信安数学基础（第二版）1-6 章课后习题答案

第一章

（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.方法：欧几里得算法
x=8,y=-7
6.s=3,t= -8
7.由欧几里得算法得：
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
12. 略

第二章

（一）判断题

1× 2.×3. √ 4. ×5. √

（二）综合题

1.55 的简化剩余系中元素个数等于 55 的欧拉函数，$\varphi(55)=\varphi(5*11)=4*10=40$

2.由欧拉定理和模的性质得：16

$$5^{30}(\bmod\ 23)$$

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

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

3.由欧拉函数定理计算的欧拉函数800：3000=2^3*5^3*3=3000*(1-1/3)*(1-1/2) *(1-1/5)=800:

4.由欧拉定理和模重复平方法得 36

$$7^{1000}(\bmod\ 47)$$

因为(7,47)=1，根据欧拉定理可知

$$7^{\varphi（47）}\equiv 1\equiv 7^{46}(\bmod\ 47)$$

因此

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

用模重复平方法 $17=10001_2$

$2^2\equiv 4\quad 2^{2^2}\equiv 2^4\equiv 4*4\equiv 16\quad 2^{2^3}\equiv 2^8\equiv 16*16\equiv 21\quad 2^{2^3}\equiv 2^{16}\equiv 21*21\equiv 9*49\equiv 9*2\equiv 18$（mod 47）

$(2)^{17}\equiv 2^{16+1}\equiv 2^{16}*2\equiv 18*2=36(\bmod\ 47)$

5、

$$5^{28}(\bmod\ 22)$$

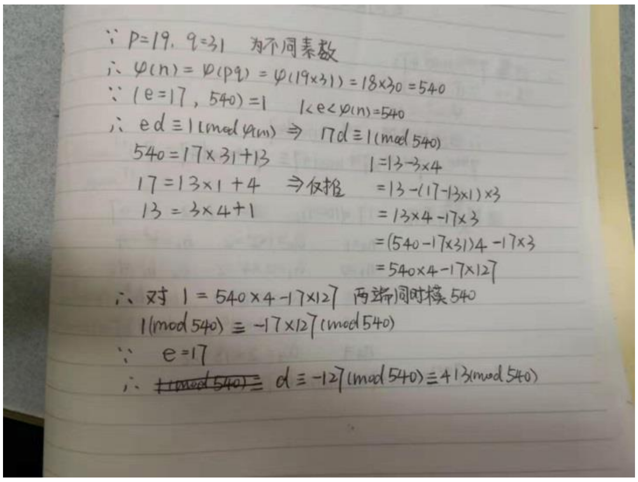
因为(5,22)=1，根据欧拉定理可知

$$5^{\varphi（22）}\equiv 5^{\varphi（2*11）}\equiv 5^{10}\equiv 1(\bmod\ 22)$$

因此

$$5^{28}(\bmod\ 22)\equiv 5^{28\ (\bmod\varphi(22))}\equiv 5^{10*2+8\ (\bmod 10)}\equiv 5^{8}\equiv \left(5^{2}(\bmod\ 22)\right)^{4}\equiv 27*3\equiv 5*3$$
$$\equiv 15(\bmod\ 22)$$

6、413



∵ $p=19,\ q=31$ 为不同素数

∴ $\varphi(n)=\varphi(pq)=\varphi(19\times 31)=18\times 30=540$

∵ $(e=17,\ 540)=1$ $\quad 1<e<\varphi(n)=540$

∴ $ed\equiv 1(\mathrm{mod}\ \varphi(n)) \Rightarrow 17d\equiv 1(\mathrm{mod}\ 540)$

$540=17\times 31+13$ $\qquad 1=13-3\times 4$

$17=13\times 1+4$ ⇒ 反推 $\quad =13-(17-13\times 1)\times 3$

$13=3\times 4+1$ $\qquad =13\times 4-17\times 3$

$=(540-17\times 31)4-17\times 3$

$=540\times 4-17\times 127$

∴ 对 $1=540\times 4-17\times 127$ 两端同时模 540

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

∵ $e=17$

∴ $\cancel{1(\mathrm{mod}\ 540)\equiv}$ $d\equiv -127(\mathrm{mod}\ 540)\equiv 413(\mathrm{mod}\ 540)$

7、（1）证明: $n=a_k a_{k-1}\dots a_1 a_0=a_k\times 10^k+a_{k-1}\times 10^{k-1}+\cdots+a_1\times 10+a_0$.

