The Collection of Difficult Problem of Elementary Number Theory

(The Second Volume)

初等数论难题集

（第二卷）

下

主　编　刘培杰

副主编　周晓东　田廷彦　许逸飞

哈尔滨工业大学出版社

HARBIN INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书共分7章:第1章同余,第2章数列中的数论问题,第3章多项式,第4章数论与函数,第5章二次剩余与同余方程,第6章不定方程,第7章数论与组合.

本书适合于数学奥林匹克竞赛选手和教练员,高等院校相关专业研究人员及数论爱好者.

图书在版编目(CIP)数据

初等数论难题集.第2卷.下/刘培杰主编.—哈尔滨:哈尔滨工业大学出版社,2010.12

ISBN 978-7-5603-2921-5

Ⅰ.①初… Ⅱ.①刘… Ⅲ.①初等数论-解题 Ⅳ.①0156.1-44

中国版本图书馆CIP数据核字(2010)第223125号

策划编辑 刘培杰
责任编辑 张永芹
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街10号 邮编150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市石桥印务有限公司
开 本 787mm×1092mm 1/16 印张30.75 字数600千字
版 次 2011年2月第1版 2011年2月第1次印刷
书 号 ISBN 978-7-5603-2921-5
印 数 1~3000册
定 价 128.00元(上、下册)

◎目录

心得 体会 拓广 疑问

第5章　二次剩余与同余方程

5.1　二次剩余

设 p 是奇素数，a 是整数，$p \nmid a$. 如果存在整数 x，使得 $x^2 \equiv a(\mathrm{mod}\ p)$，则称 a 是模 p 的二次剩余，否则称 a 是模 p 的二次非剩余. 例如 1 是模 3 的二次剩余，而 -1 是模 3 的二次非剩余.

当 x 取遍模 p 的缩剩余系 $\left\{\pm 1, \pm 2, \cdots, \pm\frac{p-1}{2}\right\}$ 中的每一个数时，x^2 的取值有 $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ 共 $\frac{p-1}{2}$ 种可能.

设整数 i, j 满足 $1 \leqslant i < j \leqslant \frac{p-1}{2}$，则 $0 < j-i < j+i < p$，故 $(j-i)(j+i) \not\equiv (\mathrm{mod}\ p)$，即 $i^2 \not\equiv j^2(\mathrm{mod}\ p)$. 这说明上述 $\frac{p-1}{2}$ 个数对模 p 互不同余. 从而在模 p 的每个缩剩余系中恰有 $\frac{p-1}{2}$ 个数是模 p 的二次剩余，而另 $(p-1)-\frac{p-1}{2}=\frac{p-1}{2}$ 个数是模 p 的二次非剩余. 且 $x^2 \equiv d(\mathrm{mod}\ p)$ 的解数为 0 或 2.

定理(欧拉判别法)　p 为大于 2 的素数，$p \nmid d$，d 是模 p 的二次剩余的充要条件是

$$d^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$$

d 是模 p 的二次非剩余的充要条件是

$$d^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\ p)$$

定理　设素数 $p > 2$，$p \nmid d_1$，$p \nmid d_2$，若 d_1 与 d_2 均为模 p 的二次剩余或均为模 p 的二次非剩余，则 $d_1 d_2$ 也是模 p 的二次剩余.

若 d_1 是二次剩余，d_2 是二次非剩余，则 $d_1 d_2$ 是二次非剩余.

引进勒让德符号如下

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

这里 $p > 2$ 为素数，d 为整数.

勒让德符号有以下性质：

心得 体会 拓广 疑问

(1)$\left(\frac{d}{p}\right)=\left(\frac{p+d}{p}\right)$;

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

(3)$\left(\frac{dc}{p}\right)=\left(\frac{d}{p}\right)\left(\frac{c}{p}\right)$;

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

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

于是计算勒让德符号变为计算:

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

定理 $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & p\equiv\pm1(\bmod 8)\\ -1, & p\equiv\pm3(\bmod 8)\end{cases}$.

定理(高斯二次互反律) 设p,q为奇素数,$p\neq q$,则

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

设奇数$p>1$,$p=p_1p_2\cdots p_s$,$p_i(1\leqslant i\leqslant s)$为素数,定义$\left(\frac{d}{p}\right)=\left(\frac{d}{p_1}\right)\cdots\left(\frac{d}{p_s}\right)$,$\left(\frac{d}{p_i}\right)$为勒让德符号,则$\left(\frac{d}{p}\right)$为雅可比符号.

注意$\left(\frac{d}{p}\right)=1$不代表$x^2\equiv d(\bmod p)$一定有解.

