# 第四章　二次剩余

1. 概念及判别
2. 勒让德符号
3. 二次同余方程

在第二章我们看到, 一般一元二次同余方程的求解可以归结为求解模为素数的一元二次同余方程.

在第二章我们看到, 一般一元二次同余方程的求解可以归结为求解模为素数的一元二次同余方程.

本章将讨论模为素数的一元二次同余方程的一般理论, 并讨论由此引出的勒让德符号, 二次互反律及雅可比符号等.

本节主要介绍二次剩余的概念及两种判别方法.

模为素数的一元二次同余方程的一般形式为

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{1}$$

其中 $p$ 为素数且 $p \nmid a$.

本节主要介绍二次剩余的概念及两种判别方法.

模为素数的一元二次同余方程的一般形式为

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{1}$$

其中 $p$ 为素数且 $p \nmid a$.

因为当 $p = 2$ 时, (1) 容易求解, 所以以下总假定 $p$ 是奇素数. 这样 $p \nmid 4a$, 于是我们得到 (1) 与

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$$

同解.

本节主要介绍二次剩余的概念及两种判别方法.

模为素数的一元二次同余方程的一般形式为

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{1}$$

其中 $p$ 为素数且 $p \nmid a$.

因为当 $p = 2$ 时, (1) 容易求解, 所以以下总假定 $p$ 是奇素数. 这样 $p \nmid 4a$, 于是我们得到 (1) 与

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$$

同解.

显然, 上式可写为

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p} \tag{2}$$

令 $y \equiv 2ax + b \pmod{p}$, 则 $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$ 与同余方程

$$y^2 \equiv b^2 - 4ac \pmod{p} \tag{3}$$

同时有解或同时无解.

令 $y \equiv 2ax + b \pmod{p}$, 则 $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$ 与同余方程

$$y^2 \equiv b^2 - 4ac \pmod{p} \tag{3}$$

同时有解或同时无解.

当有解时, 对 (3) 的每个解 $y \equiv y_0 \pmod{p}$, 可由 $y \equiv 2ax + b \pmod{p}$ 得到 $2ax \equiv y_0 - b \pmod{p}$ 的惟一解 $x \equiv x_0 \pmod{p}$, 它给出 (2) 的一个解.
容易验证, (3) 的不同解给出 (2) 的不同解, 且反过来也对.
据此, 我们只需讨论形如 $x^2 \equiv n \pmod{p}$ 的同余方程.
由于 $p|n$ 时, 该同余方程仅有一个解 $x \equiv 0 \pmod{p}$, 所以下面总假定 $p \nmid n$, 即 $(p, n) = 1$.

综上, 我们关心如下的一元二次同余方程:

$$x^2 \equiv n \pmod{p}, \tag{4}$$

其中 $p$ 是奇素数且 $(p, n) = 1$.

综上, 我们关心如下的一元二次同余方程:

$$x^2 \equiv n \pmod{p}, \tag{4}$$

其中 $p$ 是奇素数且 $(p, n) = 1$.

考虑形如 (4) 的同余方程的解, 我们有下面的定义.

**定义 1.1.** 设 $m, n \in \mathbb{Z}$, $(m, n) = 1$ 且 $m > 1$. 如果 $x^2 \equiv n \pmod{m}$ 有解, 那么称 $n$ 为模 $m$ 的**二次剩余**; 否则, 称 $n$ 为模 $m$ 的**二次非剩余**.

综上, 我们关心如下的一元二次同余方程:

$$x^2 \equiv n \pmod{p}, \tag{4}$$

其中 $p$ 是奇素数且 $(p, n) = 1$.

考虑形如 (4) 的同余方程的解, 我们有下面的定义.

**定义 1.1.** 设 $m, n \in \mathbb{Z}$, $(m, n) = 1$ 且 $m > 1$. 如果 $x^2 \equiv n \pmod{m}$ 有解, 那么称 $n$ 为模 $m$ 的**二次剩余**; 否则, 称 $n$ 为模 $m$ 的**二次非剩余**.

显然, 如果 $n$ 为模 $m$ 的二次剩余 (二次非剩余), 那么 $n + km$ $(k \in \mathbb{Z})$ 也是模 $m$ 的二次剩余 (二次非剩余). 因此, 我们总在关于模 $m$ 同余的意义下考虑模 $m$ 的二次剩余和二次非剩余.

**例 1.1.** 给出模 11 的全部二次剩余和二次非剩余.

**例 1.1.** 给出模 11 的全部二次剩余和二次非剩余.

**解:** 计算 $1, 2, \ldots, 10$ 的平方, 得:

$$
\begin{aligned}
1^2 \equiv 10^2 \equiv 1 \pmod{11},\\
2^2 \equiv 9^2 \equiv 4 \pmod{11},\\
3^2 \equiv 8^2 \equiv 9 \pmod{11},\\
4^2 \equiv 7^2 \equiv 5 \pmod{11},\\
5^2 \equiv 6^2 \equiv 3 \pmod{11}.
\end{aligned}
$$

又因为任意与 11 互素的数, 必与 $1, 2, \ldots, 10$ 中某个数关于模 11 同余, 所以模 11 的二次剩余为: $1, 3, 4, 5, 9$; 二次非剩余为: $2, 6, 7, 8, 10$. □

**例 1.1.** 给出模 11 的全部二次剩余和二次非剩余.

**解:** 计算 $1, 2, \ldots, 10$ 的平方, 得:

$$
\begin{aligned}
1^2 \equiv 10^2 \equiv 1 \pmod{11},\\
2^2 \equiv 9^2 \equiv 4 \pmod{11},\\
3^2 \equiv 8^2 \equiv 9 \pmod{11},\\
4^2 \equiv 7^2 \equiv 5 \pmod{11},\\
5^2 \equiv 6^2 \equiv 3 \pmod{11}.
\end{aligned}
$$

又因为任意与 11 互素的数, 必与 $1, 2, \ldots, 10$ 中某个数关于模 11 同余, 所以模 11 的二次剩余为: $1, 3, 4, 5, 9$; 二次非剩余为: $2, 6, 7, 8, 10$. □

在上面的例子中, 对模数 11, 二次剩余和二次非剩余的个数一样, 各有 $(11-1)/2$ 个. 一般地, 我们有下面的定理.

**定理 1.1.** 设 $p$ 是奇素数, 那么在模 $p$ 的既约剩余系 $\{1, 2, \ldots, p-1\}$ 中, 模 $p$ 的二次剩余和二次非剩余各 $(p-1)/2$ 个, 且

$$1, \quad 2^2 \bmod p, \quad \ldots, \quad \left(\frac{p-1}{2}\right)^2 \bmod p \tag{5}$$

就是模 $p$ 的全部二次剩余.

**定理 1.1.** 设 $p$ 是奇素数, 那么在模 $p$ 的既约剩余系 $\{1, 2, \ldots, p-1\}$ 中, 模 $p$ 的二次剩余和二次非剩余各 $(p-1)/2$ 个, 且

$$1, \quad 2^2 \bmod p, \quad \ldots, \quad \left(\frac{p-1}{2}\right)^2 \bmod p \tag{5}$$

就是模 $p$ 的全部二次剩余.

**证明:** 计算 $k^2$ 关于模 $p$ 的最小非负余数, 这里 $1 \leq k \leq p-1$. 若 $k^2 \equiv a \pmod{p}$, 则也有 $(p-k)^2 \equiv a \pmod{p}$, 显然 $k \not\equiv p-k \pmod{p}$. 另一方面, 由拉格朗日定理知, 同余方程 $x^2 \equiv a \pmod{p}$ 至多只有两个解, 因此当 $p \nmid a$ 时, $x^2 \equiv a \pmod{p}$ 或者正好有两个解或者无解. 因为 $1^2, 2^2, \ldots, (p-1)^2$ 共有 $p-1$ 个平方需要考虑, 所以 $1, 2, \ldots, p-1$ 中正好有 $(p-1)/2$ 个模 $p$ 的二次剩余, 从而模 $p$ 的二次非剩余个数为: $p-1-(p-1)/2 = (p-1)/2$.

