信息安全数学基础习题答案

第一章　整数的可除性

1．证明：因为 $2|n$　　所以 $n=2k$, $k\in Z$

$5|n$　所以 $5|2k$ ，　又（5，2）=1，所以 $5|k$　即 $k=5k_1$　，$k_1\in Z$

$7|n$　所以 $7|2*5k_1$,又（7，10）=1，所以 $7|k_1$　即 $k_1=7k_2$，$k_2\in Z$

所以 $n=2*5*7k_2$　即 $n=70k_2$，　$k_2\in Z$

因此 $70|n$

2．证明：因为 $a^3-a=(a-1)a(a+1)$

当 $a=3k$，$k\in Z$　　$3|a$　　则 $3|a^3-a$

当 $a=3k-1$，$k\in Z$　$3|a+1$　则 $3|a^3-a$

当 $a=3k+1$，$k\in Z$　$3|a-1$　则 $3|a^3-a$

所以 a^3-a 能被 3 整除。

3．证明：任意奇整数可表示为 $2k_0+1$，　$k_0\in Z$

$(2k_0+1)^2=4k_0^2+4k_0+1=4k_0(k_0+1)+1$

由于 k_0 与 k_0+1 为两连续整数，必有一个为偶数，所以 $k_0(k_0+1)=2k$

所以 $(2k_0+1)^2=8k+1$　　得证。

4．证明：设三个连续整数为 $a-1,a,a+1$　则 $(a-1)a(a+1)=a^3-a$

由第二题结论 $3|(a^3-a)$　　即 $3|(a-1)a(a+1)$

又三个连续整数中必有至少一个为偶数，则 $2|(a-1)a(a+1)$

又（3，2）=1　所以 $6|(a-1)a(a+1)$　得证。

5．证明：构造下列 k 个连续正整数列：

$(k+1)!+2,\ (k+1)!+3,\ (k+1)!+4,\cdots\cdots,\ (k+1)!+(k+1),\ k\in Z$

对数列中任一数 $(k+1)!+i=i[(k+1)k\cdots(i+1)(i-1)\cdots2*1+1]$，$i=2,3,4,\cdots(k+1)$

所以 $i|(k+1)!+i$　　即 $(k+1)!+i$ 为合数

所以此 k 个连续正整数都是合数。

6．证明：因为 $191^{1/2}<14$　,小于 14 的素数有 2，3，5，7，11，13

经验算都不能整除 191　　所以 191 为素数。

因为 $547^{1/2}<24$　,小于 24 的素数有 2，3，5，7，11，13，17，19，23

经验算都不能整除 547　　所以 547 为素数。

由 737=11*67 ,747=3*249 知 737 与 747 都为合数。

8．解：存在。eg：a=6,b=2,c=9

10．证明：$p_1p_2p_3|n$，　则 $n=p_1p_2p_3k$，$k\in N^+$

又 $p_1\leqslant p_2\leqslant p_3$，所以 $n=p_1p_2p_3k\geqslant p_1^3$　　即 $p_1^3\leqslant n^{1/3}$

p_1 为素数　则 $p_1\geqslant2$，又 $p_1\leqslant p_2\leqslant p_3$，所以 $n=p_1p_2p_3k\geqslant2p_2p_3\geqslant2p_2^2$

即 $p_2\leqslant(n/2)^{1/2}$　　　得证。

11．解：小于等于 $500^{1/2}$ 的所有素数为 2，3，5，7，11，13，17，19，依次删除这些素数的倍数可得所求素数：

12．证明：反证法

假设 3k+1 没有相同形式的素因数，则它一定只能表示成若干形如 3k-1 的素数相乘。　$(3k_1+1)(3k_2+1)=[(3k_1+1)k_2+k_1]*3+1$　显然若干个 3k+1 的素数相乘，得

到的还是 **3k+1** 的形式，不能得出 **3k-1** 的数，因此假设不成立，结论得证。
同理可证其他。

13. 证明：反证法

假设形如 **4k+3** 的素数只有有限个，记为 p_1，p_2，…，p_n

因为 4k+3=4k\`-1=4k-1　构造 $N=4*p_1*p_2*\cdots*p_n-1\geq 3*p_1*p_2*\cdots*p_n$

所以 $N>p_i$　$(i=1,2,\cdots,n)$

N 为 **4k-1** 形式的素数，即为 **4k+3** 的形式，所以假设不成立。

原结论正确，形如 **4k+3** 的素数有无穷多个。

28.（**1**）解：**85=1*55+30**
55=1*30+25
30=1*25+5
25=5*5
所以 **(55,85)=5**

（**2**）解：**282=1*202+80**
202=2*80+42
80=1*42+38
42=1*38+4
38=9*4+2
4=2*2
所以（**202,282**）**=2**

29.（**1**）解：**2t+1=1*(2t-1)+2**
2t-1=(t-1)*2+1
2=2*1
所以（**2t+1,2t-1**）**=1**

（**2**）解：**2(n+1)=1*2n+2**
2n=n*2
所以（**2n,2(n+1)**）**=2**

32.（**1**）解：**1=3-1*2**
=3-1*(38-12*3)
=-38+13*(41-1*38)
=13*41-14*(161-3*41)
=-14*161+55*(363-2*161)
=55*363+(-124)*(1613-4*363)
=(-124)*1613+551*(3589-2*1613)
=551*3589+(-1226)*1613
所以 **s=-1226**　　　**t=551**

（**2**）解：**1=4-1*3**
=4-1*(115-28*4)
=-115+29*(119-1*115)
=29*119+(-30)*(353-2*119)
=-30*353+89*(472-1*353)
=89*472+(-119)*(825-1*472)
=(-119)*825+208*(2947-3*825)
=208*2947+(-743)*(3772-1*2947)

