《初等数论》习题集

第 1 章

第 1 节

1. 证明定理 1。

2. 证明：若 $m - p \mid mn + pq$，则 $m - p \mid mq + np$。

3. 证明：任意给定的连续 39 个自然数，其中至少存在一个自然数，使得这个自然数的数字和能被 11 整除。

4. 设p是n的最小素约数，$n = pn_1$，$n_1 > 1$，证明：若$p > \sqrt[3]{n}$，则n_1是素数。

5. 证明：存在无穷多个自然数 n，使得 n 不能表示为

$$a^2 + p\text{（}a > 0\text{ 是整数，}p\text{为素数）}$$

的形式。

第 2 节

1. 证明：$12 \mid n^4 + 2n^3 + 11n^2 + 10n$，$n \in \mathbf{Z}$。

2. 设 $3 \mid a^2 + b^2$，证明：$3 \mid a$且 $3 \mid b$。

3. 设n，k是正整数，证明：n^k与n^{k+4}的个位数字相同。

4. 证明：对于任何整数n，m，等式$n^2 + (n + 1)^2 = m^2 + 2$ 不可能成立。

5. 设a是自然数，问$a^4 - 3a^2 + 9$ 是素数还是合数？

6. 证明：对于任意给定的 n 个整数，必可以从中找出若干个作和，使得这个和能被 n 整除。

第 3 节

1. 证明定理 1 中的结论(ⅰ)—(ⅳ)。

2. 证明定理 2 的推论 1，推论 2 和推论 3。

3. 证明定理 4 的推论 1 和推论 3。

4. 设 x，$y \in \mathbf{Z}$，$17 \mid 2x + 3y$，证明：$17 \mid 9x + 5y$。

5. 设a，b，$c \in \mathbf{N}$，c无平方因子，$a^2 \mid b^2c$，证明：$a \mid b$。

6. 设 n 是正整数，求 $\mathrm{C}_{2n}^1, \mathrm{C}_{2n}^3, \cdots, \mathrm{C}_{2n}^{2n-1}$ 的最大公约数。

第 4 节

1. 证明定理 1。

2. 证明定理 3 的推论。

3. 设 a，b 是正整数，证明：$(a + b)[a, b] = a[b, a + b]$。

4. 求正整数 a，b，使得 $a + b = 120$，$(a, b) = 24$，$[a, b] = 144$。

5. 设 a，b，c 是正整数，证明：

$$\frac{[a, b, c]^2}{[a, b][b, c][c, a]} = \frac{(a, b, c)^2}{(a, b)(b, c)(c, a)}。$$

6. 设k是正奇数，证明：$1 + 2 + \cdots + 9 \mid 1^k + 2^k + \cdots + 9^k$。

第 5 节

1. 说明例 1 证明中所用到的四个事实的依据。

2. 用辗转相除法求整数 x，y，使得 $1387x - 162y = (1387, 162)$。

3. 计算：$(27090, 21672, 11352)$。

4. 使用引理 1 中的记号，证明：$(F_{n+1}, F_n) = 1$。

5. 若四个整数 2836，4582，5164，6522 被同一个大于 1 的整数除所得的余数相同，且不等于零，求除数和余数各是多少？

6. 记$M_n = 2^n - 1$，证明：对于正整数a，b，有$(M_a, M_b) = M_{(a, b)}$。

第 6 节

1. 证明定理 1 的推论 1。

2. 证明定理 1 的推论 2。

3. 写出 22345680 的标准分解式。

4. 证明：在 $1, 2, \cdots, 2n$ 中任取 $n + 1$ 数，其中至少有一个能被另一个整除。

5. 证明：$1+\frac{1}{2}+\cdots+\frac{1}{n}$（$n \geq 2$）不是整数。

6. 设a，b是正整数，证明：存在a_1，a_2，b_1，b_2，使得

$$a = a_1a_2，\ b = b_1b_2，\ (a_2, b_2) = 1，$$

并且$[a, b] = a_2b_2$。

第 7 节

1. 证明定理 1。

2. 求使 12347!被 35^k整除的最大的k值。

3. 设 n 是正整数，x 是实数，证明：$\sum_{r=1}^{\infty}[\frac{n+2^{r-1}}{2^r}] = n$。

4. 设 n 是正整数，求方程

$$x^2 - [x^2] = (x - [x])^2$$

在$[1, n]$中的解的个数。

5. 证明：方程

$$f(x) = [x] + [2x] + [2^2x] + [2^3x] + [2^4x] + [2^5x] = 12345$$

没有实数解。

6. 证明：在 $n!$的标准分解式中，2 的指数 $h = n - k$，其中 k 是 n 的二进制表示的位数码之和。

第 8 节

1. 证明：若 $2^n + 1$ 是素数，则n是 2 的乘幂。

2. 证明：若 $2^n - 1$ 是素数，则n是素数。

3. 证明：形如 $6n + 5$ 的素数有无限多个。

4. 设 d 是正整数，$6 \nmid d$，证明：在以 d 为公差的等差数列中，连续三项都是素数的情况最多发生一次。

5. 证明：对于任意给定的正整数 n，必存在连续的 n 个自然数，使得它们都是合数。

6. 证明：级数 $\sum\limits_{n=1}^{\infty} \dfrac{1}{p_n}$ 发散，此处使用了定理 1 注 2 中的记号。

第 2 章

第 1 节

1. 证明定理 1 和定理 2。

2. 证明定理 4。

3. 证明定理 5 中的结论(ⅰ)—(ⅳ)。

4. 求 8^{1234}被 13 除的余数。

5. 设 $f(x)$是整系数多项式，并且 $f(1), f(2), \cdots, f(m)$都不能被 m 整除，则 $f(x) = 0$ 没有整数解。

6. 已知 $99 \mid \overline{62\alpha\beta427}$，求$\alpha$与$\beta$。

第 2 节

1. 证明定理 1。

2. 证明：若 $2p + 1$ 是奇素数，则

$$(p!)^2 + (-1)^p \equiv 0 \pmod{2p + 1}。$$

3. 证明：若 p 是奇素数，$N = 1 + 2 + \cdots + (p - 1)$，则

$$(p - 1)! \equiv p - 1 \pmod{N}。$$

4. 证明 Wilson 定理的逆定理：若 $n > 1$，并且

$$(n - 1)! \equiv -1 \pmod{n},$$

则 n 是素数。

5. 设m是整数，$4 \mid m$，$\{a_1, a_2, \cdots, a_m\}$与$\{b_1, b_2, \cdots, b_m\}$是模$m$的两个完

全剩余系，证明：$\{a_1b_1, a_2b_2, \cdots, a_mb_m\}$不是模$m$的完全剩余系。

6. 设$m_1, m_2, \cdots, m_n$是两两互素的正整数，δ_i（$1 \le i \le n$）是整数，并且

$$\delta_i \equiv 1 \pmod{m_i}, \qquad 1 \le i \le n,$$

$$\delta_i \equiv 0 \pmod{m_j}, \quad i \ne j, \quad 1 \le i, j \le n。$$

证明：当b_i通过模m_i（$1 \le i \le n$）的完全剩余系时，

$$b_1\delta_1 + b_2\delta_2 + \cdots + b_n\delta_n$$

通过模$m = m_1m_2\cdots m_n$的完全剩余系。

第 3 节

1. 证明定理 1。

2. 设$m_1, m_2, \cdots, m_n$是两两互素的正整数，x_i分别通过模m_i的简化剩余系（$1 \le i \le n$），$m = m_1m_2\cdots m_n$，$M_i = \dfrac{m}{m_i}$，则

$$M_1x_1 + M_2x_2 + \cdots + M_nx_n$$

通过模 m 的简化剩余系。

3. 设$m > 1$，$(a, m) = 1$，$x_1, x_2, \ldots, x_{\varphi(m)}$是模$m$的简化剩余系，证明：

$$\sum_{i=1}^{\varphi(m)} \left\{\frac{ax_i}{m}\right\} = \frac{1}{2}\varphi(m)。$$

其中$\{x\}$表示 x 的小数部分。

4. 设 m 与 n 是正整数，证明：

$$\varphi(mn)\varphi((m, n)) = (m, n)\varphi(m)\varphi(n)。$$

5. 设 a，b 是任意给定的正整数，证明：存在无穷多对正整数 m 与 n，使得

$$a\varphi(m) = b\varphi(n)。$$

6. 设 n 是正整数，证明：

(i) $\varphi(n) > \dfrac{1}{2}\sqrt{n}$；

(ii) 若 n 是合数，则$\varphi(n) \le n - \sqrt{n}$。

第 4 节

1. 证明：$1978^{103} - 1978^3$能被 10^3整除。

2. 求 313^{159}被 7 除的余数。

3. 证明：对于任意的整数a，$(a, 561) = 1$，都有$a^{560} \equiv 1 \pmod{561}$，但 561 是合数。

4. 设 p，q 是两个不同的素数，证明：

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}。$$

5. 将 $6^{12} - 1$ 分解成素因数之积。

6. 设$n\in\mathbf{N}$，$b\in\mathbf{N}$，对于$b^n + 1$的素因数，你有甚麽与例 6 相似的结论？

第 5 节

1. 证明例 2 中的结论。

2. 证明定理 2。

3. 求 $\sum\limits_{d|n}\dfrac{1}{d}$。

4. 设 $f(n)$是积性函数，证明：

(i) $\sum\limits_{d|n}\mu(d)f(d) = \prod\limits_{p|n}(1 - f(p))$

(ii) $\sum\limits_{d|n}\mu^2(d)f(d) = \prod\limits_{p|n}(1 + f(p))$。

5. 求$\varphi(n)$的 Mobius 变换。

第 3 章

第 1 节

1. 证明定理 3。

2. 写出 789 的二进制表示和五进制表示。

3. 求 $\dfrac{8}{21}$ 的小数的循环节。

4. 证明：七进制表示的整数是偶数的充要条件是它的各位数字之和为偶数。

5. 证明：既约正分数 $\dfrac{m}{n}$ 的b进制小数$(0.a_{-1}a_{-2}a_{-3}\cdots)_b$为有限小数的充要条件是$n$的每个素因数都是$b$的素因数。

第 2 节

1. 设连分数$\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \rangle$的第$k$个渐近分数为 $\dfrac{p_k}{q_k}$，证明：

$$p_k = \begin{vmatrix} a_1 & -1 & 0 & \cdots & \cdots & 0 & 0 \\ 1 & a_2 & -1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & a_3 & -1 & 0 & \cdots & 0 \\ & \cdots & & & & \cdots & \\ & \cdots & & & & \cdots & \\ 0 & \cdots & \cdots & 0 & 1 & a_{k-1} & -1 \\ 0 & 0 & \cdots & \cdots & 0 & 1 & a_k \end{vmatrix}, \quad q_k = \begin{vmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & a_2 & -1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & a_3 & -1 & 0 & \cdots & 0 \\ & \cdots & & & & \cdots & \\ & \cdots & & & & \cdots & \\ 0 & \cdots & \cdots & 0 & 1 & a_{k-1} & -1 \\ 0 & 0 & \cdots & \cdots & 0 & 1 & a_k \end{vmatrix},$$

2. 设连分数$\langle \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \rangle$的第$k$个渐近分数为 $\dfrac{p_k}{q_k}$，证明：

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}，\ k\ge 2。$$

3. 求连分数$\langle 1, 2, 3, 4, 5, \cdots \rangle$的前三个渐近分数。

4. 求连分数$\langle 2, 3, 2, 3, \cdots \rangle$的值。

5. 解不定方程：$7x - 9y = 4$。

第 3 节

1. 证明定理 4。

2. 求 $\sqrt{13}$ 的连分数。

3. 求 $2+\sqrt{3}$ 的误差$\le 10^{-5}$的有理逼近。

4. 求$\sin 18°$的误差$\le 10^{-5}$的有理逼近。

5. 已知圆周率$\pi = \langle 3, 7, 15, 1, 292, 1, 1, 1, 21, \cdots \rangle$，求$\pi$的误差$\le 10^{-6}$的有理逼近。

6. 证明：$\dfrac{1+\sqrt{5}}{2}$连分数展开的第k个渐近分数为$\dfrac{F_{k+1}}{F_k}$。此处$\{F_n\}$是Fibonacci数列。

第 4 节

1. 将方程 $3x^2 + 2x - 2 = 0$ 的正根写成连分数。

2. 求$\alpha = \langle 1, \dot{2}, \dot{3} \rangle$之值。

3. 设 a 是正整数，求 $\sqrt{a^2+1}$ 的连分数。

4. 设无理数 $\sqrt{d} = \langle a_1, a_2, \cdots, a_n, \cdots \rangle$的第$k$个渐近分数为$\dfrac{p_k}{q_k}$，证明：$\sqrt{d} = \langle a_1, \dot{a}_2, \cdots, a_n, 2\dot{a}_1 \rangle$的充要条件是

$$p_n = a_1q_n + q_{n-1}，\ dq_n = a_1p_n + p_{n-1}。$$

5. 设无理数 $\sqrt{d} = \langle a_1, a_2, \cdots, a_n, \cdots \rangle$的第$k$个渐近分数为$\dfrac{p_k}{q_k}$，且正整数$n$使得

$$p_n = a_1q_n + q_{n-1}，\ dq_n = a_1p_n + p_{n-1}，$$

证明：

(ⅰ) 当n为偶数时，p_n，q_n是不定方程$x^2 - dy^2 = 1$ 的解；

（ii） 当n为奇数时，p_{2n}，q_{2n}是不定方程$x^2 - dy^2 = 1$的解。

第 4 章

第 1 节

1. 将$\frac{17}{105}$写成三个既约分数之和，它们的分母分别是 3，5 和 7。

2. 求方程$x_1 + 2x_2 + 3x_3 = 41$的所有正整数解。

3. 求解不定方程组：

$$\begin{cases} x_1 + 2x_2 + 3x_3 = 7 \\ 2x_1 - 5x_2 + 20x_3 = 11 \end{cases}。$$

4. 甲班有学生 7 人，乙班有学生 11 人，现有 100 支铅笔分给这两个班，要使甲班的学生分到相同数量的铅笔，乙班学生也分到相同数量的铅笔，问应怎样分法？

5. 证明：二元一次不定方程 $ax + by = n$，$a > 0$，$b > 0$，$(a, b) = 1$ 的非负整数解的个数为$[\frac{n}{ab}]$或$[\frac{n}{ab}]+1$。

6. 设 a 与 b 是正整数，$(a, b) = 1$，证明：$1, 2, \cdots, ab - a - b$ 中恰有$\frac{(a-1)(b-1)}{2}$个整数可以表示成 $ax + by$（$x \ge 0$，$y \ge 0$）的形式。

第 2 节

1. 证明定理 2 推论。

2. 设 x，y，z 是勾股数，x 是素数，证明：$2z - 1$，$2(x + y + 1)$都是平方数。

3. 求整数 x，y，z，$x > y > z$，使 $x - y$，$x - z$，$y - z$ 都是平方数。

4. 解不定方程：$x^2 + 3y^2 = z^2$，$x > 0$，$y > 0$，$z > 0$，$(x, y) = 1$。

5. 证明下面的不定方程没有满足 $xyz \neq 0$ 的整数解。

（i） $x^2 + y^2 + z^2 = x^2y^2$；

（ii） $x^2 + y^2 + z^2 = 2xyz$。

6. 求方程$x^2 + y^2 = z^4$的满足$(x, y) = 1$，$2 \mid x$的正整数解。

第 3 节

1. 求方程$x^2 + xy - 6 = 0$的整数解。

2. 求方程组 $\begin{cases} x+y+z=0 \\ x^3+y^3+z^3=-18 \end{cases}$ 的整数解。

3. 求方程 $2^x - 3^y = 1$ 的正整数解。

4. 求方程 $\frac{1}{x}+\frac{1}{y}=\frac{1}{z}$ 的正整数解。

5. 设 p 是素数，求方程 $\frac{2}{p}=\frac{1}{x}+\frac{1}{y}$ 的整数解。

6. 设 $2n+1$ 个有理数 $a_1, a_2, \cdots, a_{2n+1}$ 满足条件 P：其中任意 $2n$ 个数可以分成两组，每组 n 个数，两组数的和相等，证明：

$$a_1 = a_1 = \cdots = a_{2n+1}。$$

第 5 章

第 1 节

1. 证明定理 1。

2. 解同余方程：

(i) $31x \equiv 5 \pmod{17}$；

(ii) $3215x \equiv 160 \pmod{235}$。

3. 解同余方程组：

$$\begin{cases} 3x+5y \equiv 38 \pmod{47} \\ x-\ \ y \equiv 10 \pmod{47} \end{cases}。$$

4. 设 p 是素数，$0 < a < p$，证明：

$$x \equiv b(-1)^{a-1}\frac{(p-1)(p-2)\cdots(p-a+1)}{a!} \pmod{p}。$$

是同余方程 $ax \equiv b \pmod{p}$ 的解。

5. 证明：同余方程 $a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b \pmod{m}$ 有解的充要条件是

$$(a_1, a_2, \cdots, a_n, m) = d \mid b。$$

若有解，则恰有 $d \cdot m^{n-1}$ 个解，mod m。

6. 解同余方程：$2x + 7y \equiv 5 \pmod{12}$。

第 2 节

1. 解同余方程组：$\begin{cases} x \equiv b_1 \pmod 5 \\ x \equiv b_2 \pmod 6 \\ x \equiv b_3 \pmod 7 \\ x \equiv b_4 \pmod{11} \end{cases}$。

2. 解同余方程组：$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 5 \pmod 8 \\ x \equiv 13 \pmod{25} \end{cases}$。

3. 有一队士兵，若三人一组，则余 1 人；若五人一组，则缺 2 人；若十一人一组，则余 3 人。已知这队士兵不超过 170 人，问这队士兵有几人？

4. 求一个最小的自然数 n，使得它的 $\frac{1}{2}$ 是一个平方数，它的 $\frac{1}{3}$ 是一个立方数，它的 $\frac{1}{5}$ 是一个 5 次方数。

5. 证明：对于任意给定的n个不同的素数$p_1, p_2, \cdots, p_n$，必存在连续n个整数，使得它们中的第k个数能被p_k整除。

6. 解同余方程：$3x^2 + 11x - 20 \equiv 0 \pmod{105}$。

第 3 节

1. 证明定理的推论。

2. 将例 2 中略去的部分补足。

3. 将例 4 中略去的部分补足。

4. 解同余方程$x^2 \equiv -1 \pmod{54}$。

5. 解同余方程$f(x) = 3x^2 + 4x - 15 \equiv 0 \pmod{75}$。

6. 证明：对于任意给定的正整数n，必存在m，使得同余方程$x^2 \equiv 1 \pmod m$的解数$T > n$。

第 4 节

1. 解同余方程：

(ⅰ) $3x^{11} + 2x^8 + 5x^4 - 1 \equiv 0 \pmod 7$；

(ⅱ) $4x^{20} + 3x^{12} + 2x^7 + 3x - 2 \equiv 0 \pmod 5$。

2. 判定

(ⅰ) $2x^3 - x^2 + 3x - 1 \equiv 0 \pmod 5$是否有三个解；

(ⅱ) $x^6 + 2x^5 - 4x^2 + 3 \equiv 0 \pmod 5$是否有六个解？

3. 设$(a, m) = 1$，k与m是正整数，又设$x_0^k \equiv a \pmod m$，证明同余方程

$$x^k \equiv a(\mathrm{mod}\ m)$$

的一切解x都可以表示成$x \equiv yx_0\ (\mathrm{mod}\ m)$，其中$y$满足同余方程$y^k \equiv 1\ (\mathrm{mod}\ m)$。

4. 设n是正整数，p是素数，$(n, p-1) = k$，证明同余方程$x^n \equiv 1\ (\mathrm{mod}\ p)$有$k$个解。

5. 设 p 是素数，证明：

(ⅰ) 对于一切整数x，$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1)\ (\mathrm{mod}\ p)$；

(ⅱ) $(p-1)! \equiv -1\ (\mathrm{mod}\ p)$。

6. 设 $p \geq 3$ 是素数，证明：$(x-1)(x-2)\cdots(x-p+1)$的展开式中除首项及常数项外，所有的系数都是 p 的倍数。

第 5 节

1. 同余方程$x^2 \equiv 3\ (\mathrm{mod}\ 13)$有多少个解？

2. 求出模 23 的所有的二次剩余和二次非剩余。

3. 设 p 是奇素数，证明：模 p 的两个二次剩余的乘积是二次剩余；两个二次非剩余的乘积是二次剩余；一个二次剩余和一个二次非剩余的乘积是二次非剩余。

4. 设素数 $p \equiv 3\ (\mathrm{mod}\ 4)$，$\left(\frac{n}{p}\right) = 1$，证明 $x \equiv \pm n^{\frac{p+1}{4}}\ (\mathrm{mod}\ p)$是同余方程

$$x^2 \equiv n\ (\mathrm{mod}\ p)$$

的解。

5. 设 p 是奇素数，$(n, p) = 1$，α是正整数，证明同余方程

$$x^2 \equiv n\ (\mathrm{mod}\ p^\alpha)$$

有解的充要条件是$\left(\frac{n}{p}\right) = 1$。

6. 设 p 是奇素数，证明：模 p 的所有二次剩余的乘积与$(-1)^{\frac{p+1}{2}}$ 对模 p 同余。

第 6 节

1. 已知 769 与 1013 是素数，判定方程

(ⅰ) $x^2 \equiv 1742\ (\mathrm{mod}\ 769)$；

(ⅱ) $x^2 \equiv 1503\ (\mathrm{mod}\ 1013)$。

是否有解。

2. 求所有的素数 p，使得下面的方程有解：

$$x^2 \equiv 11 \pmod{p}。$$

3. 求所有的素数 p，使得 $-2 \in QR(p)$，$-3 \in QR(p)$。

4. 设$(x, y) = 1$，试求$x^2 - 3y^2$的奇素数因数的一般形式。

5. 证明：形如 $8k + 5$（$k \in \mathbf{Z}$）的素数无穷多个。

6. 证明：对于任意的奇素数 p，总存在整数 n，使得

$$p \mid (n^2 + 1)(n^2 + 2)(n^2 - 2)。$$

第 7 节

1. 证明定理的结论(ii)，(iii)，(iv)。

2. 已知 3019 是素数，判定方程$x^2 \equiv 374 \pmod{3019}$是否有解。

3. 设奇素数为 $p = 4n + 1$ 型，且 $d \mid n$，证明：$(\frac{d}{p}) = 1$。

4. 设 p，q 是两个不同的奇素数，且 $p = q + 4a$，证明：$(\frac{a}{p}) = (\frac{a}{q})$。

5. 设 $a > 0$，$b > 0$，b 为奇数，证明：

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

6. 设 a，b，c 是正整数，$(a, b) = 1$，$2 \nmid b$，$b < 4ac$，求 $(\frac{a}{4ac-b})$与$(\frac{a}{b})$的关系。

