Chapter 1

预备知识

1.1 集合

Exercise 1

设 $A=\{a,\{a\}\}$, 下列各式成立吗？写出判断过程。

$\{a\}\in\rho(A);\{a\}\subseteq\rho(A);\{\{a\}\}\in\rho(A);\{\{a\}\}\subset\rho(A)$

Answer of exercise 1

答：

先计算幂集，然后判断幂集和各个各部分的关系。

Exercise 2

全集 $E=\{1,2,3,4,5\},A=\{1,4\},B=\{1,2,5\},C=\{2,4\}$, 计算：

1) $A\cap\sim B$

2) $(A\cup B)\cap(A\cup C)$

3) $\sim(A\cup B)$

4) $\rho(A)-\rho(C)$

Answer of exercise 2

答：

$\sim B=\{3,4\},\rho(A)=\{\phi,\{1,4\},\{1\},\{4\}\},\rho(C)=\{\phi,\{2,4\},\{2\},\{4\}\}$

1) $A\cap\sim B=\{4\}$

2) $(A\cup B)\cap(A\cup C)=\{1,2,4\}$

3) $\sim(A\cup B)=\{3\}$

4) $\rho(A)-\rho(C)=\{\{1,4\},\{1\}\}$

Exercise 3

A,B,C 是任意三个集合，证明 $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.

Answer of exercise 3

答：

先按照对称差的定义，用基本运算来表示，然后在组合为右边形式。

1.2 关系

Exercise 4

集合 $A = \{16, 17, 18, 19\}$,R 为 A 上的关系 $R = \{< 16, 17 >, < 17, 18 >, < 18, 19 >\}$，请问 R 的逆关系存在吗？如果存在请写出来。

Answer of exercise 4

答：

这道题来源于 16 级的学生做 17 级的班助，17 级的做 18 级的，18 级做 19 级的这种关系，二元逆关系总是存在的，将所有序偶倒着写就是二元逆关系。

Exercise 5

$\mathbb{Z}$ 为整数集合，请问此集合上的相等关系是等价关系吗？如果是请证明。

Answer of exercise 5

答：

首先要知道什么是等价关系：自反，传递，对称，很容易验证整数集上的相等关系符合等价定义。

Exercise 6

请证明笛卡尔积不满足结合律。

Answer of exercise 6

答：

证明不满足，其实只需要给出一个反例即可，设 $A = \{1\}, B = \{a, b\}, C = \{x, y\}$，$(A \times B) \times C = \{<< 1, a >, x >, << 1, a >, y >, << 1, b >, x >, << 1, b >, y >\}$, $A \times (B \times C) = \{< 1, < a, x >>, < 1, < a, y >>, < 1, < b, x >>, < 1, < b, y >>\}$, 显然这两个集合是不相等的。

1.3 函数

Exercise 7

$\mathbb{R}$ 为实数集合，二维向量定义为 $V_2 = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}$，矩阵 $C = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$, 定义矩阵与二维向量的乘运算 $A \cdot v_2 = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \cdot (x, y) = (a \times x + b \times y, c \times x + d \times y)$, 请问 $C \cdot v, v \in V_2$ 是从 V_2 到

V_2 的一个函数吗？并说明理由。

Answer of exercise 7

答：

判断关系是不是一个函数，就要看是否每个 x 是否有唯一的 y 对应，显然这是符合定义的。

Exercise 8

请分别给出实数域上的满射函数、单射函数、双射函数的例子，并说出原因。

Answer of exercise 8

答：

满射就是值域中所有的元素都有一个像对应，单射是定义域中没有两个不同的元素像相同，双射就是既是满射又是单射。

Chapter 2

整除

Exercise 9

证明，若 $2 \mid n, 5 \mid n, 7 \mid n$，那么 $70 \mid n$.

Answer of exercise 9

答：

$2 \mid n, 5 \mid n, 7 \mid n \Rightarrow lcm(2,5,7) \mid m \Rightarrow 70 \mid n$

Exercise 10

证明任意三个连续的正整数的乘积都被 6 整除。

Answer of exercise 10

答：

$m(m+1)(m+2)$

$m = 1, 1 \times 2 \times 3 = 6$, 成立。

设 m=k 也成立。

$m = k+1, (k+1)(k+2)(k+3) = (k+1)(k+2)k + 3(k+1)(k+2)$，可见式子的第一部分可被 6 整除，要想证明 $3(k+1)(k+2)$ 可被 6 整除，可证明 $(k+1)(k+2)$ 可被 2 整除, 不管 k 是奇数还是偶数，两个成绩项一定有个偶数项，所以可以被 2 整除。

Exercise 11

证明每个奇数的平方都具有 8k+1 的形式。

Answer of exercise 11

答：

奇数可以写为 $2k+1$, 奇数的平凡是 $(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$, 可知 $k(k+1)$ 是偶数，所以可以写成 2m 的形式，$4k(k+1)+1$ 可以写成 $8m+1$ 形式。

Exercise 12

求如下整数对的最大公因子，并写出求解过程。

(1)(55,85) (2)(202,282) (3)(666,1414) (4)(20785,44350)

Answer of exercise 12

答：

$gcd(55,85)=5, gcd(55,85)=2, gcd(666,1414)=2, gcd(20785,44350)=5$，下面给出第一对数的实际计算过程：

$85=55\times1+30$

$55=30\times1+25$

$30=25\times1+5$

$25=5\times5$

$gcd(55,85)=5$

Exercise 13

求如下整数对的最小公倍数，并写出求解过程。

(1)(231,732) (2)(-871,728)

Answer of exercise 13

答：

先求 $gcd(231,732), lcm(231,732)=(231\times732)\div gcd(231,732)$，计算结果如下：

$lcm(231,732)=56364, lcm(-871,728)=48776$

Exercise 14

求以下整数的标准分解式，并写出求解过程。

(1)36 (2)69 (3)200 (4)289

Answer of exercise 14

答：

利用小于次数的素数去依次除次数，可以整除，则找到一个素因子，依次可以找到所有素因子。分解结果如下 (sagemath factor)：

$36=2^2*3^2, 69=3*23, 200=2^3*5^2, 289=17^2$

Exercise 15

求以下整数的标准分解式，并写出求解过程。

(1)625 (2)2154 (3)2838 (4)3288

Answer of exercise 15

答：

利用小于次数的素数去依次除次数，可以整除，则找到一个素因子，依次可以找到所有素因子。分解结果如下:

$625=5^4, 2154=2*3*359, 2838=2*3*11*43, 3288=2^3*3*137$

Chapter 3

同余

Exercise 16

设模 m=16, 求解 1,9,16,17,25,160 模 16 余数, 并找出同余的数来。

Answer of exercise 16

答：

依次计算上面各数模 16 的余数，余数分别为 1、9、0、1、9、0, 根据同余定义，我们有 $1 \equiv 17(mod\ 16), 9 \equiv 25(mod\ 26), 16 \equiv 160(mod\ 26)$。

Exercise 17

求 7^{2046} 写成十进制数时的个位数。

Answer of exercise 17

答：

答案是：9, 计算过程如下：

$7^2 = 49 \equiv 9(mod 10), 9^2 = 81 \equiv 1(mod 10), 2046 = 4 \times 511 + 2 \Rightarrow 7^{2046} \equiv ((7^2)^2)^{511} \times 7^2 \equiv 9(mod 10)$

Exercise 18

求 2^{1000} 的十进制表示中的末尾两位数字。

Answer of exercise 18

答：

答案为：76，计算过程如下：

$2^0 = 1(mod 100), 2^1 = 2(mod 100), 2^2 = 4(mod 100), 2^3 = 8(mod 100), 2^4 = 16(mod 100)$
$2^5 = 32(mod 100), 2^6 = 64(mod 100), 2^7 = 28(mod 100), 2^8 = 56(mod 100), 2^9 = 12(mod 100)$
$2^{10} = 24(mod 100), 2^{11} = 48(mod 100), 2^{12} = 96(mod 100), 2^{13} = 92(mod 100), 2^{14} = 84(mod 100)$
$2^{15} = 68(mod 100), 2^{16} = 36(mod 100), 2^{17} = 72(mod 100), 2^{18} = 44(mod 100), 2^{19} = 88(mod 100)$
$2^{20} = 76(mod 100), 2^{21} = 52(mod 100), 2^{22} = 4(mod 100), 2^{23} = 8(mod 100), 2^{24} = 16(mod 100)$
$2^{25} = 32(mod 100), 2^{26} = 64(mod 100), 2^{27} = 28(mod 100), 2^{28} = 56(mod 100), 2^{29} = 12(mod 100)$

$2^{30} = 24(mod100), 2^{31} = 48(mod100), 2^{32} = 96(mod100), 2^{33} = 92(mod100), 2^{34} = 84(mod100)$
$2^{35} = 68(mod100), 2^{36} = 36(mod100), 2^{37} = 72(mod100), 2^{38} = 44(mod100), 2^{39} = 88(mod100)$
$1000 = 20 \times 50 \Rightarrow 2^{1000} = 2^{20^5}0 \equiv 2^{20} \equiv 76(mod\ 100)$

Exercise 19

已知 2019 年 9 月 29 日是星期天，问之后的 2^{100} 天是星期几？第 2^{200} 天呢？

Answer of exercise 19

答：

由于 $2^1 \equiv 2(mod\ 7), 2^2 \equiv 4(mod\ 7), 2^3 \equiv 1(mod\ 7)$

所以 $2^{3\times33} \equiv 1(mod\ 7)$

又因为 $100 = 3 \times 33 + 1$, 所以 $2^{100} = 2^{3\times33+1} = 2^{3\times33} \times 2 \equiv 2(mod\ 7)$，所以第 2^{100} 天是星期三。同理 $200 = 3 \times 66 + 2$,$2^{200} = 2^{3\times66+2} = 2^{3\times66} \times 2^2 \equiv 4(mod\ 7)$, 所以第 2^{200} 天是星期五.

Exercise 20

求 $1^5 + 2^5 + 3^5 + \ldots + 99^5$ 之和被 4 除的余数。

Answer of exercise 20

答：

$4^5 + 5^5 + 6^5 + 7^5 \equiv 0 + 1^5 + 2^5 + 3^5(mod4)$

...

$96^5 + 97^5 + 98^+99^5 \equiv 0 + 1^5 + 2^5 + 3^5(mond4)$ 共有 24 组，$24 \times (1 + 32 + 3^5) \equiv 0(mod4)$

Exercise 21

写出模 9 的一个完全剩余系，它的每个数都是奇数。

Answer of exercise 21

答：

$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}, 2k + 1, \{1, 3, 5, 7, 9, 11, 13, 15, 17\}$

Exercise 22

写出模 9 的一个完全剩余系，它的每个数都是偶数。

Answer of exercise 22

答：

$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}, 2k, \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$

Exercise 23

用模 5 和模 6 的完全剩余系，表示模 30 的完全剩余系。

Answer of exercise 23

答：

模 5 的完全剩余系 $\{0, 1, 2, 3, 4\}$

模 6 的完全剩余系 $\{0, 1, 2, 3, 4, 5\}$

5，6 互质,$30 = 5 \times 6$

m_i×5+n_j×6, $\{0, 1, 2, 3, 4, 5, 11, 17, 23, 29, 35, 10, 16, 22, 28, 34, 40, 15, 21, 27, 31, 39, 45, 20, 26, 32, 38, 44, 50\}$

Exercise 24

写出 12 的最小正缩系。

Answer of exercise 24

答：

最小正完全系 { 1,2,3,4,5,6,7,8,9,10,11,12 }, 与 12 互素的有 {1,5,7,11}

Exercise 25

用模 5 和模 6 的缩系，表示模 30 的缩系。

Answer of exercise 25

答：

5 和 6 互素,x 和 y 遍历 5 和 6 的缩系，$5x + 6y$ 也遍历模 5×6 的缩系。模 5 的缩系 $\{1, 2, 3, 4\}$，模 6 的缩系 $\{1, 5\}$，模 30 的缩系 $11, 16, 21, 30, 35, 40, 45, 50$

Exercise 26

计算以下整数的欧拉函数。

(1)24　　(2)64　　(3)187　　(4)360

Exercise 27

计算 $8 \times 9 \times 10 \times 11 \times 12 \times 13 (mod\ 7)$.

Answer of exercise 27

答：

$\because 8 \equiv 1 (mod\ 7)$

$9 \equiv 2 (mod\ 7)$

$10 \equiv 3 (mod\ 7)$

$11 \equiv 4 (mod\ 7)$

$12 \equiv 5 (mod\ 7)$

$13 \equiv 6 (mod\ 7)$

$\therefore 720 \equiv 6 (mod\ 7)$

Exercise 28

求 $229^{-1} (mod\ 281)$

Answer of exercise 28

答：

229 模 281 逆元是 27.

具体解法是首先判断 $gcd(229, 281) = 1$，逆元存在，然后利用扩展欧几里得算法求逆元 $s_i = s_{i-2} + q_{i-1}s_{i-1}, t_i = t_{i-2} + q_{i-1}t_{i-1}$：

i	r_i	q_i	s_i	t_i
0	281	-	1	0
1	229	1	0	1
2	52	4	1	-1
3	21	2	-4	5
4	10	2	9	-11
5	1	10	-22	27
5	0	-	-	-

Exercise 29

求 $3169^{-1}(mod\ 3571)$.

Answer of exercise 29

答：

利用欧几里得扩展算法计算，计算结果为：2887.

sagemath 验证语句：3169.inverse_mod(3571)

Exercise 30

解方程 $105x + 121y = 1(x, y \in \mathbb{Z})$.

Answer of exercise 30

答：

根据欧几里得扩展算法，我们有 $gcd(r_0, r_1) = s_n r_0 + t_n r_1$，我们设 $r_0 = 121, r_1 = 105$, 同时我们可知 105 与 121 互素 $(gcd(121, 105) = 1)$，可见欧几里得扩展算法最后的等式为 $121s_n + 105t_n = 1$，与所求的方程相同，我们利用扩展欧几里得算法进行计算：

	r_i	q_i	s_i	t_i
0	121	-	1	0
1	105	1	0	1
2	16	6	1	-1
3	9	1	-6	7
4	7	1	7	-8
5	2	3	-13	15
6	1	2	46	-53
7	0			

Exercise 31

求解一次同余方程 $27x \equiv 12(mod\ 15)$

Answer of exercise 31

答：

gcd(27,15)=3，所以同余方程共有 3 个解，同余方程 $9x \equiv 4(mod\ 5)$ 的一个特解是 x=1, 所以原方程全部解为 $x \equiv 1 + \frac{15}{3}t(mod\ 15), t \in 0, 1, 2$，求得其解为 1，6，11.

Exercise 32

求解一次同余方程 $24x \equiv 6(mod\ 81)$

Answer of exercise 32

答：

gcd(24,81)=3，所以同余方程共有 3 个解，同余方程 $8x \equiv 2(mod\ 27)$ 的一个特解是 x=7, 所以原方程全部解为 $x \equiv 7 + \frac{81}{3}t(mod\ 81), t \in 0, 1, 2$，求得其解为 7,34,61.

Exercise 33

求解一次同余方程 $91x \equiv 26(mod\ 169)$

Answer of exercise 33

答：

gcd(91,169)=13，并且 $13 \mid 26$, 所以同余方程共有 13 个解，同余方程 $7x \equiv 2(mod\ 13)$ 的一个特解是 x=4(可以通过遍历的方法求得), 所以原方程全部解为 $x \equiv 4 + \frac{169}{13}t(mod\ 169), t \in 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$，求得其解为 4,17,30,43,56,69,82,95,108,121,134,147,160.

Exercise 34

确定以下同余式不同解的个数，无须求出具体解。

1. $72x \equiv 47(mod\ 200)$
2. $4183x \equiv 5781(mod\ 15087)$
3. $1537x \equiv 2863(mod\ 6731)$

Answer of exercise 34

答：

gcd(72,200)=8, 但是 $8 \nmid 47$, 所以第一个方程无解。gcd(4183,15087)=47，且 $47 \mid 5781$，故第二方程有解，且解的个数为 47.gcd(1537,6731)=53, 但是 $53 \nmid 2863$，故此方程无解。

Exercise 35

求解同余方程组：$\begin{cases} x \equiv 9(mod\ 12) \\ x \equiv 6(mod\ 25) \end{cases}$

Answer of exercise 35

答：

gcd(12,25)=1, 利用中国剩余定理，唯一解为 $x \equiv 25 \times 1 \times 9 + 12 \times 23 \times 6(mod\ 12 \times 25) \equiv 1881 \equiv 81(mod\ 300)$

