod{m}$.

(1) $ac \equiv bc \pmod{m}$**;** **(2)** $a + c \equiv b + d \pmod{m}$**;**
(3) $ac \equiv bd \pmod{m}$**;** **(4)** $a^n \equiv b^n \pmod{m}$

证明: (1) 如果 $a \equiv b \pmod{m}$, 则有 $m|a-b$, 因此有 $m|(a-b)c$, 即 $m|ac-bc$, 所以 $ac \equiv bc \pmod{m}$.

(1) $ac \equiv bc \pmod{m}$; **(2)** $a + c \equiv b + d \pmod{m}$;
(3) $ac \equiv bd \pmod{m}$; **(4)** $a^n \equiv b^n \pmod{m}$

证明: (1) 如果 $a \equiv b \pmod{m}$, 则有 $m|a-b$, 因此有 $m|(a-b)c$, 即 $m|ac-bc$, 所以 $ac \equiv bc \pmod{m}$.

(2) 由 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ 知, $m|a-b$, 且 $m|c-d$, 所以 $m|a-b+c-d$, 即 $m|(a+c)-(b+d)$, 于是有 $a+c \equiv b+d \pmod{m}$.

(1) $ac \equiv bc \pmod m$; **(2)** $a + c \equiv b + d \pmod m$; **(3)** $ac \equiv bd \pmod m$; **(4)** $a^n \equiv b^n \pmod m$

证明: (1) 如果 $a \equiv b \pmod m$, 则有 $m|a-b$, 因此有 $m|(a-b)c$, 即 $m|ac-bc$, 所以 $ac \equiv bc \pmod m$.

(2) 由 $a \equiv b \pmod m$, $c \equiv d \pmod m$ 知, $m|a-b$, 且 $m|c-d$, 所以 $m|a-b+c-d$, 即 $m|(a+c)-(b+d)$, 于是有 $a+c \equiv b+d \pmod m$.

(3) 由假设知 $m|a-b$, $m|c-d$, 因此 $m|(a-b)c+b(c-d)$, 即 $m|ac-bd$, 所以 $ac \equiv bd \pmod m$.

(1) $ac \equiv bc \pmod{m}$; **(2)** $a + c \equiv b + d \pmod{m}$; **(3)** $ac \equiv bd \pmod{m}$; **(4)** $a^n \equiv b^n \pmod{m}$

证明: (1) 如果 $a \equiv b \pmod{m}$, 则有 $m|a-b$, 因此有 $m|(a-b)c$, 即 $m|ac-bc$, 所以 $ac \equiv bc \pmod{m}$.

(2) 由 $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ 知, $m|a-b$, 且 $m|c-d$, 所以 $m|a-b+c-d$, 即 $m|(a+c)-(b+d)$, 于是有 $a+c \equiv b+d \pmod{m}$.

(3) 由假设知 $m|a-b$, $m|c-d$, 因此 $m|(a-b)c+b(c-d)$, 即 $m|ac-bd$, 所以 $ac \equiv bd \pmod{m}$.

(4) 施归纳法于 n. $n=1$ 时显然成立. 假设 $n=k\ (\geq 1)$ 成立. 当 $n=k+1$ 时, 由 (3) 我们有 $aa^k \equiv bb^k \pmod{m}$, 即 $a^{k+1} \equiv b^{k+1} \pmod{m}$. 因此对 $\forall n$ 有 $a^n \equiv b^n \pmod{m}$. □

推论 1.1. 如果 $a \equiv b \pmod{m}$, 那么对任意整系数多项式 $f(x) = r_k x^k + \cdots + r_1 x + r_0$, 其中 $r_i \in \mathbb{Z},\ 0 \leq i \leq k$, 有 $f(a) \equiv f(b) \pmod{m}$.

推论 1.1. 如果 $a \equiv b \pmod{m}$, 那么对任意整系数多项式 $f(x) = r_k x^k + \cdots + r_1 x + r_0$, 其中 $r_i \in \mathbb{Z}$, $0 \le i \le k$, 有 $f(a) \equiv f(b) \pmod{m}$.

例 1.1. 求 5 除 2^{4k} 的最小非负余数 $\langle 2^{4k} \rangle_5$, 这里 k 是任意正整数.

推论 1.1. 如果 $a \equiv b \pmod{m}$, 那么对任意整系数多项式 $f(x) = r_k x^k + \cdots + r_1 x + r_0$, 其中 $r_i \in \mathbb{Z}$, $0 \le i \le k$, 有 $f(a) \equiv f(b) \pmod{m}$.

例 1.1. 求 5 除 2^{4k} 的最小非负余数 $\langle 2^{4k} \rangle_5$, 这里 k 是任意正整数.

解: 因为 $2^4 \equiv 16 \equiv 1 \pmod{5}$, 所以 $2^{4k} \equiv (2^4)^k \equiv 1^k \equiv 1 \pmod{5}$, 即 $2^{4k} \equiv 1 \pmod{5}$, 故 $\langle 2^{4k} \rangle_5 = 1$. □

例 1.2. 任意一个整数至少满足下列 5 个同余式中的一个:

$$x \equiv 0 \pmod 2,\ x \equiv 0 \pmod 3,\ x \equiv 1 \pmod 4,$$

$$x \equiv 5 \pmod 6,\ x \equiv 7 \pmod{12}.$$

例 1.2. 任意一个整数至少满足下列 5 个同余式中的一个:

$$x \equiv 0 \pmod 2,\ x \equiv 0 \pmod 3,\ x \equiv 1 \pmod 4,$$

$$x \equiv 5 \pmod 6,\ x \equiv 7 \pmod{12}.$$

证明: 显然, 任意偶数满足 $x \equiv 0 \ (\mathrm{mod}\ 2)$, 下面考虑奇数的情形. 所有奇数按模 12 分为 6 类: $12t+1$, $12t+3$, $12t+5$, $12t+7$, $12t+9$, $12t+11$, 这里 $t \in \mathbb{Z}$, 其中 $12t+1$ 满足 $x \equiv 1 \ (\mathrm{mod}\ 4)$, $12t+3$ 满足 $x \equiv 0 \ (\mathrm{mod}\ 3)$, $12t+5$ 满足 $x \equiv 1 \ (\mathrm{mod}\ 4)$, $12t+7$ 满足 $x \equiv 7 \ (\mathrm{mod}\ 12)$, $12t+9$ 满足 $x \equiv 0 \ (\mathrm{mod}\ 3)$, $12t+11$ 满足 $x \equiv 5 \ (\mathrm{mod}\ 6)$, 因此结论成立. $\square$

例 1.3. 设 n 是任意正整数, 则 $9|n$ 当且仅当 n 的各位数字 (10 进制) 之和能被 9 整除.

例 1.3. 设 n 是任意正整数, 则 $9|n$ 当且仅当 n 的各位数字 (10 进制) 之和能被 9 整除.

证明: 设 $n = r_k 10^k + r_{k-1} 10^{k-1} + \cdots + r_1 10 + r_0$, 其中 $r_0, r_1, \ldots, r_k \in \mathbb{Z}$. 考虑整系数多项式

$$f(x) = r_k x^k + r_{k-1} x^{k-1} + \cdots + r_1 x + r_0.$$

因为 $10 \equiv 1 \pmod 9$, 所以由推论1.1知 $f(10) \equiv f(1) \pmod 9$. 又因为 $f(10) = n$, $f(1) = r_k + r_{k-1} + \cdots + r_1 + r_0$, 所以 $n \equiv r_k + r_{k-1} + \cdots + r_1 + r_0 \pmod 9$, 该同余式右边正好是 n 的各位数字之和, 故 $9|n$ 当且仅当 n 的各位数字之和能被 9 整除. □

例 1.3. 设 n 是任意正整数, 则 $9|n$ 当且仅当 n 的各位数字 (10 进制) 之和能被 9 整除.

证明: 设 $n = r_k 10^k + r_{k-1}10^{k-1} + \cdots + r_1 10 + r_0$, 其中 $r_0, r_1, \ldots, r_k \in \mathbb{Z}$. 考虑整系数多项式

$$f(x) = r_k x^k + r_{k-1}x^{k-1} + \cdots + r_1 x + r_0.$$

因为 $10 \equiv 1 \pmod 9$, 所以由推论1.1知 $f(10) \equiv f(1) \pmod 9$. 又因为 $f(10) = n$, $f(1) = r_k + r_{k-1} + \cdots + r_1 + r_0$, 所以 $n \equiv r_k + r_{k-1} + \cdots + r_1 + r_0 \pmod 9$, 该同余式右边正好是 n 的各位数字之和, 故 $9|n$ 当且仅当 n 的各位数字之和能被 9 整除. □

我们可以使用例1.3中的任意正整数和它的各位数字之和关于模 9 同余的事实来检查一些乘法.

定理1.1仅仅给出了同余式的加 (减) 法和乘法性质, 我们自然会关心除法的同余性质.

然而对于除法, 一般情况下从 $ac \equiv bc \pmod{m}$ 不能得到 $a \equiv b \pmod{m}$, 即不能消去 c.

定理1.1仅仅给出了同余式的加 (减) 法和乘法性质, 我们自然会关心除法的同余性质.

然而对于除法, 一般情况下从 $ac \equiv bc \pmod{m}$ 不能得到 $a \equiv b \pmod{m}$, 即不能消去 c.

定理 1.2.

(1) 如果 $a \equiv b \pmod{m}$, 正整数 $d|m$, 那么 $a \equiv b \pmod{d}$.

定理1.1仅仅给出了同余式的加 (减) 法和乘法性质, 我们自然会关心除法的同余性质.

然而对于除法, 一般情况下从 $ac \equiv bc \pmod{m}$ 不能得到 $a \equiv b \pmod{m}$, 即不能消去 c.

定理 1.2.

(1) 如果 $a \equiv b \pmod{m}$, 正整数 $d|m$, 那么 $a \equiv b \pmod{d}$.
(2) 如果 $ac \equiv bc \pmod{m}$, 则 $a \equiv b \pmod{m/(c,m)}$.

定理1.1仅仅给出了同余式的加 (减) 法和乘法性质, 我们自然会关心除法的同余性质.

然而对于除法, 一般情况下从 $ac \equiv bc \pmod m$ 不能得到 $a \equiv b \pmod m$, 即不能消去 c.

定理 1.2.

(1) 如果 $a \equiv b \pmod m$, 正整数 $d|m$, 那么 $a \equiv b \pmod d$.
(2) 如果 $ac \equiv bc \pmod m$, 则 $a \equiv b \pmod{m/(c,m)}$.

定理1.1仅仅给出了同余式的加 (减) 法和乘法性质, 我们自然会关心除法的同余性质.

然而对于除法, 一般情况下从 $ac \equiv bc \pmod{m}$ 不能得到 $a \equiv b \pmod{m}$, 即不能消去 c.

定理 1.2.

(1) 如果 $a \equiv b \pmod{m}$, 正整数 $d|m$, 那么 $a \equiv b \pmod{d}$.
(2) 如果 $ac \equiv bc \pmod{m}$, 则 $a \equiv b \pmod{m/(c,m)}$.

证明: (1) 由 $a \equiv b \pmod{m}$ 知, $m|a-b$. 因为 $d|m$, 所以 $d|a-b$, 故 $a \equiv b \pmod{d}$.

定理1.1仅仅给出了同余式的加 (减) 法和乘法性质, 我们自然会关心除法的同余性质.

然而对于除法, 一般情况下从 $ac \equiv bc \pmod{m}$ 不能得到 $a \equiv b \pmod{m}$, 即不能消去 c.

定理 1.2.

(1) 如果 $a \equiv b \pmod{m}$, 正整数 $d|m$, 那么 $a \equiv b \pmod{d}$.
(2) 如果 $ac \equiv bc \pmod{m}$, 则 $a \equiv b \pmod{m/(c,m)}$.

证明: (1) 由 $a \equiv b \pmod{m}$ 知, $m|a-b$. 因为 $d|m$, 所以 $d|a-b$, 故 $a \equiv b \pmod{d}$.

(2) 令 $d=(c,m)$. 由 $ac \equiv bc \pmod{m}$ 知, 存在 $k \in \mathbb{Z}$ 使得 $ac-bc=km$, 于是有 $(a-b)\frac{c}{d}=k\frac{m}{d}$. 又因为 $d=(c,m)$, 所以 $(\frac{c}{d},\frac{m}{d})=1$. 从而有 $\frac{m}{d}|a-b$, 即 $a \equiv b \pmod{m/d}$. □

上面定理的一种特殊情形是: 当 $(c, m) = 1$ 时, $ac \equiv bc \pmod{m}$ 蕴含 $a \equiv b \pmod{m}$.

上面定理的一种特殊情形是: 当 $(c,m)=1$ 时, $ac \equiv bc \pmod{m}$ 蕴含 $a \equiv b \pmod{m}$.

在以后的应用中, 我们需要组合不同模的同余式. 如果 $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$, 那么一般情况下我们不能得到 $a \equiv b \pmod{mn}$. 例如, $20 \equiv 2 \pmod{3}$, $20 \equiv 2 \pmod{9}$, 但 $20 \not\equiv 2 \pmod{27}$.

上面定理的一种特殊情形是: 当 $(c,m)=1$ 时, $ac \equiv bc \pmod{m}$ 蕴含 $a \equiv b \pmod{m}$.

在以后的应用中, 我们需要组合不同模的同余式. 如果 $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$, 那么一般情况下我们不能得到 $a \equiv b \pmod{mn}$. 例如, $20 \equiv 2 \pmod{3}$, $20 \equiv 2 \pmod{9}$, 但 $20 \not\equiv 2 \pmod{27}$.

尽管如此, 我们有下面的结果.

定理 1.3. 如果 $a \equiv b \pmod{m}$, 又 $a \equiv b \pmod{n}$, 那么 $a \equiv b \pmod{[m,n]}$.

上面定理的一种特殊情形是: 当 $(c,m)=1$ 时, $ac\equiv bc \pmod m$ 蕴含 $a\equiv b \pmod m$.

在以后的应用中, 我们需要组合不同模的同余式. 如果 $a\equiv b \pmod m$, $a\equiv b \pmod n$, 那么一般情况下我们不能得到 $a\equiv b \pmod{mn}$. 例如, $20\equiv 2 \pmod 3$, $20\equiv 2 \pmod 9$, 但 $20\not\equiv 2 \pmod{27}$.

尽管如此, 我们有下面的结果.

定理 1.3. 如果 $a\equiv b \pmod m$, 又 $a\equiv b \pmod n$, 那么 $a\equiv b \pmod{[m,n]}$.

证明: 由 $a\equiv b \pmod m$ 及 $a\equiv b \pmod n$ 知, $m|a-b$ 且 $n|a-b$, 因此 $a-b$ 是 m,n 的公倍数, 所以 $[m,n]|a-b$. □

由上面的定理, 我们有下面的推论.

推论 1.2. 如果 $(m,n)=1$, 那么 $a\equiv b \pmod{mn}$ 当且仅当

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

由上面的定理, 我们有下面的推论.

推论 1.2. 如果 $(m, n) = 1$, 那么 $a \equiv b \pmod{mn}$ 当且仅当

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

证明: 由上面的定理, 充分性是显然的. 由定理1.2, 必要性也是显然的. □

由上面的定理, 我们有下面的推论.

