第5章 二次同余方程

5.1 二次同余方程的概念及二次剩余

5.2 Legendre符号

5.3 Jacobi符号

5.4 Rabin密码体制

习题

5.1 二次同余方程的概念及二次剩余

5.1 二次同余方程的概念及二次剩余

由第4章知，解一般模数的二次同余方程可归结为解素数模的二次同余方程

$$ax^2+bx+c\equiv 0 \bmod p \quad (5.1)$$

其中 $p\nmid a$。

由 $p\nmid a$ 得$(p,a)=1,(p,4a)=1$，将（5.1）两边同乘以 $4a$，得 $4a^2x^2+4abx+4ac\equiv 0 \bmod p$，$(2ax+b)^2\equiv b^2-4ac \bmod p$，做可逆变换 $y=2ax+b$（因为$(p,2a)=1$），得（5.1）的等价同余方程 $y^2\equiv b^2-4ac \bmod p$。

所以只需讨论形如 $x^2 \equiv d \bmod p$ 的同余方程。当 $p \mid d$，方程只有一个解$0 \bmod p$，所以下面恒假设 $p \nmid d$。

定义1.1 设素数 $p > 2, a \in Z, p \nmid a$ 。如果同余方程

$$x^2 \equiv a \bmod p \quad (5.2)$$

有解，则称 a是模 p的二次剩余，否则称为模 p的二次非剩余。满足（5.2）式的 x称为 a的平方根。

例1.1 由 $x^2 \equiv 1 \bmod 3$ 得 $x \equiv \pm 1 \bmod 3$，所以1是模3的二次剩余，

$x^2 \equiv -1 \bmod 3$ 无解，-1是模3的二次非剩余

$x^2 \equiv 1 \bmod 5$ 得 $x \equiv \pm 1 \bmod 5$，1是模5的二次剩余，

$x^2 \equiv -1 \bmod 5$ 得 $x \equiv \pm 2 \bmod 5$，-1是模5的二次剩余，

$x^2 \equiv 2 \bmod 5$ 无解，2是模5的二次非剩余，

$x^2 \equiv -2 \bmod 5$ 无解，-2 是模5的二次非剩余。

已知 p，模 p 的二次剩余和二次非剩余元素的个数由以下定理给出。

定理1.1 在模 p 的一个简化剩余系中，恰有 $\frac{p-1}{2}$ 个二次剩余，$\frac{p-1}{2}$ 个二次非剩余。若 a 是二次剩余，则方程（5.2）有 2个解。

证明 取模 p 的绝对最小简化剩余系

$$-\frac{p-1}{2},-\frac{p-1}{2}+1,\cdots,-1,1,\cdots,\frac{p-1}{2}-1,\frac{p-1}{2}$$

a 是模 p 的二次剩余，当且仅当 a 与以下 p-1个值中的一个同余：

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

但由于$(-j)^2 \equiv j^2 \bmod p$，所以$a$是模$p$的二次剩余，当且仅当$a$与以下$\frac{p-1}{2}$个值中的一个同余：

$$1^2, \cdots, \left(\frac{p-1}{2}-1\right)^2, \left(\frac{p-1}{2}\right)^2 \bmod p \quad (5.3)$$

这 $\frac{p-1}{2}$ 个值中任意 2个不同余。否则设 $i^2 \equiv j^2 \bmod p$ ，则得 $(i+j)(i-j) \equiv 0 \bmod p$，所以 $p \mid i+j$ 或 $p \mid i-j$。但 $1 \leqslant i,j \leqslant \frac{p-1}{2}$ ，$2 \leqslant i+j \leqslant p-1$，$|i-j| \leqslant p-1$，所以 $i=j$，矛盾。所以（5.3）给出了模 p 的全部二次剩余，其余的 $p-1-\frac{p-1}{2}=\frac{p-1}{2}$ 个元素是二次非剩余。所以若 a 是二次剩余，a 必为（5.3）中的一项，而且仅为一项。

若 $x \equiv i \bmod p$ 是（5.2）的解，则 $x \equiv -i \bmod p$ 也是解，（5.2）有2个解。 证毕。

由以上证明过程可得如下推论。

推论 设 a 是模 p 的二次剩余，则 a 与 $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2 \pmod{p}$ 中的一个且仅与一个同余。

例1.2　求模19的二次剩余。

解　由定理1.1的推论，求模19的二次剩余就是在模19的绝对最小简化剩余系 $-9,-8,\cdots,-1,1,2,\cdots,9$ 中求 a 它与 $1^2,2^2,\cdots,9^2\pmod{19}$ 中的某一个同余，列表如下：

表5.1 模19的平方表

j	1	2	3	4	5	6	7	8	9
$a\equiv j^2 \bmod 19$	1	4	9	-3	6	-2	-8	7	5

所以模19的二次剩余是$1,-2,-3,4,5,6,7,-8,9$；二次非剩余是$-1,2,3,-4,-5,-6,-7,8,-9$。

反过来看这个表，可得每个二次剩余的2个解。例如6是二次剩余，它的2个解是$\pm 5 \bmod 19$。

下一定理可直接判断a是不是模p的二次剩余，可无需在模p的绝对最小简化剩余系中逐一验证。

定理1.2 设素数 $p>2$，$p\nmid a$，则 a 是模 p 的二次剩余的充要条件是

$$a^{\frac{p-1}{2}}\equiv 1 \bmod p$$

a 是模 p 的二次非剩余的充要条件是

$$a^{\frac{p-1}{2}}\equiv -1 \bmod p$$

证明 由于$x^{p-1}-1=\left(x^2\right)^{\frac{p-1}{2}}-a^{\frac{p-1}{2}}+a^{\frac{p-1}{2}}-1=\left(x^2-a\right)q(x)+\left(a^{\frac{p-1}{2}}-1\right)$

