参考答案

第 1 章　整数的可除性

一、判断题

1.× 2. √ 3.× 4. √ 5. √ 6. √ 7. √ 8.× 9.× 10.×

二、综合题

1.101 是素数。

2.（1）5　（2）2　（3）13

3.23

4. a=4, b=1, c=-4

方法：欧几里得算法

96=72+24

72=24×3

24=96-72

108=24×4+12

24=12×2

12=108-24×4

12=108-(96-72)×4

12=108-96×4+72×4

因此得 a=4,b=1,c=-4

5. x=8, y=-7

6. s=3, t= -8

7.S=3，t= -4

8.1225=5^2×7^2

9.600=2^3×3×5^2

10.1176=2^3×3×7^2

11. (1)539 (2)1014

第二章 同余

一、判断题

1.× 2.×3. √ 4. ×5. ×

二、综合题

1. 40

55 的简化剩余系中元素个数等于 55 的欧拉函数，

$$\varphi(55)=\varphi(5\times 11)=4\times 10=40$$

2.由欧拉定理和模的性质得：16

计算$5^{30}(\bmod 23)$

因为(5,23)=1，根据欧拉定理可知

$$5^{\varphi（23）}\equiv 1\equiv 5^{22}(\bmod 23)$$

因此

$$5^{30} \equiv 5^{22+8} \equiv 5^8 \equiv (5^2)^4 \equiv (5^2(\text{mod } 23))^4 \equiv (2)^4 \equiv 16(\text{mod } 23)$$

3. 3000×(1-1/2)(1-1/3)×(1-1/5)=800
4. 由欧拉定理和模重复平方法得 36

$$7^{1000}(\text{mod } 47)$$

因为(7,47)=1，根据欧拉定理可知

$$7^{\varphi(47)} \equiv 1 \equiv 7^{46}(\text{mod } 23)$$

因此

$$7^{1000} \equiv 7^{1000\,(\text{mod}\varphi(47))} \equiv 7^{34\,(\text{mod}46)} \equiv 7^{1000\,(\text{mod}46)} \equiv \left(7^2(\text{mod } 47)\right)^{17}$$

$$\equiv (2)^{17}(\text{mod } 47)$$

用模重复平方法 $17=10001_2$

$2^2 \equiv 4 \quad 2^{2^2} \equiv 2^4 \equiv 4 \times 4 \equiv 16 \quad 2^{2^3} \equiv 2^8 \equiv 16 \times 16 \equiv 21$

$2^{2^3} \equiv 2^{16} \equiv 21 \times 21 \equiv 9 \times 49 \equiv 9 \times 2 \equiv 18$（mod 47）

$(2)^{17} \equiv 2^{16+1} \equiv 2^{16} \times 2 \equiv 18 \times 2 = 36(\text{mod } 47)$

5. 15(mod 22)
6. -127 (或者 413) (mod 540)
设p, q是两个不同的奇素数，$n = pq, e$是与pq互素的整数．如果整数e满足$1 < e < \varphi(n), (e, \varphi(n)) = 1$，那么存在整数$d$，使得$ed \equiv 1(\text{mod } \varphi(n))$．假设$p = 19$，$q = 31$，$e = 17$, 求$d$。
解析：$\varphi(n) = \varphi(p \times q) = (p-1)(q-1) = (19-1)(31-1) = 18 \times 30 = 540$

