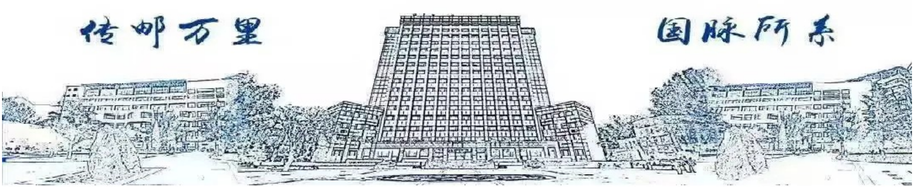
网络空间安全学院
School of Cyberspace Security, BUPT

# 信息安全数学基础

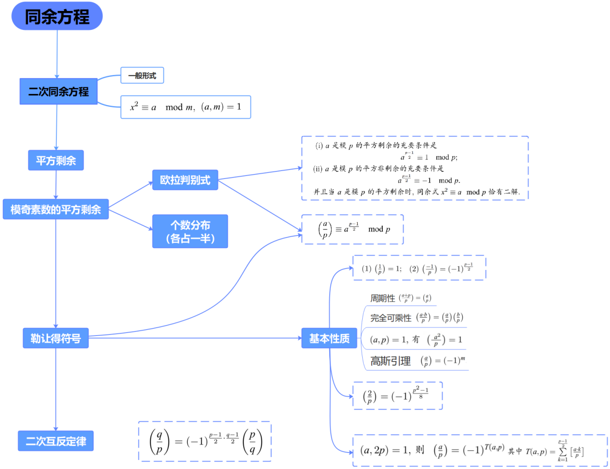
## —— 同余方程 (3)

信数课题组

北京邮电大学



# 上次课回顾



同余方程
二次同余方程
一般形式
$x^2 \equiv a \mod m,\ (a,m)=1$
平方剩余
模奇素数的平方剩余
欧拉判别式
个数分布
(各占一半)
(i) $a$ 是模 $p$ 的平方剩余的充要条件是
$a^{\frac{p-1}{2}} \equiv 1 \mod p;$
(ii) $a$ 是模 $p$ 的平方非剩余的充要条件是
$a^{\frac{p-1}{2}} \equiv -1 \mod p.$
并且当 $a$ 是模 $p$ 的平方剩余时，同余式 $x^2 \equiv a \mod p$ 恰有二解.
$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$
勒让得符号
基本性质
(1) $\left(\frac{1}{p}\right)=1$; (2) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$
周期性 $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$
完全可乘性 $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
$(a,p)=1$, 有 $\left(\frac{a^2}{p}\right)=1$
高斯引理 $\left(\frac{a}{p}\right)=(-1)^m$
$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$
$(a,2p)=1$, 则 $\left(\frac{a}{p}\right)=(-1)^{T(a,p)}$ 其中 $T(a,p)=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{a\cdot k}{p}\right]$
二次互反定律
$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$

# 目录

# 目录

对于勒让德符号以及二次互反律, 都要求模 $p$ 为素数. 现考虑模 $m$ 为奇整数, $a$ 为任意整数的情形.

### 定义 3.3.3

设 $m = p_1 \cdots p_r$ 是奇素数 $p_i$ 的乘积. 对任意整数 $a$, 定义**雅可比 (Jacobi) 符号**为

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

对于勒让德符号以及二次互反律, 都要求模 $p$ 为素数. 现考虑模 $m$ 为奇整数, $a$ 为任意整数的情形.

## 定义 3.3.3

设 $m = p_1 \cdots p_r$ 是奇素数 $p_i$ 的乘积. 对任意整数 $a$, 定义**雅可比 (Jacobi) 符号**为

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

注：雅可比符号形式上是勒让德符号的推广, 但所蕴含的意义已经不同.

雅可比符号为 $-1$, 可判断 $a$ 是模 $m$ 平方非剩余;

但雅可比符号为 1, 却不能判断 $a$ 是模 $m$ 平方剩余.

对于勒让德符号以及二次互反律, 都要求模 $p$ 为素数. 现考虑模 $m$ 为奇整数, $a$ 为任意整数的情形.

**定义 3.3.3**

设 $m = p_1 \cdots p_r$ 是奇素数 $p_i$ 的乘积. 对任意整数 $a$, 定义**雅可比 (Jacobi) 符号**为

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

注：雅可比符号形式上是勒让德符号的推广, 但所蕴含的意义已经不同.

雅可比符号为 $-1$, 可判断 $a$ 是模 $m$ 平方非剩余;

但雅可比符号为 1, 却不能判断 $a$ 是模 $m$ 平方剩余.

**例 3.3.14** 3 是模 10403 平方非剩余, 但

$$\left(\frac{3}{10403}\right) = \left(\frac{3}{101}\right)\left(\frac{3}{103}\right) = (-1)(-1) = 1.$$

## 定理 3.3.8

设 $m$ 是正奇数，则

(1) $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$; (2) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$; (3) 设 $(a,m)=1$，有 $\left(\frac{a^2}{m}\right)=1$.

**定理 3.3.8**

设 $m$ 是正奇数，则

(1) $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$; (2) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$; (3) 设 $(a,m)=1$，有 $\left(\frac{a^2}{m}\right)=1$.

证：设 $m=p_1\cdots p_r$，其中 $p_i$ 为奇素数. 根据雅可比符号的定义以及定理 3.3.5 得:

**定理 3.3.8**

设 $m$ 是正奇数，则

(1) $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$; (2) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$; (3) 设 $(a,m)=1$, 有 $\left(\frac{a^2}{m}\right)=1$.

证：设 $m=p_1\cdots p_r$, 其中 $p_i$ 为奇素数. 根据雅可比符号的定义以及定理 3.3.5 得:

(1) $\left(\frac{a+m}{m}\right)=\left(\frac{a+m}{p_1}\right)\cdots\left(\frac{a+m}{p_r}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)=\left(\frac{a}{m}\right)$.

## 定理 3.3.8

设 $m$ 是正奇数，则

(1) $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$; (2) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$; (3) 设 $(a,m)=1$，有 $\left(\frac{a^2}{m}\right)=1$.

证：设 $m=p_1\cdots p_r$，其中 $p_i$ 为奇素数. 根据雅可比符号的定义以及定理 3.3.5 得:

(1) $\left(\frac{a+m}{m}\right)=\left(\frac{a+m}{p_1}\right)\cdots\left(\frac{a+m}{p_r}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)=\left(\frac{a}{m}\right)$.

(2)
$$\begin{aligned}\left(\frac{ab}{m}\right)&=\left(\frac{ab}{p_1}\right)\cdots\left(\frac{ab}{p_r}\right)\\&=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)\\&=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{b}{p_r}\right)\\&=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right).\end{aligned}$$

## 定理 3.3.8

设 $m$ 是正奇数，则

(1) $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$; (2) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$; (3) 设 $(a,m)=1$，有 $\left(\frac{a^2}{m}\right)=1$.

证：设 $m=p_1\cdots p_r$，其中 $p_i$ 为奇素数. 根据雅可比符号的定义以及定理 3.3.5 得:

(1) $\left(\frac{a+m}{m}\right)=\left(\frac{a+m}{p_1}\right)\cdots\left(\frac{a+m}{p_r}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)=\left(\frac{a}{m}\right)$.

(2)
$$\begin{aligned}\left(\frac{ab}{m}\right)&=\left(\frac{ab}{p_1}\right)\cdots\left(\frac{ab}{p_r}\right)\\&=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)\\&=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{b}{p_r}\right)\\&=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right).\end{aligned}$$

(3) $\left(\frac{a^2}{m}\right)=\left(\frac{a^2}{p_1}\right)\cdots\left(\frac{a^2}{p_r}\right)=1$.

### 引理 3.3.2

设 $m = p_1 \cdots p_r$ 是奇数，则

$$\frac{m-1}{2} \equiv \frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2} \mod 2;$$

$$\frac{m^2-1}{8} \equiv \frac{p_1^2-1}{2} + \cdots + \frac{p_r^2-1}{2} \mod 2.$$

## 引理 3.3.2

设 $m = p_1 \cdots p_r$ 是奇数，则

$$\frac{m-1}{2} \equiv \frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2} \mod 2;$$

$$\frac{m^2-1}{8} \equiv \frac{p_1^2-1}{2} + \cdots + \frac{p_r^2-1}{2} \mod 2.$$

证：因为

$$\begin{aligned} m &\equiv \left(1+2\cdot\frac{p_1-1}{2}\right)\cdots\left(1+2\cdot\frac{p_r-1}{2}\right) \\ &\equiv 1+2\cdot\left(\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}\right) \mod 4; \\ m^2 &\equiv \left(1+8\cdot\frac{p_1^2-1}{8}\right)\cdots\left(1+8\cdot\frac{p_r^2-1}{8}\right) \\ &\equiv 1+8\cdot\left(\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}\right) \mod 16. \end{aligned}$$

所以结论成立.

**定理 3.3.9**

设 $m$ 是奇数，则

(1) $\left(\frac{1}{m}\right)=1$; (2) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$; (3) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.

**定理 3.3.9**

设 $m$ 是奇数，则

(1) $\left(\frac{1}{m}\right)=1$;  (2) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$;  (3) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.

证：因为 $m=p_1\cdots p_r$ 是奇数，其中 $p_i$ 为奇素数.

根据雅可比符号的定义，有

**定理 3.3.9**

设 $m$ 是奇数, 则

(1) $\left(\frac{1}{m}\right)=1$; (2) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$; (3) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.

证：因为 $m=p_1\cdots p_r$ 是奇数, 其中 $p_i$ 为奇素数.

根据雅可比符号的定义, 有

(1) $\left(\frac{1}{m}\right)=\left(\frac{1}{p_1}\right)\cdots\left(\frac{1}{p_r}\right)=1$.

**定理 3.3.9**

设 $m$ 是奇数, 则

(1) $\left(\frac{1}{m}\right)=1$; (2) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$; (3) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.

证：因为 $m=p_1\cdots p_r$ 是奇数, 其中 $p_i$ 为奇素数.

根据雅可比符号的定义, 有

(1) $\left(\frac{1}{m}\right)=\left(\frac{1}{p_1}\right)\cdots\left(\frac{1}{p_r}\right)=1.$

(2) $\left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_r}\right)=(-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}}=(-1)^{\frac{m-1}{2}}.$

**定理 3.3.9**

设 $m$ 是奇数，则

(1) $\left(\frac{1}{m}\right)=1$； (2) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$； (3) $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.

证：因为 $m=p_1\cdots p_r$ 是奇数，其中 $p_i$ 为奇素数.

根据雅可比符号的定义，有

$$(1)\ \left(\frac{1}{m}\right)=\left(\frac{1}{p_1}\right)\cdots\left(\frac{1}{p_r}\right)=1.$$

$$(2)\ \left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_r}\right)=(-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}}=(-1)^{\frac{m-1}{2}}.$$

再根据雅可比符号的定义以及定理 3.3.6 以及引理 3.3.2，我们有

**定理 3.3.9**

设 $m$ 是奇数, 则

(1) $\left(\frac{1}{m}\right) = 1$; (2) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$; (3) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

证：因为 $m = p_1 \cdots p_r$ 是奇数, 其中 $p_i$ 为奇素数.

根据雅可比符号的定义, 有

(1) $\left(\frac{1}{m}\right) = \left(\frac{1}{p_1}\right) \cdots \left(\frac{1}{p_r}\right) = 1.$

(2) $\left(\frac{-1}{m}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_r}\right) = (-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}} = (-1)^{\frac{m-1}{2}}.$

再根据雅可比符号的定义以及定理 3.3.6 以及引理 3.3.2, 我们有

(3) $\left(\frac{2}{m}\right) = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_r}\right) = (-1)^{\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}} = (-1)^{\frac{m^2-1}{8}}.$

## 定理 3.3.10

设 $m, n$ 都是奇数，则 $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$.

**定理 3.3.10**

设 $m, n$ 都是奇数，则 $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$.

证：设 $m = p_1 \cdots p_r, n = q_1 \cdots q_s$. 如果 $(m, n) > 1$, 则根据雅可比符号和勒让得符号的定义，我们有 $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) = 0$, 结论成立.

**定理 3.3.10**

设 $m, n$ 都是奇数, 则 $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$.

证：设 $m = p_1 \cdots p_r, n = q_1 \cdots q_s$. 如果 $(m, n) > 1$, 则根据雅可比符号和勒让得符号的定义, 我们有 $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) = 0$, 结论成立.

因此, 可设 $(m, n) = 1$. 根据雅可比符号的定义和定理 3.3.7, 我们有

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\left(\frac{n}{p_i}\right)\prod_{j=1}^{s}\left(\frac{m}{q_j}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right) = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.$$

**定理 3.3.10**

设 $m, n$ 都是奇数, 则 $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$.

证：设 $m = p_1 \cdots p_r, n = q_1 \cdots q_s$. 如果 $(m, n) > 1$, 则根据雅可比符号和勒让得符号的定义, 我们有 $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) = 0$, 结论成立.

因此, 可设 $(m, n) = 1$. 根据雅可比符号的定义和定理 3.3.7, 我们有

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\left(\frac{n}{p_i}\right)\prod_{j=1}^{s}\left(\frac{m}{q_j}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right) = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.$$

再根据引理 3.3.2,

$$\begin{aligned}\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2} &\equiv \sum_{i=1}^{r}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2}\\ &\equiv \frac{m-1}{2}\cdot\frac{n-1}{2} \mod 2.\end{aligned}$$

因此, 结论成立.

**例** 3.3.15 判断同余式 $x^2 \equiv 365 \mod 2059$ 是否有解.

**例** 3.3.15　判断同余式 $x^2 \equiv 365 \mod 2059$ 是否有解.

解：不用考虑 2059 是否是素数, 直接计算雅可比符号, 因为

$$
\begin{aligned}
\left(\frac{365}{2059}\right) &= \left(\frac{5}{2059}\right)\left(\frac{73}{2059}\right) \\
&= (-1)^{\frac{5-1}{2}\cdot\frac{2059-1}{2}}\left(\frac{2059}{5}\right)(-1)^{\frac{73-1}{2}\cdot\frac{2059-1}{2}}\left(\frac{2059}{73}\right) \\
&= \left(\frac{2^2}{5}\right)\left(\frac{15}{73}\right) \\
&= \left(\frac{3}{73}\right)\left(\frac{5}{73}\right) \\
&= \left(\frac{5}{73}\right) \\
&= (-1)^{\frac{5-1}{2}\cdot\frac{73-1}{2}}\left(\frac{73}{5}\right) \\
&= \left(\frac{3}{5}\right) \\
&= -1.
\end{aligned}
$$

**例 3.3.15** 判断同余式 $x^2 \equiv 365 \mod 2059$ 是否有解.

解：不用考虑 2059 是否是素数, 直接计算雅可比符号, 因为

$$
\begin{aligned}
\left(\frac{365}{2059}\right) &= \left(\frac{5}{2059}\right)\left(\frac{73}{2059}\right) \\
&= (-1)^{\frac{5-1}{2}\cdot\frac{2059-1}{2}}\left(\frac{2059}{5}\right)(-1)^{\frac{73-1}{2}\cdot\frac{2059-1}{2}}\left(\frac{2059}{73}\right) \\
&= \left(\frac{2^2}{5}\right)\left(\frac{15}{73}\right) \\
&= \left(\frac{3}{73}\right)\left(\frac{5}{73}\right) \\
&= \left(\frac{5}{73}\right) \\
&= (-1)^{\frac{5-1}{2}\cdot\frac{73-1}{2}}\left(\frac{73}{5}\right) \\
&= \left(\frac{3}{5}\right) \\
&= -1.
\end{aligned}
$$

所以原同余式无解.