由第4章定理4.5得$x^2-a\equiv 0 \bmod p$有2个解（即a是模p的二次剩余）的充要条件是$x^2-a \mid x^p-x=x\left(x^{p-1}-1\right)$。因$x^2-a\equiv 0 \bmod p$没有0解，即$x^2-a$没有$x$因子，所以$x^2-a \mid x^{p-1}-1$。等价于$a^{\frac{p-1}{2}}-1\equiv 0 \bmod p$，即$a^{\frac{p-1}{2}}\equiv 1 \bmod p$。又由于$(a^{\frac{p-1}{2}}+1)(a^{\frac{p-1}{2}}-1)\equiv a^{p-1}-1\equiv 0 \bmod p$，其中第2个同余式由Euler定理得。所以$p \mid a^{\frac{p-1}{2}}+1$ 或$p \mid a^{\frac{p-1}{2}}-1$。但2式不能同时成立，否则$a^{\frac{p-1}{2}}\equiv -1 \bmod p$且$a^{\frac{p-1}{2}}\equiv 1 \bmod p$，得$-1\equiv 1 \bmod p$，$2\equiv 0 \bmod p$，矛盾。

所以a是模p的二次非剩余的充要条件是 $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ 。

证毕。

从上述证明过程还可见，如果a是模p的二次剩余，

$a^{\frac{p-1}{2}} - 1 \equiv 0 \bmod p$ ，$x^2 - a \mid x^p - x$，因此 $x^2 - a \equiv 0 \bmod p$ 有2个解，这也是定理1.1的结论。

推论1 -1是模 p的二次剩余的充要条件是 $p \equiv 1 \bmod 4$。

证明 取模4的最小非负完全剩余系 $0,1,2,3$，当且仅当p在最小非负完全剩余系中取 1，即 $p \equiv 1 \bmod 4$ 时，满足方程 $(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$。 证毕。

推论2 设素数 $p>2$，$p\nmid a_1, p\nmid a_2$，则

(1) 若 a_1，a_2 均为模 p 的二次剩余，则 a_1a_2 也是模 p 的二次剩余。

(2) 若 a_1，a_2 均为模 p 的二次非剩余，则 a_1a_2 是模 p 的二次剩余。

(3) 若 a_1 是模 p 的二次剩余，a_2 是模 p 的二次非剩余，则 a_1a_2 是模 p 的二次非剩余。

证明 因为 $\left(a_1a_2\right)^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}a_2^{\frac{p-1}{2}}$，由定理1.2即得。

证毕。

例1.3 判断3是否为模17的二次剩余，7是否为模29的二次剩余。

解 因为$3^2 \equiv 9 \bmod 17 \equiv -8 \bmod 17$, $3^4 \equiv -4 \bmod 17$, $3^8 \equiv 16 \equiv -1 \bmod 17$

所以3是模17的二次非剩余。

$7^2 \equiv -9 \bmod 29$ ， $7^3 \equiv -5 \bmod 29$ ， $7^4 \equiv -6 \bmod 29$ ，

$7^7 \equiv 7^3 \cdot 7^4 \equiv 1 \bmod 29$ ，$7^{14} \equiv 1 \bmod 29$，7是模29的二次剩余。

5.2 Legendre符号

5.2 Legendre符号

要判断a是否为模p的二次剩余，由定理1.1要逐一检验a是否与$1^2,2^2,\cdots,(\frac{p-1}{2})^2 \pmod p$中的某一个同余，或者由定理1.2计算$a^{\frac{p-1}{2}} \bmod p$的值。当$p$很大时，两个方法都不实用。本节介绍一种简单方法，即求a模p的Legendre符号。

定义2.1 设素数 $p>2$，定义Legendre符号如下：

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{当 } a \text{ 是模 } p \text{ 的二次剩余；}\\ -1, & \text{当 } a \text{ 是模 } p \text{ 的二次非剩余；}\\ 0, & \text{当 } p \mid a \text{。}\end{cases}$$

所以要判断 a 是否为模 p 的二次剩余，只需计算 $\left(\frac{a}{p}\right)$ 即可。

Legendre符号有以下性质：

定理2.1 (1) $\left(\frac{a}{p}\right)=\left(\frac{p+a}{p}\right)$，一般地 $\left(\frac{a}{p}\right)=\left(\frac{a+kp}{p}\right)$，其中 $k\in Z$；

(2) $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \bmod p$；

(3) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$，即Legendre符号是完全积性的；

(4) 当 $p\nmid a$ 时，$\left(\frac{a^2}{p}\right)=1$；

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

证明极简单，略。

由上可见，当 a 增加时，$\left(\frac{a}{p}\right)$ 以 p 为周期，若 $a>p$，则总能求出 $q<p$，$(p,q)=1$，使得 $\left(\frac{a}{p}\right)=\left(\frac{q}{p}\right)$。

下面考虑如何求 $\left(\frac{2}{p}\right)$ 及一般形式的 $\left(\frac{q}{p}\right)$，为此需要以下的Gauss引理。