$$ed \equiv 17d \equiv 1(\text{mod } 540)$$

540=17×31+13　　17=13+4　　13=4×3+1

1=13-4×3=13-(17-13)×3=13×4-17×3=(540-17×31)×4-17×3
=540×4-17×127

两边同模 540 可得：

$17 \times (-127) \equiv 1(\text{mod } 540)$

$\text{d} \equiv (-127) \equiv -127 + 540 \equiv 413(\text{mod } 540)$

7. 证明：设十进制整数n=$a_k a_{k-1} \dots a_1 a_0$，则
（1）$11|n$当且仅当 $11|(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)$;
（2）$4|n$当且仅当 $4|a_1 a_0$;
（3）$8|n$当且仅当 $8|a_2 a_1 a_0$.
解析：$n = a_k a_{k-1} \dots a_1 a_0 = a_k \times 10^k + a_{k-1} \times 10^{k-1} + \cdots + a_1 \times 10 + a_0$.
n(mod 11) $\equiv a_k \times 10^k + a_{k-1} \times 10^{k-1} + \cdots + a_1 \times 10 + a_0$(mod 11)
$\equiv a_k \times (-1)^k + a_{k-1} \times (-1)^{k-1} + \cdots + a_1 \times (-1) + a_0$(mod 11)
k 为偶数，$(-1)^k \equiv 1(\text{mod } 11)$
k 为奇数 $(-1)^k \equiv -1(\text{mod } 11)$

$$n(\text{mod } 11) \equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)(\text{mod } 11).$$

因此$11|n$ ，$n(\text{mod } 11) \equiv (a_0+a_2+\cdots)-(a_1+a_3+\cdots) \equiv 0(\text{mod } 11)$.
$11|(a_0+a_2+\cdots)-(a_1+a_3+\cdots)$
（2），（3）证明类似

9. 利用 Miller-Rabin 算法判断 1001 是否素数.

解析：$1001-1=2^3\times125$，即s=3，t=125.

若取$b=2$，则$2^t=2^{125}(\text{mod } 1001)\equiv32$；$(b^t)^2\equiv23(\text{mod } 1001)$，
$(b^t)^{2^2}\equiv23^2\equiv529(\text{mod } 1001)$

结论：1001 是合数。

第三章 一次同余方程

一、选择题

1.C 2.D 3.B 4.C 5.A

二、综合题

1. 求 40 模 31 的乘法逆元.

解析：$40x\equiv1(\text{mod } 31)$
$9x\equiv1(\text{mod } 31)$
31=9×3+4 9=4×2+1
1=9-4×2=9-（31-9×3）×2=9×7-31×2
等式两边同时模 31
$9\times7\equiv1(\text{mod } 31)$
40 模 31 的逆元为 $x\equiv7(\text{mod } 31)$

2. 解方程$91x\equiv35(\text{mod } 133)$.
解析：91×x≡35（mod 133）
(91,133)=7|35，有解，有 7 个解
91/7 ×x≡1(mod 19)
13×x≡1(mod 19)
19=13+6
13=6×2+1
1=13-6×2
1=13-(19-13)×2
1=13×3-19
等式两边同时模 19
得 x≡3(mod19) 因而同余 13×x≡5（mod19）的解 x≡3×5≡15(mod19)
全解 x≡15+19×t （mod 133）(t=0,1,2,3,4,5,6)

3. 方法同上 同余方程解为 x ≡ 11(mod23) 全解为： x ≡ 11+23t(mod 161)(t=0,1,2,3,4,5,6)

4. 求解一次同余方程 $12\times7^{168}x\equiv9\text{mod}27$.

解析：（7,27）=1 ，φ（27）=18　　$7^{168}=7^{(9\times18+6)}$

原式得：12×（7^6）×x≡9(mod27)

7^2≡22(mod 27)　（7^2）^{3}≡-5×-5 ×-5≡-2×-5≡10

12×10×x≡9(mod27)

12×x≡9(mod27)

(12,27)=3|9,所以方程有解,有 3 个解

1）先求解计算$\frac{a}{(a,m)}x\equiv1(\mathrm{mod}\,\frac{m}{(a,m)})$的解，即 $4x\equiv1\,mod\,9$

采用欧几里得扩展算法　9=4×2+1

求得的解为$x\equiv x_0(\mathrm{mod}\,\frac{m}{(a,m)})$，为 $x\equiv-2\equiv7(\mathrm{mod}\,9$）

2）写出方程$\frac{a}{(a,m)}x\equiv\frac{b}{(a,m)}(\mathrm{mod}\,\frac{m}{(a,m)})$的解为$x\equiv3\times7(\mathrm{mod}\,9)$.