**例 3.3.16** 求出同余方程 $y^2 \equiv x^3 + x + 1 \mod 17$ 的所有解及解数.

**例 3.3.16** 求出同余方程 $y^2 \equiv x^3 + x + 1 \mod 17$ 的所有解及解数.

解：令 $f(x) = x^3 + x + 1$. 我们有

$$f(0) \equiv 1 \mod 17,\ y \equiv 1,\ 16 \mod 17;$$
$$f(1) \equiv 3 \mod 17,\ \text{无解};$$
$$f(2) \equiv 11 \mod 17, \text{无解};$$
$$f(3) \equiv 14 \mod 17, \text{无解};$$
$$f(4) \equiv 1 \mod 17,\quad y \equiv 1,\ 16 \mod 17;$$
$$f(5) \equiv 12 \mod 17,\ \text{无解};$$
$$f(6) \equiv 2 \mod 17,\quad y \equiv 6,\ 11 \mod 17;$$
$$f(7) \equiv 11 \mod 17,\ \text{无解};$$
$$f(8) \equiv 11 \mod 17,\ \text{无解};$$
$$f(9) \equiv 8 \mod 17,\quad y \equiv 5,\ 12 \mod 17;$$
$$f(10) \equiv 8 \mod 17,\quad y \equiv 5,\ 12 \mod 17;$$

$$
\begin{aligned}
&f(11) \equiv 0 \mod 17, \quad y \equiv 0 \mod 17;\\
&f(12) \equiv 7 \mod 17, \quad \text{无解};\\
&f(13) \equiv 1 \mod 17, \quad y \equiv 1,\ 16 \mod 17;\\
&f(14) \equiv 5 \mod 17, \quad \text{无解};\\
&f(15) \equiv 8 \mod 17, \quad y \equiv 5,\ 12 \mod 17;\\
&f(16) \equiv -1 \mod 17, y \equiv 4,\ 13 \mod 17.
\end{aligned}
$$

$$f(11) \equiv 0 \mod 17, \quad y \equiv 0 \mod 17;$$
$$f(12) \equiv 7 \mod 17, \quad \text{无解};$$
$$f(13) \equiv 1 \mod 17, \quad y \equiv 1,\ 16 \mod 17;$$
$$f(14) \equiv 5 \mod 17, \quad \text{无解};$$
$$f(15) \equiv 8 \mod 17, \quad y \equiv 5,\ 12 \mod 17;$$
$$f(16) \equiv -1 \mod 17, y \equiv 4,\ 13 \mod 17.$$

因此, 原同余方程的解为

$(0,1),(0,16),(4,1),(4,16),(6,6),(6,11),(9,5),(9,12),(10,5),$
$(10,12),(11,0),(13,1),(13,16),(15,5),(15,12),(16,4),(16,13).$

# 目录

应用二次互反律 (定理 3.3.7) 可以快速的判断 $a$ 是否为模 $p$ 平方剩余, 即二次同余方程解的存在性. 下面考虑二次同余方程的具体求解.

首先, 考虑模素数 $p$ 的平方根.

在 $x^2 \equiv a \mod p$ 有解的情况下, 即 $a$ 满足 $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \mod p$, 求该二次同余方程的解.

应用二次互反律 (定理 3.3.7) 可以快速的判断 $a$ 是否为模 $p$ 平方剩余, 即二次同余方程解的存在性. 下面考虑二次同余方程的具体求解.

首先, 考虑模素数 $p$ 的平方根.

在 $x^2 \equiv a \mod p$ 有解的情况下, 即 $a$ 满足 $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1 \mod p$, 求该二次同余方程的解.

**定理 3.3.11**

设 $p$ 是奇素数, $p-1 = 2^t \cdot s, t \geqslant 1$, 其中 $s$ 是奇整数. 设 $n$ 是模 $p$ 平方非剩余, $b := n^s \mod p$, 如果同余方程 $x^2 \equiv a \mod p$ 有解, 则

$$a^{-1}x_{t-k-1}^2 \quad \text{满足同余方程} \quad y^{2^{t-k-1}} \equiv 1 \mod p, k = 0, 1, \cdots, t-1,$$

这里 $x_{t-1} := a^{\frac{s+1}{2}} \mod p$, $x_{t-k-1} = x_{t-k} b^{j_{k-1} 2^{k-1}}$,

$$\text{其中 } j_{k-1} = \begin{cases} 0, & \text{如果 } (a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv 1 \mod p; \\ 1, & \text{如果 } (a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1 \mod p. \end{cases}$$

特别地, $x_0$ 是同余方程 $x^2 \equiv a \mod p$ 的解.

证：对于奇素数 $p$, 将 $p-1$ 写成形式 $p-1=2^t\cdot s, t\geqslant 1$, 其中 $s$ 是奇数.

证：对于奇素数 $p$, 将 $p-1$ 写成形式 $p-1=2^t\cdot s, t\geqslant 1$, 其中 $s$ 是奇数.

(1) 任意选取一个模 $p$ 平方非剩余 $n$, 即整数 $n$ 使得 $\left(\frac{n}{p}\right)=-1$,

证：对于奇素数 $p$, 将 $p-1$ 写成形式 $p-1=2^t\cdot s, t\geqslant 1$, 其中 $s$ 是奇数.

(1) 任意选取一个模 $p$ 平方非剩余 $n$, 即整数 $n$ 使得 $\left(\frac{n}{p}\right)=-1$,
再令 $b:=n^s \mod p$, 有 $b^{2^t}\equiv 1 \mod p$, $b^{2^{t-1}}\equiv -1 \mod p$,
即 $b$ 是模 $p$ 的 $2^t$ 次单位根, 但非模 $p$ 的 $2^{t-1}$ 次单位根.

证：对于奇素数 $p$, 将 $p-1$ 写成形式 $p-1=2^t\cdot s, t\geqslant 1$, 其中 $s$ 是奇数.

(1) 任意选取一个模 $p$ 平方非剩余 $n$, 即整数 $n$ 使得 $\left(\frac{n}{p}\right)=-1$,

再令 $b:=n^s \mod p$, 有 $b^{2^t}\equiv 1 \mod p$, $\quad b^{2^{t-1}}\equiv -1 \mod p$,

即 $b$ 是模 $p$ 的 $2^t$ 次单位根, 但非模 $p$ 的 $2^{t-1}$ 次单位根.

(事实上, $b^{2^t}\equiv (n^s)^{2^t}\equiv n^{s\cdot 2^t}\equiv n^{p-1}\equiv 1 \mod p$,

$$b^{2^{t-1}}\equiv (n^s)^{2^{t-1}}\equiv n^{\frac{p-1}{2}}\equiv -1 \mod p.)$$

证：对于奇素数 $p$, 将 $p-1$ 写成形式 $p-1=2^t\cdot s, t\geqslant 1$, 其中 $s$ 是奇数.

(1) 任意选取一个模 $p$ 平方非剩余 $n$, 即整数 $n$ 使得 $\left(\frac{n}{p}\right)=-1$,

再令 $b:=n^s \mod p$, 有 $b^{2^t}\equiv 1 \mod p$, $b^{2^{t-1}}\equiv -1 \mod p$,

即 $b$ 是模 $p$ 的 $2^t$ 次单位根, 但非模 $p$ 的 $2^{t-1}$ 次单位根.

(事实上, $b^{2^t}\equiv (n^s)^{2^t}\equiv n^{s\cdot 2^t}\equiv n^{p-1}\equiv 1 \mod p$,

$$b^{2^{t-1}}\equiv (n^s)^{2^{t-1}}\equiv n^{\frac{p-1}{2}}\equiv -1 \mod p.)$$

(2) 计算 $x_{t-1}:=a^{\frac{s+1}{2}} \mod p$. 有 $a^{-1}x_{t-1}^2$

满足同余方程 $y^{2^{t-1}}\equiv 1 \mod p$, 即 $a^{-1}x_{t-1}^2$ 是 $2^{t-1}$ 次单位根.

证：对于奇素数 $p$, 将 $p-1$ 写成形式 $p-1=2^t\cdot s, t\geqslant 1$, 其中 $s$ 是奇数.

(1) 任意选取一个模 $p$ 平方非剩余 $n$, 即整数 $n$ 使得 $\left(\frac{n}{p}\right)=-1$,

再令 $b:=n^s \mod p$, 有 $b^{2^t}\equiv 1 \mod p$, $b^{2^{t-1}}\equiv -1 \mod p$,

即 $b$ 是模 $p$ 的 $2^t$ 次单位根, 但非模 $p$ 的 $2^{t-1}$ 次单位根.

(事实上, $b^{2^t}\equiv (n^s)^{2^t}\equiv n^{s\cdot 2^t}\equiv n^{p-1}\equiv 1 \mod p$,

$b^{2^{t-1}}\equiv (n^s)^{2^{t-1}}\equiv n^{\frac{p-1}{2}}\equiv -1 \mod p$.)

(2) 计算 $x_{t-1}:=a^{\frac{s+1}{2}} \mod p$. 有 $a^{-1}x_{t-1}^2$

满足同余方程 $y^{2^{t-1}}\equiv 1 \mod p$, 即 $a^{-1}x_{t-1}^2$ 是 $2^{t-1}$ 次单位根.

(事实上, $(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv a^{2^{t-1}s}\equiv a^{\frac{p-1}{2}}\equiv \left(\frac{a}{p}\right)\equiv 1 \mod p$.)

证：对于奇素数 $p$, 将 $p-1$ 写成形式 $p-1=2^t\cdot s, t\geqslant 1$, 其中 $s$ 是奇数.

(1) 任意选取一个模 $p$ 平方非剩余 $n$, 即整数 $n$ 使得 $\left(\frac{n}{p}\right)=-1$,
再令 $b:=n^s \mod p$, 有 $b^{2^t}\equiv 1 \mod p$, $\quad b^{2^{t-1}}\equiv -1 \mod p$,
即 $b$ 是模 $p$ 的 $2^t$ 次单位根, 但非模 $p$ 的 $2^{t-1}$ 次单位根.
(事实上, $b^{2^t}\equiv (n^s)^{2^t}\equiv n^{s\cdot 2^t}\equiv n^{p-1}\equiv 1 \mod p$,
$$b^{2^{t-1}}\equiv (n^s)^{2^{t-1}}\equiv n^{\frac{p-1}{2}}\equiv -1 \mod p.)$$

(2) 计算 $x_{t-1}:=a^{\frac{s+1}{2}} \mod p$. 有 $a^{-1}x_{t-1}^2$
满足同余方程 $y^{2^{t-1}}\equiv 1 \mod p$, 即 $a^{-1}x_{t-1}^2$ 是 $2^{t-1}$ 次单位根.
(事实上, $(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv a^{2^{t-1}s}\equiv a^{\frac{p-1}{2}}\equiv \left(\frac{a}{p}\right)\equiv 1 \mod p$.)

(3) 如果 $t=1$, 则 $x=x_{t-1}=x_0\equiv a^{\frac{s+1}{2}} \mod p$ 满足 $x^2\equiv a \mod p$.

证：对于奇素数 $p$, 将 $p-1$ 写成形式 $p-1=2^t\cdot s, t\geqslant 1$, 其中 $s$ 是奇数.

(1) 任意选取一个模 $p$ 平方非剩余 $n$, 即整数 $n$ 使得 $\left(\frac{n}{p}\right)=-1$,

再令 $b:=n^s \mod p$, 有 $b^{2^t}\equiv 1 \mod p$, $b^{2^{t-1}}\equiv -1 \mod p$,

即 $b$ 是模 $p$ 的 $2^t$ 次单位根, 但非模 $p$ 的 $2^{t-1}$ 次单位根.

(事实上, $b^{2^t}\equiv (n^s)^{2^t}\equiv n^{s\cdot 2^t}\equiv n^{p-1}\equiv 1 \mod p$,

$$b^{2^{t-1}}\equiv (n^s)^{2^{t-1}}\equiv n^{\frac{p-1}{2}}\equiv -1 \mod p.)$$

(2) 计算 $x_{t-1}:=a^{\frac{s+1}{2}} \mod p$. 有 $a^{-1}x_{t-1}^2$

满足同余方程 $y^{2^{t-1}}\equiv 1 \mod p$, 即 $a^{-1}x_{t-1}^2$ 是 $2^{t-1}$ 次单位根.

(事实上, $(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv a^{2^{t-1}s}\equiv a^{\frac{p-1}{2}}\equiv \left(\frac{a}{p}\right)\equiv 1 \mod p.$)

(3) 如果 $t=1$, 则 $x=x_{t-1}=x_0\equiv a^{\frac{s+1}{2}} \mod p$ 满足 $x^2\equiv a \mod p$.

如果 $t\geqslant 2$, 就要寻找整数 $x_{t-2}$ 使得 $a^{-1}x_{t-2}^2$ 满足 $y^{2^{t-2}}\equiv 1 \mod p$, 即 $a^{-1}x_{t-2}^2$ 是 $2^{t-2}$ 次单位根.

若 $(a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv 1 \mod p$, 令 $j_0:=0$; 否则, $(a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv -1$ $\equiv (b^{-2})^{2^{t-2}} \mod p$, 令 $j_0:=1$. 则 $x_{t-2}:=x_{t-1}b^{j_0} \mod p$ 即为所求.

$(\cdots)$ 如此下去, 继续寻找整数 $x_{t-3}, x_{t-4}, \cdots\cdots$

$(\cdots)$ 如此下去, 继续寻找整数 $x_{t-3}, x_{t-4}, \cdots\cdots$

假设找到整数 $x_{t-k}$ 使得 $a^{-1}x_{t-k}^2$ 满足同余方程 $y^{2^{t-k}} \equiv 1 \mod p$, 即 $a^{-1}x_{t-k}^2$ 是 $2^{t-k}$ 次单位根, $(a^{-1}x_{t-k}^2)^{2^{t-k}} \equiv 1 \mod p$.

$(\cdots)$ 如此下去, 继续寻找整数 $x_{t-3}, x_{t-4}, \cdots\cdots$

假设找到整数 $x_{t-k}$ 使得 $a^{-1}x_{t-k}^2$ 满足同余方程 $y^{2^{t-k}} \equiv 1 \mod p$, 即 $a^{-1}x_{t-k}^2$ 是 $2^{t-k}$ 次单位根, $(a^{-1}x_{t-k}^2)^{2^{t-k}} \equiv 1 \mod p$.

$(k+2)$ 如果 $t = k$, 则 $x = x_{t-k} = x_0 \mod p$ 满足 $x^2 \equiv a \mod p$.