=951*2947+(-743)*3772

所以 s=951　　　　t=-743

36．证明：因为（a，4）=2　所以 a=2*(2m+1)　$m\in Z$

所以 a+b=4m+2+4n+2=4(m+n)+4=4(m+n+1)

即 4|a+b

所以（a+b,4）=4

37．证明：反证法

假设 n 为素数，则 n| $a^2-b^2=(a+b)(a-b)$

由 1.4 定理 2 知 n|a+b 或 n|a-b,与已知条件矛盾

所以假设不成立，原结论正确，n 为合数。

40．证明：（1）假设是 $2^{1/2}$ 有理数，则存在正整数 p，q，使得 $2^{1/2}=p/q$,且（p，q）=1

平方得：$p^2=2q^2$，　即 $2|p^2$，所以 p=2m，$m\in N$

因此 $p^2=4m^2=2q^2$　$q^2=2m^2$　　　q=2n，$n\in N$

则（p，q）=(2m,2n)=2(m，n)≥2 与（p，q）=1 矛盾

所以假设不成立，原结论正确，$2^{1/2}$ 不是有理数。

（2）假设是 $7^{1/2}$ 有理数，则存在正整数 m，n，使得 $7^{1/2}=p/q$,且（m，n）=1

平方得：$m^2=2n^2$，　即 $7|m^2$

将 m 表示成 n 个素数 p_i 的乘积，$m=p_1p_2p_3\cdots\cdots p_n$　，　p_i 为素数。

因为 7 为素数，假设 7 !| m，则 7 !∈{p_1，p_2，p_3，……p_n}

所以 $m^2=p_1^2p_2^2p_3^2\cdots\cdots p_n^2=(p_1p_2p_3\cdots\cdots p_n)(p_1p_2p_3\cdots\cdots p_n)$

所以 7 !| m^2，与 $7|m^2$ 矛盾，故 7|m，　m=7k

同理可知：7|n，　n=7 k_0

所以(m，n)=(7k,7 k_0)=7(k，k_0)≥7　与已知矛盾

故原结论正确，$7^{1/2}$ 不是有理数。

（3）同理可证 $17^{1/2}$ 不是有理数。

41．证明：假设 $\log_2 10$ 是有理数，则存在正整数 p，q,使得 $\log_2 10=p/q$,且（p，q）=1

又 $\log_2 10=\ln 10/\ln 2=p/q$

$\mathrm{Ln}10^q=\ln 2^p$　　$10^q=2^p$

$(2*5)^q=2^p$　　$5^q=2^{p-q}$

所以只有当 q=p=0 是成立，所以假设不成立

故原结论正确，$\log_2 10$ 是无理数。

同理可证 $\log_3 7$，$\log_{15} 21$ 都是无理数。

50．（1）解：因为 $8=2^3$，　$60=2^2*3*5$

所以 $[8,60]=2^3*3*5=120$

51．（4）解：$(47^{11}79^{11}101^{1001},41^{11}83^{111}101^{1000})=41^0 47^0 79^0 83^0 101^{1000}=101^{1000}$

$[47^{11}79^{11}101^{1001},41^{11}83^{111}101^{1000}]=41^{11}47^{11}79^{111}83^{111}101^{1001}$

第二章．同余

1．解：（1）其中之一为 9，19，11，21，13，23，15，25，17

（2）其中之一为 0，10，20，30，40，50，60，70，80

（3）．（1）或（2）中的要求对模 10 不能实现。

2．证明：当 $m>2$ 时，因为 $(m-1)^2=m^2-2m+1=m(m-2)+1$

所以 $(m-1)^2\equiv 1(\mathrm{mod}\ m)$

即 1 与 $(m-1)^2$ 在同一个剩余类中，故 $0^2,1^2,\cdots,(m-1)^2$ 一定不是模 m 的完全剩余系。

6．解：$2^1\equiv 2(\mathrm{mod}7)$，$2^2\equiv 4(\mathrm{mod}7)$，$2^3\equiv 1(\mathrm{mod}7)$

又 20080509=6693503*3

所以 $2^{20080509}=(2^3)6693503\equiv 1(\mathrm{mod}7)$

故 $2^{20080509}$ 是星期六。

7．证明：（i）因为 $a_i\equiv b_i\ (\mathrm{mod}m), 1\leqslant i\leqslant k$　　所以 $a_i=b_i+k_im$

又 $a_1+a_2+\cdots+a_k=\Sigma a_i=\Sigma(b_i+k_im)=\Sigma b_i+m*\Sigma k_i$

所以有 $\Sigma a_i\equiv\Sigma b_i\ (\mathrm{mod}\ m)$

即 $a_1+a_2+\cdots+a_k=b_1+b_2+\cdots+b_k\ (\mathrm{mod}\ m)$

（ii）因为 $a_i\equiv b_i\ (\mathrm{mod}\ m), 1\leqslant i\leqslant k$　所以 $a_i(\mathrm{mod}\ m)=b_i\ (\mathrm{mod}\ m)$

所以 $(a_1a_2\cdots a_k)\ \mathrm{mod}\ m\equiv[(a_1\mathrm{mod}\ m)(a_2\mathrm{mod}\ m)\cdots(a_k\mathrm{mod}\ m)]\mathrm{mod}\ m$

$\equiv[(b_1\mathrm{mod}\ m)(b_2\mathrm{mod}\ m)\cdots(b_k\mathrm{mod}\ m)]\mathrm{mod}\ m$