下证 (5) 是模 $p$ 的全部二次剩余. 事实上, 对任意 $1 \le k \le (p-1)/2$, 因为 $k^2 \equiv k^2 \bmod p \pmod p$, 所以 $k^2 \bmod p$ 是模 $p$ 的二次剩余. 另外, 当 $1 \le k, l \le (p-1)/2$ 且 $k \ne l$ 时, 我们有 $k^2 \bmod p \ne l^2 \bmod p$. 否则, 有

$$k^2 \equiv k^2 \bmod p = l^2 \bmod p \equiv l^2 \pmod p,$$

即 $(k+l)(k-l) \equiv 0 \pmod p$, 所以 $p|k+l$ 或 $p|k-l$. 但是 $1 < k+l < p-1$, 因此 $p|k-l$. 由于 $1 \le k, l \le (p-1)/2$, 所以 $-(p-3)/2 \le k-l \le (p-3)/2$, 故 $k = l$, 矛盾! 因为 $\{1, 2, \ldots, p-1\}$ 中只有 $(p-1)/2$ 个模 $p$ 的二次剩余, 所以 (5) 是 $\{1, 2, \ldots, p-1\}$ 中的全部二次剩余. 故定理成立. □

上面的定理回答了如下的问题: 对于给定的素数 $p$, 哪些 $n$ 是模 $p$ 的二次剩余, 哪些 $n$ 是模 $p$ 的二次非剩余.

上面的定理回答了如下的问题: 对于给定的素数 $p$, 哪些 $n$ 是模 $p$ 的二次剩余, 哪些 $n$ 是模 $p$ 的二次非剩余.

**例 1.2.** 给出模 17 的全部二次剩余和二次非剩余.

上面的定理回答了如下的问题: 对于给定的素数 $p$, 哪些 $n$ 是模 $p$ 的二次剩余, 哪些 $n$ 是模 $p$ 的二次非剩余.

**例 1.2.** 给出模 17 的全部二次剩余和二次非剩余.

**解:** 由定理1.1知, 模 17 的二次剩余为

$$1, \quad 2^2 \bmod 17, \quad \ldots, \quad 8^2 \bmod 17,$$

即 $1, 4, 9, 16, 8, 2, 15, 13$. 于是模 17 的二次非剩余为 $3, 5, 6, 7, 10, 11, 12, 14$. □

下面定理从理论上给出判别一个整数 $n$ 是否是模 $p$ 的二次剩余的方法, 通常称为欧拉判别法.

**定理 1.2 (欧拉判别法).** 设 $p$ 是奇素数, $n \in \mathbb{Z}$ 且 $p \nmid n$.

(1) $n$ 是模 $p$ 的二次剩余当且仅当 $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

下面定理从理论上给出判别一个整数 $n$ 是否是模 $p$ 的二次剩余的方法, 通常称为欧拉判别法.

**定理 1.2 (欧拉判别法).** 设 $p$ 是奇素数, $n \in \mathbb{Z}$ 且 $p \nmid n$.

(1) $n$ 是模 $p$ 的二次剩余当且仅当 $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(2) $n$ 是模 $p$ 的二次非剩余当且仅当 $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

下面定理从理论上给出判别一个整数 $n$ 是否是模 $p$ 的二次剩余的方法, 通常称为欧拉判别法.

**定理 1.2 (欧拉判别法).** 设 $p$ 是奇素数, $n \in \mathbb{Z}$ 且 $p \nmid n$.

(1) $n$ 是模 $p$ 的二次剩余当且仅当 $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(2) $n$ 是模 $p$ 的二次非剩余当且仅当 $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

下面定理从理论上给出判别一个整数 $n$ 是否是模 $p$ 的二次剩余的方法, 通常称为欧拉判别法.

**定理 1.2 (欧拉判别法).** 设 $p$ 是奇素数, $n \in \mathbb{Z}$ 且 $p \nmid n$.

(1) $n$ 是模 $p$ 的二次剩余当且仅当 $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(2) $n$ 是模 $p$ 的二次非剩余当且仅当 $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

例如, $3^{\frac{5-1}{2}} = 9 \equiv -1 \pmod{5}$, $4^{\frac{5-1}{2}} = 16 \equiv 1 \pmod{5}$, 所以 3 是 5 的二次非剩余, 而 4 是 5 的二次剩余, 即同余方程 $x^2 \equiv 3 \pmod{5}$ 无解, 而 $x^2 \equiv 4 \pmod{5}$ 有解.

欧拉判别法是一个基本方法, 但在实际应用时计算有时非常麻烦, 下节我们将寻求更简单的方法.

**证明：** 我们先证明断言: 对题设中的 $p$ 和 $n$, 下面两个同余式有且仅有一个成立

$$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad n^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

事实上, 由费马小定理知, $n^{p-1} \equiv 1 \pmod{p}$, 所以有

$$\left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p},$$

于是 $p | n^{\frac{p-1}{2}} - 1$ 或 $p | n^{\frac{p-1}{2}} + 1$. 但两者不能同时成立, 否则 $p$ 整除它们的差 $-2$, 与 $p$ 是奇素数矛盾. 故断言成立.

**证明：** 我们先证明断言: 对题设中的 $p$ 和 $n$, 下面两个同余式有且仅有一个成立

$$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad n^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

事实上, 由费马小定理知, $n^{p-1} \equiv 1 \pmod{p}$, 所以有

$$\left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p},$$

于是 $p | n^{\frac{p-1}{2}} - 1$ 或 $p | n^{\frac{p-1}{2}} + 1$. 但两者不能同时成立, 否则 $p$ 整除它们的差 $-2$, 与 $p$ 是奇素数矛盾. 故断言成立.

下证 (1) 的必要性. 如果 $n$ 是模 $p$ 的二次剩余, 则存在整数 $x_0$ 使得 $x_0^2 \equiv n \pmod{p}$. 因为 $p \nmid n$, 所以 $p \nmid x_0$, 即 $(x_0, p) = 1$. 于是由费马小定理有 $x_0^{p-1} \equiv 1 \pmod{p}$, 从而

$$n^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1 \pmod{p},$$

即 $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

下证 (1) 的充分性. 由定理1.1知, $1, 2^2 \bmod p, \ldots, \left(\frac{p-1}{2}\right)^2 \bmod p$ 是模 $p$ 的全部二次剩余. 由上面 (1) 的必要性的证明知, 这 $(p-1)/2$ 个数均是 $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 的解. 由拉格朗日定理, 这 $(p-1)/2$ 个数便是 $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 的全部解. 因此, 如果 $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, 那么存在 $1 \leq k \leq (p-1)/2$ 使得 $n \equiv k^2 \bmod p \pmod{p}$, 所以 $n$ 是模 $p$ 的二次剩余.

下证 (1) 的充分性. 由定理1.1知, $1, 2^2 \bmod p, \ldots, \left(\frac{p-1}{2}\right)^2 \bmod p$ 是模 $p$ 的全部二次剩余. 由上面 (1) 的必要性的证明知, 这 $(p-1)/2$ 个数均是 $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 的解. 由拉格朗日定理, 这 $(p-1)/2$ 个数便是 $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 的全部解. 因此, 如果 $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, 那么存在 $1 \leq k \leq (p-1)/2$ 使得 $n \equiv k^2 \bmod p \pmod{p}$, 所以 $n$ 是模 $p$ 的二次剩余.

(2) 由前面证实的断言及 (1) 即得. □

对不太大的素数 $p$, 应用定理1.1或欧拉判别法都可以计算判断 $n$ 是否是模 $p$ 的二次剩余, 但对于 $p$ 较大的情形, 这两个定理都不是太实用.

对不太大的素数 $p$, 应用定理1.1或欧拉判别法都可以计算判断 $n$ 是否是模 $p$ 的二次剩余, 但对于 $p$ 较大的情形, 这两个定理都不是太实用.

本节研究下面两个问题: (1) 对于给定的 (较大的) 素数 $p$, 如何判断 $n$ 是否是模 $p$ 的二次剩余? (2) 对于给定的 $n$, 怎样的素数 $p$ 以 $n$ 为它的二次剩余?

对不太大的素数 $p$, 应用定理1.1或欧拉判别法都可以计算判断 $n$ 是否是模 $p$ 的二次剩余, 但对于 $p$ 较大的情形, 这两个定理都不是太实用.

本节研究下面两个问题: (1) 对于给定的 (较大的) 素数 $p$, 如何判断 $n$ 是否是模 $p$ 的二次剩余? (2) 对于给定的 $n$, 怎样的素数 $p$ 以 $n$ 为它的二次剩余?