第 6 章

第 1 节

1. 设n是正整数，证明：不定方程$x^2 + y^2 = z^n$总有正整数解x，y，z。

2. 设 p 是奇素数，$(k, p) = 1$，则

$$\sum_{i=0}^{p-1}(\frac{i(i+k)}{p}) = -1,$$

此处$(\frac{a}{p})$是 Legender 符号。

3. 设素数 $p \equiv 1 \pmod 4$，$(k, p) = 1$，记

$$S(k)=\sum_{i=0}^{p-1}\left(\frac{i(i^2+k)}{p}\right),$$

则 $2\mid S(k)$，并且，对于任何整数 t，有

$$S(kt^2)=\left(\frac{t}{p}\right)S(k),$$

此处 $\left(\frac{a}{p}\right)$ 是 Legender 符号。

4. 设 p 是奇素数，$\left(\frac{m}{p}\right)=1$，$\left(\frac{n}{p}\right)=-1$，则

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

构成模 p 的一个简化剩余系。

5. 在第 3 题的条件下，并沿用第 2 题的记号，有

$$p=\left(\frac{1}{2}S(m)\right)^2+\left(\frac{1}{2}S(n)\right)^2。$$

即上式给出了形如 $4k+1$ 的素数的二平方和表示的具体方法。

6. 利用题 5 的结论，试将 $p=13$ 写成二平方和。

第 2 节

1. 若 $(x, y, z)=1$，则不存在整数 n，使得

$$x^2+y^2+z^2=4n^2。$$

2. 设 k 是非负整数，证明 2^k 不能表示三个正整数平方之和。

3. 证明：每一个正整数 n 必可以表示为 5 个立方数的代数和。

4. 证明：$16k+15$ 型的整数至少需要 15 个四次方数的和表之。

5. 证明：$16^k\cdot 31$ 不能表示为 15 个四次方数的和。

第 7 章

第 1 节

2. 求模 14 的全部原根。

3. 设 $m>1$，模 m 有原根，d 是 $\varphi(m)$ 的任一个正因数，证明：在模 m 的简化剩余系中，恰有 $\varphi(d)$ 个指数为 d 的整数，并由此推出模 m 的简化剩余系中恰有 $\varphi(\varphi(m))$ 个原根。

4. 设 $m\geq 3$，g 是模 m 的原根，$x_1, x_2, \cdots, x_{\varphi(m)}$ 是模 m 的简化剩余系，证

明：

(ⅰ) $g^{\frac{\varphi(m)}{2}} \equiv -1 \pmod{m}$；

(ⅱ) $x_1x_2\cdots x_{\varphi(m)} \equiv -1 \pmod{m}$。

5. 设$p = 2^n + 1$是一个奇素数，证明：模p的全部二次非剩余就是模p的全部原根。

6. 证明：

(ⅰ) 设p奇素数，则$M_p = 2^p - 1$的素因数必为$2pk + 1$型；

(ⅱ) 设$n \geq 0$，则$F_n = 2^{2^n} + 1$的素因数必为$2^{n+1}k + 1$型。

第 2 节

1. 求模 29 的最小正原根。

2. 分别求模 29^3和模 $2\cdot 29^3$的原根。

3. 解同余方程：$x^{12} \equiv 16 \pmod{17}$。

4. 设 p 和 $q = 4p + 1$ 都是素数，证明：2 是模 q 的一个原根。

5. 设$m \geq 3$，g_1和g_2都是模m的原根，则$g = g_1g_2$不是模m的原根。

6. 设 p 是奇素数，证明：当且仅当 $p - 1 \nmid n$ 时，有

$$1^n + 2^n + \cdots + (p-1)^n \equiv 0 \pmod{p}。$$

第 8 章

第 1 节

1. 补足定理 1 的证明。

2. 证明定理 2。

3. 证明：有理数为代数整数的充要条件是这个有理数为整数。

第 2 节

1. 证明例中的结论。

2. 证明连分数

$$\frac{1}{10+}\frac{1}{10^{2!}+}\frac{1}{10^{3!}+}\cdots\frac{1}{10^{n!}+}\cdots$$

是超越数。

3. 设ξ是一个超越数，α是一个非零的代数数，证明：$\xi + \alpha$，$\xi\alpha$，$\frac{\xi}{\alpha}$都是超越数。

第 3 节

1. 证明引理 1。

2. 证明定理 3 中的 $F\left(\frac{a}{b}\right)+F(0)$是整数。

第 9 章

第 1 节

1. 问：1948 年 2 月 14 日是星期几？

2. 问：1999 年 10 月 1 日是星期几？

第 2 节

1. 编一个有十个球队进行循环赛的程序表。

2. 编一个有九个球队进行循环赛的程序表。

第 3 节

1. 利用例 1 中的加密方法，将“ICOMETODAY”加密。

2. 已知字母 a，b，…，y，z，它们分别与整数 00，01，…，24，25 对应，又已知明文 h 与 p 分别与密文 e 与 g 对应，试求出密解公式：

$$P \equiv a'E + b' \pmod{26},$$

并破译下面的密文：“IRQXREFRXLGXEPQVEP”。

第 4 节

1. 设一 RSA 的公开加密钥为 $n = 943$，$e = 9$，试将明文 $P = 100$ 加密成密文 E。

2. 设RSA(n_A, e_A) = RSA(33, 3)，RSA(n_B, e_B) = RSA(35, 5)，A的签证信息为$M = 3$，试说明A向B发送签证M的传送和认证过程。

第 5 节

1. 设某数据库由四个文件组成：$F_1 = 4$，$F_2 = 6$，$F_3 = 10$，$F_4 = 13$。试设计一个对该数据库加密的方法，但要能取出个别的F_i（$1 \le i \le 4$），同时不影响其他文件的保密。

2. 利用本节中的秘密共享方案，设计一个由三方共管文件$M = 3$ 的方法，要求：只要有两方提供他们所掌握的数据，就可以求出文件M，但是，仅由任何一方的数据，不能求出文件M。（提示：取$p = 5$，$m_1 = 8$，$m_2 = 9$，$m_3 = 11$）

第 6 节

1. 设明文P的二进制表示是$P = (p_1p_2p_3p_4p_5p_6p_7p_8)_2$，与$P$对应的密文是$E$是$E = a_1p_1 + a_2p_2 + \cdots + a_8p_8$，如果这里的超增背包向量$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ = (5, 17, 43, 71, 144, 293, 626, 1280)，并且已知密文$E = 1999$，求明文P。

2. 给定超增背包向量(2, 3, 7, 13, 29, 59)，试设计一个背包型加密方法，将明文 $P = 51$ 加密。（提示：取 $M = 118$，$k = 77$）。

附录 1 习题参考答案

第一章 习 题 一

1. (i) 由$a \mid b$知$b = aq$，于是$b = (-a)(-q)$，$-b = a(-q)$及 $-b = (-a)q$，即$-a \mid b$，$a \mid -b$及$-a \mid -b$。反之，由 $-a \mid b$，$a \mid -b$及 $-a \mid -b$也可得$a \mid b$； (ii) 由$a \mid b$，$b \mid c$知$b = aq_1$，$c = bq_2$，于是$c = a(q_1q_2)$，即$a \mid c$； (iii) 由$b \mid a_i$知$a_i = bq_i$，于是$a_1x_1 + a_2x_2 + \cdots + a_kx_k = b(q_1x_1 + q_2x_2 + \cdots + q_kx_k)$，即$b \mid a_1x_1 + a_2x_2 + \cdots + a_kx_k$；(iv) 由$b \mid a$知$a = bq$，于是$ac = bcq$，即$bc \mid ac$； (v) 由$b \mid a$知$a = bq$，于是$|a| = |b||q|$，再由$a \neq 0$ 得$|q| \geq 1$，从而$|a| \geq |b|$，后半结论由前半结论可得。

2. 由恒等式$mq + np = (mn + pq) - (m - p)(n - q)$及条件$m - p \mid mn + pq$可知$m - p \mid mq + np$。

3. 在给定的连续 39 个自然数的前 20 个数中，存在两个自然数，它们的个位数字是 0，其中必有一个的十位数字不是 9，记这个数为 a，它的数字和为 s，则 $a, a + 1, \cdots, a + 9, a + 19$ 的数字和为 $s, s + 1, \cdots, s + 9, s + 10$，其中必有一个能被 11 整除。

4. 设不然，$n_1 = n_2n_3$，$n_2 \geq p$，$n_3 \geq p$，于是$n = pn_2n_3 \geq p^3$，即$p \leq \sqrt[3]{n}$，矛盾。

5. 存在无穷多个正整数k，使得 $2k + 1$ 是合数，对于这样的k，$(k + 1)^2$不能表示为$a^2 + p$的形式，事实上，若$(k + 1)^2 = a^2 + p$，则$(k + 1 - a)(k + 1 + a) = p$，得$k + 1 - a = 1$，$k + 1 + a = p$，即$p = 2k + 1$，此与$p$为素数矛盾。

第一章 习 题 二

1. 验证当 n =0,1，2，… ,11 时，$12|f(n)$。

2. 写$a = 3q_1 + r_1$，$b = 3q_2 + r_2$，$r_1, r_2 = 0, 1$ 或 2，由 $3 \mid a^2 + b^2 = 3Q + r_1^2 + r_2^2$知$r_1 = r_2 = 0$，即 $3 \mid a$且 $3 \mid b$。

3. 记 n=10q+r, (r=0,1,…,9)，则n^{k+4}- n^k被 10 除的余数和r^{k+4}- r^k = r^k(r^4-1)被 10 除的余数相同。对r=0,1,…,9 进行验证即可。

4. 对于任何整数n，m，等式$n^2 + (n + 1)^2 = m^2 + 2$ 的左边被 4 除的余数为 1，而右边被 4 除的余数为 2 或 3，故它不可能成立。

5 因$a^4 - 3a^2 + 9 = (a^2 - 3a + 3)(a^2 + 3a + 3)$，当$a = 1$，2 时，$a^2 - 3a + 3 = 1$，$a^4 - 3a^2 + 9 = a^2 + 3a + 3 = 7$，13，$a^4 - 3a^2 + 9$ 是素数；当$a \ge 3$ 时，$a^2 - 3a + 3 > 1$，$a^2 + 3a + 3 > 1$，$a^4 - 3a^2 + 9$ 是合数。

6. 设给定的n个整数为$a_1, a_2, \cdots, a_n$，作

$$s_1 = a_1，\ s_2 = a_1 + a_2，\ \cdots，\ s_n = a_1 + a_2 + \cdots + a_n，$$

如果s_i中有一个被n整除，则结论已真，否则存在s_i，s_j，$i < j$，使得s_i与s_j被n除的余数相等，于是$n \mid s_j - s_i = a_{i+1} + \cdots + a_j$。

第一章　习 题 三

1. (ⅰ) 因为$d \mid a$和$d \mid |a|$ 是等价的，所以$a_1, a_2, \cdots, a_k$的公约数的集合与$|a_1|, |a_2|, \cdots, |a_k|$ 的公约数的集合相同，所以它们的最大公约数相等； (ⅱ)，(ⅲ) 显然； (ⅳ) 设$(p, a) = d$，则$d \mid p$，$d \mid a$，由$d \mid p$得$d = 1$ 或$d = p$，前者推出$(p, a) = 1$，后者推出$p \mid a$。

2. (ⅰ) 由$d \mid a_i$推出$d \mid y_0 = (a_1, a_2, \cdots, a_k)$； (ⅱ) 分别以$y_0$和$Y_0$表示集合$A = \{ y;\ y = \sum_{i=1}^{k} a_i x_i,\ x_i \in \mathbf{Z},\ 1 \le i \le k \}$和$A^* = \{ y;\ y = \sum_{i=1}^{k} m a_i x_i,\ x_i \in \mathbf{Z},\ 1 \le i \le k \}$中的最小正整数，显然有$Y_0 = |m| y_0$； (ⅲ) 在推论 2 中取$m = \delta$，并用$\frac{a_1}{\delta}, \frac{a_2}{\delta}, \cdots, \frac{a_k}{\delta}$代替$a_1, a_2, \cdots, a_k$即可。

3. (ⅰ) 若$p \nmid a$，则$(p, a) = 1$，从而由$p \mid ab$推出$p \mid b$； (ⅱ) 在(ⅰ)中取$a = b$可得； (ⅲ) $(a, b_1 b_2 \cdots b_n) = (a, b_2 \cdots b_n) = \cdots = (a, b_n) = 1$。

4. 由恒等式 $9(2x + 3y) - 2(9x + 5y) = 17y$ 及 $17 \mid 2x + 3y$ 得 $17 \mid 2(9x + 5y)$，又$(17, 2) = 1$，故 $17 \mid 9x + 5y$。

5. 设$(a, b) = d$，则$a = da_1$，$b = db_1$，$(a_1, b_1) = 1$，由$a^2 \mid b^2 c$得$a_1^2 \mid b_1^2 c$，$a_1^2 \mid c$，因为c无平方因子，所以$a_1 = 1$，$a = d$，$b = ab_1$，即$a \mid b$。

6. 设 $(C_{2n}^1, C_{2n}^3, \cdots, C_{2n}^{2n-1}) = d$，由$C_{2n}^1 + C_{2n}^3 + \cdots + C_{2n}^{2n-1} = 2^{2n-1}$知$d \mid 2^{2n-1}$，设 $2^k \| n$ 并且 2^{k+1}不整除n，由 $2^{k+1} \| C_{2n}^1$ 及$2^{k+1} \mid C_{2n}^i = \frac{2n}{i} C_{2n-1}^{i-1}$，$i = 3, 5, \cdots, 2n - 1$，得$d = 2^{k+1}$。

第一章　习 题 四

1. (ⅰ)，(ⅱ) 显然； (ⅲ) 设$m_1 = [a_1, a_2, \cdots, a_k]$，$m_2 = [\,|a_1|, |a_2|, \cdots, |a_k|\,]$，

则由$a_i \mid m_1$推出$|a_i| \mid m_1$，即$m_2 \mid m_1$，同理可得$m_1 \mid m_2$，故$m_1 = m_2$；　(iv)　显然$a \mid |b|$，$b \mid |b|$，又若$a \mid m'$，$b \mid m'$，$m' > 0$，则$|b| \le m'$，故有$[a, b] = |b|$。

2.　设m是$a_1, a_2, \cdots, a_n$的任一个公倍数，由$a_1 \mid m$，$a_2 \mid m$知$[a_1, a_2] = m_2 \mid m$，由$m_2 \mid m$，$a_3 \mid m$知$[m_2, a_3] = m_3 \mid m$，…，由$m_{n-1} \mid m$，$a_n \mid m$知$[m_{n-1}, a_n] = m_n \mid m$，即$[a_1, a_2, \cdots, a_n] \mid m$。

3.　只须证 $(a+b)\dfrac{ab}{(a,b)} = a\dfrac{b(a+b)}{(b,a+b)}$，即只须证$(b, a+b) = (a, b)$，此式显然。

4.　由 $a + b = 120$ 及 $ab = (a, b)[a, b] = 24 \times 144 = 3456$ 解得 $a = 48$，$b = 72$ 或 $a = 72$，$b = 48$。

5.　因为 $[a,b,c]^2 = \dfrac{a^2b^2c^2}{(ab,bc,ca)^2}$，$[a,b][b,c][c,a] = \dfrac{a^2b^2c^2}{(a,b)(b,c)(c,a)}$，故只须证明$(a, b, c)(ab, bc, ca) = (a, b)(b, c)(c, a)$，此式用类似于例 3 的方法即可得证。

6.　设$s = 1^k + 2^k + \cdots + 9^k$，则由 $2s = (1^k + 9^k) + (2^k + 8^k) + \cdots + (9^k + 1^k) = 10q_1$ 及 $2s = (0^k + 9^k) + (1^k + 8^k) + \cdots + (9^k + 0^k) = 9q_2$得 $10 \mid 2s$和 $9 \mid 2s$，于是有 $90 \mid 2s$，从而 $1 + 2 + \cdots + 9 = 45 \mid s$。

第一章　习 题 五

1.　(i)　$a \mid b$知$b = ab_1$，由性质$(ma, mb) = |m|(a, b)$得$(a, b) = (a, ab_1) = a(1, b_1) = a$；　(ii)　由性质$(ma, mb) = |m|(a, b)$得$(a, b) = (2^{\alpha}a_1, 2^{\beta}b_1) = 2^{\beta}(2^{\alpha-\beta}a_1, b_1)$；　(iii)　由性质$(a, b) = 1 \Longrightarrow (a, bc) = (a, c)$得$(a, b) = (a, 2^{\beta}b_1) = (a, b_1)$；　(iv)　由性质$(a, b) = (|a-b|, b)$及$(a, b) = 1 \Longrightarrow (a, bc) = (a, c)$得$(a, b) = (|\dfrac{a-b}{2}|, b)$。

2.　作辗转相除：$1387 = (-162)\cdot(-8) + 91$，$-162 = 91\cdot(-2) + 20$，$91 = 20\cdot4 + 11$，$20 = 11\cdot1 + 9$，$11 = 9\cdot1 + 2$，$9 = 2\cdot4 + 1$，$2 = 1\cdot2 + 0$，由此得$n = 6$，$q_1 = -8$，$q_2 = -2$，$q_3 = 4$，$q_4 = 1$，$q_5 = 1$，$q_6 = 4$，$x = (-1)^{n-1}Q_n = 73$，$y = (-1)^nP_n = 625$，又$(1387, 162) = r_n = 1$，故 $1387\cdot73 - 162\cdot625 = 1 = (1387, 162)$。

3.　$(27090, 21672, 11352) = (4386, 10320, 11352) = (4386, 1548, 2580)$
$= (1290, 1548, 1032) = (258, 516, 1032) = (258, 0, 0) = 258$。

4.　$(F_{n+1}, F_n) = (F_n + F_{n-1}, F_n) = (F_{n-1}, F_n) = \cdots = (F_1, F_2) = 1$。

5.　设除数为 d，余数为 r，则由

$$d \mid 4582 - 2836 = 1746,\quad d \mid 5164 - 4582 = 582,\quad d \mid 6522 - 5164 = 1358$$

知 $d \mid (1746, 582, 1358) = 194$，由此得 $d = 97$，$r = 23$ 或 $d = 194$，$r = 120$。

6.　作辗转相除：

$$a = bq_1 + r_1,\qquad 0 < r_1 < |b|,$$

$$b = r_1q_2 + r_2,\qquad 0 < r_2 < r_1,$$
$$\cdots\ \cdots$$
$$r_{n-2} = r_{n-1}q_n + r_n,\quad 0 < r_n < r_{n-1},$$
$$r_{n-1} = r_nq_{n+1} + r_{n+1},\quad r_{n+1} = 0。$$

由第一式得

$$2^a - 1 = 2^{bq_1+r_1} - 2^{r_1} + 2^{r_1} - 1 = 2^{r_1}[(2^b)^{q_1} - 1] + (2^{r_1} - 1) = (2^b - 1)Q_1 + (2^{r_1} - 1),$$

即 $M_a = M_bQ_1 + M_{r_1}$，$(M_a, M_b) = (M_b, M_{r_1})$。类似可得$(M_b, M_{r_1}) = (M_{r_1}, M_{r_2})$ 等，于是 $(M_a, M_b) = (M_b, M_{r_1}) = \cdots = (M_{r_n}, M_{r_{n+1}}) = M_{r_n} = M_{(a,b)}$ 。

第一章　习 题 六

1. (ⅰ) 显然$d = p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}$（$0 \le \gamma_i \le \alpha_i$，$1 \le i \le k$）是$n$的正因数。反之，设$d$为$n$的任一个正因数，由$d\mid n$知对每一个$p_i$，$d$的标准分解式中$p_i$的指数都不超过$n$的标准分解式中$p_i$的指数，即$d$必可表示成 $p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}$（$0 \le \gamma_i \le \alpha_i$，$1 \le i \le k$）的形式； (ⅱ) 类似于(ⅰ)可证得。

2. (ⅰ) 显然对于$\lambda_i = \min\{\alpha_i, \delta_i\}$，$1 \le i \le k$，$p_1^{\lambda_1}\cdots p_k^{\lambda_k} \mid a$，$p_1^{\lambda_1}\cdots p_k^{\lambda_k} \mid b$ ，而且若$d'\mid a$，$d'\mid b$，则d'的标准分解式中p_i的指数同时不超过a和b的标准分解式中p_i的指数，即$d'\mid p_1^{\lambda_1}\cdots p_k^{\lambda_k}$ ，这就证明了$(a, b) = p_1^{\lambda_1}\cdots p_k^{\lambda_k}$ ，$\lambda_i = \min\{\alpha_i, \delta_i\}$，$1 \le i \le k$； (ⅱ) 类似于(ⅰ)即可证得。