若 i 为偶数，$10^i\equiv 1(\mathrm{mod}\ \ 11)$ 若 i 为奇数，$10^i\equiv -1(\mathrm{mod}\ \ 11)$

已知 11|n，因此 $n\ \equiv 0(\mathrm{mod}\ \ 11)$

因此 $n(\mathrm{mod}\ 11)\equiv a_k\times 10^k+a_{k-1}\times 10^{k-1}+\cdots+a_1\times 10+a_0(\mathrm{mod}\ 11)$

$$\equiv a_k\times(-1)^k+a_{k-1}\times(-1)^{k-1}+\cdots-a_3+a_2-a_1+a_0(\mathrm{mod}\ 11)$$

$$\equiv(a_0+a_2+\cdots)-(\ a_1+a_3+\cdots)\equiv 0(\mathrm{mod}\ 11).$$

故得证。

(2)、（3）证明类似，略

8 与六证明方法类似，略

9. 略

第三章

（一）选择题

1.C　2.D　3.B　4.C　5.A

（二）综合题

1. 解：由欧几里得定理得 7

$40^{-1}\ \equiv(40(\mathrm{\ mod\ }31))^{-1}\ \equiv 9^{-1}\ (\mathrm{mod}\ 31)$

实际等价于解一次同余方程 9*x≡1（mod 31）

31=9*3+4　9=4*2+1

1=9-4*2=9-（31-9*3）*2=9*7-31*2

两边同模 31 得到 9*7≡1（mod 31）

因此 40 模 31 的逆元为 7

2. 91*x≡35（mod 133）

(91,133)=7|35

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 两遍同时 mod 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(t=0,1,2,3,4,5,6)

3. 91*x≡35（mod 161）
(91=7*13,161=7*23)=7|35
91/7 *x≡1(mod 23)
13*x≡1(mod 23)
23=13+10
13=10+3
10=3*3+1
1=10-3*3
1=10-(13-10)*3=10*4-13*3=（23-13）*4-13*3
1=23*4-13*7 两遍同时 mod 23
得 x≡-7≡16(mod23） 因而同余 13*x≡5（mod23）的解 x≡-7*5≡-12≡11(mod23)
全解为：x≡11+23t（mod 161）(t=0,1,2,3,4,5,6)

5.解法一 （$12\times7^{168}=3*2^2*7^{168}$，$27=3^3$） $=3|9$
方程有解，有 3 个解。
先求解 $4\times7^{168}x\equiv1$（mod 9）
（7,9）=1

$$7^{\varphi（9）}\equiv7^{\varphi（9）}\equiv7^6\equiv1(\mathrm{mod}\ \ 9)$$

因此

$$7^{168}\equiv7^{6*28}\equiv1(\mathrm{mod}\ \ 9)$$

因此 $4\times7^{168}x\equiv4x\equiv1$（mod 9）
9=2*4+1
1=9-2*4
9=4*2+1

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

写出方程$ax\equiv b(\mathrm{mod}\,m)$的全部解为
$x\equiv7*3+9t\equiv21+9t(mod\,27)$，$t=0,1,2.$

即三个解为：$x\equiv21(mod\,27)$ $x\equiv3(mod\,27)$ $x\equiv12(mod\,27)$

解法二 求解 首先可以把大于模式 27 的倍数的给约减掉
（1） $\varphi(27)=18,(7,27)=1,7^{18}\equiv1\ \ (mod\ \ 27)$
168=18*9+6

$12 \times 7^{168}x \equiv 12 \times 7^{18*9+6}x \equiv 12 \times 7^{6}x \equiv 12 \times 49^{3}x \equiv 12x \equiv 9\ \ mod\ \ 27$

（2） (12,9)=3|9 方程有解，有 3 个解

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

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 $x \equiv -2 \equiv 7(\mathrm{mod}\,9)$）

(4) 写出方程$\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)}(\mathrm{mod}\,\frac{m}{(a,m)})$的解为$x \equiv 3 * 7(\mathrm{mod}\,9)$.