引理2.1 （Gauss引理）设素数 $p>2, p\nmid a$ ，如果

$$a\cdot 1, a\cdot 2, \cdots, a\cdot\frac{p-1}{2} \pmod p \quad (2.1)$$

中大于 $\frac{p}{2}$ 的元素个数为 n，则 $\left(\frac{a}{p}\right)=(-1)^n$ 。

证明 在（2.1）的 $\frac{p-1}{2}$ 个数中，当 $i\neq j$ 时，$ai\not\equiv aj \bmod p$

否则由 $(a,p)=1$ 得 $i\equiv j \bmod p$ 。

将其中大于 $\frac{p}{2}$ 的数记为 $r_1,\cdots,r_n$，小于 $\frac{p}{2}$ 的数记为 $s_1,\cdots,s_t$

显然 $1\leqslant p-r_i<\frac{p}{2}(1\leqslant i\leqslant n)$，且 $p-r_i\not\equiv s_j \bmod p(1\leqslant j\leqslant t)$ ，

这是因为$-\frac{p}{2}<-s_j<0$,$-\frac{p}{2}+1<p-r_i-s_j<\frac{p}{2}$, $p-r_i-s_j\not\equiv 0 \bmod p$

所以$p-r_1$,…, $p-r_n$, $s_1,\cdots,s_t$ 就是 $1,2,\cdots,\frac{p-1}{2}$ 的一个排列。

将（2.1）中的 $\frac{p-1}{2}$ 个数乘在一起，得

$$a^{\frac{p-1}{2}}\cdot\frac{p-1}{2}!\equiv s_1\cdots s_t\cdot r_1\cdots r_n=(-1)^n s_1\cdots s_t(p-r_1)\cdots(p-r_n)\equiv(-1)^n\frac{p-1}{2}!$$

又因 $\left(\frac{p-1}{2}!,p\right)=1$ ，所以 $a^{\frac{p-1}{2}}\equiv(-1)^n \bmod p$ 。 证毕。

高斯引理

对于一个与 p 互素的整数 a, Gauss 给出了另一判别法则, 以判断 a 是否为模 p 二次剩余.

引理4.3.1 (Gauss) 设 p 是奇素数. a 是整数, $(a,p)=1$. 如果整数

$$a\cdot 1,\ a\cdot 2,\ \ldots,\ a\cdot\frac{p-1}{2}$$

中模 p的最小正剩余大于$\frac{p}{2}$ 的个数是 m, 则

$$\left(\frac{a}{p}\right)=(-1)^m. \tag{3.17}$$

证 设 $a_1,\ \ldots,\ a_t$ 是 $a\cdot 1,\ a\cdot 2,\ \ldots,\ a\cdot\frac{p-1}{2}$ 模 p的小于 $\frac{p}{2}$ 的最小正剩余, $b_1,\ \ldots,\ b_m$ 是这些整数模 p 的大于 $\frac{p}{2}$ 的最小正剩余, 则

$$\left(\frac{a}{p}\right) = (-1)^m. \tag{3.17}$$

****

$$a^{\frac{p-1}{2}}(\frac{p-1}{2})! = \prod_{k=1}^{\frac{p-1}{2}}(a\cdot k) \equiv \prod_{i=1}^{t} a_i \prod_{j=1}^{m} b_j \equiv (-1)^m \prod_{i=1}^{t} a_i \prod_{j=1}^{m}(p-b_j) \pmod p.$$

易知$a_1, \ldots, a_t, p-b_1, \ldots, p-b_m$ 是模p 两两不同余的. 否则,

$$a\cdot k_i \equiv p - a\cdot k_j, \quad \text{或} \quad a\cdot k_i + a\cdot k_j \equiv 0 \pmod p.$$

因而$k_i + k_j \equiv 0 \pmod p$, 这不可能, 因为 $1 \le k_i + k_j \le \frac{p-1}{2} + \frac{p-1}{2} < p.$

这样, $a_1, \ldots, a_t, p-b_1, \ldots, p-b_m$ 是$1, \ldots, \frac{p-1}{2}$ 的一个排列,

$$a^{\frac{p-1}{2}}(\frac{p-1}{2})! \equiv (-1)^m \prod_{i=1}^{t} a_i \prod_{j=1}^{m}(p-b_j) = (-1)^m(\frac{p-1}{2})! \pmod p.$$

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

定理2.2 设素数 $p>2$，

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

（2）当 $(a,2p)=1$ 时，$\left(\frac{a}{p}\right)=(-1)^T$，其中 $T=\sum_{j=1}^{(p-1)/2}\left\lfloor\frac{ja}{p}\right\rfloor$。

证明 当 $1\leqslant j\leqslant\frac{p-1}{2}$ 时，因为 $ja=p\cdot\left\lfloor\frac{ja}{p}\right\rfloor+t_j$，其中 $0<t_j<p$，对该式两边求和，左 $=a\left(1+2+\cdots+\frac{p-1}{2}\right)=a\cdot\frac{p^2-1}{8}$

$$右=p\cdot\sum_{j=1}^{(p-1)/2}\left\lfloor\frac{ja}{p}\right\rfloor+\sum_{j=1}^{(p-1)/2}t_j=p\cdot T+\sum_{i=1}^{t}s_i+\sum_{j=1}^{n}r_j$$

$$=pT+\sum_{i=1}^{t}s_i+\sum_{j=1}^{n}(p-r_j)-np+2\sum_{j=1}^{n}r_j$$

由引理2.1的证明知 $s_1,\cdots,s_t,p-r_1,\cdots,p-r_n$ 是 $1,\cdots,\dfrac{p-1}{2}$ 的一个排列，$\sum_{i=1}^{t}s_i+\sum_{j=1}^{n}\left(p-r_j\right)=\dfrac{p^2-1}{8}$，得 $(a-1)\dfrac{p^2-1}{8}=(T-n)p+2\sum_{j=1}^{n}r_j$

$$(a-1)\frac{p^2-1}{8}\equiv(T-n)p\bmod 2\equiv(T-n)\bmod 2\equiv(T+n)\bmod 2。$$

当 $a=2$ 时，对 $1\leqslant j\leqslant\dfrac{p-1}{2}$，$ja\le p-1$，$\left\lfloor\dfrac{ja}{p}\right\rfloor=0$，所以 $T=\sum_{j=1}^{(p-1)/2}\left\lfloor\dfrac{ja}{p}\right\rfloor=0$，所以 $n\equiv\dfrac{p^2-1}{8}\bmod 2$，

