《网络空间安全数学基础》

杨 波 编著

课后习题参考答案

说明：如有错误请联系 water@snnu.edu.cn 进行更正，谢谢。

第 1 章

1. 证明：若$a|b$且$c|d$，则$ac|bd$。

解：由$a|b$可知，存在$q_1 \in Z$，使得$b = aq_1$

由$c|d$可知，存在$q_2 \in Z$，使得$d = cq_2$

因此有$bd = ac(q_1q_2)$，即$ac|bd$得证。

2. 设$n \neq 1$，证明$(n-1)^2 | n^k - 1$的充要条件是$(n-1)|k$。

解：由$(n-1+1)^k = C_k^0(n-1)^k + C_k^1(n-1)^{k-1} + ... + C_k^{k-1}(n-1) + 1$知

$n^k - 1 = (n-1)^k + ... + k(n-1)$除最后一项外，其余各项均含$(n-1)^2$因子。

充分性：

由$(n-1)|k$，则有$(n-1)^2 | k(n-1)$

因此有$(n-1)^2 | n^k - 1$成立

必要性：

由$(n-1)^2 | n^k - 1 == (n-1)^k + \cdots + k(n-1)$

可知$(n-1)^2 | k(n-1)$，即$(n-1)|k$。

3. 设$q \neq 0, \pm 1$。若对任意的a、b由$q|ab$可推出$q|a$或$q|b$至少有一个成立，证明：q一定是素数。

解：假设q是合数，则至少存在两个素因子，不妨设$q = q_1q_2$（$q_1 \leq q_1$）。

由$q = q_1q_2 | ab$有$ab = tq_1q_2$，$t \in Z$，

因此或a、或b、或ab中必有q_1q_2因子。

不妨设a中存在q_1因子（不存在q_2），b中存在q_2因子（不存在q_1），则得到

$q=q_1q_2\,|\,a$ 且 $q=q_1q_2\,|\,b$ 均不成立，矛盾，因此 q 一定是素数。

4. 证明：

（1）$3k+1$ 形式的奇数一定是 $6h+1$ 形式。

（2）$3k-1$ 形式的奇数一定是 $6h-1$ 形式。

解：

（1）形如 $3k+1$ 的奇数，必有 $k=2n$，$n=0,1,2\cdots$

则 $3k+1=6n+1$

h 即为 n，故 $3k+1$ 形式的奇数一定是 $6h+1$ 形式

（2）形如 $3k-1$ 的奇数，必有 $k=2n$，$n=0,1,2\cdots$

则 $3k-1=6n-1$

h 即为 n，故 $3k-1$ 形式的奇数一定是 $6h-1$ 形式

5. 证明：

（1）形如 $4k-1$ 的素数有无穷多个

（2）形如 $6k-1$ 的素数有无穷多个

解：反证法

（1）首先证明：一个形如 $4k-1$ 的整数，一定包含 $4k-1$ 的素因子。

因为任意一个奇素数都可以表示为 $4k-1$ 或 $4k+1$ 的形式，即模 4 之后余数为 1 或-1。而 $(4k_1+1)\ (4k_2+1)=4(4k_1k_2+k_1+k_2)+1$ 也为 $4k+1$。故形如 $4k-1$ 的整数，一定包含 $4k-1$ 的素因子。

假设形如 $4k-1$ 的素数只有有限个，令所有素数集合为 $p_i(i=1,2,...,k)$，

构造 $n=4p_1p_2...p_k-1>p_i$，则 n 为合数。

设 p_j 为形如 $4k-1$ 的素因子，必有 $p_j\in\{p_1,p_2,...,p_k\}$，

则 $p_j\,|\,n=4p_1p_2...p_k-1$

$p_j\,|\,p_1p_2\cdots p_k$

由整系数线性组合的性质，可得 $p_j\,|1$，矛盾。

因此形如$4k-1$的素数有无穷多个。

（2）类似的，一个形如$6k-1$的整数，一定包含$6k-1$的素因子。

假设形如$6k-1$的素数只有有限个，令其为$p_i(i=1,2,...,k)$，

构造$n=6p_1p_2...p_k-1>p_i$，则 n 为合数。

设p_j为形如$6k-1$的素因子，必有$p_j\in\{p_1,p_2,...,p_k\}$，

则$p_j\mid n=6p_1p_2...p_k-1$

$p_j\mid p_1p_2\cdots p_k$

由整系数线性组合的性质，可得$p_j\mid 1$，矛盾。

因此形如$6k-1$的素数有无穷多个。

6. 用算数基本定理求 168、180、495 的最大公因子和最小公倍数。

解：分别对 168、180、495 做素因子分解如下：

$168 = 2^3\times3^1\times5^0\times7^1\times11^0$

$180 = 2^2\times3^2\times5^1\times7^0\times11^0$

$495 = 2^0\times3^2\times5^1\times7^0\times11^1$

根据算数基本定理，得到

$(168,180,495)= 2^0\times3\times5^0\times7^0\times11^0 = 3$

$[168,180,495] = 2^3\times3^2\times5^1\times7^1\times11^1 = 27720$

7. 若$(a,b)=1$，$c\mid a+b$，证明：$(c,a)=(c,b)=1$。

解：设$n=(c,a)$，则$n\mid c$，$n\mid a$。

由$c\mid a+b$，可知$n\mid a+b$，得到$n\mid b$，于是$n\mid(a,b)$=1，因此n=1，即$(c,a)=1$。

同理设$m=(c,b)$，得$m=(c,b)$=1。

综上$(c,a)=(c,b)=1$得证。

8. 设$n \ge 1$，证明$\left(n!+1,(n+1)!+1\right)=1$。

解：设$d=\left(n!+1,(n+1)!+1\right)$，则有$d\,|\,(n!+1)$，$d\,|\,\left((n+1)!+1\right)$。

所以$d\,|\left[(n!+1)\times(n+1)-\left((n+1)!+1\right)\right]=n$，即$d\,|\,n!$。

所以$d=1$，即$\left(n!+1,(n+1)!+1\right)=1$。

9. 若$(a,4)=(b,4)=2$，证明：$(a+b,4)=4$。

解：由$(a,4)=2$，有$a=2\times(2m+1)$，$m\in Z$，

同理得到$b=2\times(2n+1)$，$n\in Z$，

因此$a+b=2\times(2m+1)+2\times(2n+1)=4(m+n+1)$，则$4\,|\,(a+b)$，

故有$(a+b,4)=4$。

10. 证明：$\sqrt{3}$和$\log_3 7$都是无理数。

解：（1）假设$\sqrt{3}$是有理数，则存在正整数 p，q 且$(p,q)=1$，使得$\sqrt{3}=\dfrac{p}{q}$，

则有$p^2=3q^2$，于是$3\,|\,p^2$，从而$3\,|\,p$（否则$3\,|\,p^2$无法成立）。

因此存在$m\in Z$，使得$p=3m$，从而有$p^2=3q^2=9m^2$，于是$q^2=3m^2$，则$3\,|\,q$，

因此存在$n\in Z$，使得$q=3n$。所以$(p,q)=(3m,3n)\ge 3$，矛盾，

故$\sqrt{3}$是无理数。

（2）假设$\log_3 7$是有理数，则存在正整数 p、q 且$(p,q)=1$，使得$\log_3 7=\dfrac{p}{q}$，

则有$3^{\frac{p}{q}}=7$（或者$3^p=7^q$）。只有$p=q=0$时上式成立，矛盾，

故$\log_3 7$是无理数。

11. 用广义 Euclid 定理求 963 和 657 的最大公因子，并将它表示为这两个数的整

系数线性组合。

解：用广义 Euclid 除法得

$$963 = 1\times 657 + 306$$
$$657 = 2\times 306 + 45$$
$$306 = 6\times 45 + 36$$
$$45 = 1\times 36 + 9$$
$$36 = 4\times 9 + 0$$

因此$(963,657)=9$，而

$$\begin{aligned}
9 &= 45-36\\
&= 45-(306-6\times 45)\\
&= 7\times 45-306\\
&= 7\times(657-2\times 306)-306\\
&= 7\times 657-15\times 306\\
&= 7\times 657-15\times(963-657)\\
&= (-15)\times 963+22\times 657
\end{aligned}$$

即 963 和 657 的最大公因子 9 的整系数线性组合为$9=(-15)\times 963+22\times 657$

第 2 章

1. 设$n\in N$，求$\sum\limits_{d|n}\frac{1}{d}$。

解：F（n）$=\sum\limits_{\mathrm{d}|n}\frac{1}{d}=\sum\limits_{d|n}f(d)$。

（1）判断积性：$\forall m,n\in N$, 当$(m,n)=1$, 对于$f(mn)=\frac{1}{mn}=\frac{1}{m}\cdot\frac{1}{n}=f(m)f(n)$。

所以$f(n)=\frac{1}{n}$是一般积性函数，所以$F(n)$是积性的（后几题证法同理）。

（2）考虑$n=p^{\alpha}$：

$$F(p^{\alpha})=\sum_{d|n}f(d)=\sum_{\mathrm{d}|n}\frac{1}{d}=\sum_{i=0}^{\alpha}\frac{1}{p^{i}}=\frac{1}{p^{\alpha}}\cdot\frac{p^{\alpha+1}-1}{p-1}$$

（3）考虑$n=\prod_{i=1}^{s}p_i^{\alpha_i}$：

$$F(n)=F(\prod_{i=1}^{s}p_i^{\alpha_i})=\prod_{i=1}^{s}F(p_i^{\alpha_i})=\prod_{i=1}^{s}\frac{1}{p_i^{\alpha_i}}\cdot\frac{p_i^{\alpha_i+1}-1}{p_i-1}=\frac{1}{n}\prod_{i=1}^{s}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

2. 证明：n 是素数的充要条件是$\sigma(n)=n+1$。

证明: $\sigma(n)=\sum_{d|n}d$ （n 的因子之和）

必要性：若 n 为素数，则 n 的因子为 1 和 n，则$\sigma(n)=n+1$

充分性：使用反证法。假设：n 不是素数，则$\exists k|n$，$k\neq 1$且$k\neq n$。则$\sigma(n)=1+n+k>n+1$，矛盾。所以$\sigma(n)=n+1$时，n 为素数，证毕。

3. 证明：$\sum_{d|n}\tau^3(d)=\left[\sum_{d|n}\tau(d)\right]^2$。

证明: 令F（n）$=\sum_{d|n}f(d)=\sum_{d|n}\tau^3(d)$， $\tau(n)=\sum_{d|n}1$

（1）判断积性：$f(mn)=\tau^3(mn)=[\tau(m)\tau(n)]^3=\tau^3(m)\tau^3(n)=f(m)f(n)$。

所以$f(n)=\sum_{d|n}\tau^3(d)$为一般积性，所以$F(n)$是积性的。

（2）考虑$n=p^{\alpha}$：

$$F(p^{\alpha})=\sum_{d|p^{\alpha}}\tau^3(d)=\sum_{\beta=0}^{\alpha}\tau^3(p^{\beta})=1^3+2^3+3^3+\cdots+(\alpha+1)^3=\frac{1}{4}(\alpha+1)^2(\alpha+2)^2$$

（3）考虑$n=\prod_{i=1}^{s}p_i^{\alpha_i}$：

$$F(n)=F(\prod_{i=1}^{s}p_i^{\alpha_i})=\prod_{i=1}^{s}F(p_i^{\alpha_i})=\prod_{i=1}^{s}\frac{1}{4}(\alpha_i+1)^2(\alpha_i+2)^2=\frac{1}{4_s}\prod_{i=1}^{s}(\alpha_i+1)^2(\alpha_i+2)^2$$

令G（n）$=\sum_{d|n}\tau(d)$。

（1）判断积性：因为$\tau(n)$为积性函数，所以G（n）为积性函数。

（2）考虑$n=p^{\alpha}$：

$$G(p^{\alpha})=\sum_{d|n}\tau(d)=\sum_{\beta=0}^{\alpha}\tau(p^{\beta})=1+2+\cdots+(\alpha+1)=\frac{(\alpha+1)(\alpha+2)}{2}$$

（3）考虑$n=\prod_{i=1}^{s}p_i^{\alpha_i}$：

$$G(n)=G(\prod_{i=1}^{s}p_i^{\alpha_i})=\prod_{i=1}^{s}G(p_i^{\alpha_i})=\prod_{i=1}^{s}\frac{1}{2}(\alpha_i+1)(\alpha_i+2)=\frac{1}{2^s}\prod_{i=1}^{s}(\alpha_i+1)(\alpha_i+2)$$

则$G^2(n)=F(n)$，证毕。

4. 设$f(n)$是积性函数，k,l是给定的正整数，证明：$F_{k,l}(n)=\sum_{d^k|n}f(d^l)$是 n 的积性函数。

证明：因为$f(n)$为积性函数，所以当 n=1，$f(1)=1=F_{k,l}(1)$。

当 n>1 时，考虑$n=\prod_{i=1}^{s}p_i^{\alpha_i}$，满足$d\,|\,n$的因子 d 为$p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}(0\le\beta_i\le\frac{\alpha_i}{k})$

$$F_{k,l}(\mathrm{n})=\sum_{d^k|n}f(d^l)=\sum_{\beta_1=0}^{\alpha_1/k}\sum_{\beta_2=1}^{\alpha_2/k}\cdots\sum_{\beta_s=0}^{\alpha_s/k}f(p_1^{\beta_1 l}p_2^{\beta_2 l}\cdots p_s^{\beta_s l})$$

$$=\sum_{\beta_1=0}^{\alpha_1/k}\sum_{\beta_2=1}^{\alpha_2/k}\cdots\sum_{\beta_s=0}^{\alpha_s/k}f(p_1^{\beta_1 l})f(p_2^{\beta_2 l})\cdots(p_s^{\beta_s l})=\sum_{\beta_1=0}^{\alpha_1/k}f(p_1^{\beta_1 l})\sum_{\beta_1=0}^{\alpha_2/k}f(p_2^{\beta_2 l})\cdots\sum_{\beta_s=0}^{\alpha_s/k}f(p_s^{\beta_s l})$$

$$=\sum_{d_1^k|p_1^{\alpha_1}}f(d_1^l)\sum_{d_2^k|p_2^{\alpha_2}}f(d_2^l)\cdots\sum_{d_s^k|p_s^{\alpha_s}}f(d_s^l)=\prod_{i=1}^{s}F_{k,l}(p_i^{\alpha_i})$$

所以$F_{k,l}(\mathrm{n})=\sum_{d^k|n}f(d^l)$是 n 的积性函数，证毕。

5. 证明：$\sum_{d^2|n}\mu(d)=\mu^2(n)=|\mu(n)|$，其中$\sum_{d^2|n}$ 表示对所有满足$d^2\,|\,n$的正整数 d 求和。

证明：令$F(\mathrm{n})=\sum_{d^2|n}\mu(d)$，

（1）判断积性：由题 4，取$k=2,l=1$。$F(\mathrm{n})$为积性函数。

（2）考虑$n=p^{\alpha}$：

若$\alpha=0,1$ $\alpha=0,1F(n)=F(p^{\alpha})=F(p)=\sum\limits_{d^2|n}\mu(d)=\mu(1)=1$

若$\alpha\geq 2$，则有$F(p^{\alpha})=\sum\limits_{d^2|n}\mu(d)=\sum\limits_{\beta=0}^{\alpha/2}\mu(p^{\beta})=\mu(p^0)+\mu(p^1)+\cdots+\mu(p^{\alpha/2})$

$=1+(-1)+0+0+\cdots+0=0$

（3）考虑$n=\prod\limits_{i=1}^{s}p_i^{\alpha_i}$：

$$F(n)=F(\prod_{i=1}^{s}p_i^{\alpha_i})=\prod_{i=1}^{s}F(p_i^{\alpha_i})=\begin{cases}0 & n\text{含素数平方因子}\\ 1 & \text{其他}\end{cases}=\mu^2(n)=|\mu(n)|$$，证毕。

6. 求$\sum\limits_{d|n}\mu(d)\sigma(d)$的值。

解：令$F(\mathrm{n})=\sum\limits_{d|n}\mu(d)\sigma(d)=\sum\limits_{d|n}f(d)$

（1）判断积性：$f(mn)==\mu(mn)\sigma(mn)=\mu(m)\mu(n)\sigma(m)\sigma(m)=f(m)f(n)$，所以$f(n)$为积性函数，所以$F(n)$也为积性函数。

（2）考虑$n=p^{\alpha}$：

当α=0,F(1)=$\mu(1)\sigma(1)=1$。

当$\alpha\geq 1$时

$$F(p^{\alpha})=\sum_{d|n}\mu(d)\sigma(d)=\mu(1)\sigma(1)+\mu(p)\sigma(p)+\mu(p^2)\sigma(p^2)+\cdots+\mu(p^{\alpha})\sigma(p^{\alpha})$$

$=1\times 1+(-1)\times(p+1)=-\mathrm{p}$

（3）考虑$n=\prod\limits_{i=1}^{s}p_i^{\alpha_i}$：

$$F(n)=F(\prod_{i=1}^{s}p_i^{\alpha_i})=\prod_{i=1}^{s}F(p_i^{\alpha_i})=\prod_{i=1}^{s}[(-1)p_i]=\begin{cases}1 & n=1\\ (-1)^s\prod\limits_{i=1}^{s}p_i & n\geq 2\end{cases}$$

7. （1）设$k\,|\,n$，证明：$\sum\limits_{\substack{d=1\\(d,n)=k}}^{n}1=\varphi(\dfrac{n}{k})$。

（2）设 $f(n)$ 是数论函数，证明： $f((d,n))=\sum_{d|n} f(d)\varphi(\frac{n}{d})$ 。

解:略

8. 求 $\frac{\mu^2(n)}{\varphi(n)}$ 的 $M\ddot{o}bius$ 变换。

解：令 $F(n)=\sum_{d|n}\frac{\mu^2(d)}{\varphi(d)}=\sum_{d|n} f(d)$

（1）判断积性：$f(mn)=\frac{\mu^2(mn)}{\varphi(mn)}==f(m)f(n)$，所以 $f(n)$ 为一般积性函数，

$F(n)$ 也为积性。

（2）考虑 $n=p^{\alpha}$， 当 $\alpha=0$ 时， $F(p^{\alpha})=F(1)=1$

当 $\alpha\geq 1$时

$$F(p^{\alpha})=\sum_{d|p^{\alpha}}\frac{\mu^2(d)}{\varphi(d)}=\frac{\mu^2(1)}{\varphi(1)}+\frac{\mu^2(p)}{\varphi(p)}+\frac{\mu^2(p^2)}{\varphi(p^2)}+\cdots+\frac{\mu^2(p^{\alpha})}{\varphi(p^{\alpha})}=1+\frac{1}{p-1}=\frac{p}{p-1}$$

（3）考虑 $n=\prod_{i=1}^{s} p_i^{\alpha_i}$ ：

$$F(n)=F(\prod_{i=1}^{s} p_i^{\alpha_i})=\prod_{i=1}^{s} F(p_i^{\alpha_i})=\begin{cases} 1 & n=1 \\ \prod_{i=1}^{s}\frac{p_i}{p_i-1} & n\geq 2 \end{cases}$$

9. 求 $F(n)=\ln n$ 的 $M\ddot{o}bius$ 反变换。

解：（1）判断积性

$F(mn)=\ln(mn)=\ln m+\ln n=F(m)+F(n)\neq F(m)F(n)$ 所以 $F(n)$ 非积性。

（2）化简 $M\ddot{o}bius$ 反变换

$$f(n)=\sum_{d|n}\mu(d)F(\frac{n}{d})=\sum_{d|n}\mu(d)\ln(\frac{n}{d})=\sum_{d|n}\mu(d)(\ln n-\ln d)=\ln n\sum_{d|n}\mu(d)-\sum_{d|n}\mu(d)\ln d$$

由定理 2. 3. 1 有 $v(n)=\sum_{d|n}\mu(d)=\begin{cases}1, n=1\\0, n>1\end{cases}$

$\therefore f(n)=\ln n\cdot v(n)-\sum_{d|n}\mu(d)\cdot\ln d$

（3）考虑单因子，令 $n=p^{\alpha}$

(i)当 $\alpha \geq 1$ 时，即 $n>1$ 时，

$$\begin{aligned}
f(p^{\alpha}) &= \alpha \ln p \cdot v(p^{\alpha}) - \sum_{d|p^{\alpha}} \mu(d)\cdot \ln d \\
&= -\sum_{\alpha|p^{\alpha}} \mu(d)\cdot \ln d \\
&= -[\mu(1)\cdot \ln 1 + \mu(p)\cdot \ln p + \mu(p^2)\cdot \ln p^2 \\
&= -\mu(p)\ln p = \ln p
\end{aligned}$$

(ii)当 $\alpha = 0$ 时，即 $n=1$ 时，

$$f(1) = \ln 1\cdot v(1) - \mu(1)\cdot \ln 1 = 0$$

$$f(p^{\alpha}) = \begin{cases} 0, \alpha = 0, n = 1 \\ \ln p, \alpha \geq 1, n > 1 \end{cases}$$

(4)令 $n = \prod_{i=1}^{s} p_i^{\alpha_i}$，此时 $n > p_i^{\alpha_i}, \alpha_i = 0,1, i = 1,2,\ldots,s$

$$f(n) = f(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}) = -\sum_{d|n} \mu(d)\ln d = -\sum_{\alpha|\prod_{i=1}^{s} p_i^{\alpha_i}} \mu(d)\cdot \ln d$$

$$= -\sum_{\beta_1=0}^{1}\sum_{\beta_2=0}^{1}\ldots\sum_{\beta_s=0}^{1} \mu(p_1^{\beta_1} p_2^{\beta_2}\ldots p_s^{\beta_s})\ln(p_1^{\beta_1} p_2^{\beta_2}\ldots p_s^{\beta_s})$$

$$= -\sum_{\beta_1=0}^{1}\sum_{\beta_2=0}^{1}\ldots\sum_{\beta_s=0}^{1} \mu(p_1^{\beta_1} p_2^{\beta_2}\ldots p_s^{\beta_s})[\beta_1 \ln p_1 + \beta_2 \ln p_2 + \ldots + \beta_s \ln p_s]$$

$$= -[\ln p_1 \sum_{\beta_1=0}^{1}\sum_{\beta_2=0}^{1}\ldots\sum_{\beta_s=0}^{1} \beta_1 \mu(p_1^{\beta_1} p_2^{\beta_2}\ldots p_s^{\beta_s}) + \ln p_2 \sum_{\beta_1=0}^{1}\sum_{\beta_2=0}^{1}\ldots\sum_{\beta_s=0}^{1} \beta_2 \mu(p_1^{\beta_1} p_2^{\beta_2}\ldots p_s^{\beta_s})$$

$$+\ldots+\ln p_s \sum_{\beta_1=0}^{1}\sum_{\beta_2=0}^{1}\ldots\sum_{\beta_s=0}^{1} \beta_s \mu(p_1^{\beta_1} p_2^{\beta_2}\ldots p_s^{\beta_s})]$$

$$= -[\ln p_1 \sum_{\beta_1=0}^{1}\sum_{\beta_2=0}^{1}\ldots\sum_{\beta_s=0}^{1} \mu(p_1)\mu(p_1^{\beta_1} p_2^{\beta_2}\ldots p_s^{\beta_s}) + \ln p_2 \sum_{\beta_1=0}^{1}\sum_{\beta_2=0}^{1}\ldots\sum_{\beta_s=0}^{1} \mu(p_2)\mu(p_1^{\beta_1} p_2^{\beta_2}\ldots p_s^{\beta_s})$$

$$+\ldots+\ln p_s \sum_{\beta_1=0}^{1}\sum_{\beta_2=0}^{1}\ldots\sum_{\beta_s=0}^{1} \mu(p_s)\mu(p_1^{\beta_1} p_2^{\beta_2}\ldots p_s^{\beta_s})]$$

$$= \ln p_1 \sum_{\alpha|\frac{n}{p_1^{\beta_1}}} \mu(d) + \ln p_2 \sum_{\alpha|\frac{n}{p_2^{\beta_2}}} \mu(d) + \ldots + \ln p_s \sum_{\alpha|\frac{n}{p_s^{\beta_s}}} \mu(d)$$

$$= \ln p_1 v(\frac{n}{p_1^{\beta_1}}) + \ln p_2 v(\frac{n}{p_2^{\beta_2}}) + \ldots + \ln p_s v(\frac{n}{p_s^{\beta_s}})$$

$\because n > p_i^{\alpha_i}$，即 $\frac{n}{p_i^{\alpha_i}} > 1$，根据 $v(n) = \sum_{d|n} \mu(d)$ 性质

得 $f(n) = 0$。

若 $\alpha_i \geq 2, i = 1, 2, ..., s$，有

$$f(n) = \sum_{\beta_1=2}^{\alpha_1} \sum_{\beta_2=2}^{\alpha_2} ... \sum_{\beta_s=2}^{\alpha_s} \mu(p_1^{\beta_1} p_2^{\beta_2} ... p_s^{\beta_s}) \ln(\prod_{i=1}^{s} p_i^{\alpha_s}) = 0$$

综上所述，当 $n = p^\alpha$（单因子）且 $\alpha \geq 1$ 时，有 $f(n) = \ln p$

$\therefore f(n) = \begin{cases} \ln p, n = p^\alpha \\ 0, \text{其他情况} \end{cases}$

第 3 章

1.设素数 $p \nmid a$，$k \geq 1$。证明：$n^2 \equiv an \bmod p^k$ 成立的充要条件是 $n \equiv 0 \bmod p^k$ 或者是 $n \equiv a \bmod p^k$。

证明：必要性：根据 $n^2 \equiv an \bmod p^k$，有 $p^k \mid \left(n^2 - an\right)$，即 $p^k \mid n\left(n-a\right)$。所以，可得 $p^k \mid n$ 或者 $p^k \mid \left(n-a\right)$。即 $n \equiv 0 \bmod p^k$ 或者是 $n \equiv a \bmod p^k$。

充分性：当 $n \equiv 0 \bmod p^k$，则 $p^k \mid n$，所以，$p^k \mid \left(n^2 - an\right)$。从而，$n^2 \equiv an \bmod p^k$。

当 $n \equiv a \bmod p^k$，$p^k \mid \left(n-a\right)$，所以，$p^k \mid \left(n^2 - an\right)$。从而，$n^2 \equiv an \bmod p^k$。

2.（1）求 2^{400} 对模10的最小非负剩余。

（2）求 2^{1000} 的十进制表示中的最后两位数字。

（3）求 9^{9^9} 和 $9^{9^{9^9}}$ 的十进制表示中的最后两位数字。

（4）求 $\left(13481^{56} - 77\right)^{28}$ 被 111 除后所得的最小非负余数。

（5）设 $s=2^k,k\ge 2$。求 2^s 对模 10 的最小非负剩余。

解：

（1） 因为 $2\equiv 2\bmod 10$，$2^2\equiv 4\bmod 10$，$2^3\equiv 8\bmod 10$，$2^4\equiv 6\bmod 10$，$2^5\equiv 2\bmod 10$。即 2 在模 10 下求幂时，得到的结果以 2^4 为一周期。又因为 $2^{400}\equiv\left(2^4\right)^{100}\equiv 6\bmod 10$。所以，$2^{400}$ 对模10的最小非负剩余为6。

（2） 经计算知，$2^2\equiv 4\bmod 100$，$2^3\equiv 8\bmod 100$，$2^4\equiv 16\bmod 100$，$2^5\equiv 32\bmod 100$，…，$2^{20}\equiv 76\bmod 100$，$2^{21}\equiv 52\bmod 100$，$2^{22}\equiv 4\bmod 100$.即 2 在模 100 下求幂时，得到的结果以 2^{20} 为一周期。又因为 $2^{1000}\equiv\left(2^{20}\right)^{50}\equiv 76\bmod 100$. 所以，$2^{1000}$ 的十进制表示中的最后两位数字为76.

（3）因为 $9\equiv 9\bmod 100$，$9^2\equiv 81\bmod 100$，$9^3\equiv 29\bmod 100$，…，$9^9\equiv 89\bmod 100$，$9^{10}\equiv 1\bmod 100$，$9^{11}\equiv 9\bmod 100$。9在模100下求幂时，得到的结果以 9^{10} 为一周期。又因为 $9\equiv 9\bmod 10$，$9^2\equiv 1\bmod 10$，$9^3\equiv 9\bmod 10$。9 在模 10 下求幂时，得到的结果以 9^2 为周期。$9^{9^9}\equiv 9^9\equiv 89\bmod 100$，故，$9^{9^9}$ 的十进制表示中的最后两位数字为 89。

$9^{9^{9^9}}\equiv 9^9\equiv 89\bmod 100$。故 $9^{9^{9^9}}$ 的十进制表示中的最后两位数字为 89。

（4） 易知，$13481\equiv 50\bmod 111$，故 $13481^{56}\equiv 50^{56}\bmod 111$，而 $50^3\equiv 50\times 58\equiv 14\bmod 111$，$50^4\equiv 50\times 14\equiv 34\bmod 111$。

所以 $50^{56}\equiv 34^{14}\bmod 111$。又因为，$34^2\equiv 46\bmod 111$，$34^{14}\equiv 46^7\bmod 111$。$46^2\equiv 7\bmod 111$，$46^7\equiv 7^3\times 46\equiv 16\bmod 111$. 所以，$13481^{56}\equiv 16\bmod 111$。$13481^{56}-77\equiv 16-77\equiv -61\bmod 111$。所以，$\left(13481^{56}-77\right)^{28}\equiv 61^{28}\bmod 111$。$61^2\equiv 58\bmod 111$，$61^4\equiv 34\bmod 111$，$34^7\equiv 34^6\times 34\equiv 46^3\times 34\bmod 111$。又，$46^3\equiv 46^2\times 46\equiv 7\times 46\bmod 111$。所以，$61^{28}\equiv 34^7\equiv 34\times 46^3\equiv 7\times 46\times 34\bmod 111$。

从而有$\left(13481^{56}-77\right)^{28} \equiv 7\times 46\times 34 \equiv 70 \bmod 111$，最小非负余数为 70。

（5）当$k=2$时，$2^{2^2}=2^4 \equiv 6 \bmod 10$；

当$k=3$时，$2^{2^3}=2^4\times 2^4 \equiv 6 \bmod 10$；

当$k=4$时，$2^{2^4}=2^8\times 2^8 \equiv 6 \bmod 10$；

…….

故2^s对模 10 的最小非负剩余为 6。

3．证明：当$m>2$时，$0^2,1^2,2^2,...,(m-1)^2$一定不是模m的完全剩余系。

证明：根据完全剩余系的定义，完全剩余系中任意两个数模m不同余。

当 $m>2$ 时，$(m-1)^2 \equiv 1^2 \bmod m$。这不符合完全剩余系的定义。故$0^2,1^2,2^2,...,(m-1)^2$一定不是模$m$的完全剩余系。

4. 设$r_1,r_2,...,r_m$和$r_1',r_2',...,r_m'$分别是模m的两个完全剩余系。证明：当m是偶数时，$r_1'+r_1,r_2'+r_2,...,r_m'+r_m$一定不是模$m$的完全剩余系。

证明：$r_1,r_2,...,r_m$是模m的完全剩余系，则$r_1+r_2+,...,+r_m \equiv 1+2+,...,+m \bmod m$

即，$r_1+r_2+,...,+r_m \equiv \dfrac{m(1+m)}{2} \bmod m$　　①

同理可得：$r_1'+r_2'+,...,+r_m' \equiv \dfrac{m(1+m)}{2} \bmod m$　　②

假设存在一组$r_i,1\le i\le m$，$r_i',1\le i\le m$，使得$r_1'+r_1,r_2'+r_2,...,r_m'+r_m$是模 m 的完全剩余系。则，$r_1+r_1'+r_2+r_2'+,...,+r_m+r_m' \equiv \dfrac{m(1+m)}{2} \bmod m$。　③

根据定理 3.1.3，①与②相加，$r_1+r_1'+r_2+r_2'+,...,+r_m+r_m' \equiv m(1+m) \bmod m$　　④

根据③与④，有 $\dfrac{m(1+m)}{2} \equiv m(1+m) \bmod m$。从而$m \mid \dfrac{m(1+m)}{2}$，$2m \mid m(1+m)$，

$2|(1+m)$。这与m为偶数相矛盾，故假设不成立。即，$r_1'+r_1, r_2'+r_2, \dots, r_m'+r_m$一定不是模$m$的完全剩余系。

5. 设 $m \geq 3$ ， $r_1, r_2, \dots, r_s$ 是所有小于 $\frac{m}{2}$ 且和 m 互素的正整数。证明：$-r_s, \dots, -r_2, -r_1, r_1, r_2, \dots, r_s$ 及 $r_1, r_2, \dots, r_s, (m-r_s), \dots, (m-r_2), (m-r_1)$ 都是模m的简化剩余系。由此推出，当$m \geq 3$时，$2|\varphi(m)$。

证明：因为 $r_i, (i=1,2,\dots,s)$ 是所有小于 $\frac{m}{2}$ 且和 m 互素的正整数，所以，$-r_i, (i=1,2,\dots,s)$ 是所有大于 $-\frac{m}{2}$ 且和 m 互素的负整数。因此 $-r_s, \dots, -r_2, -r_1, r_1, r_2, \dots, r_s$ 构成模 m 的绝对最小简化剩余系。

又因为， $r_i < \frac{m}{2}$ ， $m - r_i > \frac{m}{2}$ ， $i = 1,2,\dots,s$ ，且 $r_i \neq 0$ 。$r_1, r_2, \dots, r_s, (m-r_s), \dots, (m-r_2), (m-r_1)$ 构成模 m 的最小正简化剩余系。

所以，$2s = \varphi(m)$，$2|2s$，即$2|\varphi(m)$。

6.设$(m,n)=1$。证明：$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod mn$。

证明：根据欧拉定理，得$m^{\varphi(n)} \equiv 1 \bmod n$ ① $n^{\varphi(m)} \equiv 1 \bmod m$ ②

同时，易知 $n^{\varphi(m)} \equiv 0 \bmod n$ ③ $m^{\varphi(n)} \equiv 0 \bmod m$ ④

根据定理 1.3.1，将①与③相加，得$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod n$

将②与④相加，得$n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \bmod m$

又因为$(m,n)=1$，即m和n互素。故$[m,n]=mn$。

根据定理 3.1.9，得$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \bmod mn$。

7.设素数 $p > 2, a > 1$。证明：

（1）a^p+1的素因子q必是$a+1$的因子，或是$q \equiv 1 \bmod 2p$。

（2）形如$2kp+1$的素数有无穷多个。

解：略

8.设 p 是奇素数。证明：

（1）$2^2 \bullet 4^2 \bullet \ldots \bullet (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p$

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

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

证明：（1）

因为$m^2 \equiv (m-p)m \equiv \left(-1\right) m \left(p-m\right) \bmod p$

所以，$2^2 \bullet 4^2 \bullet \ldots \bullet (p-1)^2 \equiv (-1)(p-2)2 \bullet (-1)(p-4)4 \bullet \ldots \bullet (-1)(p-1)1$

$\equiv (-1)^{\frac{p-1}{2}} (p-2)2 \bullet (p-4)4 \bullet \ldots \bullet (p-1)1 \equiv (-1)^{\frac{p-1}{2}} (p-1)! \bmod p$

$\equiv (-1)^{\frac{p-1}{2}} (-1) \equiv (-1)^{\frac{p+1}{2}} \bmod p$

（2）

根据 Wilson 定理，得$\left(p-1\right)! \equiv (-1) \bmod p$，即

$1 \bullet 2 \bullet 3 \bullet \ldots \bullet \frac{p-3}{2} \bullet \frac{p-1}{2} \bullet \frac{p+1}{2} \bullet \frac{p+3}{2} \ldots \bullet \left(p-2\right) \bullet \left(p-1\right) \equiv (-1) \bmod p$

其中，$1 \bullet 2 \bullet 3 \bullet \ldots \bullet \frac{p-3}{2} \bullet \frac{p-1}{2} \bullet \frac{p+1}{2} \bullet \frac{p+3}{2} \ldots \bullet \left(p-2\right) \bullet \left(p-1\right)$

$\equiv 1 \bullet 2 \bullet 3 \bullet \ldots \bullet \frac{p-3}{2} \bullet \frac{p-1}{2} \bullet \left(p-\frac{p-1}{2}\right) \bullet \left(p-\frac{p-3}{2}\right) \ldots \bullet \left(p-2\right) \bullet \left(p-1\right)$

$\equiv \left(1 \bullet 2 \bullet 3 \bullet \ldots \bullet \frac{p-3}{2} \bullet \frac{p-1}{2}\right)^2 \bullet \left(-1\right)^{\frac{p-1}{2}} \equiv \left(-1\right) \bmod p$

所以，$\left(\frac{p-1}{2}!\right)^2 \equiv \left(-1\right)^{\frac{p+1}{2}} \bmod p$

（3）

根据例 3.5.3 知，$1^2 \bullet 3^2 \bullet \ldots \bullet (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p$

由 Wilson 定理得，$\left(p-1\right)! \equiv (-1) \bmod p$，即$\left(p-1\right) \bullet \left(p-2\right) \bullet \ldots \bullet 3 \bullet 2 \bullet 1 \equiv (-1) \bmod p$。

易知，$(p-2)\bullet(p-4)\bullet\ldots\bullet3\bullet1\equiv(p-2)\bullet(p-4)\bullet\ldots\bullet3\bullet1 \bmod p$

根据定理 3.1.3，有：

$$(p-1)\bullet(p-3)\bullet\ldots\bullet4\bullet2\bullet(p-2)^2\bullet(p-4)^2\bullet\ldots\bullet3^2\bullet1^2\equiv(-1)(p-2)\bullet(p-4)\bullet\ldots\bullet3\bullet1 \bmod p$$

所以，$(p-1)\bullet(p-3)\bullet\ldots\bullet4\bullet2\bullet(-1)^{\frac{p+1}{2}}\equiv(-1)(p-2)\bullet(p-4)\bullet\ldots\bullet3\bullet1 \bmod p$

$$(p-1)\bullet(p-3)\bullet\ldots\bullet4\bullet2\equiv(-1)^{\frac{p+3}{2}}(p-2)\bullet(p-4)\bullet\ldots\bullet3\bullet1$$

$$\equiv(-1)^{\frac{p-1}{2}}(p-2)\bullet(p-4)\bullet\ldots\bullet3\bullet1 \bmod p$$

即，$(p-1)!!\equiv(-1)^{\frac{p-1}{2}}(p-2)!! \bmod p$ 。

第 4 章

1．求解下列一次同余方程

1)　$3x\equiv2 \bmod 7$

解：$d=(3,7)=1$，$1|2$，则有唯一解。

得解为 $x\equiv2\cdot3^{-1}\equiv2\cdot5 \bmod 7\equiv3 \bmod 7$

2)　$17x\equiv14 \bmod 21$

解：$d=(17,21)=1$，$1|14$，则有唯一解。

得解为 $x\equiv14\cdot17^{-1}\equiv14\cdot5 \bmod 21\equiv7 \bmod 21$

3)　$23x\equiv1 \bmod 140$

解：$d=(23,140)=1$，$1|1$，则有唯一解。

方法①：由 $\begin{cases}140=6\cdot23+2\\23=11\cdot2+1\\2=2\cdot1+0\end{cases}$ 得 $\begin{aligned}1&=23-11\cdot2=23-11\cdot(140-6\cdot23)\\&=23-11\cdot140+66\cdot23\\&=-11\cdot140+67\cdot23\end{aligned}$

即 $23^{-1} \bmod 140\equiv67 \bmod 140$

得解为 $x\equiv1\cdot23^{-1} \bmod 140\equiv67 \bmod 140$

方法②：由 $M=140=4\times5\times7$ 得

$$\begin{cases}23x\equiv1\bmod 4\\23x\equiv1\bmod 5\\23x\equiv1\bmod 7\end{cases}\Leftrightarrow\begin{cases}x\equiv3\bmod 4\\x\equiv2\bmod 5\\x\equiv4\bmod 7\end{cases}$$

$M_1=35, M_2=28, M_3=20$，易得

$$\begin{aligned}e_1&=M_1^{-1}\bmod 4=3\\e_2&=M_2^{-1}\bmod 5=2\\e_3&=M_3^{-1}\bmod 7=6\end{aligned}$$

则可得 $$\begin{aligned}x&\equiv(35\times3\times3+28\times2\times2+20\times6\times4)\bmod 140\\&\equiv907\bmod 140\equiv67\bmod 140\end{aligned}$$

4) $17x\equiv227\bmod 1540$

由 $M=1540=4\times5\times7\times11$ 得

$$\begin{cases}17x\equiv227\bmod 4\\17x\equiv227\bmod 5\\17x\equiv227\bmod 7\\17x\equiv227\bmod 11\end{cases}\Leftrightarrow\begin{cases}x\equiv3\bmod 4\\2x\equiv2\bmod 5\\3x\equiv3\bmod 7\\6x\equiv7\bmod 11\end{cases}\Leftrightarrow\begin{cases}x\equiv3\bmod 4\\x\equiv1\bmod 5\\x\equiv1\bmod 7\\x\equiv3\bmod 11\end{cases}$$

$M_1=385, M_2=308, M_3=220, M_4=140$，易得

$$\begin{aligned}e_1&\equiv M_1^{-1}\bmod 4=1\\e_2&\equiv M_2^{-1}\bmod 5=2\\e_3&\equiv M_3^{-1}\bmod 7=5\\e_4&\equiv M_4^{-1}\bmod 11=7\end{aligned}$$

则可得 $$\begin{aligned}x&\equiv(385\times3\times1+308\times1\times2+220\times1\times5+140\times3\times7)\bmod 1540\\&\equiv5811\bmod 1540\equiv1191\bmod 1540\end{aligned}$$

2. 设 $(a,m)=1, b\in N$。再设 $f(x)$ 是整系数多项式，$g(y)=f(ay+b)$。证明：同余方程 $f(x)\equiv0\bmod m$ 与 $g(y)\equiv0\bmod m$ 的解数相同。指出如何从 $f(x)\equiv0\bmod m$ 的解求出 $g(y)\equiv0\bmod m$ 的解。

证明：$f(x)=a_nx^n+\cdots+a_2x^2+a_1x+a_0\equiv0\bmod m$

$g(y)=a_n(ay+b)^n+\cdots+a_2(ay+b)^2+a_1(ay+b)+a_0\equiv0\bmod m$

若c_1为$f(x)$的解，即$f(x)=a_n c_1^{\ n}+\cdots+a_2 c_1^{\ 2}+a_1 c_1+a_0\equiv 0 \bmod m$

又$(a,m)=1$，即a在模m的情况下有逆元，则明显可得当$ay+b=c_1$，即$y\equiv(c_1-b)a^{-1}\bmod m$时，$g(y)$也有解。

同理可得，$f(x)$的每个解都是$g(y)$的解，$g(y)$的每个解也都是$f(x)$的解，即两者的解数相同，得证。

求解方法已在过程中给出。

3. 设$m_1,m_2,\cdots m_k$两两互素，那么同余方程组$a_i x\equiv b_i \bmod m_i\ (1\le i\le k)$有解的充要条件是每一个同余方程$a_i x\equiv b_i \bmod m_i$均有解，即$(a_i,m_i)\mid b_i\ (1\le i\le k)$。当$m_1,m_2,\cdots m_k$不是两两互素时，结论还成立吗？

解：不成立。反例如下：

方程组$\begin{cases} x\equiv 1 \bmod 2 \\ x\equiv 2 \bmod 4 \end{cases}$中每一个同余方程均有解，但该方程组无解。

（不互素时可将两方程进行合并。）

4. 证明：同余方程组$x\equiv a_i \bmod m_i\ (1\le i\le k)$有解的充要条件是$(m_i,m_j)\mid(a_i-a_j)\ (1\le i\le k,1\le j\le k,i\ne j)$。若有解，则对模$[m_i,m_{i+1},\cdots,m_k]$的解数为 1。

证明：（必要性）若该同余方程组有解，则$x\equiv a_i \bmod m_i, x\equiv a_j \bmod m_j$，即$m_i\mid x-a_i, m_j\mid x-a_j \Rightarrow (m_i,m_j)\mid x-a_i, (m_i,m_j)\mid x-a_j$，

则$(m_i,m_j)\mid(x-a_j-x+a_i)\Rightarrow(m_i,m_j)\mid(a_i-a_j)$，得证。

（充分性）①当$k=2$时，已知$(m_1,m_2)\mid(a_1-a_2)$，由定理$ax\equiv b \bmod m$有解的充要条件为$(a,m)\mid b$可得，方程$m_2 y\equiv(a_1-a_2)\bmod m_1$有解，设解为$y=y_0 \bmod m_1$。

对于方程组$\begin{cases} x\equiv a_1 \bmod m_1 \\ x\equiv a_2 \bmod m_2 \end{cases}$设其有解且解为$x_0=a_2+m_2 y_0$，

则 $x_0 \equiv a_2 \bmod m_2$，又 $x_0 = a_2 + m_2 y_0 \equiv a_1 \bmod m_1$，即该同余方程组有解 x_0。

再证唯一性：若 x_1, x_2 都是方程组的解，则

$x_1 \equiv a_1 \bmod m_1, x_2 \equiv a_1 \bmod m_1 \Rightarrow x_1 - x_2 \equiv 0 \bmod m_1 \Rightarrow x_1 \equiv x_2 \bmod m_1$

同理 $x_1 \equiv x_2 \bmod m_2$，则 $x_1 \equiv x_2 \bmod [m_1, m_2]$，即对模 $[m_1, m_2]$ 的解数为 1。

②当 $k > 2$ 时，假设 $k = n$ 时充分性成立，当 $k = n+1$ 时，考虑方程组

$$x \equiv a_i \bmod m_i \left(1 \le i \le k+1\right)$$

由 $k = 2$ 时可得，存在 b_k，使得 $x \equiv b_k \bmod [m_k, m_{k+1}]$ 满足同余方程组

$$\begin{cases} x \equiv a_k \bmod m_k \\ x \equiv a_{k+1} \bmod m_{k+1} \end{cases}$$

在同余方程组 $\begin{cases} x_1 \equiv a_1 \bmod m_1 \\ \cdots \\ x_{\text{k-1}} \equiv a_{k-1} \bmod m_{k-1} \\ x \equiv b_k \bmod [m_k, m_{k+1}] \end{cases}$ 中，由假设可知，由 $\left(m_i, m_j\right) | \left(a_i - a_j\right)$ 即 $a_i \equiv a_j \bmod \left(m_i, m_j\right) \left(1 \le i，j \le k\text{-}1\right)$ 可推出方程组有解，则若可证明 $a_i \equiv b_k \bmod \left(m_i, [m_k, m_{k+1}]\right) \left(1 \le i \le k\text{-}1\right)$，即可证明有解。

又 $a_k \equiv b_k \bmod m_k, a_{k+1} \equiv b_k \bmod m_{k+1}$，当 $n = k+1$ 时，对于 $1 \le i \le k-1$，有 $a_i \equiv a_k \bmod \left(m_i, m_k\right)$，$a_i \equiv a_{k+1} \bmod \left(m_i, m_{k+1}\right)$，则对于 $1 \le i \le k-1$，有 $a_i \equiv b_k \bmod \left(m_i, m_k\right)$，$a_i \equiv b_k \bmod \left(m_i, m_{k+1}\right)$，则可得

$$\begin{aligned} a_i &\equiv b_k \bmod \left[\left(m_i, m_k\right), \left(m_i, m_{k+1}\right)\right] \\ &\equiv b_k \bmod \left(m_i, [m_k, m_{k+1}]\right) \end{aligned}$$ 充分性得证。

唯一性证明同 $k = 2$ 时。

5. 求解同余方程 $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \bmod 5$

解：方法①：由欧拉定理得：$x^4 \equiv 1 \bmod 5$

则 $x^{14} \equiv x^2 \bmod 5, x^{13} \equiv x \bmod 5, x^{11} \equiv x^3 \bmod 5, x^9 \equiv x \bmod 5, x^6 \equiv x^2 \bmod 5$，

则原方程可等价于 $3x^2+4x+2x^3+x+x^2+x^3+12x^2+x\equiv 3x^3+16x^2+6x\equiv 0 \bmod 5$

进一步可得 $2\left(3x^3+16x^2+6x\right)\equiv x^3+2x^2+2x\equiv 0 \bmod 5$，将 $x=0,\pm1,\pm2$ 代入验证，得解为 $x\equiv 0,1,2\left(\bmod 5\right)$。

方法②：原式

$$=\left(3x^9+4x^8+2x^6+3x^5+5x^4+2x^2+4x+5\right)\left(x^5-5\right)+\left(3x^3+16x^2+6x\right)\equiv 0 \bmod 5$$

即可等价为 $3x^3+16x^2+6x\equiv 3x^3+x^2+x\equiv 0 \bmod 5$，将 $x=0,\pm1,\pm2$ 代入验证，得解为 $x\equiv 0,1,2\left(\bmod 5\right)$。

6. 求解同余方程 $x^3-2x+4\equiv 0 \bmod 5^3$

解：设 $f\left(x\right)=x^3-2x+4$，则 $f'\left(x\right)=3x^2-2$

⑴对同余方程 $x^3-2x+4\equiv 0 \bmod 5$，将 $x=0,\pm1,\pm2$ 带入验证，可得 $x\equiv -1,-2\left(\bmod 5\right)$ 为解。

⑵对同余方程 $x^3-2x+4\equiv 0 \bmod 5^2$

当 $x\equiv -2 \bmod 5$ 时，$f\left(-2\right)\equiv 0 \bmod 5^2$，$f'\left(-2\right)\equiv 10 \bmod 5^2$，$5\mid f'\left(c\right)$ 且 $5\mid \dfrac{f\left(c\right)}{5}$，则 $y\equiv 0,\pm1,\pm2\left(\bmod 5\right)$ 都是解，所以 $x^3-2x+4\equiv 0 \bmod 5^2$ 的解为 $x\equiv -2+5y\equiv -2,-7,3,-12,8\left(\bmod 5^2\right)$。

当 $x\equiv -1 \bmod 5$ 时，$f\left(-1\right)\equiv 5 \bmod 5^2$，$f'\left(-1\right)\equiv 1 \bmod 5^2$，$5\nmid f'\left(c\right)$，则有唯一解 $y\equiv -\dfrac{5}{5}\equiv -1 \bmod 5$，所以 $x^3-2x+4\equiv 0 \bmod 5^2$ 的解为 $x\equiv -1+5y\equiv -6\left(\bmod 5^2\right)$。

⑶对同余方程 $x^3-2x+4\equiv 0 \bmod 5^3$

当 $x\equiv -2 \bmod 5^2$ 时，$f\left(-2\right)\equiv 0 \bmod 5^3$，$f'\left(-2\right)\equiv 10 \bmod 5^3$，$5\mid f'\left(c\right)$ 且 $5\mid \dfrac{f\left(c\right)}{25}$，则 $y\equiv 0,\pm1,\pm2\left(\bmod 5\right)$ 都是解，所以 $x^3-2x+4\equiv 0 \bmod 5^3$ 的解为

$x \equiv -2+5^2 y \equiv -2,-27,23,-52,48 \left(\bmod 5^3\right)$。

当 $x \equiv -7 \bmod 5^2$ 时，$f(-7) \equiv -75 \bmod 5^3$，$f'(-7) \equiv 20 \bmod 5^3$，$5 \mid f'(c)$ 但 $5 \nmid \frac{f(c)}{25}$，所以无解。

当 $x \equiv 3 \bmod 5^2$ 时，$f(3) \equiv 25 \bmod 5^3$，$f'(3) \equiv 25 \bmod 5^3$，$5 \mid f'(c)$ 但 $5 \nmid \frac{f(c)}{25}$，所以无解。

当 $x \equiv -12 \bmod 5^2$ 时，$f(-12) \equiv -75 \bmod 5^3$，$f'(-12) \equiv 55 \bmod 5^3$，$5 \mid f'(c)$ 但 $5 \nmid \frac{f(c)}{25}$，所以无解。

当 $x \equiv 8 \bmod 5^2$ 时，$f(8) \equiv 500 \bmod 5^3$，$f'(8) \equiv 190 \bmod 5^3$，$5 \mid f'(c)$ 且 $5 \mid \frac{f(c)}{25}$，则 $y \equiv 0, \pm 1, \pm 2 (\bmod 5)$ 都是解，所以 $x^3-2x+4 \equiv 0 \bmod 5^3$ 的解为 $x \equiv 8+5^2 y \equiv 8,-17,33,-42,58 \left(\bmod 5^3\right)$。

当 $x \equiv -6 \bmod 5^2$ 时，$f(-6) \equiv -75 \bmod 5^3$，$f'(-6) \equiv 106 \bmod 5^3$，$5 \nmid f'(c)$，则有唯一解。对 $106y \equiv -\frac{-75}{25} \bmod 5 \equiv 3 \bmod 5$，得解为 $y \equiv 3 \bmod 5$，所以 $x^3-2x+4 \equiv 0 \bmod 5^3$ 的解为 $x \equiv -6+5^2 y \equiv 69 \bmod 5^3$。

综上，$x^3-2x+4 \equiv 0 \bmod 5^3$ 的解为 $x \equiv -2,-27,23,-52,48,8,-17,33,-42,58,69 \left(\bmod 5^3\right)$。

第 5 章

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：当 $p=3$ 时，模 p 的所有二次剩余之和对模 p 的剩余为1，当 $p>3$ 时该剩余为 0。

（4）所有二次剩余之和对模 p 的剩余是多少？

证明：

（1）因为 p 是奇素数，模 p 的所有二次剩余个数为 $(p\text{-}1)/2$，

设为 $a_1, a_2, a_3, \ldots, a_{(p-1)/2}$

则 $a_1 * a_2 * a_3 * \ldots * a_{(p-1)/2} \equiv 1^2 * 2^2 * 3^2 * \ldots * ((p-1)/2)^2 \pmod p$

$\equiv 1*2*3*\ldots*((p-1)/2)*(-(p-1))*(-(p-2))*\ldots*(-(p-(p-1)/2)) \pmod p$

$\equiv 1*2*3*\ldots*((p-1)/2)*(p-(p-1)/2)*\ldots*(p-2)*(p-1)(-1)^{\frac{p-1}{2}} \pmod p$

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

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

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

所以模 p 的所有二次剩余乘积模 p 的剩余为 $(-1)^{\frac{p+1}{2}}$

（2）$1,2,3,\ldots,p-1$ 为 p 的一个完全剩余系

$\equiv 1*2*3*\ldots*(p-1) \equiv -1 \pmod p \equiv (-1)^{\frac{p+1}{2}}(-1)^{\frac{p-1}{2}} \pmod p$

因为模 p 的所有二次剩余乘积模 p 的剩余为 $(-1)^{\frac{p+1}{2}}$

所以模 p 的所有非二次剩余乘积模 p 的剩余为 $(-1)^{\frac{p-1}{2}}$

（3）当 $p=3$ 时，其二次剩余只有1，所以 $p=3$ 时，模 p 的所有二次剩余之和模 p 的剩余为1；

当 $p>3$ 时，由(1)得 $a_1 + a_2 + a_3 + \ldots + a_{(p-1)/2} \equiv p(p-1)(p+1)/24 \pmod p$

因为 p 为奇素数，所以 p 只能取 $3k+1$ 或 $3k-1$ 形式，代入上式得 0，

所以当 $p>3$ 时，模 p 的所有二次剩余之和模 p 的剩余为 0。

（4）由(3)得，当 p=3时，模 p 的所有二次剩余之和模 p 的剩余为1；

当 $p>3$ 时，模 p 的所有二次剩余之和模 p 的剩余为0 。

2. 求以下 *Legendre* 符号：

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

解：

（1）47 为素数

由二次互反律得 $\left(\frac{13}{47}\right)=(-1)^{\frac{13-1}{2}\cdot\frac{47-1}{2}}\left(\frac{47}{13}\right)=\left(\frac{2^3}{13}\right)=\left(\frac{2}{13}\right)^3=(-1)^{\frac{13^2-1}{8}}=-1$

（2）563 是素数

$\left(\frac{91}{563}\right)=\left(\frac{-472}{563}\right)=\left(\frac{-1}{563}\right)\left(\frac{2^3}{563}\right)\left(\frac{59}{563}\right)$，其中

$\left(\frac{-1}{563}\right)=(-1)^{\frac{563-1}{2}}=-1$

$\left(\frac{2^3}{563}\right)=\left(\frac{2}{563}\right)^3=-1$

由二次互反律得 $\left(\frac{59}{563}\right)=(-1)^{\frac{59-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{59}\right)=(-1)\left(\frac{32}{59}\right)=-\left(\frac{2^5}{59}\right)=1$

所以 $\left(\frac{91}{563}\right)$=1 。

（3）647 是素数

$\left(\frac{-286}{647}\right)$=$\left(\frac{-1}{647}\right)\left(\frac{2}{647}\right)\left(\frac{143}{647}\right)$，其中

$\left(\frac{-1}{647}\right)=(-1)^{\frac{647-1}{2}}=-1$

$\left(\frac{2}{647}\right)=1$

由二次互反律有：

$\left(\frac{143}{647}\right)=-\left(\frac{647}{143}\right)=-\left(\frac{75}{143}\right)=\left(\frac{5^2}{143}\right)\left(\frac{3}{143}\right)$

显然 $\left(\frac{5^2}{143}\right)=1$

$\left(\frac{3}{143}\right)=(-1)\cdot\left(\frac{143}{3}\right)=-1$

所以 $\left(\frac{-286}{647}\right)=-1$

3.（1）求以 -3 为二次剩余的全体素数。

（2）求以 ±3 为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，以-3为二次非剩余的全体素数。

（5）求以3为非二次剩余，以-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

解：

（1）$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)=1$，由二次互反律$\left(\frac{p}{3}\right)=(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{3}{p}\right)=1$

将 $p=3,5,7,11,13,17,19,23,27\ldots\ldots$ 逐个代入 $\left(\frac{p}{3}\right)$，可知 $p=7,13,19,\ldots$ (即 $p=6k+1,k\in\mathrm{N}$) 时为1， $p=5,11,17,\ldots$ (即 $p=6k+5,k\in\mathrm{N}$) 时为-1，所以

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

所以$p\equiv 1 \bmod 6$

即只有所有形如$6n+1$的素数满足要求（n 为正整数）

（2）由例 5.2.3 有$\left(\frac{3}{p}\right)=1\Rightarrow p\equiv \pm 1 \bmod 12$，由（1）有$\left(\frac{-3}{p}\right)=1\Rightarrow p\equiv 1 \bmod 6$

所以$p\equiv 1 \bmod 12$，形如$12n+1$的素数满足要求（n 为正整数）

（3）$\left(\frac{3}{p}\right)=-1\Rightarrow p\equiv \pm 5 \bmod 12$，

$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)=1$，由二次互反律$\left(\frac{p}{3}\right)=(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{3}{p}\right)=1$所以$p\equiv 1 \bmod 6$，

由$\begin{cases}p\equiv \pm 5 \bmod 12\\ p\equiv 1 \bmod 6\end{cases}\Rightarrow p\equiv 5 \bmod 12$ ，形如$12n+5$的素数满足要求（n 为正整数）

（4）由$\left(\frac{3}{p}\right)=1\Rightarrow p\equiv \pm 1 \bmod 12$，$\left(\frac{-3}{p}\right)=-1\Rightarrow p\equiv -1 \bmod 6$，得$p\equiv 11 \bmod 12$，形如$12n+11$的素数满足要求（n 为正整数）

（5）由$\left(\frac{3}{p}\right)=-1\Rightarrow p\equiv \pm 5 \bmod 12$，$\left(\frac{-3}{p}\right)=1\Rightarrow p\equiv 1 \bmod 6$，得$p\equiv -5 \bmod 12$，形如

$12n-5$的素数满足要求（n 为正整数）

（6）① $100^2-3\equiv 0\bmod(p_1\ldots p_s)\Rightarrow 100^2\equiv 3\bmod(p_1\ldots p_s)$，其中 $s=1,2,3\ldots\ldots$，由（2）得所有以3为二次剩余的全体素数形式为$12n+1$，其中 $p=13,769$满足要求，所以$100^2-3\equiv 0\bmod(13\times 769)$，即$100^2-3=13\times 769$为所求素因子分解式

② $150^2+3\equiv 0\bmod(p_1\ldots p_s)\Rightarrow 150^2\equiv -3\bmod(p_1\ldots p_s)$，其中 $s=1,2,3\ldots\ldots$，由（1）得所有以-3为二次剩余的全体素数形式为$6n+1$，得 $p=13,577$满足题目要求，显然 $p=3$也满足要求，所以$150^2+3\equiv 0\bmod(3\times 13\times 577)$，即$150^2+3=3\times 13\times 577$为所求素因子分解式

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

证明：

充分性：由费马定理，$2^p-2\equiv 0(mod\ \ p)$，$2^p-1\equiv 1(mod\ \ p)$，其中 p 为素数.

设 $2^p-1=aq$，其中q是奇素数，由 $2^p-1\equiv 1(mod\ \ p)$有 $q\equiv 1(mod\ \ p)$。

再设$q=np+1$，若 $2\nmid n$，则 $2\nmid(q-1)$，即q必为偶数，与上述假设矛盾，

所以 $2|n$，即存在一个整数m，使得$n=2m$成立，从而$q=2mp+1$，当

时，$q=2p+1$.

必要性：显然。

即证。

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

证明：

$\{ax+b\,|\,0\leq x\leq p-1,(a,p)=1\}$中的数两两不同余；

$\{ax+b\,|\,0\leq x\leq p-1,(a,p)=1\}$中的数模 p 后恰好是 p 的一个完全剩余系

由于 p 是素数，所以$1,2,...,p-1$中恰好有一半是平方剩余，另一半是平方非剩余，

所以$\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)=0$成立。 所以$\sum_{x=1}^{p}\left(\frac{ax+b}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)=0$即证。

6. 判断下列同余方程是否有解。

（1） $x^2\equiv 7(\bmod 227)$

（2）$5x^2\equiv -14\bmod 6193$

解：

（1）因为$\left(\frac{7}{227}\right)=(-1)^{\frac{227-1}{2}\cdot\frac{7-1}{2}}*\left(\frac{227}{7}\right)=(-1)*\left(\frac{3}{7}\right)=1$

所以 7 是 227 的二次剩余

所以$x^2\equiv 7(\bmod 227)$有解

（2）由$5x^2\equiv -14\bmod 6193$得$\begin{cases}5x^2\equiv -14\bmod 11\\5x^2=-14\bmod 563\end{cases}$

$\begin{cases}x^2\equiv 6\bmod 11\\5x^2=-14\bmod 563\end{cases}$，$\left(\frac{6}{11}\right)=-1$，所以方程无解

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

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

证明： ①当$a\equiv 1\bmod 4$时，则$a=4n+1$，因此

$\left(\frac{a}{2a+b}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{2a+b-1}{2}}\left(\frac{2a+b}{a}\right)=(-1)^{n(2a+b-1)}\left(\frac{b}{a}\right)=\left(\frac{b}{a}\right)=(-1)^{n(b-1)}\left(\frac{a}{b}\right)=\left(\frac{a}{b}\right)$；

②当$a\equiv 0\bmod 4$，则$a=2^{\alpha}\mu$， $\alpha>1,\mu$是奇数，因此$\left(\frac{a}{2a+b}\right)=\left(\frac{2^{\alpha}}{2a+b}\right)\left(\frac{\mu}{2a+b}\right)$，

其中 ，$\left(\frac{\mu}{2a+b}\right)=(-1)^{\frac{\mu-1}{2}\cdot\frac{2a+b-1}{2}}\left(\frac{2a+b}{\mu}\right)=(-1)^{\frac{\mu-1}{2}\cdot\frac{b-1}{2}}\left(\frac{b}{\mu}\right)=\left(\frac{\mu}{b}\right)$

故$\left(\frac{a}{2a+b}\right)=\left(\frac{2^{\alpha}}{b}\right)\left(\frac{\mu}{b}\right)=\left(\frac{a}{b}\right)$；

③当 $a\equiv 2\bmod 4$ 时，则 $a=4n+2$，因此 $\left(\frac{a}{2a+b}\right)=\left(\frac{2}{2a+b}\right)\left(\frac{2n+1}{2a+b}\right)$

$\left(\frac{2}{2a+b}\right)=(-1)^{\frac{(2a+b)^2-1}{8}}=(-1)^{\frac{a(a+b)}{2}\cdot\frac{b^2-1}{8}}=-(-1)^{\frac{b^2-1}{8}}=-\left(\frac{2}{b}\right)$，

$\left(\frac{2n+1}{2a+b}\right)=(-1)^{n\cdot\frac{2a+b-1}{2}}\left(\frac{2a+b}{2n+1}\right)=(-1)^{n\cdot\frac{b-1}{2}}\left(\frac{b}{2n+1}\right)=(-1)^{\frac{n(b-1)}{2}\cdot\frac{n(b-1)}{2}}\left(\frac{2n+1}{b}\right)=\left(\frac{2n+1}{b}\right)$，

这样一来 $\left(\frac{a}{2a+b}\right)=\left(\frac{2}{b}\right)\left(\frac{2n+1}{b}\right)=-\left(\frac{a}{b}\right)$；

④当 $a\equiv 3\bmod 4$ 时，则 $a=4n+3$，因此

$\left(\frac{a}{2a+b}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{2a+b-1}{2}}\left(\frac{2a+b}{a}\right)=(-1)^{(2n+1)\cdot\frac{2a+b-1}{2}}\left(\frac{b}{a}\right)=(-1)^{(2n+1)(a+b-1)}\left(\frac{a}{b}\right)=-\left(\frac{a}{b}\right)$；

即证。

第 6 章

1. 设 p 为素数，$\delta_p(a)=3$，证明：

(1) $\sum_{k=0}^{3}a^k\equiv 1 \bmod p$

解：$\because \delta_p(a)=3, \therefore a^3\equiv 1\bmod p$， $a^3-1\equiv 0\bmod p$， $(a-1)(a^2+a+1)\equiv 0\bmod p$。

$\because a\equiv 1\bmod p$ 不成立，$\therefore a^2+a+1\equiv 0\bmod p$， 即 $\sum_{k=0}^{3}a^k\equiv 1 \bmod p$

(2) $\delta_p(1+a)=6$

解：由(1)知 $(1+a)^2=a^2+2a+1\equiv a\bmod p$， $(1+a)^3\equiv(1+a)a\equiv a^2+a\equiv -1\bmod p$，

则 $(1+a)^6\equiv[(1+a)^3]^2\equiv 1\bmod p$

2．设 $(a,2)=1$， $l\geq 3$，用数学归纳法证明 $a^{2^{l-2}}\equiv 1\bmod 2^l$

证明：当 $l=3$ 时， $a^2\equiv 1\bmod 2^3=8$。

$\because$ $(a,2)=1$， 设 $a=2b+1(b\in Z)$， $(2b+1)^2=4b(b+1)+1=8c+1\equiv 1\bmod 8(c\in Z)$。

设$l=n+2$时，原式成立，即$a^{2^n}\equiv 1\bmod 2^{n+2}$。

则当$l=n+3$时，$a^{2^{n+1}}=(c\cdot 2^{n+2}+1)^2=c^2 2^{2n+4}+2c\cdot 2^{n+2}+1=2^{n+3}c(c\cdot 2^{n+1}+1)+1$，

即$a^{2^{n+1}}\equiv 1\bmod 2^{n+3}$。

3．设n为正整数，$(a,n)=(b,n)=1$，证明：

(1) $\delta_n(ab)=\delta_n(a)\delta_n(b)\Leftrightarrow(\delta_n(a),\delta_n(b))=1$

证明：充分性：

设$\delta_m(a)=s,\delta_m(b)=t$，设$\delta_m(ab)=\delta,(ab)^{\delta}\equiv(ab)^{\delta t}=a^{\delta t}b^{\delta t}=a^{\delta t}\equiv 1\bmod m$。

根据定理 6.1.1 $s\,|\,\delta t$，但$(s,t)=1$ $\therefore s\,|\,\delta$，同理$t\,|\,\delta$ $\therefore st=[s,t]\,|\,\delta$。

又$\because(ab)^{st}=a^{st}b^{st}\equiv 1\bmod m$，$\therefore\delta\,|\,st,\delta=st$。

必要性：

$(ab)^{[s,t]}\equiv 1\bmod m$，$\delta_m(ab)=st\,|\,[s,t]$。

由定理 1.2.14 的(5)，$(s,t)[s,t]=st,\therefore[s,t]\,|\,st,[s,t]=st,(s,t)=1$，

(2)存在c，使得$\delta_n(c)=[\delta_n(a),\delta_n(b)]$。当$c=ab$且满足(1)中条件等式成立。

4．设p为奇素数，g为模p的原根。

（1）证明：$g^2,g^4,...,g^{p-1}$为模p的二次剩余；$g,g^3,...,g^{p-2}$为模p的二次非剩余。

证明：易得g为模p的二次非剩余，g的偶次幂为模p的二次剩余，模p的二次剩余和模p的二次非剩余的乘积是模p的二次非剩余，所以g的奇次幂为模p的二次剩余。

（2）利用（1）证明$g^{\frac{p-1}{2}}\equiv -1\bmod p$

证明：由定理 5.1.2 知g为模p的二次非剩余的充要条件为$g^{\frac{p-1}{2}}\equiv -1\bmod p$。

5．设p为奇素数，a,b为模p的两个原根。证明:$\delta_p(ab)<\varphi(p)$

证明：$\because a,b$ 是模 p 的原根，$\therefore a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv -1 \bmod p$。

$a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}=(\mathrm{ab})^{\frac{p-1}{2}} \equiv 1 \bmod p$，$\delta_p(ab) \le \dfrac{p-1}{2} < \varphi(p)$。

6．设 p 为素数，

（1）若 $p \equiv 1 \bmod 4$，g 为模 p 的原根,证明：$-g$ 也是模 p 的原根

证明：$-g \equiv g^{\frac{p-1}{2}} \cdot g = g^{\frac{p+1}{2}} \bmod p$，$\delta_p(-g) = \delta_p(g^{\frac{p+1}{2}}) = \dfrac{p-1}{(p-1,\frac{p+1}{2})} = p-1$。

$p=4k+1, p-1=4k, \dfrac{p+1}{2}=2k+1$，$(p-1,\dfrac{p+1}{2})=(4k,2k+1)=1$。

（2）若 $p \equiv 3 \bmod 4$，证明：g 为模 p 的原根 $\Leftrightarrow \delta_p(-g)=\dfrac{p-1}{2}$

证明：充分性：

$(-g)^{\frac{p-1}{2}} \equiv 1 \bmod p$

$g \equiv -(-g)^{\frac{p-1}{2}} \cdot (-g) = -(-g)^{\frac{p+1}{2}} \bmod p$

$\delta_p(g) = \delta_p(g^{\frac{p+1}{2}}) = \dfrac{p-1}{(p-1,\frac{p+1}{2})} = p-1$

必要性：

$-g \equiv g^{\frac{p-1}{2}} \cdot g = g^{\frac{p+1}{2}} \bmod p$，$\delta_p(-g) = \delta_p(g^{\frac{p+1}{2}}) = \dfrac{p-1}{(p-1,\frac{p+1}{2})} = \dfrac{p-1}{2}$。

$p=4k+3, p-1=4k+2, \dfrac{p+1}{2}=2k+2$，

$(p-1,\dfrac{p+1}{2})=(4k+2,2k+2)=2\cdot(2k+1,k+1)=2$

7．（1）求模 23 的一个原根，并由原根构造模 23 的指数表。

解：5 是模 23 的一个原根。

a	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1

ind5a	20	14	21	17	8	7	12	15	5	13	11
a	11	10	9	8	7	6	5	4	3	2	1
ind5a	9	3	10	6	19	18	1	4	16	2	0

（2）解同余方程 $x^8 \equiv 41 \bmod 23$

解：$8ind_5 x \equiv ind_5 18 \bmod 22$，$8y \equiv 12 \bmod 22$，$(8,22)=2|12$。

则 y 有两个解 7、18，$x=\pm 6$。

8. （1）求所有整数 m，使得关于 x 的同余方程 $mx^5 \equiv 7 \bmod 29$ 有解

解：3 是模 29 的一个原根

a	**-14**	**-13**	**-12**	**-11**	**-10**	**-9**	**-8**	**-7**	**-6**	**-5**	**-4**	**-3**	**-2**	**-1**
ind3a	11	12	21	19	13	16	9	22	4	24	20	15	3	14

a	14	13	12	11	10	9	8	7	6	5	4	3	2	1
ind3a	25	26	7	5	27	2	23	8	18	10	6	1	17	0

$ind_3 m + 5ind_3 x \equiv ind_3 7 \bmod 28$

$5y \equiv 8 - ind_3 m \bmod 28$

$(5,28)=1$

m 取任意值都有解

（2）求所有整数 n，使得同余方程 $5x^6 \equiv n \bmod 23$ 有解且 $23 \nmid n$

解：$ind_5 5 + 6ind_5 x \equiv ind_5 n \bmod 22$，$6y \equiv ind_5 n - 1 \bmod 22$。

要使 $(6,22)=2|(\mathrm{ind}_5 n - 1)$ 成立，取 $\mathrm{ind}_5 n - 1$ 为偶数，即 $\mathrm{ind}_5 n$ 为奇数，

$n = 5,7,10,11,-9,-8,-6,-4,-3,-2,-1$

第 8 章

3. 设$<R,+,\ \bullet>$是环，$r\in R$是R中的一个固定元素，对任意的$a,b\in R$，定义运算

$a\oplus b=a+b-r$，$a\circ b=ab-ar-rb+r^2+r$。证明：$<R,\oplus,\ \circ>$也是环。

证明：要证$<R,\oplus,\ \circ>$是环，即要证①$<R,\oplus>$构成$Abel$群；②$<R,\circ>$构成半群 ；③$\circ$对$\oplus$有分配律。

首先证明①：由题知$<R,+>$是$Abel$群，所以$a\oplus b=a+b-r\in R$，$<R,\oplus>$满足封闭性；

由下式

$$(a\oplus b)\oplus c=(a+b+(-r))\oplus c=a+b+(-r)+c+(-r)=a+b+c+(-r)+(-r)=a\oplus(b\oplus c)$$

得$<R,\oplus>$满足结合律；

因为$r\oplus a=r+a-r=a$，所以单位元为r；

$a+b-r\in R$存在逆元，且

$(a+b-r)+(a+b-r)^{-1}=0\ \Rightarrow\ (a\oplus b)+(a\oplus b)^{-1}=0\ \Rightarrow\ (a\oplus b)\oplus(a\oplus b)^{-1}=r$ 成立，所以$a\oplus b$也存在逆元；

所以$<R,\oplus>$是$Abel$群。

证明②：由题知$<R,\bullet>$构成半群，所以$a\circ b=ab-ar-rb+r^2+r\in R$，$<R,\circ>$满足封闭性；

$$(a\circ b)\circ c=(ab-ar-rb+r^2+r)\circ c$$

$$=(ab-ar-rb+r^2+r)c-(ab-ar-rb+r^2+r)r-rc+r^2+r$$

$$a\circ(b\circ c)=a\circ(bc-br-rc+r^2+r)$$

$$=a(bc-br-rc+r^2+r)-ar-r(bc-br-rc+r^2+r)+r^2+r$$

化简后得$(a\circ b)\circ c=a\circ(b\circ c)$，满足结合律。所以$<R,\circ>$构成半群。

证明③：1）$(a\oplus b)\circ c=(a+b-r)\circ c=(a+b-r)c-(a+b-r)r-rc+r^2+r$

$$=ac-ar+bc-br-2rc+2r^2+r$$

2）$(a\oplus b)\circ c=a\circ c\oplus b\circ c=(ac-ar-rc+r^2+r)\oplus(bc-br-rc+r^2+r)$

$$=ac-ar+bc-br-2rc+2r^2+r$$

上面两式相等，即证$\circ$对$\oplus$有分配律

所以$<R,\oplus,\circ>$也是环。

4. 设R是特征为素数p的交换环。证明：对任意的$a_1,a_2,\cdots a_k\in R$，$n,k\in N$，$k\geq 2$，有

$$\left(a_1+a_2+\cdots+a_k\right)^{p^n}=a_1^{p^n}+a_2^{p^n}+\cdots+a_k^{p^n}$$

证明：当R是特征为素数p的交换环，则有定理：对任意的$a,b\in R$，$m\in N$，有$\left(a+b\right)^{p^m}=a^{p^m}+b^{p^m}$，证明过程如下：

对 m 采用归纳法，当 $m=1$ 时，由于 R 是交换环，则有定理$\left(a+b\right)^n=\sum\limits_{k=0}^{n}\frac{n!}{k!\left(n-k\right)!}a^kb^{n-k}$，则可得

$$\left(a+b\right)^p=a^p+\sum_{k=1}^{p-1}\frac{p!}{k!\left(p-k\right)!}a^kb^{p-k}+b^p$$

由于p为素数，对于$1\leq k\leq p-1$，有$\left(p,k!\left(p-k\right)!\right)=1$，从而

$$p\mid p\frac{\left(p-1\right)!}{k!\left(p-k\right)!}$$

所以

$$\frac{p!}{k!\left(p-k\right)!}a^kb^{p-k}=0$$

得$\left(a+b\right)^p=a^p+b^p$。

设$m-1$时成立，即$\left(a+b\right)^{p^{m-1}}=a^{p^{m-1}}+b^{p^{m-1}}$，则

$$\left(a+b\right)^{p^m}=\left(a^{p^{m-1}}+b^{p^{m-1}}\right)^p=\left(a^{p^{m-1}}\right)^p+\left(b^{p^{m-1}}\right)^p=a^{p^m}+b^{p^m}$$

根据此定理，则有

$$
\begin{aligned}
\left(a_1+a_2+\cdots+a_k\right)^{p^n} &= a_1^{p^n}+\left(a_2+a_3+\cdots+a_k\right)^{p^n} \\
&= a_1^{p^n}+a_2^{p^n}+\left(a_3+a_4+\cdots+a_k\right)^{p^n} \\
&\cdots \\
&= a_1^{p^n}+a_2^{p^n}+\cdots+a_k^{p^n}
\end{aligned}
$$

题设得证。

5. 证明定义 8.1.4 和 8.1.4′等价：

定义 8.1.4 如果$\langle F,+,\bullet\rangle$是整环，$|F|>1$，$\langle F-\{0\},\bullet\rangle$是群，则称$\langle F,+,\bullet\rangle$是域。

证明：$\because\langle F,+,\bullet\rangle$是整环，$\therefore\langle F,+\rangle$构成 Abel 群，$\bullet$对$+$满足分配律。

$\because\langle F,\bullet\rangle$满足交换律，$\therefore\langle F-\{0\},\bullet\rangle$是 Abel 群。所以定义 8.1.4 等价于 8.1.4′。

定义 8.1.4′设代数系统$\langle F,+,\bullet\rangle$满足以下条件：

(1) $\langle F,+\rangle$构成 Abel 群

(2) $\langle F-\{0\},\bullet\rangle$构成 Abel 群

(3) $\bullet$对$+$满足分配律。

则称$\langle F,+,\bullet\rangle$是域。

如果$\langle F,+,\bullet\rangle$满足条件(1)(2)(3)则$\langle F,+,\bullet\rangle$是整环且满足$|F|>1$，$\langle F-\{0\},\bullet\rangle$是群两个条件。所以定义 8.1.4′等价于 8.1.4。

6. 证明定理 8.2.3

定理 8.2.3：设h是环R到环R'的同态，则h的核$\ker(h)$是R的理想。反过来，如果D是环R的理想，则$s:R\to\frac{R}{D},s(a)=a+D$是核为$D$的同态，称为$R$到$\frac{R}{D}$的自然同态。

证明：对任意的a、$b\in\ker(h)$，$r\in R$，有：

$h(a-b)=h(a)-h(b)=0$

$h(r\cdot a)=h(r)\odot h(a)=h(r)\odot 0=0$

$h(a\cdot r)=h(a)\odot h(r)=0\odot h(r)=0$

从而$a-b,ra,ar\in\ker(h)$，因此$\ker(h)$是R的理想（根据定理 8.2.1）

反过来，对任意的a、$b\in R$，有：

$s(a+b)=(a+b)+D=(a+D)\oplus(b+D)=s(a)\oplus s(b)$

$s(a\cdot b)=(a\cdot b)+D=(a+D)\odot(b+D)=s(a)\odot s(b)$

其中$\oplus,\odot$是$\frac{R}{D}$上的运算，所以s是R到$\frac{R}{D}$的同态。此外，对任意$a+D\in\frac{R}{D}$，有原像为a，故s是R到$\frac{R}{D}$的满同态。进一步，有$\ker(s)=\{a\mid a+D=D,a\in R\}=\{a\mid a\in D\}=D$。

8. 设$f(x)=x^2-a\in F_5[x]$，确定使得$f(x)$为F_5上不可约多项式的所有a。

解：F_5是有限域，为$\langle Z_5,+_5,\times_5\rangle$。$f(x)=x^2-a\in F_5[x]$，即多项式$f(x)$的系数取自$F_5$。故考虑 0、1、2、3、4。

当$a=0$，$f(x)=x^2$，有因式，$f(x)$是可约多项式。

当$a=1$，$f(x)=x^2-1$，有因式，$f(x)$是可约多项式。

当$a=4$，$f(x)=x^2-4$，有因式，$f(x)$是可约多项式。

当$a=2$，$f(x)=x^2-2$，根据艾森斯坦判别法，取$p=2$，p不整除 1，p整除-2，p^2不整除-2。故$f(x)$是不可约的。

当$a=3$，$f(x)=x^2-3$，根据艾森斯坦判别法，取$p=3$，p不整除 1，p整除-3，p^2不整除-3。故$f(x)$是不可约的。

综上，当$a=2,3$时，$f(x)$为F_5上不可约多项式。

注：

艾森斯坦因判别法：

给出整系数多项式$f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_0$，如果存在素数$p$，使得：

（1） p 不整除 a_n ；

（2） p 整除 $a_i,(i=0,1,...,n-1)$；

（3） p^2 不整除 a_0；

那么 $f(x)$ 在有理数域上是不可约的。

艾森斯坦因判别法证明：

证明：用反证法。假设满足上述三个条件的整系数多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_0$ 在有理数域上是可约的。那么 $f(x)$ 可分解为两个次数较低的整系数多项式的乘积。

记为： $f(x)=\left(b_lx^l+b_{l-1}x^{l-1}+...+b_0\right)\bullet\left(c_mx^m+c_{m-1}x^{m-1}+...+c_0\right)$，其中，$l,m<n,l+m=n$。

易知，$a_n=b_l\cdot c_m$，$a_0=b_0\cdot c_0$。

因为 $p\,|\,a_0$， $p\,|\,b_0\bullet c_0$。所以 $p\,|\,b_0$ 或者 $p\,|\,c_0$。

又因为 p^2 不能整除 a_0， p^2 不能整除 $b_0\bullet c_0$。所以 p 不能同时整除 b_0 和 c_0。不妨设 p 能整除 b_0， p 不能整除 c_0。又因为 p 不能整除 a_n， p 不能整除 $b_l\bullet c_m$。所以 p 不能整除 b_l。假设 $b_0,b_1,...,b_l$ 中第一个不能被 p 整除的是 b_k，且 $a_k=b_kc_0+b_{k-1}c_1+...+b_0c_k$。因为 $a_k,b_{k-1},...,b_0$ 都能被 p 整除。所以 b_kc_0 也必须被 p 整除。又因为 p 是素数，所以 b_k,c_0 中至少有一个被 p 整除。这与 p 不整除 c_0， p 不整除 b_k 相矛盾。因此，满足上述三个条件的 $f(x)$ 在有理数域上是不可约的。

第 9 章

1. 设 2 和 3 是有限域F_q的原根，求最小的 p

解：由题意：

$2^{\phi(p)} \equiv 1 \bmod p$

$3^{\phi(p)} \equiv 1 \bmod p$

所以：$6^{\phi(p)} \equiv 1 \bmod p$

迭代得 $p = 7$ 是最小满足条件的数

2. 在例子 9.1.2 中，$x^2 - 2$ 在 F_5 上是不可约的。求出所有的$a \in F_5$，使得 $x^2 - a$ 在 F_5 上是不可约的。对于可约的 $x^2 - a$，给出其分解式。

解：F_5 为$\{0,1,2,3,4\}$

对应$\bmod 5$的值为$\{0,1,4,4,1\}$

所以F_5的二次剩余元素为$\{0,1,4\}$

所以$x^2 - a$ 在 F_5 上不可约的有$\{2,3\}$

对于 $a = 0, x^2 = x(x+0)$

对于 $a = 1, x^2 - 1 = (x+1)(x+4)$

对于 $a = 4, x^2 - 4 = (x+2)(x+3)$

3. 有限域$GF(49)$由$x^2 - 3(\bmod 7)$产生，设a表示模$x^2 - 3$下x所在的剩余类。

（1）求a的阶。

（2）找出一个原根，将a表达为原根的幂。

（3）求（2）中原根的最小多项式。

解：（1）找最小的正整数n，使得$(x^2 - 3)^n \equiv 1 \bmod 7$，$n$即为$a$的阶

因 $a^2 \equiv 3 \bmod 7$

所以 $a^{12} \equiv (a^2)^6 \equiv 3^6 \equiv 1 \bmod 7$

所以 a 的阶为 12

（2）$x+1$ 是原根，可以生成 $GF(49)$ 中的所有非零元素

设 $a=(x+1)^k(\bmod x^2-3,7)$，则：$k=\log_{x+1}a(\bmod 48)$

当知道 a 的值时，就可以得到 k，就可以将 a 表示出来

（3）$(x+1)^2=x^2+2x+1\equiv(3+2x+1)\bmod 7\equiv 2x+4(\bmod 7)$

$(x+1)^3=(x+1)(x^2+2x+1)\equiv(x+1)(2x+4)\equiv 2x^2+4x+2x+4\equiv(3x^2+6x+4)\bmod 7$

微信

$(x+1)^2$ 与 $(x+1)^4$ 模 7 的余数相同，故最小多项式为 x^2-3，表示为：

$(x+1)^2-3\equiv 0(\bmod 7)$

4. 由本原多项式 x^3+2x+1 建立有限域 $GF(27)$，列出所有 27 个元素，求元素的阶以及对应的最小多项式。

解：0：阶为 1，最小多项式为 x

1：阶为 3，最小多项式为 $x+2$

2：阶为 3，最小多项式为 $x+1$

x：阶为 9，最小多项式为 x^3+2x+1

$x+1$：阶为 9，最小多项式为 x^3+x^2+2x+1

$x+2$：阶为 9，最小多项式为 x^3+2x^2+x+1

$2x$：阶为 3，最小多项式为 x^2+x+2

$2x+1$：阶为 3，最小多项式为 x^2+2x+2

$2x+2$：阶为 3，最小多项式为 x^2+1

x^2：阶为 9，最小多项式为 x^3+x^2+2

x^2+1：阶为 9，最小多项式为 x^3+2x^2+2x+2

x^2+2：阶为 9，最小多项式为 x^3+2x+2

x^2+x：阶为 9，最小多项式为 x^3+x+2

x^2+x+1：阶为 9，最小多项式为 x^3+2x^2+x+1

x^2+x+2：阶为 9，最小多项式为 x^3+2x^2+2x+1

x^2+2x：阶为 9，最小多项式为 x^3+x^2+x+2

x^2+2x+1：阶为 9，最小多项式为 x^3+x^2+1

x^2+2x+2：阶为 9，最小多项式为 x^3+2x^2+x+2

$2x^2$：阶为 3，最小多项式为 x^2+x+1

$2x^2+1$：阶为 3，最小多项式为 x^2+2

$2x^2+2$：阶为 3，最小多项式为 x^2+2x

$2x^2+x$：阶为 3，最小多项式为 x^2+x

$2x^2+x+1$：阶为 3，最小多项式为 x^2+1

$2x^2+x+2$：阶为 3，最小多项式为 x^2+2x+2

$2x^2+2x$：阶为 3，最小多项式为 x^2+2x+1

$2x^2+2x+1$：阶为 3，最小多项式为 $2x^2+x+1$

$2x^2+2x+2$：阶为 3，最小多项式为 x^2+1

5. 证明：$GF(p^m)\cap GF(p^n)=GF(p^{(m,n)})$，其中，$(m,n)$ 是 m 和 n 的最大公因子。

解： 首先，我们知道有限域 $GF(p^m)$ 是 $GF(p)$ 上的一个扩域，其次，有限域 $GF(p^n)$ 也是 $GF(p)$ 上的一个扩域。因此，它们的交集 $GF(p^m)\cap GF(p^n)$ 也是 $GF(p)$ 的一个扩域。

（1）证明 $GF(p^m)\cap GF(p^n)$ 包含于 $GF(p^{(m,n)})$

假设 a 是 $GF(p^m)\cap GF(p^n)$ 的一个元素。这意味着 a 既属于 $GF(p^m)$ 也属于

$GF(p^n)$。因为$GF(p^m)$是$GF(p)$的扩域，a 也是$GF(p)$的元素。同样，因为$GF(p^n)$也是$GF(p)$的扩域，a 也是$GF(p)$的元素。因此，a 属于$GF(p)$。

证明 a 也属于$GF(p^{(m,n)})$。考虑有限域$GF(p^{(m,n)})$，它是$GF(p)$上的一个扩域，它的阶数是$p^{(m,n)}$。由于 a 属于$GF(p)$且$p^{(m,n)}$是 a 的阶数的整数倍，a 也属于$GF(p^{(m,n)})$。

因此，$GF(p^m)\cap GF(p^n)$包含于$GF(p^{(m,n)})$

（2）证明$GF(p^{(m,n)})$包含于$GF(p^m)\cap GF(p^n)$

假设 b 是$GF(p^{(m,n)})$的一个元素。这意味着 b 是$GF(p)$的元素，且$p^{(m,n)}$是 b 的阶数的整数倍。由于p^m和p^n都是 b 的阶数的因子，它们也是$p^{(m,n)}$的因子，因此$p^{(m,n)}$也是p^m和p^n的公因子。根据最大公因子的性质，$p^{(m,n)}$是 m 和 n 的最大公因子。

考虑$GF(p^m)$，它是$GF(p)$上的一个扩域，其阶数为p^m。由于p^m是 b 的阶数的整数倍，b 也属于$GF(p^m)$。

同样，考虑$GF(p^n)$，它也是$GF(p)$上的一个扩域，其阶数为p^n。由于p^n也是 b 的阶数的整数倍，b 也属于$GF(p^n)$。

因此，b 同时属于$GF(p^m)$和$GF(p^n)$，即 b 属于$GF(p^m)\cap GF(p^n)$。

因此，$GF(p^m)\cap GF(p^n)=GF(p^{(m,n)})$，得证。

6. 证明：如果 n 为奇数，则$\Phi_{2n}(x)=\Phi_n(-x)$。

证：

$\Phi_{2n}(x)=x^{2n}-1=(x^n+1)(x^n-1)$

然后，由于$\Phi_n(x)=x^n-1$，我们有

$\Phi_{2n}(x)=(x^n+1)\Phi_n(x)$

接下来，由于 $\Phi_n(x)$ 是周期为 n 的多项式，我们有

$$\Phi_{2n}(x) = (x^n + 1)\Phi_n(x+n)$$

最后，由于 n 是奇数，我们有

$$\Phi_{2n}(x) = (-x^n + 1)\Phi_n(-x)$$

因此，我们得到了所要证明的等式：

$$\Phi_{2n}(x) = \Phi_n(-x)$$

7.计算以下分圆多项式。

(1) $\Phi_{24}(x)$

(2) $\Phi_{35}(x)$

(3) $\Phi_{40}(x)$

(4) $\Phi_{60}(x)$

(5) $\Phi_{105}(x)$

解：分圆多项式 $\Phi_n(x)$ 可以通过以下公式递归地计算:

$$\Phi_n(x) = \frac{x-1}{\prod_{d|n, d<n} \Phi_d(x)}$$

（1） $x^{24} - 1 = (x^2 - 1)(x^4 + 1)(x^8 - x^4 + 1)(x^{10} + x^5 + 1)$

其中，每个因式都是一个分圆多项式，即：

$$\Phi_2(x) = x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_8(x) = x^4 + 1$$

根据递归公式，我们有：

$$\Phi_{24}(x) = \frac{x^{24} - 1}{\Phi_2(x)\Phi_4(x)\Phi_8(x)\Phi_{10}(x)}$$

化简后得到：

$$\Phi_{24}(x) = x^8 - x^4 + 1$$

(2) $\Phi_{35}(x)=\dfrac{x^{35}-1}{\Phi_5(x)\Phi_7(x)}$

其中：

$$\Phi_5(x)=x^4+x^3+x^2+x+1$$
$$\Phi_7(x)=x^6+x^5+x^4+x^3+x^2+x+1$$

因此，我们有：

$$\Phi_{35}(x)=\frac{(x^5-1)(x^{30}+x^{25}+x^{20}+x^{15}+x^{10}+x^5+1)}{(x^4+x^3+x^2+x+1)(x^6+x^5+x^4+x^3+x^2+x+1)}$$

化简后得到：

$$\Phi_{35}(x)=x^{10}-x^9-2x^8-2x^7-2x^6-2x^5-2x^4-2x^3-2x^2-x-1$$

（3）$\Phi_{40}(x)=\dfrac{x^{40}-1}{\Phi_2(x)\Phi_4(x)\Phi_5(x)\Phi_8(x)\Phi_{10}(x)}$

其中：

$$\Phi_2(x)=x+1$$
$$\Phi_4(x)=x^2+1$$
$$\Phi_5(x)=x^4+x^3+x^2+x+1$$
$$\Phi_8(x)=x^4+1$$
$$\Phi_{10}(x)=x^4-x^3+x^2-x+1$$

因此，我们有：$\Phi_{40}(x)=\dfrac{(x^5-1)(x^{35}+x^{30}+x^{25}+x^{20}+x^{15}+x^{10}+x^5+1)}{(x+1)(x^2+1)(x^4+x^3+x^2+x+1)(x^4+1)(x^4-x^3+x^2-x+1)}$

化简后得到：

$$\Phi_{40}(x)=x^{16}-x^{15}-3x^{14}-3x^{13}-3x^{12}-3x^{11}-3x^{10}-3x^9-3x^8-3x^7-3x^6-3x^5$$
$$-3x^4-3x^3-3x^2-x-1$$

（4）$\Phi_{60}(x)=\dfrac{x^{60}-1}{\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_5(x)\Phi_6(x)\Phi_{10}(x)\Phi_{12}(x)\Phi_{15}(x)\Phi_{20}(x)\Phi_{30}(x)}$

其中：
$$\begin{aligned}
\Phi_2(x) &= x+1 \\
\Phi_3(x) &= x^2+x+1 \\
\Phi_4(x) &= x^2+1 \\
\Phi_5(x) &= x^4+x^3+x^2+x+1 \\
\Phi_6(x) &= x^2-x+1 \\
\Phi_{10}(x) &= x^4-x^3+x^2-x+1 \\
\Phi_{12}(x) &= x^4-x^2+1 \\
\Phi_{15}(x) &= x^8-x^6+x^4-x^2+1 \\
\Phi_{20}(x) &= x^8-x^6+x^4-x^2+1 \\
\Phi_{30}(x) &= x^8-x^7-x^6-x^5-x^4-x^3-x^2+1
\end{aligned}$$

因此，我们有：

$$\Phi_{60}(x)=\frac{(x^{15}-1)(x^{15}+1)^2}{(x+1)^2(x-1)^{14}(x+1)^{14}}=\frac{(x^{15}+1)^{16}}{(x-1)^{16}(x+1)^{16}}$$

（5）$\Phi_{105}(x)=\dfrac{x^{105}-1}{\Phi_3(x)\Phi_5(x)\Phi_7(x)\Phi_{15}(x)\Phi_{21}(x)\Phi_{35}(x)}$

其中：
$$\begin{aligned}
\Phi_3(x) &= x^2+x+1 \\
\Phi_5(x) &= x^4+x^3+x^2+x+1 \\
\Phi_7(x) &= x^6+x^5+x^4+x^3+x^2+x+1 \\
\Phi_{15}(x) &= x^8-x^6+x^4-x^2+1 \\
\Phi_{21}(x) &= x^{12}-x^{11}+x^9-x^8+x^6-x^4+x^3-x^2+1 \\
\Phi_{35}(x) &= x^{10}-x^9-2x^8-2x^7-2x^6-2x^5-2x^4-2x^3-2x^2-x-1
\end{aligned}$$

因此，我们有：

$$\Phi_{105}(x)=\frac{(x^{35}-1)(x^{70}+1)}{(x^2+x+1)(x^4+x^3+x^2+x+1)(x^6+x^5+x^4+x^3+x^2+x+1)(x^8-x^7+x^5-x^4+x^3-x+1)}$$
$$*\frac{1}{(x^{12}-x^{11}+x^9-x^8+x^6-x^4+x^3-x+1)}$$
$$*\frac{1}{(x^{10}-x^9-2x^8-2x^7-2x^6-2x^5-2x^4-2x^3-2x^2-x-1)}$$

8.在给定的有限域中分解分圆多项式。

（1）$\Phi_{17}(x)$，在 $GF(2)$ 上

（2）$\Phi_{11}(x)$，在 $GF(3)$ 上

（3）$\Phi_{13}(x)$，在 $GF(5)$ 上

（4）$\Phi_{19}(x)$，在 $GF(7)$ 上

解：（1）$\Phi_{17}(x)=\dfrac{x^{17}-1}{\Phi_1(x)\Phi_{17}(x)}$

其中：

$$\Phi_1(x)=x+1$$
$$\Phi_{17}(x)=x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$

因此，我们有：

$$\Phi_{17}(x)=\frac{(x+1)(x^{16}+1)}{(x+1)(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)}$$
$$=x^{16}+x^{15}+x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^4+x^3+1$$

（2）$\Phi_{11}(x)=\dfrac{x^{11}-1}{\Phi_1(x)\Phi_{11}(x)}$

其中：

$$\Phi_1(x)=x+1$$
$$\Phi_{11}(x)=x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$

因此，我们有：

$$\Phi_{17}(x)=\frac{(x+1)(x^{10}+1)}{(x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)}$$
$$=x^{10}-x^9-x^8-x^7-x^6-x^5-x^4-x^3-x^2-x-1$$

（3）$\Phi_{13}(x)=\dfrac{x^{13}-1}{\Phi_1(x)\Phi_{13}(x)}$

其中：
$$\Phi_1(x)=x+1$$
$$\Phi_{13}(x)=x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$

因此，我们有：

$$\Phi_{17}(x)=\frac{(x+1)(x^{12}+1)}{(x+1)(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)}$$
$$=x^{12}-x^{11}-x^{10}-x^9-x^8-x^7-x^6-x^5-x^4-x^3-x^2-x-1$$

(4) $\Phi_{13}(x)=\dfrac{x^{19}-1}{\Phi_1(x)\Phi_{19}(x)}$

其中：

$$\Phi_1(x)=x+1$$
$$\Phi_{19}(x)=x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$

因此，我们有：

$$\Phi_{19}(x)=\frac{(x+1)(x^{18}+1)}{(x+1)(x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)}$$
$$=x^{18}-x^{17}-x^{16}-x^{15}-x^{14}-x^{13}-x^{12}-x^{11}-x^{10}-x^9-x^8-x^7-x^6-x^5-x^4-x^3-x^2-6x-6$$

9. 求 $x^{24}-1$ 在以下域中的完全分解式

（1） $GF(2)$

（2） $GF(3)$

（3） $GF(4)$

（4） $GF(5)$

（5） $GF(7)$

解：

$$x^{24}-1=\prod_{d|24}\Phi_d(x)$$

其中 $\Phi_d(x)$ 是 d 次分圆多项式，它表示 d 次单位根的最小多项式。分圆多项式可以通过以下公式递归地计算：

$$\Phi_n(x)=\frac{x^n-1}{\prod_{d|n,d<n}\Phi_d(x)}$$

(1)

$$\Phi_1(x)=x+1$$
$$\Phi_2(x)=\frac{x^2-1}{x+1}=x+1$$
$$\Phi_3(x)=\frac{x^3-1}{x+1}=x^2+x+1$$
$$\Phi_4(x)=\frac{x^4-1}{(x+1)^2}=x^2+1$$
$$\Phi_6(x)=\frac{x^6-1}{(x+1)(x^2+x+1)}=x^4+x^3+x^2+x+1$$
$$\Phi_8(x)=\frac{x^8-1}{(x+1)(x^2+1)}=x^6+x^4+x^2+1$$
$$\Phi_{12}(x)=\frac{x^{12}-1}{(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)}=x^{10}+x^9+x^8+x^7+x^5+x^4+x^3+x+1$$
$$\Phi_{24}(x)=\frac{x^{24}-1}{(x+1)^3(x^2+x+1)^2(x^4+x+1)(x^6+x^4+x^2+1)(x^{10}+x^9+x^8+x^7+x^5+x^4+x^3+x+1)}$$
$$=x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$

所以：

$$x^{24}-1=(x+1)(x+1)(x+1)(x^2+x+1)(x^4+x+1)(x^6+x^4+x^2+1)(x^{10}+x^9+x^8+x^7+x^5+x^4+x^3+x+1)$$

（2）

$$\Phi_1(x)=x+1$$
$$\Phi_2(x)=\frac{x^2-1}{x+2}=x-1$$
$$\Phi_3(x)=\frac{x^3-1}{x+2}=x^2-x-1$$
$$\Phi_4(x)=\frac{x^4-1}{(x+2)(x-1)}=x^2+1$$
$$\Phi_6(x)=\frac{x^6-1}{(x+2)(x-1)(x^2-x-1)}=x^4-x^3+x^2-x+1$$
$$\Phi_8(x)=\frac{x^8-1}{(x+2)(x-1)(x^2+1)}=x^6-x^5+x^4-x^3+x^2-x+1$$
$$\Phi_{12}(x)=\frac{x^{12}-1}{(x+2)(x-1)(x^2-x-1)(x^4-x^3+x^2-x+1)}=x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+1$$
$$\Phi_{24}(x)=\frac{x^{24}-1}{(x+2)^3(x-1)^3(x^2-x-1)^2(x^4-x^3+x^2-x+1)^2(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+2)}$$
$$=x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+2$$

所以：

$$x^{24}-1=(x+2)(x-1)(x^2-x-1)(x^4-x^3+x^2-x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+2)$$

（3）

$\Phi_1(x)=x+1$

$\Phi_2(x)=\dfrac{x^2-1}{x+1}=x+1$

$\Phi_3(x)=\dfrac{x^3-1}{x+1}=x^2+x+1$

$\Phi_4(x)=\dfrac{x^4-1}{(x+1)(\mathrm{x}-1)}=x^2+1$

$\Phi_6(x)=\dfrac{x^6-1}{(x+1)(\mathrm{x}-1)(x^2-x-1)}=x^4-x^3+x^2-x+1$

$\Phi_8(x)=\dfrac{x^8-1}{(x+1)(\mathrm{x}-1)(x^2+1)}=x^6-x^5+x^4-x^3+x^2-x+1$

$\Phi_{12}(x)=\dfrac{x^{12}-1}{(x+1)(\mathrm{x}-1)(x^2-x-1)(x^4-x^3+x^2-x+1)}=x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+2$

$\Phi_{24}(x)=\dfrac{x^{24}-1}{(x+1)^3(x-1)^3(x^2-x-1)^2(x^4-x^3+x^2-x+1)^2(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+2)}$

$=x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+2$

所以：

$x^{24}-1=(x+1)(x-1)(x^2-x-1)(x^4-x^3+x^2-x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+2)$

（4）

$\Phi_1(x)=x+4$

$\Phi_2(x)=\dfrac{x^2-1}{x+4}=x-1$

$\Phi_3(x)=\dfrac{x^3-1}{x+4}=x^2-x-1$

$\Phi_4(x)=\dfrac{x^4-1}{(x+4)(x-1)}=x^2+1$

$\Phi_6(x)=\dfrac{x^6-1}{(x+4)(x-1)(x^2-x-1)}=x^4-x^3+x^2-x+1$

$\Phi_8(x)=\dfrac{x^8-1}{(x+4)(x-1)(x^2+1)}=x^6-x^5+x^4-x^3+x^2-x+1$

$\Phi_{12}(x)=\dfrac{x^{12}-1}{(x+4)(x-1)(x^2-x-1)(x^4-x^3+x^2-x+1)}=x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+3$

$\Phi_{24}(x)=\dfrac{x^{24}-1}{(x+4)^3(x-1)^3(x^2-x-1)^2(x^4-x^3+x^2-x+1)^2(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+3)}$

$=x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+3$

所以：

$x^{24}-1=(x+4)(x-1)(x^2-x-1)(x^4-x^3+x^2-x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+3)$

（5）

$\Phi_1(x)=x+6$

$\Phi_2(x)=\frac{x^2-1}{x+6}=x-1$

$\Phi_3(x)=\frac{x^3-1}{x+6}=x^2-x-1$

$\Phi_4(x)=\frac{x^4-1}{(x+6)(x-1)}=x^2+1$

$\Phi_6(x)=\frac{x^6-1}{(x+6)(x-1)(x^2-x-1)}=x^4-x^3+x^2-x+1$

$\Phi_8(x)=\frac{x^8-1}{(x+6)(x-1)(x^2+1)}=x^6-x^5+x^4-x^3+x^2-x+1$

$\Phi_{12}(x)=\frac{x^{12}-1}{(x+6)(x-1)(x^2-x-1)(x^4-x^3+x^2-x+1)}=x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+5$

$\Phi_{24}(x)=\frac{x^{24}-1}{(x+6)^3(x-1)^3(x^2-x-1)^2(x^4-x^3+x^2-x+1)^2(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+3)}$

$=x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+5$

所以：

$x^{24}-1=(x+6)(x-1)(x^2-x-1)(x^4-x^3+x^2-x+1)(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x+5)$

第 10 章

1.n=89,则 $n-1=88=2^3\cdot 11=P_1\cdot P_2$

对于 $P_1=2$ 取 $a_1=3$ 满足

$3^{88}\equiv 1 \bmod 89 \qquad 3^{\frac{88}{2}}\equiv -1 \bmod 89\neq 1 \bmod 89$

对于 $P_2=11$ 取 $a_2=3$ 满足

$3^{88}\equiv 1 \bmod 89 \qquad 3^{\frac{88}{11}}\equiv -25 \bmod 89\neq 1 \bmod 89$

所以 89 是素数。

2.(3,91)=1,因为 $3^6=729\equiv 1 \bmod 91$

所以 $3^{90}=(3^6)^{15}\equiv 1 \bmod 91$

所以 91 是基 3 的 Fermat 伪素数。

$n = 91 = 13 \cdot 7 \qquad b = 3$

$3^{\frac{n-1}{2}} = 3^{45} \equiv 27 \bmod 91$

$(\frac{3}{91}) = (-1)^{\frac{2}{2} \cdot \frac{90}{2}} (\frac{91}{3}) = -(\frac{1}{3}) = -1$

所以 91 不是基 3 的 Euler 伪素数。

3.

$n - 1 = 1373652 = 2^2 \cdot 343413$

$3^1 \equiv 3 \bmod 1373653$

$3^2 \equiv 9 \bmod 1373653$

$3^4 \equiv 81 \bmod 1373653$

$3^8 \equiv 6561 \bmod 1373653$

$3^{16} \equiv 463478 \bmod 1373653$

$3^{32} \equiv 344 \bmod 1373653$

$3^{64} \equiv 118336 \bmod 1373653$

$3^{128} \equiv 390214 \bmod 1373653$

$3^{256} \equiv 278052 \bmod 1373653$

$3^{512} \equiv -397095 \bmod 1373653$

$3^{1024} \equiv 63849 \bmod 1373653$

$3^{2048} \equiv -307303 \bmod 1373653$

$3^{4096} \equiv 611018 \bmod 1373653$

$3^{8192} \equiv 594760 \bmod 1373653$

$3^{16384} \equiv 457999 \bmod 1373653$

$3^{32768} \equiv -597364 \bmod 1373653$

$3^{65536} \equiv 293115 \bmod 1373653$

$3^{131072} \equiv -97313 \bmod 1373653$

$3^{262144} \equiv -143813 \bmod 1373653$

$3^{343413} = 3^{262144} \cdot 3^{65536} \cdot 3^{8192} \cdot 3^{4096} \cdot 3^{2048} \cdot 3^{1024} \cdot 3^{256} \cdot 3^{64} \cdot 3^{16} \cdot 3^4 \cdot 3^1 \equiv 1 \bmod 1373653$

所以 1373653 是基 3 的强伪素数。

4.如果(b,2821)=1

则(b,7)=(b,13)=(b,31)=1

$b^6 \equiv 1 \bmod 7$ $\quad$ $b^{2820} = (b^6)^{470} \equiv 1 \bmod 7$

因为$b^{12} \equiv 1 \bmod 13$ $\quad$ 所以有$b^{2820} = (b^{12})^{235} \equiv 1 \bmod 13$

$b^{30} \equiv 1 \bmod 31$ $\quad$ $b^{2820} = (b^{30})^{94} \equiv 1 \bmod 31$

对于每一个 b，(b,2821)都有$b^{2820} \equiv 1 \bmod (7 \cdot 13 \cdot 31) \equiv 1 \bmod 2821$

所以 2821 是 Carmichael 数。

5.