3. $22345680 = 2^4\cdot 3\cdot 5\cdot 7\cdot 47\cdot 283$。

4. 写$i = 2^{\alpha_i}\lambda_i$，$2\nmid\lambda_i$，$i = 1, 2, \cdots, 2n$，则$\lambda_i$为 1, 2, ⋯, $2n$中的奇数，即λ_i只能取n个数值，在$n + 1$ 个这样的数中，必存在$\lambda_i = \lambda_j$（$i \ne j$），于是易知i与j成倍数关系。

5. 写$i = 2^{\alpha_i}\lambda_i$，$2\nmid\lambda_i$，$i = 1, 2, \cdots, n$，令$\alpha = \max\{\alpha_1, \alpha_2, \cdots, \alpha_n\} = \alpha_k$，显然$\alpha \ge 1$，且由第一节例 5 知使$\alpha = \alpha_k$的$k$（$1 \le k \le n$）是唯一的，取$T = 2^{\alpha-1}\lambda_1\lambda_2\cdots\lambda_n$，若$S$是整数，则$ST = T + \dfrac{T}{2} + \cdots + \dfrac{2^{\alpha-1}\lambda_1\lambda_2\cdots\lambda_n}{2^{\alpha_k}\lambda_k} + \cdots + \dfrac{T}{n}$中除$\dfrac{2^{\alpha-1}\lambda_1\lambda_2\cdots\lambda_n}{2^{\alpha_k}\lambda_k}$项外都是整数，矛盾。

6. 设 $a = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，$b = p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$ ，令

$$a_2 = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k},\quad \gamma_i = \begin{cases} \alpha_i, & \alpha_i = \max\{\alpha_i, \beta_i\}, \\ 0, & \text{其它}, \end{cases} \quad a_1 = \frac{a}{a_2},$$

$$b_2 = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k},\quad \delta_i = \begin{cases} \beta_i, & \text{当}\beta_i = \max\{\alpha_i, \beta_i\} \ne \alpha_i, \\ 0, & \text{其它}, \end{cases} \quad b_1 = \frac{b}{b_2},$$

则a_1，a_2，b_1，b_2使得$a = a_1a_2$，$b = b_1b_2$，$(a_2, b_2) = 1$，并且$[a, b] = a_2b_2$。

第一章　习 题 七

1. (ⅰ), (ⅱ), (ⅲ)　显然；　(ⅳ)　由$[x + y] = [[x] + \{x\} + [y] + \{y\}] = [x] + [y] + [\{x\} + \{y\}]$即可证得；　(ⅴ)　由$[-x] = [-([x] + \{x\})] = -[x] + [-\{x\}]$即可证得；(ⅵ)　由$\{-x\} = \{-([x] + \{x\})\} = \{-\{x\}\}$即可证得。

2. $[\frac{12347}{7}] + [\frac{12347}{7^2}] + [\frac{12347}{7^3}] + \cdots = 1763 + 251 + 35 + 5 = 2054$。

3. 由例 4 得$[x + \frac{1}{2}] = [2x] - [x]$，于是

$$\sum_{r=1}^{\infty}[\frac{n+2^{r-1}}{2^r}] = \sum_{r=1}^{\infty}[\frac{n}{2^r} + \frac{1}{2}] = \sum_{r=1}^{\infty}([\frac{n}{2^{r-1}}] - [\frac{n}{2^r}]) = [n] = n\text{。}$$

4.　设$x = a + \alpha$，a=1,2,…,n-1，$0 \le \alpha < 1$。代入原方程得到$[2a\alpha + \alpha^2] = 2a\alpha$，知$2a\alpha \in \mathbf{Z}$，$\alpha$的可能取值是 $0, \frac{1}{2a}, \cdots, \frac{2a-1}{2a}$，即有 $2a$ 个解。由于 $x=n$ 也是解，因此，共有 $2(1 + 2 + \cdots + n - 1) + 1$ 个解。

5. 设$x = n + \alpha$, $n \in \mathbf{Z}$, $1 \le \alpha < 1$, 则$f(x) = [x] + [2x] + [2^2x] + [2^3x] + [2^4x] + [2^5x] = n + 2n + 2^2n + 2^3n + 2^4n + 2^5n + [2\alpha] + [2^2\alpha] + [2^3\alpha] + [2^4\alpha] + [2^5\alpha]$，由此得 $63n \le f(x) \le 63n + 1 + 3 + 7 + 15 + 31 \le 63n + 57$，另一方面，12345 为 $63k + 60$ 型，故$f(x) \ne 12345$。

6. 设$n = a_0 + 2a_1 + 2^2a_2 + \cdots + 2^sa_s$，$a_i = 0$ 或 1，则

$$\begin{aligned} h &= [\frac{n}{2}] + [\frac{n}{2^2}] + [\frac{n}{2^3}] + \cdots \\ &= (a_1 + 2a_2 + 2^2a_3 + \cdots + 2^{s-1}a_s) + (a_2 + 2a_3 + \cdots + 2^{s-2}a_s) + \cdots + a_s \\ &= (2-1)a_1 + (2^2-1)a_2 + \cdots + (2^s-1)a_s \\ &= (a_0 + 2a_1 + 2^2a_2 + \cdots + 2^sa_s) - (a_0 + a_1 + a_2 + \cdots + a_s) = n - k\text{。} \end{aligned}$$

第一章　习 题 八

1. 设不然，则$n = 2^m n_1$，$2 \nmid n_1$，$n_1 > 1$，$2^{2^m n_1} + 1 = (2^{2^m} + 1)Q$，$1 < 2^{2^m} + 1 < 2^n + 1$，表明 $2^n + 1$ 是合数，矛盾。

2. 设不然，则$n = n_1 n_2$，$1 < n_1 < n$，则 $2^n - 1 = 2^{n_1 n_2} - 1 = (2^{n_1} - 1)Q$，$1 < 2^{n_1} - 1 < 2^n + 1$，表明 $2^n - 1$ 是合数，矛盾。

3. 若 $6n + 5$ 型的素数只有有限个，记为$p_1, p_2, \cdots, p_k$，作$A = 6\,p_1p_2\cdots p_k - 1$，显然$A > 1$，$A$是奇数，且$A$是 $6n + 5$ 型的整数，故A必存在一个 $6n + 5$ 型的素因数p，从而$p = p_i$（$1 \le i \le k$），由$p \mid A$，$p \mid p_1p_2\cdots p_k$推出$p \mid 1$，矛盾。

4. 设p_1，$p_2 = d + p_1$，$p_3 = 2d + p_1$，首先$p_1 \ne 2$ 且d是偶数，于是 $3 \nmid d$，从而对任意给定的d，p_1，p_2，p_3中有且只有一个被 3 整除，即p_1，p_2，p_3有且只有一个等于 3，故p_1，p_2，p_3最多只有一组。

5. 显然下面 n 个正整数$(n + 1)! + 2$，$(n + 1)! + 2$，$\cdots$，$(n + 1)! + (n + 1)$满足要求。

6. 设不然，则存在k，使得 $\sum\limits_{n=k+1}^{\infty}\dfrac{1}{p_n} < \dfrac{1}{2}$，设$Q = p_1p_2\cdots p_k$，考虑 $1 + nQ$，$n\in\mathbf{N}$，显然它们都不能被$p_1, p_2, \cdots, p_k$整除，即 $1 + nQ$的标准分解式中的素数都只能在$p_{k+1}, p_{k+2}, \cdots$中，从而对于任意的$r \ge 1$，有

$$\sum_{n=1}^{r}\frac{1}{1+nQ} \le \sum_{n=1}^{\infty}\Big(\sum_{m=k+1}^{\infty}\frac{1}{p_m}\Big)^n < \sum_{n=1}^{\infty}\Big(\frac{1}{2}\Big)^n,$$

右边是一个收敛的级数，故由比较判别法知 $\sum\limits_{n=1}^{\infty}\dfrac{1}{1+nQ}$ 也收敛，但事实上 $\sum\limits_{n=1}^{\infty}\dfrac{1}{1+nQ}$ 是一个发散级数，矛盾。

第二章　习 题 一

1. 定理 1 的证明：如果(ⅰ)成立，$m \mid a - b$，$a - b = mq$，$a = b + mq$，知(ⅱ)成立；如果(ⅱ)成立，写$a = q_1m + r_1, b = q_2m + r_2$，$0 \le r_1, r_2 \le m - 1$，则$q_1m + r_1 = q_2m + r_2 + mq$，由此得$r_1 = r_2$，知(iii)成立；如果(iii)成立，$a = q_1m + r, b = q_2m + r$，$0 \le r \le m - 1$，则$a - b = m(q_1 - q_2)$，$m \mid a - b$，知(ⅰ)成立。定理 2 的证明：结论(ⅰ)与(ⅱ)显然。(iii)　由定理 1 及$a \equiv b$，$b \equiv c \pmod m$可知存在整数q_1，q_2，使得$a = b + q_1m$，$b = c + q_2m$，因此$a = c + (q_1 + q_2)m$，推出$a \equiv c \pmod m$。定理 2 得证。

2. 由$x \equiv y \pmod m$得$x^i \equiv y^i \pmod m$，由$a_i \equiv b_i \pmod m$得$a_ix^i \equiv b_iy^i \pmod m$，

再由可加性得 $\sum_{i=0}^{n} a_i x^i \equiv \sum_{i=0}^{n} b_i y^i \pmod m$。

3. （i） 由 $a \equiv b \pmod m$ 得 $m \mid a - b$，又 $d \mid m$，故 $d \mid a - b$，即 $a \equiv b \pmod d$；（ii）由 $a \equiv b \pmod m$ 得 $m \mid a - b$，故 $km \mid ka - kb$，即 $ak \equiv bk \pmod{mk}$；（iii） 由 $a \equiv b \pmod{m_i}$ 得 $m_i \mid a - b$，故 $[m_1, m_2, \cdots, m_k] \mid a - b$，即 $a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$；（iv）由 $a \equiv b \pmod m$ 得 $a = mq + b$，故 $(a, m) = (b, m)$；（v） 由 $ac \equiv bc \pmod m$ 得 $m \mid ac - bc = c(a - b)$，又 $(c, m) = 1$，故 $m \mid a - b$，即 $a \equiv b \pmod m$。

4. 因为 $8^2 \equiv -1 \pmod{13}$，所以 $8^{1234} = (8^2)^{617} \equiv (-1)^{617} \equiv -1 \equiv 12 \pmod{13}$，即 8^{1234} 被 13 除的余数是 12。

5. 对任意的整数 x，$x \equiv r \pmod m$，$1 \le r \le m$，于是 $f(x) \equiv f(r) \not\equiv 0 \pmod m$，从而 $f(x) \ne 0$，所以方程 $f(x) = 0$ 没有整数解。

6. 由 $99 \mid \overline{62\alpha\beta427}$ 得 $9 \mid \overline{62\alpha\beta427}$，$11 \mid \overline{62\alpha\beta427}$。从 $9 \mid \overline{62\alpha\beta427}$ 得 $\alpha + \beta = 6$ 或 $\alpha + \beta = 15$，从 $11 \mid \overline{62\alpha\beta427}$ 得 $\alpha - \beta = -2$ 或 $\alpha - \beta = 9$，于是解关于 α，β 的方程组

$$\begin{cases} \alpha + \beta = 6 \\ \alpha - \beta = -2 \end{cases} \text{或} \begin{cases} \alpha + \beta = 6 \\ \alpha - \beta = 9 \end{cases} \text{或} \begin{cases} \alpha + \beta = 15 \\ \alpha - \beta = -2 \end{cases} \text{或} \begin{cases} \alpha + \beta = 15 \\ \alpha - \beta = 9 \end{cases}$$

得 $\alpha = 2$，$\beta = 4$。

第二章 习 题 二

1. 若 A 是模 m 的完全剩余系，显然（i）与（ii）成立。反之，满足（i）与（ii）的一组数必分别来自于模 m 的每一个不同的剩余类，即 A 是模 m 的完全剩余系。

2. 由威尔逊定理知 $-1 \equiv (2p)! = p!(p+1)\cdots(2p) \equiv (-1)^p (p!)^2 \pmod{2p+1}$，由此得 $(p!)^2 + (-1)^p \equiv 0 \pmod{2p+1}$。

3. 由 $(p-1)! \equiv p - 1 \pmod p$，$(p-1)! \equiv p - 1 \pmod{p-1}$ 以及 $(p, p-1) = 1$ 得 $(p-1)! \equiv p - 1 \pmod{p(p-1)}$，又 $2N = p(p-1)$，故 $(p-1)! \equiv p - 1 \pmod N$。

4. 设不然，$n = n_1 n_2$，$1 < n_1 < n$，由 $(n-1)! \equiv -1 \pmod{n_1}$ 得 $0 \equiv -1 \pmod{n_1}$，矛盾。

5. 设 $4 \mid m$，如果 $\{a_1b_1, a_2b_2, \cdots, a_mb_m\}$ 是模 m 的完全剩余系，则其中的奇数与偶数各半，又 $\{a_1, a_2, \cdots, a_m\}$ 与 $\{b_1, b_2, \cdots, b_m\}$ 也是模 m 的两个完全剩余系，故 a_ib_i 必须使 a_i，b_i 同为奇数或偶数，即 $a_ib_i \not\equiv 2 \pmod 4$，这对于 $4 \mid m$ 的模 m 的完全剩余系是不可能的。

6. （i） 由 b_i 通过 m_i 个数可知 $b_1\delta_1 + b_2\delta_2 + \cdots + b_n\delta_n$ 通过 $m = m_1m_2\cdots m_n$ 个数；（ii） 如果 $b_1'\delta_1 + b_2'\delta_2 + \cdots + b_n'\delta_n \equiv b_1''\delta_1 + b_2''\delta_2 + \cdots + b_n''\delta_n \pmod m$，则 $b_1'\delta_1 + b_2'\delta_2 + \cdots + b_n'\delta_n \equiv b_1''\delta_1 + b_2''\delta_2 + \cdots + b_n''\delta_n \pmod{m_i}$，即 $b_i' \equiv b_i'' \pmod{m_i}$，$b_i' = b_i''$。故 $b_1\delta_1 + b_2\delta_2 + \cdots + b_n\delta_n$ 通过模 $m = m_1m_2\cdots m_n$ 的完全剩余系。

第二章　习 题 三

1. 若 A 是模 m 的简化剩余系，显然(i)，(ii)与(iii) 成立。反之，满足(i)，(ii)与(iii) 的一组数必分别来自于模 m 得每一个不同的与模 m 互素的剩余类，即它是模 m 的简化剩余系。

2. 对n施行数学归纳法。当$n = 2$ 时，由定理 3 知命题成立，假定命题在n时成立，即$x = M_1'x_1 + M_2'x_2 + \cdots + M_n'x_n$通过模$m = m_1m_2\cdots m_n$的简化剩余系，则

$$\begin{aligned}&m_{n+1}x + m_1m_2\cdots m_nx_{n+1}\\ &= m_{n+1}M_1'x_1 + m_{n+1}M_2'x_2 + \cdots + m_{n+1}M_n'x_n + m_1m_2\cdots m_nx_{n+1}\\ &= M_1x_1 + M_2x_2 + \cdots + M_nx_n + M_{n+1}x_{n+1}\end{aligned}$$

通过模$m_1m_2\cdots m_nm_{n+1}$的简化剩余系，由归纳原理知命题对一切$n \ge 2$ 成立。

3. 写$ax_i = mq_i + r_i$，$0 \le r_i < m$，由x_i通过模m的简化剩余系知r_i通过模m的最小非负简化剩余系，于是由例 1 得

$$\sum_{i=1}^{\varphi(m)}\{\frac{ax_i}{m}\} = \sum_{i=1}^{\varphi(m)}\{q_i + \frac{r_i}{m}\} = \sum_{i=1}^{\varphi(m)}\frac{r_i}{m} = \frac{1}{m}\sum_{i=1}^{\varphi(m)} r_i = \frac{1}{2m}m\varphi(m) = \frac{1}{2}\varphi(m)。$$

4. 设 $m = p_1^{\alpha_1}\cdots p_k^{\alpha_k}m_1$，$n = p_1^{\beta_1}\cdots p_k^{\beta_k}n_1$，$p_i \nmid m_1$，$p \nmid n_1$，$(m_1,n_1) = 1$，则

$$\varphi(mn) = \varphi(p_1^{\alpha_1+\beta_1}\cdots p_k^{\alpha_k+\beta_k}m_1n_1) = p_1^{\alpha_1+\beta_1}\cdots p_k^{\alpha_k+\beta_k}\prod_{i=1}^{k}(1-\frac{1}{p_i})\varphi(m_1)\varphi(n_1),$$

$$\varphi((m,n)) = \varphi(p_1^{\min\{\alpha_1,\beta_1\}}\cdots p_k^{\min\{\alpha_k,\beta_k\}}) = (m,n)\prod_{i=1}^{k}(1-\frac{1}{p_i}),$$

由此得

$$\begin{aligned}\varphi(mn)\varphi((m,n)) &= (m,n)\, p_1^{\alpha_1}\cdots p_k^{\alpha_k}\prod_{i=1}^{k}(1-\frac{1}{p_i})\varphi(m_1)\, p_1^{\beta_1}\cdots p_k^{\beta_k}\prod_{i=1}^{k}(1-\frac{1}{p_i})\varphi(n_1)\\ &= (m,n)\varphi(m)\varphi(n)。\end{aligned}$$

5. 设 $a = p_1^{\alpha_1}\cdots p_k^{\alpha_k}m_1$，$b = p_1^{\beta_1}\cdots p_k^{\beta_k}n_1$，$p_i \nmid m_1$，$p \nmid n_1$，$(m_1,n_1) = 1$，取 $m = p_1^{\beta_1}\cdots p_k^{\beta_k}n_1^2m_1k$，$n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}m_1^2n_1k$，$(k, a) = (k, b) = 1$，则可得 $\frac{\varphi(m)}{\varphi(n)} = \frac{b}{a}$，即 $a\varphi(m) = b\varphi(n)$。

6. (i) 当$n = 1$ 时显然；当$n = 2^\alpha$时，$\varphi(2^\alpha) = 2^{\alpha-1} > \frac{1}{2}\sqrt{2^\alpha}$（$\alpha \ge 1$）；当$n = p^\alpha$，$p$为奇素数时，$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} > \sqrt{p^\alpha}$（$\alpha \ge 1$）；现在设 $n = 2^\alpha p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，则 $\varphi(n) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k}) > \frac{1}{2}\sqrt{2^\alpha}\sqrt{p_1^{\alpha_1}}\cdots\sqrt{p_k^{\alpha_k}} < \frac{1}{2}\sqrt{n}$。(ii) 设$n$是合数，$p_0$为$n$的最小素因数，则$p_0 \le \sqrt{n}$，于是

$$\varphi(n) = n\prod_{p|n}(1-\frac{1}{p}) \le n(1-\frac{1}{p_0}) \le n(1-\frac{1}{\sqrt{n}}) = n-\sqrt{n} \text{。}$$

第二章　习 题 四

1.　因 $10^3 = 2^3 5^3$，显然 $1978^{103} - 1978^3 \equiv 0 \pmod{2^3}$，再由 $1978^{100} \equiv 1 \pmod{5^3}$ 得 $1978^{103} - 1978^3 \equiv 0 \pmod{5^3}$，故 $1978^{103} - 1978^3 \equiv 0 \pmod{10^3}$。

2.　$313^{159} = 5^{159} = (5^6)^{26}5^3 \equiv 5^3 = 25\cdot 5 \equiv 4\cdot 5 \equiv 6 \pmod 7$。

3.　因 $561 = 3\cdot 11\cdot 17$，对于一切整数a，$(a, 561) = 1$，有$(a, 3) = 1$，$(a, 11) = 1$，$(a, 17) = 1$，　由费马定理可得$a^{560} = (a^2)^{280} \equiv 1 \pmod 3$，$a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}$，$a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$，故$a^{560} \equiv 1 \pmod{561}$。

4.　由费马定理$q^{p-1} \equiv 1 \pmod p$，$p^{q-1} \equiv 1 \pmod q$，$p^{q-1} + q^{p-1} \equiv 1 \pmod p$，$p^{q-1} + q^{p-1} \equiv 1 \pmod q$，故$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$。

5.　$6^{12} - 1 = (6^3 - 1)(6^3 + 1)(6^6 + 1) =5\cdot 43\cdot 7\cdot 31\cdot 46657$，对于 46657，它的素因数必为 $12k + 1$ 型，经检验的 $46657 = 13\cdot 37\cdot 97$，故 $6^{12} - 1 = 5\cdot 7\cdot 13\cdot 31\cdot 37\cdot 43\cdot 97$。

6.　设素数$p \mid b^n + 1$，即$b^n \equiv -1 \pmod p$，于是$b^{2n} \equiv 1 \pmod p$，由例 5 得下面两种情形之一成立：

(i)　$p \mid b^d - 1$ 对于 $2n$的某个因数$d < 2n$成立；

(ii)　$p \equiv 1 \pmod{2n}$。

第二章　习 题 五

1.　设 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，则$n$正因数可表示为$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$（$0 \le \gamma_i \le \alpha_i$，$1 \le i \le k$），于是$d(n) = \sum_{d|n} 1 = \sum_{i=1}^{k} \sum_{0\le\gamma_i\le\alpha_i} 1$ $=(1 + \alpha_1)(1 + \alpha_2)\cdots(1 + \alpha_k)$。由上式立知$d(n)$是积性函数，但$d(4) = 3 \ne 4 = d(2)d(2)$，故$d(n)$不是完全积性函数。