$(\cdots)$ 如此下去, 继续寻找整数 $x_{t-3}, x_{t-4}, \cdots\cdots$

假设找到整数 $x_{t-k}$ 使得 $a^{-1}x_{t-k}^2$ 满足同余方程 $y^{2^{t-k}} \equiv 1 \mod p$,
即 $a^{-1}x_{t-k}^2$ 是 $2^{t-k}$ 次单位根, $(a^{-1}x_{t-k}^2)^{2^{t-k}} \equiv 1 \mod p$.

$(k+2)$ 如果 $t = k$, 则 $x = x_{t-k} = x_0 \mod p$ 满足 $x^2 \equiv a \mod p$.

如果 $t \geqslant k+1$, 就要寻找整数 $x_{t-k-1}$ 使得

$$a^{-1}x_{t-k-1}^2 \quad \text{满足同余方程} \quad y^{2^{t-k-1}} \equiv 1 \mod p,$$

即 $a^{-1}x_{t-k-1}^2$ 是 $2^{t-k-1}$ 次单位根.

$(\cdots)$ 如此下去, 继续寻找整数 $x_{t-3}, x_{t-4}, \cdots\cdots$

假设找到整数 $x_{t-k}$ 使得 $a^{-1}x_{t-k}^2$ 满足同余方程 $y^{2^{t-k}} \equiv 1 \mod p$,
即 $a^{-1}x_{t-k}^2$ 是 $2^{t-k}$ 次单位根, $(a^{-1}x_{t-k}^2)^{2^{t-k}} \equiv 1 \mod p$.

$(k+2)$ 如果 $t = k$, 则 $x = x_{t-k} = x_0 \mod p$ 满足 $x^2 \equiv a \mod p$.

如果 $t \geqslant k+1$, 就要寻找整数 $x_{t-k-1}$ 使得

$$a^{-1}x_{t-k-1}^2 \quad \text{满足同余方程} \quad y^{2^{t-k-1}} \equiv 1 \mod p,$$

即 $a^{-1}x_{t-k-1}^2$ 是 $2^{t-k-1}$ 次单位根.

若 $(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv 1 \mod p$, 令 $j_{k-1} := 0$;

否则, $(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1 \equiv (b^{-2^k})^{2^{t-k-2}} \mod p$, 令 $j_{k-1} := 1$.

$(\cdots)$ 如此下去, 继续寻找整数 $x_{t-3}, x_{t-4}, \cdots\cdots$

假设找到整数 $x_{t-k}$ 使得 $a^{-1}x_{t-k}^2$ 满足同余方程 $y^{2^{t-k}} \equiv 1 \mod p$,

即 $a^{-1}x_{t-k}^2$ 是 $2^{t-k}$ 次单位根, $(a^{-1}x_{t-k}^2)^{2^{t-k}} \equiv 1 \mod p$.

$(k+2)$ 如果 $t = k$, 则 $x = x_{t-k} = x_0 \mod p$ 满足 $x^2 \equiv a \mod p$.

如果 $t \geqslant k+1$, 就要寻找整数 $x_{t-k-1}$ 使得

$$a^{-1}x_{t-k-1}^2 \quad \text{满足同余方程} \quad y^{2^{t-k-1}} \equiv 1 \mod p,$$

即 $a^{-1}x_{t-k-1}^2$ 是 $2^{t-k-1}$ 次单位根.

若 $(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv 1 \mod p$, 令 $j_{k-1} := 0$;

否则, $(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1 \equiv (b^{-2^k})^{2^{t-k-2}} \mod p$, 令 $j_{k-1} := 1$.

则 $x_{t-k-1} := x_{t-k}b^{j_{k-1}2^{k-1}} \mod p$ 即为所求.

特别地, 对于 $k=t-1$, 我们有

$$\begin{aligned} x &= x_0 \\ &\equiv x_1 b^{j_{t-2}2^{t-2}} \\ &\vdots \\ &\equiv x_{t-1} b^{j_0+j_1 2+\cdots+j_{t-2}2^{t-2}} \\ &\equiv a^{\frac{s+1}{2}} b^{j_0+j_1 2+\cdots+j_{t-2}2^{t-2}} \mod p. \end{aligned}$$

满足同余方程 $x^2 \equiv a \mod p$.

特别地, 对于 $k=t-1$, 我们有

$$\begin{aligned} x &= x_0 \\ &\equiv x_1 b^{j_{t-2}2^{t-2}} \\ &\vdots \\ &\equiv x_{t-1} b^{j_0+j_1 2+\cdots+j_{t-2}2^{t-2}} \\ &\equiv a^{\frac{s+1}{2}} b^{j_0+j_1 2+\cdots+j_{t-2}2^{t-2}} \mod p. \end{aligned}$$

满足同余方程 $x^2 \equiv a \mod p$.

**例 3.3.17** 求解同余方程 $x^2 \equiv 157 \mod 2029$.

特别地, 对于 $k = t-1$, 我们有

$$\begin{aligned} x &= x_0 \\ &\equiv x_1 b^{j_{t-2}2^{t-2}} \\ &\vdots \\ &\equiv x_{t-1} b^{j_0+j_1 2+\cdots+j_{t-2}2^{t-2}} \\ &\equiv a^{\frac{s+1}{2}} b^{j_0+j_1 2+\cdots+j_{t-2}2^{t-2}} \pmod p. \end{aligned}$$

满足同余方程 $x^2 \equiv a \mod p$.

**例 3.3.17** 求解同余方程 $x^2 \equiv 157 \mod 2029$.

解：计算勒让得符号

$$\left(\frac{157}{2029}\right) = (-1)^{\frac{157-1}{2}\cdot\frac{2029-1}{2}}\left(\frac{2029}{157}\right) = \left(\frac{145}{157}\right) = \left(\frac{5}{157}\right)\left(\frac{29}{157}\right),$$

而 $\left(\frac{5}{157}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{157-1}{2}}\left(\frac{157}{5}\right) = \left(\frac{2}{5}\right) = -1,$

$$\begin{aligned} \left(\frac{29}{157}\right) &= (-1)^{\frac{29-1}{2}\cdot\frac{157-1}{2}}\left(\frac{157}{29}\right) = \left(\frac{12}{29}\right) = \left(\frac{3}{29}\right) \\ &= (-1)^{\frac{3-1}{2}\cdot\frac{29-1}{2}}\left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = -1. \end{aligned}$$

所以, $\left(\frac{157}{2029}\right) = \left(\frac{5}{157}\right)\left(\frac{29}{157}\right) = 1$. 故原同余方程有解.

对于奇素数 $p = 2029$, 将 $p-1$ 写成形式 $p-1 = 2028 = 2^2 \cdot 507$, 其中 $t = 2$, $s = 507$ 是奇数.

对于奇素数 $p = 2029$, 将 $p-1$ 写成形式 $p-1 = 2028 = 2^2 \cdot 507$, 其中 $t = 2$, $s = 507$ 是奇数.

(1) 任意选取一个模 2029 平方非剩余 $n = 2$,

即整数 $n = 2$ 使得 $\left(\frac{2}{2029}\right) = -1$, 再令 $b := 2^{507} \equiv 992 \mod 2029$.

对于奇素数 $p=2029$, 将 $p-1$ 写成形式 $p-1=2028=2^2\cdot 507$, 其中 $t=2$, $s=507$ 是奇数.

(1) 任意选取一个模 2029 平方非剩余 $n=2$,

即整数 $n=2$ 使得 $\left(\frac{2}{2029}\right)=-1$, 再令 $b:=2^{507}\equiv 992 \mod 2029$.

(2) 计算 $x_{t-1}=x_1:=157^{\frac{507+1}{2}}\equiv 157^{254}\equiv 729 \mod 2029$ 以及

$a^{-1}\equiv 1861 \mod 2029$.

对于奇素数 $p = 2029$, 将 $p-1$ 写成形式 $p-1 = 2028 = 2^2 \cdot 507$, 其中 $t = 2$, $s = 507$ 是奇数.

(1) 任意选取一个模 2029 平方非剩余 $n = 2$,

即整数 $n = 2$ 使得 $\left(\frac{2}{2029}\right) = -1$, 再令 $b := 2^{507} \equiv 992 \mod 2029$.

(2) 计算 $x_{t-1} = x_1 := 157^{\frac{507+1}{2}} \equiv 157^{254} \equiv 729 \mod 2029$ 以及

$a^{-1} \equiv 1861 \mod 2029$.

(3) 因为 $a^{-1}x_1^2 \equiv 1861 \cdot 729^2 \equiv -1 \mod 2029$, 令 $j_0 := 1$,

计算 $x \equiv x_0 \equiv x_1 b^{j_0} = 729 \cdot 992 \equiv 844 \mod 2029$.

则 $x \equiv x_0 \equiv 844 \mod 2029$ 和 $x \equiv p - x_0 \equiv 1185 \mod 2029$ 是同余方程 $x^2 \equiv 157 \mod 2029$ 的两个解.

其次, 考虑模合数 $m$ 平方根. 即模为合数 $m$ 的二次同余方程

$$x^2 \equiv a \mod m, \ (a, m) = 1$$

有解的条件及解的个数.

当 $m = 2^\delta p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \delta \geqslant 0, \alpha_i \geqslant 0, \ i = 1, \cdots, k$ 时,

其次, 考虑模合数 $m$ 平方根. 即模为合数 $m$ 的二次同余方程

$$x^2 \equiv a \mod m, \ (a,m)=1$$

有解的条件及解的个数.

当 $m = 2^{\delta} p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \delta \geqslant 0, \alpha_i \geqslant 0, \ i=1,\cdots,k$ 时,

同余方程 $x^2 \equiv a \mod m, \ (a,m)=1$ 等价于同余方程组

$$\begin{cases} x^2 \equiv a \mod 2^{\delta}, \\ x^2 \equiv a \mod p_1^{\alpha_1}, \\ \qquad \vdots \\ x^2 \equiv a \mod p_k^{\alpha_k}. \end{cases}$$

其次, 考虑模合数 $m$ 平方根. 即模为合数 $m$ 的二次同余方程

$$x^2 \equiv a \mod m,\ (a, m) = 1$$

有解的条件及解的个数.

当 $m = 2^\delta p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \delta \geqslant 0, \alpha_i \geqslant 0,\ i = 1, \cdots, k$ 时,
同余方程 $x^2 \equiv a \mod m,\ (a, m) = 1$ 等价于同余方程组

$$\begin{cases} x^2 \equiv a \mod 2^\delta, \\ x^2 \equiv a \mod p_1^{\alpha_1}, \\ \qquad\vdots \\ x^2 \equiv a \mod p_k^{\alpha_k}. \end{cases}$$

因此, 需要讨论同余方程 $x^2 \equiv a \mod p^\alpha, (a, p) = 1, \alpha > 0, p$ 为奇素数时有解的条件及解的个数, 还需要讨论同余方程 $x^2 \equiv a \mod 2^\alpha, (a, 2) = 1, \alpha > 0$ 有解的条件及解的个数.

**定理 3.3.12**

设 $p$ 是奇素数. 则同余方程 $x^2 \equiv a \mod p^{\alpha}$, $(a,p)=1, \alpha>0$ 有解的充要条件是 $a$ 为模 $p$ 平方剩余, 且有解时, 解数为 2.

**定理 3.3.12**

设 $p$ 是奇素数. 则同余方程 $x^2 \equiv a \mod p^\alpha$, $(a,p)=1, \alpha>0$ 有解的充要条件是 $a$ 为模 $p$ 平方剩余, 且有解时, 解数为 2.

证：设同余方程有解, 即存在整数 $x \equiv x_1 \mod p^\alpha$ 使得 $x_1^2 \equiv a \mod p^\alpha$, 则我们有 $x_1^2 \equiv a \mod p$, 即 $a$ 为模 $p$ 平方剩余, 因此必要性成立.

**定理 3.3.12**

设 $p$ 是奇素数. 则同余方程 $x^2 \equiv a \mod p^\alpha$, $(a,p)=1, \alpha > 0$ 有解的充要条件是 $a$ 为模 $p$ 平方剩余, 且有解时, 解数为 2.

证：设同余方程有解, 即存在整数 $x \equiv x_1 \mod p^\alpha$ 使得 $x_1^2 \equiv a \mod p^\alpha$, 则我们有 $x_1^2 \equiv a \mod p$, 即 $a$ 为模 $p$ 平方剩余, 因此必要性成立.

反过来, 设 $a$ 为模 $p$ 平方剩余, 那么存在整数 $x \equiv x_1 \mod p^\alpha$ 使得

$$x_1^2 \equiv a \mod p.$$

**定理 3.3.12**

设 $p$ 是奇素数. 则同余方程 $x^2 \equiv a \mod p^\alpha$, $(a,p)=1, \alpha>0$ 有解的充要条件是 $a$ 为模 $p$ 平方剩余, 且有解时, 解数为 2.

证：设同余方程有解, 即存在整数 $x \equiv x_1 \mod p^\alpha$ 使得 $x_1^2 \equiv a \mod p^\alpha$, 则我们有 $x_1^2 \equiv a \mod p$, 即 $a$ 为模 $p$ 平方剩余, 因此必要性成立.

反过来, 设 $a$ 为模 $p$ 平方剩余, 那么存在整数 $x \equiv x_1 \mod p^\alpha$ 使得

$$x_1^2 \equiv a \mod p.$$

令 $f(x) = x^2 - a$, 则

$$f'(x) = 2x, \ (f'(x_1), p) = (2x_1, p) = 1.$$

**定理 3.3.12**

设 $p$ 是奇素数. 则同余方程 $x^2 \equiv a \mod p^\alpha$, $(a,p)=1, \alpha>0$ 有解的充要条件是 $a$ 为模 $p$ 平方剩余, 且有解时, 解数为 2.

证：设同余方程有解, 即存在整数 $x \equiv x_1 \mod p^\alpha$ 使得 $x_1^2 \equiv a \mod p^\alpha$, 则我们有 $x_1^2 \equiv a \mod p$, 即 $a$ 为模 $p$ 平方剩余, 因此必要性成立.

反过来, 设 $a$ 为模 $p$ 平方剩余, 那么存在整数 $x \equiv x_1 \mod p^\alpha$ 使得

$$x_1^2 \equiv a \mod p.$$

令 $f(x) = x^2 - a$, 则

$$f'(x) = 2x, \ (f'(x_1), p) = (2x_1, p) = 1.$$

根据定理 3.4.6（后面给出高次同余方程的定理结论及其证明）, 从同余方程 $x^2 \equiv a \mod p$ 的解 $x \equiv x_1 \mod p$, 可递归地推出唯一的 $x \equiv x_\alpha \mod p^\alpha$ 使得 $x_\alpha^2 \equiv a \mod p^\alpha$.

**定理 3.3.12**

设 $p$ 是奇素数. 则同余方程 $x^2 \equiv a \mod p^\alpha$, $(a,p)=1, \alpha>0$ 有解的充要条件是 $a$ 为模 $p$ 平方剩余, 且有解时, 解数为 2.