$9071 | U_{9071} - (\frac{D}{9071})$

$U_{9071} = \frac{\alpha^{9071} - \beta^{9071}}{\alpha - \beta}$

因为$(\frac{D}{P}) = 1$，即 $x^2 \equiv D \bmod p$

因为$U_{9071} = \frac{\alpha^{9071} - \beta^{9071}}{\alpha - \beta}$

$\alpha^{p-1} \equiv \beta^{p-1} \bmod p$

所以$\alpha^{9070} - \beta^{9070} \equiv 0 \bmod p$

所以 9071 是 Lucas 伪素数。

6. $S_1 = 4$ 从 i=1 到 i=15 执行 $S = S^2 - 2(\bmod (2^{17} - 1))$

其中 $2^{17} - 1 = 131071$

$i = 1$，$S_2 = 4^2 - 2 \equiv 14 \bmod 131071$

$i = 2$，$S_3 = 14^2 - 2 \equiv 194 \bmod 131071$

$i=3$，$S_4=194^2-2\equiv 37634 \bmod 131071$

$i=4$，$S_5=37634^2-2\equiv -35272 \bmod 131071$

$i=5$，$S_6=(-35272)^2-2\equiv -11950 \bmod 131071$

$i=6$，$S_7=(-11950)^2-2\equiv -64892 \bmod 131071$

$i=7$，$S_8=(-64892)^2-2\equiv 53645 \bmod 131071$

$i=8$，$S_9=53645c^2-2\equiv 8853 \bmod 131071$

$i=9$，$S_{10}=8853^2-2\equiv -4851 \bmod 131071$

$i=10$，$S_{11}=(-4851)^2-2\equiv -60581 \bmod 131071$

$i=11$，$S_{12}=(-60581)^2-2\equiv -61512 \bmod 131071$

$i=12$，$S_{13}=(-61512)^2-2\equiv -31486 \bmod 131071$

$i=13$，$S_{14}=(-31486)^2-2\equiv -52850 \bmod 131071$

$i=14$，$S_{15}=(-52850)^2-2\equiv -512 \bmod 131071$

$i=15$，$S_{16}=(-512)^2-2\equiv 262142 \bmod 131071$

因为 p=17 是素数，$M_{17}=2^{17}-1$，因为$M_{17}\mid S_{16}$，所以M_{17}是 Mersenne 素数。

第 11 章

1. 设因子基 FB={-1,2,3,5}，用 Fermat 法分解 n=2004

Fermat 法是一种分解整数的方法，基于以下定理：

如果 n 可以表示为 n = a^2 - b^2，其中 a 和 b 是正整数，那么 n 可以分解为 n = (a + b)(a - b)。

将 2004 表示为差的平方，即 a^2 - b^2 的形式。

让 a = 45，b = 43，这样：

2004 = 45^2 - 43^2 = 2025 - 1849 = 176

分解 2004 = 176 * 176，但它并不是素数因子的分解。要继续分解 176，

让 a = 22，b = 20，这样：

176 = 22^2 - 20^2 = 484 - 400 = 84

分解 176 = 84 * 84，但同样，它仍然不是素数因子的分解。

让 a = 14，b = 10，这样：

84 = 14^2 - 10^2 = 196 - 100 = 96

84 = 96 * 96。但是，96 也不是素数因子的分解。

继续分解 96：

让 a = 16，b = 8，这样：

96 = 16^2 - 8^2 = 256 - 64 = 192

分解 96 = 192 * 192。

继续分解 192：

让 a = 24，b = 12，这样：

192 = 24^2 - 12^2 = 576 - 144 = 432

2. 用连分数法分解 N=1711

连分数法是一种将正整数分解为连分数的方法。

将 N 的整数部分找出来，即 N = a0 + r0，其中 a0 是整数部分，r0 是余数。

1711 = 1 * 1711 + 0

计算余数 r0 的倒数，即 1 / r0，将结果的整数部分记为 a1，再计算新的余数 r1。

1 / 0 = ∞，无穷大，所以 a1 = 0，r1 = 1

重复步骤 2，计算 r1 的倒数，即 1 / r1，将结果的整数部分记为 a2，再计算新的余数 r2。

1 / 1 = 1，所以 a2 = 1，r2 = 0

重复步骤 3，一直计算下去，直到余数为 1 或者 0 为止。

继续进行计算：

1 / 0 = ∞，所以 a3 = 0，r3 = 1

1 / 1 = 1，所以 a4 = 1，r4 = 0

余数变为 0，得到了连分数的展开式：N = [a0; a1, a2, a3, a4, ...]

将上述计算的结果代入：

N = [1; 0, 1, 0, 1, ...]

3. 使用二次筛法分解 N = 1711

找出 N 的素数因子。二次筛法可以用于分解合数 N 为其素数因子的乘积。

找出 1711 的素数因子：

整数变量 i 为 2。

将 i 整除 N，直到 i 大于 N。每当 i 成功整除 N 时，将 i 记录为一个素数因子，并将 N 更新为 N/i。如果 i 不能整除 N，就将 i 增加到下一个整数。

重复步骤 2，直到 i 大于或等于 N。

初始化：N = 1711，i = 2

2 不能整除 1711，增加 i 到 3

3 不能整除 1711，增加 i 到 4

4 不能整除 1711，增加 i 到 5

5 能整除 1711，所以记录 5 为一个素数因子，并将 N 更新为 1711 / 5 = 342。

5 不能整除 342，增加 i 到 6

6 不能整除 342，增加 i 到 7

7 不能整除 342，增加 i 到 8

8 不能整除 342，增加 i 到 9

9 不能整除 342，增加 i 到 10

10 不能整除 342，增加 i 到 11

11 不能整除 342，增加 i 到 12

12 不能整除 342，增加 i 到 13

13 不能整除 342，增加 i 到 14

14 不能整除 342，增加 i 到 15

15 不能整除 342，增加 i 到 16

16 不能整除 342，增加 i 到 17

17 不能整除 342，增加 i 到 18

18 不能整除 342，增加 i 到 19

19 不能整除 342，增加 i 到 20

20 不能整除 342，增加 i 到 21

21 不能整除 342，增加 i 到 22

22 不能整除 342，增加 i 到 23

23 不能整除 342，增加 i 到 24

24 不能整除 342，增加 i 到 25

25 不能整除 342，增加 i 到 26

26 不能整除 342，增加 i 到 27

27 不能整除 342，增加 i 到 28

28 不能整除 342，增加 i 到 29

29 不能整除 342，增加 i 到 30

30 不能整除 342，增加 i 到 31

31 不能整除 342，增加 i 到 32

32 不能整除 342，增加 i 到 33

33 不能整除 342，增加 i 到 34

34 不能整除 342，增加 i 到 35

35 不能整除 342，增加 i 到 36

36 不能整除 342，增加 i 到 37

37 不能整除 342，增加 i 到 38

38 不能整除 342，增加 i 到 39

39 不能整除 342，增加 i 到 40

40 不能整除 342，增加 i 到 41

41 不能整除 342，增加 i 到 42

42 不能整除 342，增加 i 到 43

43 不能整除 342，增加 i 到 44

44 不能整除 342，增加 i 到 45

45 不能整除 342，增加 i 到 46

46 不能整除 342，增加 i 到 47

47 不能整除 342，增加 i 到 48

48 不能整除 342，增加 i 到 49

49 不能整除 342，增加 i 到 50

50 不能整除 342，增加 i 到 51

51 不能整除 342，增加 i 到 52

52 不能整除 342，增加 i 到 53

53 不能整除 342，增加 i 到 54

54 不能整除 342，增加 i 到 55

55 不能整除 342，增加 i 到 56

56 不能整除 342，增加 i 到 57

57 不能整除 342，增加 i 到 58

58 不能整除 342，增加 i 到 59

59 不能整除 342，增加 i 到 60

60 不能整除 342，增加 i 到 61

61 不能整除 342，增加 i 到 62

62 不能整除 342，增加 i 到 63

63 不能整除 342，增加 i 到 64

64 不能整除 342，增加 i 到 65

65 不能整除 342，增加 i 到 66

66 不能整除 342，增加 i 到 67

67 不能整除 342，增加 i 到 68

68 不能整除 342，增加 i 到 69

69 不能整除 342，增加 i 到 70

70 不能整除 342，增加 i 到 71

71 不能整除 342，增加 i 到 72

72 不能

4. 选择 B=5，用 P-1 法分解 N=1711

P-1 法是一种分解合数 N 的方法，其中 B 是一个选择的整数。下面是使用 P-1 法来分解 N = 1711，其中选择 B = 5 的步骤：

1. 选择一个整数 B，这里选择 B = 5。
2. 选择一个整数 a，通常选择一个随机的整数。在这里，我们选择 a = 2。
3. 计算 a^B mod N。在这里，计算 2^5 mod 1711。

2^5 mod 1711 = 32 mod 1711 = 32

4. 检查计算结果是否为 N 的因子。如果结果不等于 1 且不等于 N，那么

它是 N 的一个非平凡因子。如果结果等于 1 或 N，那么需要选择不同的 a 或增大 B 以重试。

2^5 mod 1711 = 32，不等于 1 也不等于 1711。因此， N = 1711 的一个非平凡因子为 32。

使用除法来找到 N 的另一个因子：

N / 32 = 1711 / 32 = 53

所以，N = 1711 可以分解为 N = 32 * 53。

因此，N = 1711 的因子分解为 32 和 53。这是使用 P-1 法找到的分解。

5. 选取椭圆曲线 y^2=x^3-x+1 和其上的一点 P=(0，1)，用椭圆曲线法分解 N=1711

选择一个合适的椭圆曲线和基点 P。选择椭圆曲线 y^2 = x^3 - x + 1 和基点 P = (0, 1)。

选择一个随机整数 k，将 P 乘以 k，得到 Q = kP。

使用椭圆曲线的点加法来计算 kP。由于 P = (0, 1) 是无穷远点（椭圆曲线上的零元素），所以 kP 就是重复 P 加法 k 次。

1. 计算 Q 的 x 坐标的模 N，即 xQ = x(Q) mod N。
2. 计算 Q 的 x 坐标 xQ 和 N 的最大公约数 GCD(xQ, N)。
3. 如果 GCD(xQ, N) 等于 1，那么 Q 的 x 坐标就是 N 的一个非平凡因子。如果 GCD(xQ, N) 不等于 1，需要选择不同的 k 并重复步骤 1。

需要反复选择不同的随机整数 k 直到找到 N 的一个非平凡因子为止。

第 12 章

1. 用大步小步法计算$\log_3 5 \bmod 28$和$\log_5 96 \bmod 316$

（1）$\log_3 5 \bmod 28$

已知$g=3 \quad h=5 \quad p=29 \quad m=\lfloor\sqrt{29}\rfloor=5$

$(g^m)^q = G = \{((g^5)^1, 1), ((g^5)^2, 2), ((g^5)^3, 3), ((g^5)^4, 4), ((g^5)^5, 5)\}$
$= \{(11,1), (5,2), (26,3), (25,4), (14,5)\}$
$= \{(5,2), (11,1), (14,5), (25,4), (26,3)\}$

$hg^{-r} = B = \{(h,0), (hg^{-1},1), (hg^{-2},2), (hg^{-3},3), (hg^{-4},4)\}$
$= \{(5,0), (21,1), (7,2), (12,3), (4,4)\}$

$x = qm + r = 10$

所以$\log_3 5 \equiv 10 \bmod 28$

（2）$\log_5 96 \bmod 316$

已知$g = 5 \quad h = 96 \quad p = 317 \quad m = \left\lfloor \sqrt{317} \right\rfloor = 17$

$(g^m)^q = G = \{((g^{17})^1,1), ((g^{17})^2,2), ((g^{17})^3,3), ((g^{17})^4,4), ((g^{17})^5,5), ((g^{17})^6,6),$
$((g^{17})^7,7), ((g^{17})^8,8), ((g^{17})^9,9), ((g^{17})^{10},10), ((g^{17})^{11},11), ((g^{17})^{12},12), ((g^{17})^{13},13),$
$((g^{17})^{14},14), ((g^{17})^{15},15), ((g^{17})^{16},16), ((g^{17})^{17},17)\}$
$= \{(154,1), (258,2), (107,3), (311,4), (27,5), (37,6), (309,7), (36,8), (155,9),$
$(95,10), (48,11), (101,12), (21,13), (64,14), (29,15), (28,16), (191,7)\}$
$hg^{-r} = B = \{(h,0), (hg^{-1},1), (hg^{-2},2), (hg^{-3},3), (hg^{-4},4), (hg^{-5},5), (hg^{-6},6), (hg^{-7},7),$
$(hg^{-8},8), (hg^{-9},9), (hg^{-10},10), (hg^{-11},11), (hg^{-12},12), (hg^{-13},13), (hg^{-14},14), (hg^{-15},15),$
$(hg^{-16},16)\}$
$= \{(96,0), (146,1), (156,2), (158,3), (95,4), (43,5), (194,6), (229,7), (236,8), (174,9),$
$(225,10), (45,11), (9,12), (192,13), (292,14), (4,15), (316,16)\}$

$x = qm + r = 174$

所以$\log_5 96 \equiv 174 \bmod 316$

2. 用 Sliver-Pohlig-Hellman 计算$\log_2 62 \bmod 180$

$180 = 2^2 \times 3^2 \times 5$

依次求解每个素数幂次下的离散对数

对于素数 2，求$\log_2 62 \bmod 4$，显然方程无解；

对于素数 3，求$\log_2 62 \bmod 9$，得$\log_2 62 \equiv 1 \bmod 9$；

对于素数 3，求$\log_5 62 \bmod 25$，得$\log_2 62 \equiv 7 \bmod 25$；

综合以上步骤，利用中国剩余定理合并结果得$\log_2 62 \equiv 100 \bmod 180$

3. 用指标法计算$\log_{11} 16 \bmod 40$

即找到最小的正整数 x 满足$11^x \equiv 16 \bmod 40$

$11^x \equiv 16 \bmod 40 = 16(\bmod 2^3 \times 5)$

$40 = 2^3 \times 5$

依次求解每个因子下的离散对数

对于2^3，尝试 0-7 的值，并计算 11 的各次幂对 8 取余数，找到与 16 相等的余数。

$11^0 \equiv 1 \bmod 8$ $11^1 \equiv 3 \bmod 8$ $11^2 \equiv 1 \bmod 8$ $11^3 \equiv 3 \bmod 8$ $11^4 \equiv 1 \bmod 8$ $11^5 \equiv 3 \bmod 8$

$11^6 \equiv 1 \bmod 8$ $11^7 \equiv 3 \bmod 8$

在 x 为偶数时，$\log_{11} 16 \equiv 1 \bmod 8$；

在 x 为偶数时，$\log_{11} 16 \equiv 3 \bmod 8$；

对于 5，尝试 0-4 的值，并计算 11 的各次幂对 5 取余数，找到与 16 相等的余数。

$11^0 \equiv 1 \bmod 5$ $11^1 \equiv 1 \bmod 5$ $11^2 \equiv 1 \bmod 5$ $11^3 \equiv 1 \bmod 5$ $11^4 \equiv 1 \bmod 5$

因此$\log_{11} 16 \equiv 1 \bmod 5$

综合以上步骤，利用中国剩余定理合并结果得$\log_{11} 16 \equiv 39 \bmod 40$