2.　若不恒为零的数论函数 $f(n)$是完全积性函数，必为积性函数，故 $f(1) =1$ 且 $f(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = f(p_1)^{\alpha_1} f(p_2)^{\alpha_2} \cdots f(p_k)^{\alpha_k}$。反之，若整数 m，n 中有一个等于 1，显然有 $f(mn) = f(m)f(n)$，若 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$，$n = p_1^{\beta_1} \cdots p_k^{\beta_k}$，则

$$\begin{aligned} f(mn) &= f(p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k}) \\ &= f(p_1)^{\alpha_1+\beta_1} \cdots f(p_k)^{\alpha_k+\beta_k} = f(p_1)^{\alpha_1} \cdots f(p_k)^{\alpha_k} f(p_1)^{\beta_1} \cdots f(p_k)^{\beta_k} \\ &= f(m) f(m) \text{。} \end{aligned}$$

3. $\sum\limits_{d|n}\frac{1}{d}=\frac{1}{n}\sum\limits_{d|n}\frac{n}{d}=\frac{1}{n}\sum\limits_{d|n}d=\frac{\sigma(n)}{n}$。

4. (i) 当 $n=1$ 时，右边的连乘理解为 1，等式成立。设 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，则有 $\sum\limits_{d|n}\mu(d)f(d)=\prod\limits_{p_i|n}(1+\mu(p_i)f(p_i)+\cdots+\mu(p_i^{\alpha_i})f(p_i^{\alpha_i}))=\prod\limits_{p_i|n}(1-f(p_i))$； (ii) 当 $n=1$ 时，右边的连乘理解为 1，等式成立。设 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，则有 $\sum\limits_{d|n}\mu^2(d)f(d)=\prod\limits_{p_i|n}(1+\mu^2(p_i)f(p_i)+\cdots+\mu^2(p_i^{\alpha_i})f(p_i^{\alpha_i}))=\prod\limits_{p_i|n}(1+f(p_i))$。

5. 当 $n=1$ 时，$\sum\limits_{d|n}\varphi(d)=1$，设 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，则

$$\begin{aligned}\sum_{d|n}\varphi(d)&=\sum_{d_1|p_1^{\alpha_1}}\varphi(d_1)\cdots\sum_{d_{k1}|p_k^{\alpha_k}}\varphi(d_k)\\&=[1+(p_1-1)+\cdots+(p_1^{\alpha_1}-p_1^{\alpha_1-1})]\cdots[1+(p_k-1)+\cdots+(p_k^{\alpha_k}-p_k^{\alpha_k-1})]\\&=p_1^{\alpha_1}\cdots p_k^{\alpha_k}=n\text{。}\end{aligned}$$

第三章 习 题 一

1. 对于任意的正实数α，写$\alpha=[\alpha]+\{\alpha\}$，则由定理 1，定理 2 可知$[\alpha]$与$\{\alpha\}$可分别唯一地表示为$\sum\limits_{i=0}^{k}a_ib^i$与$\sum\limits_{i=-1}^{-\infty}a_ib^i$ 形式，故α可以唯一的表示为$\alpha=\sum\limits_{i=-1}^{-\infty}a_ib^i$（$0\le a_i\le b-1$，且对于任何正整数$m$，都存在$n>m$，使得$a_{-n}<b-1$）的形式。

2. $789=(1100010101)_2=(11124)_5$。

3. $\frac{8}{21}=0.\dot{3}8095\dot{2}$。

4. 由$n=(a_k\cdots a_1a_0)_7=a_k7^k+\cdots+a_17+a_0\equiv a_k+\cdots+a_1+a_0 \pmod 2$得

$$2\mid n=(a_k\cdots a_1a_0)_7\Longleftrightarrow 2\mid a_k+\cdots+a_1+a_0\text{。}$$

5. 若$\frac{m}{n}=(0.a_{-1}a_{-2}\cdots a_{-k})_b$，则$b^km=n(a_{-1}b^{k-1}+a_{-2}b^{k-2}+\cdots+a_{-k})$，即$n\mid b^km$，$n\mid b^k$，故$n$的每个素因数都是$b$的因素数。反之，若$n$的每个素因数都是$b$的素因数，则必存在$k$，使得$n\mid b^k$，即$b^k=nn_1$，$\frac{m}{n}=\frac{1}{b^k}mn_1=\frac{1}{b^k}(a_lb^l+\cdots+a_1b+a_0)$，故$\frac{m}{n}$的$b$进制小数 $(0.a_{-1}a_{-2}a_{-3}\cdots)_b$为有限小数。

第三章 习 题 二

1. 显然$p_1 = |a_1| = a_1$，$p_2 = \begin{vmatrix} a_1 & -1 \\ 1 & a_2 \end{vmatrix} = a_1a_2 + 1$，当$k \geq 3$ 时，有

$$p_k = a_k\begin{vmatrix} a_1 & -1 & 0 & \cdots & 0 \\ 1 & a_2 & -1 & \cdots & 0 \\ 0 & 1 & a_3 & \cdots & 0 \\ & \cdots & & \cdots & \\ 0 & 0 & 0 & \cdots & a_{k-1} \end{vmatrix} + \begin{vmatrix} a_1 & -1 & \cdots & 0 & 0 \\ 1 & a_2 & \cdots & 0 & 0 \\ & \cdots & & \cdots & \\ 0 & 0 & \cdots & a_{k-2} & -1 \\ 0 & 0 & \cdots & 0 & 1 \end{vmatrix} = a_kp_{k-1} + {}_kp_{k-2}\text{,}$$

此与定理 1 中p_k的递推式一致；

显然$q_1 = 1$，$p_2 = \begin{vmatrix} 1 & 0 \\ 0 & a_2 \end{vmatrix} = a_2$，当$k \geq 3$ 时，有

$$q_k = a_k\begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & a_2 & -1 & \cdots & 0 \\ 0 & 1 & a_3 & \cdots & 0 \\ & \cdots & & \cdots & \\ 0 & 0 & 0 & \cdots & a_{k-1} \end{vmatrix} + \begin{vmatrix} a_1 & 0 & \cdots & 0 & 0 \\ 1 & a_2 & \cdots & 0 & 0 \\ & \cdots & & \cdots & \\ 0 & 0 & \cdots & a_{k-2} & -1 \\ 0 & 0 & \cdots & 0 & 1 \end{vmatrix} = a_kq_{k-1} + {}_kq_{k-2}\text{,}$$

此与定理 1 中q_k的递推式一致。

2. 当 $k = 2$ 时，由

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_1a_2+1 & a_1 \\ a_2 & 1 \end{pmatrix} = \begin{pmatrix} p_2 & p_1 \\ q_2 & q_1 \end{pmatrix}$$

知 $k = 2$ 时成立，归纳假定

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}$$

成立，则

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_{k+1} & 1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}\begin{pmatrix} a_{k+1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{k+1}p_k + p_{k-1} & p_k \\ a_{k+1}q_k + q_{k-1} & q_k \end{pmatrix} = \begin{pmatrix} p_{k+1} & p_k \\ q_{k+1} & q_k \end{pmatrix},$$

由归纳原理知对一切 $k \geq 2$ 有$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}$。

3. 由$a_1 = 1$，$a_2 = 2$，$a_3 = 3$ 得$p_1 = 1$，$p_2 = 3$，$p_3 = 10$，$q_1 = 1$，$q_2 = 2$，$q_3 = 7$，

故连分数$\langle 1, 2, 3, 4, 5, \cdots \rangle$的前三个渐近分数为$\frac{p_1}{q_1}=1$，$\frac{p_2}{q_2}=\frac{3}{2}$，$\frac{p_3}{q_3}=\frac{10}{7}$。

4. 设 $x=\langle 2, 3, 2, 3, \cdots \rangle$，则 $x = 2+\dfrac{1}{3+\dfrac{1}{x}}$，由此解得$x=\dfrac{3+\sqrt{15}}{3}$。

5. 易知$\dfrac{7}{9}=\dfrac{1}{1+\dfrac{2}{7}}=\dfrac{1}{1+\dfrac{1}{3+\dfrac{1}{2}}}=\langle 0, 1, 3, 2 \rangle$，$p_1=0$，$p_2=1$，$p_3=3$，$q_1=1$，$q_2=1$，$q_3=4$，于是 $7\cdot 4-9\cdot 3=(-1)^4=1$，故 $7x-9y=4$ 有特解$x_0=16$，$y_0=12$，原方程的一切整数解为$x=16+9t$，$y=12+7t$，$t\in\mathbf{Z}$。

第三章　习 题 三

1. （ⅰ） 记$\alpha_k=\langle a_{k+1}, a_{k+2}, \cdots, a_n \rangle$，$\beta_k=\langle \beta_{k+1}, \beta_{k+2}, \cdots, \beta_m \rangle$，由$\alpha_0=\beta_0=\dfrac{a}{b}$知$a_1=[\alpha_0]=[\beta_0]=b_1$，由 $a_1+\dfrac{1}{\alpha_1}=b_1+\dfrac{1}{\beta_1}$ 推出$\alpha_1=\beta_1$，从而$a_1=[\alpha_1]=[\beta_1]=b_1$，$\cdots$，反复以上推理最后可得$n=m$，$a_i=b_i$（$1\le i\le n$）；（ⅱ） 由(ⅰ)知$\dfrac{a}{b}$可唯一地表示为$\langle a_1, a_2, \cdots, a_n \rangle$，$a_n>1$，又易知$\langle a_1, a_2, \cdots, a_n \rangle$还可以另写成简单连分数$\langle a_1, a_2, \cdots, a_n-1, 1 \rangle$，但仅此而已，故有理数$\dfrac{a}{b}$仅有此两种表示成简单连分数的方法。

2. $\sqrt{13}=\langle 3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6, 1, 1, \cdots \rangle$。

3. 经计算 $2+\sqrt{3}=\langle 3, 1, 2, 1, 2, \cdots \rangle$，由此得$p_1=3$，$p_2=4$，$p_3=11$，$p_4=15$，$p_5=41$，$p_6=56$，$p_7=153$，$p_8=209$，$p_9=571$，$p_{10}=780$，$p_{11}=2131$，$\cdots$，$q_1=1$，$q_2=1$，$q_3=3$，$q_4=4$，$q_5=11$，$q_6=15$，$q_7=41$，$q_8=56$，$q_9=153$，$q_{10}=209$，$q_{11}=571$，$\cdots$，于是$\left|2+\sqrt{3}-\dfrac{780}{209}\right|<\dfrac{1}{209\cdot 571}<\dfrac{1}{10^5}$，故$\dfrac{780}{209}$即为所求。

4. $\sin 18^\circ=\dfrac{\sqrt{5}-1}{4}=\langle 0, 3, 4, 4, 4, 4, \cdots \rangle$，得$p_1=0$，$p_2=1$，$p_3=4$，$p_4=17$，$p_5=72$，$p_6=305$，$q_1=1$，$q_2=3$，$q_3=13$，$q_4=55$，$q_5=233$，$q_6=987$，于是$\left|\sin 18^\circ-\dfrac{72}{233}\right|<\dfrac{1}{233\cdot 987}<\dfrac{1}{10^5}$，故$\dfrac{72}{233}$即为所求。

5. π的前几个渐近分数为$\dfrac{3}{1}$，$\dfrac{22}{17}$，$\dfrac{333}{106}$，$\dfrac{355}{113}$，$\dfrac{103993}{33102}$，$\dfrac{104308}{33215}$，$\cdots$，其中$\dfrac{355}{113}$和$\dfrac{10993}{33102}$分别满足误差满足$\le 10^{-6}$和$\le 10^{-9}$的要求。

6. $\dfrac{1+\sqrt{5}}{2} = \langle 1, 1, 1, 1, 1, \cdots \rangle$，由此易得$p_k = p_{k-1} + p_{k-2} = F_k + F_{k-1} = F_{k+1}$，$q_k = q_{k-1} + q_{k-2} = F_{k-1} + F_{k-2} = F_k$，故$\dfrac{p_k}{q_k} = \dfrac{F_{k+1}}{F_k}$。

第三章　习 题 四

1. 方程 $3x^2 + 2x - 2 = 0$ 的正根$\dfrac{\sqrt{7}-1}{3} = \langle 0, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \cdots \rangle$。

2. $\alpha = \langle 1,\dot{2},\dot{3} \rangle = 1 + \dfrac{1}{2+\dfrac{1}{2+\alpha}}$，解得$x = \dfrac{\sqrt{15}-1}{2}$。

3. $\sqrt{a^2+1} = a + (\sqrt{a^2+1} - a) = a + \dfrac{1}{\sqrt{a^2+1}+a} = a + \dfrac{1}{2a+(\sqrt{a^2+1}-a)} = \cdots = \langle a, 2a, 2a, 2a, 2a, \cdots \rangle$。

4. 若$\sqrt{d} = \langle a_1,\dot{a}_2,\cdots,a_n,2\dot{a}_1 \rangle$，则

$$\sqrt{d} = \langle a_1,\dot{a}_2,\cdots,a_n,2\dot{a}_1 \rangle = \langle a_1,a_2,\cdots,a_n,a_1+\sqrt{d} \rangle = \frac{(a_1+\sqrt{d})p_n + p_{n-1}}{(a_1+\sqrt{d})q_n + q_{n-1}},$$

得$(dq_n - a_1p_n - p_{n-1}) + (a_1p_n + p_{n-1} - p_n)\sqrt{d} = 0$，由$\sqrt{d}$是无理数得$p_n = a_1q_n + q_{n-1}$，$dq_n = a_1p_n + p_{n-1}$，反之，若$p_n = a_1q_n + q_{n-1}$，$dq_n = a_1p_n + p_{n-1}$，则

$$\alpha = \langle a_1,\dot{a}_2,\cdots,a_n,2\dot{a}_1 \rangle = \langle a_1,a_2,\cdots,a_n,a_1+\alpha \rangle = \frac{(a_1+\alpha)p_n + p_{n-1}}{(a_1+\alpha)q_n + q_{n-1}},$$

得α满足方程$q_n\alpha^2 + (a_1q_n + q_{n-1} - p_n)\alpha - (a_1p_n + p_{n-1}) = 0$，即$\alpha^2 = d$，$\alpha = \sqrt{d}$。

5. 由第 4 题可得到。

第四章　习 题 一

1. 设 $\frac{17}{105}=\frac{x}{3}+\frac{y}{5}+\frac{z}{7}$，即 $35x+21y+15z=17$，因$(35, 21)=7$，$(7, 15)=1$，$1\mid 17$，故有解。分别解 $5x+3y=t$，$7t+15z=17$ 得 $x=-t+3u$，$y=2t-5u$，$u\in\mathbf{Z}$，$t=11+15v$，$z=-4-7v$，$v\in\mathbf{Z}$，消去 t 得 $x=-11-15v+3u$，$y=22+30v-5u$，$z=-4-7v$，u，$v\in\mathbf{Z}$。对于任意的确定的 u 和 v 的值，都给出一种表示法。

2. 分别解$x_1+2x_2=t$，$t+3x_3=41$ 得$x_1=t-2u$，$x_2=u$，$u\in\mathbf{Z}$，$t=41-3v$，$x_3=v$，$v\in\mathbf{Z}$，消去t得$x_1=41-3v-2u$，$x_2=u$，$x_3=v$，u，$v\in\mathbf{Z}$。由此得原方程的全部正整数解为$(x_1, x_2, x_3)=(41-3v-2u, u, v)$，$u>0$，$v>0$，$41-3v-2u>0$。

3. 消去x_1得 $9x_2-14x_3=3$，解得$x_2=-9+14t$，$x_3=-6+9t$，$t\in\mathbf{Z}$，从而得不定方程组的解为$x_1=43-55t$，$x_2=-9+14t$，$x_3=-6+9t$，$t\in\mathbf{Z}$，

4. 设甲、乙班的学生每人分别得 x，y 支铅笔，则 $7x+11y=100$，解这个不定方程得 $x=8$，$y=4$。

5. 二元一次不定方程 $ax+by=n$ 的一切整数解为 $\begin{cases}x=x_0-bt\\ y=y_0+at\end{cases}$，$t\in\mathbf{Z}$，于是由 $x\ge 0$，$y\ge 0$ 得 $-\frac{y_0}{a}\le t\le\frac{x_0}{b}$，但区间$[-\frac{y_0}{a}, \frac{x_0}{b}]$的长度是 $\frac{n}{ab}$，故此区间内的整数个数为$[\frac{n}{ab}]$或$[\frac{n}{ab}]+1$。

6. 因为 $0, 1, 2, \cdots, ab-a-b$ 中共有$(a-1)(b-1)$个数，故只须证明 n 与 $g-n$（$g=ab-a-b$）有且只有一个能表示成 $ax+by$（$x\ge 0$，$y\ge 0$）的形式。如果 n 与 $g-n$ 都能表示成 $ax+by$（$x\ge 0$，$y\ge 0$）的形式，即 $ax+by=n$（$x\ge 0$，$y\ge 0$），$ax'+by'=g-n$（$x'\ge 0$，$y'\ge 0$），则 $a(x+x')+b(y+y')=g$，这是不可能的；如果 n 不能表示成 $ax+by$（$x\ge 0$，$y\ge 0$）的形式，则因为二元一次不定方程 $ax+by=n$ 的一切整数解为 $\begin{cases}x=x_0-bt\\ y=y_0+at\end{cases}$，$t\in\mathbf{Z}$，所以当 t 使 $0\le x\le b-1$ 时，必有 $y\le -1$，于是 $a(b-1-x)+b(-1-y)=g-n$，即 $g-n$ 能表示成 $ax+by$（$x\ge 0$，$y\ge 0$）的形式。

第四章　习 题 二

1. 设有理数 $x=\frac{l}{m}$，$y=\frac{n}{m}$（$m\ne 0$）满足方程$x^2+y^2=1$，即$l^2+n^2=m^2$，于是得$l=\pm 2abd$，$n=\pm(a^2-b^2)d$，$m=\pm(a^2+b^2)d$或$l=\pm(a^2-b^2)d$，$m=\pm 2abd$，$m=\pm(a^2$

$+ b^2)d$，由此得$(x, y) = (\pm\frac{2ab}{a^2+b^2}, \pm\frac{a^2-b^2}{a^2+b^2})$或$(\pm\frac{a^2-b^2}{a^2+b^2}, \pm\frac{2ab}{a^2+b^2})$。反之，代入方程$x^2 + y^2 = 1$即知这样的点在单位圆周上。

2. 由$x^2 = (z + y)(z - y)$及x是素数得$z + y = x^2$，$z - y = 1$，于是$2z - 1 = x^2$，$2(x + y + 1) = (x + 1)^2$都是平方数。

3. 设$x - y = a^2$，$y - z = b^2$，$x - z = c^2$，则$a^2 + b^2 = c^2$，由此得$x = (u^2 + v^2)^2 + t$，$y = (u^2 - v^2)^2 + t$或$4u^2v^2 + t$，$z = t$，$u, v, t\in\mathbf{Z}$。

4. 设$(z - x, z + x) = d$，易知$d = 1$或 2。由$(z - x)(z + x) = 3y^2$得$z - x = 3da^2$，$z + x = db^2$，$y = dab$或$z - x = db^2$，$z + x = 3da^2$，$y = dab$，$a > 0$，$b > 0$，$(a, b) = 1$。(ⅰ)当$d = 1$：$x = \frac{|b^2 - 3a^2|}{2}$，$y = ab$，$z = \frac{b^2 + 3a^2}{2}$，$a > 0$，$b > 0$，$(a, b) = 1$，$3\nmid b$，$a, b$同为奇数；(ⅱ) 当$d = 2$：$x = |b^2 - 3a^2|$，$y = 2ab$，$z = b^2 + 3a^2$，$a > 0$，$b > 0$，$(a, b) = 1$，$3\nmid b$，$a, b$一奇一偶。反之，易验证(ⅰ)或(ⅱ)是原不定方程的解，且$x > 0$，$y > 0$，$z > 0$，$(x, y) = 1$。

5. (ⅰ) 设x，y，z是$x^2 + y^2 + z^2 = x^2y^2$的整数解，如果x，y同为奇数，则$x^2 + y^2 + z^2 \equiv 2$，$3 \pmod 4$，$x^2y^2 \equiv 1 \pmod 4$，此不可能；如果x，y一奇一偶，则$x^2 + y^2 + z^2 \equiv 1$，$2 \pmod 4$，$x^2y^2 \equiv 0 \pmod 4$，此也不可能。所以x，y同为偶数，z也是偶数，令$x = 2x_1$，$y = 2y_1$，$z = 2z_1$，代入原方程得$x_1^2 + y_1^2 + z_1^2 = 2^2x_1^2y_1^2$，反复以上的推理可得$x$，$y$，$z$能被 2 的任意次乘幂整除，只能$x = y = z = 0$。 (ⅱ) 类似于(ⅰ)可证。

6. 设x，y，z是$x^2 + y^2 = z^4$的满足$(x, y) = 1$，$2\mid x$的正整数解，则$x = 2ab$，$y = a^2 - b^2$，$z^2 = a^2 + b^2$，$a > b > 0$，$(a, b) = 1$，a, b一奇一偶， 再由$z^2 = a^2 + b^2$得$a = 2uv$，$b = u^2 - v^2$， $z = u^2 + v^2$ 或 $a = u^2 - v^2$，$b = 2uv$， $z = u^2 + v^2$， $u > v > 0$，$(u, v) = 1$，u, v一奇一偶，于是得$x = 4uv(u^2 - v^2)$，$y = |u^4 + v^4 - 6u^2v^2|$，$z = u^2 + v^2$，$u > v > 0$，$(u, v) = 1$，$u, v$一奇一偶。反之，易验证它是原不定方程的整数解，且$x > 0$，$y > 0$，$z > 0$，$(x, y) = 1$，$2\mid x$。

第四章 习 题 三

1. 由 $x(x + y) = 6$ 得$(x, y) = (1, 5)$，$(-1, -5)$，$(2, 1)$，$(-2, -1)$，$(3, -1)$，$(-3, 1)$，$(6, -5)$，$(-6, 5)$。

2. 由第一个方程得 $z = -(x + y)$，代入第二个方程经化简得 $xyz = -6$，由此得$(x, y, z) = (1, 2, -3)$，$(2, 1, -3)$，$(1, -3, 2)$，$(2, -3, 1)$，$(-3, 1, 2)$，$(-3, 2, 1)$，