证：设同余方程有解, 即存在整数 $x \equiv x_1 \mod p^\alpha$ 使得 $x_1^2 \equiv a \mod p^\alpha$, 则我们有 $x_1^2 \equiv a \mod p$, 即 $a$ 为模 $p$ 平方剩余, 因此必要性成立.

反过来, 设 $a$ 为模 $p$ 平方剩余, 那么存在整数 $x \equiv x_1 \mod p^\alpha$ 使得

$$x_1^2 \equiv a \mod p.$$

令 $f(x)=x^2-a$, 则

$$f'(x)=2x,\ (f'(x_1),p)=(2x_1,p)=1.$$

根据定理 3.4.6（后面给出高次同余方程的定理结论及其证明）, 从同余方程 $x^2 \equiv a \mod p$ 的解 $x \equiv x_1 \mod p$, 可递归地推出唯一的 $x \equiv x_\alpha \mod p^\alpha$ 使得 $x_\alpha^2 \equiv a \mod p^\alpha$.

因为 $x^2 \equiv a \mod p$ 只有两个解, 所以 $x^2 \equiv a \mod p^\alpha$ 的解数为 2.

**定理 3.3.13**

设 $\alpha > 1$, 则同余方程 $x^2 \equiv a \mod 2^{\alpha}, (a, 2) = 1$ 有解的充要条件是

(i) 当 $\alpha = 2$ 时, $a \equiv 1 \mod 4$;

(ii) 当 $\alpha \geqslant 3$ 时, $a \equiv 1 \mod 8$.

进一步, 当 $\alpha = 2$ 时, 解数是 2; 当 $\alpha \geqslant 3$ 时, 解数是 4.

## 定理 3.3.13

设 $\alpha > 1$, 则同余方程 $x^2 \equiv a \mod 2^\alpha, (a,2) = 1$ 有解的充要条件是

(i) 当 $\alpha = 2$ 时, $a \equiv 1 \mod 4$;

(ii) 当 $\alpha \geqslant 3$ 时, $a \equiv 1 \mod 8$.

进一步, 当 $\alpha = 2$ 时, 解数是 2; 当 $\alpha \geqslant 3$ 时, 解数是 4.

证：必要性. 设同余方程 $x^2 \equiv a \mod 2^\alpha, (a,2) = 1, \alpha > 0$ 有解, 则存在整数 $x_1$ 使得 $x_1^2 \equiv a \mod 2^\alpha$. 根据 $(a,2) = 1$, 我们有 $(x_1,2) = 1$.

记 $x_1 = 1 + t \cdot 2$, 上式可写成

$$a \equiv 1 + t(t+1) \cdot 2^2 \mod 2^\alpha.$$

注意到 $2 \mid t(t+1)$, 我们有

(i) 当 $\alpha = 2$ 时, $a \equiv 1 \mod 4$;

(ii) 当 $\alpha \geqslant 3$ 时, $a \equiv 1 \mod 8$.

因此必要性成立.

充分性. 当必要条件满足时, 则

(i) 当 $\alpha = 2$ 时, $a \equiv 1 \mod 4$, 这时 $x \equiv 1, 3 \mod 2^2$ 是同余方程 $x^2 \equiv a \mod 2^\alpha, (a, 2) = 1, \alpha > 0$ 仅有的二解.

充分性. 当必要条件满足时, 则

(i) 当 $\alpha = 2$ 时, $a \equiv 1 \mod 4$, 这时 $x \equiv 1, 3 \mod 2^2$ 是同余方程 $x^2 \equiv a \mod 2^\alpha, (a, 2) = 1, \alpha > 0$ 仅有的二解.

(ii) 当 $\alpha \geqslant 3$ 时, $a \equiv 1 \mod 8$, 这时

对于 $\alpha = 3$, 易验证 $x \equiv \pm 1, \pm 5 \mod 2^3$ 是 $x^2 \equiv a \mod 2^\alpha, (a, 2) = 1, \alpha > 0$ 仅有的 4 解, 它们可以表示为

$$\pm(1 + t_3 \cdot 2^2),\ t_3 = 0, 1, \cdots \quad \text{或者} \quad \pm\,(x_3 + t_3 \cdot 2^2),\ t_3 = 0, 1, \cdots .$$

充分性. 当必要条件满足时, 则

(i) 当 $\alpha=2$ 时, $a\equiv 1 \mod 4$, 这时 $x\equiv 1,3 \mod 2^2$ 是同余方程 $x^2\equiv a \mod 2^\alpha, (a,2)=1, \alpha>0$ 仅有的二解.

(ii) 当 $\alpha\geqslant 3$ 时, $a\equiv 1 \mod 8$, 这时

对于 $\alpha=3$, 易验证 $x\equiv \pm1,\pm5 \mod 2^3$ 是 $x^2\equiv a \mod 2^\alpha, (a,2)=1, \alpha>0$ 仅有的 4 解, 它们可以表示为

$$\pm(1+t_3\cdot 2^2),\ t_3=0,1,\cdots \quad 或者 \quad \pm(x_3+t_3\cdot 2^2),\ t_3=0,1,\cdots .$$

对于 $\alpha=4$, 考虑到 $x^2\equiv a \mod 2^4$ 的解一定满足 $x^2\equiv a \mod 2^3$, 于是将上述 $x^2\equiv a \mod 2^3$ 的解 $\pm(x_3+t_3\cdot 2^2)$ 代入 $x^2\equiv a \mod 2^4$, 即令 $(x_3+t_3\cdot 2^2)^2\equiv a \mod 2^4$, 同时注意到 $2x_3(t_3\cdot 2^2)\equiv t_3\cdot 2^3 \mod 2^4$, 则有 $x_3^2+t_3\cdot 2^3\equiv a \mod 2^4$, 进而求得 $t_3\equiv \frac{a-x_3^2}{2^3} \mod 2$.

故同余式 $x^2\equiv a \mod 2^4$ 的解可表示为

$$\pm(1+4\cdot\frac{a-x_3^2}{2^3}+t_4\cdot 2^3),\ t_4=0,1,\cdots \quad 或者 \quad \pm(x_4+t_4\cdot 2^3),\ t_4=0,1,\cdots .$$

充分性. 当必要条件满足时, 则

(i) 当 $\alpha = 2$ 时, $a \equiv 1 \mod 4$, 这时 $x \equiv 1, 3 \mod 2^2$ 是同余方程 $x^2 \equiv a \mod 2^\alpha, (a, 2) = 1, \alpha > 0$ 仅有的二解.

(ii) 当 $\alpha \geqslant 3$ 时, $a \equiv 1 \mod 8$, 这时

对于 $\alpha = 3$, 易验证 $x \equiv \pm 1, \pm 5 \mod 2^3$ 是 $x^2 \equiv a \mod 2^\alpha, (a, 2) = 1, \alpha > 0$ 仅有的 4 解, 它们可以表示为

$$\pm(1 + t_3 \cdot 2^2),\ t_3 = 0, 1, \cdots \quad 或者 \quad \pm(x_3 + t_3 \cdot 2^2),\ t_3 = 0, 1, \cdots .$$

对于 $\alpha = 4$, 考虑到 $x^2 \equiv a \mod 2^4$ 的解一定满足 $x^2 \equiv a \mod 2^3$, 于是将上述 $x^2 \equiv a \mod 2^3$ 的解 $\pm(x_3 + t_3 \cdot 2^2)$ 代入 $x^2 \equiv a \mod 2^4$, 即令 $(x_3 + t_3 \cdot 2^2)^2 \equiv a \mod 2^4$, 同时注意到 $2x_3(t_3 \cdot 2^2) \equiv t_3 \cdot 2^3 \mod 2^4$, 则有 $x_3^2 + t_3 \cdot 2^3 \equiv a \mod 2^4$, 进而求得 $t_3 \equiv \frac{a - x_3^2}{2^3} \mod 2$.

故同余式 $x^2 \equiv a \mod 2^4$ 的解可表示为

$$\pm(1 + 4 \cdot \frac{a - x_3^2}{2^3} + t_4 \cdot 2^3),\ t_4 = 0, 1, \cdots \quad 或者 \quad \pm(x_4 + t_4 \cdot 2^3),\ t_4 = 0, 1, \cdots .$$

对于 $\alpha \geqslant 4$, 如果满足同余方程 $x^2 \equiv a \mod 2^{\alpha-1}$ 的解为

$$x = \pm(x_{\alpha-1} + t_{\alpha-1} \cdot 2^{\alpha-2}), \quad t_{\alpha-1} = 0, 1, \cdots,$$

则同理地令 $(x_{\alpha-1} + t_{\alpha-1} \cdot 2^{\alpha-2})^2 \equiv a \mod 2^{\alpha}$,

并注意到 $2x_{\alpha-1}(t_{\alpha-1} \cdot 2^{\alpha-2}) \equiv t_{\alpha-1} \cdot 2^{\alpha-1} \mod 2^{\alpha}$, 则有

$$x_{\alpha-1}^2 + t_{\alpha-1} \cdot 2^{\alpha-1} \equiv a \mod 2^{\alpha},$$

进而求得 $t_{\alpha-1} \equiv \frac{a-x_{\alpha-1}^2}{2^{\alpha-1}} \mod 2$.

故同余方程 $x^2 \equiv a \mod 2^{\alpha}$ 的解可表示为

$$\pm(x_{\alpha-1} + \frac{a-x_{\alpha-1}^2}{2^{\alpha-1}} \cdot 2^{\alpha-2} + t_{\alpha} \cdot 2^{\alpha-1}), \; t_{\alpha} = 0, 1, \cdots$$

或者

$$\pm(x_{\alpha} + t_{\alpha} \cdot 2^{\alpha-1}), \; t_{\alpha} = 0, 1, \cdots.$$

它们对模 $2^{\alpha}$ 为 4 个解, 即 $x_{\alpha}, x_{\alpha} + 2^{\alpha-1}, -x_{\alpha}, -(x_{\alpha} + 2^{\alpha-1})$.

例 3.3.18 求解同余方程 $x^2 \equiv 57 \mod 64$.

**例** 3.3.18　求解同余方程 $x^2 \equiv 57 \mod 64$.

解：因为 $57 \equiv 1 \mod 8$, 所以同余方程有 4 个解.

**例** 3.3.18 求解同余方程 $x^2 \equiv 57 \mod 64$.

解：因为 $57 \equiv 1 \mod 8$, 所以同余方程有 4 个解.

$\alpha = 3$ 时, 同余方程 $x^2 \equiv 57 \mod 2^3$ 的解为 $\pm(1 + t_3 \cdot 2^2)$, $t_3 = 0, 1, \cdots$

**例 3.3.18** 求解同余方程 $x^2 \equiv 57 \mod 64$.

解：因为 $57 \equiv 1 \mod 8$, 所以同余方程有 4 个解.

$\alpha = 3$ 时, 同余方程 $x^2 \equiv 57 \mod 2^3$ 的解为 $\pm(1 + t_3 \cdot 2^2)$, $t_3 = 0, 1, \cdots$

$\alpha = 4$ 时, 令 $(1 + t_3 \cdot 2^2)^2 \equiv 57 \mod 2^4$, 可得 $t_3 \equiv \frac{57-1^2}{8} \equiv 1 \mod 2$.

故同余方程 $x^2 \equiv 57 \mod 2^4$ 的解为

$$\pm(1 + 1 \cdot 2^2 + t_4 \cdot 2^3) = \pm(5 + t_4 \cdot 2^3), \ t_4 = 0, 1, \cdots$$

**例 3.3.18** 求解同余方程 $x^2 \equiv 57 \mod 64.$

解：因为 $57 \equiv 1 \mod 8$, 所以同余方程有 4 个解.

$\alpha = 3$ 时, 同余方程 $x^2 \equiv 57 \mod 2^3$ 的解为 $\pm(1 + t_3 \cdot 2^2)$, $t_3 = 0, 1, \cdots$

$\alpha = 4$ 时, 令 $(1 + t_3 \cdot 2^2)^2 \equiv 57 \mod 2^4$, 可得 $t_3 \equiv \frac{57-1^2}{8} \equiv 1 \mod 2.$

故同余方程 $x^2 \equiv 57 \mod 2^4$ 的解为

$$\pm(1 + 1 \cdot 2^2 + t_4 \cdot 2^3) = \pm(5 + t_4 \cdot 2^3), \ t_4 = 0, 1, \cdots$$

$\alpha = 5$ 时, 令 $(5 + t_4 \cdot 2^3)^2 \equiv 57 \mod 2^5$, 可得 $t_4 \equiv \frac{57-5^2}{16} \equiv 0 \mod 2.$

故同余方程 $x^2 \equiv 57 \mod 2^5$ 的解为

$$\pm(5 + 0 \cdot 2^3 + t_5 \cdot 2^4) = \pm(5 + t_5 \cdot 2^4), \ t_5 = 0, 1, \cdots$$

**例 3.3.18** 求解同余方程 $x^2 \equiv 57 \mod 64$.

解：因为 $57 \equiv 1 \mod 8$, 所以同余方程有 4 个解.

$\alpha = 3$ 时, 同余方程 $x^2 \equiv 57 \mod 2^3$ 的解为 $\pm(1 + t_3 \cdot 2^2),\ t_3 = 0, 1, \cdots$

$\alpha = 4$ 时, 令 $(1 + t_3 \cdot 2^2)^2 \equiv 57 \mod 2^4$, 可得 $t_3 \equiv \frac{57-1^2}{8} \equiv 1 \mod 2$.

故同余方程 $x^2 \equiv 57 \mod 2^4$ 的解为

$$\pm(1 + 1 \cdot 2^2 + t_4 \cdot 2^3) = \pm(5 + t_4 \cdot 2^3),\ t_4 = 0, 1, \cdots$$

$\alpha = 5$ 时, 令 $(5 + t_4 \cdot 2^3)^2 \equiv 57 \mod 2^5$, 可得 $t_4 \equiv \frac{57-5^2}{16} \equiv 0 \mod 2$.

故同余方程 $x^2 \equiv 57 \mod 2^5$ 的解为

$$\pm(5 + 0 \cdot 2^3 + t_5 \cdot 2^4) = \pm(5 + t_5 \cdot 2^4),\ t_5 = 0, 1, \cdots$$

$\alpha = 6$ 时, 令 $(5 + t_5 \cdot 2^4)^2 \equiv 57 \mod 2^6$, 可得 $t_5 \equiv \frac{57-5^2}{32} \equiv 1 \mod 2$.

故同余方程 $x^2 \equiv 57 \mod 2^6$ 的解为

$$\pm(5 + 1 \cdot 2^4 + t_6 \cdot 2^5) = \pm(21 + t_6 \cdot 2^5),\ t_6 = 0, 1, \cdots$$

**例 3.3.18** 求解同余方程 $x^2 \equiv 57 \mod 64$.

解：因为 $57 \equiv 1 \mod 8$, 所以同余方程有 4 个解.

$\alpha = 3$ 时, 同余方程 $x^2 \equiv 57 \mod 2^3$ 的解为 $\pm(1 + t_3 \cdot 2^2)$, $t_3 = 0, 1, \cdots$

$\alpha = 4$ 时, 令 $(1 + t_3 \cdot 2^2)^2 \equiv 57 \mod 2^4$, 可得 $t_3 \equiv \frac{57-1^2}{8} \equiv 1 \mod 2$.