而当 $(a,2p)=1$ 时，a 必为奇数，$a-1\equiv 0\bmod 2$，所以上式得 $T\equiv n\bmod 2$，由Gauss引理即得 $\left(\dfrac{a}{p}\right)=(-1)^T$。 证毕。

T的几何意义：

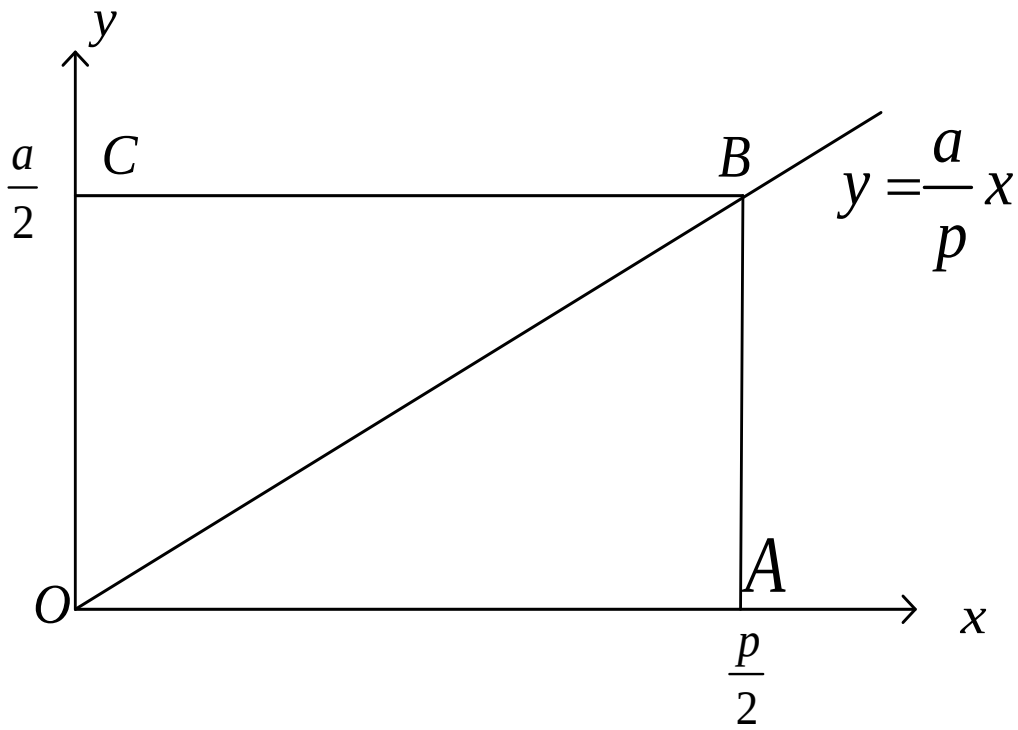

图1　*Rt*! *OAB* 内部的整数点的个数示例

表示图1中 x轴、直线 $x=\frac{p}{2}$ 、直线 $y=\frac{a}{p}x$ 所围成的内部的整数点的个数，这是因为

（1） 线段 AB 上 $x=\frac{p}{2}$，无整数点。线段 OB 上，因 $(a,p)=1, p \nmid a$ ，无整数点。

（2） 当 $0<j<\frac{p}{2}$ 时，线段 $x=j$ 上整数点个数为 $\left\lfloor \frac{aj}{p} \right\rfloor$，所以 $Rt\triangle OAB$ 内部整数点个数为 $\sum_{j=0}^{p-1/2} \left\lfloor \frac{aj}{p} \right\rfloor = T$。

如果 $a=q$，其中 $q\neq p$ 为素数，则有 $\left(\frac{q}{p}\right)=(-1)^T$。类似地有 $\left(\frac{p}{q}\right)=(-1)^S$，其中 $S=\sum_{l=1}^{(q-1)/2}\left\lfloor\frac{lp}{q}\right\rfloor$ 为图1中 $Rt\triangle OCB$ 内部整数点个数。

而 $S+T$ 是矩形 $OABC$ 内部整数点的个数，因此 $S+T=\frac{p-1}{2}\cdot\frac{q-1}{2}$

所以有 $\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right)=(-1)^{S+T}=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$。得如下定理。

定理2.3（二次互反律） 设素数 p,q 均大于 2，$p\neq q$，则

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

或写成

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

二次互反律的意义：$\left(\frac{a}{p}\right)$ 以 p 为周期，若 $a>p$，则总能找到 $q<p$，$(p,q)=1$，使得 $\left(\frac{a}{p}\right)=\left(\frac{q}{p}\right)$。由二次互反律知，要求 $\left(\frac{q}{p}\right)$，只须求 $\left(\frac{p}{q}\right)$，它的周期 $q<p$，即所求的Legendre符号的周期越来越小，最后变为求形如 $\left(\frac{1}{p}\right)$ 或 $\left(\frac{2}{p}\right)$ 的Legendre符号。