$\equiv(b_1b_2\cdots b_k)\ \mathrm{mod}\ m$

所以 $a_1a_2\cdots a_k\equiv a_1a_2\cdots a_k(\mathrm{mod}\ m)$

8．证明：如果 $a^2\equiv b^2(\mathrm{mod}\ p)$　则 $a^2=b^2+kp$，$k\in Z$

即 $kp=a^2-b^2=(a+b)(a-b)$　　所以 $p|(a+b)(a-b)$

又 p 为素数，根据 1.4 定理 2 知 $p|a+b$ 或 $p|a-b$　得证。

9．证明：如果 $a^2\equiv b^2(\mathrm{mod}\ n)$　则 $a^2=b^2+kn$，$k\in Z$

即 $kn=a^2-b^2=(a+b)(a-b)$　　所以 $n|(a+b)(a-b)$

由 $n=pq$ 知 $kpq=a^2-b^2=(a+b)(a-b)$

因为 n!|a-b，n!|a+b，所以 p,q 不能同时为 a-b 或 a+b 的素因数。

不妨设 $p|a-b$，$q|a+b$，则 q!|a-b，p!|a+b　即 $(q, a-b)=1, (p, a+b)=1$

因此 $(n, a-b)=(pq, a-b)=(p, a-b)=p>1$

$(n, a+b)=(pq, a+b)=(q, a+b)=q>1$

故原命题成立。

10．证明：因为 $a\equiv b\ (\mathrm{mod}\ c)$　则 $a=cq+b$，$q\in Z$

根据 1.3 定理 3 知 $(a, c)=(b, c)$

17．解：（1）$a_k+a_{k-1}+\cdots+a_0=1+8+4+3+5+8+1=30$

因为 3|30，9!|30　所以 1843581 能被 3 整除，不能被 9 整除。

（2）$a_k+a_{k-1}+\cdots+a_0=1+8+4+2+3+4+0+8+1=31$

因为 3!|31，9!|31　所以 184234081 不能被 3 整除，也不能被 9 整除。

（3）$a_k+a_{k-1}+\cdots+a_0=8+9+3+7+7+5+2+7+4+4=56$

因为 3!|56，9!|56　所以 8937752744 不能被 3 整除，也不能被 9 整除。

（4）$a_k+a_{k-1}+\cdots+a_0=4+1+5+3+7+6+8+9+1+2+2+4+6=58$

因为 3!|58，9!|58　所以 4153768912246 不能被 3 整除，也不能被 9 整除。

20．解：（89878*58965）mod9≡[(89878mod9)*(58965mod9)]mod9≡(4*6)mod9

≡6(mod9)　≡5299?56270(mod9)

又 5299?56270≡(45+?)mod9≡?(mod9)

所以　?=6　　即未知数字为 6。

21．解：（1）因为 875961*2753≡[(36mod9)(17mod9)]mod9 ≡0(mod9)

2410520633≡26(mod9) ≡8(mod9)

所以等式 875961*2753=2410520633 不成立

（2）因为 14789*23567≡[(29mod9)(23mod9)]mod9 ≡1(mod9)

348532367≡41(mod9) ≡5(mod9)

所以等式 14789*23567=348532367 不成立

（3）因为 24789*43717≡[(30mod9)(22mod9)]mod9 ≡3(mod9)

1092700713≡30(mod9) ≡3(mod9)

所以等式 24789*43717=1092700713 可能成立

（4）这种判断对于判断等式不成立时简单明了，但对于判断等式成立时，可能会较复杂。

22．解：因为 7 为素数，由 Wilso 定理知：(7-1)! ≡-1(mod7) 即 6! ≡-1（mod7）

所以 8*9*10*11*12*13≡1*2*3*4*5*6(mod7) ≡6!(mod7) ≡-1(mod7)

31．证明：因为 $c_1,c_2,\cdots,c_{j(m)}$ 是模 m 的简化剩余系

对于任一 c_i，有 $m-c_i$ 也属于模 m 的简化剩余系

所以 $c_i+(m-c_i)\equiv0(\bmod m)$

因此 $c_1+c_2+\cdots+c_{j(m)}\equiv0(\bmod m)$

32．证明：因为 $a^{j(m)}\equiv1(\bmod m)$ 所以 $a^{j(m)}-1\equiv0(\bmod m)$

$a^{j(m)}-1=(a-1)(1+a+a^2+\cdots+a^{j(m)-1})\equiv0(\bmod m)$

又（a-1,m）=1

所以 $1+a+a^2+\cdots+a^{j(m)-1}\equiv0(\bmod m)$

33．证明：因为 7 为素数，由 Fermat 定理知 $a^7\equiv a(\bmod 7)$

又（a，3）=1 所以(a,9)=1 由 Euler 定理知 $a^{j(9)}\equiv a^6\equiv1(\bmod 9)$ 即 $a^7\equiv a(\bmod 9)$