推论 1.2. 如果 $(m,n)=1$, 那么 $a \equiv b \pmod{mn}$ 当且仅当

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

证明: 由上面的定理, 充分性是显然的. 由定理1.2, 必要性也是显然的. $\square$

推论1.2的意义在于研究模 m 为合数的同余可以转化为研究模为 m 的标准分解中素数幂的同余. 例如, $a \equiv b \pmod{12}$ 等价于 $a \equiv b \pmod{2^2}$ 和 $a \equiv b \pmod{3}$.

1. 同余定义及基本性质

2. 剩余系

3. 欧拉函数与麦比乌斯函数

4. 一次同余方程

5. 中国剩余定理

6. 模为素数的高次同余方程

7. 模为合数的高次同余方程

由命题1.1知, 模 m 同余是 $\mathbb{Z}$ 上的等价关系, 它将全体整数划分为 m 个等价类, 用 $\mathbb{Z}_m$ 表示全体等价类组成的集合.

由命题1.1知, 模 m 同余是 $\mathbb{Z}$ 上的等价关系, 它将全体整数划分为 m 个等价类, 用 $\mathbb{Z}_m$ 表示全体等价类组成的集合.

同一等价类中的元素具有相同的余数, 每个等价类中的元素由公式 $km+r$ $(k\in\mathbb{Z})$ 给出, 这里 r 是该等价类对应的余数, 因此余数相同的整数在同一个等价类.

由命题1.1知, 模 m 同余是 $\mathbb{Z}$ 上的等价关系, 它将全体整数划分为 m 个等价类, 用 $\mathbb{Z}_m$ 表示全体等价类组成的集合.

同一等价类中的元素具有相同的余数, 每个等价类中的元素由公式 $km + r$ $(k \in \mathbb{Z})$ 给出, 这里 r 是该等价类对应的余数, 因此余数相同的整数在同一个等价类.

换言之, 等价类是由余数惟一确定的, 因此我们可以用 $[r]$ 表示等价类. 于是有 $\mathbb{Z}_3 = \{[0], [1], [2]\}$. 在不引起混淆的情况下, 我们有时直接用余数 r 表示等价类, 在这种记号下, $\mathbb{Z}_3 = \{0, 1, 2\}$.

由命题1.1知, 模 m 同余是 $\mathbb{Z}$ 上的等价关系, 它将全体整数划分为 m 个等价类, 用 $\mathbb{Z}_m$ 表示全体等价类组成的集合.

同一等价类中的元素具有相同的余数, 每个等价类中的元素由公式 $km+r$ $(k\in\mathbb{Z})$ 给出, 这里 r 是该等价类对应的余数, 因此余数相同的整数在同一个等价类.

换言之, 等价类是由余数惟一确定的, 因此我们可以用 $[r]$ 表示等价类. 于是有 $\mathbb{Z}_3=\{[0],[1],[2]\}$. 在不引起混淆的情况下, 我们有时直接用余数 r 表示等价类, 在这种记号下, $\mathbb{Z}_3=\{0,1,2\}$.

定理1.1实际上定义了 $\mathbb{Z}_m$ 上的加 (减) 和乘运算, 这些运算不依赖于等价类中代表元的选取. 在很多情况下, 我们都只需要从每个等价类中选取一个元素来讨论, 而不必考虑等价类中的所有元素.

定义 2.1. 设 $S \subseteq \mathbb{Z}$, 如果任意整数都与 S 中正好一个元素关于模 m 同余, 则称 S 是模 m 的一个**完全剩余系**(或简称为**剩余系**).

定义 2.1. 设 $S \subseteq \mathbb{Z}$, 如果任意整数都与 S 中正好一个元素关于模 m 同余, 则称 S 是模 m 的一个**完全剩余系**(或简称为**剩余系**).

例如, $\{0, 1, 2\}$ 和 $\{-3, 4, 8\}$ 都是模 3 的完全剩余系.

定义 2.1. 设 $S \subseteq \mathbb{Z}$, 如果任意整数都与 S 中正好一个元素关于模 m 同余, 则称 S 是模 m 的一个**完全剩余系**(或简称为**剩余系**).

例如, $\{0, 1, 2\}$ 和 $\{-3, 4, 8\}$ 都是模 3 的完全剩余系.

对任意正整数 m, 因为任一整数用 m 去除得到的最小非负余数必定是 $0, 1, 2, \ldots, m-1$ 中的某个数, 即任一整数关于模 m 必定与 $0, 1, 2, \ldots, m-1$ 中某一数同余, 所以 $S = \{0, 1, 2, \ldots, m-1\}$ 是模 m 的一个完全剩余系, 该完全剩余系称作**标准剩余系**或**最小非负完全剩余系**.

定理 2.1. 设 $S = \{a_1, a_2, \ldots, a_k\} \subseteq \mathbb{Z}$, 则 S 是模 m 的一个完全剩余系的充要条件是:

(1) $k = m$;

定理 2.1. 设 $S=\{a_1,a_2,\ldots,a_k\}\subseteq\mathbb{Z}$, 则 S 是模 m 的一个完全剩余系的充要条件是:

(1) $k=m$;

(2) 当 $i\neq j$ 时, $a_i\not\equiv a_j \pmod{m}$.

定理 2.1. 设 $S = \{a_1, a_2, \ldots, a_k\} \subseteq \mathbb{Z}$, 则 S 是模 m 的一个完全剩余系的充要条件是:

(1) $k = m$;

(2) 当 $i \neq j$ 时, $a_i \not\equiv a_j \pmod{m}$.

定理 2.1. 设 $S=\{a_1,a_2,\ldots,a_k\}\subseteq\mathbb{Z}$, 则 S 是模 m 的一个完全剩余系的充要条件是:

(1) $k=m$;

(2) 当 $i\neq j$ 时, $a_i\not\equiv a_j \pmod m$.

证明: 如果 S 是模 m 的一个完全剩余系, 那么由定义知 $|S|=m$. 另外由定义, S 中每个元素都只与自身同余, 即不同元素关于模 m 是不同余的, 所以必要性成立.

定理 2.1. 设 $S = \{a_1, a_2, \ldots, a_k\} \subseteq \mathbb{Z}$, 则 S 是模 m 的一个完全剩余系的充要条件是:

(1) $k = m$;

(2) 当 $i \neq j$ 时, $a_i \not\equiv a_j \pmod{m}$.

证明: 如果 S 是模 m 的一个完全剩余系, 那么由定义知 $|S| = m$. 另外由定义, S 中每个元素都只与自身同余, 即不同元素关于模 m 是不同余的, 所以必要性成立.

反过来, 假设 $k = m$, 且 S 中任意两个元素关于模 m 均不同余, 那么 S 中每个元素都属于 $\mathbb{Z}_m$ 中不同的等价类, 每个等价类正好包含 S 中一个元素, 而任意整数属于且仅属于一个等价类, 这表明任意整数都与 S 中正好一个元素关于模 m 同余, 所以 S 是模 m 的一个完全剩余系, 充分性成立. $\square$

上面定理表明, 任意 m 个互不同余的数构成模 m 的一个完全剩余系.

从一个给定的完全剩余系, 我们可以使用下面的定理构造新的完全剩余系.

定理 2.2. 设 $S=\{a_1,a_2,\ldots,a_m\}$ 是模 m 的一个完全剩余系, $(k,m)=1$, 则 $S'=\{ka_1+b,ka_2+b,\ldots,ka_m+b\}$ 也是模 m 的一个完全剩余系, 这里 b 是任意整数.

上面定理表明, 任意 m 个互不同余的数构成模 m 的一个完全剩余系.

从一个给定的完全剩余系, 我们可以使用下面的定理构造新的完全剩余系.

定理 2.2. 设 $S=\{a_1,a_2,\ldots,a_m\}$ 是模 m 的一个完全剩余系, $(k,m)=1$, 则 $S'=\{ka_1+b,ka_2+b,\ldots,ka_m+b\}$ 也是模 m 的一个完全剩余系, 这里 b 是任意整数.

证明: 由定理2.1知, 我们只需证明当 $i\neq j$ 时, $ka_i+b\not\equiv ka_j+b \pmod m$ 即可. 下面用反证法来证明, 假设 $ka_i+b\equiv ka_j+b \pmod m$, 那么必然有 $ka_i\equiv ka_j \pmod m$, 即 $m|k(a_i-a_j)$. 因为 $(k,m)=1$, 所以 $m|a_i-a_j$, 即 $a_i\equiv a_j \pmod m$, 这与 S 是模 m 的一个完全剩余系矛盾, 因此定理成立.

例 2.1. 设 m 是正偶数, $\{a_1, a_2, \ldots, a_m\}$ 和 $\{b_1, b_2, \ldots, b_m\}$ 都是模 m 的完全剩余系, 试证 $\{a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m\}$ 不是模 m 的完全剩余系.

例 2.1. 设 m 是正偶数, $\{a_1, a_2, \ldots, a_m\}$ 和 $\{b_1, b_2, \ldots, b_m\}$ 都是模 m 的完全剩余系, 试证 $\{a_1+b_1, a_2+b_2, \ldots, a_m+b_m\}$ 不是模 m 的完全剩余系.

证明: 因为 $\{a_1, a_2, \ldots, a_m\}$ 是模 m 的完全剩余系, 所以 $\sum_{i=1}^m a_i \equiv \sum_{i=1}^m i = \frac{m(m+1)}{2} \equiv \frac{m}{2} \pmod m$. 同理, 有 $\sum_{i=1}^m b_i \equiv \frac{m}{2} \pmod m$. 如果 $\{a_1+b_1, a_2+b_2, \ldots, a_m+b_m\}$ 也是模 m 的完全剩余系, 则同理也有 $\sum_{i=1}^m (a_i+b_i) \equiv \frac{m}{2} \pmod m$.

但是 $\sum_{i=1}^m (a_i+b_i) = \sum_{i=1}^m a_i + \sum_{i=1}^m b_i \equiv \frac{m}{2} + \frac{m}{2} = m \equiv 0 \pmod m$, 所以 $\frac{m}{2} \equiv 0 \pmod m$, 矛盾! 故 $\{a_1+b_1, a_2+b_2, \ldots, a_m+b_m\}$ 不是模 m 的完全剩余系. $\square$

在模 m 的一个完全剩余系 S 中, 有的数与 m 互素, 有的数与 m 不互素, 所有与 m 互素的数构成的集合称作模 m 的一个**既约剩余系**. 例如, $\{1,2\}$ 和 $\{4,8\}$ 都是模 3 的既约剩余系.

在模 m 的一个完全剩余系 S 中, 有的数与 m 互素, 有的数与 m 不互素, 所有与 m 互素的数构成的集合称作模 m 的一个**既约剩余系**. 例如, $\{1, 2\}$ 和 $\{4, 8\}$ 都是模 3 的既约剩余系.

因为当 $(a, m) = 1$ 时, a 所在的等价类中的数都与 m 互素, 当 $(a, m) > 1$ 时, a 所在的等价类中的数都与 m 不互素, 所以既约剩余系中元素的个数与原来所取的完全剩余系无关, 而由 m 惟一决定.

在模 m 的一个完全剩余系 S 中, 有的数与 m 互素, 有的数与 m 不互素, 所有与 m 互素的数构成的集合称作模 m 的一个**既约剩余系**. 例如, $\{1,2\}$ 和 $\{4,8\}$ 都是模 3 的既约剩余系.

因为当 $(a,m)=1$ 时, a 所在的等价类中的数都与 m 互素, 当 $(a,m)>1$ 时, a 所在的等价类中的数都与 m 不互素, 所以既约剩余系中元素的个数与原来所取的完全剩余系无关, 而由 m 惟一决定.

欧拉用 $\phi(m)$ 表示模 m 的既约剩余系所含元素的个数, 换言之, 对任意正整数 m, $\phi(m)$ 表示所有不大于 m 且与 m 互素的正整数的个数, 这样得到的函数 $\phi:\mathbb{N}\longrightarrow\mathbb{N}$ 称作**欧拉函数**. 显然, 由定义 $\phi(1)=\phi(2)=1$, $\phi(3)=\phi(4)=2$, $\phi(5)=4, \ldots$.

与完全剩余系类似, 我们有如下判定一个集合是否是既约剩余系的定理.

定理 2.3. 设 $S = \{a_1, a_2, \ldots, a_k\} \subseteq \mathbb{Z}$, 则 S 是模 m 的一个既约剩余系的充要条件是:

(1) $k = \phi(m)$;

与完全剩余系类似, 我们有如下判定一个集合是否是既约剩余系的定理.

定理 2.3. 设 $S = \{a_1, a_2, \ldots, a_k\} \subseteq \mathbb{Z}$, 则 S 是模 m 的一个既约剩余系的充要条件是:

(1) $k = \phi(m)$;

(2) 当 $i \neq j$ 时, $a_i \not\equiv a_j \pmod{m}$;

与完全剩余系类似, 我们有如下判定一个集合是否是既约剩余系的定理.

定理 2.3. 设 $S = \{a_1, a_2, \ldots, a_k\} \subseteq \mathbb{Z}$, 则 S 是模 m 的一个既约剩余系的充要条件是:

(1) $k = \phi(m)$;

(2) 当 $i \neq j$ 时, $a_i \not\equiv a_j \pmod{m}$;

(3) 对任意 $a_i \in S$, 都有 $(a_i, m) = 1$.

与完全剩余系类似, 我们有如下判定一个集合是否是既约剩余系的定理.

定理 2.3. 设 $S=\{a_1,a_2,\ldots,a_k\}\subseteq\mathbb{Z}$, 则 S 是模 m 的一个既约剩余系的充要条件是:

(1) $k=\phi(m)$;

(2) 当 $i\neq j$ 时, $a_i\not\equiv a_j \pmod m$;

(3) 对任意 $a_i\in S$, 都有 $(a_i,m)=1$.

与完全剩余系类似, 我们有如下判定一个集合是否是既约剩余系的定理.

定理 2.3. 设 $S=\{a_1,a_2,\ldots,a_k\}\subseteq\mathbb{Z}$, 则 S 是模 m 的一个既约剩余系的充要条件是:

(1) $k=\phi(m)$;

(2) 当 $i\neq j$ 时, $a_i\not\equiv a_j \pmod{m}$;

(3) 对任意 $a_i\in S$, 都有 $(a_i,m)=1$.

证明: 必要性由定义即得, 下面考虑充分性. 因为 $a_i\not\equiv a_j \pmod{m}$, 所以 S 中的 k 个数属于 $\mathbb{Z}_m$ 的 k 个不同的等价类, 又因为 $k=\phi(m)$, S 中每个元素都与 m 互素, 所以 $a_1,a_2,\ldots,a_k$ 是模 m 的完全剩余系中全部与 m 互素的数, 因此 S 是模 m 的既约剩余系, 这就证明了充分性. $\square$

与定理2.2类似, 我们有下面的结果.

定理 2.4. 设 $S=\{a_1,a_2,\ldots,a_{\phi(m)}\}$ 是模 m 的一个既约剩余系, $(k,m)=1$, 则 $S'=\{ka_1,\ ka_2,\ldots,ka_{\phi(m)}\}$ 也是模 m 的一个既约剩余系.

与定理2.2类似, 我们有下面的结果.

定理 2.4. 设 $S=\{a_1,a_2,\ldots,a_{\phi(m)}\}$ 是模 m 的一个既约剩余系, $(k,m)=1$, 则 $S'=\{ka_1,\,ka_2,\ldots,ka_{\phi(m)}\}$ 也是模 m 的一个既约剩余系.

证明: 因为当 $i\neq j$ 时, $a_i\not\equiv a_j \pmod{m}$, 又 $(k,m)=1$, 所以 $ka_i\not\equiv ka_j \pmod{m}$. 另外, 对任意 $ka_i\in S'$, 因为 $(k,m)=1$, 所以有 $(ka_i,m)=(a_i,m)=1$. 于是由定理2.3知, S' 是模 m 的一个既约剩余系, 因此定理成立. □

定理 2.5 (欧拉定理). 设 $a \in \mathbb{Z}$, m 是正整数, 如果 $(a, m) = 1$, 那么 $a^{\phi(m)} \equiv 1 \pmod{m}$.

定理 2.5 (欧拉定理). 设 $a \in \mathbb{Z}$, m 是正整数, 如果 $(a, m) = 1$, 那么 $a^{\phi(m)} \equiv 1 \pmod{m}$.

证明: 设 $S = \{a_1, a_2, \ldots, a_{\phi(m)}\}$ 是模 m 的一个既约剩余系, 则由定理2.4知, $S' = \{aa_1, aa_2, \ldots, aa_{\phi(m)}\}$ 也是模 m 的一个既约剩余系, 所以 S' 中任一数必与 S 中某个数关于模 m 同余, 于是有

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} a_i = \prod_{i=1}^{\phi(m)} (aa_i) \equiv \prod_{i=1}^{\phi(m)} a_i \pmod{m}, \qquad (1)$$

即 $m | (a^{\phi(m)} - 1) \cdot \prod_{i=1}^{\phi(m)} a_i$.

定理 2.5 (欧拉定理). 设 $a \in \mathbb{Z}$, m 是正整数, 如果 $(a, m) = 1$, 那么 $a^{\phi(m)} \equiv 1 \pmod{m}$.

证明: 设 $S = \{a_1, a_2, \ldots, a_{\phi(m)}\}$ 是模 m 的一个既约剩余系, 则由定理2.4知, $S' = \{aa_1, aa_2, \ldots, aa_{\phi(m)}\}$ 也是模 m 的一个既约剩余系, 所以 S' 中任一数必与 S 中某个数关于模 m 同余, 于是有

$$a^{\phi(m)} \prod_{i=1}^{\phi(m)} a_i = \prod_{i=1}^{\phi(m)} (aa_i) \equiv \prod_{i=1}^{\phi(m)} a_i \pmod{m}, \qquad (1)$$

即 $m | (a^{\phi(m)} - 1) \cdot \prod_{i=1}^{\phi(m)} a_i$.

另一方面, 由既约剩余系定义知, 对所有 $1 \le i \le \phi(m)$ 都有 $(a_i, m) = 1$, 所以 $(\prod_{i=1}^{\phi(m)} a_i, m) = 1$, 从而 $m | a^{\phi(m)} - 1$, 即 $a^{\phi(m)} \equiv 1 \pmod{m}$, 故定理成立. □

欧拉定理的一种特殊情形是 $m = p$, 这里 p 是素数. 此时, $\phi(p) = p - 1$, 代入 (1) 式即得下面的费马小定理, 它是费马于 1640 年提出, 欧拉 1736 年证明的.

定理 2.6 (费马小定理). 如果 $a \in \mathbb{Z}$, p 是素数, 则

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

特别地, 若 $p \nmid a$, 则

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

欧拉定理的一种特殊情形是 $m = p$, 这里 p 是素数. 此时, $\phi(p) = p - 1$, 代入 (1) 式即得下面的费马小定理, 它是费马于 1640 年提出, 欧拉 1736 年证明的.

定理 2.6 (费马小定理). 如果 $a \in \mathbb{Z}$, p 是素数, 则

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

特别地, 若 $p \nmid a$, 则

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

证明: 若 $p|a$, 则 $a^p \equiv a \pmod p$ 显然成立. 若 $p \nmid a$, 则有 $(p, a) = 1$, 于是由欧拉定理知, $a^{p-1} = a^{\phi(p)} \equiv 1 \pmod p$, 即 $a^{p-1} \equiv 1 \pmod p$, 用 a 乘该同余式两边即得 $a^p \equiv a \pmod p$. 这就证明了定理. □

费马小定理说, 如果 p 是素数, 那么对任意整数 a 都有 $a^p \equiv a \pmod p$. 因此如果存在整数 b 使得 $b^n \not\equiv b \pmod n$, 那么 n 必定不是素数.

例如, 63 不是素数, 因为 $2^{63} = (2^6)^{10} \cdot 2^3 \equiv 2^3 \not\equiv 2 \pmod{63}$.

值得注意的是, 这种判定 n 是合数的方法不需要对 n 进行分解.

费马小定理说, 如果 p 是素数, 那么对任意整数 a 都有 $a^p \equiv a \pmod{p}$. 因此如果存在整数 b 使得 $b^n \not\equiv b \pmod{n}$, 那么 n 必定不是素数.

例如, 63 不是素数, 因为 $2^{63} = (2^6)^{10} \cdot 2^3 \equiv 2^3 \not\equiv 2 \pmod{63}$.

值得注意的是, 这种判定 n 是合数的方法不需要对 n 进行分解.

例 2.2. 求 $\langle 3^{301} \rangle_{11}$.

费马小定理说, 如果 p 是素数, 那么对任意整数 a 都有 $a^p \equiv a \pmod{p}$. 因此如果存在整数 b 使得 $b^n \not\equiv b \pmod{n}$, 那么 n 必定不是素数.

例如, 63 不是素数, 因为 $2^{63} = (2^6)^{10} \cdot 2^3 \equiv 2^3 \not\equiv 2 \pmod{63}$.

值得注意的是, 这种判定 n 是合数的方法不需要对 n 进行分解.

例 2.2. 求 $\langle 3^{301} \rangle_{11}$.

解: 由费马小定理知, $3^{10} \equiv 1 \pmod{11}$, 所以

$$3^{301} = (3^{10})^{30} \cdot 3 \equiv 3 \pmod{11},$$

于是得 $\langle 3^{301} \rangle_{11} = 3$. $\square$

1. 同余定义及基本性质

2. 剩余系

3. 欧拉函数与麦比乌斯函数

4. 一次同余方程

5. 中国剩余定理

6. 模为素数的高次同余方程

7. 模为合数的高次同余方程

在上节欧拉定理中, 当 a 和 m 互素时, 我们有公式 $a^{\phi(m)} \equiv 1 \pmod{m}$, 其中欧拉函数 $\phi(m)$ 表示模 m 的既约剩余系中所含元素的个数, 它正好等于不大于 m 且与 m 互素的正整数的个数.

在上节欧拉定理中, 当 a 和 m 互素时, 我们有公式 $a^{\phi(m)} \equiv 1 \pmod{m}$, 其中欧拉函数 $\phi(m)$ 表示模 m 的既约剩余系中所含元素的个数, 它正好等于不大于 m 且与 m 互素的正整数的个数.

但是, 除非能找到计算 $\phi(m)$ 的有效方法, 否则欧拉定理的用途不能完全发挥出来. 显然, 我们不想列出 1 到 m 的所有整数来检查每个数是否与 m 互素. 例如, 如果 $m \approx 10^3$, 会耗费许多时间, 但对 $m \approx 10^{100}$ 这么大的数则几乎是不可能的.

在上节欧拉定理中, 当 a 和 m 互素时, 我们有公式 $a^{\phi(m)} \equiv 1 \pmod m$, 其中欧拉函数 $\phi(m)$ 表示模 m 的既约剩余系中所含元素的个数, 它正好等于不大于 m 且与 m 互素的正整数的个数.

但是, 除非能找到计算 $\phi(m)$ 的有效方法, 否则欧拉定理的用途不能完全发挥出来. 显然, 我们不想列出 1 到 m 的所有整数来检查每个数是否与 m 互素. 例如, 如果 $m \approx 10^3$, 会耗费许多时间, 但对 $m \approx 10^{100}$ 这么大的数则几乎是不可能的.

这节我们讨论计算欧拉函数 $\phi(m)$ 的一般方法, 以及与欧拉函数密切相关的另外一类函数 —— 麦比乌斯函数.

定理 3.1.

(1) 如果 p 是素数且 $\alpha \geq 1$, 则

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}. \tag{2}$$

定理 3.1.

(1) 如果 p 是素数且 $\alpha \geq 1$, 则

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}. \tag{2}$$

(2) 如果 $(a, b) = 1$, 那么

$$\phi(ab) = \phi(a)\phi(b). \tag{3}$$

定理 3.1.

(1) 如果 p 是素数且 $\alpha \geq 1$, 则

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}. \tag{2}$$

(2) 如果 $(a, b) = 1$, 那么

$$\phi(ab) = \phi(a)\phi(b). \tag{3}$$

定理 3.1.

(1) 如果 p 是素数且 $\alpha \geq 1$, 则

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}. \tag{2}$$

(2) 如果 $(a, b) = 1$, 那么

$$\phi(ab) = \phi(a)\phi(b). \tag{3}$$

证明: (1) 考虑模 p^α 的完全剩余系 $S = \{1, 2, \ldots, p^\alpha\}$, 在 S 中与 p^α 不互素的数只有 p 的倍数: $p, 2p, \ldots, p^{\alpha-1}p$, 这总共有 $p^{\alpha-1}$ 个, 其余 $p^\alpha - p^{\alpha-1}$ 个数都是与 p^α 互素的, 因此 p^α 的既约剩余系含有 $p^\alpha - p^{\alpha-1}$ 个元素, 故

$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

$(a, b) = 1 \Rightarrow \phi(ab) = \phi(a)\phi(b)$

(2) 设 $S_a = \{x_1, x_2, \ldots, x_{\phi(a)}\}$ 和 $S_b = \{y_1, y_2, \ldots, y_{\phi(b)}\}$ 分别是模 a 和模 b 的既约剩余系. 由既约剩余系性质易知, 如果 $x_i \neq x_{i'}$ $(1 \leq i, i' \leq \phi(a))$ 或者 $y_j \neq y_{j'}$ $(1 \leq j, j' \leq \phi(b))$, 那么 $bx_i + ay_j \neq bx_{i'} + ay_{j'}$. 因此
$S_{ab} = \{bx_i + ay_j | 1 \leq i \leq \phi(a), 1 \leq j \leq \phi(b)\}$ 中含有
$\phi(a)\phi(b)$ 个数. 欲证 (3) 式, 我们只需证明 S_{ab} 是 ab 的一个既约剩余系即可. 我们分三步来证明.

$(a,b)=1 \Rightarrow \phi(ab)=\phi(a)\phi(b)$

(2) 设 $S_a=\{x_1,x_2,\ldots,x_{\phi(a)}\}$ 和 $S_b=\{y_1,y_2,\ldots,y_{\phi(b)}\}$ 分别是模 a 和模 b 的既约剩余系. 由既约剩余系性质易知, 如果 $x_i \neq x_{i'}$ $(1 \le i, i' \le \phi(a))$ 或者 $y_j \neq y_{j'}$ $(1 \le j, j' \le \phi(b))$, 那么 $bx_i+ay_j \neq bx_{i'}+ay_{j'}$. 因此
$S_{ab}=\{bx_i+ay_j | 1 \le i \le \phi(a), 1 \le j \le \phi(b)\}$ 中含有
$\phi(a)\phi(b)$ 个数. 欲证 (3) 式, 我们只需证明 S_{ab} 是 ab 的一个既约剩余系即可. 我们分三步来证明.

(i) 先证: S_{ab} 中任意两个数关于模 ab 均不同余. 假设
$bx_i+ay_j, bx_{i'}+ay_{j'} \in S_{ab}$ 使得 $bx_i+ay_j \equiv bx_{i'}+ay_{j'}$
$\pmod{ab}$, 那么必有 $bx_i+ay_j \equiv bx_{i'}+ay_{j'} \pmod{a}$, 于是
$bx_i \equiv bx_{i'} \pmod{a}$. 因为 $(a,b)=1$, 所以 $x_i \equiv x_{i'} \pmod{a}$.
又因为 $x_i, x_{i'} \in S_a$, 所以 $x_i = x_{i'}$. 同理可得 $y_j = y_{j'}$, 矛盾!

$(a,b)=1 \Rightarrow \phi(ab)=\phi(a)\phi(b)$

(ii) 再证: S_{ab} 中任一数都与 ab 互素. 任意 $bx_i+ay_j \in S_{ab}$, 因为 $(x_i,a)=1$ 且 $(a,b)=1$, 所以 $(bx_i,a)=1$, 故 $(bx_i+ay_j,a)=1$.

同理, $(bx_i+ay_j,b)=1$. 于是 $(bx_i+ay_j,ab)=1$.

$(a,b)=1 \Rightarrow \phi(ab)=\phi(a)\phi(b)$

(iii) 最后证: 任一与 ab 互素的数都与 S_{ab} 中某个数关于模 ab 同余. 假设整数 c 与 ab 互素, 即 $(c,ab)=1$. 因为 $(a,b)=1$, 所以存在 $x_0, y_0 \in \mathbb{Z}$ 使得 $bx_0+ay_0=1$. 令 $x=cx_0$, $y=cy_0$, 则有 $bx+ay=c$. 因为 $(c,ab)=1$, 所以 $(c,a)=1$, 即 $(bx+ay,a)=1$, 故 $(bx,a)=1$, 从而 $(x,a)=1$. 因此存在 $x_i \in S_a$ 使得 $x \equiv x_i \pmod{a}$.

同理, 存在 $y_j \in S_b$ 使得 $y \equiv y_j \pmod{b}$. 因此我们有 $bx \equiv bx_i \pmod{ab}$, $ay \equiv ay_j \pmod{ab}$, 所以 $bx+ay \equiv bx_i+ay_j \pmod{ab}$, 即 $c \equiv bx_i+ay_j \pmod{ab}$. 这说明与 ab 互素的数都与 S_{ab} 中某个数关于模 ab 同余.

$(a,b)=1 \Rightarrow \phi(ab)=\phi(a)\phi(b)$

(iii) 最后证: 任一与 ab 互素的数都与 S_{ab} 中某个数关于模 ab 同余. 假设整数 c 与 ab 互素, 即 $(c,ab)=1$. 因为 $(a,b)=1$, 所以存在 $x_0,y_0\in\mathbb{Z}$ 使得 $bx_0+ay_0=1$. 令 $x=cx_0$, $y=cy_0$, 则有 $bx+ay=c$. 因为 $(c,ab)=1$, 所以 $(c,a)=1$, 即 $(bx+ay,a)=1$, 故 $(bx,a)=1$, 从而 $(x,a)=1$. 因此存在 $x_i\in S_a$ 使得 $x\equiv x_i \pmod a$.

同理, 存在 $y_j\in S_b$ 使得 $y\equiv y_j \pmod b$. 因此我们有 $bx\equiv bx_i \pmod{ab}$, $ay\equiv ay_j \pmod{ab}$, 所以 $bx+ay\equiv bx_i+ay_j \pmod{ab}$, 即 $c\equiv bx_i+ay_j \pmod{ab}$. 这说明与 ab 互素的数都与 S_{ab} 中某个数关于模 ab 同余.

由 (i)–(iii) 知, S_{ab} 是 ab 的一个既约剩余系, 故 (3) 成立.

定理 3.2. 设 m 的标准分解为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, 则

$$\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}). \tag{4}$$

定理 3.2. 设 m 的标准分解为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, 则

$$\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}). \tag{4}$$

证明: 由公式 (3) 和 (2) 有

$$\phi(m) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})$$

定理 3.2. 设 m 的标准分解为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, 则

$$\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}). \tag{4}$$

证明: 由公式 (3) 和 (2) 有

$$\begin{aligned} \phi(m) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\ &= \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}) \end{aligned}$$

定理 3.2. 设 m 的标准分解为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，则

$$\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}). \tag{4}$$

证明: 由公式 (3) 和 (2) 有

$$\begin{aligned}
\phi(m) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}) \\
&= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})
\end{aligned}$$

定理 3.2. 设 m 的标准分解为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，则

$$\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}). \tag{4}$$

证明: 由公式 (3) 和 (2) 有

$$\begin{aligned}
\phi(m) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}) \\
&= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})
\end{aligned}$$

定理 3.2. 设 m 的标准分解为 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, 则

$$\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}). \qquad (4)$$

证明: 由公式 (3) 和 (2) 有

$$\begin{aligned}
\phi(m) &= \phi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \cdots \phi(p_k^{\alpha_k}) \\
&= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\
&= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}) \\
&= m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}),
\end{aligned}$$

所以定理成立. □

例如, $\phi(300) = \phi(2^2 \cdot 3 \cdot 5^2) = 300(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 80$.

由公式 (4) 稍作变形, 我们有
$\phi(m) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdots(p_k-1)$, 因此当 $m > 2$ 时, $\phi(m)$ 总是偶数.

例如, $\phi(300)=\phi(2^2\cdot 3\cdot 5^2)=300(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})=80.$

由公式 (4) 稍作变形, 我们有
$\phi(m)=p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdots(p_k-1)$, 因此当 $m>2$ 时, $\phi(m)$ 总是偶数.

有时为了紧凑, 我们也将公式 (4) 写成

$$\phi(m)=m\cdot\prod_{p|m}(1-\frac{1}{p}),$$

这里 p 是素数.

定理 3.3.

(1) 设 $(a,b)=d$, 那么 $\phi(ab)=\phi(a)\phi(b)\frac{d}{\phi(d)}$.

例如, $\phi(300)=\phi(2^2\cdot 3\cdot 5^2)=300(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})=80.$

由公式 (4) 稍作变形, 我们有
$\phi(m)=p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdots(p_k-1)$, 因此当 $m>2$ 时, $\phi(m)$ 总是偶数.

有时为了紧凑, 我们也将公式 (4) 写成

$$\phi(m)=m\cdot\prod_{p|m}(1-\frac{1}{p}),$$

这里 p 是素数.

定理 3.3.

(1) 设 $(a,b)=d$, 那么 $\phi(ab)=\phi(a)\phi(b)\frac{d}{\phi(d)}$.

(2) 如果 $a|b$, 那么 $\phi(a)|\phi(b)$.

证明: (1) 由定理3.2得

$$\frac{\phi(ab)}{ab} = \prod_{p|ab}(1-\frac{1}{p}) = \frac{\prod_{p|a}(1-\frac{1}{p})\cdot\prod_{p|b}(1-\frac{1}{p})}{\prod_{p|(a,b)}(1-\frac{1}{p})}$$

证明: (1) 由定理3.2得

$$\begin{aligned}
\frac{\phi(ab)}{ab} &= \prod_{p|ab}(1-\frac{1}{p}) = \frac{\prod_{p|a}(1-\frac{1}{p})\cdot\prod_{p|b}(1-\frac{1}{p})}{\prod_{p|(a,b)}(1-\frac{1}{p})} \\
&= \frac{\frac{\phi(a)}{a}\cdot\frac{\phi(b)}{b}}{\frac{\phi(d)}{d}} = \frac{1}{ab}\phi(a)\phi(b)\frac{d}{\phi(d)},
\end{aligned}$$

证明: (1) 由定理3.2得

$$\begin{aligned}\frac{\phi(ab)}{ab} &= \prod_{p|ab}(1-\frac{1}{p}) = \frac{\prod_{p|a}(1-\frac{1}{p})\cdot\prod_{p|b}(1-\frac{1}{p})}{\prod_{p|(a,b)}(1-\frac{1}{p})} \\ &= \frac{\frac{\phi(a)}{a}\cdot\frac{\phi(b)}{b}}{\frac{\phi(d)}{d}} = \frac{1}{ab}\phi(a)\phi(b)\frac{d}{\phi(d)},\end{aligned}$$

因此 $\phi(ab)=\phi(a)\phi(b)\frac{d}{\phi(d)}$.

证明: (1) 由定理3.2得

$$\frac{\phi(ab)}{ab} = \prod_{p|ab}(1-\frac{1}{p}) = \frac{\prod_{p|a}(1-\frac{1}{p})\cdot\prod_{p|b}(1-\frac{1}{p})}{\prod_{p|(a,b)}(1-\frac{1}{p})}$$

$$= \frac{\frac{\phi(a)}{a}\cdot\frac{\phi(b)}{b}}{\frac{\phi(d)}{d}} = \frac{1}{ab}\phi(a)\phi(b)\frac{d}{\phi(d)},$$

因此 $\phi(ab)=\phi(a)\phi(b)\frac{d}{\phi(d)}$.

(2) 设 $b=ac$, $(a,c)=e$, 则由 (1) 知

$$\frac{\phi(b)}{\phi(a)} = \frac{ac\cdot\prod_{p|ac}(1-\frac{1}{p})}{a\cdot\prod_{p|a}(1-\frac{1}{p})} = \frac{c\cdot\prod_{p|a}(1-\frac{1}{p})\cdot\prod_{p|\frac{c}{e}}(1-\frac{1}{p})}{\prod_{p|a}(1-\frac{1}{p})}$$

证明: (1) 由定理3.2得

$$\frac{\phi(ab)}{ab} = \prod_{p|ab}(1-\frac{1}{p}) = \frac{\prod_{p|a}(1-\frac{1}{p})\cdot\prod_{p|b}(1-\frac{1}{p})}{\prod_{p|(a,b)}(1-\frac{1}{p})}$$

$$= \frac{\frac{\phi(a)}{a}\cdot\frac{\phi(b)}{b}}{\frac{\phi(d)}{d}} = \frac{1}{ab}\phi(a)\phi(b)\frac{d}{\phi(d)},$$

因此 $\phi(ab)=\phi(a)\phi(b)\frac{d}{\phi(d)}$.

(2) 设 $b=ac$, $(a,c)=e$, 则由 (1) 知

$$\frac{\phi(b)}{\phi(a)} = \frac{ac\cdot\prod_{p|ac}(1-\frac{1}{p})}{a\cdot\prod_{p|a}(1-\frac{1}{p})} = \frac{c\cdot\prod_{p|a}(1-\frac{1}{p})\cdot\prod_{p|\frac{c}{e}}(1-\frac{1}{p})}{\prod_{p|a}(1-\frac{1}{p})}$$

$$= e\cdot\frac{c}{e}\cdot\prod_{p|\frac{c}{e}}(1-\frac{1}{p}) = e\cdot\phi(\frac{c}{e})\in\mathbb{Z},$$

证明: (1) 由定理3.2得

$$
\begin{aligned}
\frac{\phi(ab)}{ab} &= \prod_{p|ab}(1-\frac{1}{p}) = \frac{\prod_{p|a}(1-\frac{1}{p})\cdot\prod_{p|b}(1-\frac{1}{p})}{\prod_{p|(a,b)}(1-\frac{1}{p})} \\
&= \frac{\frac{\phi(a)}{a}\cdot\frac{\phi(b)}{b}}{\frac{\phi(d)}{d}} = \frac{1}{ab}\phi(a)\phi(b)\frac{d}{\phi(d)},
\end{aligned}
$$

因此 $\phi(ab)=\phi(a)\phi(b)\frac{d}{\phi(d)}$.

(2) 设 $b=ac$, $(a,c)=e$, 则由 (1) 知

$$
\begin{aligned}
\frac{\phi(b)}{\phi(a)} &= \frac{ac\cdot\prod_{p|ac}(1-\frac{1}{p})}{a\cdot\prod_{p|a}(1-\frac{1}{p})} = \frac{c\cdot\prod_{p|a}(1-\frac{1}{p})\cdot\prod_{p|\frac{c}{e}}(1-\frac{1}{p})}{\prod_{p|a}(1-\frac{1}{p})} \\
&= e\cdot\frac{c}{e}\cdot\prod_{p|\frac{c}{e}}(1-\frac{1}{p}) = e\cdot\phi(\frac{c}{e})\in\mathbb{Z},
\end{aligned}
$$

因此 $\phi(a)|\phi(b)$, 定理成立. □

定理 3.4. 设 m 是正整数, 则 $\sum_{d|m}\phi(d)=m$.

定理 3.4. 设 m 是正整数, 则 $\sum_{d|m}\phi(d)=m$.

证明: 考虑有理数集 $S=\{\frac{r}{m}|r=1,2,\ldots,m\}$. 设 S^* 是将 S 中每个 $\frac{r}{m}$ 化为既约分数所得的集合, 显然 S^* 中没有两个分数的值是相同的. 对任意 $1\le r\le m$, 若 $\frac{r}{m}=\frac{c}{d}$, 这里后者是既约分数, 那么

$$(c,d)=1,\ c\le d,\ d|m. \tag{5}$$

反之, 对于给定的 m, 任一满足 (5) 式中三个条件的分数 $\frac{c}{d}$ (这里 c,d 均为正整数) 均属于 S^*, 而满足 (5) 式中三个条件的分数 $\frac{c}{d}$ 的总个数为 $\sum_{d|m}\phi(d)$. 因为 $|S^*|=m$, 于是 $\sum_{d|m}\phi(d)=m$, 所以定理成立. □

定理 3.4. 设 m 是正整数, 则 $\sum_{d|m}\phi(d)=m$.

证明: 考虑有理数集 $S=\{\frac{r}{m}|r=1,2,\ldots,m\}$. 设 S^* 是将 S 中每个 $\frac{r}{m}$ 化为既约分数所得的集合, 显然 S^* 中没有两个分数的值是相同的. 对任意 $1\le r\le m$, 若 $\frac{r}{m}=\frac{c}{d}$, 这里后者是既约分数, 那么

$$(c,d)=1,\ c\le d,\ d|m. \tag{5}$$

反之, 对于给定的 m, 任一满足 (5) 式中三个条件的分数 $\frac{c}{d}$ (这里 c,d 均为正整数) 均属于 S^*, 而满足 (5) 式中三个条件的分数 $\frac{c}{d}$ 的总个数为 $\sum_{d|m}\phi(d)$. 因为 $|S^*|=m$, 于是 $\sum_{d|m}\phi(d)=m$, 所以定理成立. □

例如, $m=6$ 时,

$\sum_{d|6}\phi(d)=\phi(1)+\phi(2)+\phi(3)+\phi(6)=1+1+2+2=6.$

在数论中, 经常出现像欧拉函数这种定义在正整数集上的实值或复值函数, 这类函数称为**数论函数**.

与欧拉函数一样, 许多数论函数 f 具有如下性质: 当 $(a,b)=1$ 时, $f(ab)=f(a)f(b)$. 具有这种性质的数论函数称为**积性函数**.

下面介绍的麦比乌斯函数是另外一个重要的积性函数.

在数论中, 经常出现像欧拉函数这种定义在正整数集上的实值或复值函数, 这类函数称为**数论函数**.

与欧拉函数一样, 许多数论函数 f 具有如下性质: 当 $(a,b)=1$ 时, $f(ab)=f(a)f(b)$. 具有这种性质的数论函数称为**积性函数**.

下面介绍的麦比乌斯函数是另外一个重要的积性函数.

在定理3.4中, 我们得到了公式 $m=\sum_{d|m}\phi(d)$. 更一般地, 我们考虑公式 $f(m)=\sum_{d|m}g(d)$, 这里 f,g 是两个数论函数, 它通过函数 g 计算它的和函数 f 的值. 一个自然的问题是, 是否可以通过函数 f 方便地计算 g 的值呢?

在数论中, 经常出现像欧拉函数这种定义在正整数集上的实值或复值函数, 这类函数称为**数论函数**.

与欧拉函数一样, 许多数论函数 f 具有如下性质: 当 $(a,b)=1$ 时, $f(ab)=f(a)f(b)$. 具有这种性质的数论函数称为**积性函数**.

下面介绍的麦比乌斯函数是另外一个重要的积性函数.

在定理3.4中, 我们得到了公式 $m=\sum_{d|m}\phi(d)$. 更一般地, 我们考虑公式 $f(m)=\sum_{d|m}g(d)$, 这里 f,g 是两个数论函数, 它通过函数 g 计算它的和函数 f 的值. 一个自然的问题是, 是否可以通过函数 f 方便地计算 g 的值呢?

我们先看 m 值较小的几个实例, 由 $f(m)$ 的定义有:

$f(m) = \sum_{d|m} g(d)$

$$
\begin{aligned}
f(1) &= g(1),\\
f(2) &= g(1) + g(2),\\
f(3) &= g(1) + g(3),\\
f(4) &= g(1) + g(2) + g(4),\\
f(5) &= g(1) + g(5),\\
f(6) &= g(1) + g(2) + g(3) + g(6),\\
f(7) &= g(1) + g(7),\\
f(8) &= g(1) + g(2) + g(4) + g(8).
\end{aligned}
$$

因此我们得到

$$
\begin{aligned}
g(1) &= f(1), \\
g(2) &= f(2) - f(1), \\
g(3) &= f(3) - f(1), \\
g(4) &= f(4) - f(2), \\
g(5) &= f(5) - f(1), \\
g(6) &= f(6) - f(3) - f(2) + f(1), \\
g(7) &= f(7) - f(1), \\
g(8) &= f(8) - f(4).
\end{aligned}
$$

观察知, $g(m)$ 是一些形如 $\pm f(m/d)$ 的项之和, 其中 $d|m$.

由此, 我们猜测 $g(m)$ 可以表示为

$$g(m) = \sum_{d|m} \mu(d) f(\frac{m}{d}), \tag{6}$$

这里 μ 是一个数论函数.

由此, 我们猜测 $g(m)$ 可以表示为

$$g(m) = \sum_{d|m} \mu(d) f(\frac{m}{d}), \tag{6}$$

这里 μ 是一个数论函数.

如果 (6) 成立, 那么, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = 0$.

由此, 我们猜测 $g(m)$ 可以表示为

$$g(m) = \sum_{d|m} \mu(d) f(\frac{m}{d}), \tag{6}$$

这里 μ 是一个数论函数.

如果 (6) 成立, 那么, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = 0$.

另外, 对素数 p 有 $f(p) = g(1) + g(p)$, 即 $g(p) = f(p) - f(1)$, 因此如果 (6) 成立, 那么 $\mu(p) = -1$.

由此, 我们猜测 $g(m)$ 可以表示为

$$g(m) = \sum_{d|m} \mu(d) f(\frac{m}{d}), \tag{6}$$

这里 μ 是一个数论函数.

如果 (6) 成立, 那么, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = 0$.

另外, 对素数 p 有 $f(p) = g(1) + g(p)$, 即 $g(p) = f(p) - f(1)$, 因此如果 (6) 成立, 那么 $\mu(p) = -1$.

进一步, 当 $m = p^2$ 时, 由 $f(p^2) = g(1) + g(p) + g(p^2)$ 得, $g(p^2) = f(p^2) - f(p)$, 这蕴含 $\mu(p^2) = 0$.

由此, 我们猜测 $g(m)$ 可以表示为

$$g(m) = \sum_{d|m} \mu(d) f(\frac{m}{d}), \tag{6}$$

这里 μ 是一个数论函数.

如果 (6) 成立, 那么, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = 0$.

另外, 对素数 p 有 $f(p) = g(1) + g(p)$, 即 $g(p) = f(p) - f(1)$, 因此如果 (6) 成立, 那么 $\mu(p) = -1$.

进一步, 当 $m = p^2$ 时, 由 $f(p^2) = g(1) + g(p) + g(p^2)$ 得, $g(p^2) = f(p^2) - f(p)$, 这蕴含 $\mu(p^2) = 0$.

类似地, 不难发现, 对任意素数 p 和整数 $k \geq 2$, $\mu(p^k) = 0$.

由此, 我们猜测 $g(m)$ 可以表示为

$$g(m) = \sum_{d|m} \mu(d) f(\frac{m}{d}), \tag{6}$$

这里 μ 是一个数论函数.

如果 (6) 成立, 那么, $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = 0$.

另外, 对素数 p 有 $f(p) = g(1) + g(p)$, 即 $g(p) = f(p) - f(1)$, 因此如果 (6) 成立, 那么 $\mu(p) = -1$.

进一步, 当 $m = p^2$ 时, 由 $f(p^2) = g(1) + g(p) + g(p^2)$ 得, $g(p^2) = f(p^2) - f(p)$, 这蕴含 $\mu(p^2) = 0$.

类似地, 不难发现, 对任意素数 p 和整数 $k \geq 2$, $\mu(p^k) = 0$.

因此, 如果猜测 μ 是积性函数, 那么 μ 的值将由它在素数幂上的取值完全决定, 这种分析最终导致如下定义.

定义 3.1. 麦比乌斯函数$\mu : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ 定义为

$$\mu(m) = \begin{cases} 1 & m = 1; \\ (-1)^k & m = p_1 p_2 \cdots p_k, p_1, p_2 \ldots, p_k \text{是互不相同的素数} \\ 0 & \text{否则}. \end{cases}$$

定义 3.1. 麦比乌斯函数$\mu : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ 定义为

$$\mu(m) = \begin{cases} 1 & m = 1; \\ (-1)^k & m = p_1 p_2 \cdots p_k, p_1, p_2 \ldots, p_k \text{是互不相同的素数} \\ 0 & \text{否则}. \end{cases}$$

由定义知, 对任意正整数 m, $\mu(m)$ 的值是 0 或 ± 1. 例如, $\mu(2) = \mu(3) = -1$, $\mu(4) = 0$, $\mu(6) = 1$.

正如我们所猜测, 麦比乌斯函数的确是积性函数.

定理 3.5. 如果 $(a,b)=1$, 那么 $\mu(ab)=\mu(a)\mu(b)$.

正如我们所猜测, 麦比乌斯函数的确是积性函数.

定理 3.5. 如果 $(a,b)=1$, 那么 $\mu(ab)=\mu(a)\mu(b)$.

证明: 分情况讨论:

(1) 如果 $a=1$ 或 $b=1$, 那么因为 $\mu(1)=1$, 显然成立.

正如我们所猜测, 麦比乌斯函数的确是积性函数.

定理 3.5. 如果 $(a,b)=1$, 那么 $\mu(ab)=\mu(a)\mu(b)$.

证明: 分情况讨论:

(1) 如果 $a=1$ 或 $b=1$, 那么因为 $\mu(1)=1$, 显然成立.

(2) 如果 a 或 b 有素数平方因数, 那么 ab 必有素数平方因数. 此时, $\mu(a)=0$ 或 $\mu(b)=0$, 并且 $\mu(ab)=0$, 所以定理也成立.

正如我们所猜测, 麦比乌斯函数的确是积性函数.

定理 3.5. 如果 $(a,b)=1$, 那么 $\mu(ab)=\mu(a)\mu(b)$.

证明: 分情况讨论:

(1) 如果 $a=1$ 或 $b=1$, 那么因为 $\mu(1)=1$, 显然成立.

(2) 如果 a 或 b 有素数平方因数, 那么 ab 必有素数平方因数. 此时, $\mu(a)=0$ 或 $\mu(b)=0$, 并且 $\mu(ab)=0$, 所以定理也成立.

(3) 否则, 可假设 a 可以分解成 s 个不同的素因数之积, b 可以分解成 t 个不同的素因数之积. 因此, $\mu(a)=(-1)^s$, $\mu(b)=(-1)^t$. 因为 $(a,b)=1$, 所以 ab 可以分解成 $s+t$ 个不同的素因数之积, 于是 $\mu(ab)=(-1)^{s+t}$, 即 $\mu(ab)=\mu(a)\mu(b)$. 故定理成立. □

定理 3.6. 如果整数 $m > 1$, 那么 $\sum_{d|m} \mu(d) = 0$.

定理 3.6. 如果整数 $m>1$, 那么 $\sum_{d|m}\mu(d)=0$.

证明: 设 m 的标准分解为 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, 则

$$\begin{aligned}\sum_{d|m}\mu(d)=&\mu(1)+[\mu(p_1)+\mu(p_2)+\cdots+\mu(p_k)]\\&+[\mu(p_1p_2)+\cdots+\mu(p_{k-1}p_k)]\\&+\cdots\\&+\mu(p_1p_2\cdots p_k)\\=&1+\binom{k}{1}(-1)+\binom{k}{2}(-1)^2+\cdots+\binom{k}{k}(-1)^k\\=&(1-1)^k\\=&0,\end{aligned}$$

即 $\sum_{d|m}\mu(d)=0$. 因此定理成立. □

在给出麦比乌斯函数的定义前, 我们考虑了公式 $f(m)=\sum_{d|m} g(d)$ 中 m 取一些特殊值的情形. 一般地,

定义 3.2. 如果数论函数 f 和 g 满足

$$f(m)=\sum_{d|m} g(d),$$

则称 f 是 g 的**麦比乌斯变换**, g 是 f 的**麦比乌斯逆变换**.

在给出麦比乌斯函数的定义前，我们考虑了公式 $f(m)=\sum_{d|m} g(d)$ 中 m 取一些特殊值的情形. 一般地,

定义 3.2. 如果数论函数 f 和 g 满足

$$f(m)=\sum_{d|m} g(d),$$

则称 f 是 g 的**麦比乌斯变换**, g 是 f 的**麦比乌斯逆变换**.

若 f 是 g 的麦比乌斯变换, 则显然也有 $f(m)=\sum_{d|m} g(\frac{m}{d})$.

在给出麦比乌斯函数的定义前，我们考虑了公式 $f(m)=\sum_{d|m} g(d)$ 中 m 取一些特殊值的情形. 一般地，

定义 3.2. 如果数论函数 f 和 g 满足

$$f(m)=\sum_{d|m} g(d),$$

则称 f 是 g 的**麦比乌斯变换**，g 是 f 的**麦比乌斯逆变换**.

若 f 是 g 的麦比乌斯变换，则显然也有 $f(m)=\sum_{d|m} g(\frac{m}{d})$.

由定理3.4中 $m=\sum_{d|m}\phi(d)$ 知，将每个正整数映为自身的恒等函数是欧拉函数 ϕ 的麦比乌斯变换，而 ϕ 是该恒等函数的麦比乌斯逆变换.

若 f 是 g 的麦比乌斯变换，那么可用下面的麦比乌斯反演公式通过 f 求 g.

定理 3.7 (麦比乌斯反演公式). 如果 f 是 g 的麦比乌斯变换, 即

$$f(m)=\sum_{d|m} g(d), \tag{7}$$

则有

$$g(m)=\sum_{d|m} \mu(d) f(\frac{m}{d}). \tag{8}$$

反过来, 若 f 和 g 满足 (8) 式, 则 (7) 式也成立.

$f(m) = \sum_{d|m} g(d) \Rightarrow g(m) = \sum_{d|m} \mu(d) f(\frac{m}{d})$

若 f 和 g 满足 (7) 式, 则由定理3.6得

$$\begin{aligned}
\sum_{d|m} \mu(d) f(\frac{m}{d}) &= \sum_{d|m} \mu(d) \Big(\sum_{d'|\frac{m}{d}} g(d') \Big) \\
&= \sum_{dd'|m} \mu(d) g(d') \\
&= \sum_{d'|m} \sum_{d|\frac{m}{d'}} \mu(d) g(d') \\
&= \sum_{d'|m} g(d') \Big(\sum_{d|\frac{m}{d'}} \mu(d) \Big) \\
&= g(m)\mu(1) = g(m),
\end{aligned}$$

所以 (8) 式成立.

$$g(m)=\sum_{d|m}\mu(d)f(\tfrac{m}{d}) \Rightarrow f(m)=\sum_{d|m}g(d)$$

反过来, 假设 f 和 g 满足 (8) 式, 则类似可得

$$\begin{aligned}
\sum_{d|m} g(d) &= \sum_{d|m} g(\frac{m}{d}) = \sum_{d|m}\sum_{d'|\frac{m}{d}} \mu(d')f(\frac{m}{dd'}) \\
&= \sum_{d|m}\sum_{d'|\frac{m}{d}} \mu(\frac{m}{dd'})f(d') \\
&= \sum_{dd'|m} \mu(\frac{m}{dd'})f(d') \\
&= \sum_{d'|m} f(d')\Big(\sum_{d|\frac{m}{d'}} \mu(\frac{m}{dd'})\Big) \\
&= f(m)\mu(1) = f(m),
\end{aligned}$$

因此 (7) 式成立, 故定理成立. □

因为将每个正整数映为自身的恒等函数是欧拉函数 ϕ 的麦比乌斯变换, 所以利用麦比乌斯反演公式我们可以如下表示欧拉函数.

推论 3.1. 设整数 $m > 1$, 则 $\phi(m) = \sum_{d|m} \mu(d)\frac{m}{d}$.

证明: 由麦比乌斯反演公式即得. □

定义 4.1. 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, 其中 $a_i \in \mathbb{Z}$, 则称

$$f(x) \equiv 0 \pmod m \tag{9}$$

为模 m **的一元同余方程**. 如果 $m \nmid a_n$, 则 n 称作 (9) 的**次数**. 如果 x_0 满足 $f(x_0) \equiv 0 \pmod m$, 那么 $x \equiv x_0 \pmod m$ 称作 (9) 的**解**或**根**. 如果 (9) 的两个解关于模 m 互不同余, 那么称它们是不相同的解.

定义 4.1. 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, 其中 $a_i\in\mathbb{Z}$, 则称

$$f(x)\equiv 0 \pmod{m} \tag{9}$$

为**模 m 的一元同余方程**. 如果 $m\nmid a_n$, 则 n 称作 (9) 的**次数**. 如果 x_0 满足 $f(x_0)\equiv 0 \pmod{m}$, 那么 $x\equiv x_0 \pmod{m}$ 称作 (9) 的**解或根**. 如果 (9) 的两个解关于模 m 互不同余, 那么称它们是不相同的解.

根据定义, 将模 m 的标准剩余系中的每个元素代入 (9) 式即可确定它的所有解.
代入法是求解同余方程的基本方法, 但对于模数较大的情形, 计算量很大. 本节将讨论一次同余方程的公式解, 即讨论一个一次同余方程是否有解, 有多少个不同的解, 如何用公式给出它的所有解等问题.

我们先讨论一元一次同余方程的求解问题. 一元一次同余方程的一般形式是 $ax \equiv b \pmod{m}$, 其中 $a, b, m \in \mathbb{Z}$, $m > 0$ 且 $m \nmid a$. 我们分 $(a, m) = 1$ 和 $(a, m) > 1$ 两种情况来讨论它的解.

我们先讨论一元一次同余方程的求解问题. 一元一次同余方程的一般形式是 $ax \equiv b \pmod{m}$, 其中 $a, b, m \in \mathbb{Z}$, $m > 0$ 且 $m \nmid a$. 我们分 $(a, m) = 1$ 和 $(a, m) > 1$ 两种情况来讨论它的解.

定理 4.1. 设 $(a, m) = 1$, 那么一元一次同余方程 $ax \equiv b \pmod{m}$ 有且仅有一个解, 该解为 $x \equiv ba^{\phi(m)-1} \pmod{m}$.

我们先讨论一元一次同余方程的求解问题. 一元一次同余方程的一般形式是 $ax \equiv b \pmod{m}$, 其中 $a, b, m \in \mathbb{Z}$, $m > 0$ 且 $m \nmid a$. 我们分 $(a, m) = 1$ 和 $(a, m) > 1$ 两种情况来讨论它的解.

定理 4.1. 设 $(a, m) = 1$, 那么一元一次同余方程 $ax \equiv b \pmod{m}$ 有且仅有一个解, 该解为 $x \equiv ba^{\phi(m)-1} \pmod{m}$.

证明: 直接将 $x \equiv ba^{\phi(m)-1} \pmod{m}$ 代入同余方程验证, 由欧拉定理 $a^{\phi(m)} \equiv 1 \pmod{m}$ 知, 它显然是原同余方程的解, 这就证明了解的存在性. 关于惟一性, 假设它有两个不同的解 x_1 和 x_2, 则有 $ax_1 \equiv b \pmod{m}$ 和 $ax_2 \equiv b \pmod{m}$, 所以 $a(x_1 - x_2) \equiv 0 \pmod{m}$. 又因为 $(a, m) = 1$, 所以 $x_1 \equiv x_2 \pmod{m}$, 矛盾! □

例 4.1. 解同余方程 $3x \equiv 7 \pmod{80}$.

例 4.1. 解同余方程 $3x \equiv 7 \pmod{80}$.

解: 因为 $(3, 80) = 1$, 所以 $3x \equiv 7 \pmod{80}$ 有惟一解. 又因为

$$\phi(80) = \phi(2^4 \cdot 5) = \phi(2^4)\phi(5) = (2^4 - 2^3) \cdot 4 = 32,$$

故由定理4.1该惟一解为

$$x \equiv 7 \cdot 3^{\phi(80)-1} \equiv 7 \cdot 3^{31} \equiv 7 \cdot 3^3 \cdot (3^4)^7 \equiv 7 \cdot 3^3 \equiv 29 \pmod{80},$$

即 $x \equiv 29 \pmod{80}$. □

定理 4.2. 设 $(a, m) = d$, 那么一元一次同余方程

$$ax \equiv b \pmod{m} \tag{10}$$

有解当且仅当 $d|b$. 若方程 (10) 有解, 则恰有 d 个解:

$$x \equiv x_0 + k\frac{m}{d} \pmod{m}, \ k = 0, 1, 2, \ldots, d-1,$$

其中 x_0 是 (10) 的一个特解.

定理 4.2. 设 $(a,m)=d$, 那么一元一次同余方程

$$ax \equiv b \pmod{m} \tag{10}$$

有解当且仅当 $d|b$. 若方程 (10) 有解, 则恰有 d 个解:

$$x \equiv x_0 + k\frac{m}{d} \pmod{m},\ k=0,1,2,\dots,d-1,$$

其中 x_0 是 (10) 的一个特解.

证明: 如果方程 (10) 有解, 则由 $d|a$ 和 $d|m$ 知 $d|b$. 反过来, 假设 $d|b$. 因为 $(\frac{a}{d},\frac{m}{d})=1$, 所以由定理4.1知

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \tag{11}$$

有惟一解, 设为 $x \equiv x_0 \pmod{\frac{m}{d}}$. 易见 $x \equiv x_0 \pmod{m}$ 是 (10) 的解. 故 (10) 有解当且仅当 $d|b$.