雅可比符号的性质有些很易推导,注意有:

$\left(\frac{dc}{p}\right)=\left(\frac{d}{p}\right)\left(\frac{c}{p}\right)$;

$\left(\frac{d}{p_1p_2}\right)=\left(\frac{d}{p_1}\right)\left(\frac{d}{p_2}\right)$;

$(p,d)=1$时,$\left(\frac{d^2}{p}\right)=\left(\frac{d}{p^2}\right)=1$.

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

定理 若$P,Q>1$,为奇数,$(P,Q)=1$,则

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

5.1.1 设p是奇素数. 证明:-1是模p的二次剩余的充要条件是$p\equiv1(\bmod 4)$.

证明 先证必要性. 设有整数a,使得$a^2\equiv-1(\bmod p)$,显然$p\nmid a$,故由费马小定理知

心得 体会 拓广 疑问

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

从而$\frac{p-1}{2}$应为偶数，即 $p \equiv 1 \pmod 4$.

再证充分性. 若 $p \equiv 1 \pmod 4$，即$\frac{p-1}{2}$为偶数，于是

$$\begin{aligned}(p-1)! &= 1 \times 2 \times \cdots \times \frac{p-1}{2} \times (p-1) \times \\ &\quad (p-2) \times \left(p - \frac{p-1}{2}\right) \equiv \\ &\quad 1 \times 2 \times \cdots \times \frac{p-1}{2} \times (-1) \times (-2) \times \cdots \times \\ &\quad \left(-\frac{p-1}{2}\right) \pmod{p} = \\ &\quad (-1)^{\frac{p-1}{2}} \times 1^2 \times 2^2 \times \cdots \times \left(\frac{p-1}{2}\right)^2 = \\ &\quad \left[\left(\frac{p-1}{2}\right)!\right]^2\end{aligned}$$

从而由威尔逊定理即知$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$.

本题的这个结论十分重要，利用它便可以证明形如 $4n+1$，$n=1,2,\cdots$ 的质数有无限多个.

5.1.2　证明：形如 $p \equiv 1 \pmod 4$ 的素数有无穷多个.

证明　设N是任意正整数，$p_1, p_2, \cdots, p_s$是不超过N的全部形如 $p \equiv 1 \pmod 4$ 的素数. 令

$$q = 4(p_1 p_2 \cdots p_s)^2 + 1$$

如果 q 本身是素数，由于 $p_i (i = 1,2,\cdots,s)$ 为素因数，故必有 $q > N$，而 $q \equiv 1 \pmod 4$，从而存在大于N的形如 $p \equiv 1 \pmod 4$ 的素数 q.

如果q本身不是素数，由于q是奇数，故它必具有奇素因数a，$q \equiv 0 \pmod a$. 从而 -1 是模a的平方剩余，$\left(\frac{-1}{a}\right) = 1$. 因此，必有 $a \equiv 1 \pmod 4$. 又由于$p_i \nmid q (i = 1,2,\cdots,s)$，故 $a \neq p_i (i = 1,2,\cdots, s)$，从而知 $a > N$. 这表示存在大于N的形如 $p \equiv 1 \pmod 4$ 的素数 a.

由于N是任取之正整数，因此形如 $p \equiv 1 \pmod 4$ 的素数有无穷多个.

心得 体会 拓广 疑问

5.1.3 (1)设p是素数,如果a和b是模p的平方剩余,取c使$a \equiv bc(\mathrm{mod}\ p)$,则$c$也是模$p$的平方剩余.

(2)证明:若$ab \equiv 1(\mathrm{mod}\ p)$($p$是素数),则$a$和$b$同时为模$p$的平方剩余或同时为非平方剩余.试推广上述结论,找出关于r的条件,当$ab \equiv r(\mathrm{mod}\ p)$时,$a$和$b$同为模$p$的平方剩余或同为非平方剩余.

证明 (1)由于a和b均与p互素,所以c也与p互素,故有

$$\left(\frac{a}{p}\right)=\left(\frac{bc}{p}\right)=\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)$$

由于a和b均为模p的平方剩余,故$\left(\frac{a}{p}\right)=1$,$\left(\frac{b}{p}\right)=1$,从而$\left(\frac{c}{p}\right)=1$,所以$c$是模$p$的平方剩余.

(2)由于

$$1=\left(\frac{1}{p}\right)=\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

故当$\left(\frac{a}{p}\right)=1$时,$\left(\frac{b}{p}\right)=1$,又当$\left(\frac{a}{p}\right)=-1$时,$\left(\frac{a}{p}\right)=-1$,$p$为素数,故$a$和$b$同为平方剩余,或同为非平方剩余.