Exercise 36

求解同余方程组：$\begin{cases} x \equiv 5(mod\ 7) \\ x \equiv 12(mod\ 15) \\ x \equiv 18(mod\ 22) \end{cases}$

Answer of exercise 36

答：

$gcd(7,15)=1, gcd(15,22)=1, gcd(7,22)=1$，可以看出以上方程组的模两两互素，根据中国剩余定理，我们有:

$x \equiv 5(mod\ 7), m = 7 \times 15 \times 22 = 2310$

$M_1 = 15 \times 22 = 330, M_1' = 1(mod\ 7)$

$M_2 = 7 * 22 = 154, M_2' = 4(mod\ 15)$

$M_3 = 7 * 15 = 105, M_3' = 13(mod\ 22)$

$x = M_1M_1'b_1 + M_2M_2'b_2 + M_3M_3'b_3 = 15 \times 1 \times 5 + 154 \times 4 \times 12 + 105 \times 13 \times 18(mod\ 2310) \equiv 1272(mod\ 2310)$

Exercise 37

求解同余方程组：$\begin{cases} x \equiv 5(mod\ 9) \\ 3x \equiv 12(mod\ 5) \\ 4x \equiv 18(mod\ 7) \end{cases}$

Answer of exercise 37

答：

先看 $3x \equiv 12(mod\,5)$ 的解，由于 $gcd(3,5)=1$，所以 $x \equiv 12 \times 3^{\varphi(5)-1} \equiv 12 \times 3^3 \equiv 324 \equiv 4(mod\,5)$

再看 $4x \equiv 18(mod\ 7)$ 的解，由于 $gcd(4,7)=1$，所以 $x \equiv 4 \times 18^{\varphi(7)-1} \equiv 4 \times 18^5 \equiv 1(mod\ 5)$

也可以直接化简为以下方程组。

方程组等价于：

$\begin{cases} x \equiv 5(mod\ 9) \\ x \equiv 4(mod\ 5) \\ x \equiv 1(mod\ 7) \end{cases}$

由于 9,5,7 两两互素，根据中国剩余定理计算可得 x=239.

Exercise 38

有总数不满 50 人的一队士兵，一至三报数，最后一人报一，一至五报数，最后一人报二，一至七报数，最后一人报二，这支队伍共有士兵多少人。

Answer of exercise 38

答：

根据题意列出方程：

$$\begin{cases} x \equiv 1(mod\ 3) \\ x \equiv 2(mod\ 5) \\ x \equiv 2(mod\ 7) \end{cases}$$

3,5,7 两两互素，根据中国剩余定理，$m = 3 \times 5 \times 7 = 105, M_1 = 35, M_1' = 2, M_2 = 21, M_2' = 1, M_3 = 15, M_3' = 1, x \equiv 35 \times 2 \times 1 + 21 \times 1 \times 2 + 15 \times 1 \times 2 \equiv 142 \equiv 37(mod\ 105)$

Chapter 4

二次剩余

Exercise 39

求模 23 的二次剩余和非二次剩余

Answer of exercise 39

答：

23 的一个完全剩余系为 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23，依次计算 $i^2(mod\ 23)$，计算结果组成的集合就是模 23 二次剩余组成的集合，完全剩余系中不包含在此集合中的元素就是非二次剩余。