例2.1 求 $\left(\frac{137}{227}\right)$

解 227为素数，

$$\left(\frac{137}{227}\right)=\left(\frac{-90}{227}\right)=\left(\frac{-1}{227}\right)\left(\frac{2\cdot 3^2\cdot 5}{227}\right)=(-1)\left(\frac{2}{227}\right)\left(\frac{3^2}{227}\right)\left(\frac{5}{227}\right)$$

其中 $\left(\frac{2}{227}\right)=(-1)^{\frac{227^2-1}{8}}=-1$，$\left(\frac{3^2}{227}\right)=1$，$\left(\frac{5}{227}\right)=\left(\frac{227}{5}\right)=\left(\frac{2}{5}\right)=-1$

所以 $\left(\frac{137}{227}\right)=-1$。表明同余方程 $x^2\equiv 137 \bmod 227$ 无解。

例2.2 判断同余方程（1）$x^2 \equiv -1 \bmod 365$；

（2） $x^2 \equiv 2 \bmod 3599$ 是否有解，有解时求出其解数。

解 （1） 365 不是素数，$365 = 5 \cdot 73$，所以同余方程与同余方程组 $\begin{cases} x^2 \equiv -1 \bmod 5 \\ x^2 \equiv -1 \bmod 73 \end{cases}$ 等价。由 $\left(\frac{-1}{5}\right) = 1, \left(\frac{-1}{73}\right) = 1$，同余方程组有解，原方程的解数为4。

（2） 3599 不是素数，$3599 = 59 \cdot 61$，同余方程等价于同余方程组 $\begin{cases} x^2 \equiv 2 \bmod 59 \\ x^2 \equiv 2 \bmod 61 \end{cases}$ 由于 $\left(\frac{2}{59}\right) = -1$，所以无解。

例2.3 求所有奇素数p，它分别以3为其二次剩余和二次非剩余。

解 就是分别求满足$\left(\frac{3}{p}\right)=1$和$\left(\frac{3}{p}\right)=-1$的奇素数$p$。

因为$\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$，由定理1.2的推论1，

$(-1)^{\frac{p-1}{2}}=\begin{cases}1, & p\equiv 1 \bmod 4\\ -1, & p\equiv -1 \bmod 4\end{cases}$。在求$\left(\frac{p}{3}\right)$时，将$p=3,5,7,11,13,17,19,\cdots$一一代入知$p=7,13,19,\cdots$（即$p=6k+1\ (k\in N)$）时为$1$，$p=5,11,17,\cdots$（即$p=6k+5, k\in N$）时为$-1$，所以

$$\left(\frac{p}{3}\right)=\begin{cases}\dfrac{1}{3}=1, & p\equiv 1 \bmod 6\\ \left(\dfrac{-1}{3}\right)=-1, & p\equiv -1 \bmod 6\end{cases}$$

所以$\left(\frac{3}{p}\right)=1$ 的充要条件是$p\equiv 1 \bmod 4$ 且 $p\equiv 1 \bmod 6$ ，即 $p\equiv 1 \bmod 12$；或 $p\equiv -1 \bmod 4$ 且 $p\equiv -1 \bmod 6$ ，即 $p\equiv -1 \bmod 12$。

而$\left(\frac{3}{p}\right)=-1$ 的充要条件是 $p\equiv 1 \bmod 4$ 且 $p\equiv -1 \bmod 6$ ，或 $p\equiv -1 \bmod 4$且 $p\equiv 1 \bmod 6$ 。即 $p\equiv 5 \bmod 4$ 且$p\equiv 5 \bmod 6$ 或$p\equiv -5 \bmod 4$且 $p\equiv -5 \bmod 6$ 。所以$p\equiv 5 \bmod 12$或$p\equiv -5 \bmod 12$

例2.4 分别求以11为其二次剩余和二次非剩余的所有奇素数 p。

解 $$\left(\frac{11}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{11}\right),\ (-1)^{\frac{p-1}{2}}=\begin{cases}1, p\equiv 1 \bmod 4\\ -1, p\equiv -1 \bmod 4\end{cases}。$$

对模11的绝对最小完全剩余系 $\pm 1, \pm 2, \pm 3, \pm 4, \pm 5$ 中的每个值计算可得

$$\left(\frac{p}{11}\right)=\begin{cases}1, & p\equiv 1,-2,3,4,5 \pmod{11}\\ -1, & p\equiv -1,2,-3,-4,-5 \pmod{11}\end{cases}$$

由同余方程组 $\begin{cases} p \equiv a_1 \bmod 4 \\ p \equiv a_2 \bmod 11 \end{cases}$ 得 $p \equiv \left(-11a_1 + 12a_2\right) \bmod 44$。

$\left(\frac{11}{p}\right) = 1$ 当且仅当 $a_1 = 1, a_2 = 1, -2, 3, 4, 5,$ 或

$a_1 = -1, a_2 = -1, 2, -3, -4, -5$，所以 $p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \ (\bmod 44)$

同理 $\left(\frac{11}{p}\right) = -1$ 当且仅当 $a_1 = 1, a_2 = -1, 2, -3, -4, -5$；或

$a_1 = -1, a_2 = 1, -2, 3, 4, 5$。所以 $p = \pm 3, \pm 13, \pm 15, \pm 17, \pm 21 (\bmod 44)$