故同余方程 $x^2 \equiv 57 \mod 2^4$ 的解为

$$\pm(1 + 1 \cdot 2^2 + t_4 \cdot 2^3) = \pm(5 + t_4 \cdot 2^3),\ t_4 = 0, 1, \cdots$$

$\alpha = 5$ 时, 令 $(5 + t_4 \cdot 2^3)^2 \equiv 57 \mod 2^5$, 可得 $t_4 \equiv \frac{57-5^2}{16} \equiv 0 \mod 2$.

故同余方程 $x^2 \equiv 57 \mod 2^5$ 的解为

$$\pm(5 + 0 \cdot 2^3 + t_5 \cdot 2^4) = \pm(5 + t_5 \cdot 2^4),\ t_5 = 0, 1, \cdots$$

$\alpha = 6$ 时, 令 $(5 + t_5 \cdot 2^4)^2 \equiv 57 \mod 2^6$, 可得 $t_5 \equiv \frac{57-5^2}{32} \equiv 1 \mod 2$.

故同余方程 $x^2 \equiv 57 \mod 2^6$ 的解为

$$\pm(5 + 1 \cdot 2^4 + t_6 \cdot 2^5) = \pm(21 + t_6 \cdot 2^5),\ t_6 = 0, 1, \cdots$$

因此, 同余方程模 $64 = 2^6$ 的解是 $21, 53, -21 \equiv 43, -53 \equiv 11 \mod 64$.

# 目录

首先, 考虑如何将模正整数 $m = m_1 m_2 \cdots m_k$ 同余方程的求解转化为模 ($k$ 个两两互素的正整数) $m_i$ 同余方程的求解, 以及它们的解数关系.

首先, 考虑如何将模正整数 $m = m_1m_2\cdots m_k$ 同余方程的求解转化为模 ($k$ 个两两互素的正整数) $m_i$ 同余方程的求解, 以及它们的解数关系.

**定理 3.4.1**

设 $m_1,\cdots,m_k$ 是 $k$ 个两两互素的正整数, $m = m_1\cdots m_k$, 则同余方程 $f(x)\equiv 0 \mod m$ 与同余方程组

$$\begin{cases} f(x)\equiv 0 \mod m_1 \\ \quad\vdots \\ f(x)\equiv 0 \mod m_k \end{cases}$$

等价. 如果用 $T_i$ 表示同余方程 $f(x)\equiv 0 \mod m_i$ 的解数 $i=1,\cdots,k$, $T$ 表示同余方程 $f(x)\equiv 0 \mod m$ 的解数, 则 $T = T_1\cdots T_k$.

证：由中国剩余定理 (定理 3.2.1), 上述同余方程与同余方程组等价.

证：由中国剩余定理 (定理 3.2.1), 上述同余方程与同余方程组等价.

下面给出解数证明. 设同余方程 $f(x) \equiv 0 \mod m_i$ 的解是 $b_i$, $i = 1, \cdots, k$, 则由中国剩余定理 (定理 3.2.1), 可求得同余方程组

$$\begin{cases} x \equiv b_1 \mod m_1 \\ \vdots \\ x \equiv b_k \mod m_k \end{cases}$$

的解是 $x \equiv b_1 \cdot M_1' \cdot M_1 + \cdots + b_k \cdot M_k' \cdot M_k \mod m$.

因为 $f(x) \equiv f(b_i) \equiv 0 \mod m_i$, $i = 1, \cdots, k$, 所以 $x$ 也是 $f(x) \equiv 0 \mod m$ 的解. 故 $x$ 随 $b_i$ 遍历 $f(x) \equiv 0 \mod m_i$ 的所有解 $(i = 1, \cdots, k)$ 而遍历 $f(x) \equiv 0 \mod m$ 的所有解, 即

$$\begin{cases} f(x) \equiv 0 \mod m_1 \\ \vdots \\ f(x) \equiv 0 \mod m_k \end{cases}$$

的解数为 $T = T_1 \cdots T_k$.

**例 3.4.1** 求解同余式 $f(x) \equiv x^4 + 2x^3 + 8x + 9 \equiv 0 \mod 35.$

**例 3.4.1** 求解同余式 $f(x) \equiv x^4 + 2x^3 + 8x + 9 \equiv 0 \mod 35.$

解：由定理 3.4.1 知, 原同余方程等价于同余方程组

$$\begin{cases} f(x) \equiv 0 \mod 5, \\ f(x) \equiv 0 \mod 7. \end{cases}$$

**例 3.4.1** 求解同余式 $f(x) \equiv x^4 + 2x^3 + 8x + 9 \equiv 0 \mod 35$.

解：由定理 3.4.1 知, 原同余方程等价于同余方程组

$$\begin{cases} f(x) \equiv 0 \mod 5, \\ f(x) \equiv 0 \mod 7. \end{cases}$$

直接验算,

$f(x) \equiv 0 \mod 5$ 的解为 $x \equiv 1, 4 \mod 5$,

$f(x) \equiv 0 \mod 7$ 的解为 $x \equiv 3, 5, 6 \mod 7$.

根据中国剩余定理, 可求得同余方程组

$$\begin{cases} x \equiv b_1 \mod 5, \\ x \equiv b_2 \mod 7. \end{cases}$$

的解为 $x \equiv b_1 \cdot 3 \cdot 7 + b_2 \cdot 3 \cdot 5 \equiv b_1 \cdot 21 + b_2 \cdot 15 \mod 35$.

**例 3.4.1** 求解同余式 $f(x) \equiv x^4 + 2x^3 + 8x + 9 \equiv 0 \mod 35$.

解：由定理 3.4.1 知, 原同余方程等价于同余方程组

$$\begin{cases} f(x) \equiv 0 \mod 5, \\ f(x) \equiv 0 \mod 7. \end{cases}$$

直接验算,

$f(x) \equiv 0 \mod 5$ 的解为 $x \equiv 1, 4 \mod 5$,

$f(x) \equiv 0 \mod 7$ 的解为 $x \equiv 3, 5, 6 \mod 7$.

根据中国剩余定理, 可求得同余方程组

$$\begin{cases} x \equiv b_1 \mod 5, \\ x \equiv b_2 \mod 7. \end{cases}$$

的解为 $x \equiv b_1 \cdot 3 \cdot 7 + b_2 \cdot 3 \cdot 5 \equiv b_1 \cdot 21 + b_2 \cdot 15 \mod 35$. 故原同余方程的解为 $x \equiv 31, 26, 6, 24, 19, 34 \mod 35$, 共 $2 \cdot 3 = 6$ 个.

# 目录

现在我们考虑如何求解模素数 $p$ 的同余方程

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

其中 $a_n \not\equiv 0 \mod p$.

现在我们考虑如何求解模素数 $p$ 的同余方程

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

其中 $a_n \not\equiv 0 \mod p$.

首先, 考虑多项式欧几里德除法.

**引理 3.4.1 (多项式欧几里得除法)**

设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 为 $n$ 次整系数多项式, $g(x) = x^m + \cdots + b_1 x + b_0$ 为 $m \geqslant 1$ 次首一整系数多项式, 则存在整系数多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x) = q(x) \cdot g(x) + r(x), \ \deg r(x) < \deg g(x).$$

证：分以下两种情形讨论：

(i) $n < m$. 取 $q(x) = 0, r(x) = f(x)$, 结论成立.

现在我们考虑如何求解模素数 $p$ 的同余方程

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

其中 $a_n \not\equiv 0 \mod p$.

首先, 考虑多项式欧几里德除法.

**引理 3.4.1 (多项式欧几里得除法)**

设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$ 为 $n$ 次整系数多项式, $g(x) = x^m + \cdots + b_1 x + b_0$ 为 $m \geqslant 1$ 次首一整系数多项式, 则存在整系数多项式 $q(x)$ 和 $r(x)$ 使得

$$f(x) = q(x) \cdot g(x) + r(x), \ \deg r(x) < \deg g(x).$$

证：分以下两种情形讨论：

(i) $n < m$. 取 $q(x) = 0, r(x) = f(x)$, 结论成立.

(ii) $n \geqslant m$. 对 $f(x)$ 的次数 $n$ 作数学归纳法.

对于 $n=m$, 有

$$f(x)-a_n\cdot g(x)=(a_{n-1}-a_n\cdot b_{m-1})x^{n-1}+\cdots+(a_1-a_n\cdot b_1)x+(a_0-a_n\cdot b_0).$$

因此, $q(x)=a_n, r(x)=f(x)-a_n\cdot g(x)$ 即为所求.

对于 $n=m$, 有

$$f(x)-a_n\cdot g(x)=(a_{n-1}-a_n\cdot b_{m-1})x^{n-1}+\cdots+(a_1-a_n\cdot b_1)x+(a_0-a_n\cdot b_0).$$

因此, $q(x)=a_n, r(x)=f(x)-a_n\cdot g(x)$ 即为所求.

假设 $n-1\geqslant m$ 时, 结论成立.

对于 $n>m$, 有

$$f(x)-a_nx^{n-m}\cdot g(x)=(a_{n-1}-a_n\cdot b_{m-1})x^{n-1}+\cdots+(a_{n-m}-a_n\cdot b_0)x^{n-m}$$
$$+a_{n-m-1}x^{n-m-1}+\cdots+a_0.$$

这说明 $f(x)-a_nx^{n-m}\cdot g(x)$ 是次数小于等于 $n-1$ 的多项式. 对其运用归纳假设或情形 (i), 存在整系数多项式 $q_1(x)$ 和 $r_1(x)$ 使得

$$f(x)-a_nx^{n-m}\cdot g(x)=q_1(x)\cdot g(x)+r_1(x),\quad \deg r_1(x)<\deg g(x).$$

对于 $n = m$, 有

$$f(x) - a_n \cdot g(x) = (a_{n-1} - a_n \cdot b_{m-1})x^{n-1} + \cdots + (a_1 - a_n \cdot b_1)x + (a_0 - a_n \cdot b_0).$$

因此, $q(x) = a_n, r(x) = f(x) - a_n \cdot g(x)$ 即为所求.

假设 $n - 1 \geqslant m$ 时, 结论成立.

对于 $n > m$, 有

$$f(x) - a_n x^{n-m} \cdot g(x) = (a_{n-1} - a_n \cdot b_{m-1})x^{n-1} + \cdots + (a_{n-m} - a_n \cdot b_0)x^{n-m} + a_{n-m-1}x^{n-m-1} + \cdots + a_0.$$

这说明 $f(x) - a_n x^{n-m} \cdot g(x)$ 是次数小于等于 $n - 1$ 的多项式. 对其运用归纳假设或情形 (i), 存在整系数多项式 $q_1(x)$ 和 $r_1(x)$ 使得

$$f(x) - a_n x^{n-m} \cdot g(x) = q_1(x) \cdot g(x) + r_1(x), \quad \deg r_1(x) < \deg g(x).$$

因此, $q(x) = a_n x^{n-m} + q_1(x), r(x) = r_1(x)$ 即为所求.

根据数学归纳法原理, 结论成立.

其次, 由定理 2.2.14 (费马小定理), 多项式 $x^p - x \mod p$ 对任何整数取值为零, 所以借助于此以及多项式欧几里得除法, 可将高次多项式的求解转化为次数不超过 $p-1$ 的多项式的求解.

其次, 由定理 2.2.14 (费马小定理), 多项式 $x^p - x \mod p$ 对任何整数取值为零, 所以借助于此以及多项式欧几里得除法, 可将高次多项式的求解转化为次数不超过 $p-1$ 的多项式的求解.

**定理 3.4.2**

同余方程 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \mod p$ 与一个次数不超过 $p-1$ 的模 $p$ 的同余方程等价.

其次, 由定理 2.2.14 (费马小定理), 多项式 $x^p - x \mod p$ 对任何整数取值为零, 所以借助于此以及多项式欧几里得除法, 可将高次多项式的求解转化为次数不超过 $p-1$ 的多项式的求解.

**定理 3.4.2**

同余方程 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \mod p$ 与一个次数不超过 $p-1$ 的模 $p$ 的同余方程等价.

证：由多项式的欧几里德除法, 存在整系数多项式 $q(x), r(x)$ 使得

$$f(x) = q(x)(x^p - x) + r(x),$$

其中 $r(x)$ 的次数小于等于 $p-1$.

由定理 2.2.14 (费马小定理), 对任何整数 $x$, 都有 $x^p - x \equiv 0 \mod p$.

故同余方程 $f(x) \equiv 0 \mod p$ 等价于同余方程 $r(x) \equiv 0 \mod p$.

**例** 3.4.2 求与同余方程

$$f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \mod 5.$$

等价的次数小于 5 的同余方程.

**例 3.4.2** 求与同余方程

$$f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \mod 5.$$

等价的次数小于 5 的同余方程.

解：作多项式欧几里德除法, 我们有

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ = & (3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5)(x^5 - x) \\ & + (3x^3 + 16x^2 + 6x). \end{aligned}$$

**例 3.4.2** 求与同余方程

$$f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \mod 5.$$

等价的次数小于 5 的同余方程.

解：作多项式欧几里德除法, 我们有

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ = & (3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5)(x^5 - x) \\ & + (3x^3 + 16x^2 + 6x). \end{aligned}$$

所以, 原同余方程等价于

$$r(x) = 3x^3 + 16x^2 + 6x \equiv 3x^3 + x^2 + x \equiv 0 \mod 5.$$

再次, 考虑同余方程的解与一次同余方程的关系.

再次, 考虑同余方程的解与一次同余方程的关系.

### 定理 3.4.3

设 $1 \leqslant k \leqslant n$. 如果 $x \equiv x_i \mod p$, $i = 1, \cdots, k$, 是同余方程 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \mod p$ 的 $k$ 个不同解, 则对任何整数 $x$, 都有

$$f(x) \equiv f_k(x) \cdot (x - x_1) \cdot \quad \cdots \quad \cdot (x - x_k) \mod p,$$

其中 $f_k(x)$ 是 $n-k$ 次多项式, 首项系数是 $a_n$.

再次, 考虑同余方程的解与一次同余方程的关系.

**定理 3.4.3**

设 $1 \leqslant k \leqslant n$. 如果 $x \equiv x_i \mod p$, $i = 1, \cdots, k$, 是同余方程 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \mod p$ 的 $k$ 个不同解, 则对任何整数 $x$, 都有

$$f(x) \equiv f_k(x) \cdot (x - x_1) \cdot \quad \cdots \quad \cdot (x - x_k) \mod p,$$

其中 $f_k(x)$ 是 $n-k$ 次多项式, 首项系数是 $a_n$.

证：由多项式的欧几里德除法, 存在多项式 $f_1(x)$ 和 $r(x)$ 使得

$$f(x) = f_1(x) \cdot (x - x_1) + r(x),\ 0 = \deg r_(x) < \deg (x - x_1).$$

易知, $f_1(x)$ 的次数是 $n-1$, 首项系数是 $a_n, r(x) = r$ 为整数.