$(10)\ ax \equiv b \pmod{m}$ $(11)\ \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

若 (10) 有解 x_0, 则由前面的结论知 $d|b$, 因此 (11) 有意义. 显然, (10) 与 (11) 等价, 也就是说 (10) 的解都是 (11) 的解, 反过来 (11) 的解也都是 (10) 的解, 这样求解 (10) 就转化为求解 (11) 了. 需要注意的是 (10) 和 (11) 的模不同, (11) 的相同的解不一定就是 (10) 的相同的解, 下面我们在 (11) 的相同的解中来求出 (10) 的所有不相同的解.

$(10)\ ax \equiv b \pmod{m}$ $(11)\ \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

假设 (11) 的惟一解为 $x \equiv x_0 \pmod{\frac{m}{d}}$, 那么所有形如 $x_0 + k\frac{m}{d}$(其中 k 是任意整数) 的数都满足 (11), 因此所有这些数中关于模 m 不同余的数就是 (10) 的所有解. 因为

$$x_0 + k_1\frac{m}{d} \equiv x_0 + k_2\frac{m}{d} \pmod{m}$$

当且仅当 $\frac{k_1-k_2}{d}m \equiv 0 \pmod{m}$, 即当且仅当 $k_1 \equiv k_2 \pmod{d}$. 因此在所有形如 $x_0 + k\frac{m}{d}$ 的数中, 只要 k 取关于模 d 不同余的数即可得到所有关于模 m 不同余的数, 于是

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}$$

就是 (10) 的所有解. 故定理成立. □

定理4.2的证明过程实际上也给出了一种求解一般一元一次同余方程的方法.

例 4.2. 解同余方程 $9x \equiv 21 \pmod{240}$.

定理4.2的证明过程实际上也给出了一种求解一般一元一次同余方程的方法.

例 4.2. 解同余方程 $9x \equiv 21 \pmod{240}$.

解: 因为 $(9, 240) = 3|21$, 所以 $9x \equiv 21 \pmod{240}$ 有 3 个解. 在例4.1中, 我们已经得到 $3x \equiv 7 \pmod{80}$ 的惟一解 $x \equiv 29 \pmod{80}$, 因此 $x \equiv 29 \pmod{240}$ 是 $9x \equiv 21 \pmod{240}$ 的一个特解, 从而它的全部解为: $x \equiv 29 \pmod{240}$, $x \equiv 29 + 80 \equiv 109 \pmod{240}$, $x \equiv 29 + 2 \cdot 80 \equiv 189 \pmod{240}$. □

定理4.2的证明过程实际上也给出了一种求解一般一元一次同余方程的方法.

例 4.2. 解同余方程 $9x \equiv 21 \pmod{240}$.

解: 因为 $(9, 240) = 3|21$, 所以 $9x \equiv 21 \pmod{240}$ 有 3 个解. 在例4.1中, 我们已经得到 $3x \equiv 7 \pmod{80}$ 的惟一解 $x \equiv 29 \pmod{80}$, 因此 $x \equiv 29 \pmod{240}$ 是 $9x \equiv 21 \pmod{240}$ 的一个特解, 从而它的全部解为: $x \equiv 29 \pmod{240}$, $x \equiv 29 + 80 \equiv 109 \pmod{240}$, $x \equiv 29 + 2 \cdot 80 \equiv 189 \pmod{240}$. □

对于多元一次同余方程 $a_1x_1 + a_2x_2 + \cdots + a_kx_k \equiv b \pmod{m}$, 用数学归纳法不难证明它有解的充要条件是 $d|b$, 这里 $d = (a_1, a_2, \ldots, a_k, m)$. 如果 $d|b$, 那么该方程恰有 $m^{k-1}d$ 个解.

在代数方程中, 两个不同的一元一次方程不可能有公共解, 因此在代数方程中不存在一元一次方程组的求解问题.

在代数方程中, 两个不同的一元一次方程不可能有公共解, 因此在代数方程中不存在一元一次方程组的求解问题.

但对于模不相同的一元一次同余方程, 这个问题是有意义的, 因为它等价于求满足不同整除条件的整数.

在代数方程中, 两个不同的一元一次方程不可能有公共解, 因此在代数方程中不存在一元一次方程组的求解问题.

但对于模不相同的一元一次同余方程, 这个问题是有意义的, 因为它等价于求满足不同整除条件的整数.

本节我们讨论一次同余方程组的求解.

例 5.1. 求最小的正整数使得它被 3 除余 2, 被 5 除余 1, 被 7 除余 6.

例 5.1. 求最小的正整数使得它被 3 除余 2, 被 5 除余 1, 被 7 除余 6.

解: 由由题意, 所求的整数即是满足下面三个同余方程的最小正整数:

$$x \equiv 2 \pmod 3 \tag{12}$$

$$x \equiv 1 \pmod 5 \tag{13}$$

$$x \equiv 6 \pmod 7 \tag{14}$$

由 (12) 式知存在 $k \in \mathbb{Z}$ 使得 $x = 3k + 2$, 将其代入 (13) 式得

$$3k + 2 \equiv 1 \pmod 5, \text{即} 3k \equiv 4 \pmod 5,$$

它有惟一解 $k \equiv 3 \pmod 5$.

(14) $x \equiv 6 \pmod 7$

于是存在 $r \in \mathbb{Z}$ 使得 $k = 5r + 3$, 所以 $x = 15r + 11$, 将其代入 (14) 式得

$$15r + 11 \equiv 6 \pmod 7, \text{即} 15r \equiv 2 \pmod 7,$$

它有惟一解 $r \equiv 2 \pmod 7$. 因此存在 $s \in \mathbb{Z}$ 使得 $r = 7s + 2$, 从而 $x = 105s + 41$. 反过来, 易见对任意 $s \in \mathbb{Z}$, $x = 105s + 41$, 即 $x \equiv 41 \pmod{105}$, 满足 (12–14) 式, 故所求的整数是 41. □

关于一般同余方程组的求解, 我们有下面的中国剩余定理, 也称为孙子定理.

定理 5.1 (中国剩余定理). 设 $m_1, m_2, \ldots, m_k$ 是 k 个两两互素的正整数, $m = m_1 m_2 \cdots\ m_k$, $M_i = m/m_i$, $1 \le i \le k$, 那么同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

有惟一解

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

其中 M_i' 满足 $M_i M_i' \equiv 1 \pmod{m_i}$.

证明: 由题设, 对任意 $1 \le i, j \le k$, 当 $i \neq j$ 时 $(m_i, m_j) = 1$, 所以有 $(M_i, m_i) = 1$, 于是存在 $M_i' \in \mathbb{Z}$ 使得 $M_i M_i' \equiv 1 \pmod{m_i}$. 因为当 $i \neq j$ 时, 显然有 $m_j | M_i$, 所以对每个 j $(1 \le j \le k)$ 有

$$\sum_{i=1}^{k} b_i M_i M_i' \equiv b_j M_j M_j' \equiv b_j \pmod{m_j},$$

因此 $x \equiv \sum_{i=1}^{k} b_i M_i M_i' \pmod{m}$ 是定理中同余方程组的解.

证明: 由题设, 对任意 $1 \le i, j \le k$, 当 $i \ne j$ 时 $(m_i, m_j) = 1$, 所以有 $(M_i, m_i) = 1$, 于是存在 $M_i' \in \mathbb{Z}$ 使得 $M_i M_i' \equiv 1 \pmod{m_i}$. 因为当 $i \ne j$ 时, 显然有 $m_j | M_i$, 所以对每个 j $(1 \le j \le k)$ 有

$$\sum_{i=1}^{k} b_i M_i M_i' \equiv b_j M_j M_j' \equiv b_j \pmod{m_j},$$

因此 $x \equiv \sum_{i=1}^{k} b_i M_i M_i' \pmod{m}$ 是定理中同余方程组的解.

下证解的惟一性. 设 x_1, x_2 都是定理中同余方程组的解, 则对所有 j $(1 \le j \le k)$ 有 $x_1 \equiv x_2 \pmod{m_j}$, 所以 $x_1 \equiv x_2 \pmod{[m_1, m_2, \ldots, m_k]}$. 因为 $m_1, m_2, \ldots, m_k$ 是两两互素的, 所以 $[m_1, m_2, \ldots, m_k] = m_1 m_2 \cdots m_k = m$, 于是有 $x_1 \equiv x_2 \pmod{m}$, 故原同余方程组只有惟一解. □

上面定理的证明中提供了同余方程组的公式解法. 下面利用这种方法求解例5.1中的同余方程组.

例 5.2. 解同余方程组

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 6 \pmod 7). \end{cases}$$

上面定理的证明中提供了同余方程组的公式解法. 下面利用这种方法求解例5.1中的同余方程组.

例 5.2. 解同余方程组

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 6 \pmod 7). \end{cases}$$

解: 我们直接用中国剩余定理求解. 这里 $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $m = 105$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$. 分别解同余方程 $35M_1' \equiv 1 \pmod 3$, $21M_2' \equiv 1 \pmod 5$, $15M_3' \equiv 1 \pmod 7$, 得 $M_1' \equiv 2 \pmod 3$, $M_2' \equiv 1 \pmod 5$, $M_3' \equiv 1 \pmod 7$. 于是同余方程组的解为

$$\begin{aligned} x &\equiv 2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 1 + 6 \cdot 15 \cdot 1 \pmod{105} \\ &\equiv 41 \pmod{105}. \end{aligned}$$

注 5.1. 设 $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 是 m 的标准分解, 那么由中国剩余定理知同余方程组

$$\begin{cases} x \equiv r_1 \pmod{p_1^{\alpha_1}} \\ x \equiv r_2 \pmod{p_2^{\alpha_2}} \\ \quad\vdots \\ x \equiv r_k \pmod{p_k^{\alpha_k}} \end{cases}$$

关于模 m 有惟一解. 因此对任意 x, $1 \leq x \leq m$, 如果知道了所有 $p_i^{\alpha_i}$ $(1 \leq i \leq k)$ 除 x 的余数 r_i, 则可惟一确定 x 的值.

下面考虑模可能不互素的情况. 由推论1.2知, 当 $(m, n) = 1$, 同余方程

$$x \equiv b \pmod{mn}$$

的解是同余方程组

$$\begin{cases} x \equiv b \pmod{m} \\ x \equiv b \pmod{n}. \end{cases}$$

的解, 反过来也成立. 因此模不互素的同余方程组也可以用中国剩余定理来求解.

下面考虑模可能不互素的情况. 由推论1.2知, 当 $(m,n)=1$, 同余方程

$$x \equiv b \pmod{mn}$$

的解是同余方程组

$$\begin{cases} x \equiv b \pmod{m} \\ x \equiv b \pmod{n}. \end{cases}$$

的解, 反过来也成立. 因此模不互素的同余方程组也可以用中国剩余定理来求解.

先看一个例子.

例 5.3. 试解同余方程组

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{12}. \end{cases}$$

解: 因为 $12 = 3 \cdot 4$, 所以原同余方程组与下面的同余方程组同解:

$$\begin{cases} x \equiv 3 & \pmod 8 \\ x \equiv 7 \equiv 1 & \pmod 3 \\ x \equiv 7 \equiv 3 & \pmod 4. \end{cases}$$

因为 $x \equiv 3 \pmod 8$ 蕴含 $x \equiv 3 \pmod 4$, 所以原同余方程组等价于

$$\begin{cases} x \equiv 3 \pmod 8 \\ x \equiv 1 \pmod 3. \end{cases}$$

因为 $(3, 8) = 1$, 所以由中国剩余定理可得解为 $x \equiv 19 \pmod{24}$. $\square$

下面的例子表明, 模不互素时同余方程组未必有解.

例 5.4. 试解同余方程组

$$\begin{cases} x \equiv 5 \pmod{8} \\ x \equiv 7 \pmod{12}. \end{cases}$$

下面的例子表明, 模不互素时同余方程组未必有解.

例 5.4. 试解同余方程组

$$\begin{cases} x \equiv 5 \pmod 8 \\ x \equiv 7 \pmod{12}. \end{cases}$$

解: 原同余方程组与下面的同余方程组同解:

$$\begin{cases} x \equiv 5 & \pmod 8 \\ x \equiv 7 \equiv 1 & \pmod 3 \\ x \equiv 7 \equiv 3 & \pmod 4. \end{cases}$$

因为 $x \equiv 5 \pmod 8$ 与 $x \equiv 3 \pmod 4$ 没有公共解, 所以原同余方程组无解. □

下面给出模可能不互素的同余方程组有解的充要条件.

定理 5.2. 同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2}. \end{cases} \tag{15}$$

有解的充要条件是 $(m_1, m_2) | b_1 - b_2$. 如果 (15) 有解, 那么 (15) 关于模 $[m_1, m_2]$ 只有惟一解.

下面给出模可能不互素的同余方程组有解的充要条件.

定理 5.2. 同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2}. \end{cases} \tag{15}$$

有解的充要条件是 $(m_1, m_2) | b_1 - b_2$. 如果 (15) 有解, 那么 (15) 关于模 $[m_1, m_2]$ 只有惟一解.

证明: 先证必要性. 设 x_0 是同余方程组 (15) 的一个解, 则有 $x_0 \equiv b_1 \pmod{m_1}$ 和 $x_0 \equiv b_2 \pmod{m_2}$, 所以 $x_0 \equiv b_1 \pmod{(m_1, m_2)}$, $x_0 \equiv b_2 \pmod{(m_1, m_2)}$, 于是有 $b_1 \equiv b_2 \pmod{(m_1, m_2)}$, 即 $(m_1, m_2) | b_1 - b_2$.

下证充分性. 设 $(m_1, m_2)|b_1 - b_2$, 则由定理4.2知同余方程

$$m_2 y \equiv b_1 - b_2 \pmod{m_1}$$

有解, 设为 t. 于是下面两式成立:

$$m_2 t + b_2 \equiv b_1 \pmod{m_1}, \qquad m_2 t + b_2 \equiv b_2 \pmod{m_2},$$

这说明 $m_2 t + b_2$ 是 (15) 的一个解.

下证充分性. 设 $(m_1, m_2) | b_1 - b_2$, 则由定理4.2知同余方程

$$m_2 y \equiv b_1 - b_2 \pmod{m_1}$$

有解, 设为 t. 于是下面两式成立:

$$m_2 t + b_2 \equiv b_1 \pmod{m_1}, \qquad m_2 t + b_2 \equiv b_2 \pmod{m_2},$$

这说明 $m_2 t + b_2$ 是 (15) 的一个解.

最后证明解的惟一性. 设 x_1, x_2 都是 (15) 的解, 那么显然有

$$x_1 \equiv x_2 \pmod{m_1}, \qquad x_1 \equiv x_2 \pmod{m_2},$$

所以 $x_1 - x_2$ 是 m_1, m_2 的公倍数, 故 $[m_1, m_2] | x_1 - x_2$, 即 $x_1 \equiv x_2 \pmod{[m_1, m_2]}$. 因此 (15) 关于模 $[m_1, m_2]$ 只有惟一解. □

中国剩余定理可以作如下推广: 对于一般的同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv b_k \pmod{m_k}, \end{cases} \tag{16}$$

不难证明它有解的充要条件是对任意 $1 \le i, j \le k$, 都有 $(m_i, m_j) | b_i - b_j$. 并且可以证明, 如果 (16) 有解, 那么它的解关于模 $[m_1, m_2, \ldots, m_k]$ 是惟一的.

考虑模 p 的一元 n 次同余方程

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod p, \quad (17)$$

这里 p 是素数且 $p \nmid a_n$.

如果要求它的解, 只需把 p 的完全剩余系中的数一一代入即可求出所有解.