显然当r是模p的平方剩余时,即当

$$\left(\frac{r}{p}\right)=1$$

时,a,b同为平方剩余或同为非平方剩余.

5.1.4 如果p是任一奇素数,证明:分数$\frac{1}{p}$的小数展式有$\frac{p-1}{2}$位数字的循环,或循环的位数是$\frac{p-1}{2}$的因数,当且仅当$p=\pm 3^{K}(\mathrm{mod}\ 40)$.

证明 当且仅当$10^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$,就会出现$\frac{p-1}{2}$位数字的循环小数展开式,或循环位数为$\frac{p-1}{2}$的某些因子.这就是欧拉准则:10是二次余式$(\mathrm{mod}\ p)$.

现在已知5是形如$5n \pm 1$的任何素数的二次余式,而8是形如$8m \pm 1$为任何素数的二次余数.又如果5和2都是余式或都非余式,则10是一个二次余式$(\mathrm{mod}\ p)$.于是p必为上述两种形式或者都不是;即$p=4n \pm r$,其中$r=1,3,9$或27.因为$3^4=81=1(\mathrm{mod}\ 40)$,这就是所求的结果(已经假定$p \neq 5$).

心得 体会 拓广 疑问

5.1.5　设 p 是素数，证明：当 $p \equiv 1 \pmod 4$ 时，两整数 a 和 $p-a$ 同为平方剩余或同为非平方剩余；而当 $p \equiv 3 \pmod 4$ 时，a 和 $p-a$ 中一个是平方剩余，另一个是非平方剩余.

证明　由于 $p-a \equiv -a \pmod p$，故

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

当 $p \equiv 1 \pmod 4$ 时，有 $\left(\frac{-1}{p}\right)=1$，故

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

因此，当 $\left(\frac{a}{p}\right)=1$ 时，$\left(\frac{p-a}{p}\right)=1$；当 $\left(\frac{a}{p}\right)=-1$ 时，$\left(\frac{p-a}{p}\right)=-1$. p 又为素数，所以 a 和 $p-a$ 同为模 p 的平方剩余或同为非平方剩余，反之亦然.

又当 $p \equiv 3 \pmod 4$ 时，$\left(\frac{-1}{p}\right)=-1$，从而

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

因此，当 $\left(\frac{a}{p}\right)=1$ 时，$\left(\frac{p-a}{p}\right)=-1$，当 $\left(\frac{a}{p}\right)=-1$ 时，$\left(\frac{p-a}{p}\right)=1$，$p$ 又为素数，故两数 a 和 $p-a$ 一个是模的平方剩余，另一个是非平方剩余.

5.1.6　证明：

(1) $n^2+(n+1)^2=2m^2$ 不可能成立.

(2) 仅当 -1 是模 k 的平方剩余时，$n^2+(n+1)^2=km^2$ 才能成立.

证明　(1) 如果 $n^2+(n+1)^2=2m^2$ 成立，则有

$$n^2+(n+1)^2 \equiv 0 \pmod 2$$

但 $n^2+(n+1)^2=2n^2+2n+1$，于是

$$n^2+(n+1)^2 \equiv 1 \pmod 2$$

因此便有 $1 \equiv 0 \pmod 2$，但这不可能.

(2) 当 $n^2+(n+1)^2=km^2$ 成立时，就有 $n^2+(n+1)^2 \equiv 0 \pmod k$，于是有

$$2n^2+2n+1 \equiv 0 \pmod k$$

故有

$$4n^2+4n+2 \equiv 0 \pmod k$$

$$4n^2+4n+1 \equiv -1 \pmod k$$

心得 体会 拓广 疑问

即 $$(2n+1)^2 \equiv -1 \pmod{k}$$

这表示 $x=2n+1$ 是同余式 $x^2 \equiv -1 \pmod{k}$ 的解,故 -1 是模 k 的平方剩余.

5.1.7 证明:如果 x 和 y 没有公因子,则 $x^{2^n}+y^{2^n}$(其中 n 是正整数)的每一个奇数因子为形式 $2^{n+1}m+1$.

证明 设 p 是一奇素数,使得 $x^{2^n}+y^{2^n} \equiv 0 \pmod{p}$. 因为 $(x,y)=1$,所以有 $x \not\equiv 0, y \not\equiv 0 \pmod{p}$,于是

$$(xy^{-1})^{2^n} \equiv -1 \pmod{p}$$

其中 y^{-1} 是模 p 剩余的乘法群中 y 的逆. 所以同余式

$$u^{2^n} \equiv -1 \pmod{p}$$

有解. 根据欧拉准则

$$(-1)^{\frac{p-1}{d}} \equiv 1 \pmod{p} \qquad ①$$

其中 $d=(p-1,2^n)$. 由①可得 $\frac{p-1}{d}$ 是偶数. 于是根据 d 的定义,得出 $p-1$ 可被 2^{n+1} 除尽. 因此

$$p=2^{n+1}m+1 \qquad ②$$

最后,因为式②的那些数的每一个乘积也是上述形式. 本题得证.

5.1.8 设正奇数 m 的素因数分解式是

$$m=p_1^{l_1}p_2^{l_2}\cdots p_r^{l_r}$$

这时,如果 $(a,m)=1$,则定义 $\left(\frac{a}{m}\right)$ 的意义如下

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)^{l_1}\left(\frac{a}{p_2}\right)^{l_2}\cdots\left(\frac{a}{p_r}\right)^{l_r}$$

其中 $\left(\frac{a}{p_i}\right)$ $(i=1,2,\cdots,r)$ 是勒让德符号. 称 $\left(\frac{a}{m}\right)$ 为雅可比(Jacobi)符号. 试证明:

(1) 若 $a \equiv b \pmod{m}$,则 $\left(\frac{a}{m}\right)=\left(\frac{b}{m}\right)$;

(2) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$, $\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$;

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

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

(5) $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$.

心得 体会 拓广 疑问

证明　(1) 如果 $a \equiv b(\bmod m)$,则

$$a \equiv b(\bmod p_i)(i = 1,2,\cdots,r)$$

故由勒让德符号的性质,有

$$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right) \quad (i = 1,2,\cdots,r)$$

再由$\left(\frac{a}{m}\right)$的定义,知(1)成立.

(2) 由于

$$\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)(i = 1,2,\cdots,r)$$

故(2)的第一式成立.

将 mn 作素因数分解,就可得到第二式.

(3) 设 $m > 1$,当 $m = p_1 p_2,\cdots,p_s(p_1,p_2,\cdots,p_s$ 均为奇素数,不必相异),根据定义

$$\left(\frac{-1}{m}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_s}\right)$$

由勒让德符号的性质,有

$$\left(\frac{-1}{p_i}\right) = (-1)^{\frac{p_i-1}{2}}(i = 1,2,\cdots,s)$$

于是

$$\left(\frac{-1}{m}\right) = (-1)^{\sum_{i=1}^{s}\frac{p_i-1}{2}}$$

为此只要证明

$$\sum_{i=1}^{s}\frac{p_i - 1}{2} \equiv \frac{p_1 p_2\cdots p_s - 1}{2} \equiv \frac{m-1}{2}(\bmod 2)$$

当 $s = 2$ 时,由于$(p_1 - 1)(p_2 - 1) \equiv 0(\bmod 4)$,故

$$(p_1 - 1)(p_2 - 1) = p_1 p_2 - (p_1 + p_2) + 1 = (p_1 p_2 - 1) - (p_1 - 1) - (p_2 - 1) \equiv 0(\bmod 4)$$

从而有

$$\frac{p_1 p_2 - 1}{2} \equiv \frac{p_1 - 1}{2} + \frac{p_2 - 1}{2}(\bmod 2)$$

又因为$(p_1 p_2\cdots p_k - 1)(p_{k+1} - 1) \equiv 0(\bmod 4)$,故

$$(p_1 p_2\cdots p_{k+1} - 1) \equiv (p_1 p_2\cdots p_k - 1) + (p_{k+1} - 1)(\bmod 4)$$

从而有

$$\frac{p_1 p_2\cdots p_{k+1} - 1}{2} \equiv \frac{p_1 p_2\cdots p_k - 1}{2} \equiv \frac{p_{k+1} - 1}{2}(\bmod 2)$$

再由归纳法假设,对于一切正整数 s,就有

$$\sum_{i=1}^{s}\frac{p_i - 1}{2} \equiv \frac{p_1 p_2\cdots p_s - 1}{2} = \frac{m-1}{2}(\bmod 2)$$

心得 体会 拓广 疑问

故 $$\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$$

(4) 由

$$\left(\frac{2}{m}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_s}\right)$$

而 $$\left(\frac{2}{p_i}\right)=(-1)^{\frac{p_i^2-1}{8}}(i=1,2,\cdots,s)$$

故 $$\left(\frac{2}{m}\right)=(-1)^{\sum_{i=1}^{s}\frac{p_i^2-1}{8}}$$

为此,只需证明

$$\sum_{i=1}^{s}\frac{p_i^2-1}{8}\equiv\frac{(p_1p_2\cdots p_s)^2-1}{8}\equiv\frac{m^2-1}{8}(\mathrm{mod}\ 2)$$

当 $s=2$ 时,由于 $p_1^2-1\equiv 0(\mathrm{mod}\ 8)$,$p_2^2-1\equiv 0(\mathrm{mod}\ 8)$,故

$$(p_1^2-1)(p_2^2-1)\equiv 0(\mathrm{mod}\ 64)$$

从而

$$(p_1^2-1)(p_2^2-1)=(p_1p_2)^2-(p_1^2+p_2^2)+1=[(p_1p_2)^2-1]-(p_1^2-1)-(p_2^2-1)\equiv 0(\mathrm{mod}\ 64)$$

故

$$\frac{(p_1p_2)^2-1}{8}\equiv\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}(\mathrm{mod}\ 2)$$

又由于 $[(p_1p_2\cdots p_k)^2-1](p_{k+1}^2-1)\equiv 0(\mathrm{mod}\ 64)$,故

$$(p_1p_2\cdots p_{k+1})^2-1\equiv[(p_1p_2\cdots p_k)^2-1]+[p_{k+1}^2-1](\mathrm{mod}\ 64)$$

从而

$$\frac{(p_1p_2\cdots p_{k+1})^2-1}{8}\equiv\frac{(p_1p_2\cdots p_k)^2-1}{8}+\frac{p_{k+1}^2-1}{8}(\mathrm{mod}\ 2)$$

再由归纳法假设,对于任意正整数 s,就有

$$\frac{(p_1p_2\cdots p_s)^2-1}{8}\equiv\sum_{i=1}^{s}\frac{p_i^2-1}{8}(\mathrm{mod}\ 2)$$

故有

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

(5) 设 m,n 的素因数分解为

$$m=p_1p_2\cdots p_r,n=q_1q_2\cdots q_s$$

根据定义,有

$$\left(\frac{n}{m}\right)=\left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_r}\right)$$

心得 体会 拓广 疑问

$$\left(\frac{m}{n}\right)=\left(\frac{p_1}{n}\right)\left(\frac{p_2}{n}\right)\cdots\left(\frac{p_r}{n}\right)$$

从而有

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=\left(\frac{p_1}{n}\right)\left(\frac{p_2}{n}\right)\cdots\left(\frac{p_r}{n}\right)\left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_r}\right)=$$

$$\left(\frac{p_1}{n}\right)\left(\frac{n}{p_1}\right)\left(\frac{p_2}{n}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{p_r}{n}\right)\left(\frac{n}{p_r}\right)$$

由于有$\frac{m-1}{2}\equiv\sum_{i=1}^{r}\frac{p_i-1}{2}(\bmod 2)$，为此只需证明

$$\left(\frac{p_i}{n}\right)\left(\frac{n}{p_i}\right)=(-1)^{\frac{p_i-1}{2}\cdot\frac{n-1}{2}}(i=1,2,\cdots,r)$$

由于

$$\left(\frac{n}{p_i}\right)=\left(\frac{q_1}{p_i}\right)\left(\frac{q_2}{p_i}\right)\cdots\left(\frac{q_s}{p_i}\right)$$

$$\left(\frac{p_i}{n}\right)=\left(\frac{p_i}{q_1}\right)\left(\frac{p_i}{q_2}\right)\cdots\left(\frac{p_i}{q_s}\right)(i=1,2,\cdots,r)$$

$$\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)=(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}(i=1,2,\cdots,r;j=1,2,\cdots,s)$$

又由于$\sum_{j=1}^{s}\frac{q_j-1}{2}\equiv\frac{n-1}{2}(\bmod 2)$，故

$$\left(\frac{n}{p_i}\right)\left(\frac{p_i}{n}\right)=(-1)^{\sum_{i=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_i-1}{2}}=(-1)^{\frac{p_i-1}{2}\cdot\frac{n-1}{2}}$$

因此$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$.

注　本题引进的符号$\left(\frac{a}{m}\right)$称为雅可比符号，所以引进这个符号，是因为在计算勒让德符号之值时，最大的困难是分解分子成素因数，在分子很大时，这实际上办不到，雅可比符号可避免这个困难. 另外，雅可比符号和勒让德符号相异之处是当$\left(\frac{a}{m}\right)=1$时，$a$不一定是模$m$的平方剩余. 例如，$\left(\frac{2}{3}\right)=-1$，$\left(\frac{2}{5}\right)=-1$，于是由定义就有$\left(\frac{2}{15}\right)=1$，但2不是模15的平方剩余.

5.1.9　设p是奇素数，证明：模p的平方剩余类的个数是$\frac{p-1}{2}$. 当$l\geqslant 3$时，模2^l的平方剩余类有几个？

证法1　模p的最小绝对剩余系是

$$\pm\frac{p-1}{2},\ \pm\frac{p-3}{2},\cdots,\ \pm 2,\ \pm 1,0$$

心得 体会 拓广 疑问

显然,模 p 的平方剩余类除了这些数的平方所属的剩余类外,别无其他. 另一方面,可以证明

$$\left(\frac{p-1}{2}\right)^2,\left(\frac{p-3}{2}\right)^2,\cdots,2^2,1$$

各自所属的剩余类是相异的$\left(\text{共}\frac{p-1}{2}\text{个}\right)$. 事实上,设

$$1\leqslant i\leqslant\frac{p-1}{2},1\leqslant j\leqslant\frac{p-1}{2}$$

如果有 $i^2\equiv j^2(\bmod p)$,则 $i^2-j^2=(i+j)(i-j)\equiv 0(\bmod p)$,从而 $p\mid(i+j)$ 或 $p\mid(i-j)$,但由于 $0<i+j\leqslant\frac{p-1}{2}+\frac{p-1}{2}<p$,故 $p\nmid(i+j)$,因此

$$i\equiv j(\bmod p)$$

又因为 $|i-j|\leqslant i+j<p$,故 $i=j$,所以$\left(\frac{p-1}{2}\right)^2,\left(\frac{p-3}{2}\right)^2,\cdots,2^2,1$ 所属的剩余类互异,这样便证明了模 p 的平方剩余类的个数是 $\frac{p-1}{2}$.

证法 2 设模 p 的一个简化剩余系为

$$a_1,a_2,\cdots,a_{p-1}$$

同余式 $x^2\equiv a_i^2(\bmod p)(i=1,2,\cdots,p-1)$ 的解关于模 p 是两个,所以在 $a_1^2,a_2^2,\cdots,a_{p-1}^2$ 中与 a_i^2 属于同一个剩余类的,除了 a_i^2 外,必还有一个. 也就是说,$a_1^2,a_2^2,\cdots,a_{p-1}^2$ 中两两属于同一个剩余类. 所以模 p 的平方剩余类的个数是 $\frac{p-1}{2}$.

又因为模 2^l 的简化类的个数是

$$\varphi(2^l)=2^l\left(1-\frac{1}{2}\right)=2^{l-1}$$

如设模 2^l 的一个简化剩余系是

$$a_1,a_2,\cdots,a_r(r=2^{l-1})$$

同余式

$$x^2\equiv a_i^2(\bmod 2^l)(i=1,2,\cdots,r)$$

有四个解,因此 $a_1^2,a_2^2,\cdots,a_r^2$ 中每四个属于一个平方剩余类,所以模 2^l 的平方剩余类的个数是

$$\frac{r}{4}=\frac{2^{l-1}}{4}=2^{l-3}$$

5.1.10 由无穷递减的费马方法证明形如 $3n+2$ 的奇素数 p 有二次非剩余 -3.

心得 体会 拓广 疑问

证明　如果 -3 不是所有形如 $3n+2$ 的素数的非剩余，则设 p 是这种形式的满足同余式 $x^2 \equiv 3 \pmod{p}$ 的最小奇素数，设 $x=e$ 是这一同余式的解，这里 $e<p$，可以假定 e 是偶数，因为如果 e 是奇数，则同余式的另一解 $p-e$ 将是偶数. 首先考虑 $e^2 \equiv 1 \pmod{3}$ 的情形，记

$$e^2 \equiv -3 \pmod{p} \text{ 或 } e^2 = -3 + fp, f < p, f \text{ 奇数} \qquad ①$$

因此 $pf = e^2 + 3 \equiv 4 \pmod{3}$，因为 $p \equiv 2 \pmod{3}$，得

$$f \equiv 2 \pmod{3}$$

此时 f 是奇数且形如 $3n+2$，它一定有一个形如 $3n+2$ 的奇素数因子 q，因为如果它所有的因子形如 3 或 $3n+1$，则它们的乘积将形如 $3n$ 和 $3n+1$，由 ①，有 $e^2 \equiv -3 \pmod{f}$，则

$$e^2 \equiv -3 \pmod{q}$$

而这后一同余式，与 -3 是形如 $3n+2$ 的最小素数 p 的二次剩余这一假设矛盾.