例2.5 证明满足 $p \equiv 1 \bmod 4$ 的素数有无穷多个。

证明 反证，假设满足条件的素数有有限个，它们构成的集合记为 $A=\{p_1,\cdots,p_k\}$，构造 $P=1+(2p_1\cdots p_k)^2$，满足 $P \equiv 1 \bmod 4$，P不是素数，否则 $P \in A$，不可能。

设 p是 P的素因子，则 $\left(\frac{-1}{p}\right)=\left(\frac{-1+P}{p}\right)=\left(\frac{2(p_1\cdots p_k)^2}{p}\right)=1$ 。

由定理1.2的推论1，$p \equiv 1 \bmod 4$，所以 $p \in A$ 。由 $p \mid P$ ，$p \mid (2p_1\cdots p_k)^2$，得 $p \mid \left(P-(2p_1\cdots p_k)^2\right)=1$，矛盾。

5.3 Jacobi符号

5.3 Jacobi符号

在求Legendre符号$\left(\frac{a}{p}\right)$时，需要求出a的素因数分解，然后再用Legendre符号的性质和二次互反律，但当a很大时，计算复杂。为了避免这种复杂的计算，引入Jacobi符号。

定义3.1 设$P=p_1\cdots p_s$，其中$p_j(1\leqslant j\leqslant s)$是素数，定义$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_s}\right)$，其中$\left(\frac{a}{p_j}\right)(1\leqslant j\leqslant s)$是模$p_j$的Legendre符号。称$\left(\frac{a}{P}\right)$为Jacobi符号。

由定义3.1及Legendre符号的性质，容易推出Jacobi符号有以下性质。

定理3.1

(1) $\left(\frac{1}{P}\right)=1$;

(2) $\left(\frac{a}{P}\right)=\begin{cases}0, & (a,P)>1\\ \pm 1, & (a,P)=1\end{cases}$;

(3) $\left(\frac{a}{P}\right)=\left(\frac{a+P}{P}\right)$;

(4) $\left(\frac{ab}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$;

(5) $\left(\frac{a}{P_1P_2}\right)=\left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)$;

(6) 当 $(a,P)=1$ 时, $\left(\frac{a^2}{P}\right)=\left(\frac{a}{P^2}\right)=1$ 。

为了得到Jacobi符号的进一步性质，需要以下引理。

引理3.1 设 $a_j \equiv 1 \bmod m\,(1 \leqslant j \leqslant s), a = a_1 \cdots a_s$ ，则

$$\frac{a-1}{m} \equiv \frac{a_1-1}{m} + \cdots + \frac{a_s-1}{m} \pmod{m}$$

证明 对 s 用归纳法。$s=2$ 时，

$a-1=a_1a_2-1=(a_1-1)+(a_2-1)+(a_1-1)(a_2-1)$，由 $a_j \equiv 1 \bmod m$，知 $a \equiv 1 \bmod m$，所以

$$\frac{a-1}{m} \equiv \frac{a_1-1}{m} + \frac{a_2-1}{m} + \frac{(a_1-1)(a_2-1)}{m} \equiv \frac{a_1-1}{m} + \frac{a_2-1}{m} \pmod{m},$$

其中第3项中 $m^2 \mid (a_1-1)(a_2-1)$ 。

设 $s=k$ 时，结论成立，

当 $s=k+1$ 时，$a=(a_1\cdots a_2)a_{k+1}$，$\dfrac{a-1}{m}\equiv\dfrac{a_1\cdots a_k-1}{m}+\dfrac{a_{k+1}-1}{m}\pmod m$

$\equiv\left(\dfrac{a_1-1}{m}+\cdots+\dfrac{a_k-1}{m}\right)+\dfrac{a_{k+1}-1}{m}\pmod m$ 。 证毕。

定理3.2 $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$，$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$。

证明 设 $P=p_1\cdots p_s$，则 $\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_s}\right)=(-1)^{\frac{p_1-1}{2}}\cdots(-1)^{\frac{p_s-1}{2}}$

$=(-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_s-1}{2}}$。在引理3.1中，取 $m=2,a_j=p_j(1\leqslant j\leqslant s)$，

得 $\frac{p_1-1}{2}+\cdots+\frac{p_s-1}{2}\equiv\frac{P-1}{2}\bmod 2$，所以 $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$，

$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\cdots\left(\frac{2}{p_s}\right)=(-1)^{\frac{p_1^2-1}{8}}\cdots(-1)^{\frac{p_s^2-1}{8}}=(-1)^{\frac{p_1^2-1}{8}+\cdots+\frac{p_s^2-1}{8}}$。

由于 p_j 是奇素数，设 $p_j = 2k+1$，则 $p_j^2 - 1 = 4k(k+1)$，k 和 $(k+1)$ 是2个连续的整数，必有一个偶数，所以 $8 \mid (p_j^2 - 1)$，$p_j^2 \equiv 1 \bmod 8$ 。

在引理3.1中，取 $m = 8, a_j = p_j^2 (1 \leqslant j \leqslant s)$ ，就有

$$\frac{P^2-1}{8} \equiv \frac{p_1^2-1}{8} + \cdots + \frac{p_s^2-1}{8} \pmod 8$$，所以 $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$。

证毕。

Jacobi符号也有互反律。

定理3.3 设 P,Q 是奇数，满足 $P>1,Q>1,(P,Q)=1$，则 $\left(\frac{Q}{P}\right)\cdot\left(\frac{P}{Q}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$。