当然, 当 p 和 n 太大时, 代入验算的计算量比较大, 但是除此之外, 我们还没有一般的简便方法 (在第 4 章中, 我们将深入讨论模 p 的一元二次同余方程).

考虑模 p 的一元 n 次同余方程

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0 \pmod p, \quad (17)$$

这里 p 是素数且 $p\nmid a_n$.

如果要求它的解, 只需把 p 的完全剩余系中的数一一代入即可求出所有解.

当然, 当 p 和 n 太大时, 代入验算的计算量比较大, 但是除此之外, 我们还没有一般的简便方法 (在第 4 章中, 我们将深入讨论模 p 的一元二次同余方程).

尽管如此, 我们可以采用下面的方法适当降低某些同余方程的计算困难.

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

首先, 由同余的性质知, 如果方程 (17) 中 $f(x)$ 的某个系数的绝对值大于或等于 p, 那么可以把该系数化为与之同余但绝对值小于 p 的数.

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

首先, 由同余的性质知, 如果方程 (17) 中 $f(x)$ 的某个系数的绝对值大于或等于 p, 那么可以把该系数化为与之同余但绝对值小于 p 的数.

再如果 $f(x)$ 的次数 $n \geq p$, 那么可以利用费马小定理 $x^p \equiv x \pmod{p}$ 将 $f(x)$ 化为次数小于 p 且与之同余的方程 $r(x)$, 即 $f(x) \equiv r(x) \pmod{p}$, 显然 $f(x)$ 的解和 $r(x)$ 的解是一致的. 因此解 (17) 转化为解 $r(x) \equiv 0 \pmod{p}$, 因为 $r(x)$ 的次数比 $f(x)$ 的低, 所以计算比较简便.

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

又如果 $f(x)$ 可以分解成一些因式之积, 不妨设 $f(x) \equiv g_1(x) g_2(x) \pmod{p}$, 即 $g_i(x)$, $i = 1, 2$, 是 $f(x)$ 关于模 p 的因式, 那么解 (17) 就转化为解同余方程

$$g_1(x) \equiv 0 \pmod{p} \text{ 和 } g_2(x) \equiv 0 \pmod{p}.$$

因为 $g_1(x)$ 和 $g_2(x)$ 的次数都比 $f(x)$ 低, 因此较容易计算.

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$$

又如果 $f(x)$ 可以分解成一些因式之积, 不妨设 $f(x) \equiv g_1(x) g_2(x) \pmod{p}$, 即 $g_i(x)$, $i = 1, 2$, 是 $f(x)$ 关于模 p 的因式, 那么解 (17) 就转化为解同余方程

$$g_1(x) \equiv 0 \pmod{p} \quad \text{和} \quad g_2(x) \equiv 0 \pmod{p}.$$

因为 $g_1(x)$ 和 $g_2(x)$ 的次数都比 $f(x)$ 低, 因此较容易计算.

另外, 如果我们知道了 (17) 的一个解 $x \equiv a \pmod{p}$, 那么由 $f(x) = (x-a)g(x) + r$ 我们有 $r \equiv 0 \pmod{p}$, 因此 $f(x) \equiv (x-a)g(x) \pmod{p}$, 即 $x - a$ 是 $f(x)$ 关于模 p 的因式. 于是只要解出了 $g(x) \equiv 0 \pmod{p}$, 便可得到 (17) 的解.

例 6.1. 解同余方程 $f(x) = 6x^7 + 3x^6 - 7x^5 + x + 2 \equiv 0 \pmod 5$.

例 6.1. 解同余方程 $f(x) = 6x^7 + 3x^6 - 7x^5 + x + 2 \equiv 0 \pmod 5$.

解: 用上面介绍的方法简化该同余方程得

$$f(x) \equiv x^3 + 3x^2 - x + 2 \equiv 0 \pmod 5.$$

将模 5 的完全剩余系中的数 $0, 1, 2, 3, 4$ 代入验算, 即知它有 3 个解:

$$x \equiv 1, 2, 4 \pmod 5,$$

因此同余方程 $f(x) \equiv 0 \pmod 5$ 的解为 $x \equiv 1, 2, 4 \pmod 5$. □

下面的定理给出同余方程解的个数的上界.

定理 6.1 (拉格朗日定理). 设 p 是素数且 $p \nmid a_n$, 则

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}, \tag{18}$$

至多有 n 个解.

下面的定理给出同余方程解的个数的上界.

定理 6.1 (拉格朗日定理). 设 p 是素数且 $p \nmid a_n$, 则

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}, \quad (18)$$

至多有 n 个解.

证明: 我们对 $f(x)$ 的次数 n 进行归纳证明. 当 $n = 1$ 时, 有 $f(x) = a_1 x + a_0 \equiv 0 \pmod{p}$, 此时 $p \nmid a_1$. 因此 $(a_1, p) = 1$, 所以由定理4.1知 $f(x) \equiv 0 \pmod{p}$ 有惟一解.

下面的定理给出同余方程解的个数的上界.

定理 6.1 (拉格朗日定理). 设 p 是素数且 $p \nmid a_n$, 则

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}, \quad (18)$$

至多有 n 个解.

证明: 我们对 $f(x)$ 的次数 n 进行归纳证明. 当 $n = 1$ 时, 有 $f(x) = a_1 x + a_0 \equiv 0 \pmod{p}$, 此时 $p \nmid a_1$. 因此 $(a_1, p) = 1$, 所以由定理4.1知 $f(x) \equiv 0 \pmod{p}$ 有惟一解.

假设定理对 $n-1$ $(n \geq 2)$ 为真, 下证 n 的情形.

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod p$$

当 $n \geq p$ 时, (18) 至多只有 p 个解, 定理显然成立.

$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod p$

当 $n \geq p$ 时, (18) 至多只有 p 个解, 定理显然成立.若 $n < p$, 利用反证法假设 (18) 至少有 $n+1$ 个解, 不失一般性我们假设 (18) 有 $n+1$ 个解 $x_0, x_1, \ldots, x_n$, 其中对任意 $0 \leq i < j \leq n$, 都有 $x_i \not\equiv x_j \pmod p$. 令 $F(x) = f(x) - f(x_0)$, 则有

$$F(x) = \sum_{i=1}^{n} a_i(x^i - x_0^i) = (x - x_0)g(x),$$

这里 $g(x)$ 是首项系数为 a_n 的 $n-1$ 次整系数多项式. 因为对任意 $1 \leq j \leq n$, $F(x_j) \equiv 0 \pmod p$, 即 $(x_j - x_0)g(x_j) \equiv 0 \pmod p$, 又因为当 $1 \leq j \leq n$ 时 $x_0 \not\equiv x_j \pmod p$, 所以当 $1 \leq j \leq n$ 时都有 $g(x_j) \equiv 0 \pmod p$. 故 $n-1$ 次同余方程 $g(x) \equiv 0 \pmod p$ 有 n 个解, 矛盾! □

值得注意的是, 同余方程 (18) 不一定有解, 即使有解, 解的个数也不一致, 拉格朗日定理仅仅是给出了解的个数的最好上限.

例 6.2.

(1) $x^3 \equiv 8 \pmod{13}$ 有 3 个解: $x \equiv 1, 5, 6 \pmod{13}$.

值得注意的是, 同余方程 (18) 不一定有解, 即使有解, 解的个数也不一致, 拉格朗日定理仅仅是给出了解的个数的最好上限.

例 6.2.

(1) $x^3 \equiv 8 \pmod{13}$ 有 3 个解: $x \equiv 1, 5, 6 \pmod{13}$.

(2) $x^2 + 3x + 4 \equiv 0 \pmod 7$ 仅有 1 个解: $x \equiv 2 \pmod 7$.

值得注意的是, 同余方程 (18) 不一定有解, 即使有解, 解的个数也不一致, 拉格朗日定理仅仅是给出了解的个数的最好上限.

例 6.2.

(1) $x^3 \equiv 8 \pmod{13}$ 有 3 个解: $x \equiv 1, 5, 6 \pmod{13}$.

(2) $x^2 + 3x + 4 \equiv 0 \pmod 7$ 仅有 1 个解: $x \equiv 2 \pmod 7$.

(3) $x^3 + 4x^2 + x + 1 \equiv 0 \pmod 5$ 没有解.

值得注意的是, 同余方程 (18) 不一定有解, 即使有解, 解的个数也不一致, 拉格朗日定理仅仅是给出了解的个数的最好上限.

例 6.2.

(1) $x^3 \equiv 8 \pmod{13}$ 有 3 个解: $x \equiv 1, 5, 6 \pmod{13}$.

(2) $x^2 + 3x + 4 \equiv 0 \pmod{7}$ 仅有 1 个解: $x \equiv 2 \pmod{7}$.

(3) $x^3 + 4x^2 + x + 1 \equiv 0 \pmod{5}$ 没有解.

值得注意的是, 同余方程 (18) 不一定有解, 即使有解, 解的个数也不一致, 拉格朗日定理仅仅是给出了解的个数的最好上限.

例 6.2.

(1) $x^3 \equiv 8 \pmod{13}$ 有 3 个解: $x \equiv 1, 5, 6 \pmod{13}$.

(2) $x^2 + 3x + 4 \equiv 0 \pmod{7}$ 仅有 1 个解: $x \equiv 2 \pmod{7}$.

(3) $x^3 + 4x^2 + x + 1 \equiv 0 \pmod{5}$ 没有解.

另外需要注意的是, 拉格朗日定理只有在模为素数时才成立. 例如, 3 次同余方程 $x^3 - x \equiv 0 \pmod{6}$ 有 6 个解: $x \equiv 0, 1, 2, 3, 4, 5 \pmod{6}$.

下面是拉格朗日定理的两个推论.

推论 6.1. 设 p 是素数, 如果同余方程

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p},$$

的解的个数大于 n, 那么对每个 $0 \le i \le n$, 都有 $p | a_i$.

下面是拉格朗日定理的两个推论.

推论 6.1. 设 p 是素数, 如果同余方程

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p},$$

的解的个数大于 n, 那么对每个 $0 \le i \le n$, 都有 $p | a_i$.

推论 6.2. 设 p 是素数, $d|p-1$, 则 $x^d \equiv 1 \pmod p$ 恰有 d 个解.

推论 6.2. 设 p 是素数, $d|p-1$, 则 $x^d \equiv 1 \pmod p$ 恰有 d 个解.

下面给出 n 次同余方程有 n 个不同解的充要条件.

定理 6.2. 设 p 是素数, $n < p$, 且 $p \nmid a_n$, 则同余方程

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p},$$

有 n 个不同的解当且仅当 $f(x)$ 是 $x^p - x$ 关于模 p 的因式.

下面给出 n 次同余方程有 n 个不同解的充要条件.

定理 6.2. 设 p 是素数, $n < p$, 且 $p \nmid a_n$, 则同余方程

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p},$$

有 n 个不同的解当且仅当 $f(x)$ 是 $x^p - x$ 关于模 p 的因式.

根据欧拉函数的定义, 我们知道 p 是素数当且仅当 $\phi(p) = p - 1$. 下面定理给出一个数是素数的另一充要条件.

定理 6.3 (威尔逊定理). 设 p 是大于 1 的正整数, 则 p 是素数当且仅当 $(p-1)! \equiv -1 \pmod{p}$.

根据欧拉函数的定义, 我们知道 p 是素数当且仅当 $\phi(p) = p - 1$. 下面定理给出一个数是素数的另一充要条件.

定理 6.3 (威尔逊定理). 设 p 是大于 1 的正整数, 则 p 是素数当且仅当 $(p-1)! \equiv -1 \pmod p$.

证明: (充分性) 假设 p 不是素数, 则 p 必有小于 p 的素因数, 设为 q. 因此有 $(p-1)! \equiv 0 \pmod q$, 从而 $(p-1)! \not\equiv -1 \pmod q$. 但由 $(p-1)! \equiv -1 \pmod p$ 知 $(p-1)! \equiv -1 \pmod q$, 矛盾! 故当 $(p-1)! \equiv -1 \pmod p$ 时 p 必为素数.

根据欧拉函数的定义, 我们知道 p 是素数当且仅当 $\phi(p) = p - 1$. 下面定理给出一个数是素数的另一充要条件.

定理 6.3 (威尔逊定理). 设 p 是大于 1 的正整数, 则 p 是素数当且仅当 $(p-1)! \equiv -1 \pmod{p}$.

证明: (充分性) 假设 p 不是素数, 则 p 必有小于 p 的素因数, 设为 q. 因此有 $(p-1)! \equiv 0 \pmod{q}$, 从而 $(p-1)! \not\equiv -1 \pmod{q}$. 但由 $(p-1)! \equiv -1 \pmod{p}$ 知 $(p-1)! \equiv -1 \pmod{q}$, 矛盾! 故当 $(p-1)! \equiv -1 \pmod{p}$ 时 p 必为素数.

(必要性) 设 p 是素数, 则由费马小定理知 $x \equiv 1, 2, \ldots p-1 \pmod{p}$ 都是 $x^{p-1} - 1 \equiv 0 \pmod{p}$ 的解, 所以有 $x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \pmod{p}$. 令 $x = p$ 得 $-1 \equiv (p-1)! \pmod{p}$, 故定理成立. $\square$

本节讨论模为合数的高次同余方程的解法, 其基本思想是利用下面的定理将合数模转化为素数模来处理.

定理 7.1. 设 $m_1, m_2, \ldots, m_k$ 是 k 个两两互素的正整数, $m = m_1 m_2 \cdots m_k$, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, 那么

$$f(x) \equiv 0 \pmod{m} \tag{19}$$

有解的充要条件是同余方程组

$$\begin{cases} f(x) \equiv 0 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \\ \qquad \vdots \\ f(x) \equiv 0 \pmod{m_k}. \end{cases} \tag{20}$$

有解. 如果 (20) 中 $f(x) \equiv 0 \pmod{m_i}$ $(i = 1, 2, \ldots, k)$ 有 n_i 个解, 那么 (19) 有 $\prod_{i=1}^{k} n_i$ 个解.

证明： 定理中充要条件的证明是显然的. 我们仅仅证明后半部分. 设 $f(x) \equiv 0 \pmod{m_i}$ $(i = 1, 2, \ldots, k)$ 的 n_i 个不同的解为 $x \equiv x_{i1} \pmod{m_i}$, $x \equiv x_{i2} \pmod{m_i}$, $\ldots$, $x \equiv x_{in_i} \pmod{m_i}$.

当 i 跑遍 $1, 2, \ldots, k$ 时, 对其中任一组

$$\begin{cases} x \equiv x_{1j_1} \pmod{m_1} \\ x \equiv x_{2j_2} \pmod{m_2} \\ \quad\vdots \\ x \equiv x_{kj_k} \pmod{m_k}, \end{cases} \tag{21}$$

由中国剩余定理 (21) 有惟一解 $x \equiv x_0 \pmod{m}$, 显然它是 (19) 的解, 并且容易验证, 上述 $x_{1j_1}, x_{2j_2}, \ldots, x_{kj_k}$ 的不同选取给出 (19) 的不同解. 因为 $x_{1j_1}, x_{2j_2}, \ldots, x_{kj_k}$ 的取法有 $\prod_{i=1}^{k} n_i$ 种, 所以 (19) 至少有 $\prod_{i=1}^{k} n_i$ 个解.