因为 $f(x_1) \equiv 0 \mod p$, 所以 $r \equiv 0 \mod p$, 即有

$$f(x) \equiv f_1(x) \cdot (x - x_1) \mod p.$$

因为 $f(x_1) \equiv 0 \mod p$, 所以 $r \equiv 0 \mod p$, 即有

$$f(x) \equiv f_1(x) \cdot (x - x_1) \mod p.$$

再由 $f(x_i) \equiv 0 \mod p$ 及 $x_i \not\equiv x_1 \mod p,\ i = 2, \cdots, k$ 得到

$$f_1(x_i) \equiv 0 \mod p,\ i = 2, \cdots, k.$$

因为 $f(x_1) \equiv 0 \mod p$, 所以 $r \equiv 0 \mod p$, 即有

$$f(x) \equiv f_1(x) \cdot (x - x_1) \mod p.$$

再由 $f(x_i) \equiv 0 \mod p$ 及 $x_i \not\equiv x_1 \mod p,\ i = 2, \cdots, k$ 得到

$$f_1(x_i) \equiv 0 \mod p,\ i = 2, \cdots, k.$$

类似地, 对于多项式 $f_1(x)$ 可找到多项式 $f_2(x)$ 使得

$$f_1(x) \equiv f_2(x) \cdot (x - x_2) \mod p, \quad 且 \quad f_2(x_i) \equiv 0 \mod p,\ i = 3, \cdots, k.$$

如此下去, 有

$$f_{k-1}(x) \equiv f_k(x) \cdot (x - x_k) \mod p.$$

因为 $f(x_1) \equiv 0 \mod p$, 所以 $r \equiv 0 \mod p$, 即有

$$f(x) \equiv f_1(x) \cdot (x - x_1) \mod p.$$

再由 $f(x_i) \equiv 0 \mod p$ 及 $x_i \not\equiv x_1 \mod p,\ i = 2, \cdots, k$ 得到

$$f_1(x_i) \equiv 0 \mod p,\ i = 2, \cdots, k.$$

类似地, 对于多项式 $f_1(x)$ 可找到多项式 $f_2(x)$ 使得

$$f_1(x) \equiv f_2(x) \cdot (x - x_2) \mod p, \quad 且 \quad f_2(x_i) \equiv 0 \mod p,\ i = 3, \cdots, k.$$

如此下去, 有

$$f_{k-1}(x) \equiv f_k(x) \cdot (x - x_k) \mod p.$$

故 $f(x) \equiv f_k(x) \cdot (x - x_1) \cdot \cdots \cdot (x - x_k) \mod p.$

**例 3.4.3** 我们有同余方程

$$\begin{aligned}&3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x\\=\ &x(x-1)(x-2)(3x^{11}+3x^{10}+3x^9+4x^7+3x^6+x^5+2x^4\\&+x^2+3x+3) \mod 5.\end{aligned}$$

根据定理 3.4.3 及定理 2.2.14 (费马小定理), 可以立即得到

**推论 3.4.1**

设 $p$ 是一个素数. 则

(i) 对任何整数 $x$, 有 $x^{p-1}-1\equiv(x-1)\cdots(x-(p-1)) \mod p$.

(ii) (Wilson 定理) $(p-1)!+1\equiv 0 \mod p$.

**例 3.4.3** 我们有同余方程

$$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x$$
$$=x(x-1)(x-2)(3x^{11}+3x^{10}+3x^9+4x^7+3x^6+x^5+2x^4$$
$$+x^2+3x+3) \mod 5.$$

根据定理 3.4.3 及定理 2.2.14 (费马小定理), 可以立即得到

**推论 3.4.1**

设 $p$ 是一个素数. 则

(i) 对任何整数 $x$, 有 $x^{p-1}-1\equiv(x-1)\cdots(x-(p-1)) \mod p$.

(ii) (Wilson 定理) $(p-1)!+1\equiv 0 \mod p$.

注：由 Wilson 定理, 可得到整数是否为素数的判别条件. 整数 $n$ 为素数的充要条件是 $(n-1)!+1\equiv 0 \mod n$.

最后, 讨论模 $p$ 同余方程的解数.

现在, 我们先给出同余方程解数的上界估计.

最后, 讨论模 $p$ 同余方程的解数.

现在, 我们先给出同余方程解数的上界估计.

**定理 3.4.4**

同余方程 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod p, a_n \not\equiv 0 \pmod p$ 的解数不超过它的次数.

最后, 讨论模 $p$ 同余方程的解数.

现在, 我们先给出同余方程解数的上界估计.

**定理 3.4.4**

同余方程 $f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0 \pmod p, a_n\not\equiv 0 \pmod p$ 的解数不超过它的次数.

证：反证法. 设同余方程 $f(x)=a_nx^n+\cdots+a_1x+a_0\equiv 0 \pmod p$ 的解数超过 $n$ 个, 则它至少有 $n+1$ 个解, 设它们为

$$x\equiv c_i \pmod p,\ \ i=1,\cdots,n,n+1.$$

最后, 讨论模 $p$ 同余方程的解数.

现在, 我们先给出同余方程解数的上界估计.

**定理 3.4.4**

同余方程 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \mod p, a_n \not\equiv 0 \mod p$ 的解数不超过它的次数.

证：反证法. 设同余方程 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \mod p$ 的解数超过 $n$ 个, 则它至少有 $n+1$ 个解, 设它们为

$$x \equiv c_i \mod p, \ i = 1, \cdots, n, n+1.$$

对于 $n$ 个解 $c_1, \cdots, c_n$, 可得到

$$f(x) \equiv (x - c_1) \cdots (x - c_n) f_n(x) \mod p.$$

因为 $f(c_{n+1}) \equiv 0 \mod p$, 所以

$$(c_{n+1} - c_1) \cdots (c_{n+1} - c_n) f_n(c_{n+1}) \equiv 0 \mod p.$$

又因为 $c_i \not\equiv c_{n+1} \pmod p$, $i = 1, \cdots, n$, 且 $p$ 是素数,
故 $f_n(c_{n+1}) \equiv 0 \pmod p$.
而 $f_n(x)$ 是首项系数为 $a_n \not\equiv 0 \pmod p$, 次数为 $n - n = 0$ 的多项式,
故 $p \mid a_n$, 矛盾.

**推论 3.4.2**

次数小于 $p$ 的整系数多项式对所有整数取值模 $p$ 为零的充要条件是其系数被 $p$ 整除.

又因为 $c_i \not\equiv c_{n+1} \mod p$, $i = 1, \cdots, n$, 且 $p$ 是素数,
故 $f_n(c_{n+1}) \equiv 0 \mod p$.
而 $f_n(x)$ 是首项系数为 $a_n \not\equiv 0 \mod p$, 次数为 $n - n = 0$ 的多项式,
故 $p \mid a_n$, 矛盾.

**推论 3.4.2**

次数小于 $p$ 的整系数多项式对所有整数取值模 $p$ 为零的充要条件是其系数被 $p$ 整除.

证: 充分性显然. 下证必要性.

若不然, 多项式 $f(x)$ 有某个系数不能被 $p$ 整除, 则 $f(x) \mod p$ 是一个首项系数 $\not\equiv 0 \mod p$ 且次数小于 $p$ 的多项式.

根据定理 3.4.4, 同余方程 $f(x) \equiv 0 \mod p$ 的解的个数小于 $p$, 这与题设条件 “对所有整数取值模 $p$ 为零”, 即有 $p$ 个解, 矛盾!

故结论成立.

再给出同余方程解数的判断.

**定理 3.4.5**

设 $p$ 是一个素数, $n$ 是一个正整数, $n \leqslant p$, 那么同余方程

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

有 $n$ 个解的充要条件是 $x^p - x$ 被 $f(x)$ 除所得余式的所有系数都是 $p$ 的倍数.

再给出同余方程解数的判断.

**定理 3.4.5**

设 $p$ 是一个素数, $n$ 是一个正整数, $n \leqslant p$, 那么同余方程

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

有 $n$ 个解的充要条件是 $x^p - x$ 被 $f(x)$ 除所得余式的所有系数都是 $p$ 的倍数.

证：必要性. 因为 $f(x)$ 是首一多项式, 由多项式的欧几里得除法知, 存在整系数多项式 $q(x)$ 和 $r(x)$ 使得

$$x^p - x = q(x) \cdot f(x) + r(x)$$

其中 $r(x)$ 的次数小于 $n$, $q(x)$ 的次数是 $p - n$.

再给出同余方程解数的判断.

**定理 3.4.5**

设 $p$ 是一个素数, $n$ 是一个正整数, $n \leqslant p$, 那么同余方程

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

有 $n$ 个解的充要条件是 $x^p - x$ 被 $f(x)$ 除所得余式的所有系数都是 $p$ 的倍数.

证：必要性. 因为 $f(x)$ 是首一多项式, 由多项式的欧几里得除法知, 存在整系数多项式 $q(x)$ 和 $r(x)$ 使得

$$x^p - x = q(x) \cdot f(x) + r(x)$$

其中 $r(x)$ 的次数小于 $n$, $q(x)$ 的次数是 $p - n$.

若同余方程 $f(x) = x^n + \cdots + a_1 x + a_0 \equiv 0 \mod p$ 有 $n$ 个解, 则由定理 2.2.14 (费马小定理), 这 $n$ 个解都是 $x^p - x \equiv 0 \mod p$ 的解.

又由 $x^p - x = q(x) \cdot f(x) + r(x)$ 知,
这 $n$ 个解也是 $r(x) \equiv 0 \mod p$ 的解.
但 $r(x)$ 的次数小于 $n$, 由推论 3.4.2 知, $r(x)$ 的系数都是 $p$ 的倍数.

又由 $x^p - x = q(x) \cdot f(x) + r(x)$ 知,
这 $n$ 个解也是 $r(x) \equiv 0 \mod p$ 的解.
但 $r(x)$ 的次数小于 $n$, 由推论 3.4.2 知, $r(x)$ 的系数都是 $p$ 的倍数.
充分性. 若多项式 $r(x)$ 的系数都被 $p$ 整除, 则由推论 3.4.2 知,
$r(x)$ 对所有整数 $x$ 取值模 $p$ 为零.
根据定理 2.2.14 (费马小定理), 对任何整数 $x$, 有 $x^p - x \equiv 0 \mod p$.
因此, 对任何整数 $x$, 有 $q(x) \cdot f(x) \equiv 0 \mod p$, 即有 $p$ 个不同的解

$$x \equiv 0, 1, \cdots, p-1 \mod p.$$

又由 $x^p - x = q(x) \cdot f(x) + r(x)$ 知,
这 $n$ 个解也是 $r(x) \equiv 0 \mod p$ 的解.
但 $r(x)$ 的次数小于 $n$, 由推论 3.4.2 知, $r(x)$ 的系数都是 $p$ 的倍数.
充分性. 若多项式 $r(x)$ 的系数都被 $p$ 整除, 则由推论 3.4.2 知,
$r(x)$ 对所有整数 $x$ 取值模 $p$ 为零.
根据定理 2.2.14 (费马小定理), 对任何整数 $x$, 有 $x^p - x \equiv 0 \mod p$.
因此, 对任何整数 $x$, 有 $q(x) \cdot f(x) \equiv 0 \mod p$, 即有 $p$ 个不同的解

$$x \equiv 0, 1, \cdots, p-1 \mod p.$$

由此可得 $f(x) \equiv 0 \mod p$ 的解数 $k = n$. 若不然, $k < n$.

又由 $x^p - x = q(x)\cdot f(x) + r(x)$ 知,
这 $n$ 个解也是 $r(x) \equiv 0 \mod p$ 的解.
但 $r(x)$ 的次数小于 $n$, 由推论 3.4.2 知, $r(x)$ 的系数都是 $p$ 的倍数.
充分性. 若多项式 $r(x)$ 的系数都被 $p$ 整除, 则由推论 3.4.2 知,
$r(x)$ 对所有整数 $x$ 取值模 $p$ 为零.
根据定理 2.2.14 (费马小定理), 对任何整数 $x$, 有 $x^p - x \equiv 0 \mod p$.
因此, 对任何整数 $x$, 有 $q(x)\cdot f(x) \equiv 0 \mod p$, 即有 $p$ 个不同的解

$$x \equiv 0, 1, \cdots, p-1 \mod p.$$

由此可得 $f(x) \equiv 0 \mod p$ 的解数 $k = n$. 若不然, $k < n$.
又次数为 $p-n$ 的多项式 $q(x)$ 的同余方程 $q(x) \equiv 0 \mod p$ 的解数
$h \leqslant p-n$, 所以 $q(x)\cdot f(x) \equiv 0 \mod p$ 的解数小于等于 $k+h < p$,
矛盾.

**推论 3.4.3**

设 $p$ 是一个素数, $d$ 是 $p-1$ 的正因数, 则多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

**推论 3.4.3**

设 $p$ 是一个素数, $d$ 是 $p-1$ 的正因数, 则多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

证：因为 $d \mid p-1$, 所以存在整数 $q$ 使得 $p-1=q\cdot d$. 这样, 有因式分解

$$x^{p-1}-1=(x^d)^p-1=(x^{d(p-1)}+x^{d(p-2)}+\cdots+x^d+1)(x^d-1)+p\cdot 0.$$

根据定理 3.4.5, 多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

**推论 3.4.3**

设 $p$ 是一个素数, $d$ 是 $p-1$ 的正因数, 则多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

证：因为 $d \mid p-1$, 所以存在整数 $q$ 使得 $p-1=q\cdot d$. 这样, 有因式分解

$$x^{p-1}-1=(x^d)^p-1=(x^{d(p-1)}+x^{d(p-2)}+\cdots+x^d+1)(x^d-1)+p\cdot 0.$$

根据定理 3.4.5, 多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

**例 3.4.4** 判断同余方程 $2x^3+5x^2+6x+1\equiv 0 \mod 7$ 是否有三个解.

**推论 3.4.3**

设 $p$ 是一个素数, $d$ 是 $p-1$ 的正因数, 则多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

证：因为 $d \mid p-1$, 所以存在整数 $q$ 使得 $p-1=q\cdot d$. 这样, 有因式分解

$$x^{p-1}-1=(x^d)^p-1=(x^{d(p-1)}+x^{d(p-2)}+\cdots+x^d+1)(x^d-1)+p\cdot 0.$$

根据定理 3.4.5, 多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

**例 3.4.4** 判断同余方程 $2x^3+5x^2+6x+1\equiv 0 \mod 7$ 是否有三个解.

解：首先, 需将多项式变成首一的. 注意到 $4\cdot 2\equiv 1 \mod 7$, 我们有

$$4(2x^3+5x^2+6x+1)\equiv x^3-x^2+3x-3 \mod 7.$$

**推论 3.4.3**

设 $p$ 是一个素数, $d$ 是 $p-1$ 的正因数, 则多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

证：因为 $d \mid p-1$, 所以存在整数 $q$ 使得 $p-1=q\cdot d$. 这样, 有因式分解

$$x^{p-1}-1=(x^d)^p-1=(x^{d(p-1)}+x^{d(p-2)}+\cdots+x^d+1)(x^d-1)+p\cdot 0.$$

根据定理 3.4.5, 多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

**例 3.4.4** 判断同余方程 $2x^3+5x^2+6x+1\equiv 0 \mod 7$ 是否有三个解.

解：首先, 需将多项式变成首一的. 注意到 $4\cdot 2\equiv 1 \mod 7$, 我们有

$$4(2x^3+5x^2+6x+1)\equiv x^3-x^2+3x-3 \mod 7.$$

此同余方程与原同余方程等价. 作多项式的欧几里德除法, 我们有

$$x^7-x=x(x^3+x^2-2x-2)\cdot(x^3-x^2+3x-3)+7x(x^2-1).$$

**推论 3.4.3**

设 $p$ 是一个素数, $d$ 是 $p-1$ 的正因数, 则多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

证：因为 $d \mid p-1$, 所以存在整数 $q$ 使得 $p-1=q\cdot d$. 这样, 有因式分解

$$x^{p-1}-1=(x^d)^p-1=(x^{d(p-1)}+x^{d(p-2)}+\cdots+x^d+1)(x^d-1)+p\cdot 0.$$

根据定理 3.4.5, 多项式 $x^d-1$ 模 $p$ 有 $d$ 个不同的根.