3. 当$y = 1$ 时，$x = 2$，若$y \ge 2$，$x \ge 3$，则 $-3^y \equiv 1 \pmod 8$，这是不可能的，故原方程的正整数解只有$(x, y) = (2, 1)$。

4. 显然$x > z$，$y > z$，令$x = z + s$，$y = z + t$，s，$t\in\mathbf{N}$，代入原方程可得$z^2 = st$，

于是$s = a^2d$，$t = b^2d$，$z = abd$，其中$a, b, d\in\mathbf{N}$，$(a, b) = 1$，由此得$x = abd + a^2d$，$y = abd + b^2d$，$z = abd$，反之，将上式代入原方程知它们是原方程的正整数解。

5. 不妨设$x \le y$，当$p = 2$ 时，$(x, y) = (2, 2)$。下设p是奇素数，令 $2x = p + s$，$2y = p + t$，s，$t\in\mathbf{Z}$，$s \le t$，代入原方程可得$p^2 = st$，由此得$s = 1$，$t = p^2$或$s = p$，$t = p$或$s = -p^2$，$t = -1$，即$(x, y) = (\frac{p+1}{2},\frac{p(p+1)}{2}) = (p, p) = (\frac{p(1-p)}{2},\frac{p-1}{2})$。

6. 设M，b为任意的有理数，容易证明：若$a_1, a_2, \cdots, a_{2n+1}$具有性质$P$，则(ⅰ) M，$Ma_1, Ma_2, \cdots, Ma_{2n+1}$也具有性质$P$；(ⅱ) $a_1 + b, a_2 + b, \cdots, a_{2n+1} + b$也具有性质$P$。由此我们可假定$a_1, a_2, \cdots, a_{2n+1}$都是整数，且$a_1 = 0$。由性质$P$易知$a_i$都是偶数，于是由(ⅰ)知$\frac{a_1}{2},\frac{a_2}{2},\cdots,\frac{a_{2n+1}}{2}$也具有性质$P$，并且它们都是整数，且$\frac{a_1}{2} = 0$。反复以上推理可知对于任意的正整数$k$，$\frac{a_1}{2^k},\frac{a_2}{2^k},\cdots,\frac{a_{2n+1}}{2^k}$也具有性质$P$，故只可能$a_1 = a_1 = \cdots = a_{2n+1} = 0$。

第五章　习 题 一

1. (ⅰ) 若$f(x_0) \equiv 0 \pmod m$，则$f(x_0) + b(x_0) \equiv b(x_0) \pmod m$成立，反之，若$f(x_0) + b(x_0) \equiv b(x_0) \pmod m$，则$f(x_0) \equiv 0 \pmod m$成立；(ⅱ) 若$f(x_0) \equiv 0 \pmod m$，则$bf(x_0) \equiv 0 \pmod m$成立，反之，若$bf(x_0) \equiv 0 \pmod m$，则由$(b, m) = 1$ 得$f(x_0) \equiv 0 \pmod m$成立；(iii) 若$g(x_0)h(x_0) \equiv 0 \pmod m$，则由$m$是素数得$g(x_0) \equiv 0 \pmod m$或$h(x_0) \equiv 0 \pmod m$。

2. (ⅰ) $x \equiv 4 \pmod{17}$；(ⅱ) $x \equiv 1$，48，95，142，189 (mod 235)。

3. 消去 y 得 $8x \equiv 41 \pmod{47}$，解得 $x \equiv 11 \pmod{47}$，代入原方程组中的第二式得 $y \equiv 1 \pmod{47}$。故原方程组的解为 $x \equiv 11 \pmod{47}$，$y \equiv 1 \pmod{47}$。

4. 首先易知 $b(-1)^{a-1}\frac{(p-1)(p-2)\cdots(p-a+1)}{a!}$ 是整数，又由$(a, p) = 1$ 知方程 $ax \equiv b \pmod p$解唯一，故只须将 $x \equiv b(-1)^{a-1}\frac{(p-1)(p-2)\cdots(p-a+1)}{a!} \pmod p$代入 $ax \equiv b \pmod p$验证它是同余方程的解即可。

5. 必要性显然，下证充分性。当$n = 1$ 时，由定理 2 知命题成立。假设$n = k$时结论已真，考虑$a_1x_1 + a_2x_2 + \cdots + a_kx_k + a_{k+1}x_{k+1} \equiv b \pmod m$，令$(a_1, a_2, \cdots, a_k, m) = d_1$，$(d_1, a_{k+1}) = d$，因为同余方程$a_{k+1}x_{k+1} \equiv b \pmod{d_1}$有解，其解数为$d$，mod d_1，记$m = d_1m_1$，则解数为dm_1，mod m。现在固定一个解x_{k+1}，由归纳假定知$a_1x_1 + a_2x_2 + \cdots + a_kx_k \equiv b - a_{k+1}x_{k+1} \pmod m$有解，其解数为$d_1 m^{k-1}$，mod m，从而$a_1x_1 + a_2x_2 + \cdots + a_kx_k + a_{k+1}x_{k+1} \equiv b \pmod m$有解，其解数为$dm_1\cdot d_1m^{k-1} = d\cdot m^k$，mod m。由归

纳原理知命题对于一切$n \ge 1$成立。

6. 因为(2, 12) = 2，(2, 7) = 1$\mid$5，故同余方程有解，其解数为 1 12^{2-1} = 12，mod 12。先解同余方程 $7y \equiv 5 \pmod 2$，得$y \equiv 1 \pmod 2$，写成$y \equiv 1 + 2t \pmod{12}$，$t = 0, 1, 2, \cdots, 5$，对于固定的$t$，解同余方程 $2x \equiv 5 - 7(1 + 2t) \equiv -2 - 2t \pmod{12}$，得$x \equiv -1 - t \pmod 6$，写成$x \equiv -1 - t + 6s \pmod{12}$，$s = 0, 1$，故原方程组的解为$x \equiv -1 - t + 6s \pmod{12}$，$y \equiv 1 + 2t \pmod{12}$，$s = 0, 1$，$t = 0, 1, 2, \cdots, 5$。

第五章　习 题 二

1. $m = 5\cdot6\cdot7\cdot11 = 2310$；$M_1 = 6\cdot7\cdot11 = 462$，$M_2 = 5\cdot7\cdot11 = 385$，$M_3 = 5\cdot6\cdot11 = 330$，$M_4 = 5\cdot6\cdot7 = 210$；由 $462\cdot M_1' \equiv 1 \pmod 5$得$M_1' = 3$，$385\cdot M_2' \equiv 1 \pmod 6$得$M_2' = 1$，$330\cdot M_3' \equiv 1 \pmod 7$得$M_3' = 1$，$210\cdot M_4' \equiv 1 \pmod 5$得$M_4' = 1$。所以原同余方程组的解为$x \equiv 3\cdot462\cdot b_1 + 1\cdot385\cdot b_2 + 1\cdot330\cdot b_3 + 1\cdot210\cdot b_4 \pmod{2310}$。

2. 因为(15, 8) = 1$\mid$8 − 5，(15, 25) = 5$\mid$8 − 13，(8, 25) = 1$\mid$5 − 13，故原同余方程组有解，解数唯一，mod [15, 8, 25] = 600。将第一个同余方程的解$x = 8 + 15t_1$，$t_1\in\mathbf{Z}$，代入第二个同余方程得$t_1 \equiv 3 \pmod 8$，即$t_1 = 3 + 8t_2$，$t_2\in\mathbf{Z}$，$x = 53 + 120t_2$，代入第三个同余方程得$t_2 \equiv 3 \pmod 5$，即$t_2 = 3 + 5t_3$，$t_3\in\mathbf{Z}$，$x = 413 + 600t_3$，所以原同余方程组的解为$x \equiv 413 \pmod{600}$。

注：此处所使用的解法思路简单，但比较繁。

3. 设士兵有 x 人，由题意得 $x \equiv 1 \pmod 3$，$x \equiv -2 \pmod 5$，$x \equiv 3 \pmod{11}$，由孙子定理得 $x \equiv 58 \pmod{165}$，故 $x = 58$ 人。

4. 可设$n = 2^{\alpha}3^{\beta}5^{\gamma}$，由条件得

$$\alpha \equiv 1 \pmod 2,\quad \alpha \equiv 0 \pmod 3,\quad \alpha \equiv 0 \pmod 5;$$
$$\beta \equiv 0 \pmod 2,\quad \beta \equiv 1 \pmod 3,\quad \beta \equiv 0 \pmod 5;$$
$$\gamma \equiv 0 \pmod 2,\quad \gamma \equiv 0 \pmod 3,\quad \gamma \equiv 1 \pmod 5,$$

由孙子定理得$\alpha \equiv 15 \pmod{30}$，$\beta \equiv 10 \pmod{30}$，$\gamma \equiv 6 \pmod{30}$，故$n = 2^{15}3^{10}5^{6}$。

5. 作同余方程组：$x \equiv 0 \pmod{p_1}$，$x \equiv -1 \pmod{p_2}$，…，$x \equiv -n + 1 \pmod{p_n}$，由孙子定理知此同余方程组有解$x$，于是$x$，$x + 1$，…，$x + n - 1$ 满足要求。

6. 因 $105 = 3\cdot5\cdot7$，同余方程 $3x^2 + 11x - 20 \equiv 0 \pmod 3$的解为$x \equiv 1 \pmod 3$，同余方程 $3x^2 + 11x - 38 \equiv 0 \pmod 5$的解为$x \equiv 0, 3 \pmod 5$，同余方程 $3x^2 + 11x - 20 \equiv 0 \pmod 7$的解为$x \equiv 2，6 \pmod 7$，故原同余方程有 4 解，mod 105。作同余方程组：$x \equiv b_1 \pmod 3$，$x \equiv b_2 \pmod 5$，$x \equiv b_3 \pmod 7$，其中$b_1 = 1$，$b_2 = 0，3$，$b_3 = 2，6$，由孙子定理得原同余方程的解为$x \equiv 13，55，58，100 \pmod{105}$。

第五章　习 题 三

1. （ⅰ） 由定理知存在整数$x_2 = a + pt_1$，$t_1\in\mathbf{Z}$，使得$x \equiv x_2 \pmod{p^2}$是同余方程$f(x) \equiv 0 \pmod{p^2}$的解，$x_2 \equiv a \pmod{p}$。再由定理知存在整数$x_3 = x_2 + p^2t_2$，$t_2\in\mathbf{Z}$，使得$x \equiv x_3 \pmod{p^3}$是同余方程$f(x) \equiv 0 \pmod{p^3}$的解，$x_3 \equiv x_2 \equiv a \pmod{p}$，如此继续下去，最后知存在整数$x_\alpha = x_{\alpha-1} + p^{\alpha-1}t_{\alpha-1}$，$t_{\alpha-1}\in\mathbf{Z}$，使得$x \equiv x_\alpha \pmod{p^\alpha}$是同余方程$f(x) \equiv 0 \pmod{p^\alpha}$的解，$x_\alpha \equiv x_{\alpha-1} \equiv \cdots \equiv x_2 \equiv a \pmod{p}$；（ⅱ） 由条件知同余方程$f(x) \equiv 0 \pmod{p}$的每一个解$x \equiv x_1 \pmod{p}$都不是$f'(x) \equiv 0 \pmod{p}$的解，即$f'(x_1) \not\equiv 0 \pmod{p}$，于是由(ⅰ)知可导出$f(x) \equiv 0 \pmod{p^\alpha}$的解$x \equiv x_\alpha \pmod{p^\alpha}$，且由(ⅰ)的证明过程知只能导出唯一的解$x \equiv x_\alpha \pmod{p^\alpha}$。

2. 对$x \equiv 2 \pmod{5}$，令$x = 2 + 5t$代入同余方程 $2x^2 + 13x - 34 \equiv 0 \pmod{5^2}$得$t \equiv 0 \pmod{5}$，于是$x = 2 + 5(5t_1) = 2 + 25t_1$，代入同余方程 $2x^2 + 13x - 34 \equiv 0 \pmod{5^3}$得到$t \equiv 0 \pmod{5}$， 于是$x = 2 + 25(5t_2) = 2 + 125t_2$，即$x \equiv 2 \pmod{5^3}$是同余方程 $2x^2 + 13x - 34 \equiv 0 \pmod{5^3}$的一个解。

3. 对$x_0 = 4$，则由$(4 + 7x_1 + 7^2x_2)^2 \equiv 2 \pmod{7^2}$得$x_1 \equiv 5 \pmod{7}$，$x_1 = 5$。再由$(4 + 7\cdot5 + 7^2x_2)^2 \equiv 2 \pmod{7^3}$得$x_2 \equiv 4 \pmod{7}$，$x_2 = 4$，这样，求得原同余方程的一个解是$x \equiv 4 + 7\cdot5 + 7^2\cdot4 = 235 \pmod{7^3}$

4. 因 $54 = 2\cdot3^3$，而$x^2 \equiv -1 \pmod{3}$无解，故$x^2 \equiv -1 \pmod{54}$也无解。

5. 因 $75 = 3\cdot5^2$，先解$f(x) \equiv 0 \pmod{3}$，用逐一代入法得解$x \equiv 0 \pmod{3}$；再解$f(x) \equiv 0 \pmod{5^2}$，用逐一代入法得$f(x) \equiv 0 \pmod{5}$的解为$x \equiv 0$，$2 \pmod{5}$，对于$x \equiv 0 \pmod{5}$，令$x = 5t$代入$f(x) \equiv 0 \pmod{25}$得$t \equiv 2 \pmod{5}$， 于是$x = 5(2 + 5t_2) = 10 + 25t_2$，即$x \equiv 10 \pmod{25}$是$f(x) \equiv 0 \pmod{25}$的一个解，对于$x \equiv 2 \pmod{5}$，令$x = 2 + 5t$代入$f(x) \equiv 0 \pmod{25}$得$t \equiv 4 \pmod{5}$， 于是$x = 2 + 5(4 + 5t_2) = 22 + 25t_2$， 即$x \equiv 22 \pmod{25}$是$f(x) \equiv 0 \pmod{25}$的一个解；最后构造同余方程组$x \equiv b_1 \pmod{3}$，$x \equiv b_2 \pmod{25}$，$b_1 = 0$，$b_2 = 10$，22，由孙子定理得$f(x) \equiv 0 \pmod{75}$的两个解$x \equiv 10$，$72 \pmod{75}$。

6. 令$m = p_1p_2\cdots p_k$，p_i是不同的奇素数，由$x^2 \equiv 1 \pmod{p_i}$的解数$T_i = 2$，故$T = T_1T_2\cdots T_k = 2^k$，当$k$充分大时，必有 $2^k > n$。

第五章　习 题 四

1. （ⅰ） 原同余方程等价于 $3x^5 + 5x^4 + 2x^2 - 1 \equiv 0 \pmod{7}$，用$x = 0$，$\pm1$，$\pm2$，$\pm3$ 代入知后者无解； （ⅱ） 原同余方程等价于 $2x^4 + 2x^3 + 3x - 2 \equiv 0 \pmod{5}$，将$x = 0$，$\pm1$，$\pm2$ 代入，知后者有解$x \equiv \pm1 \pmod{5}$。

2. （ⅰ） $2x^3 - x^2 + 3x - 1 \equiv 0 \pmod{5}$等价于$x^3 - 3x^2 + 4x - 3 \equiv 0 \pmod{5}$，又$x^5 - x = (x^3 - 3x^2 + 4x - 3)(x^2 + 3x + 5) + (6x^2 - 12x + 15)$，其中$r(x) = 6x^2 - 12x + 15$ 的

系数不都是 5 的倍数，故原方程没有三个解；（ii） 因为这是对模 5 的同余方程，故原方程不可能有六个解。

3. 设x_1是$x^k \equiv a(\bmod m)$的任意一个解，则一次同余方程$yx_0 \equiv x_1 (\bmod m)$有解$y$，再由$y^k a \equiv y^k x_0^k \equiv (yx_0)^k \equiv x_1^k \equiv a (\bmod m)$得$y^k \equiv 1 (\bmod m)$，即$x_1$可以表示成$x \equiv yx_0 (\bmod m)$，其中$y$满足同余方程$y^k \equiv 1 (\bmod m)$；反之，易知如此形式的$x$是$x^k \equiv a(\bmod m)$的解。

4. 由$k \mid p-1$知同余方程$x^k \equiv 1 (\bmod p)$恰有k个解，又由$k \mid n$知这k个解也是同余方程$x^n \equiv 1 (\bmod p)$的解。下证同余方程$x^n \equiv 1 (\bmod p)$的解必是同余方程$x^k \equiv 1 (\bmod p)$的解，事实上，若$x_0^n \equiv 1 (\bmod p)$，记$k = sn + t(p-1)$。若$s > 0$，$t < 0$，则$x_0^k \equiv x_0^k x_0^{-t(p-1)} = x_0^{k-t(p-1)} = x_0^{sn} \equiv (x_0^n)^s \equiv 1 (\bmod p)$；若$s < 0$，$t > 0$，则可类似证明。

5. （i） $x^{p-1} - 1 \equiv 0 (\bmod p)$有解$x \equiv 1$，2，⋯，$p-1 (\bmod p)$，故对于一切整数$x$，$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) (\bmod p)$； （ii） 在(i)中令$x = p$。

6. 令$(x-1)(x-2)\cdots(x-p+1) = x^{p-1} - a_{p-2}x^{p-2} + \cdots + a_2x^2 - a_1x + a_0$，其中$a_{p-2} = 1 + 2 + \cdots + (p-1) = \dfrac{p(p-1)}{2}$是$p$的倍数，考虑同余方程$f(x) \equiv 0 (\bmod p)$，$f(x) = x^{p-1} + a_{p-3}x^{p-3} - \cdots + a_2x^2 - a_1x + a_0$，显然它有解$x \equiv 1$，2，⋯，$p-1 (\bmod p)$，故$x^p - x = f(x)x + r(x)$中的余式$r(x) = -a_{p-3}x^{p-2} + \cdots - a_2x^3 + a_1x^2 - (a_0+1)x$的系数都是$p$的倍数。

第五章　习 题 五

1. 因$11^{\frac{13-1}{2}} \equiv 11^6 = 121^3 \equiv 4^3 \equiv 12 \equiv -1(\bmod 13)$，故$x^2 \equiv 11 (\bmod 13)$无解。

2. 模 23 的所有的二次剩余为 $x \equiv 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 (\bmod 23)$，二次非剩余为 $x \equiv 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22 (\bmod 23)$。

3. 设 a，b 为模 p 的二次剩余，有 $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv 1\cdot 1 \equiv 1 (\bmod p)$，再设 c，d 为模 p 的二次非剩余，有 $(cd)^{\frac{p-1}{2}} = c^{\frac{p-1}{2}} d^{\frac{p-1}{2}} \equiv (-1)(-1) \equiv 1 (\bmod p)$，以及 $(ac)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} c^{\frac{p-1}{2}} \equiv 1\cdot(-1) \equiv 1 (\bmod p)$知结论成立。

4. 由欧拉判别法知 $n^{\frac{p-1}{2}} \equiv 1(\bmod p)$， 两边乘$n$得$(n^{\frac{p+1}{4}})^2 \equiv n(\bmod p)$，由此知$x^2 \equiv n (\bmod p)$的解是$x \equiv \pm n^{\frac{p+1}{4}} (\bmod p)$。

5. 若$x^2 \equiv n (\bmod p^\alpha)$有解$x \equiv x_0 (\bmod p^\alpha)$，则$x_0^2 \equiv n (\bmod p)$，故 $\left(\dfrac{n}{p}\right) = 1$，反之，

若 $(\frac{n}{p}) = 1$，则$x^2 \equiv n \pmod p$有解$x \equiv x_0 \pmod p$，因$p \nmid 2x_0$，故此解可导出$x^2 \equiv n$ (mod p^{α})的一个解$x \equiv x_{\alpha} \pmod {p^{\alpha}}$，即$x^2 \equiv n \pmod {p^{\alpha}}$有解。

6. 设$x_1, x_2, \cdots, x_k$为模p的所有二次剩余，则

$$x_1x_2\cdots x_k \equiv 1^2 2^2 \cdots (\frac{p-1}{2})^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \equiv (-1)^{\frac{p+1}{2}} \pmod p。$$

第五章 习 题 六

1. （i） 因 $(\frac{1742}{769}) = (\frac{204}{769}) = (\frac{4}{769})(\frac{3}{769})(\frac{17}{769}) = (\frac{1}{3})(\frac{4}{17}) = 1$，原同余方程有解；（ii） $(\frac{1503}{1013}) = (\frac{490}{1013}) = (\frac{2}{1013})(\frac{5}{1013})(\frac{49}{1013}) = -(\frac{1013}{5}) = -(\frac{3}{5}) = 1$，原同余方程有解。

2. 由 $(\frac{11}{p}) = 1$推出$(-1)^{\frac{p-1}{2}}(\frac{p}{11}) = 1$，由此得

$$\begin{cases} (-1)^{\frac{p-1}{2}} = 1 \\ (\frac{p}{11}) = 1 \end{cases} \text{或} \begin{cases} (-1)^{\frac{p-1}{2}} = -1 \\ (\frac{p}{11}) = -1 \end{cases},$$

即

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 1,3,4,5,9 \pmod{11} \end{cases} \text{或} \begin{cases} p \equiv -1 \pmod 4 \\ p \equiv -1,-3,-4,-5,-9 \pmod{11} \end{cases},$$

解之得 $p \equiv \pm 1$，± 5，± 7，± 9，$\pm 19 \pmod{44}$。

3. 由 $-2 \in QR(p)$，$-3 \in QR(p)$推得 $(\frac{-2}{p}) = 1$，$(\frac{-3}{p}) = 1$，即

$$\begin{cases} (\frac{-1}{p}) = 1 \\ (\frac{2}{p}) = 1 \\ (\frac{3}{p}) = 1 \end{cases}，\text{或} \begin{cases} (\frac{-1}{p}) = -1 \\ (\frac{2}{p}) = -1 \\ (\frac{3}{p}) = -1 \end{cases}。$$

解之得 $p \equiv 1$，或 $11 \pmod{24}$。

4. 设奇素数$p \mid x^2 - 3y^2$，即$x^2 \equiv 3y^2 \pmod p$，由$(x, y) = 1$ 易证$(3y^2, p) = 1$，于

是 $(\frac{3y^2}{p})=(\frac{3}{p})=1$，由此得$p$的一般形式为 $12k\pm1$ 型。

5. 若 $8k+5$ 型的素数只有有限个，记为$p_1, p_2, \cdots, p_k$，作$A=(2\,p_1p_2\cdots p_k)^2+1$，显然$A>1$，$A$是奇数，设奇素数$p\,|\,A$，即$(2\,p_1p_2\cdots p_k)^2\equiv-1\pmod p$，$(\frac{-1}{p})=1$，由此得$p$的一般形式为 $8k+1$ 或 $8k+5$ 型，由$A\equiv5\pmod 8$知A的素因数p中至少有一个是 $8k+5$ 型的，对这个p，有$p=p_i$（$1\le i\le k$），由$p\,|\,A$，$p\,|\,p_1p_2\cdots p_k$推出$p\,|\,1$，矛盾。

6. 当$p=4k+1$ 时，同余方程$x^2\equiv-1\pmod p$有解$x\equiv n\pmod p$，即$p\,|\,n^2+1$，从而$p\,|\,(n^2+1)(n^2+2)(n^2-2)$； 当$p=8k+3$ 时，同余方程$x^2\equiv-2\pmod p$有解$x\equiv n\pmod p$，即$p\,|\,n^2+2$，从而$p\,|\,(n^2+1)(n^2+2)(n^2-2)$；当$p=8k+7$ 时，同余方程$n^2\equiv2\pmod p$有解$x\equiv n\pmod p$，即$p\,|\,n^2-2$，从而$p\,|\,(n^2+1)(n^2+2)(n^2-2)$。

第五章　习 题 七

1. (ii) 显然； (iii) 设$m=p_1p_2\cdots p_k$，则

$$(\frac{a_1a_2\cdots a_t}{m})=(\frac{a_1a_2\cdots a_t}{p_1})(\frac{a_1a_2\cdots a_t}{p_2})\cdots(\frac{a_1a_2\cdots a_t}{p_k})$$
$$=(\frac{a_1}{p_1})\cdots(\frac{a_t}{p_1})(\frac{a_1}{p_2})\cdots(\frac{a_t}{p_2})\cdots(\frac{a_1}{p_k})\cdots(\frac{a_t}{p_k})=(\frac{a_1}{m})(\frac{a_2}{m})\cdots(\frac{a_t}{m})。$$

(iv) $(\frac{a^2b}{m})=(\frac{a}{m})(\frac{a}{m})(\frac{b}{m})=(\frac{b}{m})$。

2. 因 $(\frac{374}{3019})=(\frac{2}{3019})(\frac{187}{3019})=(-1)(-1)(\frac{27}{187})=(\frac{3}{187})=-(\frac{1}{3})=-1$，原同余方程无解。

3. 设$d=\pm2^{\alpha}d_1$，d_1为正奇数，$(\frac{d}{p})=(\frac{\pm1}{p})(\frac{2}{p})^{\alpha}(\frac{d_1}{p})=(\frac{2}{p})^{\alpha}(\frac{d_1}{p})$，当$\alpha>0$ 时，$p=8n+1$ 型，$(\frac{2}{p})=1$，当$d_1>1$ 时，$(\frac{d_1}{p})=(\frac{p}{d_1})=(\frac{1}{d_1})=1$，所以 $(\frac{d}{p})=(\frac{2}{p})^{\alpha}(\frac{d_1}{p})=1$。

4. 由 $p=q+4a$ 知 p，q 同为 $4k+1$ 或同为 $4k+3$，当 p，q 同为 $4k+1$ 时，有 $(\frac{a}{p})=(\frac{-4a}{p})=(\frac{p-4a}{p})=(\frac{q}{p})=(\frac{p}{q})=(\frac{q+4a}{q})=(\frac{4a}{q})=(\frac{a}{q})$，当 p，q 同为 $4k+$

3 时，有 $(\frac{a}{p}) = -(\frac{-4a}{p}) = -(\frac{p-4a}{p}) = -(\frac{q}{p}) = (\frac{p}{q}) = (\frac{q+4a}{q}) = (\frac{4a}{q}) = (\frac{a}{q})$。

5. 当$a \equiv 0 \pmod 4$时，则 $2a+b \equiv b \pmod 8$，令$a = 2^{\alpha}a_1$，a_1为奇数，于是有 $(\frac{a}{2a+b}) = (\frac{2}{2a+b})^{\alpha}(\frac{a_1}{2a+b}) = (\frac{2}{b})^{\alpha}(\frac{a_1}{2a+b})$，若$a_1 = 1$，$(\frac{a_1}{2a+b}) = (\frac{a_1}{b})$，若$a_1 > 1$，$(\frac{a_1}{2a+b}) = (-1)^{\frac{a_1-1}{2}\cdot\frac{b-1}{2}}(\frac{b}{a_1}) = (\frac{a_1}{b})$，故得$(\frac{a}{2a+b}) = (\frac{2}{b})^{\alpha}(\frac{a_1}{b}) = (\frac{a}{b})$；当$a \equiv 1 \pmod 4$时，若$a = 1$，$(\frac{a}{2a+b}) = (\frac{a}{b})$，若$a > 1$，$(\frac{a}{2a+b}) = (\frac{b}{a}) = (\frac{a}{b})$，故有 $(\frac{a}{2a+b}) = (\frac{a}{b})$；类似地，当$a \equiv 2 \pmod 4$时，令$a = 2a_1$，$a_1$为奇数，于是 $(\frac{a}{2a+b}) = (\frac{2}{2a+b})(\frac{a_1}{2a+b}) = -(\frac{2}{b})(\frac{a_1}{2a+b}) = -(\frac{2}{b})(\frac{a_1}{b}) = -(\frac{a}{b})$；当$a \equiv 3 \pmod 4$时，$(\frac{a}{2a+b}) = (-1)^{\frac{2a+b-1}{2}}(\frac{2a+b}{a}) = (-1)^{\frac{2a+b-1}{2}}(\frac{b}{a}) = (-1)^{a}(\frac{a}{b}) = -(\frac{a}{b})$。

6. 若a为奇数，有 $(\frac{a}{4ac-b}) = (-1)^{\frac{a-1}{2}\cdot\frac{4ac-b-1}{2}}(\frac{-b}{a}) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}(\frac{b}{a}) = (\frac{a}{b})$，若$a$为偶数，于是 $4ac-b$与b同为 $8k \pm 1$ 或同为 $8k \pm 3$，即 $(\frac{2}{4ac-b}) = (\frac{2}{b})$，设$a = 2^{\alpha}a_1$，$a_1$ 为 奇 数 ， 有 $(\frac{a}{4ac-b}) = (\frac{2}{4ac-b})^{\alpha}(\frac{a_1}{4ac-b}) = (\frac{2}{b})^{\alpha}(\frac{a_1}{4ac-b}) = (\frac{2}{b})^{\alpha}(-1)^{\frac{a_1-1}{2}\cdot\frac{4ac-b-1}{2}}(\frac{-b}{a_1}) = (\frac{2}{b})^{\alpha}(-1)^{\frac{a_1-1}{2}\cdot\frac{b-1}{2}}(\frac{b}{a_1}) = (\frac{2}{b})^{\alpha}(\frac{a_1}{b}) = (\frac{a}{b})$。

第六章　习 题 一

1. 设a，b，c是不定方程$x^2 + y^2 = z^2$的正整数解，则易知$x = ac^{n-1}$，$y = bc^{n-1}$，$z = c^2$是不定方程$x^2 + y^2 = z^n$的正整数解。

2. 对于每一个i，$0 < i < p$，令i'满足$i'i \equiv 1 \pmod p$，$0 < i' < p$，于是 $\sum\limits_{i=0}^{p-1}(\frac{i(i+k)}{p}) = \sum\limits_{i=1}^{p-1}(\frac{i(i+k)}{p}) = \sum\limits_{i=1}^{p-1}(\frac{i'^2 i(i+k)}{p}) = \sum\limits_{i'=0}^{p-1}(\frac{1+ik}{p}) - 1 = -1$。

3. 由 $p \equiv 1 \pmod 4$知 $(\frac{-1}{p}) = 1$，于是 $S(k) = \sum\limits_{i=0}^{p-1}(\frac{i(i^2+k)}{p}) = \sum\limits_{i=1}^{p-1}(\frac{i(i^2+k)}{p}) =$

$\sum\limits_{i=1}^{\frac{p-1}{2}}(\frac{i(i^2+k)}{p})+\sum\limits_{i=1}^{\frac{p-1}{2}}(\frac{(p-i)[(p-i)^2+k]}{p})=2\sum\limits_{i=1}^{\frac{p-1}{2}}(\frac{i(i^2+k)}{p})$，故 $2\mid S(k)$；又对于任何整数 t，若 $t\equiv 0 \pmod p$，则 $S(kt^2)=\sum\limits_{i=0}^{p-2}(\frac{i}{p})=(\frac{t}{p})S(k)=0$，若 $t\not\equiv 0 \pmod p$，则

$$S(kt^2)=\sum_{i=0}^{p-1}(\frac{i(i^2+kt^2)}{p})=\sum_{i=0}^{p-1}(\frac{it[(it)^2+kt^2]}{p})=(\frac{t^3}{p})\sum_{i=0}^{p-1}(\frac{i(i^2+k)}{p})=(\frac{t}{p})S(k)。$$

4. 显然 $m\cdot 1^2, m\cdot 2^2, \cdots, m\cdot(\frac{p-1}{2})^2, n\cdot 1^2, n\cdot 2^2, \cdots, n\cdot(\frac{p-1}{2})^2$ 中共有 $p-1$ 个数；又易知 $m\cdot i_1^2\not\equiv m\cdot i_2^2 \pmod p$，$n\cdot j_1^2\not\equiv n\cdot j_2^2 \pmod p$，若 $m\cdot i^2\equiv n\cdot j^2 \pmod p$，则可推得 $(\frac{mn}{p})=1$， 这是一个矛盾；最后易知 $(m\cdot i^2, p)=(n\cdot j^2, p)=1$。故给定数组构成模 p 的一个简系。

5. 由题 2 和题 3 知 $\frac{p-1}{2}S^2(m)\frac{p-1}{2}S^2(n)=\sum\limits_{t=1}^{\frac{p-1}{2}}S^2(mt^2)+\sum\limits_{t=1}^{\frac{p-1}{2}}S^2(nt^2)=\sum\limits_{k=1}^{p-1}S^2(k)$

$$=\sum_{k=1}^{p-1}\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}(\frac{ij(i^2+k)(j^2+k)}{p})==\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}\sum_{k=1}^{p-1}(\frac{ij(i^2+k)(j^2+k)}{p})。$$

当 $j^2\not\equiv i^2 \pmod p$，令 $j^2+k=z$，则 $(i^2+k)(j^2+k)=z[z+(i^2-j^2)]$，$(i^2-j^2, p)=1$，有

$$\sum_{k=1}^{p-1}(\frac{ij(i^2+k)(j^2+k)}{p})=(\frac{ij}{p})[\sum_{k=0}^{p-1}(\frac{(i^2+k)(j^2+k)}{p})-1]$$

$$=(\frac{ij}{p})[\sum_{k=0}^{p-1}(\frac{z(z+(i^2-j^2))}{p})-1]=-2(\frac{ij}{p})；$$

当 $j^2\equiv i^2 \pmod p$，有

$$\sum_{k=1}^{p-1}(\frac{ij(i^2+k)(j^2+k)}{p})=(\frac{ij}{p})\sum_{k=0}^{p-1}(\frac{i^2+k}{p})^2=(p-2)(\frac{ij}{p})。$$

故

$$\frac{p-1}{2}S^2(m)+\frac{p-1}{2}S^2(n)=\sum_{i=1}^{p-1}\sum_{\substack{j=1\\ i^2\not\equiv j^2\ (mon p)}}^{p-1}[-2(\frac{ij}{p})]+\sum_{i=1}^{p-1}\sum_{\substack{j=1\\ i^2\equiv j^2\ (mon p)}}^{p-1}(p-2)(\frac{ij}{p})$$

$$=-2\sum_{i=1}^{p-1}\sum_{j=1}^{p-1}(\frac{ij}{p})+p\sum_{i=1}^{p-1}\sum_{\substack{j=1\\ i^2\equiv j^2\ (mon p)}}^{p-1}(\frac{ij}{p})=-2\sum_{i=1}^{p-1}(\frac{i}{p})\sum_{j=1}^{p-1}(\frac{j}{p})+\sum_{i=1}^{p-1}\sum_{\substack{j=1\\ j=i}}^{p-1}(\frac{ij}{p})+\sum_{i=1}^{p-1}\sum_{\substack{j=1\\ j=p-i}}^{p-1}(\frac{ij}{p})$$

$$=0+2p(p-1)=2p(p-1)。$$

由此得 $p=(\frac{1}{2}S(m))^2+(\frac{1}{2}S(n))^2$。

6. 取$m = 1$，$n = 2$，则$S(m) = 6$，$S(n) = -4$，由此得 $13 = 3^2 + 2^2$。

第六章　习 题 二

1. 设$x^2 + y^2 + z^2 = 4n^2$成立，若x，y都是奇数，则$x^2 + y^2 + z^2 \equiv 2$ 或 $3 \pmod 4$，此不可能；若x，y一奇一偶，则$x^2 + y^2 + z^2 \equiv 1$ 或 $2 \pmod 4$，此也不可能；故只能x，y都是偶数，此时z也是偶数，与$(x, y, z) = 1$ 矛盾。

2. 设$x^2 + y^2 + z^2 = 2^k$，x，y，$z > 0$，若$k \geq 2$，可得x，y，z都是偶数，于是令$x = 2x_1$，$y = 2y_1$，$z = 2z_1$，代入得$x_1^2 + y_1^2 + z_1^2 = 2^{k-2}$，若$k - 2 \geq 2$，类似于上面的的推理可得$x_1$，$y_1$，$z_1$都是偶数，于是令$x_1 = 2x_2$，$y_1 = 2y_2$，$z_1 = 2z_2$，代入得$x_2^2 + y_2^2 + z_2^2 = 2^{k-4}$，$\cdots$，最后推出，存在$a$，$b$，$c > 0$，$a^2 + b^2 + c^2 = 2^0$或 2^1，显然这是不可能的。

3. 由$n^3 - n \equiv 0 \pmod 6$得$n^3 - n = 6x$，于是$n = n^3 - (x + 1)^3 - (x - 1)^3 + x^3 + x^3$。

4. 若 $16k + 15 = x_1^4 + x_2^4 + \cdots + x_{14}^4$，由$x^4 \equiv 0$ 或 $1 \pmod{16}$知上式不可能成立。

5. 若 $16^k\cdot 31 = x_1^4 + x_2^4 + \cdots + x_{15}^4$，由$x^4 \equiv 0$ 或 $1 \pmod{16}$知$x_1, x_2, \cdots, x_{15}$都是偶数，于是令$x_1 = 2x_{1,1}$，$x_2 = 2x_{2,1}$，$\cdots$，$x_{15} = 2x_{15,1}$，代入得

$$16^{k-1}\cdot 31 = x_{1,1}^4 + x_{2,1}^4 + \cdots + x_{15,1}^4,$$

反复以上推理，最后可得 $31 = x_{1,k}^4 + x_{2,k}^4 + \cdots + x_{15,k}^4$，但易知 31 不能表示为 15 个四次方数的和，故 $16^k\cdot 31$ 不能表示为 15 个四次方数的和。

第七章　习 题 一

1. 经计算得$\delta_{11}(1) = 1$，$\delta_{11}(2) = 10$，$\delta_{11}(3) = 5$，$\delta_{11}(4) = 5$，$\delta_{11}(5) = 5$，$\delta_{11}(6) = 10$，$\delta_{11}(7) = 10$，$\delta_{11}(8) = 10$，$\delta_{11}(9) = 5$，$\delta_{11}(10) = 2$，列表得

a	1	2	3	4	5	6	7	8	9	10
$\delta_{11}(a)$	1	10	5	5	5	10	10	10	5	2

2. $x \equiv 3$，$5 \pmod{14}$是模 14 的全部原根。

3. 因g^1，g^2，$\cdots$，$g^{\varphi(m)}$构成模m的简化剩余系，由$d = \delta_m(g^\lambda) = \dfrac{\varphi(m)}{(\lambda,\varphi(m))}$得

$(\lambda,\varphi(m)) = \dfrac{\varphi(m)}{d}$，令$\lambda = \dfrac{\varphi(m)}{d}t$，则

$$(\lambda,\varphi(m)) = \frac{\varphi(m)}{d}\text{，}\ 1 \le \lambda \le \varphi(m) \Longleftrightarrow (t, d) = 1\text{，}\ 1 \le t \le d\text{，}$$

故恰有$\varphi(d)$个t，使得$(t, d) = 1$，从而知故恰有$\varphi(d)$个λ，使得$\delta_m(g^\lambda) = d$。特别地，取$d = \varphi(m)$知模m的简化剩余系中恰有$\varphi(\varphi(m))$个原根。

4. （i） 因$g^1, g^2, \cdots, g^{\varphi(m)}$为模$m$的简化剩余系，设同余方程$x^2 \equiv 1 \pmod m$的解为$x \equiv g^r \pmod m$，即$(g^r)^2 = g^{2r} \equiv 1 \pmod m$，由此得 $2r \equiv 0 \pmod{\varphi(m)}$，$\varphi(m) \mid 2r$，又由$m \ge 3$ 知$\varphi(m)$是偶数，得 $\frac{\varphi(m)}{2} \mid r$，$r = \frac{\varphi(m)}{2}$ 或$\varphi(m)$。另一方面，同余方程$x^2 \equiv 1 \pmod m$至少有解$x \equiv 1$，$-1 \pmod m$，由$g^{\varphi(m)} \equiv 1 \pmod m$推出 $g^{\frac{\varphi(m)}{2}} \equiv -1 \pmod m$。

（ii） 因$g^1, g^2, \cdots, g^{\varphi(m)}$也为模$m$的简化剩余系，故

$$x_1x_2\cdots x_{\varphi(m)} \equiv g^1g^2\cdots g^{\varphi(m)} \equiv g^{\frac{\varphi(m)(\varphi(m)+1)}{2}} \equiv g^{\frac{\varphi(m)}{2}\varphi(m)}g^{\frac{\varphi(m)}{2}} \equiv g^{\frac{\varphi(m)}{2}} \equiv -1 \pmod m\text{。}$$

5. 在模p的简化剩余系中有 $\frac{p-1}{2} = 2^{n-1}$个二次非剩余，在模p的简化剩余系中有$\varphi(\varphi(p)) = \varphi(2^n) = 2^{n-1}$个原根，又设$g$是模$p$原根，则 $g^{\frac{p-1}{2}} \equiv -1 \pmod m$，即$g$是模$p$的二次非剩余。

6. （i） 由 $2^p \equiv 1 \pmod q$知$\delta_q(2) \mid p$，于是$\delta_q(2) = 1$ 或p，但易知$\delta_q(2) \ne 1$，故$\delta_q(2) = p$，再由$\delta_q(2) \mid \varphi(q) = q - 1$ 知$q - 1 = pt$，其中t必为偶数，故q为 $2pk + 1$ 型；

（ii） 由 $2^{2^n} \equiv -1 \pmod q$，即$2^{2^{n+1}} \equiv 1 \pmod q$ 知$\delta_q(2) \mid 2^{n+1}$，于是$\delta_q(2) = 2^r$，$0 \le r \le n + 1$，又由 $2^{2^n} \equiv -1 \pmod q$知$\delta_q(2) \ne 2^r$，$0 \le r \le n$，故$\delta_q(2) = 2^{n+1}$，再由$\delta_q(2) \mid \varphi(q) = q - 1$ 知$q - 1 = 2^{n+1}k$，故q为 $2pk + 1$ 型。

第七章 习 题 二

1. 因$\varphi(29) = 28 = 2^2\cdot 7$，由

$$2^{\frac{\varphi(29)}{2}} = 2^{14} \not\equiv 1 \pmod{29}\text{，}\quad 2^{\frac{\varphi(29)}{7}} = 2^4 \not\equiv 1 \pmod{29}$$

知 2 是模 29 的最小正原根。

2. 由 2 是模 29 的原根及 $2^{29-1} = 2^{28} = 2^{28} \not\equiv 1 \pmod{29^2}$知 2 是模 29^3的原根；由 2 是模 29^3的原根及 2 是偶数知 $2 + 29^3$是模 $2\cdot 29^3$的原根。

3. 易得 3 是模 17 的原根，3^i（$i = 0, 1, 2, \cdots, 15$）构成模 17 的简化剩余系，列表为

i	0	1	2	3	4	5	6	7

$3^i \pmod{17}$	1	3	9	10	13	5	15	11
i	8	9	10	11	12	13	14	15
$3^i \pmod{17}$	16	14	8	7	4	12	2	6

由上表知 $3^8 \equiv 16 \pmod{17}$，设$x \equiv 5^y \pmod{17}$，则 $12y \equiv 8 \pmod{16}$，由此解得$y_1 \equiv 2$，$y_2 \equiv 6$，$y_3 \equiv 10$，$y_4 \equiv 14 \pmod{16}$，查上表得$x_1 \equiv 9$，$x_2 \equiv 15$，$x_3 \equiv 8$，$x_4 \equiv 2 \pmod{17}$。

4. 由$\delta_q(2) \mid \varphi(q) = 4p$知$\delta_q(2) = 1$，2，4，$p$，$2p$或 $4p$，若 $2^4 \equiv 1 \pmod q$，则$q \mid 2^4 - 1 = 15 = 3\cdot5$，即$q = 3$ 或 5，这是不可能的，故$\delta_q(2) \ne 1$，$\delta_q(2) \ne 2$，$\delta_q(2) \ne 4$，又 q 是 $8k + 5$ 型的数，2 是q的二次非剩余，即 $2^{\frac{q-1}{2}} = 2^{2p} \not\equiv 1 \pmod q$，故$\delta_q(2) \ne p$，$\delta_q(2) \ne 2p$，所以$\delta_q(2) = 4p = \varphi(q)$，2 是模$q$的一个原根。

5. 存在一个λ，$(\lambda,\varphi(m)) = 1$，使得$g_2 \equiv g_1^{\lambda} \pmod m$，于是$g_1g_2 \equiv g_1^{\lambda+1} \pmod m$，又由$m \ge 3$ 知$\varphi(m)$是偶数，λ是奇数，$\lambda + 1$ 是偶数，$(\lambda + 1,\varphi(m)) \ne 1$，故$g = g_1g_2$不是模$m$的原根。

6. 当$p - 1 \mid n$时，则 $1^n + 2^n + \cdots + (p - 1)^n \equiv p - 1 \not\equiv 0 \pmod p$，当$p - 1 \nmid n$时，设$g$是$p$的一个原根，则 $1^n + 2^n + \cdots + (p - 1)^n \equiv (1\cdot g)^n + (2\cdot g)^n + \cdots + [(p - 1)g]^n \equiv [1^n + 2^n + \cdots + (p - 1)^n]g^n \pmod p$，得$[1^n + 2^n + \cdots + (p - 1)^n](1 - g^n) \equiv 0 \pmod p$，由$(1 - g^n) \not\equiv 0 \pmod p$知 $1^n + 2^n + \cdots + (p - 1)^n \equiv 0 \pmod p$。

第八章　习 题 一

1. 考虑函数

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(x-(\alpha_i-\beta_j))，\quad \prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i\beta_j) \text{ 与 } \prod_{i=1}^{n}\prod_{j=1}^{m}(x-\frac{\alpha_i}{\beta_j})。$$

2. 设α是代数数，则$b_n\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$，其中$b_i$都是整数，$b_n \ne 0$，两边乘以$b_n^{\,n-1}$得$(b_n\alpha)^n + b_{n-1}(b_n\alpha)^{n-1} + \cdots + b_n^{\,n-2}b_1(b_n\alpha) + b_n^{\,n-1}b_0 = 0$，由此知$b_n\alpha$是代数整数。

3. 有理数 r 是方程 $x - r = 0$，若 r 是代数整数，则方程的系数 r 是整数，反之，若 r 是整数，则由定义知 r 是代数整数。

第八章　习 题 二

1. （ⅰ） 令 $\alpha=\frac{1}{2}+\frac{1}{2^{2!}}++\cdots+\frac{1}{2^{n!}}+\cdots=\sum\limits_{n=1}^{\infty}a^{-r_n}$ ，这里$a=2$，$r_n=n!$，由 $\lim\limits_{n\to\infty}\frac{r_{n+1}}{r_n}=\lim\limits_{n\to\infty}\frac{(n+1)!}{n!}=\infty$知$\alpha=\sum\limits_{n=1}^{\infty}a^{-r_n}$ 是超越数。 （ⅱ） 类似于(ⅰ)即可得证。

2. 令 $\alpha=\cfrac{1}{10+\cfrac{1}{10^{2!}+\cdots+\cfrac{1}{10^{n!}+\cdots}}}=\langle 0,a_1,a_2,\cdots,a_n\cdots\rangle$，$\frac{p_n}{q_n}$ 是α的第n个渐近分数，则$|\alpha-\frac{p_n}{q_n}|<\frac{1}{q_nq_{n+1}}<\frac{1}{a_{n+1}q_n^2}\le\frac{1}{a_{n+1}}$，这里$a_{n+1}=10^{(n+1)!}$，由$q_1<a_1+1$ 及 $\frac{q_{n+1}}{q_n}=a_{n+1}+\frac{q_{n-1}}{q_n}<a_{n+1}+1$ 可得$q_n<(a_1+1)(a_2+1)\cdots(a_n+1)<2\cdot10^{2\cdot n!}=a_n^2$，因此 $|\alpha-\frac{p_n}{q_n}|<\frac{1}{a_{n+1}}=\frac{1}{a_n^{n+1}}<\frac{1}{a_n^n}<\frac{1}{q_n^{\frac{1}{2}n}}$， 由Liouville定理知$\alpha$不是代数数，故$\alpha$必是超越数。

3. 若$\xi+\alpha=\beta$是一个代数数，则$\xi=\beta-\alpha$也是一个代数数，此与ξ是一个超越数矛盾。其它情形可类似地证明。

第八章　习 题 三

1. （ⅰ） 对于每一个k，$k=1, 2, \cdots, d$，设$g(x)=(x-k)^p$，$f(x)=g(x)h(x)$，则有 $f^{(i)}(x)=\sum\limits_{j=0}^{i}C_i^j\,g^{(j)}(x)h^{(i-j)}(x)$，$i=0, 1, \cdots, p-1$，显然$g^{(j)}(k)=0$，$0\le j\le p-1$，故$f^{(i)}(k)=0$，$i=0, 1, \cdots, p-1$； (ii) 由第一章第五节的定理可证； (iii) 设$g(x)=x^{p-1}$，$h(x)=(x-1)^p\cdots(x-d)^p$，则有$f^{(p-1)}(x)=\frac{1}{(p-1)!}\sum\limits_{j=0}^{p-1}C_{p-1}^j\,g^{(j)}(x)h^{(p-1-j)}(x)$，显然$g^{(j)}(0)=0$，$0\le j\le p-2$，故$f^{(p-1)}(0)=\frac{1}{(p-1)!}g^{(p-1)}(0)h^{(0)}(0)=(-1)^p\cdots(-d)^p=(-1)^{dp}(d!)^p$。

2. 由 $f(x)=\frac{1}{n!}x^n(a-bx)^n$ 易知：当 $0\le i\le n-1$ 时，$f^{(i)}(\frac{a}{b})=f^{(i)}(0)=0$；当$n\le i\le 2n$时，$f^{(i)}(\frac{a}{b})$ 和$f^{(i)}(0)$都是整数，于是由

$$F(x)=f(x)-f''(x)+f^{(4)}(x)-\cdots+(-1)^nf^{(2n)}(x)$$

可知 $F(\frac{a}{b})+F(0)$是整数。

第九章 习 题 一

1. $N = 1947$，$c = 19$，$y = 47$，$m = 12$，$k = 14$，$W(1947, 12, 14) \equiv 14 - 38 + 47 + [\frac{47}{4}] + [\frac{19}{4}] + [2.6\cdot 12 - 0.2] \equiv 6 \pmod 7$，即 1948 年 2 月 14 日是星期六？

2. $N = 1999$，$c = 19$，$y = 66$，$m = 8$，$k = 1$，$W(1999 ,10, 1) \equiv 1 - 38 + 99 + [\frac{99}{4}] + [\frac{19}{4}] + [2.6\cdot 8 - 0.2] \equiv 5 \pmod 7$，即 1999 年 10 月 1 日是星期五。

第九章 习 题 二

1. 十个球队进行循环赛的程序表为

	1	2	3	4	5	6	7	8	9	10
1	9	8	7	6	10	4	3	2	1	5
2	10	9	8	7	6	5	4	3	2	1
3	2	1	9	8	7	10	5	4	3	6
4	3	10	1	9	8	7	6	5	4	2
5	4	3	2	1	9	8	10	6	5	7
6	5	4	10	2	1	9	8	7	6	3
7	6	5	4	3	2	1	9	10	7	8
8	7	6	5	10	3	2	1	9	8	4
9	8	7	6	5	4	3	2	1	10	9

2. 九个球队进行循环赛的程序表为：

	1	2	3	4	5	6	7	8	9
1	9	8	7	6		4	3	2	1
2		9	8	7	6	5	4	3	2
3	2	1	9	8	7		5	4	3
4	3		1	9	8	7	6	5	4

5	4	3	2	1	9	8		6	5
6	5	4		2	1	9	8	7	6
7	6	5	4	3	2	1	9		7
8	7	6	5		3	2	1	9	8
9	8	7	6	5	4	3	2	1	

第九章　习 题 三

1.　"ICOMETODAY"的密文是"LFRPHWRGDB"。

2.　由e $\Longrightarrow$ h，g $\Longrightarrow$ p得 $7 \equiv 4a' + b' \pmod{26}$，$15 \equiv 6a' + b' \pmod{26}$，解得 $a' \equiv 4$，$17 \pmod{26}$，因$(4, 26) \neq 1$，故$a' \equiv 17 \pmod{26}$，由此得$b' \equiv 17 \pmod{26}$，所以密解公式为$P \equiv 17a' + 17 \pmod{26}$，列表如下

E	a	b	c	d	e	f	g	h	i	j	k	l	m
P	r	i	z	q	h	y	p	g	x	o	f	w	n
E	N	o	p	q	r	s	t	u	v	w	x	y	z
P	e	v	m	d	u	l	c	t	k	b	s	j	a

由上表，密文"IRQXREFRXLGXEPQVEP"经破译得到明文"BADIANKAISHIXINGDONG"（八点开始行动）。

第九章　习 题 四

1.　$E \equiv 100^9 \equiv 262 \pmod{943}$，即$E = 262$，又 $943 = 23{\cdot}41$，$p = 23$，$q = 41$，$\varphi(n) = 22{\cdot}40 = 880$，由 $9d \equiv 1 \pmod{880}$解得$d = 489$，于是

$$
\begin{aligned}
P &\equiv 262^{489} \equiv (748)^{244}{\cdot}262 \equiv (305)^{122}{\cdot}262 \equiv (611)^{61}{\cdot}262 \equiv (836)^{30}{\cdot}715 \\
&\equiv (133)^{15}{\cdot}715 \equiv (715)^{7}{\cdot}133{\cdot}715 \equiv (715)^{8}{\cdot}133 \equiv (119)^{4}{\cdot}133 \\
&\equiv (16)^{2}{\cdot}133 \equiv 256{\cdot}133 \equiv 100 \pmod{943}。
\end{aligned}
$$

2.　因A知$d_A = 7$，$e_B = 5$，计算$E_1 \equiv 3^7 \equiv 9 \pmod{33}$，$E \equiv 9^5 \equiv 4 \pmod{35}$，于是$A$可将$E = 04$ 传送给B，因B知$d_B = 5$，$e_A = 3$，计算$E_1 \equiv 4^5 \equiv 9 \pmod{35}$，$M \equiv 9^3 \equiv 3 \pmod{33}$，于是$B$认证了$A$的签证$M = 03$。

第九章　习 题 五

1.　取$m_1 = 5$，$m_2 = 7$，$m_3 = 11$，$m_4 = 17$，则$M = 6545$，$M_1 = 1309$，$M_2 = 935$，$M_3 = 595$，$M_4 = 385$，$M_1' = 4$，　$M_2' = 2$，　$M_3' = 1$，　$M_4' = 14$。对集合$\{4, 6, 10, 13\}$进行加密，得到$E \equiv 4M_1M_1' + 6M_2M_2' + 10M_3M_3' + 13M_4M_4' \equiv 3464 \pmod{46189}$，即$E = 3464$。若要求出$F_3$，则由$F_3 \equiv 3464 = 10 \pmod{11}$。

2.　$M = 3$，$p = 5$，$m_1 = 8$，$m_2 = 9$，$m_3 = 11$，因 $8\cdot9 > 5\cdot11$，取$t = 10 < \frac{8\cdot9}{5} - 1$，$E_1 \equiv 3 + 10\cdot5 \equiv 5 \pmod 8$，$E_2 \equiv 3 + 10\cdot5 \equiv 8 \pmod 9$，$E_3 \equiv 3 + 10\cdot5 \equiv 9 \pmod{11}$，于是分配给三方的数据分别为$E_1 = 5$，$E_2 = 8$，$E_3 = 9$。由$E_1$，$E_2$，$E_3$中的任意两个都可以确定出$M$，例如，已知$E_2 = 8$，$E_3 = 9$，则由$x \equiv 8 \pmod 9$，$x \equiv 9 \pmod{11}$可得解$x \equiv 53 \pmod{9\cdot11}$，从而$M = 53 - 10\cdot5 = 3$。

第九章　习 题 六

1.　因$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$超增背包向量，容易得到不定方程

$$5p_1 + 17p_2 + 43p_3 + 71p_4 + 144p_5 + 293p_6 + 626p_7 + 1280p_8 = 1999$$

的 0–1 解为$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8) = (1, 1, 0, 1, 0, 0, 1, 1)$，故密文$E$对应的明文$P = (11010011)_2 = 211$。

2.　计算$b_1 \equiv 77\cdot2 \equiv 36 \pmod{118}$，取$b_1 = 36$，$b_2 \equiv 77\cdot3 \equiv 113 \pmod{118}$，取$b_2 = 113$，$b_3 \equiv 77\cdot7 \equiv 67 \pmod{118}$，取$b_3 = 67$，$b_4 \equiv 77\cdot13 \equiv 57 \pmod{118}$，取$b_4 = 57$，$b_5 \equiv 77\cdot29 \equiv 109 \pmod{118}$，取$b_5 = 109$，$b_6 \equiv 77\cdot59 \equiv 59 \pmod{118}$，取$b_6 = 59$，于是对外公开的加密向量是$(36, 113, 67, 57, 109)$，又$P = 51 = (110011)_2$，故$P$对应的密文为$E = 36\cdot1 + 113\cdot1 + 67\cdot0 + 57\cdot0 + 109\cdot1 + 59\cdot1 = 317$，若要从$E = 317$ 得到明文P，则计算 $23\cdot317 \equiv 93 \pmod{118}$，解不定方程

$$2p_1 + 3p_2 + 7p_3 + 13p_4 + 29p_5 + 59p_6 = 93$$

的 0–1 解得$(p_1, p_2, p_3, p_4, p_5, p_6) = (1, 1, 0, 0, 1, 1)$，故$P = (110011)_2 = 51$。

1　证明：$a_1,a_2\cdots,a_n$ 都是 m 的倍数。

$\therefore$ 存在 n 个整数 $p_1,p_2,\cdots p_n$ 使

$a_1=p_1m_1,a_2=p_2m_2,\cdots,a_n=p_nm_n$

又 $q_1,q_2,\cdots,q_n$ 是任意 n 个整数

$\therefore q_1a_1+q_2a_2+\cdots+q_na_n=(p_1q_1+q_2p_2+\cdots+q_np_n)m$

即 $q_1a_1+q_2a_2+\cdots+q_na_n$ 是 m 的整数

2　证：　$\because n(n+1)(2n+1)=n(n+1)(n+2+n-1)$

$=n(n+1)(n+2)+(n-1)n(n+1)$

$6/n(n+1)(n+2),6/(n-1)n(n+1)$

$\therefore 6/n(n+1)(n+2)+(n-1)n(n+1)$

从而可知　$6/n(n+1)(2n+1)$

3　证：　$\because a,b$ 不全为 0

$\therefore$ 在整数集合 $S=\{ax+by\mid x,y\in Z\}$ 中存在正整数，因而

有形如 $ax+by$ 的最小整数 ax_0+by_0

$\forall x,y\in Z$，由带余除法有 $ax+by=(ax_0+by_0)q+r,0\le r<ax_0+by_0$

则　$r=(x-x_0q)a+(y-y_0q)b\in S$，由 ax_0+by_0 是 S 中的最小整数知 $r=0$

$\therefore ax_0+by_0/ax+by$　下证 P_8 第二题

$\because ax_0+by_0/ax+by$　（x,y 为任意整数）　$\therefore ax_0+by_0/a,ax_0+by_0/b$

$\therefore ax_0+by_0/(a,b)$．又有 $(a,b)/a,(a,b)/b$

$\therefore (a,b)/ax_0+by_0$　故 $ax_0+by_0=(a,b)$

4　证：作序列　$\cdots,-\frac{3|b|}{2},-|b|,-\frac{|b|}{2},0,\frac{|b|}{2},|b|,\frac{3|b|}{2},\cdots$ 则 a 必在此序列的某两项之间（区间段）

即存在一个整数q，使$\frac{q}{2}|b| \le a < \frac{q+1}{2}|b|$成立

(i)当q为偶数时，若$b>0$. 则令$s=\frac{q}{2}, t=a-bs=a-\frac{q}{2}b$，则有

$$0 \le a-bs=t=a-\frac{q}{2}b=a-\frac{q}{2}|b|<\frac{q}{2}|b| \therefore |t|<\frac{|b|}{2}$$

若$b<0$ 则令$s=-\frac{q}{2}, t=a-bs=a+\frac{q}{2}b$，则同样有$|t|<\frac{|b|}{2}$

(ii)当q为奇数时，若$b>0$则令$s=\frac{q+1}{2}, t=a-bs=a-\frac{q+1}{2}b$，则有

$$-\frac{|b|}{2} \le t=a-bs=a-\frac{q+1}{2}b=a-\frac{q+1}{2}|b|<0 \therefore |t| \le \frac{|b|}{2}$$

若 $b<0$，则令$s=-\frac{q+1}{2}, t=a-bs=a+\frac{q+1}{2}b$

则同样有 $|t| \le \frac{|b|}{2}$

综上 存在性得证 下证唯一性

当b为奇数时，设$a=bs+t=bs_1+t_1$则$|t-t_1|=|b(s_1-s)|>|b|$

而$|t| \le \frac{|b|}{2}, |t_1| \le \frac{|b|}{2} \therefore |t-t_1| \le |t|+|t_1| \le |b|$ 矛盾 故$s=s_1, t=t_1$

当b为偶数时，s,t不唯一，举例如下：此时$\frac{b}{2}$为整数

$$3 \cdot \frac{b}{2}=b \cdot 1+\frac{b}{2}=b \cdot 2+(-\frac{b}{2}), t_1=\frac{b}{2}, |t_1| \le \frac{b}{2}$$

$$a=bs_1+t_1=bs_2+t_2, t_2=-\frac{b}{2}, |t_2| \le \frac{b}{2}$$

5.证：令此和数为 S，根据此和数的结构特点，我们可构造一个整数 M，使 MS 不是整数，从而证明 S 不是整数

（1） 令 S=$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{n}$，取 M=$2^{k-1} \cdot 3 \cdot 5 \cdot 7 \cdots p$这里 k 是使$2^k \le n$最大整数，p 是不大于 n 的最大奇数。则在 1，2，3，---，n 中必存在一个$n_0=2^k$，所以

$$MS=M+\frac{M}{2}+\frac{M}{3}+\cdots+\frac{M}{n_0}+\cdots+\frac{M}{n}$$

由 M=$2^{k-1} \cdot 3 \cdot 5 \cdot 7 \cdots p$知$\frac{M}{2}$，$\frac{M}{3}, \cdots, \frac{M}{n}$必为整数，$\frac{M}{n_0}=\frac{3 \cdot 5 \cdot 7 \cdots p}{2}$显

然不是整数，

$\therefore$ MS 不是整数，从而 S 不是整数

（2） 令 M=$3^{k-1}\cdot 5\cdot 7\cdots(2n-1)$ 则 SM=$\frac{M}{3}+\frac{M}{5}+\cdots+\frac{M}{2n-1}+\frac{M}{2n+1}$，

由 M=$3^{k-1}\cdot 5\cdot 7\cdots(2n-1)$ 知 $\frac{M}{3},\frac{M}{5},\cdots,\frac{M}{2n-1}$，而

$\frac{M}{2n+1}=\frac{3^{k-1}\cdot 5\cdot 7\cdots(2n-1)}{2n+1}$ 不为整数

$\therefore$ SM 不为整数，从而 $S=\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n+1}$ 也不是整数

1. 证：设 d' 是 a，b 的任一公因数，$\therefore$ d'|a，d'|b

由带余除法

$a=bq_1+r_1,b=r_1q_2+r_2,\cdots,r_{n-2}=r_{n-1}q_n+r_n,r_{n-1}=r_nq_{n+1},0=r_{n+1}\le r_n<r_{n-1}<\cdots<r_1<b$

$\therefore (a,b)=r_n$。

$\therefore$ $d'|a-bq_1=r_1$，$d'|b-r_1q_2=r_2$，---，$d'|r_{n-2}=r_{n-1}q_n+r_n=(a,b)$，

即 d' 是 (a,b) 的因数。

反过来 $(a,b)|a$ 且 $(a,b)|b$，若 $d''|(a,b)$, 则 $d''|a,d''|b$，所以 (a,b) 的因数

都是 a,b 的公因数，从而 a,b 的公因数与 (a,b) 的因数相同。

2. 见本书 P2，P3 第 3 题证明。

3. 有§1 习题 4 知：$\forall a,b\in Z,b\ne 0,\exists s,t\in Z$, 使 $a=bs+t,|t|\le\frac{b}{2}$。，

$\therefore \exists s_1,t_1$，使 $b=s_1t+t_1,|t_1|\le\frac{|t|}{2}\le\frac{b}{2^2},\cdots$, 如此类推知：

$\exists s_n,t_n,t_{n-2}=t_{n-1}s_n+t_n$；　　$\exists s_{n+1},t_{n+1},t_{n-1}=t_ns_{n+1}+t_{n+1}$；　　且

$|t_n|\le\frac{|t_{n-1}|}{2}\le\frac{|t_{n-2}|}{2^2}\le\cdots\le\frac{|t|}{2^n}\le\frac{|b|}{2^{n+1}}$

而 b 是一个有限数，$\therefore \exists n\in N$, 使 $t_{n+1}=0$

$\therefore (a,b)=(b,t)=(t,t_1)=(t_1,t_2)=\cdots=(t_n,t_{n+1})=(t_n,0)=t_n$，存在

其求法为 $(a,b)=(b,a-bs)=(a-bs,b-(a-bs)s_1)=\cdots$

$\therefore (76501,9719)=(9719,76501-9719\times 7)=(8468,9719-8468)=(1251,8468-1251\times 6$

4。证：由 P3§1 习题 4 知在（1）式中有

$$0=r_{n+1}<r_n\le\frac{r_{n-1}}{2}\le\frac{r_{n-2}}{2^2}\le\cdots\le\frac{r_1}{2^{n-1}}\le\frac{b}{2^n}，\ 而\ r_{n\ge1}$$

$$\therefore 1\le\frac{b}{2^n},\therefore 2^n\le b，\quad \therefore n\le\log_2 b=\frac{\log b}{\log 2}，\ 即\ n\le\frac{\log b}{\log 2}$$

1，证：必要性。若 $(a,b)=1$，则由推论 1.1 知存在两个整数 s，t 满足：$as+bt=(a,b)$，

$\therefore as+bt=1$

充分性。若存在整数 s，t 使 as+bt=1，则 a，b 不全为 0。

又因为 $(a,b)\mid a,(a,b)\mid b$，所以 $(a,b\mid as+bt)$ 即 $(a,b)\mid 1$。又 $(a,b)>0$，

$\therefore (a,b)=1$

2．证：设 $[a_1,a_2,\cdots,a_n]=m_1$，则 $a_i\mid m_1(i=1,2,\cdots,n)$

$\therefore |a_i|\mid m_1(i=1,2,\cdots,n)$ 又设 $[|a_1|,|a_2|,\cdots,|a_n|]=m_2$ 则

$m_2\mid m_1$。反之若 $|a_i|\mid m_2$，则 $a_i\mid m_2$，$\therefore m_1\mid m_2$。

从而 $m_1=m_2$，即 $[a_1,a_2,\cdots,a_n]=[|a_1|,|a_2|,\cdots,|a_n|]_2$

3．证：设（1）的任一有理根为 $\frac{p}{q}$，$(p,q)=1,q>1$。则

$$a_n(\frac{p}{q})^n+a_{n-1}(\frac{p}{q})^{n-1}+\cdots+a_1\frac{p}{q}+a_0=0$$

$$\therefore a_np^n+a_{n-1}p^{n-1}q+\cdots+a_1pq^{n-1}+a_0q^n=0 \qquad （2）$$

由 $(2)-a_np^n=a_{n-1}p^{n-1}q+\cdots+a_1pq^{n-1}+a_0q^n$，

所以 q 整除上式的右端，所以 $q\mid a_np^n$，又 $(p,q)=1,q>1$，所以 $(q,p^n)=1,\therefore q\mid a_n$；

又由（2）有 $a_np^n+a_{n-1}p^{n-1}q+\cdots+a_1pq^{n-1}=-a_0q^n$

因为 p 整除上式的右端，所以 $P\mid a_0q^n$，$(p,q)=1,q>1$，所以 $(q^n,p)=1,\therefore p\mid a_n$

故（1）的有理根为 $\frac{p}{q}$，且 $p\mid a_0, q\mid a_n$。

假设 $\sqrt{2}$ 为有理数，$x=\sqrt{2}, \therefore x^2-2=0$，次方程为整系数方程，则由上述结论，可知其有有理根只能是

$\pm1,\pm2$，这与 $\sqrt{2}$ 为其有理根矛盾。故 $\sqrt{2}$ 为无理数。

另 证 ， 设 $\sqrt{2}$ 为 有 理 数 $\sqrt{2}=\frac{p}{q}$， $(p,q)=1, q>1$ ， 则

$2=\frac{p^2}{q^2}, \therefore 2q^2=p^2, \therefore (p^2,q^2)=(2q^2,p^2)=q^2>1$

但由 $(p,q)=1, q>1$ 知 $(p^2,q^2)=1$，矛盾，故 $\sqrt{2}$ 不是有理数。

1． 见书后。

2． 解：因为 8|848,所以 $8\mid A, A=82798848=8\times10349856=2^3\times B$，

又 8|856，所以 8|B， $B=8\times1293732=2^3\times C$，

又 4|32，所以 4|C， $C=4\times323433=2^2\times D$

又 9|（3+2+3+4+3+3），所以 9|D， $D=9\times35937=3^2\times E$，

又 9|（3+5+9+3+7），所以 9|E， $E=9\times3993$

又 $3993=3\times1331=3\times11^3$

所以 $A=2^8 3^5 11^3$；同理有 $81057226635000=2^3\cdot3^3\cdot5^4\cdot7^3\cdot11^2\cdot17\cdot23\cdot37$。

3．证：$\because \gamma_i=\min(\alpha_i,\beta_i)$， $\therefore 0\le\gamma_i\le\alpha_i, 0\le\gamma_i\le\beta_i$

$\therefore p_i^{\gamma_i}\mid p_i^{\alpha_i}, p_i^{\gamma_i}\mid p_i^{\beta_i} \quad (i=1,2\cdots k)$ $\qquad \therefore \prod_{i=1}^{k} p_i^{\gamma_i} \Big| \prod_{i=1}^{k} p_i^{\alpha_i}$， $\therefore \prod_{i=1}^{k} p_i^{\gamma_i} \Big| \prod_{i=1}^{k} p_i^{\beta_i}$.

$\therefore p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}\mid(a,b)$，又显然 $(a,b)\mid p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}$

$\therefore p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}=(a,b)$，同理可得 $p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k}=[a,b]$， $\delta_i=\max\{\alpha_i,\beta_i\}$

推广.设 $a_1=p_1^{\beta_{11}}p_2^{\beta_{12}}\cdots p_k^{\beta_{1k}}, a_2=p_1^{\beta_{21}}p_2^{\beta_{22}}\cdots p_k^{\beta_{2k}},\cdots,a_n=p_1^{\beta_{n1}}p_2^{\beta_{n2}}\cdots p_k^{\beta_{nk}}$

(其中 p_j 为质数 $j=1,2,\cdots,k,a_i$ 为任意 n 个正整数 $i=1,2,\cdots,n,\beta_{ij}\geq 0$)

则 $p_1^{\gamma_{i1}}p_2^{\gamma_{i2}}\cdots p_k^{\gamma_{ik}}=(a_1,a_2,\cdots,a_n),\gamma_{ij}=\min\limits_{1\leq i\leq n}\{\beta_{ij}\}\ j=1,2,\cdots,k$

$p_1^{\delta_{i1}}p_2^{\delta_{i2}}\cdots p_k^{\delta_{ik}}=[a_1,a_2,\cdots,a_n],\delta_{ij}=\max\limits_{1\leq i\leq n}\{\beta_{ij}\}\ j=1,2,\cdots,k$

4．证：由 $p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}=(a,b)$，$p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k}=[a,b]$,有

$$(a,b)[a,b]=p_1^{\gamma_1+\delta_1}p_2^{\gamma_2+\delta_2}\cdots p_k^{\gamma_k+\delta_k}=p_1^{\alpha_1+\beta_1}p_2^{\alpha_2+\beta_2}\cdots p_k^{\alpha_k+\beta_k}=ab$$

从而有 $[a,b]=\dfrac{ab}{(a,b)}$.

5．证：（反证法）设 $n=2^k l$（l 为奇数）则

$$2^n+1=2^{2^k\cdot l}+1=(2^{2^k})^l+1=(2^{2^k}+1)[2^{2^k\cdot(l-1)}-2^{2^k\cdot(l-2)}+\cdots+1]$$

$\because 1<2^{2^k}+1<(2^{2^k})^l+1=2^n+1$，$\therefore\ 2^n+1$ 为合数矛盾，故 n 一定为 2 的方幂.

2.(i)证:：设 $[\alpha]=m$.则由性质 II 知 $m\leq\alpha<m+1$,所以 $nm\leq n\alpha<nm+n$，

所以 $nm\leq[n\alpha]<nm+n$，所以 $m\leq\dfrac{[n\alpha]}{n}<m+1$，又在 m 与 m+ 1 之间只有唯一整数 m，所以 $[\dfrac{[n\alpha]}{n}]=m=[\alpha]$.

(ii)[证一]设 $\dfrac{k}{n}\leq\{\alpha\}<\dfrac{k+1}{n},k=0,1,2,\cdots,n-1$,则 $k\leq n\{\alpha\}<k+1,\therefore[n\alpha]=n[\alpha]+k$

①当 $i+k\leq n-1$ 时, $\{\alpha\}+\dfrac{i}{n}<\dfrac{k+1+i}{n}\leq 1,[\alpha+\dfrac{i}{n}]=[\alpha]$ ；

②当 $i+k\geq n$ 时, $2>\{\alpha\}+\dfrac{i}{n}\geq\dfrac{k+i}{n}\geq 1,[\alpha+\dfrac{i}{n}]=[\alpha]+1$;

$$\therefore[\alpha]+[\alpha+\frac{1}{n}]+\cdots+[\alpha+\frac{n-1}{n}]=\sum_{i=0}^{n-1}[\alpha+\frac{1}{n}]=\sum_{i-0}^{n-1-k}[\alpha+\frac{i}{n}]+\sum_{i=n-k}^{n-1}[\alpha+\frac{i}{n}]$$
$$=(n-k)[\alpha]+k([\alpha]+1)=n[\alpha]+k$$

$$\therefore\sum_{i=0}^{n-1}[\alpha+\frac{i}{n}]=[n\alpha]$$

[证二]令 $f(\alpha)=\sum\limits_{i=0}^{n-1}[\alpha+\dfrac{i}{n}]-[n\alpha],\because\ f(\alpha+\dfrac{1}{n})=\sum\limits_{i=0}^{n-1}[\alpha+\dfrac{i+1}{n}]-[n\alpha+1]\equiv f(\alpha)$

$$\because\ f(\alpha+\frac{1}{n})=\sum_{i=0}^{n-1}[\alpha+\frac{i+1}{n}]-[n\alpha+1]\equiv f(\alpha)$$

$\therefore f(\alpha)$是以$\dfrac{1}{n}$为周期的函数。

又当$\alpha\in[0,1)$时, $f(\alpha)=0-0=0, \therefore \alpha\in R, f(\alpha)\equiv 0$，即$\sum_{i=0}^{n-1}[\alpha+\dfrac{1}{n}]=[n\alpha]$。

[评注]：[证一]充分体现了 常规方法的特点，而[证二]则表现了较高的技巧。

3.（i）证：由高斯函数[x]的定义有$\alpha=[\alpha]+r,\beta=[\beta]+s, 0\le r<1; 0\le s<1$。则

$$\alpha-\beta=[\alpha]-[\beta]+r-s, r-s<1$$

当$r-s\ge 0$时,$[\alpha-\beta]=[\alpha]-[\beta]$

当$r-s<0$时,$[\alpha-\beta]=[\alpha]-[\beta]-1$

故 $[\alpha-\beta]=[\alpha]-[\beta]$或$[\alpha-\beta]+1=[\alpha]-[\beta]$

（ii）证：设$\alpha=[\alpha]+x,\beta=[\beta]+y, 0\le x,y<1$，则有$0\le x+y=\{\alpha\}+\{\beta\}<2$

下面分两个区间讨论：

① 若 $0\le x+y<1$，则 $[x+y]=0$，所以 $[\alpha+\beta]=[\alpha]+[\beta]$，所以

$$\begin{aligned}&[2\alpha]+[2\beta]=[2[\alpha]+2x]+[2[\beta]+2y]=2[\alpha]+2[\beta]+2([x]+[y])\\&\ge 2[\alpha]+2[\beta]=[\alpha]+[\beta]+[\beta]+[\alpha]=[\alpha]+[\alpha+\beta]+[\beta]\end{aligned}$$

② 若 $1\le x+y<2$，则 $[x+y]=1$，所以 $[\alpha+\beta]=[\alpha]+[\beta]+1$。所以

$$\begin{aligned}&[2\alpha]+[2\beta]=[2[\alpha]+2x]+[2[\beta]+2y]=2[\alpha]+2[\beta]+2([x]+[y])\\&\ge 2[\alpha]+2[\beta]+2([x]+[1-x])\xleftrightarrow{\because x\ge 1-y}=[\alpha]+[\beta]+[\beta]+[\alpha]+2+2([x]+[-x])\\&\ge 2[\alpha]+2[\beta]+1=[\alpha]+[\alpha+\beta]+[\beta]\end{aligned}$$

2.3

1 证：由$(\pm\dfrac{2ab}{a^2+b^2})+(\pm\dfrac{a^2-b^2}{a^2+b^2})=1$知$(\pm\dfrac{2ab}{a^2+b^2},\pm\dfrac{a^2-b^2}{a^2+b^2})$ 及$(\pm\dfrac{a^2-b^2}{a^2+b^2},\pm\dfrac{2ab}{a^2+b^2})$都是单位圆周$x^2+y^2=1$上的有理点。

另一方面，单位圆周$x^2+y^2=1$上的有理点可表示为$x=\dfrac{q}{p}, y=\dfrac{r}{p}, p>0$，于是得$q^2+r^2=p^2$，又 $q^2+r^2=p^2$ 的一切非整数解都可表示为：

$q=2ab, p=a^2+b^2, r=a^2-b^2, (a,b不全为0)$，于是第一象限中 $x^2+y^2=1$ 上的有理点可表示为 $(\frac{2ab}{a^2+b^2},\frac{a^2-b^2}{a^2+b^2}),(a,b不全为0)$，由于单位圆周上的有理点的对称性，放 $x^2+y^2=1$ 上的任意有理点可表为 $(\pm\frac{2ab}{a^2+b^2},\pm\frac{a^2-b^2}{a^2+b^2})$ 及 $(\pm\frac{a^2-b^2}{a^2+b^2},\pm\frac{2ab}{a^2+b^2})$，其中 a，b 不全为 0，± 号可任意取。

3．2

1. 证：由 u,v 的取值可得 $p^{s-t}p^t=p^s$ 个数，若 $u_1+p^{s-t}v_1\equiv u_2+p^{s-t}v_2 \pmod{p^s}$，

$u_1+p^{s-t}v_1\equiv u_2+p^{s-t}v_2 \pmod{p^{s-t}}$ 则 $u_1\equiv u_2 \pmod{p^{s-t}}$，又 $0\le u_1,u_2<p^{s-t}$，$\therefore u_1=u_2$。

又 $p^{s-t}v_1\equiv p^{s-t}v_2 \pmod{p^{s-t}}, v_1\equiv v_2 \pmod{p^t}$，又 $0\le v_1,v_2<p^t$，$\therefore v_1=v_2$。

$\therefore u_1+p^{s-t}v_1$ 与 $u_2+p^{s-t}v_2$ 为同一数，矛盾，故原命题成立。

3.（i）的引理

对任何正整数 a，可以唯一的表示成 $a=3^n a_n+3^{n-1}a_{n-1}+\cdots+3a_1+a_0$ 的形式，其中 $0\le a_i\le 3,(i=1,2,\cdots,n)$。

证：（i）$H=\frac{3^{n-1}-1}{3-1}=3^n+3^{n-1}+\cdots+3+1$

设 $A=3^n x_n+3^{n-1}x_{n-1}+\cdots+3x_1+x_0,(x_i=0,\pm1,i=1,2,\cdots,n)$

$A+H=3^n(x_n+1)+3^{n-1}(x_{n-1}+1)+\cdots+3(x_1+1)+(x_0+1)$

由于 x_i 取值 $0,\pm1$ 故 x_i+1 取值为 0，1，2。这样的数有 2H+1 个，其中最小的 数为 0，最大的数为 2H，所以 A+H 可以表示下列各数：0，1，2，$\cdots,2H$，上列数中减去 H 得 $-H,-H+1,-H+2,\cdots,-1,0,1,\cdots,H$，则 A 可表示上列各数，且表示唯一。

（ii）事实上，只需 $1斤,3斤,3^2斤,\cdots,3^n斤$ 这样的（n+1）个砝码即可。由（I）知 1 到 H 中任一斤有且仅有一种表示法 $\sum_{i=0}^{n}(3^i x_i).(x_i=-1,0,1)$，当 $x_i=-1$ 时，将砝码 3^i 放在重物盘中；当 $x_i=0$ 时，不放砝码 3^i；当 $x_i=1$ 时，将砝码 3^i 放在砝码盘中。如此即可。

3.3

1. 证：$\because (a_i, m) = 1$, 由定理 1 知 a_i 所在的模 m 的剩余系是与模 m 互质的。又已知 $a_1, a_2, \cdots a_{\varphi(m)}$ 两两对模 m 不同余，所以这 $\varphi(m)$ 个整数分别属于不同的模 m 的剩余类。再由定理 1 知结论成立。

2 .证：设模 m 的一个简化剩余系是 $r_1, r_2, \cdots, r_{\varphi(m)}, (1 \le r_i \le m)$，即 $(r_i, m) = 1$，由于 $(a, m) = 1$，当 ξ 通过 m 的简化剩余系 $\xi_1, \xi_2, \cdots, \xi_{\phi(m)}$ 时，由定理 3 知，$a\xi_1, a\xi_2, \cdots, a\xi_{\phi(m)}$ 也通过模 m 的剩余系。故对 $1 \le i \le \varphi(m)$，存在 $j(1 \le j \le \varphi(m))$ 使

$a\xi_i \equiv mq_i + r_j \Rightarrow \frac{a\xi_i}{m} = q_i + \frac{r_j}{m} \Rightarrow \{\frac{a\xi_i}{m}\} = \frac{r_j}{m}$,

$$\therefore \sum_{i=1}^{\varphi(m)} \{\frac{a\xi_i}{m}\} = \sum_{j=1}^{\phi(m)} \frac{r_j}{m} = \frac{1}{m} \cdot \frac{m}{2} \phi(m) = \frac{\varphi(m)}{2}.$$

3.（i）证：由定理 5 知：p 为质数时，$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$。

所以 $\phi(1) + \phi(p) + \cdots + \phi(p^\alpha) = 1 + (p-1) + p^2(1 - \frac{1}{p}) + \cdots + p^\alpha(1 - \frac{1}{p}) = p^\alpha$ 即证。

（ii）证:设整数 m 的所有正约数是 $d_1, d_2, \cdots, d_{T(m)}$,考察 m 的完全剩余系 $1, 2, \cdots, m$ （1）

对(1)中任一数 a,设(a, m)=d,则 $d \mid m$,即(1)中任一数与 m 的最大公约数是 $d_1, d_2, \cdots, d_{T(m)}$ 中的数。反之，对每一个 d_i，（1）中必有一数 a 使 $(a, m) = d_i$（例如 $a = a_i$），而且对（1）中任一数不可能出现 $(a, m) = d_i, (a, m) = d_j.(i \ne j)$，于是，将（1）中的数按其与 m 的最大公约数的情形分类：（1）中与 m 的最大公约数是 d_1 的数有 $\varphi(\frac{m}{d_1})$ 个；（1）中与 m 的最大公约数是 d_2 的数有 $\varphi(\frac{m}{d_2})$ 个；---，（1）中与 m 的最大公约数是 d_1 的数有 $\varphi(\frac{m}{d_1})$ 个；所以

$\varphi(\frac{m}{d_1}) + \phi(\frac{m}{d_2}) + \cdots + \varphi(\frac{m}{d_{T(m)}}) = m$,即 $\sum_{d_i \mid m} \varphi(\frac{m}{d_i}) = m$,注意 $\frac{m}{d_i}$ 是 m 的约数,所以 $\sum_{d \mid m} \varphi(\frac{m}{d}) = m$

2.4

1. 解:$10^{10}\equiv(-2)^{10}\equiv 1024\equiv 4(\bmod 6)$,即$10^{10}=6q+4,(q\in N)$，因为$(10,7)=1$，由欧拉定理有$10^6\equiv 1(\bmod 7)$,所以$10^{10^{10}}\equiv 10^{6q+4}\equiv(10^6)^q 10^4\equiv 1^q 10^4\equiv(-3)^4\equiv 4(\bmod 7)$

所以从今天起再过$10^{10^{10}}$天是星期五.

3.(i)证：对a用数学归纳法.①当 a=2 时,证明$(h_1+h_2)^p\equiv h_1^p+h_2^p(\bmod p)$,

$$(h_1+h_2)^p=\sum_{i=0}^{p}(C_p^i h_1^{p-i}h_2^i)$$,对$C_p^i(1\le i\le p)$有$C_p^i=\dfrac{A_p^i}{i!}$为整数$\Rightarrow i!\,|\,A_p^i$,

又因为$(1,p)=(2,p)=\cdots=(i,p)$,所以$(i!,p)=1$。$\therefore i!\,|\,(p-1)\cdots(p-i+1)$，所以可设$q=\dfrac{(p-1)\cdots(p-i+1)}{i!}$为整数。$\therefore C_p^i=pq$,即$p\,|\,C_p^i,C_p^i\equiv 0(\bmod p)$。

所以$(h_1+h_2)^p\equiv h_1^p+h_2^p(\bmod p)$。

②假设命题对k成立，即$(h_1+h_2+\cdots+h_k)^p\equiv h_1^p+h_2^p+\cdots h_k(\bmod p)$，则对于$(k+1)$有

$$(h_1+h_2+\cdots+h_k+h_{k+1})^p\equiv(h_1+h_2+\cdots+h_k)^p+h_{k+1}^p\equiv h_1^p+h_2^p+\cdots+h_k^p+h_{k+1}^p(\bmod p)$$

所以命题对$(k+1)$也成立。综合①，②可知对一切自然数 a，命题成立。

（ii）证：$a^p=(\underbrace{1+1+\cdots+1}_{a个1})^p=\underbrace{1^p+1^p+\cdots+1^p}_{a个1^p}\equiv a(\bmod p)$。