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

$x \equiv 3 + 9t(mod\,27)$，$t = 0,1,2.$

即三个解为：$x \equiv 3(mod\,27)$ $x \equiv 12(mod\,27)$ $x \equiv 21(mod\,27)$

5. 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.略

第四章

（一）选择题

1.C 2.A 3.B

（二）综合题

1.（151/373）= -1

解一：151 和 373 都是正奇数，根据二次互反定律$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}\left(\frac{p}{q}\right)$

$$\left(\frac{151}{373}\right)=(-1)^{\frac{151-1}{2}\times\frac{373-1}{2}}\left(\frac{373}{151}\right)=(-1)^{75\times186}\left(\frac{151*2+71}{151}\right)=\left(\frac{71}{151}\right)$$

$$\left(\frac{151}{373}\right)=\left(\frac{71}{151}\right)=(-1)^{\frac{71-1}{2}\times\frac{151-1}{2}}\left(\frac{151}{71}\right)=(-1)\left(\frac{71*2+9}{71}\right)=(-1)\left(\frac{9}{71}\right)=(-1)\left(\frac{3}{71}\right)^2$$

$$\left(\frac{3}{71}\right)=(-1)^{\frac{3-1}{2}\times\frac{71-1}{2}}\left(\frac{71}{3}\right)=(-1)\left(\frac{2}{3}\right)=(-1)(-1)^{\frac{3^2-1}{8}}=1$$

$$\left(\frac{151}{373}\right)=-1$$

解二、$\left(\frac{151}{373}\right)$ 勒让得符号　等价于$x^2\equiv151(mod\,373)$ 无解还是有解，可用欧拉判别

$$151^{\frac{373-1}{2}}\equiv151^{\frac{373-1}{2}}\equiv151^{186}\text{（mod 373）}$$

采用模重复平方或者平方剩余 可得$151^{186}\equiv372\equiv-1$（mod 373）

因此$\left(\frac{151}{373}\right)=-1$

2.方程无解

解：可知 91=7*13,为合数，$11x^2\equiv-3(mod\,91)$ 等价于求解方程组

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

即$x^2\equiv4^{-1}\times-3(mod\,7)$　有解，并且$x^2\equiv11^{-1}\times-3(mod\,13)$ 有解，原二次同余方程$x^2\equiv-3(mod\,91)$才有解。

$x^2\equiv-3*2\equiv1(mod\,7)$，易知二次同余方程有解

13=11+2 11=2*5+1 1=11-2*5=11-（13-11）*5==11*6-13*5

$$11^{-1}\equiv6$$

$x^2\equiv-3*6\equiv8(mod\,13)$ 因为 13 很小，可穷举 13 的平方剩余为 $1^2\equiv1(mod\,13)$　$2^2\equiv4(mod\,13)$　$3^2\equiv9(mod\,13)$　$4^2\equiv3(mod\,13)$　$5^2\equiv12(mod\,13)$　$6^2\equiv10(mod\,13)$

可知 8 是模 13 的平方非剩余　$x^2\equiv-3*6\equiv8(mod\,13)$ 无解

也可以用欧拉判别求解

$$8^{\frac{13-1}{2}}\equiv8^6\equiv((-5)^2)^3\equiv(-1)^3\equiv-1\text{（mod 13）}$$

因此$11x^2\equiv-3(mod\,91)$ 无解

3.方程有解

解：　$x^2\equiv111\equiv40(mod\,71)$

用欧拉判别

$$40^{\frac{71-1}{2}}\equiv40^{35}\text{（mod 71）}$$

用模重复平方法 35=100011_2

$40^2\equiv5^28^2\equiv5^2*-7\equiv-33$　$40^4\equiv33^2\equiv24$　$40^8\equiv24^2\equiv8$　$40^{16}\equiv64\equiv-7$　$40^{32}\equiv49$

$(40)^{35}\equiv40^{32+2+1}\equiv49*(-33)*40\equiv22*33*40\equiv1(\text{mod }47)$

解法二 也可用勒让得符号来求解

$$\left(\frac{40}{71}\right)=\left(\frac{2}{71}\right)^3\left(\frac{5}{71}\right)$$

71mod 8 等于-1，因此 $\left(\frac{2}{71}\right)=1$ 因此

$\left(\frac{40}{71}\right)=\left(\frac{5}{71}\right)=(-1)^{\frac{71-1}{2}\times\frac{5-1}{2}}\left(\frac{71}{5}\right)=\left(\frac{1}{5}\right)=1$

因此方程有解

4.方程无解

解：$x^2\equiv 360(mod\ 2011)$

2011 是素数，用勒让得符号来求解

$$\left(\frac{360}{2011}\right)=\left(\frac{2^3\times 3^2\times 5}{2011}\right)$$

2011mod 8 等于 3，因此 $\left(\frac{2}{2011}\right)=-1$

$$\left(\frac{3}{2011}\right)=(-1)^{\frac{2011-1}{2}\times\frac{3-1}{2}}\left(\frac{2011}{3}\right)=(-1)^{1005}\left(\frac{1}{3}\right)=-1$$

$$\left(\frac{5}{2011}\right)=(-1)^{\frac{2011-1}{2}\times\frac{5-1}{2}}\left(\frac{2011}{5}\right)=(-1)^{1005*2}\left(\frac{1}{5}\right)=1$$

$\left(\frac{360}{2011}\right)=\left(\frac{2^3\times 3^2\times 5}{2011}\right)=\left(\frac{2}{2011}\right)^3\left(\frac{3}{2011}\right)^2\left(\frac{5}{2011}\right)=-1$

因此方程无解

5.方程无解

$$x^2\equiv 99(mod\ 323)$$

323=17*19 合数，等价于求解方程组

$\begin{cases}x^2\equiv 99(mod\ 17)\\x^2\equiv 99(mod\ 19)\end{cases}$ 等价于 $\begin{cases}x^2\equiv 14(mod\ 17)\\x^2\equiv 4(mod\ 19)\end{cases}$

易知 $x^2\equiv 4(mod\ 19)$ 有解

$x^2\equiv 14(mod\ 17)$ 可用欧拉判别

$$14^{\frac{17-1}{2}}\equiv(-3)^8\equiv 9^4\equiv 16\equiv -1\ (\mathrm{mod}\ \ 17)$$

$x^2\equiv 14(mod\ 17)$ 无解，方程组无解，因此$x^2\equiv 99(mod\ 323)$ 无解

6、略

第五章

（一）判断题

1.× 2. × 3. × 4. × 5. ×

（二）综合题

二、综合题

1. 已知 6 是模 41 的原根, $9\equiv 6^{30}$(mod41), 求 $ord_{41}(9)$.

解：6是模41的原根因此可知$\varphi(41)=40$, $6^{40}\equiv 1 \pmod{41}$ $9\equiv 6^{30} \pmod{41}$

$1\equiv 6^{40*3}\equiv 6^{30*4} \ (mod\ 41)$,

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

2. 5的简化剩余系为{1,2,3,4,}，且计算可得

$1^1\equiv 1$;

$2^1\equiv 2$, $2^2\equiv 4$, $2^3\equiv 3$, $2^4\equiv 1$;

$3^1\equiv 3$, $3^2\equiv 4$, $3^3\equiv 2$, $3^4\equiv 1$;

$4^1\equiv 4$, $4^2\equiv 1$;

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$2p^\alpha$形式，原根肯定存在。原根个数为$\varphi(\varphi(22))=\varphi(10)=4$

22为偶数。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不是摸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：

$7^1\equiv 7$, $7^3\equiv 13$, $7^7\equiv 17$, $7^9\equiv 19$(mod22).

即模 22 的所有 4 个原根为 7,13,17,19

4、已知模 26 的原根存在, 求出模 26 的所有原根.

方法类似，

解：26=2*13，满足$2p^\alpha$形式，原根肯定存在。原根个数为$\varphi(\varphi(26))=\varphi(12)=4$

26为偶数，根据相关定理可知阶为$\varphi(26)$的因子，即（1,2,3,4,6,12）

从先判断g=3是否为模26的原根，因3^3(mod26)≡1. 所以3不是摸26的原根.

5^2(mod26)≡-1. 5^4(mod26)≡1，所以5不是摸26的原根.

7^6(mod26)≡-1.因此7是模22的原根

因此模26的所有原根7^d,其中d为模12的简化剩余系{1,5,7,11}。

模22的所有原根为：

$7^1 \equiv 7$, $7^5 \equiv 11$, $7^7 \equiv 19$, $7^{11} \equiv 15 \pmod{26}$.

即模 26 的所有 4 个原根为 7,11,15,19

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: 5 对模 17 的阶为 16，可知 5 是模 17 的一个原根，根据定理可知，$0 < a < 17$，

$$a = 5^x$$

则 $\mathrm{ord}_{17}(5^x)=\frac{\mathrm{ord}_{17}(5)}{(\mathrm{ord}_{17}(5),x)}$=8，即, $(\mathrm{ord}_{17}(5), x)$=（16，x）=2, 与与 16 的最大公约数为 2 的，x=2,6,10,14.