3）写出方程$ax\equiv b(\mathrm{mod}\,m)$的全部解为

$x\equiv3+9t(mod\,27)$，$t=0,1,2.$

3 个解：$x\equiv3(mod\,27)$　$x\equiv12(mod\,27)$　$x\equiv21(mod\,27)$

5. 解一次同余方程组

$$\begin{cases}x\equiv2(\mathrm{mod}\,5)\\x\equiv5(\mathrm{mod}\,11).\\x\equiv3(\mathrm{mod}\,17)\end{cases}$$

解析：M=5×11×17=935

M_1=187　　M_2=85　M_3=55

187=5×37+2

5=2×2+1

1=5-2×2

1=5-2×（187-5×37）

1=5-2×187+2×5×37

1=5×(1+2×37)-2×187

M_1^{-1}≡-2(mod 5)≡3(mod 5)

同理得：　M_2^{-1}≡7(mod 11)

M_3^{-1}≡13(mod 17)

全解为：x≡187×3×2+85×7×5+55×13×3≡632（mod 935）

6. 原式化解得：

x≡4(mod 17)

x≡7(mod 11)

由中国剩余定理得：M_1^{-1}≡14(mod 17)

M_2^{-1}≡2(mod 11)

x≡106(mod187)

7. 求下面同余方程组的解

$$\begin{cases}3x+y\equiv 7(\mathrm{mod}\ 23)\\ x+2y\equiv 6(\mathrm{mod}\ 23)\end{cases}.$$

解析：6x+2y≡14(mod23)

x+2y ≡6(mod23)

相减得： 5x≡8(mod23)

求解得：x≡20(mod23)

求解 2y ≡-14 ≡9(mod23)

解得：y≡16(mod 23)

第四章 二次同余

一、选择题

1.C 2.A 3.B

二、综合题

1.（151/373）= -1

2. 判断判断$11x^2\equiv -3(\mathrm{mod}\ 91)$是否有解。

解题思路：可以用勒让得符号，也可以用欧拉判别

$$11x^2\equiv -3(\mathrm{mod}\ 7\times 13)$$

因此等价于方程组

$$\begin{cases}11x^2\equiv 4x^2\equiv -3(\mathrm{mod}\ 7)\\ 11x^2\equiv -3(\mathrm{mod}\ 13)\end{cases}$$

$4\times 4^{-1}x^2\equiv x^2\equiv 4^{-1}\times -3(\mathrm{mod}\ 7)$

$11\times 11^{-1}x^2\equiv x^2\equiv 11^{-1}\times -3(\mathrm{mod}\ 13)$

7=4+3 4=3+1 1=4-3=4-(7-4)=4×2-7

$4^{-1}\equiv 2(\mathrm{mod}7)$

同理 13=7+6 7=6+1 1=7-6=7-（13-7）=7×2-13

$11^{-1}\equiv 2(\mathrm{mod}13)$

方程组化简为 $x^2\equiv 4^{-1}\times -3\equiv -6=1(\mathrm{mod}\ 7)$ 有解

$x^2\equiv 11^{-1}\times -3\equiv -6\equiv 7(\mathrm{mod}\ 13)$ 无解

或者

$11x^2\equiv -3(\mathrm{mod}\ 91)$等价于 $11x^2\equiv 88(\mathrm{mod}\ 91)$，因（11，91）=1

故去判断$x^2\equiv 8(\mathrm{mod}\ 91)$

等价于判断方程组

$$\begin{cases}x^2\equiv 1(\mathrm{mod}\ 7)\\ x^2\equiv 8(\mathrm{mod}\ 13)\end{cases}$$

容易知道$x^2\equiv 8(\mathrm{mod}\ 13)$无解

3. 判断方程$x^2\equiv 111(\mathrm{mod}\ 71)$是否有解。

解析：方程有解

$x^2 \equiv 111 \equiv 40 (\mathrm{mod}\ 71)$

解题思路：可以用勒让得符号，也可以用欧拉判别

4. 判断二次同余方程$x^2 \equiv 360 (\mathrm{mod}\ 2011)$解的情况。

解析：方程无解

解题思路：可以用勒让得符号，也可以用欧拉判别

2011 是奇素数，用勒让得符号判断方程有解还是无解

$$\left(\frac{360}{2011}\right) = \left(\frac{6^2 \times 5 \times 2}{2011}\right)$$

$$\left(\frac{6^2}{2011}\right) = 1$$

$$\left(\frac{2}{2011}\right) = (-1)^{\frac{2011^2-1}{8}} = -1$$

$$\left(\frac{5}{2011}\right) = (-1)^{\frac{5-1}{2}\times\frac{2011-1}{2}}\left(\frac{2011}{5}\right) = \left(\frac{2011}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$$\left(\frac{360}{2011}\right) = 1 \times -1 \times 1 = -1$$

所以二次同余方程无解

5. 判断$x^2 \equiv 99 (\mathrm{mod}\ 323)$是否有解。

解析：方程无解

323=17×19 不是素数，若$x^2 \equiv 99 (\mathrm{mod}\ 323)$有解

必须满足$x^2 \equiv 99 (\mathrm{mod}\ 17)$

$x^2 \equiv 99 (\mathrm{mod}\ 19)$

必须同时有解

则判断

$$\left(\frac{99}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{7 \times 2}{17}\right)$$

$$\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = 1$$

$$\left(\frac{7}{17}\right) = (-1)^{\frac{7-1}{2}\times\frac{17-1}{2}}\left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = (-1)^{\frac{7-1}{2}\times\frac{3-1}{2}}\left(\frac{7}{3}\right) = -1 \times \left(\frac{1}{3}\right) = -1$$

$x^2 \equiv 99 (\mathrm{mod}\ 17)$ 无解

因此$x^2 \equiv 99 (\mathrm{mod}\ 323)$无解

第 5 章 原根和离散对数

一、判断题

1~5. ×××××

二、综合题

1. 已知 6 是模 41 的原根, $9=6^{30}$(mod 41),求$ord_{41}(9)$.
   解：6 是模 41 的原根，因此可知$\varphi(41) = 40$, $6^{40}\equiv1$(mod 41)　$9\equiv6^{30}$(mod 41)
   $1\equiv(6^{40})^{3}\equiv(6^{30})^{4}$(mod41),因此$ord_{41}(9)=4$

2. 写出模 5 的全部原根.
   解：5 是素数，肯定有原根，原根个数 $\varphi(\varphi(5))=\varphi(4)=2$. 5 是比较小素数，因此可以用穷举方法进行求解原根

   5 的简化剩余系为{1,2,3,4,}，且计算可得
   $1^1\equiv1$;
   $2^1\equiv2$, $2^2\equiv4$, $2^3\equiv3$, $2^4\equiv1$;
   $3^1\equiv3$, $3^2\equiv4$, $3^3\equiv2$, $3^4\equiv1$;
   $4^1\equiv4$, $4^2\equiv1$;
   因此根据原根定义，可知 2 和 3 是模 5 的原根。

3. 已知模 22 的原根存在, 求出模 22 的所有原根.
   解：22=2×11，满足 2 形式，原根肯定存在。原根个数为 $\varphi((22))=\varphi(10)=4$
   22 为偶数，因此不能用 2.8.1 定理。根据相关定理可知阶为 $\varphi((22)$的因子，即（1,5,10）
   （2,22）不互素，因此，
   从先判断g=3 是否为模 22 的原根，因 3^5(mod22)≡1. 所以 3 不是模 22 的原根. 5^5(mod22)≡1. 7^5(mod22)≡-1，因此 7 是模 22 的原根
   因此模 22 的所有原根 7^d,其中d为模 10 的简化剩余系{1,3,7,9}。模 22 的所有原根为：
   $7^1\equiv7$,　$7^3\equiv13$, $7^7\equiv17$, $7^9\equiv19$(mod22).
   即模 22 的所有 4 个原根为 7,13,17,19
4. 与第 3 题类似，略

5. 已知 5 对模 17 的阶为 16, 列出所有模 17 阶为 8 的整数 a(0<a<17).
   解：$\varphi(17)=16$, $5^{16}\equiv1$(mod17)。
   $ord_{17}(a)=8$，即$a^8\equiv1$(mod 17)　　$a^8\equiv1\equiv5^{16}\equiv(5^2)^8$(mod 17)
   5 是模 17 的原根，ord17(5)=16，因此ord17(5^2)=8