反过来, 设 $x \equiv x_0 \pmod{m}$ 是 (19) 的任意一个解, 即 $f(x_0) \equiv 0 \pmod{m}$, 那么必然有 $f(x_0) \equiv 0 \pmod{m_i}$ $(i = 1, 2, \ldots, k)$, 因此 x_0 应与 $f(x) \equiv 0 \pmod{m_i}$ 的 n_i 个解中的某个关于模 m_i 同余, 即存在一组 $x_{1j_1}, x_{2j_2}, \ldots, x_{kj_k}$ 使得 x_0 满足 (21), 这表明 (19) 的每个解都产生于某个形如 (21) 的同余方程组. 故 (19) 的解得个数不大于 $\prod_{i=1}^{k} n_i$.

综上, (19) 有 $\prod_{i=1}^{k} n_i$ 个解. □

例 7.1. 求平方与自身最后三位数字 (不足部分以 0 补充) 相同的所有整数.

例 7.1. 求平方与自身最后三位数字 (不足部分以 0 补充) 相同的所有整数.

解: 由题意, 我们只需求 $x^2 \equiv x \pmod{1000}$ 的解即可. 因为 $1000 = 2^3 \cdot 5^3$, 所以由定理7.1的证明知, 可以先分别求出 $x^2 \equiv x \pmod{2^3}$ 和 $x^2 \equiv x \pmod{5^3}$ 的解. 前者的解为 $x \equiv 0, 1 \pmod{2^3}$, 后者的解为 $x \equiv 0, 1 \pmod{5^3}$, 它们产生 4 个不同的同余方程组:

$$\begin{cases} x \equiv 0 \pmod{2^3} \\ x \equiv 0 \pmod{5^3}, \end{cases} \quad \begin{cases} x \equiv 1 \pmod{2^3} \\ x \equiv 1 \pmod{5^3}, \end{cases}$$

$$\begin{cases} x \equiv 1 \pmod{2^3} \\ x \equiv 0 \pmod{5^3}, \end{cases} \quad \begin{cases} x \equiv 0 \pmod{2^3} \\ x \equiv 1 \pmod{5^3}. \end{cases}$$

从而由中国剩余定理可求得

$x \equiv 0, 1, 376, 625 \pmod{1000}$. □

一般地, 由定理7.1及其证明知, 如果 m 的标准分解为 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, 那么解

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0 \pmod m$$

转化为先解

$$f(x)\equiv 0 \pmod{p_i^{\alpha_i}}\ (i=1,2\ldots,k),$$

再利用中国剩余定理求解这些解的组合构成的同余方程组. 因此求解模为合数的同余方程的关键是求解形如

$$f(x)\equiv 0 \pmod{p^\alpha} \tag{22}$$

的同余方程, 这里 p 是素数.

$\alpha=1$ 的情形在前一节已经讨论, 下面主要关心 $\alpha\geq 2$ 的情况.

我们先比较 (22) 和同余方程

$$f(x) \equiv 0 \pmod{p^{\alpha+1}} \tag{23}$$

的解, 这里 $\alpha \geq 1$.

显然 (23) 的解一定是 (22) 的解, 但反过来未必成立.

例如 $f(x) = x$, $p = 2$, $\alpha = 1$ 时, 2 是 $f(x) \equiv 0 \pmod 2$ 的解, 但 2 不是 $f(x) \equiv 0 \pmod{2^2}$ 的解.

我们先比较 (22) 和同余方程

$$f(x) \equiv 0 \pmod{p^{\alpha+1}} \tag{23}$$

的解, 这里 $\alpha \geq 1$.

显然 (23) 的解一定是 (22) 的解, 但反过来未必成立.

例如 $f(x) = x$, $p = 2$, $\alpha = 1$ 时, 2 是 $f(x) \equiv 0 \pmod 2$ 的解, 但 2 不是 $f(x) \equiv 0 \pmod{2^2}$ 的解.

尽管如此, 我们可以在 (22) 的解中寻找 (23) 的解. 观察知, 如果 (22) 的解 $x \equiv x_0 \pmod{p^\alpha}$ 给出 (23) 的一个解 $x \equiv x_0' \pmod{p^{\alpha+1}}$, 那么必有 $x_0' \equiv x_0 \pmod{p^\alpha}$.

我们先看看当 $\alpha = 1$ 时如何在 (22) 的解中寻找 (23) 的解.

设 $x \equiv x_0 \pmod{p}$ 是 $f(x) \equiv 0 \pmod{p}$ 的解, 如果它能给出 $f(x) \equiv 0 \pmod{p^2}$ 的一个解, 那么必然存在 $k \in \mathbb{Z}$ 使得 $x \equiv x_0 + kp \pmod{p^2}$ 是 $f(x) \equiv 0 \pmod{p^2}$ 的解.

我们先看看当 $\alpha = 1$ 时如何在 (22) 的解中寻找 (23) 的解.

设 $x \equiv x_0 \pmod{p}$ 是 $f(x) \equiv 0 \pmod{p}$ 的解, 如果它能给出 $f(x) \equiv 0 \pmod{p^2}$ 的一个解, 那么必然存在 $k \in \mathbb{Z}$ 使得 $x \equiv x_0 + kp \pmod{p^2}$ 是 $f(x) \equiv 0 \pmod{p^2}$ 的解.

因此对于给定的 x_0, 我们只要求出对应的 k 即可. 如果这样的 k 不存在, 那么表明原来的 x_0 不能给出 $f(x) \equiv 0 \pmod{p^2}$ 的解.

为了求 k, 我们令
$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$, 因此有

$$\begin{aligned} f(x+y) &= a_n(x+y)^n + a_{n-1}(x+y)^{n-1} + \cdots + a_1(x+y) + a_0 \\ &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) + \\ &\quad (na_n x^{n-1} y + (n-1)a_{n-1}x^{n-2}y + \cdots + a_1 y) + \cdots \\ &= f(x) + yf'(x) + y^2 g(x,y), \end{aligned}$$

其中 $g(x,y)$ 是关于 x, y 的某个整系数多项式, 于是
$f(x_0+kp) = f(x_0) + kpf'(x_0) + k^2p^2 g(x_0, kp) \equiv f(x_0) + kpf'(x_0) \pmod{p^2}$. 因为 $f(x_0) \equiv 0 \pmod{p}$, $f(x_0+kp) \equiv 0 \pmod{p^2}$, 所以用 p 除上面式子得 $kf'(x_0) \equiv -\frac{f(x_0)}{p} \pmod{p}$, 这是一个关于 k 的一元一次同余方程, 可求出 k, 进而可求得 $f(x) \equiv 0 \pmod{p^2}$ 的解.

利用同样的思想, 我们可以对任意 $\alpha\ (\geq 1)$, 在 $f(x) \equiv 0 \pmod{p^\alpha}$ 的解中寻找 $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 的解.

利用同样的思想, 我们可以对任意 $\alpha\ (\geq 1)$, 在 $f(x) \equiv 0 \pmod{p^\alpha}$ 的解中寻找 $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 的解.

定理 7.2. 设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$, x_0 是 $f(x) \equiv 0 \pmod{p^\alpha}$ 的一个解.

(1) 如果 $p \nmid f'(x_0)$, 那么 $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 恰好有一个解 $x \equiv x_0 + kp^\alpha \pmod{p^{\alpha+1}}$, 其中 k 是 $f'(x_0)k \equiv -\frac{f(x_0)}{p^\alpha} \pmod{p}$ 的惟一解.

利用同样的思想, 我们可以对任意 $\alpha\ (\geq 1)$, 在 $f(x) \equiv 0 \pmod{p^\alpha}$ 的解中寻找 $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 的解.

定理 7.2. 设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$, x_0 是 $f(x) \equiv 0 \pmod{p^\alpha}$ 的一个解.

(1) 如果 $p \nmid f'(x_0)$, 那么 $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 恰好有一个解 $x \equiv x_0 + kp^\alpha \pmod{p^{\alpha+1}}$, 其中 k 是 $f'(x_0)k \equiv -\frac{f(x_0)}{p^\alpha} \pmod{p}$ 的惟一解.

(2) 如果 $p | f'(x_0)$, $p^{\alpha+1} | f(x_0)$, 那么 $f(x) \equiv 0 \pmod{p^{\alpha+1}}$ 有 p 个解: $x \equiv x_0 + kp^\alpha \pmod{p^{\alpha+1}}$, 其中 $k = 0, 1, \ldots, p-1$.

利用同样的思想, 我们可以对任意 $\alpha\ (\geq 1)$, 在 $f(x)\equiv 0 \pmod{p^\alpha}$ 的解中寻找 $f(x)\equiv 0 \pmod{p^{\alpha+1}}$ 的解.

定理 7.2. 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, $f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1$, x_0 是 $f(x)\equiv 0 \pmod{p^\alpha}$ 的一个解.

(1) 如果 $p\nmid f'(x_0)$, 那么 $f(x)\equiv 0 \pmod{p^{\alpha+1}}$ 恰好有一个解 $x\equiv x_0+kp^\alpha \pmod{p^{\alpha+1}}$, 其中 k 是 $f'(x_0)k\equiv -\frac{f(x_0)}{p^\alpha} \pmod{p}$ 的惟一解.

(2) 如果 $p|f'(x_0)$, $p^{\alpha+1}|f(x_0)$, 那么 $f(x)\equiv 0 \pmod{p^{\alpha+1}}$ 有 p 个解: $x\equiv x_0+kp^\alpha \pmod{p^{\alpha+1}}$, 其中 $k=0,1,\ldots,p-1$.

(3) 如果 $p|f'(x_0)$, $p^{\alpha+1}\nmid f(x_0)$, 那么 $f(x)\equiv 0 \pmod{p^{\alpha+1}}$ 没有解 x 满足 $x\equiv x_0 \pmod{p^\alpha}$.

例 7.2. 解同余方程 $x^3 + 8x^2 - x - 1 \equiv 0 \pmod{11^2}$.

例 7.2. 解同余方程 $x^3+8x^2-x-1\equiv 0 \pmod{11^2}$.

解: 令 $f(x)=x^3+8x^2-x-1$, 则 $f'(x)=3x^2+16x-1$. 解 $f(x)\equiv 0 \pmod{11}$ 得 $x_1\equiv 4 \pmod{11}$, $x_2\equiv 5 \pmod{11}$.

(1) 当 $x_1\equiv 4 \pmod{11}$ 时, $f(4)=187$, $f'(4)=111\equiv 1 \pmod{11}$. 因为 $p=11\nmid f'(4)$, 所以由定理7.2(1) 知 $f(x)\equiv 0 \pmod{11^2}$ 有惟一解 $x\equiv x_1+kp\equiv 4+11k \pmod{11^2}$, 其中 k 是 $f'(4)k\equiv -\frac{f(4)}{11} \pmod{11}$ 的惟一解, 即 $k\equiv -\frac{187}{11}\equiv 5 \pmod{11}$. 故 $x\equiv 4+11\cdot 5\equiv 59 \pmod{11^2}$ 是 $f(x)\equiv 0 \pmod{11^2}$ 的一个解.

例 7.2. 解同余方程 $x^3+8x^2-x-1\equiv 0 \pmod{11^2}$.

解: 令 $f(x)=x^3+8x^2-x-1$, 则 $f'(x)=3x^2+16x-1$. 解 $f(x)\equiv 0 \pmod{11}$ 得 $x_1\equiv 4 \pmod{11}$, $x_2\equiv 5 \pmod{11}$.

(1) 当 $x_1\equiv 4 \pmod{11}$ 时, $f(4)=187$, $f'(4)=111\equiv 1 \pmod{11}$. 因为 $p=11\nmid f'(4)$, 所以由定理7.2(1) 知 $f(x)\equiv 0 \pmod{11^2}$ 有惟一解 $x\equiv x_1+kp\equiv 4+11k \pmod{11^2}$, 其中 k 是 $f'(4)k\equiv -\frac{f(4)}{11} \pmod{11}$ 的惟一解, 即 $k\equiv -\frac{187}{11}\equiv 5 \pmod{11}$. 故 $x\equiv 4+11\cdot 5\equiv 59 \pmod{11^2}$ 是 $f(x)\equiv 0 \pmod{11^2}$ 的一个解.

(2) 当 $x_2\equiv 5 \pmod{11}$ 时, $f(5)=319$, $f'(5)=154\equiv 0 \pmod{11}$. 因为 $p=11\nmid f'(5)$, 但是 $11^2\nmid f'(5)$, 所以由定理7.2(3) 知 $f(x)\equiv 0 \pmod{11^2}$ 没有关于模 11 同余于 5 的解.

例 7.2. 解同余方程 $x^3+8x^2-x-1\equiv 0 \pmod{11^2}$.

解: 令 $f(x)=x^3+8x^2-x-1$, 则 $f'(x)=3x^2+16x-1$. 解 $f(x)\equiv 0 \pmod{11}$ 得 $x_1\equiv 4 \pmod{11}$, $x_2\equiv 5 \pmod{11}$.

(1) 当 $x_1\equiv 4 \pmod{11}$ 时, $f(4)=187$, $f'(4)=111\equiv 1 \pmod{11}$. 因为 $p=11\nmid f'(4)$, 所以由定理7.2(1) 知 $f(x)\equiv 0 \pmod{11^2}$ 有惟一解 $x\equiv x_1+kp\equiv 4+11k \pmod{11^2}$, 其中 k 是 $f'(4)k\equiv -\frac{f(4)}{11} \pmod{11}$ 的惟一解, 即 $k\equiv -\frac{187}{11}\equiv 5 \pmod{11}$. 故 $x\equiv 4+11\cdot 5\equiv 59 \pmod{11^2}$ 是 $f(x)\equiv 0 \pmod{11^2}$ 的一个解.

(2) 当 $x_2\equiv 5 \pmod{11}$ 时, $f(5)=319$, $f'(5)=154\equiv 0 \pmod{11}$. 因为 $p=11\nmid f'(5)$, 但是 $11^2\nmid f'(5)$, 所以由定理7.2(3) 知 $f(x)\equiv 0 \pmod{11^2}$ 没有关于模 11 同余于 5 的解.

例 7.2. 解同余方程 $x^3+8x^2-x-1\equiv 0 \pmod{11^2}$.

解: 令 $f(x)=x^3+8x^2-x-1$, 则 $f'(x)=3x^2+16x-1$. 解 $f(x)\equiv 0 \pmod{11}$ 得 $x_1\equiv 4 \pmod{11}$, $x_2\equiv 5 \pmod{11}$.

(1) 当 $x_1\equiv 4 \pmod{11}$ 时, $f(4)=187$, $f'(4)=111\equiv 1 \pmod{11}$. 因为 $p=11\nmid f'(4)$, 所以由定理7.2(1) 知 $f(x)\equiv 0 \pmod{11^2}$ 有惟一解 $x\equiv x_1+kp\equiv 4+11k \pmod{11^2}$, 其中 k 是 $f'(4)k\equiv -\frac{f(4)}{11} \pmod{11}$ 的惟一解, 即 $k\equiv -\frac{187}{11}\equiv 5 \pmod{11}$. 故 $x\equiv 4+11\cdot 5\equiv 59 \pmod{11^2}$ 是 $f(x)\equiv 0 \pmod{11^2}$ 的一个解.

(2) 当 $x_2\equiv 5 \pmod{11}$ 时, $f(5)=319$, $f'(5)=154\equiv 0 \pmod{11}$. 因为 $p=11\nmid f'(5)$, 但是 $11^2\nmid f'(5)$, 所以由定理7.2(3) 知 $f(x)\equiv 0 \pmod{11^2}$ 没有关于模 11 同余于 5 的解.

综上, 原同余方程仅有一个解: $x\equiv 59 \pmod{11^2}$. □