又(7,9)=1， 所以 $a^7\equiv a(\bmod 7*9)$

即 $a^7\equiv a(\bmod 63)$

34．证明：因为 $32760=2^3*3^2*5*7*13$ 又(a,32760)=1

所以(a,2)=(a,3)=(a,5)=(a,7)=(a,13)=1

有：$a^{j(13)}\equiv1(\bmod 13)$ 即 $a^{12}\equiv1(\bmod 13)$

$a^{j(8)}\equiv a^4\equiv1(\bmod 8)$ 即 $a^{12}\equiv1(\bmod 8)$

$a^{j(5)}\equiv a^4\equiv1(\bmod 5)$ 即 $a^{12}\equiv1(\bmod 5)$

$a^{j(7)}\equiv a^6\equiv1(\bmod 7)$ 即 $a^{12}\equiv1(\bmod 7)$

$a^{j(9)}\equiv a^6\equiv1(\bmod 9)$ 即 $a^{12}\equiv1(\bmod 9)$

又因为[5,7,8,9,13]=32760

所以 $a^{12}\equiv1(\bmod 32760)$

35．证明：因为(p,q)=1 p,q 都为素数 所以 j (p)=p-1， j (q)=q-1

由 Euler 定理知：$p^{j(q)}\equiv1(\bmod q)$ $q^{j(p)}\equiv1(\bmod p)$

即 $p^{q-1}\equiv1(\bmod q)$ $q^{p-1}\equiv1(\bmod p)$

又 $q^{p-1}\equiv0(\bmod q)$ $p^{q-1}\equiv0(\bmod p)$

所以 $p^{q-1}+q^{p-1}\equiv1(\bmod q)$ $q^{p-1}+p^{q-1}\equiv1(\bmod p)$

又[p,q]=pq 所以 $p^{q-1}+q^{p-1}\equiv1(\bmod pq)$

36．证明：因为(m,n)=1

由 Euler 定理知：$m^{j(n)}\equiv1(\bmod n)$ $n^{j(m)}\equiv1(\bmod m)$

所以 $m^{j(n)}+n^{j(m)}\equiv(m^{j(n)}\bmod n)+(n^{j(m)}\bmod n)\equiv1+0\equiv1(\bmod n)$

同理有：$m\varphi(n)+n\varphi(m)\equiv 1(\mathrm{mod}\,m)$

又 $[m,n]=mn$　所以 $m\varphi(n)+n\varphi(m)\equiv 1(\mathrm{mod}\,mn)$

第三章.同余式

1.（1）解：因为（3，7）=1 | 2 故原同余式有解

又 3x≡1（mod7）　所以 特解 x_0`≡5（mod7）

同余式 3x≡2（mod7）的一个特解 x_0≡2* x_0`=2*5≡3（mod7）

所有解为：x≡3（mod7）

（3）解：因为（17，21）=1 | 14 故原同余式有解

又 17x≡1（mod21）　所以 特解 x_0`≡5（mod21）

同余式 17x≡14（mod21）的一个特解 x_0≡14* x_0`=14*5≡7（mod21）

所有解为：x≡7（mod21）

2.（1）解：因为（127，1012）=1 | 833 故原同余式有解

又 127x≡1（mod1012）　所以 特解 x_0`≡255（mod1012）

同余式 127x≡833（mod1012）的一个特解 x_0≡833* x_0`=833*255≡907（mod1012）

所有解为：x≡907（mod1012）

3．见课本 3.2 例 1

7.（1）解：因为（5，14）=1

由 Euler 定理知，同余方程 5x≡3（mod14）的解为：

$x\equiv 5^{\varphi(14)-1}*3\equiv 9$（mod14）

（2）解：因为（4，15）=1

由 Euler 定理知，同余方程 4x≡7（mod15）的解为：

$x\equiv 4^{\varphi(15)-1}*7\equiv 13$（mod15）

（3）解：因为（3，16）=1

由 Euler 定理知，同余方程 3x≡5（mod16）的解为：

$x\equiv 3^{\varphi(16)-1}*5\equiv 7$（mod16）

11．证明：由中国剩余定理知方程解为：

$x\equiv a_1M_1M_1`+a_2M_2M_2`+\cdots\cdots+a_kM_kM_k`$（mod m）

因为 m_i 两两互素，又中国剩余定理知：$M_iM_i`\equiv 1$（mod m_i）

又 $M_i=m/m_i$　所以（m，M_i）≡1（mod m_i）

所以 $M_iM_i`=M_i^{\varphi(m_i)}\equiv$（mod m_i）

代入方程解为 $x\equiv a_1M_1^{\varphi(m_1)}+a_2M_2^{\varphi(m_2)}+\cdots\cdots+a_kM_k^{\varphi(m_k)}(\mathrm{mod}\ m)$ 得证。

12．（1）解：由方程组得：3x+3y≡2(mod7)

6x+6y≡4(mod7)　x+y≡-4(mod7)

X≡5(mod 7)　y≡5 (mod 7)

（2）解：由方程组得：2x+6y≡2(mod7)　2x-y≡2(mod7)

6x+8y≡4(mod7)　x-y≡-4(mod7)

X≡6(mod 7)　y≡3 (mod 7)

13．见课本 3.2 例 4

14．同课本 3.2 例 3　$2^{1000000}\equiv 562$（mod1309）

15．（1）解：等价同余式组为：

$23x \equiv 1 \pmod{4}$

$23x \equiv 1 \pmod{5}$

$23x \equiv 1 \pmod{7}$

所以 $x \equiv 3 \pmod{4}$ $\quad x \equiv 2 \pmod{5}$ $\quad x \equiv 4 \pmod{7}$

所以 $x \equiv 3*35*3 + 2*28*2 + 4*20*6 \equiv 67 \pmod{140}$

（2）解：等价同余式组为：

$17x \equiv 1 \pmod{4}$

$17x \equiv 1 \pmod{5}$

$17x \equiv 1 \pmod{7}$

$17x \equiv 1 \pmod{11}$

所以 $x \equiv 1 \pmod{4}$ $\quad x \equiv 2 \pmod{5}$ $\quad x \equiv -3 \pmod{7}$ $\quad x \equiv 7 \pmod{11}$

所以 $x \equiv 1*385*1 + 2*308*2 + (-3)*220*5 + 7*140*7 \equiv 557 \pmod{1540}$

19．解：$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x \equiv 0 \pmod{7}$

左边 $=(x^7-x)(3x^7+4x^6+2x^4+x^2+3x+4)+ x^6+2x^5+2x^2+15x^2+5x$

所以原同余式可化简为：$x^6+2x^5+2x^2+15x^2+5x \equiv 0 \pmod{7}$

直接验算得解为：$x \equiv 0 \pmod{7}$ $\quad x \equiv 6 \pmod{7}$

20．解：$f'(x) \equiv 4x^3+7 \pmod{243}$

直接验算的同余式 $f(x) \equiv 0 \pmod{3}$ 有一解：$x_1 \equiv 1 \pmod{3}$

$f'(x_1) \equiv 4*1^3*7 = -1 \pmod{3}$ $\quad f'(x_1)^{-1} \equiv -1 \pmod{3}$

所以 $t_1 \equiv -f(x_1)*(f'(x_1)^{-1} \pmod{3})/3^1 \equiv 1 \pmod{3}$

$x_2 \equiv x_1+3t_1 \equiv 4 \pmod{9}$

$t_2 \equiv -f(x_2)*(f'(x_1)^{-1} \pmod{3})/3^2 \equiv 2 \pmod{3}$

$x_3 \equiv x_2+3^2 t_2 \equiv 22 \pmod{27}$

$t_3 \equiv -f(x_3)*(f'(x_1)^{-1} \pmod{3})/3^3 \equiv 0 \pmod{3}$

$x_4 \equiv x_3+3^3 t_3 \equiv 22 \pmod{81}$

$t_5 \equiv -f(x_4)*(f'(x_1)^{-1} \pmod{3})/3^4 \equiv 2 \pmod{3}$

$x_5 \equiv x_4+3^4 t_4 \equiv 184 \pmod{243}$

所以同余式 $f(x) \equiv 0 \pmod{243}$ 的解为：$x_5 \equiv 184 \pmod{243}$

第四章．二次同余式与平方剩余

2．解：对 $x=0,1,2,3,4,5,6$ 时，分别求出 y

$x=0, y^2 \equiv 1 \pmod{7}, y \equiv 1,6 \pmod{7}$

$x=4, y^2 \equiv 4 \pmod{7}, y \equiv 2,5 \pmod{7}$

当 $x=1,2,3,5,6$ 时均无解

5．解：对 $x=0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16$ 时，分别求出 y

$x=0, y^2 \equiv 1 \pmod{17}, y \equiv 1,16 \pmod{17}$

$x=1, y^2 \equiv 3 \pmod{17}$，无解

$x=2, y^2 \equiv 11 \pmod{17}$，无解

$x=3, y^2 \equiv 14 \pmod{17}$，无解

$x=4, y^2 \equiv 1 \pmod{17}, y \equiv 1,16 \pmod{17}$

$x=5, y^2 \equiv 12 \pmod{17}$，无解

$x=6, y^2\equiv 2(\bmod 17), y\equiv 6,11(\bmod 17)$

$x=7, y^2\equiv 11(\bmod 17)$,无解

$x=8, y^2\equiv 11(\bmod 17)$,无解

$x=9, y^2\equiv 8(\bmod 17), y\equiv 5,12(\bmod 17)$

$x=10, y^2\equiv 8(\bmod 17), y\equiv 5,12(\bmod 17)$

$x=11, y^2\equiv 0(\bmod 17), y\equiv 0(\bmod 17)$

$x=12, y^2\equiv 7(\bmod 17)$,无解

$x=13, y^2\equiv 1(\bmod 17), y\equiv 1,16(\bmod 17)$

$x=14, y^2\equiv 5(\bmod 17)$,无解

$x=15, y^2\equiv 8(\bmod 17), y\equiv 5,12(\bmod 17)$

$x=16, y^2\equiv 16(\bmod 17), y\equiv 4,13(\bmod 17)$

10. 解:(1).$(17/37)=(-1)^{(17-1)(37-1)/(2*2)}*(37/17)=-1$

(4).$(911/2003)=(-1)^{(2003-1)(911-1)/(2*2)}*(2003/911)=1/3=1$

(6).$(7/20040803)=(-1)^{(7-1)(20040803-1)/(2*2)}*(20040803/7)=1$

12. 解:(1).因为$(-2/67)=(65/67)=1$

所以-2 是 67 的平方剩余

所以 $x^2\equiv -2(\bmod 67)$有 2 个解。

(4).因为$(2/37)=(-1)^{(37*37-1)/8}=-1$

所以 2 是 37 的平方非剩余

所以 $x^2\equiv 2(\bmod 37)$无解。

14. 证明:(1)因为 p 为其素数,模 p 的所有二次剩余个数为$(p-1)/2$个,

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

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

$\equiv 1*2*3\cdots((p-1)/2)*(-(p-1))*(-(p-2))*\cdots(-(p-(p-1)/2))(\bmod\ p)$

$\equiv 1*2*3\cdots((p-1)/2)*(p-(p-1)/2)\cdots*(p-2)*(p-1)(-1)^{(p-1)/2}(\bmod\ p)$

$\equiv (p-1)!*(-1)^{(p-1)/2}(\bmod\ p)$

$\equiv (-1)*(-1)^{(p-1)/2}(\bmod\ p)$　　(2.4 定理 3)

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

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

(2)1,2,3,…p-1 为 p 的一个完全剩余系

$1*2*2\cdots*(p-1)\equiv -1(\bmod\ p)\ \equiv (-1)^{(p+1)/2}(-1)^{(p-1)/2}(\bmod\ p)$

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

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

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

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

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

所以当 p>3 时,模 p 的所有二次剩余之和模 p 的剩余为 0。

(4)因为模 p 的所有二次非剩余之和与所有二次剩余之和的和可以被 p 整除

所以由(3)得,当 p=3 时,模 p 的所有二次非剩余之和模 p 的剩余为-1;

当 p>3 时,模 p 的所有二次非剩余之和模 p 的剩余为 0。

16. 解:(1).因为$(7/227)=(-1)^{(227-1)(7-1)/(2*2)}*(227/7)=1$

所以 7 是 227 的二次剩余

所以 $x^2\equiv 7(\bmod 227)$有解

(3）.因为 11 对 91 的逆元是 58

所以原同余方程等价于 $x^2 \equiv 16 \pmod{91}$

又 16 是 91 的平方剩余

所以 $11x^2 \equiv -6 \pmod{91}$ 有解

21．证明：应用模重复平方法

$11=2^0+2^1+2^3$

令 x=23, b=2, a=1

(1) $x_0=1$　　$a_0=a*b\equiv 2 \pmod{23}$　　$b_1=b^2\equiv 4 \pmod{23}$

(2) $x_1=1$　　$a_1=a_0*b_1\equiv 8 \pmod{23}$　　$b_2=b_1^2\equiv 16 \pmod{23}$

(3) $x_2=0$　　$a_2=a_1*b_2^0\equiv 8 \pmod{23}$　　$b_3=b_2^2\equiv 3 \pmod{23}$

(4) $x_3=1$　　$a_3=a_2*b_3\equiv 1 \pmod{23}$

所以 $2^{11}\equiv 1 \pmod{23}$　　即 $23|2^{11}-1$

$47|2^{23}-1$ 与 $503|2^{251}-1$ 应用同样的方法得证。

第五章．原根与指标

1．解：因为 j (13)=12, 所以只需对 12 的因数 d=1,2,3,4,6,12, 计算 $a^d \pmod{12}$

因为 $2^1\equiv 2$，$2^2\equiv 4$，$2^3\equiv 8$，$2^4\equiv 3$，$2^6\equiv -1$，$2^{12}\equiv 1 \pmod{13}$

所以 2 模 13 的指数为 12；

同理可得：5 模 13 的指数为 4，10 模 13 的指数为 6。

2．解：因为 j (19)=18, 所以只需对 18 的因数 d=1,2,3,6,9,18 计算 $a^d \pmod{12}$

因为 $3^1\equiv 3$，$3^2\equiv 9$，$3^3\equiv 8$，$3^6\equiv 7$，$3^9\equiv -1$，$2^{18}\equiv 1 \pmod{13}$

所以 3 模 19 的指数为 18；

同理可得：7 模 19 的指数为 3，10 模 19 的指数为 18。

3．解：因为 j (m)= j (81)=54=2*3^3, 所以 j (m) 的素因数为 $q_1=2, q_2=3$, 进而

j (m)/q_1=27，　j (m)/q_2=18

这样，只需验证：g^{27}, g^{18} 模 m 是否同余于 1。对 2，4，5，6…逐个验算：

因为 $2^{27}\neq 1 \pmod{81}$　$2^{18}\neq 1 \pmod{81}$　根据 5.2 定理 8 得

所以 2 是模 81 的原根

7．证明：因为（a，m）=1，　故由 $ord_m(a)=st$ 知：$a^{st}\equiv 1 \pmod{m}$　即 $(a^s)^t\equiv 1 \pmod{m}$

不妨令 $ord_m(a^s)=r$　则 $a^{sr}\equiv 1 \pmod{m}$　所以 st|sr

由 $(a^s)^t\equiv 1 \pmod{m}$ 得 r|t　即 t＝k*r　k∈N≥1　r≤t　所以 sr≤st

所以 sr=st　所以 r=t

所以 $ord_m(a^s)=t$

8．解：存在

举例：如 n=7, d=3　因为 j (7)=6　d=3|6

存在 a=2　(2,7)=1，$2^{j(7)}\equiv 1 \pmod{7}$　又 $2^3\equiv 1 \pmod{7}$

所以 $ord_7(2)=3$　满足条件。

10．证明：因为 p 为一个奇素数，p-1/2 也是一个奇素数

所以 j (p)=p-1=2*(p-1)/2　即 j (p)的不同素因数为 2，p-1/2

又因为 $a^{j(p)/2}=a^{p-1/2}\neq 1 \pmod{p}$　$a^{j(p)/[(p-1)/2]}=a^2\neq 1 \pmod{p}$

根据 5.2 定理 8 得 a 是模 p 的原根。

15. 证明：反证法

假设 n 是一个合数，令 $ord_n(a)=m$　则 $a^m\equiv 1(mod\ n)$

因为 $a^{n-1}\equiv 1(mod\ n)$　所以由 5.1 定理 1 得 m|n-1　即 n-1=k*m

对 n-1 的所有素因数 q，必可找到一个 q_1 使 $m|((n-1)/q_1)$

所以 $a^{n-1/q}=a^{m*t}\equiv 1(mod\ n)$ 与已知条件矛盾，故假设不成立，原结论得证。

16. 解：因为 $d=(n,\varphi(m))=(22,\varphi(41))=(22,40)=2$　　ind5=22

所以$(n,\varphi(m))|ind5$，同余式有解

等价同余式为 $22indx\equiv ind5(mod40)$　即 $11indx\equiv 11(mod20)$

解得：indx=1,21(mod40)

所以原同余式解为 x=6,35(mod41)

17. 解：因为 $d=(n,\varphi(m))=(22,\varphi(41))=(22,40)=2$　　ind29=7

(2,7)=1　所以原同余式无解。

第六章．素性检验

1. 证明：因为 91=13*7 是奇合数，　　(3,91)=1

又 $3^6=729\equiv 1(mod91)$　则 $3^{91-1}=3^{90}\equiv(3^6)^{15}\equiv 1(mod91)$

则 91 是对于基 3 的拟素数。

2. 证明：因为 45=5*3*3 是奇合数，　　(17,45)=1

由 Euler 定理：$17^4\equiv 1(mod5)$　$17^2\equiv 1(mod3)$

所以 $17^4\equiv 1(mod3)$　所以 $17^4\equiv 1(mod45)$

则 $17^{45-1}=17^{44}\equiv(17^4)^{11}\equiv 1(mod45)$

则 45 是对于基 17 的拟素数。

同理 45 是对于基 19 的拟素数。

10. 证明：25=5*5 是奇素数　设 n=25　$n-1=24=2^3*3$　则 t=3　(7,25)=1

$7^3\equiv 18(mod25)$　$7^{2*3}\equiv -1(mod25)$

所以 25 是基于 7 的强拟素数。

15. 证明：n=561=3*11*17　为奇素数　（561,2）=1

$b^{(n-1)/2}\equiv 2^{(561-1)/2}\equiv 2^{280}\equiv 1(mod561)$

$(b/n)=(2/561)=(-1)^{(561*561-1)/8}=1$

所以 $2^{280}\equiv(2/561)(mod561)$

所以 561 是对于基 2 的 Euler 拟素数。

第八章．群

2． 证明：群 G 是交换群的充要条件是对任意 $a,b\in G$，有 $(ab)^2=a^2b^2$。

证明：$\Rightarrow$ 必要性：若 G 是交换群，则对任意 $a,b\in G$，有 $ab=ba$，从而

$$(ab)^2=abab=aabb=a^2b^2。$$

$\Leftarrow$ 充分性：若对任意 $a,b\in G$，有 $(ab)^2=a^2b^2$。那么

$$ba=ebae=a^{-1}(ab)^2b^{-1}=a^{-1}a^2b^2b^{-1}=eabe=ab。$$

因此群 G 是交换群。

4. 设 G 是 n 阶有限群。证明：对任意元 $a\in G$，有 $a^n=e$。

证明：任取 $a\in G$，考虑 a 生成的循环群 $\langle a\rangle$。不妨设 $|\langle a\rangle|=q$。根据拉格朗日定理，有 $q\,|\,n$，从而存在正整数 k，使得 $n=qk$。因为 $a^q=e$（否则 $|\langle a\rangle|\neq q$），所以 $a^n=(a^q)^k=e^k=e$。

6. 设 G 是一个群。记 $cent(G)=\{a\in G\,|\,(\forall b\in G)ab=ba\}$。证明：$cent(G)$ 是 G 的正规子群。

证明：首先证明 $cent(G)$ 是 G 的子群。任取 $a_1,a_2\in cent(G)$，$b\in G$。计算

$$ba_1a_2^{-1}=a_1ba_2^{-1}=a_1(b^{-1})^{-1}a_2^{-1}=a_1(a_2b^{-1})^{-1}=a_1(b^{-1}a_2)^{-1}=a_1a_2^{-1}(b^{-1})^{-1}=a_1a_2^{-1}b。$$

因此，$a_1a_2^{-1}\in cent(G)$，从而 $cent(G)$ 是 G 的子群。

再证明 $cent(G)$ 是 G 的正规子群。任取 $a\in G,\ x\in a\ \mathrm{cent}(G)\ a^{-1}$。那么存在 $y\in \mathrm{cent}(G)$，使得 $x=aya^{-1}$。由 y 的交换性，有 $x=aya^{-1}=aa^{-1}y=ey=y\in \mathrm{cent}(G)$。从而 $a\ \mathrm{cent}(G)\ a^{-1}\subset \mathrm{cent}(G)$，$cent(G)$ 是 G 的正规子群。

7. 设 a 是群 G 的一个元素。证明：映射 $s: x\to axa^{-1}$ 是 G 到自身的自同构。

证明：（1）任取 $x,y\in G$。计算

$$s(xy)=a(xy)a^{-1}=axeya^{-1}=axa^{-1}aya^{-1}=s(x)s(y)$$

因此 s 是同态映射。

（2）若 $x,y\in G$，且 $s(x)=s(y)$。那么 $axa^{-1}=aya^{-1}$，从而

$$x=a^{-1}axa^{-1}a=a^{-1}aya^{-1}a=y,$$

因此 s 是单射。

（3）任取 $c\in G$。由于 $s(a^{-1}ca)=a(a^{-1}ca)a^{-1}=ece=c$，故 s 是满射。

综上所述，映射 $s:x\to axa^{-1}$ 是 G 到自身的自同构。

8. 设 H 是群 G 的子群。在 G 中定义关系 $R: aRb\Leftrightarrow b^{-1}a\in H$。证明：

（i） R 是等价关系。
（ii） aRb 的充要条件是 $aH=bH$。

证明：（i）任取 $a\in G$。既然 H 是群 G 的子群，那么 $e\in H$。因此 $a^{-1}a=e\in H$，这说明 aRa，即 R 满足自反性。

取 $a,b\in G$ 满足 aRb。那么 $b^{-1}a\in H$。根据 H 是群 G 的子群以及逆元的性质，我们有 $a^{-1}b=(b^{-1}a)^{-1}\in H$，这说明 bRa，即 R 满足对称性。

取 $a,b,c\in G$ 满足 aRb， bRc。那么 $b^{-1}a\in H$， $c^{-1}b\in H$。根据 H 是群 G 的子群，我们有 $c^{-1}a=(c^{-1}b)(b^{-1}a)\in H$。 从而 aRc 成立，即 R 满足传递性。

综上所述 R 是等价关系。

（ii）即要证明： $b^{-1}a\in H\Leftrightarrow aH=bH$。

$\Leftarrow$ 充分性：设 $aH=bH$，则 $a=ae\in aH=bH$，于是存在 $h\in H$ 使得 $a=bh$，左右两边同乘 b^{-1}，得 $b^{-1}a=b^{-1}bh=h\in H$。

$\Rightarrow$ 必要性：如果 $b^{-1}a\in H$。对任意 $c\in aH$，存在 $h_2\in H$ 使得 $c=ah_2$。进而，

$$c=b(b^{-1}a)h_2=bh_1h_2\in bH,$$

因此， $aH\subset bH$。

同样，对任意 $c\in bH$，存在 $h_3\in H$ 使得 $c=bh_3$，进而 $c=a(b^{-1}a)^{-1}h_3=ah_1^{-1}h_2\in aH$。因此 $bH\subset aH$，故 $aH=bH$。

2007 年试题

1 证明：如果 a 是整数，则 a^3-a 能被 3 整除。

2 用广义欧几里德算法求最大公因子 (4655,12075)

3 设 m 是一个正整数，$a \equiv b(\bmod m)$，如果 $d \mid m$，证明：$a \equiv b(\bmod d)$。

4 解方程 $987x \equiv 610(\bmod 2668)$

5 解方程组 $\begin{cases} x \equiv 2(\bmod 3) \\ x \equiv 1(\bmod 5) \\ x \equiv 1(\bmod 7) \end{cases}$

6 计算 3 模 19 的指数。

7 计算 $\left(\frac{6}{53}\right)$ 的 Legendre 符号

8 证明：91 是对基 3 的拟素数。

9 设 f 是群 G 到 G' 的一个同态，$\ker f=\{a \mid a \in G, f(a)=e'\}$，其中 e' 是 G' 的单位元。证明：$\ker f$ 是 G 的子群。

10 设 a 是群 G 的一个元素。证明：映射 $s: x \to axa^{-1}$ 是 G 到自身的自同构。

2007 年试题答案

1 证明：因为 **a³-a=(a-1)a(a+1)**

当 **a=3k，k∈Z　3|a　则 3|a³-a**

当 **a=3k-1，k∈Z　3|a+1　则 3|a³-a**

当 **a=3k+1，k∈Z　3|a-1　则 3|a³-a**

所以 **a³-a** 能被 **3** 整除。

2. **12075=2*4655+2765**

4655=1*2765+1890

2765=1*1890+875

1890=2*875+140

875=6*140+35

140=4*35

所以 (4655,12075) =35

3. 因为 d|m，所以存在整数 m' 使得 $m = dm'$。又因为 $a \equiv b(\bmod m)$，所以存在整数 k 使得 $a = b + mk$。该式又可以写成 $a = b + d(m'k)$。故 $a \equiv b(\bmod d)$。

4. $987x \equiv 610(\bmod 2668)$

计算最大公因式(987,2668)=1，所以原同余式有解且只有一个解。利用广义欧几里德除法，求同余式 $987x \equiv 1(\bmod 2668)$ 的解为 $x_0' = 2495(\bmod 2668)$。再写出同余式 $987x \equiv 610(\bmod 2668)$ 的解为 $x_0 = 610 * x_0' = 610 * 2495 \equiv 1190(\bmod 2668)$。

5 令 $m_1 = 3, m_2 = 5, m_3 = 7$， $m = 3*5*7 = 105$，

$M_1 = 5*7 = 35, M_2 = 3*7 = 21, M_3 = 3*5 = 15$。

分别求解同余式 $M_i' M_i \equiv 1(\bmod m_i)$（$i$=1,2,3）

得到 $M_1' = 2$， $M_2' = 1$， $M_3' = 1$。故同余式的解为

$$\begin{aligned} x &\equiv M_1'M_1 * 2 + M_2'M_2 * 1 + M_3'M_3 * 1(\bmod 105) \\ &\equiv 2*35*2 + 1*21*1 + 1*15*1(\bmod 105) \\ &\equiv 71(\bmod 105) \end{aligned}$$

6 解：因为 j **(19)=18,**所以只需对 **18** 的因数 **d=1,2,3,6,9,18** 计算 a^d**(mod12)**

因为 $3^1 \equiv 3$，$3^2 \equiv 9$，$3^3 \equiv 8$，$3^6 \equiv 7$，$3^9 \equiv -1$，$2^{18} \equiv 1(\bmod 13)$

所以 **3** 模 **19** 的指数为 **18**;

7

$$\begin{aligned} \left(\frac{6}{53}\right) &= \left(\frac{2}{53}\right)\left(\frac{3}{53}\right) \\ &= (-1)^{(53^2-1)/8} \cdot (-1)^{(3-1)(53-1)/4} \left(\frac{53}{3}\right) \\ &= -1 \cdot 1 \cdot \left(\frac{2}{3}\right) = -1 \cdot (-1)^{(3^2-1)/8} = 1 \end{aligned}$$

8 证明：因为 **91=13*7** 是奇合数， **(3,91)=1**

又 $3^6 = 729 \equiv 1(\bmod 91)$ 　则 $3^{91-1} = 3^{90} \equiv (3^6)^{15} \equiv 1(\bmod 91)$

则 **91** 是对于基 **3** 的拟素数。

9 对任意 $a,b\in \ker f$，有 $f(a)=e', f(b)=e'$，从而，

$$f(ab^{-1})=f(a)f(b^{-1})=f(a)f(b)^{-1}=f(a)f(a)^{-1}=e'。$$

因此，$ab^{-1}\in \ker f$，$\ker f$ 是群 G 的子群。

10 证明：（1）任取 $x,y\in G$。计算

$$s(xy)=a(xy)a^{-1}=axeya^{-1}=axa^{-1}aya^{-1}=s(x)s(y)$$

因此 s 是同态映射。

（2）若 $x,y\in G$，且 $s(x)=s(y)$。那么 $axa^{-1}=aya^{-1}$，从而

$$x=a^{-1}axa^{-1}a=a^{-1}aya^{-1}a=y,$$

因此 s 是单射。

（3）任取 $c\in G$。由于 $s(a^{-1}ca)=a(a^{-1}ca)a^{-1}=ece=c$，故 s 是满射。

综上所述，映射 $s: x\to axa^{-1}$ 是 G 到自身的自同构。