现在考虑 $e^2 \equiv 0 \pmod{3}$ 的情形，记 $e = 3^a k, k \not\equiv 0 \pmod{3}$，因 $e^2 \equiv -3 \pmod{p}$，有 $3^{2a}k^2 \equiv -3 \pmod{p}$；至此

$$3^{2a-1}k^2 \equiv -1 \pmod{p}$$

或

$$3^{2a-1}k^2 + 1 = ph, h < p, h \text{ 奇数} \qquad ②$$

因此 $ph \equiv 1 \pmod{3}$，而 $p \equiv 2 \pmod{3}$，则 $h \equiv 2 \pmod{3}$，因此 h 是奇数且形如 $3n+2$，它一定有形如 $3n+2$ 的奇素数因子 r，由 ② 有 $3^{2a-1}k^2 \equiv -1 \pmod{h}$，因此 $3^{2a-1}k^2 \equiv -1 \pmod{r}$，且 $3^{2a}k^2 \equiv -3 \pmod{r}$.

因为再次导出不存在形如 $3n+2$ 的最小奇素数，-3 是其二次剩余这样的矛盾，因而证明了定理，由此可得，形如 $3n+2$ 的素数 p 的任意非二次剩余对形如 $-3a^2, a = 1, 2, \cdots, \dfrac{p-1}{2}$ 的数是同余 $(\bmod p)$.

5.1.11　证明：对任给正整数 m, n，总存在正整数 k，使得 $2^k - m$ 至少有 n 个不同的素因子.

证明　固定 m，不妨设 m 为奇数. 现证明对任何正整数 n，总存在 k_n，使得 $2^{k_n} - m$ 至少有 n 个不同的素因子. 对 n 用归纳法：

(1) 当 $n=1$ 时，$2^{3m} - m$ 至少有一个素因子.

(2) 假设 $2^{k_n} - m$ 至少有 n 个不同的素因子，令 $A_n = 2^{k_n} - m$，则 $(A_n, 2) = 1$，且 $2^{k_n + \varphi(A_n^2)} - m \equiv 2^{k_n} - m \equiv A_n \pmod{A_n^2}$，因此

$$A_n \mid 2^{k_n + \varphi(A_n^2)} - m$$

心得 体会 拓广 疑问

取素数 $p, p \mid \dfrac{2^{k_n+\varphi(A_n^2)}-m}{A_n}$. 由 $\dfrac{2^{k_n+\varphi(A_n^2)}-m}{A_n} \equiv 1 \pmod{A_n}$, 知 p 不能整除 A_n, 所以 $2^{k_n+\varphi(A_n^2)}-m$ 至少有 $n+1$ 个不同素因子. 由数学归纳法知结论成立.

5.1.12 证明:形如 $p \equiv 1 \pmod 8$ 的素数有无穷多个.

证明 设 N 是任意正整数, $p_1, p_2, \cdots, p_s$ 是不超过 N 的一切形如 $p \equiv 1 \pmod 8$ 的素数. 记

$$q = (2p_1p_2\cdots p_s)^4 + 1$$

显然 q 的任意素因数 a 异于 2, 且 $x = 2p_1p_2\cdots p_s$ 是同余式

$$x^4 + 1 \equiv 0 \pmod a$$

的解. 因此 $a \equiv 1 \pmod 8$. 又由于 $p_i (i = 1,2,\cdots,s)$ 不是 q 的因数, 故 $a \neq p_i (i = 1,2,\cdots,s)$, 从而 $a > N$. 因此形如 $p \equiv 1 \pmod 8$ 的素数有无穷多个.

5.1.13 证明:形如 $p \equiv 7 \pmod 8$ 的素数有无穷多个.

证明 设 N 是任意正整数, $p_1, p_2, \cdots, p_s$ 是不超过 N 的一切形如 $p \equiv 7 \pmod 8$ 的素数, 记

$$q = (p_1p_2\cdots p_s)^2 - 2$$

由于 p_i 是形如 $p \equiv 7 \pmod 8$ 的素数, 故必为奇素数. 从而 $(p_1p_2\cdots p_s)^2$ 是奇数, 所以 $2 \nmid q$. 今设 a 是 q 的任一素因数(如果 q 本身是素数, a 就取作 q), 于是 $q \equiv 0 \pmod a$, 2 是模 a 的平方剩余, 即 $\left(\dfrac{2}{a}\right) = 1$. 根据定理, 知 $a \equiv 1 \pmod 8$ 或者 $a \equiv 7 \pmod 8$. 又由于 $p_i^2 \equiv 7^2 \equiv 1 \pmod 8$, 故