**定义 2.1.** 设 $p$ 是奇素数, $(p, n) = 1$, 定义

$$\left(\frac{n}{p}\right) = \begin{cases} 1 \text{ 若}n\text{是模}p\text{的二次剩余} \\ -1 \text{ 若}n\text{是模}p\text{的二次非剩余}, \end{cases}$$

称函数 $\left(\frac{n}{p}\right)$ 为**勒让德符号**.

对不太大的素数 $p$, 应用定理1.1或欧拉判别法都可以计算判断 $n$ 是否是模 $p$ 的二次剩余, 但对于 $p$ 较大的情形, 这两个定理都不是太实用.

本节研究下面两个问题: (1) 对于给定的 (较大的) 素数 $p$, 如何判断 $n$ 是否是模 $p$ 的二次剩余? (2) 对于给定的 $n$, 怎样的素数 $p$ 以 $n$ 为它的二次剩余?

**定义 2.1.** 设 $p$ 是奇素数, $(p,n)=1$, 定义

$$\left(\frac{n}{p}\right)=\begin{cases} 1 \text{ 若}n\text{是模}p\text{的二次剩余} \\ -1 \text{ 若}n\text{是模}p\text{的二次非剩余}, \end{cases}$$

称函数 $\left(\frac{n}{p}\right)$ 为**勒让德符号**.

例如, $\left(\frac{1}{17}\right)=\left(\frac{4}{17}\right)=\left(\frac{9}{17}\right)=\left(\frac{15}{17}\right)=1$, $\left(\frac{3}{17}\right)=\left(\frac{5}{17}\right)=-1$.

## 注 2.1.

(1) 显然, 对任意奇素数 $p$ 我们有 $\left(\frac{1}{p}\right) = 1$ 和 $\left(\frac{n^2}{p}\right) = 1$.

另外, 当 $n \equiv m \pmod{p}$ 时, $\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$.

## 注 2.1.

(1) 显然, 对任意奇素数 $p$ 我们有 $\left(\frac{1}{p}\right) = 1$ 和 $\left(\frac{n^2}{p}\right) = 1$.
另外, 当 $n \equiv m \pmod{p}$ 时, $\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$.

(2) 勒让德符号仅仅对素数定义, 因此 $\left(\frac{4}{15}\right)$ 没有意义.

## 注 2.1.

(1) 显然, 对任意奇素数 $p$ 我们有 $\left(\frac{1}{p}\right) = 1$ 和 $\left(\frac{n^2}{p}\right) = 1$.
另外, 当 $n \equiv m \pmod{p}$ 时, $\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$.

(2) 勒让德符号仅仅对素数定义, 因此 $\left(\frac{4}{15}\right)$ 没有意义.

(3) 勒让德符号仅对奇素数定义, 因此 $\left(\frac{n}{2}\right)$ 没有定义. 因为每个与 2 互素的数都是模 2 的二次剩余, 所以研究模 2 的二次剩余不是太有意义的事情.

## 注 2.1.

(1) 显然, 对任意奇素数 $p$ 我们有 $\left(\frac{1}{p}\right)=1$ 和 $\left(\frac{n^2}{p}\right)=1$.
另外, 当 $n\equiv m \pmod p$ 时, $\left(\frac{n}{p}\right)=\left(\frac{m}{p}\right)$.

(2) 勒让德符号仅仅对素数定义, 因此 $\left(\frac{4}{15}\right)$ 没有意义.

(3) 勒让德符号仅对奇素数定义, 因此 $\left(\frac{n}{2}\right)$ 没有定义. 因为每个与 2 互素的数都是模 2 的二次剩余, 所以研究模 2 的二次剩余不是太有意义的事情.

(4) 由欧拉判别法知, $\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}} \pmod p$.

**定理 2.1.** 设 $p$ 为奇素数, $p \nmid mn$, 则

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

**定理 2.1.** 设 $p$ 为奇素数, $p \nmid mn$, 则

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

**证明:** 因为 $p \nmid mn$, 所以 $p \nmid m$ 且 $p \nmid n$, 于是

$$\left(\frac{mn}{p}\right) \equiv (mn)^{\frac{p-1}{2}} \equiv m^{\frac{p-1}{2}} \cdot n^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod{p}.$$

但是 $\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod{p}$ 只可能取 $0, 2$ 或 $-2$, 故上式给出 $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$. □

于是, 当 $n = \pm 2^m p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 时, 其中 $m$ 为非负整数, $p_i$ $(1 \leq i \leq k)$ 为素数且 $2 < p_1 < p_2 < \cdots < p_k$, 有

$$\left(\frac{n}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^m \left(\frac{p_1}{p}\right)^{\alpha_1} \left(\frac{p_2}{p}\right)^{\alpha_2} \cdots \left(\frac{p_k}{p}\right)^{\alpha_k}.$$

于是, 当 $n = \pm 2^m p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 时, 其中 $m$ 为非负整数, $p_i$ $(1 \leq i \leq k)$ 为素数且 $2 < p_1 < p_2 < \cdots < p_k$, 有

$$\left(\frac{n}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^m \left(\frac{p_1}{p}\right)^{\alpha_1} \left(\frac{p_2}{p}\right)^{\alpha_2} \cdots \left(\frac{p_k}{p}\right)^{\alpha_k}.$$

因为 $\left(\frac{1}{p}\right) = 1$, 所以对任意满足 $(n, p) = 1$ 的整数 $n$, 计算 $\left(\frac{n}{p}\right)$ 时只需计算出下面三种值:

$$\left(\frac{-1}{p}\right), \quad \left(\frac{2}{p}\right), \quad \left(\frac{q}{p}\right), \quad (q\text{为奇素数}).$$

于是, 当 $n=\pm 2^m p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 时, 其中 $m$ 为非负整数, $p_i\ (1 \le i \le k)$ 为素数且 $2 < p_1 < p_2 < \cdots < p_k$, 有

$$\left(\frac{n}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^m \left(\frac{p_1}{p}\right)^{\alpha_1} \left(\frac{p_2}{p}\right)^{\alpha_2} \cdots \left(\frac{p_k}{p}\right)^{\alpha_k}.$$

因为 $\left(\frac{1}{p}\right) = 1$, 所以对任意满足 $(n,p)=1$ 的整数 $n$, 计算 $\left(\frac{n}{p}\right)$ 时只需计算出下面三种值:

$$\left(\frac{-1}{p}\right), \quad \left(\frac{2}{p}\right), \quad \left(\frac{q}{p}\right), \quad (q\text{为奇素数}).$$

为此, 我们先计算 $\left(\frac{-1}{p}\right)$.

**定理 2.2.** 对任意奇素数 $p$, 有

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{若 } p \equiv 1 \pmod 4 \\ -1 & \text{若 } p \equiv -1 \pmod 4. \end{cases}$$

**定理 2.2.** 对任意奇素数 $p$, 有

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{若 } p \equiv 1 \pmod 4 \\ -1 & \text{若 } p \equiv -1 \pmod 4. \end{cases}$$

**证明:** 因为 $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$, 又因为 $\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}$ 只可能取值 $0, 2$ 或 $-2$, 所以 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, 故定理成立. □

作为定理2.2的应用, 我们看两个例子.

**例 2.1.** 每个形如 $4k+3$ 的素数 $p$ 都不能写成两个平方之和.

作为定理2.2的应用, 我们看两个例子.

**例 2.1.** 每个形如 $4k+3$ 的素数 $p$ 都不能写成两个平方之和.

**证明:** 使用反证法, 假设 $p = 4k+3 = x^2+y^2$, 则 $x^2+y^2 \equiv 0 \pmod{p}$, 即 $x^2 \equiv -y^2 \pmod{p}$. 因为 $(y,p)=1$, 所以关于 $z$ 的同余方程 $yz \equiv 1 \pmod{p}$ 有惟一解, 设为 $z_0$, 即 $yz_0 \equiv 1 \pmod{p}$. 于是

$$x^2 z_0^2 \equiv -y^2 z_0^2 \equiv -(yz_0)^2 \equiv -1 \pmod{p},$$

即 $(xz_0)^2 \equiv -1 \pmod{p}$, 故 $\left(\frac{-1}{p}\right) = 1$. 这与定理2.2矛盾! 因此这样的 $p$ 不能写成两个平方之和. □

**例 2.2.** 每个形如 $4k+1$ 的素数 $p$ 都能写成两个平方之和, 且这种写法惟一.

**例 2.2.** 每个形如 $4k+1$ 的素数 $p$ 都能写成两个平方之和, 且这种写法惟一.

为了计算 $\left(\frac{2}{p}\right)$, 我们需要下面的定理.

**定理 2.3 (高斯引理).** 设 $p$ 是一个奇素数, $(n,p)=1$. 如果下面 $(p-1)/2$ 个数

$$n \bmod p,\ 2n \bmod p,\ \ldots,\ \frac{(p-1)n}{2} \bmod p \tag{6}$$

中有 $m$ 个大于 $p/2$, 那么 $\left(\frac{n}{p}\right)=(-1)^m$.

为了计算 $\left(\frac{2}{p}\right)$, 我们需要下面的定理.

**定理 2.3 (高斯引理).** 设 $p$ 是一个奇素数, $(n,p)=1$. 如果下面 $(p-1)/2$ 个数

$$n \bmod p,\ 2n \bmod p,\ \ldots,\ \frac{(p-1)n}{2} \bmod p \tag{6}$$

中有 $m$ 个大于 $p/2$, 那么 $\left(\frac{n}{p}\right)=(-1)^m$.

例如, 我们可以用高斯引理来求 $\left(\frac{3}{17}\right)$. 为此, 我们先列出 (6) 中的所有数:

$$3\bmod 17,\ 6\bmod 17,\ 9\bmod 17,\ 12\bmod 17,$$

$$15\bmod 17,\ 18\bmod 17,\ 21\bmod 17,\ 24\bmod 17,$$

即 $3,6,9,12,15,1,4,7$. 这些数中大于 $17/2$ 的数只有 3 个, 所以 $\left(\frac{3}{17}\right)=(-1)^3=-1$.

**定理 2.4.** 对任意奇素数 $p$, 有

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

**定理 2.4.** 对任意奇素数 $p$, 有

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

**证明:** 在高斯引理中取 $n = 2$, 则 (6) 给出:

$$2 \bmod p,\ 2 \cdot 2 \bmod p,\ 3 \cdot 2 \bmod p,\ \ldots,\ \left(\frac{p-1}{2}\right) \cdot 2 \bmod p,$$

其中满足 $\frac{p}{2} < 2k < p$, 即 $\frac{p}{4} < k < \frac{p}{2}$ 的 $k$ 的个数 $m = \lfloor \frac{p}{2} \rfloor - \lfloor \frac{p}{4} \rfloor$. 令 $p = 8l + r$, $r = 1, 3, 5, 7$, 则有 $m = 2l + \lfloor \frac{r}{2} \rfloor - \lfloor \frac{r}{4} \rfloor \equiv 0, 1, 1, 0 \pmod 2$, 因此

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

为了证明随后的二次互反律, 我们先介绍一个引理.

**引理 2.1.** 设 $p$ 是一个奇素数, $n$ 是一个奇数, $(n,p)=1$, 则 $\left(\frac{n}{p}\right)=(-1)^{T(n,p)}$, 其中 $T(n,p)=\sum_{k=1}^{(p-1)/2}\left\lfloor\frac{kn}{p}\right\rfloor$.

为了证明随后的二次互反律, 我们先介绍一个引理.

**引理 2.1.** 设 $p$ 是一个奇素数, $n$ 是一个奇数, $(n,p)=1$, 则 $\left(\frac{n}{p}\right)=(-1)^{T(n,p)}$, 其中 $T(n,p)=\sum_{k=1}^{(p-1)/2}\left\lfloor\frac{kn}{p}\right\rfloor$.

**例 2.3.** 使用引理 2.1 计算 $\left(\frac{7}{11}\right)$ 和 $\left(\frac{11}{7}\right)$.

**例 2.3.** 使用引理 2.1 计算 $\left(\frac{7}{11}\right)$ 和 $\left(\frac{11}{7}\right)$.

**解:** 因为

$$\begin{aligned}\sum_{k=1}^{5}\lfloor\frac{7k}{11}\rfloor &= \lfloor\frac{7}{11}\rfloor+\lfloor\frac{14}{11}\rfloor+\lfloor\frac{21}{11}\rfloor+\lfloor\frac{28}{11}\rfloor+\lfloor\frac{35}{11}\rfloor\\ &= 0+1+1+2+3=7,\end{aligned}$$

所以 $\left(\frac{7}{11}\right)=(-1)^7=-1$.

**例 2.3.** 使用引理 2.1 计算 $\left(\frac{7}{11}\right)$ 和 $\left(\frac{11}{7}\right)$.

**解:** 因为

$$\begin{aligned}\sum_{k=1}^{5}\lfloor\frac{7k}{11}\rfloor &= \lfloor\frac{7}{11}\rfloor+\lfloor\frac{14}{11}\rfloor+\lfloor\frac{21}{11}\rfloor+\lfloor\frac{28}{11}\rfloor+\lfloor\frac{35}{11}\rfloor\\ &= 0+1+1+2+3=7,\end{aligned}$$

所以 $\left(\frac{7}{11}\right)=(-1)^7=-1$.

同理, 由于

$$\begin{aligned}\sum_{k=1}^{3}\lfloor\frac{11k}{7}\rfloor &= \lfloor\frac{11}{7}\rfloor+\lfloor\frac{22}{7}\rfloor+\lfloor\frac{33}{7}\rfloor\\ &= 1+3+4=8,\end{aligned}$$

所以 $\left(\frac{11}{7}\right)=(-1)^8=1$. □

上面例子表明, 11 是模 7 的二次剩余, 但 7 不是模 11 的二次剩余.

上面例子表明, 11 是模 7 的二次剩余, 但 7 不是模 11 的二次剩余.

一个自然的问题是, 对两个不同的奇素数 $p, q$, 勒让德符号 $\left(\frac{q}{p}\right)$ 和 $\left(\frac{p}{q}\right)$ 之间有关系吗?

上面例子表明, 11 是模 7 的二次剩余, 但 7 不是模 11 的二次剩余.

一个自然的问题是, 对两个不同的奇素数 $p, q$, 勒让德符号 $\left(\frac{q}{p}\right)$ 和 $\left(\frac{p}{q}\right)$ 之间有关系吗?

**定理 2.5 (二次互反律).** 设 $p, q$ 是两个不同的奇素数, 则

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

上面例子表明, 11 是模 7 的二次剩余, 但 7 不是模 11 的二次剩余.

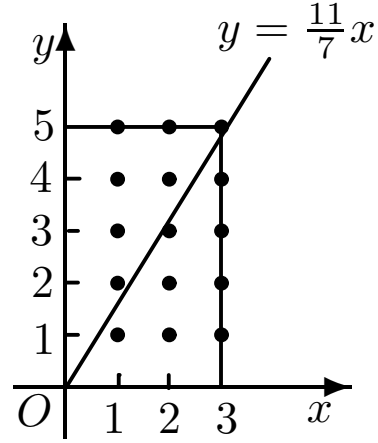
一个自然的问题是, 对两个不同的奇素数 $p, q$, 勒让德符号 $\left(\frac{q}{p}\right)$ 和 $\left(\frac{p}{q}\right)$ 之间有关系吗?

**定理 2.5 (二次互反律).** 设 $p, q$ 是两个不同的奇素数, 则

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

在给出证明之前, 我们再考察一下例2.3. 令 $p = 7$, $q = 11$. 考虑整点 $(x, y)$, 其中 $1 \le x \le \frac{7-1}{2} = 3$, $1 \le y \le \frac{11-1}{2} = 5$, 这样的整点共 15 个. 值得注意的是, 这些整点都不满足 $11x = 7y$, 否则有 $11|7y$, 即 $11|y$, 但 $1 \le y \le 5$, 矛盾!

依据 $11x$ 与 $7y$ 的大小 (见下图), 我们将这 15 个点分成两组:

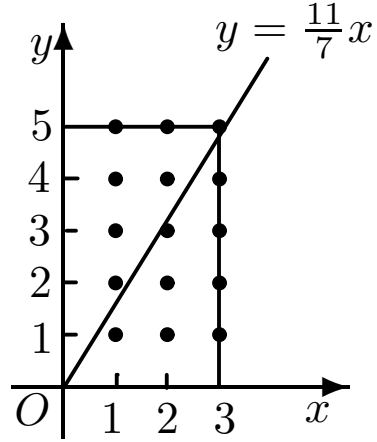



(1) 满足 $1 \leq x \leq 3, 1 \leq y \leq 5, 11x > 7y$ 的整点 $(x, y)$ 正好满足条件 $1 \leq x \leq 3, 1 \leq y \leq \frac{11}{7}x$. 因为对每个给定的 $x$ $(1 \leq x \leq 3)$, $y$ 有 $\lfloor \frac{11}{7}x \rfloor$ 个可能的取值, 所以满足 $1 \leq x \leq 3, 1 \leq y \leq 5, 11x > 7y$ 的整点的总数为 $\sum_{k=1}^{3} \lfloor \frac{11k}{7} \rfloor = \lfloor \frac{11}{7} \rfloor + \lfloor \frac{22}{7} \rfloor + \lfloor \frac{33}{7} \rfloor = 8$. 这些点分别是 $(1,1), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (3,4)$.

(2) 满足 $1 \le x \le 3, 1 \le y \le 5, 11x < 7y$ 的整点 $(x, y)$ 正好满足条件 $1 \le y \le 5, 1 \le x \le \frac{7}{11}y$. 因为对每个给定的 $y$ $(1 \le y \le 5)$, $x$ 有 $\lfloor \frac{7}{11}y \rfloor$ 个可能的取值, 所以满足 $1 \le x \le 3, 1 \le y \le 5, 11x < 7y$ 的整点的总数为

$$\sum_{k=1}^{5} \lfloor \frac{7k}{11} \rfloor = \lfloor \frac{7}{11} \rfloor + \lfloor \frac{14}{11} \rfloor + \lfloor \frac{21}{11} \rfloor + \lfloor \frac{28}{11} \rfloor + \lfloor \frac{35}{11} \rfloor = 7,$$

这些点分别是 $(1,2), (1,3), (1,4), (1,5), (2,4), (2,5), (3,5)$.



因为

$$\frac{7-1}{2}\cdot\frac{11-1}{2}=3\cdot 5=15=\sum_{k=1}^{3}\lfloor\frac{11k}{7}\rfloor+\sum_{k=1}^{5}\lfloor\frac{7k}{11}\rfloor,$$

所以

$$\begin{aligned}(-1)^{\frac{7-1}{2}\cdot\frac{11-1}{2}}&=(-1)^{\sum_{k=1}^{3}\lfloor\frac{11k}{7}\rfloor+\sum_{k=1}^{5}\lfloor\frac{7k}{11}\rfloor}\\&=(-1)^{\sum_{k=1}^{3}\lfloor\frac{11k}{7}\rfloor}\cdot(-1)^{\sum_{k=1}^{5}\lfloor\frac{7k}{11}\rfloor}.\end{aligned}$$

由引理2.1知, $\left(\frac{11}{7}\right)=(-1)^{\sum_{k=1}^{3}\lfloor\frac{11k}{7}\rfloor}$, $\left(\frac{7}{11}\right)=(-1)^{\sum_{k=1}^{5}\lfloor\frac{7k}{11}\rfloor}$, 所以有

$$\left(\frac{11}{7}\right)\left(\frac{7}{11}\right)=(-1)^{\frac{7-1}{2}\cdot\frac{11-1}{2}}.$$

**注 2.2.** 关于二次互反律, 我们有下面两个注记:

(1) 由勒让德符号的定义知, $\left(\frac{q}{p}\right)$ 和 $\left(\frac{p}{q}\right)$ 分别刻画了二次同余方程 $x^2 \equiv q \pmod{p}$ 和 $x^2 \equiv p \pmod{q}$ 是否有解, 即 $q$ 是否是模 $p$ 的二次剩余和 $p$ 是否是模 $q$ 的二次剩余. 这两个问题中任意一个的模数和剩余的位置互换就成了另外一个问题, 定理 2.5 刻画了这两者之间的关系, 所以称为二次互反律.

**注 2.2.** 关于二次互反律, 我们有下面两个注记:

(1) 由勒让德符号的定义知, $\left(\frac{q}{p}\right)$ 和 $\left(\frac{p}{q}\right)$ 分别刻画了二次同余方程 $x^2 \equiv q \pmod{p}$ 和 $x^2 \equiv p \pmod{q}$ 是否有解, 即 $q$ 是否是模 $p$ 的二次剩余和 $p$ 是否是模 $q$ 的二次剩余. 这两个问题中任意一个的模数和剩余的位置互换就成了另外一个问题, 定理 2.5 刻画了这两者之间的关系, 所以称为二次互反律.

(2) 设 $p, q$ 是两个不同的奇素数, 则二次互反律也可表为

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right),$$

因此

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{若 } p \equiv 1 \pmod{4} \text{ 或 } q \equiv 1 \pmod{4} \\ -\left(\frac{q}{p}\right) & \text{若 } p \equiv q \equiv -1 \pmod{4}. \end{cases}$$

**例 2.4.** 计算 $\left(\frac{13}{17}\right)$ 和 $\left(\frac{17}{13}\right)$.

**例 2.4.** 计算 $\left(\frac{13}{17}\right)$ 和 $\left(\frac{17}{13}\right)$.

**解:** 因为 $13 \equiv 17 \equiv 1 \pmod 4$, 所以 $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$. 而 $\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2^2}{13}\right) = 1$, 故 $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = 1$. □

**例 2.5.** 计算 $\left(\frac{713}{1009}\right)$.

**例 2.5.** 计算 $\left(\frac{713}{1009}\right)$.

**解:** 由 $713 = 23 \cdot 31$ 得, $\left(\frac{713}{1009}\right) = \left(\frac{23 \cdot 31}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$. 因为 $1009 \equiv 1 \pmod 4$, 所以

$$\begin{aligned}\left(\frac{23}{1009}\right) &= \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \left(\frac{2^2 \cdot 5}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right) \\ &= \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1;\end{aligned}$$

**例 2.5.** 计算 $\left(\frac{713}{1009}\right)$.

**解:** 由 $713 = 23 \cdot 31$ 得, $\left(\frac{713}{1009}\right) = \left(\frac{23\cdot 31}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$. 因为 $1009 \equiv 1 \pmod 4$, 所以

$$\begin{aligned}
\left(\frac{23}{1009}\right) &= \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \left(\frac{2^2\cdot 5}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right) \\
&= \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1; \\
\left(\frac{31}{1009}\right) &= \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) \\
&= \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) \\
&= \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{4}{3}\right) = -\left(\frac{2^2}{3}\right) = -1.
\end{aligned}$$

**例 2.5.** 计算 $\left(\frac{713}{1009}\right)$.

**解:** 由 $713 = 23 \cdot 31$ 得, $\left(\frac{713}{1009}\right) = \left(\frac{23\cdot 31}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$. 因为 $1009 \equiv 1 \pmod 4$, 所以

$$\begin{aligned}
\left(\frac{23}{1009}\right) &= \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \left(\frac{2^2\cdot 5}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right) \\
&= \left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1; \\
\left(\frac{31}{1009}\right) &= \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) \\
&= \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) \\
&= \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{4}{3}\right) = -\left(\frac{2^2}{3}\right) = -1.
\end{aligned}$$

故 $\left(\frac{713}{1009}\right) = (-1)(-1) = 1$. □

**例 2.6.** 求以 11 为其二次剩余的所有奇素数 $p$.

**例 2.6.** 求以 11 为其二次剩余的所有奇素数 $p$.

**解：** 由二次互反律有, $\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{11}\right)$. 显然, 我们有

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{若 } p \equiv 1 \pmod 4 \\ -1 & \text{若 } p \equiv 3 \pmod 4. \end{cases}$$

**例 2.6.** 求以 11 为其二次剩余的所有奇素数 $p$.

**解：** 由二次互反律有, $\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{11}\right)$. 显然, 我们有

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{若 } p \equiv 1 \pmod 4 \\ -1 & \text{若 } p \equiv 3 \pmod 4. \end{cases}$$

另外, 直接计算知,

$$\left(\frac{p}{11}\right) = \begin{cases} 1 & \text{若 } p \equiv 1, 3, 4, 5, 9 \pmod{11} \\ -1 & \text{若 } p \equiv 2, 6, 7, 8, 10 \pmod{11}. \end{cases}$$

**例 2.6.** 求以 11 为其二次剩余的所有奇素数 $p$.

**解：** 由二次互反律有, $\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{11}\right)$. 显然, 我们有

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{若 } p \equiv 1 \pmod 4 \\ -1 & \text{若 } p \equiv 3 \pmod 4. \end{cases}$$

另外, 直接计算知,

$$\left(\frac{p}{11}\right) = \begin{cases} 1 & \text{若 } p \equiv 1, 3, 4, 5, 9 \pmod{11} \\ -1 & \text{若 } p \equiv 2, 6, 7, 8, 10 \pmod{11}. \end{cases}$$

由定义, 11 是模 $p$ 的二次剩余的充要条件是 $\left(\frac{11}{p}\right) = 1$.