**例** 3.4.4 判断同余方程 $2x^3+5x^2+6x+1\equiv 0 \mod 7$ 是否有三个解.

解：首先, 需将多项式变成首一的. 注意到 $4\cdot 2\equiv 1 \mod 7$, 我们有

$$4(2x^3+5x^2+6x+1)\equiv x^3-x^2+3x-3 \mod 7.$$

此同余方程与原同余方程等价. 作多项式的欧几里德除法, 我们有

$$x^7-x=x(x^3+x^2-2x-2)\cdot(x^3-x^2+3x-3)+7x(x^2-1).$$

根据定理 3.4.5, 原同余式的解数是 3.

例 3.4.5 求解同余方程 $21x^{18} + 2x^{15} - x^{10} + 4x - 3 \equiv 0 \mod 7$.

**例 3.4.5** 求解同余方程 $21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0 \mod 7.$

解：首先, 去掉系数为 7 的倍数的项, 得到

$$2x^{15}-x^{10}+4x-3\equiv 0 \mod 7.$$

**例 3.4.5** 求解同余方程 $21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0 \mod 7$.

解：首先, 去掉系数为 7 的倍数的项, 得到

$$2x^{15}-x^{10}+4x-3\equiv 0 \mod 7.$$

其次, 作多项式的欧几里德除法, 我们有

$$2x^{15}-x^{10}+4x-3=(2x^8-x^3+2x^2)(x^7-x)+(-x^4+2x^3+4x-3).$$

**例 3.4.5** 求解同余方程 $21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0 \mod 7$.

解：首先, 去掉系数为 7 的倍数的项, 得到

$$2x^{15}-x^{10}+4x-3\equiv 0 \mod 7.$$

其次, 作多项式的欧几里德除法, 我们有

$$2x^{15}-x^{10}+4x-3=(2x^8-x^3+2x^2)(x^7-x)+(-x^4+2x^3+4x-3).$$

故原同余方程等价于同余方程

$$x^4-2x^3-4x+3\equiv 0 \mod 7.$$

**例 3.4.5** 求解同余方程 $21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0 \mod 7$.

解：首先, 去掉系数为 7 的倍数的项, 得到

$$2x^{15}-x^{10}+4x-3\equiv 0 \mod 7.$$

其次, 作多项式的欧几里德除法, 我们有

$$2x^{15}-x^{10}+4x-3=(2x^8-x^3+2x^2)(x^7-x)+(-x^4+2x^3+4x-3).$$

故原同余方程等价于同余方程

$$x^4-2x^3-4x+3\equiv 0 \mod 7.$$

直接验算

$$x=0,\pm1,\pm2,\pm3\ \ (\text{或}\ \ 0,1,2,3,4,5,6)$$

都不是上述同余方程的解.

**例 3.4.5** 求解同余方程 $21x^{18} + 2x^{15} - x^{10} + 4x - 3 \equiv 0 \mod 7$.

解：首先, 去掉系数为 7 的倍数的项, 得到

$$2x^{15} - x^{10} + 4x - 3 \equiv 0 \mod 7.$$

其次, 作多项式的欧几里德除法, 我们有

$$2x^{15} - x^{10} + 4x - 3 = (2x^8 - x^3 + 2x^2)(x^7 - x) + (-x^4 + 2x^3 + 4x - 3).$$

故原同余方程等价于同余方程

$$x^4 - 2x^3 - 4x + 3 \equiv 0 \mod 7.$$

直接验算

$$x = 0, \pm 1, \pm 2, \pm 3 \ (\text{或} \ \ 0, 1, 2, 3, 4, 5, 6)$$

都不是上述同余方程的解.

故原同余方程无解.

**例 3.4.6** 求解同余方程

$$f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \mod 5.$$

**例** 3.4.6 求解同余方程

$$f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \mod 5.$$

解：方法一. 作多项式欧几里德除法, 我们有

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ = & (3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5)(x^5 - x) \\ & + (3x^3 + 16x^2 + 6x). \end{aligned}$$

**例 3.4.6** 求解同余方程

$$f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \mod 5.$$

解：方法一. 作多项式欧几里德除法, 我们有

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ = & (3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5)(x^5 - x) \\ & + (3x^3 + 16x^2 + 6x). \end{aligned}$$

原同余方程等价于 $3x^3 + 16x^2 + 6x \equiv 3x^3 + x^2 + x \equiv 0 \mod 5$.

直接验算, 解为 $x \equiv 0, 1, 2 \mod 5$.

**例 3.4.6** 求解同余方程

$$f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \mod 5.$$

解：方法一. 作多项式欧几里德除法, 我们有

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ = & (3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5)(x^5 - x) \\ & + (3x^3 + 16x^2 + 6x). \end{aligned}$$

原同余方程等价于 $3x^3 + 16x^2 + 6x \equiv 3x^3 + x^2 + x \equiv 0 \mod 5$.

直接验算, 解为 $x \equiv 0, 1, 2 \mod 5$.

方法二. 由恒等同余方程 $x^p - x \equiv 0 \mod p$ 可得,

对于任意正整数 $t, k$, $x^{t+k(p-1)} \equiv x^t \mod p$. 特别 $(p = 5)$,

$x^{14} \equiv x^{10} \equiv x^6 \equiv x^2$, $x^{13} \equiv x^9 \equiv x^5 \equiv x$, $x^{11} \equiv x^7 \equiv x^3 \mod 5$.

**例 3.4.6** 求解同余方程

$$f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod 5.$$

解：方法一. 作多项式欧几里德除法, 我们有

$$\begin{aligned}&3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ = &(3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5)(x^5 - x) \\ &+ (3x^3 + 16x^2 + 6x).\end{aligned}$$

原同余方程等价于 $3x^3 + 16x^2 + 6x \equiv 3x^3 + x^2 + x \equiv 0 \pmod 5$.

直接验算, 解为 $x \equiv 0, 1, 2 \pmod 5$.

方法二. 由恒等同余方程 $x^p - x \equiv 0 \pmod p$ 可得,

对于任意正整数 $t, k$, $x^{t+k(p-1)} \equiv x^t \pmod p$. 特别 $(p = 5)$,

$x^{14} \equiv x^{10} \equiv x^6 \equiv x^2$, $x^{13} \equiv x^9 \equiv x^5 \equiv x$, $x^{11} \equiv x^7 \equiv x^3 \pmod 5$.

因此, 原同余方程等价于 $3x^3 + 16x^2 + 6x \equiv 0 \pmod 5$.

进而等价于 $2(3x^3 + 16x^2 + 6x) \equiv x^3 - 3x^2 + 2x \equiv 0 \pmod 5$.

**例 3.4.6** 求解同余方程

$$f(x) = 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \mod 5.$$

解：方法一. 作多项式欧几里德除法, 我们有

$$\begin{aligned} & 3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \\ = & (3x^9 + 4x^8 + 2x^6 + 3x^5 + 5x^4 + 2x^2 + 4x + 5)(x^5 - x) \\ & + (3x^3 + 16x^2 + 6x). \end{aligned}$$

原同余方程等价于 $3x^3 + 16x^2 + 6x \equiv 3x^3 + x^2 + x \equiv 0 \mod 5.$

直接验算, 解为 $x \equiv 0, 1, 2 \mod 5.$

方法二. 由恒等同余方程 $x^p - x \equiv 0 \mod p$ 可得,

对于任意正整数 $t, k,\ x^{t+k(p-1)} \equiv x^t \mod p$. 特别 $(p = 5)$,

$x^{14} \equiv x^{10} \equiv x^6 \equiv x^2,\ x^{13} \equiv x^9 \equiv x^5 \equiv x,\ x^{11} \equiv x^7 \equiv x^3 \mod 5.$

因此, 原同余方程等价于 $3x^3 + 16x^2 + 6x \equiv 0 \mod 5.$

进而等价于 $2(3x^3 + 16x^2 + 6x) \equiv x^3 - 3x^2 + 2x \equiv 0 \mod 5.$

直接验算, 同余方程的解为 $x \equiv 0, 1, 2 \mod 5.$

# 目录

因为任一正整数 $m$ 有标准分解式 $m = \prod_p p^\alpha$, 由定理 3.4.1 知,
求解同余方程 $f(x) \equiv 0 \mod m$ 只需求解同余方程 $f(x) \equiv 0 \mod p^\alpha$.
因此, 我们讨论 $p$ 为素数时, 同余方程 $f(x) \equiv 0 \mod p^\alpha$ 的解法.

因为任一正整数 $m$ 有标准分解式 $m = \prod_{p} p^{\alpha}$, 由定理 3.4.1 知,
求解同余方程 $f(x) \equiv 0 \mod m$ 只需求解同余方程 $f(x) \equiv 0 \mod p^{\alpha}$.
因此, 我们讨论 $p$ 为素数时, 同余方程 $f(x) \equiv 0 \mod p^{\alpha}$ 的解法.
设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ 为整系数多项式,
记 $f'(x) = n \cdot a_n x^{n-1} + (n-1) \cdot a_{n-1} x^{n-2} + \cdots + 2 \cdot a_2 x + a_1$,
称 $f'(x)$ 为 $f(x)$ 的导式.

因为任一正整数 $m$ 有标准分解式 $m = \prod_p p^\alpha$, 由定理 3.4.1 知,
求解同余方程 $f(x) \equiv 0 \mod m$ 只需求解同余方程 $f(x) \equiv 0 \mod p^\alpha$.
因此, 我们讨论 $p$ 为素数时, 同余方程 $f(x) \equiv 0 \mod p^\alpha$ 的解法.
设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ 为整系数多项式,
记 $f'(x) = n \cdot a_n x^{n-1} + (n-1) \cdot a_{n-1}x^{n-2} + \cdots + 2 \cdot a_2 x + a_1$,
称 $f'(x)$ 为 $f(x)$ 的导式.

**定理 3.4.6**

设 $x \equiv x_1 \mod p$ 是同余方程 $f(x) \equiv 0 \mod p$ 的一个解, 且 $(f'(x), p) = 1$, 则同余方程 $f(x) \equiv 0 \mod p^\alpha$ 有解 $x \equiv x_\alpha \mod p^\alpha$, 其中 $x_\alpha$ 由下面关系式递归得到:

$$\begin{cases} x_i \equiv x_{i-1} + t_{i-1} \cdot p^{i-1} \mod p^i, \\ t_{i-1} \equiv \frac{-f(x_{i-1})}{p^{i-1}} \cdot (f'(x_1)^{-1} \mod p) \mod p, \end{cases}$$

$i = 2, \cdots, \alpha$.

证：对 $\alpha \geqslant 2$ 作数学归纳法.

证：对 $\alpha \geqslant 2$ 作数学归纳法.

当 $\alpha = 2$ 时, 根据假设条件, 同余方程 $f(x) \equiv 0 \mod p$ 有解

$$x = x_1 + t_1 \cdot p, \quad t_1 = 0, \pm 1, \pm 2, \cdots .$$

所以, 考虑关于 $t_1$ 的同余式 $f(x_1 + t_1 \cdot p) \equiv 0 \mod p^2$ 的求解.

证：对 $\alpha \geqslant 2$ 作数学归纳法.

当 $\alpha = 2$ 时, 根据假设条件, 同余方程 $f(x) \equiv 0 \mod p$ 有解

$$x = x_1 + t_1 \cdot p,\ \ t_1 = 0, \pm 1, \pm 2, \cdots .$$

所以, 考虑关于 $t_1$ 的同余式 $f(x_1 + t_1 \cdot p) \equiv 0 \mod p^2$ 的求解.

由泰勒公式, 我们有 $f(x_1) + f'(x_1)(t_1 \cdot p) \equiv 0 \mod p^2$.

证：对 $\alpha \geqslant 2$ 作数学归纳法.

当 $\alpha = 2$ 时, 根据假设条件, 同余方程 $f(x) \equiv 0 \mod p$ 有解

$$x = x_1 + t_1 \cdot p,\ \ t_1 = 0, \pm 1, \pm 2, \cdots .$$

所以, 考虑关于 $t_1$ 的同余式 $f(x_1 + t_1 \cdot p) \equiv 0 \mod p^2$ 的求解.

由泰勒公式, 我们有 $f(x_1) + f'(x_1)(t_1 \cdot p) \equiv 0 \mod p^2$.

因为 $f(x_1) \equiv 0 \mod p$, 所以上述同余方程可写成

$$f'(x_1) \cdot t_1 \equiv \frac{-f(x_1)}{p} \mod p.$$

证：对 $\alpha \geqslant 2$ 作数学归纳法.

当 $\alpha = 2$ 时, 根据假设条件, 同余方程 $f(x) \equiv 0 \mod p$ 有解

$$x = x_1 + t_1 \cdot p, \quad t_1 = 0, \pm 1, \pm 2, \cdots .$$

所以, 考虑关于 $t_1$ 的同余式 $f(x_1 + t_1 \cdot p) \equiv 0 \mod p^2$ 的求解.

由泰勒公式, 我们有 $f(x_1) + f'(x_1)(t_1 \cdot p) \equiv 0 \mod p^2$.

因为 $f(x_1) \equiv 0 \mod p$, 所以上述同余方程可写成

$$f'(x_1) \cdot t_1 \equiv \frac{-f(x_1)}{p} \mod p.$$

又因为 $(f'(x_1), p) = 1$, 根据定理 3.1.3, 这个同余方程对模 $p$ 有且仅有一解

$$t_1 \equiv \frac{-f(x_1)}{p}(f'(x_1)^{-1} \mod p) \mod p.$$

即 $x \equiv x_2 \equiv x_1 + t_1 \cdot p \mod p^2$ 是同余方程 $f(x) \equiv 0 \mod p^2$ 的解.

故 $\alpha = 2$ 时结论成立.

证：对 $\alpha \geqslant 2$ 作数学归纳法.

当 $\alpha = 2$ 时, 根据假设条件, 同余方程 $f(x) \equiv 0 \mod p$ 有解

$$x = x_1 + t_1 \cdot p,\ \ t_1 = 0, \pm 1, \pm 2, \cdots .$$

所以, 考虑关于 $t_1$ 的同余式 $f(x_1 + t_1 \cdot p) \equiv 0 \mod p^2$ 的求解.