$1^2 = 1(mod23), 2^2 = 4(mod23), 3^2 = 9(mod23), 4^2 = 16(mod23)$

$5^2 = 2(mod23), 6^2 = 13(mod23), 7^2 = 3(mod23), 8^2 = 18(mod23)$

$9^2 = 12(mod23), 10^2 = 8(mod23), 11^2 = 6(mod23), 12^2 = 6(mod23)$

$13^2 = 8(mod23), 14^2 = 12(mod23), 15^2 = 18(mod23), 16^2 = 3(mod23)$

$17^2 = 13(mod23), 18^2 = 2(mod23), 19^2 = 16(mod23), 20^2 = 9(mod23)$

$21^2 = 4(mod23), 22^2 = 1(mod23), 23^2 = 0(mod23)$

二次剩余为 0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18

非二次剩余 5，7，10，11，14，15，17，19，20，21，22

Exercise 40

求满足方程 $E : y^2 \equiv x^2 - 2x + 1(mod\ 7)$ 的所有点。

Answer of exercise 40

答：

首先观察方程的左边是 $y^2(mod\ 7)$ 的形式，其最终结果是模 7 的二次剩余，我们计算模 7 的二次剩余，可知为：0，1，2，4。

$1^2 = 1(mod7), 2^2 = 4(mod7), 3^2 = 2(mod7), 4^2 = 2(mod7), 5^2 = 4(mod7), 6^2 = 1(mod7), 7^2 = 0(mod7)$

$(7k)^2 \equiv 0(mod\ 7), (7k + 1or6)^2 \equiv 1(mod\ 7), (7k + 3or4)^2 \equiv 2(mod\ 7), (7k + 2or5)^2 \equiv 4(mod\ 7)$

以上方程等价于：

$x^2-2x+1 \equiv 0(mod\ 7)$ or $x^2-2x+1 \equiv 1(mod\ 7)$ or $x^2-2x+1 \equiv 2(mod\ 7)$ or $x^2-2x+1 \equiv 4(mod\ 7)$,

对这四个同余式进一步变形，得

$(x-1)^2 \equiv 0(mod\ 7)$ or $(x-1)^2 \equiv 1(mod\ 7)$ or $(x-1)^2 \equiv 2(mod\ 7)$ or $(x-1)^2 \equiv 4(mod\ 7)$, 根据模 7 的二次剩余，进一步知道：

$x \equiv 1(mod\ 7), x \equiv 9(mod\ 7), x \equiv 4(mod\ 7), x \equiv 6(mod\ 7)$

所以满足以上方程的点为 (0,1)(1,9)(6,9)(3,4)(4,4)(2,6)(5,6) 只要对应的 y 和 x 于这些点同余就满足方程。

Exercise 41

利用欧拉判别条件判断 2 是否是 29 的二次剩余。

Answer of exercise 41

答：

29 是奇素数，gcd(2,29)=1，根据欧拉判别条件 $a^{\frac{p-1}{2}} = 2^{\frac{29-1}{2}} = 2^14 = 16384 \equiv -1(mod\ 29)$, 所以 2 不是 29 的二次剩余。

Exercise 42

利用勒让德符号判断 2 是否是 73 的二次剩余。

Answer of exercise 42

答：

73 为奇素数，根据书中定理我们有

$$(\frac{2}{73}) = \begin{cases} 1, if\ p \equiv \pm 1(mod\ 8) \\ -1, if\ p \equiv \pm 3(mod\ 8) \end{cases},$$

$\because 73(mod\ 8) \equiv 1, \therefore (\frac{2}{73}) = 1$,2 是 73 的二次剩余。

Exercise 43

计算勒让德符号 $(\frac{17}{37})$.

Exercise 44

计算勒让德符号 $(\frac{37}{25411})$(备注：25411 为素数)

Answer of exercise 44

答：

$gcd(37, 25411) = 1$

根据二次互反定律，我们有：

$\left(\frac{37}{25411}\right) = (-1)^{\frac{37-1}{2}\frac{25411-1}{2}}(\frac{25411}{37}) = (\frac{29}{37}) = (-1)^{\frac{29-1}{2}\frac{37-1}{2}}(\frac{37}{29}) = (\frac{8}{29})$, 然后可以根据二次剩余的定义，知 $(\frac{8}{29}) = 8^{\frac{29-1}{2}}(mod\ 29) \equiv 28 \equiv -1(mod\ 29)$

Chapter 5

原根与指数

Exercise 45

34 对模 37 的次数是多少？

Answer of exercise 45

答：

解法一：可以按照定义去求，遍历一个完全系：$34^0 = 134^1 = 34, 34^2 = 9, 34^3 = 10, 34^4 = 7, 34^5 = 16, 34^6 = 26, 34^7 = 33, 34^8 = 12, \underline{34^9 = 1}, 34^{10} = 34, 34^{11} = 9, 34^{12} = 10, 34^{13} = 7, 34^{14} = 16, 34^{15} = 26, 34^{16} = 33, 34^{17} = 12, \underline{34^{18} = 1}, 34^{19} = 34, 34^{20} = 9, 34^{21} = 10, 34^{22} = 7, 34^{23} = 16, 34^{24} = 26, 34^{25} = 33, 34^{26} = 12, \underline{34^{27} = 1}, 34^{28} = 34, 34^{29} = 9, 34^{30} = 10, 34^{31} = 7, 34^{32} = 16, 34^{33} = 26, 34^{34} = 33, 34^{35} = 12, 34^{36} = 1$

由计算结果可知 34 对模 37 的次数为 9.