而 $\left(\frac{11}{p}\right)=1$ 等价于 $p$ 是下面某个同余方程组的解:

$$\begin{cases} x \equiv b_1 \pmod 4 \\ x \equiv b_2 \pmod{11}, \end{cases} \tag{7}$$

其中 $(b_1, b_2) \in$

$\{(1,1),(1,3),(1,4),(1,5),(1,9),(3,2),(3,6),(3,7),(3,8),(3,10)\}$.

而 $\left(\frac{11}{p}\right)=1$ 等价于 $p$ 是下面某个同余方程组的解:

$$\begin{cases} x \equiv b_1 \pmod 4 \\ x \equiv b_2 \pmod{11}, \end{cases} \tag{7}$$

其中 $(b_1, b_2) \in$

$\{(1,1),(1,3),(1,4),(1,5),(1,9),(3,2),(3,6),(3,7),(3,8),(3,10)\}$.

由中国剩余定理, 对每组 $(b_1, b_2)$, (7) 有惟一解

$x \equiv -11b_1 + 12b_2 \pmod{44}$, 于是

$$p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \pmod{44}.$$

所以当 $p$ 是以上形式的素数时, 11 是其二次剩余.

而 $\left(\frac{11}{p}\right)=1$ 等价于 $p$ 是下面某个同余方程组的解:

$$\begin{cases} x \equiv b_1 \pmod 4 \\ x \equiv b_2 \pmod{11}, \end{cases} \tag{7}$$

其中 $(b_1, b_2) \in$

$\{(1,1),(1,3),(1,4),(1,5),(1,9),(3,2),(3,6),(3,7),(3,8),(3,10)\}$.

由中国剩余定理, 对每组 $(b_1, b_2)$, (7) 有惟一解

$x \equiv -11b_1 + 12b_2 \pmod{44}$, 于是

$$p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \pmod{44}.$$

所以当 $p$ 是以上形式的素数时, 11 是其二次剩余.

进而可以推出, 当 $p$ 为下述形式的素数时

$$p \equiv \pm 3, \pm 13, \pm 15, \pm 17, \pm 21 \pmod{44},$$

11 是其二次非剩余.

1. 概念及判别

2. 勒让德符号

3. 二次同余方程

在 4.1 节中我们已经看到, 求解一般的一元二次同余方程的关键是求解形如 $x^2 \equiv n \pmod{p}$ 的方程. 本节将给出这类方程的解法和解数.

在 4.1 节中我们已经看到, 求解一般的一元二次同余方程的关键是求解形如 $x^2 \equiv n \pmod{p}$ 的方程. 本节将给出这类方程的解法和解数.

我们先讨论 $p$ 为奇素数的情形, 即: $x^2 \equiv n \pmod{p}$, 其中 $p$ 是奇素数, $p \nmid n$.

由勒让德符号的定义知, 当 $\left(\frac{n}{p}\right) = -1$ 时, 该同余方程无解.

当 $\left(\frac{n}{p}\right) = 1$ 时, 该同余方程有解, 且有两个解.

当 $p$ 不太大时, 可将 $x = 1, 2, \ldots, (p-1)/2$ 直接代入验证, 但是当 $p$ 较大时, 这种代入法求解比较困难. 下面的定理解决了这个问题.

**定理 3.1.** 设 $p$ 是奇素数, $p \nmid n$, $\left(\frac{n}{p}\right) = 1$.

(1) 当 $p \equiv 3 \pmod 4$ 时, $x^2 \equiv n \pmod p$ 的解为 $x \equiv \pm n^{\frac{p+1}{4}} \pmod p$.

**定理 3.1.** 设 $p$ 是奇素数, $p \nmid n$, $\left(\frac{n}{p}\right) = 1$.

(1) 当 $p \equiv 3 \pmod 4$ 时, $x^2 \equiv n \pmod p$ 的解为 $x \equiv \pm n^{\frac{p+1}{4}} \pmod p$.

(2) 当 $p \equiv 5 \pmod 8$ 时,

**定理 3.1.** 设 $p$ 是奇素数, $p \nmid n$, $\left(\frac{n}{p}\right) = 1$.

(1) 当 $p \equiv 3 \pmod 4$ 时, $x^2 \equiv n \pmod p$ 的解为
$x \equiv \pm n^{\frac{p+1}{4}} \pmod p$.

(2) 当 $p \equiv 5 \pmod 8$ 时,

(2.1) 若 $n^{\frac{p-1}{4}} \equiv 1 \pmod p$, 则 $x^2 \equiv n \pmod p$ 的解为
$x \equiv \pm n^{\frac{p+3}{8}} \pmod p$.

**定理 3.1.** 设 $p$ 是奇素数, $p \nmid n$, $\left(\frac{n}{p}\right) = 1$.

(1) 当 $p \equiv 3 \pmod 4$ 时, $x^2 \equiv n \pmod p$ 的解为
$x \equiv \pm n^{\frac{p+1}{4}} \pmod p$.

(2) 当 $p \equiv 5 \pmod 8$ 时,

(2.1) 若 $n^{\frac{p-1}{4}} \equiv 1 \pmod p$, 则 $x^2 \equiv n \pmod p$ 的解为
$x \equiv \pm n^{\frac{p+3}{8}} \pmod p$.

(2.2) 若 $n^{\frac{p-1}{4}} \equiv -1 \pmod p$, 则 $x^2 \equiv n \pmod p$ 的解为
$x \equiv \pm \left(\frac{p-1}{2}\right)! \cdot n^{\frac{p+3}{8}} \pmod p$.

**定理 3.1.** 设 $p$ 是奇素数, $p \nmid n$, $\left(\frac{n}{p}\right) = 1$.

(1) 当 $p \equiv 3 \pmod 4$ 时, $x^2 \equiv n \pmod p$ 的解为
$x \equiv \pm n^{\frac{p+1}{4}} \pmod p$.

(2) 当 $p \equiv 5 \pmod 8$ 时,

(2.1) 若 $n^{\frac{p-1}{4}} \equiv 1 \pmod p$, 则 $x^2 \equiv n \pmod p$ 的解为
$x \equiv \pm n^{\frac{p+3}{8}} \pmod p$.

(2.2) 若 $n^{\frac{p-1}{4}} \equiv -1 \pmod p$, 则 $x^2 \equiv n \pmod p$ 的解为
$x \equiv \pm \left(\frac{p-1}{2}\right)! \cdot n^{\frac{p+3}{8}} \pmod p$.

(3) 当 $p \equiv 1 \pmod 8$ 时, $x^2 \equiv n \pmod p$ 的解为
$x \equiv \pm n^{\frac{h+1}{2}} N^{s_k} \pmod p$, 其中 $N$ 是模 $p$ 的任意二次非剩余, $h$ 满足 $p - 1 = 2^k h$ 和 $2 \nmid h$, $s_k$ 是待定的整数.

下面应用定理3.1解同余方程.

**例 3.1.** 解下列同余方程:

(1) $x^2 \equiv 3 \pmod{11}$.

下面应用定理3.1解同余方程.

**例 3.1.** 解下列同余方程:

(1) $x^2 \equiv 3 \pmod{11}$.

(2) $x^2 \equiv 3 \pmod{13}$.

下面应用定理3.1解同余方程.

**例 3.1.** 解下列同余方程:

(1) $x^2 \equiv 3 \pmod{11}$.

(2) $x^2 \equiv 3 \pmod{13}$.

(3) $x^2 \equiv 2 \pmod{17}$.

下面应用定理3.1解同余方程.

**例 3.1.** 解下列同余方程:

(1) $x^2 \equiv 3 \pmod{11}$.

(2) $x^2 \equiv 3 \pmod{13}$.

(3) $x^2 \equiv 2 \pmod{17}$.

下面应用定理3.1解同余方程.

**例 3.1.** 解下列同余方程:

(1) $x^2 \equiv 3 \pmod{11}$.

(2) $x^2 \equiv 3 \pmod{13}$.

(3) $x^2 \equiv 2 \pmod{17}$.

**解:** (1) 因为 $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1$, 且 $11 \equiv 3 \pmod 4$, 所以由定理3.1(1), $x^2 \equiv 3 \pmod{11}$ 的解为 $x \equiv \pm 3^{\frac{11+1}{4}} \equiv \pm 5 \pmod{11}$.

下面应用定理3.1解同余方程.

**例 3.1.** 解下列同余方程:

(1) $x^2 \equiv 3 \pmod{11}$.

(2) $x^2 \equiv 3 \pmod{13}$.

(3) $x^2 \equiv 2 \pmod{17}$.

**解:** (1) 因为 $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1$, 且 $11 \equiv 3 \pmod 4$, 所以由定理3.1(1), $x^2 \equiv 3 \pmod{11}$ 的解为 $x \equiv \pm 3^{\frac{11+1}{4}} \equiv \pm 5 \pmod{11}$.

(2) 因为 $\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$, 又因为 $13 \equiv 5 \pmod 8$ 且 $3^{\frac{13-1}{4}} = 3^3 \equiv 1 \pmod{13}$, 所以由定理3.1(2.1), $x^2 \equiv 3 \pmod{13}$ 的解为 $x \equiv \pm 3^{\frac{13+3}{8}} \equiv \pm 9 \pmod{13}$.

## $x^2 \equiv 2 \pmod{17}$

(3) 因为 $\left(\frac{2}{17}\right) = 1$, 且 $17 \equiv 1 \pmod 8$, 所以可以利用定理3.1(3) 的证明过程求解: 首先计算知, $N = 3$ 是模 17 的一个二次非剩余, 即 $\left(\frac{3}{17}\right) = -1$. 于是有 $3^{\frac{17-1}{2}} \equiv -1 \pmod{17}$, 即 $3^{2^3} \equiv -1 \pmod{17}$.

## $x^2 \equiv 2 \pmod{17}$

(3) 因为 $\left(\frac{2}{17}\right) = 1$, 且 $17 \equiv 1 \pmod 8$, 所以可以利用定理3.1(3) 的证明过程求解: 首先计算知, $N = 3$ 是模 17 的一个二次非剩余, 即 $\left(\frac{3}{17}\right) = -1$. 于是有 $3^{\frac{17-1}{2}} \equiv -1 \pmod{17}$, 即 $3^{2^3} \equiv -1 \pmod{17}$.另一方面, 由 $\left(\frac{2}{17}\right) = 1$ 知, $2^{\frac{17-1}{2}} \equiv 1 \pmod{17}$, 即 $2^{2^3} \equiv 1 \pmod{17}$, 因此 $(2^{2^2} - 1)(2^{2^2} + 1) \equiv 0 \pmod{17}$, 进而 $2^{2^2} \equiv -1 \pmod{17}$. 于是我们得到 $2^{2^2} \cdot 3^{2^3} \equiv 1 \pmod{17}$.

## $x^2 \equiv 2 \pmod{17}$

(3) 因为 $\left(\frac{2}{17}\right) = 1$, 且 $17 \equiv 1 \pmod 8$, 所以可以利用定理3.1(3) 的证明过程求解: 首先计算知, $N = 3$ 是模 17 的一个二次非剩余, 即 $\left(\frac{3}{17}\right) = -1$. 于是有 $3^{\frac{17-1}{2}} \equiv -1 \pmod{17}$, 即 $3^{2^3} \equiv -1 \pmod{17}$.另一方面, 由 $\left(\frac{2}{17}\right) = 1$ 知, $2^{\frac{17-1}{2}} \equiv 1 \pmod{17}$, 即 $2^{2^3} \equiv 1 \pmod{17}$, 因此 $(2^{2^2} - 1)(2^{2^2} + 1) \equiv 0 \pmod{17}$, 进而 $2^{2^2} \equiv -1 \pmod{17}$. 于是我们得到 $2^{2^2} \cdot 3^{2^3} \equiv 1 \pmod{17}$.重复前面的过程, 有 $(2^2 \cdot 3^{2^2} - 1)(2^2 \cdot 3^{2^2} + 1) \equiv 0 \pmod{17}$, 由此得 $2^2 \cdot 3^{2^2} \equiv 1 \pmod{17}$. 于是有 $(2 \cdot 3^2 - 1)(2 \cdot 3^2 + 1) \equiv 0 \pmod{17}$, 由此得 $2 \cdot 3^2 \equiv 1 \pmod{17}$. 进一步, 我们有 $2^2 \cdot 3^2 \equiv 2 \pmod{17}$, 故 $x \equiv \pm 6 \pmod{17}$ 是 $x^2 \equiv 2 \pmod{17}$ 的解. □

下面的定理给出了模为奇素数幂的一元二次同余方程的解的个数.

**定理 3.2.** 设 $p$ 是一个奇素数, $p \nmid n$, 则二次同余方程

$$x^2 \equiv n \pmod{p^\alpha} \tag{8}$$

的解数与 $x^2 \equiv n \pmod{p}$ 的解数相同, 其中 $\alpha > 1$.

下面的定理给出了模为奇素数幂的一元二次同余方程的解的个数.

**定理 3.2.** 设 $p$ 是一个奇素数, $p \nmid n$, 则二次同余方程

$$x^2 \equiv n \pmod{p^\alpha} \tag{8}$$

的解数与 $x^2 \equiv n \pmod{p}$ 的解数相同, 其中 $\alpha > 1$.

**例 3.2.** 求 $x^2 \equiv 47 \pmod{11^2}$ 的解.

**例 3.2.** 求 $x^2 \equiv 47 \pmod{11^2}$ 的解.

**解:** 首先, 我们不难发现 $x^2 \equiv 47 \equiv 3 \pmod{11}$ 有解 $x \equiv \pm 5 \pmod{11}$, 因此 $x^2 \equiv 47 \pmod{11^2}$ 应该有两个解. 这两个解的形式为 $x \equiv 11k + 5 \pmod{11^2}$ 或 $x \equiv 11k - 5 \pmod{11^2}$, 其中 $k$ 待定.

**例 3.2.** 求 $x^2 \equiv 47 \pmod{11^2}$ 的解.

**解:** 首先, 我们不难发现 $x^2 \equiv 47 \equiv 3 \pmod{11}$ 有解 $x \equiv \pm 5 \pmod{11}$, 因此 $x^2 \equiv 47 \pmod{11^2}$ 应该有两个解. 这两个解的形式为 $x \equiv 11k + 5 \pmod{11^2}$ 或 $x \equiv 11k - 5 \pmod{11^2}$, 其中 $k$ 待定.

若解的形式为 $x \equiv 11k + 5 \pmod{11^2}$, 则代入得

$$47 \equiv (11k+5)^2 \equiv 11^2k^2+110k+25 \equiv 110k+25 \pmod{11^2},$$

即 $110k \equiv 22 \pmod{11^2}$, 这等价于 $10k \equiv 2 \pmod{11}$, 解之得 $k \equiv 9 \pmod{11}$, 故 $x \equiv 11 \cdot 9 + 5 \equiv 104 \pmod{11^2}$ 是 $x^2 \equiv 47 \pmod{11^2}$ 的一个解. 于是, 另一个解为 $x \equiv -104 \equiv 17 \pmod{11^2}$.

**例 3.2.** 求 $x^2 \equiv 47 \pmod{11^2}$ 的解.

**解:** 首先, 我们不难发现 $x^2 \equiv 47 \equiv 3 \pmod{11}$ 有解 $x \equiv \pm 5 \pmod{11}$, 因此 $x^2 \equiv 47 \pmod{11^2}$ 应该有两个解. 这两个解的形式为 $x \equiv 11k + 5 \pmod{11^2}$ 或 $x \equiv 11k - 5 \pmod{11^2}$, 其中 $k$ 待定.