$5^2 \equiv 8 \pmod{17}$，$5^6 \equiv 2 \pmod{17}$，$5^{10} \equiv 9 \pmod{17}$ $5^{14} \equiv 15 \pmod{17}$

即所求的整数有 2,8,9,15

6、已知 6 对模 41 的阶为 40, 列出所有模 41 阶为 8 的整数$a(0 < a < 41)$.

与上一题方法类似，

$\frac{40}{(40,x)}$=8 $(40, x) = 5$，x=5,15,25,35

$6^5 \equiv 27 \pmod{41}$，$6^{15} \equiv 3 \pmod{41}$，$6^{25} \equiv 14 \pmod{41}$ $6^{35} \equiv 38 \pmod{41}$

整数 a 为：3,14,27,38

7、已知 6 对模 41 的阶为 40, 列出所有模 41 阶为 10 的整数$a(0 < a < 41)$.

与上一题方法类似，整数 a 为：

$\frac{40}{(40,x)}$=10 $(40, x) = 4$，x=4,12,28,36

$6^4 \equiv 25 \pmod{41}$，$6^{12} \equiv 4 \pmod{41}$，$6^{28} \equiv 31 \pmod{41}$ $6^{36} \equiv 23 \pmod{41}$

整数 a 为：4,23,25,31

8、 已知m =13^3的原根存在, 求模m的原根有多少个？

解 ： $\varphi(\varphi(13^3)) = \varphi\left(13^3 * \left(1 - \frac{1}{13}\right)\right) = \varphi(13^2 * 12) = 13^2 * 12 * \frac{12}{13} * \frac{1}{2} * \frac{2}{3} = 13 * 12 * 4 = 624$

9、模 101 的原根个数有多少个？

解：$\varphi(\varphi(100)) = \varphi(40) = 40 * \frac{1}{2} * \frac{4}{5} = 16$

10. 已知 $\mathrm{ord}_{41}(18)=5$, 快速求 $18^{18} \pmod{41}$.

解： $18^{18} \equiv 18^{18 \bmod 5} \equiv 18^3 \equiv 10 \pmod{41}$

11. 略

第六章

1. 略
2. 略
3. $F_2[x]$中的多项式x^5+x+1 是否为不可约多项式.

解：判断等于或者小于 2 次的不可约多项式是否能整除x^5+x+1

1 次: $x,x+1$

2 次: x^2+x+1

$$x^5+x+1=x(x^4+1)+1$$
$$x^5+x+1=(\mathrm{x}+1)(x^4+x^3+x^2+x)+1$$
$$x^5+x+1=(x^2+x+1)(x^3+x^2+1)$$

因此x^5+x+1是可约

4、判断$F_2[x]$中的多项式x^5+x^2+1 是否为不可约多项式.

以上一题解法类似：

$$x^5+x^2+1=x(x^4+x)+1$$
$$x^5+x^2+1=(\mathrm{x}+1)(x^4+x^3+x^2)+1$$
$$x^5+x^2+1=(x^2+x+1)(x^3+x^2)+1$$

因此x^5+x^2+1是不可约

5、以上一题方法类似，$x^8+x^4+x^3+x+1$是不可约多项式

6.已知x^4+x+1是$F_2[x]$中的不可约多项式，$F_2[x]/\ x^4+x+1$的余式构成一个有限域 GF(2^4). 回答下列问题:

（1） 这个有限域中，加法恒等元和乘法恒等元各是什么？

（2） 在域 GF(2^4)上计算$(x^2+1)\times(x^3\ \ +1)$.

（3） 在域 GF(2^4)上计算$(x^2)^{-1}(\mathrm{mod}\,x^4+x+1)$.

解： (1) 加法恒等元和乘法恒等元各 0 和 1

(2) $(x^2+1)\times(x^3\ \ +1)\equiv x^5+x^3+x^2+1\equiv x^3+x+1$（mod x^4+x+1）.

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

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

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

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

两边同模 x^4+x+1可得

$$x^2(1+x^3+x^2)\equiv 1(mod x^4+x+1)$$

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

7. 已知$g(x)=x^4+x+1$是$F_2[x]$中的不可约多项式，从而$F_2[x]/(x^4+x+1)$是一个域. 求$f(x)$，使得$f(x)\times x^3\ \ \equiv 1(\mathrm{mod}\,g(x))$.

解类似上一题，$x^4+x+1=x^3x+(x+1)$

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

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

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

因此 $f(x)=x^3+x^2+x+1$