   因此所有模 17 阶为 8 的整数a为（a,16）=2 的 5^a，
   即 $5^2\equiv8$(mod 17)，$5^6\equiv2$(mod 17)，$5^{10}\equiv9$(mod 17)，$5^{14}\equiv15$(mod 17)，
   模 17 的阶为 8 的整数 a 为 2, 8, 9, 15

6. 略
7. 略

8. 已知$m=13^3$ 的原根存在, 求模m的原根有多少个？
   解：原根个数为$\varphi(\varphi(13^3))=\varphi(13^3\times(1-1/13))=\varphi(13^2\times12)=\varphi(13^2\times2^2\times3)$

$=13^2\times2^2\times3\times(1-1/13)(1-1/2)(1-1/3)=624$

9. 解：原根个数为$\varphi(\varphi(101))=\varphi(100)=\varphi(2^2\times5^2)=100\times(1-1/2)(1-1/5)=40$

10. 已知$ord_{41}(18)=5$,快速求 $18^{18}(mod41)$.

解：$ord^{41}(18)=5$，$18^5\equiv1$（mod 41）

$18^{18}\equiv18^{5\times3+3}\equiv18^3(mod41)\equiv18^2\times18\equiv37\times18\equiv10(mod41)$

第 6 章 近世代数基础

3. 可约多项式

$x^5+x+1=(x^2+x+1)(x^3+x^2+1)$, 可约

4. 不可约多项式

$x^5+x^2+1=x(x^4+x)+1$，

$x^5+x^2+1=(x+1)(x^4+x^3+x^2)+1$，

$x^5+x^2+1=(x^2+x+1)(x^3+x^2)+1$

因此 x^5+x^2+1 为不可约多项式，

5. 不可约，这就是高级加密标准选用的不可约多项式

6. (1)加法单位元为 0,乘法单位元为 1. (2) x^3+x+1. (3) x^3+x^2+1.

解析：（1）$F_2[x]/\ x^4+x+1$的余式构成一个有限域F，加法单位元为 0，，乘法单位元为 1。

（2）$(x^2+1)\times(x^3\ +1)\equiv x^5+x^3+x^2+1\equiv x(x^4+x+1)+x^2+x++x^3+x^2+1\equiv x^3+x+1(\mathrm{mod}\,x^4+x+1)$

（3）$(x^2)^{-1}(\mathrm{mod}\,x^4+x+1)$求多项式逆元，可采用欧几里德的多项式方法求解

$x^4+x+1=x^2\times(x^2)+(x+1)$

$x^2=(x+1)(x+1)+1$

$1=x^2-(x+1)(x+1)$

$1=x^2-(x+1)\big((x^4+x+1)-x^2\times x^2\big)$

$1=x^2-(x+1)\big((x^4+x+1)-x^2\times x^2\big)$

$1=x^2(1+(x+1)x^2)-(x+1)(x^4+x+1)$

$1=x^2(1+x^3+x^2)-(x+1)(x^4+x+1)$

等式两边模多项式x^4+x+1

$x^2(1+x^3+x^2)\equiv1(\mathrm{mod}(x^4+x+1))$

$(x^2)^{-1}\equiv x^3+x^2+1(\mathrm{mod}\,x^4+x+1)$

7. $(x^3)^{-1}=(x^3+x^2+x+1)(\mathrm{mod}\ g(x))$

解析：$x^4+x+1=x\times x^3+(x+1)$

$x^3 = (x+1)(x^2+x+1)+1$

$1 = x^3 - (x+1)(x^2+x+1)$

$1 = x^3 - \big((x^4+x+1) - (x \times x^3)\big)(x^2+x+1)$

$1 = x^3(1 + x(x^2+x+1)) - (x^4+x+1)(x^2+x+1)$

等式两边模多项式x^4+x+1

$(x^3+x^2+x+1) \times x^3 \ \equiv 1(\bmod g(x))$

$f(x) = x^3+x^2+x+1$

第 7 章 椭圆曲线基础

2.(5,2)

3.(2,4,)

4. (5,2)

5.略

6.(1) (0010, 1101) (2)(1111,0100)