$$q = p_1^2p_2^2\cdots p_s^2 - 2 \equiv -1 \pmod 8$$

因此, 如果对于 q 的一切素因数 a 均有 $a \equiv 1 \pmod 8$, 那么就有 $q \equiv 1 \pmod 8$, 但这与 $q \equiv -1 \pmod 8$ 矛盾. 所以 q 一定含有形如 $a \equiv 7 \pmod 8$ 的素因数. 又由于 $p_i \nmid q (i = 1,2,\cdots,s)$, 故 $a \neq p_i (i = 1,2,\cdots,s)$, 从而 $a > N$. 这表示存在大于任取正整数 N 的素数 a, 故形如 $p \equiv 7 \pmod 8$ 的素数有无穷多个.

5.1.14 证明:形如 $p \equiv 3 \pmod 8$ 的素数有无穷多个.

证明 设 N 是任意正整数, $p_1, p_2, \cdots, p_s$ 是不超过 N 的一切形如 $p \equiv 3 \pmod 8$ 的素数, 记

$$q = (p_1p_2\cdots p_s)^2 + 2$$

心得 体会 拓广 疑问

显然,q 的任意素因数 a 均异于 2,否则将有 $(p_1p_2\cdots p_s)^2 \equiv 0 \pmod 2$,即 $p_1p_2\cdots p_s \equiv 0 \pmod 2$,但是 $p_i \equiv 3 \equiv 1 \pmod 2$ $(i = 1,2,\cdots,s)$,这是不可能的. 于是 -2 是模 a 的平方剩余,即

$$\left(\frac{-2}{a}\right) = 1$$

因此,$a \equiv 1 \pmod 8$ 或 $a \equiv 3 \pmod 8$. 如果 q 的所有素因数均有 $a \equiv 1 \pmod 8$,那么就应有 $q \equiv 1 \pmod 8$,这样就有

$$(p_1p_2\cdots p_s)^2 \equiv -1 \pmod 8$$

但是,$p_i(i = 1,2,\cdots,s)$ 均为奇数,应有 $p_i^2 \equiv 1 \pmod 8$,这样就有 $1 \equiv -1 \pmod 8$,这是不可能的. 因此 q 的素因数中,一定有形如 $a \equiv 3 \pmod 8$ 的素因数,又由于 $a \neq p_i(i = 1,2,\cdots,s)$,故必有 $a > N$. 因此形如 $p \equiv 3 \pmod 8$ 的素数有无穷多个.

5.1.15　证明:形如 $p \equiv 1 \pmod 6$ 的素数有无穷多个.

证明　设 N 是任意正整数,$p_1,p_2,\cdots,p_s$ 是不超过 N 的一切形如 $p \equiv 1 \pmod 6$ 的素数,记

$$q = 4(p_1p_2\cdots p_s)^2 + 3$$

q 的任意素因数 a 不能是 2,否则 $3 \equiv 0 \pmod 2$,这是不可能的. 因此 -3 是模 a 的平方剩余,即

$$\left(\frac{-3}{a}\right) = 1$$

由 $a \equiv 1 \pmod 6$,可以证明 $a \neq p_i(i = 1,2,\cdots,s)$. 事实上,如果 a 与某个 p_i 相等,则 $3 \equiv 0 \pmod a$,但是 a 是形如 $a \equiv 1 \pmod 6$ 的素数,故这是不可能的. 从而 $a > N$. 因此形如 $p \equiv 1 \pmod 6$ 的素数有无穷多个.

注　由本题知,形如 $p \equiv 1 \pmod 3$ 的素数也有无穷多个. 在习题中,读者不难证明,形如 $p \equiv 2 \pmod 3$ 的素数也有无穷多个.

狄利克雷曾经证明,只要 $(a,b) = 1$,那么形如 $p \equiv a \pmod b$ 的素数有无穷多个. 这里 $(a,b) = 1$ 是必要的,例如只有一个素数具有形式 $p \equiv 3 \pmod 6$,它就是 3,而没有一个素数具有 $p \equiv 4 \pmod 6$ 的形式. 狄利克雷的重大贡献在于条件 $(a,b) = 1$ 还是充分的. 要证明这个重要定理,已不属于初等数论的范围.

5.1.16　设 $F_n = 2^{2^n} + 1, n > 1$,则 F_n 的任一素因数 p 具有形状 $p = 2^{n+2}k + 1, k > 0$.

证明　因为 $2^{2^n} \equiv -1 \pmod p$,可设

$$p = 2^{n+1}h + 1, h > 0 \qquad ①$$