证明 设 $P=p_1\cdots p_s,Q=q_1\cdots q_r$，其中 p_j,q_i 都为素数，且 $p_j\neq q_i$（否则与 $(P,Q)=1$ 矛盾）（$1\leqslant j\leqslant s,1\leqslant i\leqslant r$）。

$$\left(\frac{Q}{P}\right)=\prod_{j=1}^{s}\left(\frac{Q}{p_j}\right)=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)=\prod_{j=1}^{s}\prod_{i=1}^{r}\left[\left(\frac{p_j}{q_i}\right)(-1)^{\frac{p_j-1}{2}\frac{q_i-1}{2}}\right]$$

$$=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_j}{q_i}\right)\cdot\prod_{j=1}^{s}\prod_{i=1}^{r}(-1)^{\frac{p_j-1}{2}\frac{q_i-1}{2}}$$

$$=\left(\frac{P}{Q}\right)\cdot(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_j-1}{2}\frac{q_i-1}{2}}=\left(\frac{P}{Q}\right)\cdot(-1)^{\sum_{j=1}^{s}\frac{p_j-1}{2}\cdot\sum_{i=1}^{r}\frac{q_i-1}{2}}$$

$$=\left(\frac{P}{Q}\right)(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}$$

最后一步由定理3.2的证明过程得。 证毕。

以上性质表明：为了计算Jacobi符号（包括Legendre符号作为它的特殊情形），我们并不需要求素因子分解式。例如105虽然不是素数，在计算Legendre符号$\left(\frac{105}{317}\right)$时，可以先把它看作Jacobi符号来计算，由上述两个定理得：

$$\left(\frac{105}{317}\right)=\left(\frac{317}{105}\right)=\left(\frac{2}{105}\right)=1$$

一般在计算$\left(\frac{m}{n}\right)$时，如果有必要，可用$m \bmod n$代替m，而互反律用以减小$\left(\frac{m}{n}\right)$中的n。

可见，引入Jacobi符号对计算Legendre符号是十分方便的，但应强调指出Jacobi符号和Legendre符号的本质差别是： Jacobi符号 $\left(\frac{a}{n}\right)$ 不表示方程 $x^2 \equiv a \bmod n$ 是否有解。比如 $n = p_1 p_2$, a 关于 p_1 和 p_2 都不是二次剩余，即 $x^2 \equiv a \bmod p_1$ 和 $x^2 \equiv a \bmod p_2$ 都无解，由中国剩余定理知 $x^2 \equiv a \bmod n$ 也无解。但是，由于 $\left(\frac{a}{p_1}\right) = \left(\frac{a}{p_2}\right) = -1$ ，所以 $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) = 1$ 。即 $x^2 \equiv a \bmod n$ 虽无解，但Jacobi符号 $\left(\frac{a}{n}\right)$ 却为1。

例3.1 考虑方程 $x^2 \equiv 2 \bmod 3599$，由于 $3599=59\times 61$ ，所以方程等价于方程组

$$\begin{cases} x^2 \equiv 2 \bmod 59 \\ x^2 \equiv 2 \bmod 61 \end{cases}$$

由于 $\left(\frac{2}{59}\right)=-1$，所以方程组无解，但Jacobi符号

$$\left(\frac{2}{3599}\right)=(-1)^{\left(3599^2-1\right)/8}=1$$ 。

5.4 Rabin密码体制

5.4 Rabin密码体制

Rabin密码体制是基于大整数分解问题及二次剩余问题的。设 n是两个大素数 p和q的乘积。由定理1.1知，1到 $p-1$之间有一半是模p的二次剩余（记这些数的集合为 Q_p），另一半是模 p的二次非剩余（记这些数的集合为NQ_p），对 q也有类似结论（分别记两个集合为Q_q和 NQ_q）。另一方面，a是模n的二次剩余，当且仅当a既是模 p的二次剩余也是模q的二次剩余，即 $a \in Q_p \bigcap Q_q$ 。所以对满足

$$0<a<n,(a,n)=1$$

的 a，有一半满足 $\left(\frac{a}{n}\right)=1$（$a\in Q_p\bigcap Q_q$ 或 $a\in NQ_p\bigcap NQ_q$）另一半满足 $\left(\frac{a}{n}\right)=-1$（$a\in Q_p\bigcap NQ_q$ 或 $a\in NQ_p\bigcap Q_q$ ）。而在满足 $\left(\frac{a}{n}\right)=1$ 的 a 中，有一半满足 $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$（$a\in Q_p\bigcap Q_q$ ），这些 a 就是模 n 的二次剩余；另一半满足 $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$（$a\in NQ_p\bigcap NQ_q$），这些 a 是模 n 的二次非剩余。

设a是模n的二次剩余，即存在x使得 $x^2 \equiv a \bmod n$ 成立，因 a既是模 p的二次剩余，又是模 q的二次剩余，所以存在 y、z，使得 $(\pm y)^2 \equiv a \bmod p, (\pm z)^2 \equiv a \bmod q$。当 $p \equiv q \equiv 3 \bmod 4$ 时，y 和 z 可容易地求出。

定理4.1 设素数$p \equiv 3 \bmod 4$，若a是模p的二次剩余，则a的平方根是$\pm a^{\frac{p+1}{4}} \bmod p$。

证明 由$p \equiv 3 \bmod 4$得，$p+1=4k$，即$\frac{1}{4}(p+1)$是一整数。因a是模p的二次剩余，故

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

设 $x^2 \equiv a \bmod p$ 的根为 y，即 $y^2 \equiv a \bmod p$，则

$$\left(a^{\frac{p+1}{4}}\right)^2 \equiv \left(y^{\frac{p+1}{2}}\right)^2 \equiv \left(y^2\right)^{\frac{p+1}{2}} \equiv a^{\frac{p+1}{2}} \equiv a^{(p-1)/2} \cdot a \equiv a \bmod p$$