若解的形式为 $x \equiv 11k + 5 \pmod{11^2}$, 则代入得

$$47 \equiv (11k+5)^2 \equiv 11^2k^2+110k+25 \equiv 110k+25 \pmod{11^2},$$

即 $110k \equiv 22 \pmod{11^2}$, 这等价于 $10k \equiv 2 \pmod{11}$, 解之得 $k \equiv 9 \pmod{11}$, 故 $x \equiv 11 \cdot 9 + 5 \equiv 104 \pmod{11^2}$ 是 $x^2 \equiv 47 \pmod{11^2}$ 的一个解. 于是, 另一个解为 $x \equiv -104 \equiv 17 \pmod{11^2}$.

综上, $x^2 \equiv 47 \pmod{11^2}$ 的解为 $x \equiv 104 \pmod{11^2}$ 或 $x \equiv 17 \pmod{11^2}$.

**定理 3.3.** 设 $n$ 是一个奇数.

(1) $x^2 \equiv n \pmod 2$ 有且仅有一个解.

**定理 3.3.** 设 $n$ 是一个奇数.

(1) $x^2 \equiv n \pmod 2$ 有且仅有一个解.

(2) $x^2 \equiv n \pmod{2^2}$ 有解当且仅当 $n \equiv 1 \pmod 4$. 当 $x^2 \equiv n \pmod{2^2}$ 有解时, 它共有两个解.

**定理 3.3.** 设 $n$ 是一个奇数.

(1) $x^2 \equiv n \pmod 2$ 有且仅有一个解.

(2) $x^2 \equiv n \pmod{2^2}$ 有解当且仅当 $n \equiv 1 \pmod 4$. 当 $x^2 \equiv n \pmod{2^2}$ 有解时, 它共有两个解.

(3) 对任意 $\alpha \geq 3$, $x^2 \equiv n \pmod{2^\alpha}$ 有解当且仅当 $n \equiv 1 \pmod 8$. 当 $x^2 \equiv n \pmod{2^\alpha}$ 有解时, 它共有四个解; 若 $x_0$ 是它的一个解, 那么其余三个解分别为 $-x_0$ 和 $\pm x_0 + 2^{\alpha-1}$.

**定理 3.3.** 设 $n$ 是一个奇数.

(1) $x^2 \equiv n \pmod 2$ 有且仅有一个解.

(2) $x^2 \equiv n \pmod{2^2}$ 有解当且仅当 $n \equiv 1 \pmod 4$. 当 $x^2 \equiv n \pmod{2^2}$ 有解时, 它共有两个解.

(3) 对任意 $\alpha \geq 3$, $x^2 \equiv n \pmod{2^\alpha}$ 有解当且仅当 $n \equiv 1 \pmod 8$. 当 $x^2 \equiv n \pmod{2^\alpha}$ 有解时, 它共有四个解; 若 $x_0$ 是它的一个解, 那么其余三个解分别为 $-x_0$ 和 $\pm x_0 + 2^{\alpha-1}$.

**定理 3.3.** 设 $n$ 是一个奇数.

(1) $x^2 \equiv n \pmod 2$ 有且仅有一个解.

(2) $x^2 \equiv n \pmod{2^2}$ 有解当且仅当 $n \equiv 1 \pmod 4$. 当 $x^2 \equiv n \pmod{2^2}$ 有解时, 它共有两个解.

(3) 对任意 $\alpha \geq 3$, $x^2 \equiv n \pmod{2^\alpha}$ 有解当且仅当 $n \equiv 1 \pmod 8$. 当 $x^2 \equiv n \pmod{2^\alpha}$ 有解时, 它共有四个解; 若 $x_0$ 是它的一个解, 那么其余三个解分别为 $-x_0$ 和 $\pm x_0 + 2^{\alpha-1}$.

**例 3.3.** 解下面的同余方程:

(1) $x^2 \equiv 55 \pmod{2^8}$.

**例 3.3.** 解下面的同余方程:

(1) $x^2 \equiv 55 \pmod{2^8}$.

(2) $x^2 \equiv 41 \pmod{2^8}$.

**例 3.3.** 解下面的同余方程:

(1) $x^2 \equiv 55 \pmod{2^8}$.

(2) $x^2 \equiv 41 \pmod{2^8}$.

**例 3.3.** 解下面的同余方程:

(1) $x^2 \equiv 55 \pmod{2^8}$.

(2) $x^2 \equiv 41 \pmod{2^8}$.

**解:** (1) 因为 $55 \equiv 7 \pmod 8$, 所以由定理3.3(3) 知, $x^2 \equiv 55 \pmod{2^8}$ 无解.

## $x^2 \equiv 41 \pmod{2^8}$

(2) 因为 $41 \equiv 1 \pmod 8$, 所以由定理3.3(3) 知, $x^2 \equiv 41 \pmod{2^8}$ 有四个解. 显然 $x = 1$ 满足 $x^2 \equiv 41 \pmod{2^3}$.

## $x^2 \equiv 41 \pmod{2^8}$

(2) 因为 $41 \equiv 1 \pmod 8$, 所以由定理3.3(3) 知, $x^2 \equiv 41 \pmod{2^8}$ 有四个解. 显然 $x = 1$ 满足 $x^2 \equiv 41 \pmod{2^3}$. 由定理3.3(3) 的证明知,

$$x \equiv 1 + 2^2 \cdot \frac{41 - 1}{2^3} \equiv 5 \pmod{2^4}$$

是 $x^2 \equiv 41 \pmod{2^4}$ 的解.

## $x^2 \equiv 41 \pmod{2^8}$

(2) 因为 $41 \equiv 1 \pmod 8$, 所以由定理3.3(3) 知, $x^2 \equiv 41 \pmod{2^8}$ 有四个解. 显然 $x = 1$ 满足 $x^2 \equiv 41 \pmod{2^3}$. 由定理3.3(3) 的证明知,

$$x \equiv 1 + 2^2 \cdot \frac{41-1}{2^3} \equiv 5 \pmod{2^4}$$

是 $x^2 \equiv 41 \pmod{2^4}$ 的解. 同理, 有 $x \equiv 5 + 2^3 \cdot \frac{41-5^2}{2^4} \equiv 13 \pmod{2^5}$ 是 $x^2 \equiv 41 \pmod{2^5}$ 的解;

$x \equiv 13 + 2^4 \cdot \frac{41-13^2}{2^5} \equiv 13 \pmod{2^6}$ 是 $x^2 \equiv 41 \pmod{2^6}$ 的解; $x \equiv 13 + 2^5 \cdot \frac{41-13^2}{2^6} \equiv 13 \pmod{2^7}$ 是 $x^2 \equiv 41 \pmod{2^7}$ 的解; $x \equiv 13 + 2^6 \cdot \frac{41-13^2}{2^7} \equiv 13 \pmod{2^8}$ 是 $x^2 \equiv 41 \pmod{2^8}$ 的解.

## $x^2 \equiv 41 \pmod{2^8}$

(2) 因为 $41 \equiv 1 \pmod 8$, 所以由定理3.3(3) 知, $x^2 \equiv 41 \pmod{2^8}$ 有四个解. 显然 $x = 1$ 满足 $x^2 \equiv 41 \pmod{2^3}$.

由定理3.3(3) 的证明知,

$$x \equiv 1 + 2^2 \cdot \frac{41-1}{2^3} \equiv 5 \pmod{2^4}$$

是 $x^2 \equiv 41 \pmod{2^4}$ 的解. 同理, 有 $x \equiv 5 + 2^3 \cdot \frac{41-5^2}{2^4} \equiv 13 \pmod{2^5}$ 是 $x^2 \equiv 41 \pmod{2^5}$ 的解;

$x \equiv 13 + 2^4 \cdot \frac{41-13^2}{2^5} \equiv 13 \pmod{2^6}$ 是 $x^2 \equiv 41 \pmod{2^6}$ 的解; $x \equiv 13 + 2^5 \cdot \frac{41-13^2}{2^6} \equiv 13 \pmod{2^7}$ 是 $x^2 \equiv 41 \pmod{2^7}$ 的解; $x \equiv 13 + 2^6 \cdot \frac{41-13^2}{2^7} \equiv 13 \pmod{2^8}$ 是 $x^2 \equiv 41 \pmod{2^8}$ 的解.

故 $x^2 \equiv 41 \pmod{2^8}$ 的全部解为

$x \equiv \pm 13, \pm 13 + 2^7 \pmod{2^8}$.