解法二：

可以证明，$ord_m(a) \mid \varphi(m)$，所以，37 的欧拉函数是 36，6 的所有因子是 1, 2, 3, 4, 6, 9, 12, 18, 36，依次计算 $a^l (mod\ 37), l \in 1, 2, 3, 4, 6, 9, 12, 18, 36,$ 结果为 1 的 l 最小取值为次数。

Exercise 46

判断 47，55，59 的原根是否存在。若存在，求出其所有原根。

Answer of exercise 46

答：

47 是奇素数，根据定理，我们知道 47 的原根存在。

55 的标准分解式 5×11，根据定理其不是 $2, 4, p^l, 2p^l$ 的形式，故 55 没有原根。

59 是奇素数，根据定理，我们知道 59 的原根存在。

Exercise 47

求 47 所有原根。

Answer of exercise 47

答：

47 是奇素数，根据定理，我们知道 47 的原根存在。

$\varphi(47) = 46$,46 的标准分解式为 2×23,46 互素的因子 g 为 3，5，7，9，...，计算 g^{23}, g^2：

$3^{23} \equiv 1, 3^2 \equiv 9$,3 不是原根

$4^{23} \equiv 1, 4^2 \equiv 16$,4 不是原根

$5^{23} \equiv 46, 5^2 \equiv 25$,5 是原根

5^l，l 遍历 46 的缩系，{ 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45 }，得到所有原根为 { 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45 }.

Chapter 6

编程练习

Exercise 48

编写程序计算两个大数 (任意精度) 的四则运算 $(+, -, \times, \div)$, 模运算。注：32 位系统，C 语言长整型为 $2^{32} - 1 = 4294967295$，64 位系统是 $2^{64} - 1$.

Exercise 49

编程实现埃拉托色尼 (Eratosthenes，古希腊数学家) 筛选法寻找素数，按一定的步长计算一系列不同范围内的素数 (500∼1000000)，并记录算法所用时间，并画出不同范围时算法所用时间的变化曲线。注：不同范围搜寻的时间可以以一定的格式写到文本文件中，比如 34,500 < 换行 >，每一个搜寻范围形成这样一行数据，然后将这个数据文件导入 excel，用 excel 生成图形。

Exercise 50

利用 C 语言已有的运算，编写程序计算两个数的最大公约数。

Exercise 51

利用 GMP 实现任意精度的两个数的最大公约数的求解。

Exercise 52

编程判断两个数是否互素。

Exercise 53

1858 年法国密码学家维吉尼亚提出一种以移位替换为基础的周期替换密码,c 称为 Vigenère Cipher，这种密码是多表替换密码的一种。令英文字母 a,b,⋯,z 对应于从 0 到 25 的整数，明文是 n 个字母组成的字符串，即 $M = m_1m_2m_3m_4 \dots m_n$，密钥也是一个字符串 $K = k_1k_2 \dots k_q$，通常短一些，加密后的密文 $C = c_1c_2 \dots c_n$，$c_i = m_i + k_i \ (mod\ 26)$，如果 $q < n$，将密钥进行周期性延展，解密为 $m_i = c_i - k_i (mod\ 26)$。

编写程序实现 Vigenère 加解密。

Exercise 54

编写程序计算 22345680 的标准分解式。

Exercise 55

编写程序实现求解一个整数的标准分解，同时在分解完成后，输出分解所用的时长。

Exercise 56

编写程序实现输入范围的素数生成，并且明确程序有能力求解的范围。

Exercise 57

编程判断同余方程 $ax \equiv b(mod\ m)$ 是否有解，如果有解，求出所有的解。

Exercise 58

编写程序实现利用中国剩余定理求解同余方程组。