所以 $a^{\frac{p+1}{4}}$ 和 $p - a^{\frac{p+1}{4}}$ 是方程 $x^2 \equiv a \bmod p$ 的两个根。

证毕。

定理4.2　设$n=pq$，求解方程 $x^2 \equiv a \bmod n$ 与分解n是等价的。

证明　当已知n的分解 p和 q, 可分别得方程$x^2 \equiv a \bmod p$和$x^2 \equiv a \bmod q$, 设2个方程的解分别是$x \equiv \pm y \bmod p, x \equiv \pm z \bmod q$由中国剩余定理可求得 $x \bmod n$，即为$a \bmod n$ 的四个平方根。

反过来，已知 $a \bmod n$ 的两个不同的平方根（$u \bmod n$ 和 $w \bmod n$，且$u \not\equiv \pm w \bmod n$），就可分解$n$。

事实上由 $u^2 \equiv w^2 \bmod n$ 得 $(u+w)(u-w) \equiv 0 \bmod n$，但 n 不能整除 $u+w$ 也不能整除 $u-w$，否则由 $n \mid (u+w)$ 或 $n \mid (u-w)$ 得 $u \equiv -w \bmod n$ 或 $u \equiv w \bmod n$。

由 $(u+w)(u-w) \equiv 0 \bmod n$ 得 $p \mid (u+w)(u-w)$ 及 $q \mid (u+w)(u-w)$ 所以必有 $p \mid (u+w)$ 或 $p \mid (u-w)$ 及 $q \mid (u+w)$ 或 $q \mid (u-w)$。

当 $p\left|(u+w)\right.$ 时，必有 $q\nmid(u+w)$，否则 $n=pq\left|(u+w),u\equiv -w \bmod n\right.$。所以当 $p\left|(u+w)\right.$ 时，必有 $q\left|(u-w)\right.$。同理当 $p\left|(u-w)\right.$ 时，必有 $q\left|(u+w)\right.$。

在第一种情况下，$(n,u+w)=p,\quad (n,u-w)=q$ ；

在第二种情况下，$(n,u-w)=p,\quad (n,u+w)=q$。因此得到了 $\boldsymbol{n}$的两个因子。

证毕。

对RSA密码体制， 被分解成功，该体制便被破译，即破译RSA的难度不超过大整数的分解。但还不能证明破译RSA和分解大整数是等价的，虽然这一结论已得到普遍共识。

Rabin密码体制是对RSA的一种修正，它有以下两个特点：

- 它不是以一一对应的单向陷门函数为基础，对同一密文，可能有两个以上对应的明文。
- 破译该体制等价于对大整数的分解。

RSA中选取的公开钥 e 满足 $1<e<\varphi(n)$，且 $(e,\varphi(n))=1$。

Rabin密码体制则取 $e=2$ 。

1．密钥的产生

随机选择两个大素数 p、q ，满足 $p\equiv q\equiv 3 \bmod 4$ ，即这两个素数形式为 $4k+3$；计算 $n=p\cdot q$ 。以 n 作为公开钥，p 、q 作为秘密钥。

2．加密

$$c\equiv m^2 \bmod n$$

其中 m 是明文分组，c 是对应的密文分组。

3．解密

解密就是求 c 模 n 的平方根，即解 $x^2 \equiv c \bmod n$ 。由定理4.1和定理4.2可得方程的4个解，即每一密文对应的明文不唯一。为了有效地确定明文,可在 m 中加入某些信息，如发送者的身份号、接收者的身份号、日期、时间等。

习题

1. 设 p 是奇素数，

(1) 证明：模 p 的所有二次剩余的乘积对模 p 的剩余是 $(-1)^{\frac{p+1}{2}}$

(2) 证明：模 p 的所有二次非剩余的乘积对模 p 的剩余是 $(-1)^{\frac{p-1}{2}}$

(3) 证明：模 p 的所有二次剩余之和对模 p 的剩余是：当 $p=3$ 时为1，当 $p>3$ 时为0；

(4) 所有二次剩余之和对模 p 的剩余是多少？

2. 求Legendre符号：

(1) $\left(\frac{13}{47}\right)$ (2) $\left(\frac{91}{563}\right)$ (3) $\left(\frac{-286}{647}\right)$

3.（1）求以-3为其二次剩余的全体素数；

（2）求以± 3为其二次剩余的全体素数；

（3）求以± 3为二次非剩余的全体素数；

（4）求以3为二次剩余、-3为二次非剩余的全体素数；

（5）求以3为二次非剩余、-3为二次剩余的全体素数；

（6）求100^2-3、150^2+3的素因数分解式。

4. 设p是素数，$p\equiv 3 \bmod 4$，证明：$2p+1$是素数的充要条件是$2^p \equiv 1 \bmod (2p+1)$。

5. 设素数 $p \geq 3$，$p \nmid a$，证明：$\sum_{x=1}^{p}\left(\frac{ax+b}{p}\right)=0$。

6. 判断下列同余方程是否有解：

（1）$x^2 \equiv 7 \bmod 227$；（2）$5x^2 \equiv -14 \bmod 6193$。

7. 设 a, b 是正整数，$2 \nmid b$，证明对Jacobi符号有以下结论：

$$\left(\frac{a}{2a+b}\right)=\begin{cases}\left(\frac{a}{b}\right), & a \equiv 0,1 \pmod 4;\\ -\left(\frac{a}{b}\right), & a \equiv 2,3 \pmod 4。\end{cases}$$