由泰勒公式, 我们有 $f(x_1) + f'(x_1)(t_1 \cdot p) \equiv 0 \mod p^2$.

因为 $f(x_1) \equiv 0 \mod p$, 所以上述同余方程可写成

$$f'(x_1) \cdot t_1 \equiv \frac{-f(x_1)}{p} \mod p.$$

又因为 $(f'(x_1), p) = 1$, 根据定理 3.1.3, 这个同余方程对模 $p$ 有且仅有一解

$$t_1 \equiv \frac{-f(x_1)}{p}(f'(x_1)^{-1} \mod p) \mod p.$$

即 $x \equiv x_2 \equiv x_1 + t_1 \cdot p \mod p^2$ 是同余方程 $f(x) \equiv 0 \mod p^2$ 的解.

故 $\alpha = 2$ 时结论成立.

假设对 $i - 1,\ 3 \leqslant i \leqslant \alpha$ 结论成立, 即同余方程

$f(x) \equiv 0 \mod p^{i-1}$ 有解 $x = x_{i-1} + t_{i-1} \cdot p^{i-1}$, $t_{i-1} = 0, \pm 1, \pm 2, \cdots$ .

考虑关于 $t_{i-1}$ 的同余方程 $f(x_{i-1} + t_{i-1} \cdot p^{i-1}) \equiv 0 \mod p^i$ 的求解.

$f(x) \equiv 0 \mod p^{i-1}$ 有解 $x = x_{i-1} + t_{i-1} \cdot p^{i-1}$, $t_{i-1} = 0, \pm1, \pm2, \cdots$ .
考虑关于 $t_{i-1}$ 的同余方程 $f(x_{i-1} + t_{i-1} \cdot p^{i-1}) \equiv 0 \mod p^i$ 的求解.
由泰勒公式及 $p^{2(i-1)} \geqslant p^i$, 我们有

$$f(x_{i-1}) + f'(x_{i-1})(t_{i-1} \cdot p^{i-1}) \equiv 0 \mod p^i.$$

因为 $f(x_{i-1}) \equiv 0 \mod p^{i-1}$, 所以上述同余方程可写成

$$f'(x_{i-1}) \cdot t_{i-1} \equiv \frac{-f(x_{i-1})}{p^{i-1}} \mod p.$$

$f(x) \equiv 0 \mod p^{i-1}$ 有解 $x = x_{i-1} + t_{i-1} \cdot p^{i-1}$, $t_{i-1} = 0, \pm 1, \pm 2, \cdots$ .
考虑关于 $t_{i-1}$ 的同余方程 $f(x_{i-1} + t_{i-1} \cdot p^{i-1}) \equiv 0 \mod p^i$ 的求解.
由泰勒公式及 $p^{2(i-1)} \geqslant p^i$, 我们有

$$f(x_{i-1}) + f'(x_{i-1})(t_{i-1} \cdot p^{i-1}) \equiv 0 \mod p^i.$$

因为 $f(x_{i-1}) \equiv 0 \mod p^{i-1}$, 所以上述同余方程可写成

$$f'(x_{i-1}) \cdot t_{i-1} \equiv \frac{-f(x_{i-1})}{p^{i-1}} \mod p.$$

又因为 $f'(x_{i-1}) \equiv f'(x_{i-2}) \equiv \cdots \equiv f'(x_1) \mod p$,
进而 $(f'(x_{i-1}), p) = \cdots = (f'(x_1), p) = 1$.

$f(x) \equiv 0 \mod p^{i-1}$ 有解 $x = x_{i-1} + t_{i-1} \cdot p^{i-1}$, $t_{i-1} = 0, \pm 1, \pm 2, \cdots$ .
考虑关于 $t_{i-1}$ 的同余方程 $f(x_{i-1} + t_{i-1} \cdot p^{i-1}) \equiv 0 \mod p^i$ 的求解.
由泰勒公式及 $p^{2(i-1)} \geqslant p^i$, 我们有

$$f(x_{i-1}) + f'(x_{i-1})(t_{i-1} \cdot p^{i-1}) \equiv 0 \mod p^i.$$

因为 $f(x_{i-1}) \equiv 0 \mod p^{i-1}$, 所以上述同余方程可写成

$$f'(x_{i-1}) \cdot t_{i-1} \equiv \frac{-f(x_{i-1})}{p^{i-1}} \mod p.$$

又因为 $f'(x_{i-1}) \equiv f'(x_{i-2}) \equiv \cdots \equiv f'(x_1) \mod p$,
进而 $(f'(x_{i-1}), p) = \cdots = (f'(x_1), p) = 1$.
根据定理 3.1.3, 这个同余方程对模 $p$ 有且仅有一解

$$\begin{aligned} t_{i-1} &\equiv \frac{-f(x_{i-1})}{p^{i-1}} (f'(x_{i-1})^{-1} \mod p) \\ &\equiv \frac{-f(x_{i-1})}{p^{i-1}} (f'(x_1)^{-1} \mod p) \mod p, \end{aligned}$$

即 $x \equiv x_i \equiv x_{i-1} + t_{i-1} \cdot p^{i-1} \mod p^i$ 是 $f(x) \equiv 0 \mod p^i$ 的解.
结论成立.

**例 3.4.7** 求解同余方程 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \mod 27$.

**例** 3.4.7 求解同余方程 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \mod 27$.

解：方法一. 由定理 3.4.6 证明过程,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

**例 3.4.7** 求解同余方程 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \mod 27$.

解：方法一. 由定理 3.4.6 证明过程,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

以 $x = 1 + t_1 \cdot 3$ 代入同余方程 $f(x) \equiv 0 \mod 9$, 可得到

$$f(1) + f'(1) \cdot t_1 \cdot 3 \equiv 0 \mod 9.$$

**例 3.4.7** 求解同余方程 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \mod 27$.

解：方法一. 由定理 3.4.6 证明过程,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

以 $x = 1 + t_1 \cdot 3$ 代入同余方程 $f(x) \equiv 0 \mod 9$, 可得到

$$f(1) + f'(1) \cdot t_1 \cdot 3 \equiv 0 \mod 9.$$

因为 $f(1) \equiv 3 \mod 9$, $f'(1) \equiv 2 \mod 9$, 则将上述同余方程写成 $3 + 2 \cdot t_1 \cdot 3 \equiv 0 \mod 9$, 即 $2 \cdot t_1 \equiv -1 \mod 3$, 解得 $t_1 \equiv 1 \mod 3$.

**例 3.4.7** 求解同余方程 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \mod 27$.

解：方法一. 由定理 3.4.6 证明过程,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

以 $x = 1 + t_1 \cdot 3$ 代入同余方程 $f(x) \equiv 0 \mod 9$, 可得到

$$f(1) + f'(1) \cdot t_1 \cdot 3 \equiv 0 \mod 9.$$

因为 $f(1) \equiv 3 \mod 9$, $f'(1) \equiv 2 \mod 9$, 则将上述同余方程写成 $3 + 2 \cdot t_1 \cdot 3 \equiv 0 \mod 9$, 即 $2 \cdot t_1 \equiv -1 \mod 3$, 解得 $t_1 \equiv 1 \mod 3$.

故同余方程 $f(x) \equiv 0 \mod 9$ 的解为 $x_2 \equiv 1 + t_1 \cdot 3 \equiv 4 \mod 9$.

**例** 3.4.7 求解同余方程 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \mod 27$.

解：方法一. 由定理 3.4.6 证明过程,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

以 $x = 1 + t_1 \cdot 3$ 代入同余方程 $f(x) \equiv 0 \mod 9$, 可得到

$$f(1) + f'(1) \cdot t_1 \cdot 3 \equiv 0 \mod 9.$$

因为 $f(1) \equiv 3 \mod 9$, $f'(1) \equiv 2 \mod 9$, 则将上述同余方程写成 $3 + 2 \cdot t_1 \cdot 3 \equiv 0 \mod 9$, 即 $2 \cdot t_1 \equiv -1 \mod 3$, 解得 $t_1 \equiv 1 \mod 3$.

故同余方程 $f(x) \equiv 0 \mod 9$ 的解为 $x_2 \equiv 1 + t_1 \cdot 3 \equiv 4 \mod 9$.

再以 $x = 4 + t_2 \cdot 9$ 代入同余方程 $f(x) \equiv 0 \mod 27$, 可得到

$$f(4) + f'(4) \cdot t_2 \cdot 9 \equiv 0 \mod 27.$$

**例 3.4.7** 求解同余方程 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \mod 27$.

解：方法一. 由定理 3.4.6 证明过程,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

以 $x = 1 + t_1 \cdot 3$ 代入同余方程 $f(x) \equiv 0 \mod 9$, 可得到

$$f(1) + f'(1) \cdot t_1 \cdot 3 \equiv 0 \mod 9.$$

因为 $f(1) \equiv 3 \mod 9$, $f'(1) \equiv 2 \mod 9$, 则将上述同余方程写成 $3 + 2 \cdot t_1 \cdot 3 \equiv 0 \mod 9$, 即 $2 \cdot t_1 \equiv -1 \mod 3$, 解得 $t_1 \equiv 1 \mod 3$.

故同余方程 $f(x) \equiv 0 \mod 9$ 的解为 $x_2 \equiv 1 + t_1 \cdot 3 \equiv 4 \mod 9$.

再以 $x = 4 + t_2 \cdot 9$ 代入同余方程 $f(x) \equiv 0 \mod 27$, 可得到

$$f(4) + f'(4) \cdot t_2 \cdot 9 \equiv 0 \mod 27.$$

因为 $f(4) \equiv 18 \mod 27$, $f'(4) \equiv 20 \mod 27$, 则将上述同余方程写成 $18 + 20 \cdot t_2 \cdot 9 \equiv 0 \mod 27$, 即 $2 \cdot t_2 \equiv -2 \mod 3$, 解得 $t_2 \equiv 2 \mod 3$.

**例 3.4.7** 求解同余方程 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \mod 27$.

解：方法一. 由定理 3.4.6 证明过程,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

以 $x = 1 + t_1 \cdot 3$ 代入同余方程 $f(x) \equiv 0 \mod 9$, 可得到

$$f(1) + f'(1) \cdot t_1 \cdot 3 \equiv 0 \mod 9.$$

因为 $f(1) \equiv 3 \mod 9$, $f'(1) \equiv 2 \mod 9$, 则将上述同余方程写成 $3 + 2 \cdot t_1 \cdot 3 \equiv 0 \mod 9$, 即 $2 \cdot t_1 \equiv -1 \mod 3$, 解得 $t_1 \equiv 1 \mod 3$.

故同余方程 $f(x) \equiv 0 \mod 9$ 的解为 $x_2 \equiv 1 + t_1 \cdot 3 \equiv 4 \mod 9$.

再以 $x = 4 + t_2 \cdot 9$ 代入同余方程 $f(x) \equiv 0 \mod 27$, 可得到

$$f(4) + f'(4) \cdot t_2 \cdot 9 \equiv 0 \mod 27.$$

因为 $f(4) \equiv 18 \mod 27$, $f'(4) \equiv 20 \mod 27$, 则将上述同余方程写成 $18 + 20 \cdot t_2 \cdot 9 \equiv 0 \mod 27$, 即 $2 \cdot t_2 \equiv -2 \mod 3$, 解得 $t_2 \equiv 2 \mod 3$.

故同余方程 $f(x) \equiv 0 \mod 27$ 的解为 $x_3 \equiv 4 + t_2 \cdot 9 \equiv 22 \mod 27$.

方法二. 由定理 3.4.6 的结论,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

方法二. 由定理 3.4.6 的结论,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

首先, 计算

$$f'(x_1) = 4 \cdot 1^3 + 7 \equiv 2 \mod 3,\ f'(x_1)^{-1} \equiv 2 \mod 3;$$

方法二. 由定理 3.4.6 的结论,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

首先, 计算

$$f'(x_1) = 4 \cdot 1^3 + 7 \equiv 2 \mod 3, \ f'(x_1)^{-1} \equiv 2 \mod 3;$$

其次, 计算

$$\begin{cases} t_1 \equiv \frac{-f(x_1)}{3}(f'(x_1)^{-1} \mod 3) \equiv 1 \mod 3 \\ x_2 \equiv x_1 + t_1 \cdot 3 \equiv 4 \mod 9; \end{cases}$$

方法二. 由定理 3.4.6 的结论,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

首先, 计算

$$f'(x_1) = 4 \cdot 1^3 + 7 \equiv 2 \pmod 3,\ f'(x_1)^{-1} \equiv 2 \pmod 3;$$

其次, 计算

$$\begin{cases} t_1 \equiv \frac{-f(x_1)}{3}(f'(x_1)^{-1} \pmod 3) \equiv 1 \pmod 3 \\ x_2 \equiv x_1 + t_1 \cdot 3 \equiv 4 \pmod 9; \end{cases}$$

最后, 计算

$$\begin{cases} t_2 \equiv \frac{-f(x_2)}{3^2}(f'(x_2)^{-1} \pmod 3) \equiv 2 \pmod 3 \\ x_3 \equiv x_2 + t_2 \cdot 3^2 \equiv 22 \pmod{27}. \end{cases}$$

方法二. 由定理 3.4.6 的结论,

对于 $f(x) \equiv x^4 + 7x + 4 \mod 27$ 有 $f'(x) \equiv 4x^3 + 7 \mod 27$.

直接验算知, 同余方程 $f(x) = 0 \mod 3$ 有一解 $x_1 \equiv 1 \mod 3$.

首先, 计算

$$f'(x_1) = 4 \cdot 1^3 + 7 \equiv 2 \mod 3, \ f'(x_1)^{-1} \equiv 2 \mod 3;$$

其次, 计算

$$\begin{cases} t_1 \equiv \frac{-f(x_1)}{3}(f'(x_1)^{-1} \mod 3) \equiv 1 \mod 3 \\ x_2 \equiv x_1 + t_1 \cdot 3 \equiv 4 \mod 9; \end{cases}$$

最后, 计算

$$\begin{cases} t_2 \equiv \frac{-f(x_2)}{3^2}(f'(x_2)^{-1} \mod 3) \equiv 2 \mod 3 \\ x_3 \equiv x_2 + t_2 \cdot 3^2 \equiv 22 \mod 27. \end{cases}$$

因此, 同余方程 $f(x) \equiv 0 \mod 27$ 的解为 $x_3 \equiv 22 \mod 27$.

# 本课作业

1. 计算 $\left(\frac{127}{715}\right)$.
2. 求解同余方程 $x^2 \equiv 41 \mod 401$.
3. 求解同余方程 $5x^2 + 3x - 4 \equiv 0 \mod 10$.
4. 将同余方程
$$49x^5 + 25x^3 - 6x^2 + 3x - 10 \equiv 0 \mod 23$$
化成和它等价但首项系数为 1 的同余方程.
5. 利用恒等同余方程 $x^p \equiv x \mod p$ 把下列同余方程化简
$$2x^{18} + 5x^{16} - 20x^{13} - 3x^{11} + 25x^{10} + 4x^8 + 16x^6 - x^3 + 5x + 8 \equiv 0 \mod 7.$$

# 交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn