第一次作业

1.6

证明：因为$\sqrt{191}<14$，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$\sqrt{547}<24$，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 可知，737 与 747 都为合数。

1.11

解：小于等于$\sqrt{500}$的素数有 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。

1.17

(1) 78F5

(2) 2F4E

1.18

(1) 1010 1011 1100 1101 1110 1111 1010

(2) 1101 1110 1111 1010 1100 1110 1101 1010

(3) 1001 1010 0000 1010 1011

第二次作业

1.28

(1) (55, 85) = 5

(2) (202, 282) = 2

(3) (666, 1414) = 2

(4) (20785, 44530) = 5

1.32

(1) (1613, 3589) = 1，s = -1226，t = 551

(3) (20041, 37516) = 1，s = 13173，t = -7037

1.33

(1) (7, 10, 15) = 3*7 + (-2)*10 + 0*15 = 1

(2) (70, 98, 105) = -21*70 + 14*98 +1*105 = 7

(3) (180, 330, 405, 590) = 1014*180 + (-507)*330 + (-39)*405 + 1*590 = 5

1.50

(1) [8, 60] = 120

(2) [14, 18] = 126
(3) [49, 77] = 539
(4) [132, 253] = 3036

1.51
(1) $(a, b) = 2^2 * 3^3 * 5^3 * 7^2$ 　　$[a, b] = 2^7 * 3^5 * 5^5 * 7^7$
(2) $(a, b) = 1$ 　　$[a, b] = 2 * 3 * 5 * 7 * 11 * 13 * 17 * 19 * 23 * 29 = 6469693230$
(3) $(a, b) = 2 * 5 * 11 = 110$ 　　$[a, b] = 2^3 * 3 * 5^7 * 7 * 11^{13} * 13$
(4) $(a, b) = 101^{1000}$ 　　$[a, b] = 41^{11} * 47^{11} * 79^{111} * 83^{111} * 101^{1001}$

第三次作业

2.1
(1) 奇数完全剩余系，其中之一是 9、19、11、21、13、23、15、25、17。
(2) 偶数完全剩余系，其中之一是 0、10、20、30、40、50、60、70、80。
(3)（1）或（2）中的要求对模 10 不能实现。

2.6

解：$2^1 \equiv 2\left(\bmod 7\right)$， $2^2 \equiv 4\left(\bmod 7\right)$， $2^3 \equiv 1\left(\bmod 7\right)$

又 20080509 = 6693503*3

所以 $2^{20080509} \equiv \left(2^3\right)^{6693503} \equiv 1\left(\bmod 7\right)$

故 $2^{20080509}$ 是星期六。

2.17

(1) $a_k + a_{k-1} + ... + a_0 = 1+8+4+3+5+8+1 = 30$

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

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

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

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

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

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

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

2.19
解：不能被 5 和 13 整除。

第四次作业

1. 已知今天为周一，问2^{2020}天后为周几？

解　2^3=1 mod 7，而$2^{2020}=(2^3)^{673}\cdot 2\equiv 2 \ \mathrm{mod}\ 7$，因此$2^{2020}$天后是周三。

2. 写出模9的两个完全剩余系，要求其中一个完全剩余系中每个数均为奇数，另一个中每个数均为偶数。问对模10能否写出这样的两个剩余系？

解　均为偶数的完全剩余系为：0,10,2,12,4,14,6,16,8。

均为奇数的完全剩余系为：9,1,11,3,13,5,15,7,17。

对模10不存在上述完全剩余系，因为$\forall a,k\in Z, a+10k$与a有相同的奇偶性，不存在某一个完全剩余系满足其每一位元素均为奇数（或者偶数）。

3. 证明设a与b是整数，k与m是正整数,且$a\equiv b(\mathrm{mod}\ \ m)$,则$a^k\equiv b^k(\mathrm{mod}\ \ m)$。

证明　由于$a\equiv b(\mathrm{mod}\ \ m)$,

则由同余定义得: $m|a-b$,

又 $a^k-b^k=(a-b)(a^{k-1}+a^{k-2}b+\cdots ab^{k-2}+b^{k-1})$

因此 $a-b|a^k-b^k$,

结合 $m|a-b$,故由整除的传递性, $m|a^k-b^k$,即 $a^k\equiv b^k(\mathrm{mod}\ \ m)$。

4. 仿照例 2.3.10，给出$m=5$的最小非负剩余表。

解　设a表示第一列数,为与m互素的给定数. 设x表示第一行数,遍历模m的简化剩余系. 设a所在行与x所在列的交叉位置表示ax模m最小非负剩余. 则我们得到如下的列表：

$a\backslash x$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

5. 求$\varphi(2020)$。

解　2020的标准分解式为：$2020=2^2\cdot 5\cdot 101$

所以$\varphi(2020)=2020\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right)\cdot\left(1-\frac{1}{101}\right)=800$。

6. 证明如果m是正整数，a是与m互素的整数，且$(a-1,m)=1$，证明：

$$1+a+a^2+\cdots+a^{\varphi(m)-1}\equiv 0(\mathrm{mod}\ \ m)$$

证明　由欧拉定理有 $a^{\varphi(m)}\equiv 1(\mathrm{mod}\ \ m)$, 所以$a^{\varphi(m)}-1\equiv 0(\mathrm{mod} m)$

又$a^{\varphi(m)}-1=(a-1)\left(1+a+a^2+\cdots+a^{\varphi(m)-1}\right)\equiv 0(\mathrm{mod}\ \ \mathrm{m})$

且$(a-1,m)=1$

所以 $1+a+a^2+\cdots+a^{\varphi(m)-1}\equiv 0(\mathrm{mod}\ \ m)$。

7. 利用模重复平方算法计算$21^{39}\mathrm{mod}\ \ 100$。

解　将$39=1\times 2^0+1\times 2^1+1\times 2^2+0\times 2^3+0\times 2^4+1\times 2^5$二进制转换后，即

$(39)_2=100111$。

利用模重复平方算法：

$n_0=1 \qquad a_0=21, b_0=21^2\equiv 41 \mod 100$

$n_1=1 \qquad a_1=a_0\times b_0\equiv 61, b_1=b_0^2\equiv 81 \mod 100$

$n_2=1 \qquad a_2=a_1\times b_1\equiv 41, b_2=b_1^2\equiv 61 \mod 100$

$n_3=0 \qquad a_3=a_2\equiv 41, b_3=b_2^2\equiv 21 \mod 100$

$n_4=0 \qquad a_4=a_3\equiv 41, b_4=b_3^2\equiv 41 \mod 100$

$n_5=1 \qquad a_5=a_4\times b_4\equiv 81 \mod 100$

得到$21^{39}\equiv 81 \mod 100$。

8. 求解同余方程：$256x=179 \pmod{337}$。

解　由于(256,337)=1，所以方程组有唯一解。

考虑$256x\equiv 1 \pmod{337}$，广义欧几里得算法计算得到一个特解为$x\equiv 104 \pmod{337}$。故$256x\equiv 179 \pmod{337}$的一个特解为$x\equiv 104\times 179\equiv 81 \pmod{337}$。

9. 求解同余方程：$28x\equiv 21 \pmod{35}$。

解　由于$(28,35)=7$，且$7|21$，此同余方程有7个解。

考虑$4x=3 \pmod 5$，其特解为$x_0\equiv 2 \pmod 5$，所以原同余方程$28x\equiv 21 \pmod{35}$的一个特解为

$$x_0\equiv 2 \pmod{35}$$

所以原同余式的全部解为：$x\equiv 2+5t \pmod{35}, t=0,1,2,\cdots,6$ 或者 $x\equiv 2,7,12,17,22,27,32 \pmod{35}$。

10. 一个数被 3 除余 1，被 4 除余 2，被 5 除余 4，这个数最小是几？

解　实例化为同余方程组$\begin{cases} x\equiv 1 \pmod 3 \\ x\equiv 2 \pmod 4 \\ x\equiv 4 \pmod 5 \end{cases}$，运用中国剩余定理求解同余方程组：$m=3\times 4\times 5=60, M_1=4\times 5=20, M_2=3\times 5=15, M_3=3\times 4=12$

分别求解同余式$M_i'\times M_i\equiv 1 \pmod{m_i}$，得到$M_1'=2, M_2'=3, M_3'=3.$

则此同余方程组的解为：$x\equiv b_1M_1M_1'+b_2M_2M_2'+b_3M_3M_3'\equiv 1\times 20\times 2+2\times 15\times 3+4\times 12\times 3\equiv 34 \pmod{60}$，即最小的$x$为 34。

11. 一个数被 3 除余 2，被 7 除余 4，被 8 除余 5，这个数最小是几？

解　解题过程同于第 8 题,最后结果为 53。

12. 求解同余方程组

$$\begin{cases} x\equiv 3 & \pmod 8 \\ x\equiv 11 & \pmod 5 \\ x\equiv 1 & \pmod{15} \end{cases}$$

解　由于$m_1=8, m_2=5, m_3=15$，因此m_1,m_2,m_3并不两两互素,故不能直接应用中国剩余定理。

首先，易看出所求方程组与方程组(1)同解：

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 11 \pmod{5} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases} \qquad (1)$$

且$x \equiv 11 \pmod{5}$与$x \equiv 1 \pmod{5}$同解，因此进一步方程组(1)与方程组(2)同解：

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases} \qquad (2)$$

此时,直接运用中国剩余定理给出解: $x \equiv 91 \pmod{120}$。

13. 利用中国剩余定理计算$2^{2020} \bmod 77$。

解 令 $x = 2^{2020}$. 因为 $77 = 7 \cdot 11$, 所以计算 $x(\bmod 77)$等价于求解同余式组

$$\begin{cases} x \equiv 2^{2020} (\bmod 7) \\ x \equiv 2^{2020} (\bmod 11) \end{cases}$$

由 Euler 定理给出 $2^{\varphi(7)} \equiv 2^6 \equiv 1(\bmod 7)$, 以及 2020= 336·6+4,所以$x \equiv 2^{2020} \equiv (2^6)^{336} \cdot 2^4 \equiv 2(\bmod 7)$。

类似的，因为$2^{\varphi(11)} \equiv 2^{10} \equiv 1(\bmod 11)$，2020 =202·10,所以$x \equiv 2^{2020} \equiv (2^{10})^{202} \equiv 1(\bmod 11)$。

令$m_1 = 7, m_2 = 11, m = m_1 \cdot m_2 = 77, M_1 = m_2 = 11, M_2 = m_1 = 7$,分别求解同余式$11M_1' \equiv 1(\bmod 7), 7M_2' \equiv 1(\bmod 11)$，得到$M_1' = 2, M_2' = 8$，

故 $x \equiv 2 \cdot 11 \cdot 2 + 8 \cdot 7 \cdot 1 \equiv 100 \equiv 23(\bmod 77)$

因此，$2^{2020} \equiv 23(\bmod 77)$。

14. 设p为素数，$f(x)$为整系数多项式，且$f(x) = q(x)(x^p - x) + r(x)$，其中$q(x), r(x)$均为整系数多项式，且$r(x)$的次数小于$p$，证明$\forall\ a \in \mathrm{Z}, f(a) \equiv r(a) \pmod{p}$。

证明 由 Fermat 小定理，$a^p \equiv a \pmod{p}$，所以：$\forall a \in Z, p | q(a)(a^p - a)$

从而有: $p | f(a) - r(a)$

即：$f(a) \equiv r(a)(mod\ \ p)$

15. 证明若p和q是不同的素数,则$p^{q-1} + q^{p-1} \equiv 1 \pmod{p \cdot q}$。

证明 因为 $(p, q) = 1$,则由 Euler 定理知：

$$p^{\varphi(q)} = p^{q-1} \equiv 1 \pmod{q},\ q^{\varphi(p)} = q^{p-1} \equiv 1 \pmod{p}。$$

所以 $p^{q-1} + q^{p-1} \equiv 0 + 1 \equiv 1 \pmod{p}$

同理 $p^{q-1} + q^{p-1} \equiv 1 + 0 \equiv 1 \pmod{q}$

又 $[p, q] = p \cdot q$,

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

第五次作业

3.1

(1) 因为(17, 21) = 1 | 14，故原同余式有解

又$17x \equiv 1 \pmod{21}$的特解为$x_0 \equiv 5 \pmod{21}$

同余式$17x \equiv 14 \pmod{21}$的一个特解$x_0 \equiv 14 * x_0 = 14 * 5 \equiv 7 \pmod{21}$

所以解为：$x \equiv 7 \pmod{21}$

(2) 因为(15, 25) = 5 !| 9，故原同余式无解。

3.12

解：$m = m_1 \cdot m_2 \cdot m_3 = 990$

$M_1 = m_2 \cdot m_3 = 110,\ M_2 = m_1 \cdot m_3 = 99,\ M_3 = m_1 \cdot m_2 = 90$

$M_1' \cdot M_1 = 1 (\bmod m_1) \Rightarrow M_1' = 5 (\bmod 9)$

$M_2' \cdot M_2 = 1 (\bmod m_2) \Rightarrow M_2' = 9 (\bmod 10)$

$M_3' \cdot M_3 = 1 (\bmod m_3) \Rightarrow M_3' = 6 (\bmod 11)$

所以，$x = 550 b_1 + 891 b_2 + 540 b_3 (\bmod 990)$

3.18

解：$2^{1000000}$ (mod 1309) = 562

第六次作业

3.23

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

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

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

得解为：$x \equiv 0 \pmod 7 \quad x \equiv 6 \pmod 7$

3.24

解：$f'(x) \equiv 4x^3 + 7 \pmod{243}$

直接验算得同余式 $f(x) \equiv 0 \pmod 3$，有解 $x_1 \equiv 1 \pmod 3$

$f'(x_1) \equiv -1 \pmod 3$

$t_1 \equiv -f(x_1) * \left(f'(x_1)^{-1} \pmod 3\right) / 3^1 \equiv 1 \pmod 3, \qquad x_2 \equiv x_1 + 3t_1 \equiv 4 \pmod 9$

$t_2 \equiv -f(x_2) * \left(f'(x_1)^{-1} \pmod 3\right) / 3^2 \equiv 2 \pmod 3, \qquad x_3 \equiv x_2 + 3^2 t_2 \equiv 22 \pmod{27}$

$t_3 \equiv -f(x_3) * \left(f'(x_1)^{-1} \pmod 3\right) / 3^3 \equiv 0 \pmod 3, \qquad x_4 \equiv x_3 + 3^3 t_3 \equiv 22 \pmod{81}$

$t_4 \equiv -f(x_4) * \left(f'(x_1)^{-1} \pmod 3\right) / 3^4 \equiv 2 \pmod 3, \qquad x_5 \equiv x_4 + 3^4 t_4 \equiv 184 \pmod{243}$

所以，同余式 $f(x)\equiv 0 \pmod 3$ 的解为 $x_5\equiv 184 \pmod{243}$

4.1

(1) 模 p = 13 的二次剩余为 1、3、4、9、10、12，二次非剩余为 2、5、6、7、8、11。

4.2

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。

4.9

解：x = 12、33、72、93 (mod 105)。

第七次作业

4.13

略

4.20

(1) (17 / 37) = -1

(2) (151 / 373) = -1

(3) (191 / 397) = 1

(4) (911 / 2003) = 1

(5) (37 / 200723) = -1

(6) (7 / 20040803) = 1

4.26

(1) (7 / 227) = 1，有解

(2) (11 / 511) = -1，无解

(3) 有解

(4) 无解

第八次作业

5.1

解：$\because \varphi(13)=12\quad \therefore$ 只需对12的因数 $d=1,2,3,4,6,12$，计算 a^d

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

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。

5.2

解：$\because \varphi(19)=18 \quad \therefore$只需对18的因数$d=1,2,3,6,9,18$，计算$a^d\ (\bmod 19)$

$\because 3^1 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 8,\ 3^6 \equiv 7,\ 3^9 \equiv -1,\ 3^{18} \equiv 1 (\bmod 19)$

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。

5.3

解：$\because \varphi(11)=10=2\times 5 \quad \therefore q_1=2,\ q_2=5$

因此$\varphi(11)/q_1=5,\ \varphi(11)/q_2=2$

只需要验证 g^5，g^2 模 11 是否同余于 1 即可。对 2，3 等逐个演算，有

$2^5 = 10$，$6^5 = 10$，$7^5 = 10$，$8^5 = 10$ (mod 11)

所以，模 11 的原根有 2、6、7、8。