1、证明: $191, 547$ 都是素数, $737, 747$ 都是合数.

2、利用$Eratosthenes$ 筛法求出500 以内的全部素数.

3、求如下整数对的最大公因数:

(1) $(55, 85)$. (2) $(202, 282)$.

4、运用广义欧几里得除法求整数s, t 使得$sa + tb = (a, b)$.

(1) $1613, 3589$. (2) $2947,\ 3772$.

5、求出下列各对数的最大公因子及最小公倍数

(3) $2^3 5^7 11^{13},\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. (4) $47^{11} 79^{111} 101^{1001},\ 41^{11} 83^{111} 101^{1000}$.

1、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。

2、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：

3、

（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

4、

（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

5、

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

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

1. (1) 写出模9 的一个完全剩余系,它的每个数是奇数.
(2) 写出模9 的一个完全剩余系,它的每个数是偶数.
(3) (1)或(2)中的要求对模10的完全剩余系能实现吗?

2、下面哪些整数能被3整除，其中又有哪些整数能被9整除？

(1) 1843581. (2) 184234081. (3) 8937752744 (1) 4153768912246.

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、 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。

1. 求出下列一次同余方程的所有解.

(1) $3x \equiv 2 \pmod 7$. （2） $18x \equiv 30 \pmod{42}$

2. 将同余式方程化为同余式组来求解.

$$23x \equiv 1 \pmod{140}$$

3. 求模$p = 13,\ 23$ 的二次剩余和二次非剩余

4. 计算下列勒让得符号:

(1) $\left(\frac{17}{37}\right)$ （2）$\left(\frac{911}{2003}\right)$

5. 求下列同余方程的解数:

(1) $x^2 \equiv -2 \pmod{67}$ （2）$x^2 \equiv 2 \pmod{37}$.（3）$11x^2 \equiv -6 \pmod{91}$

1．（1）解：因为（3，7）=1 | 2 故原同余式有解

又 $3x\equiv1$（mod7） 所以 特解 $x_0' \equiv 5$（mod7）

同余式 $3x\equiv2$（mod7）的一个特解 $x_0\equiv2*x_0'=2*5\equiv3$（mod7）

所有解为：$x\equiv3$（mod7）

（2）解：$\because (18,42)=6|30$，

$\therefore$同余式有6个解，且等价于

$3x\equiv5(\bmod 7)$，

经观察可得$x\equiv4(\bmod 7)$

因此所求的6个解为

$x\equiv4,11,18,25,32,39(\bmod 42)$

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

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

4. （1）$(17/37) = (-1)^{(17-1)(37-1)/(2*2)} * (37/17) = -1$

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

5. （1）因为 $(-2/67) = (65/67) = 1$

所以 -2 是 67 的平方剩余

所以 $x^2 \equiv -2 \pmod{67}$ 有 2 个解。

（2）．因为（2/37）$=(-1)^{(37*37-1)/8}=-1$

所以 2 是 37 的平方非剩余

所以 $x^2\equiv 2 \pmod{37}$ 无解。

（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

1. 计算$2, 5, 10$ 模13 的指数.

2. 求模81的最小原根及原根的数量

3. 求解同余式

$$x^{22} \equiv 5 \pmod{41}.$$

4. 求解同余式

$$x^{22} \equiv 29 \pmod{41}.$$

1. 解：因为 $\varphi(13)=12$, 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 $\varphi(m)=\varphi(81)=54=2*3^3$, 所以 $\varphi(m)$ 的素因数为 $q_1=2$, $q_2=3$, 进而

$$\varphi(m)/q_1=27, \qquad \varphi(m)/q_2=18$$

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

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

所以 $(n,\varphi(m))\mid \mathrm{ind}5$，同余式有解

等价同余式为 $22\,\mathrm{ind}x\equiv \mathrm{ind}5 \pmod{40}$　　即 $11\,\mathrm{ind}x\equiv 11 \pmod{20}$

解得：$\mathrm{ind}x=1,21 \pmod{40}$

所以原同余式解为 $x=6,35 \pmod{41}$

4. 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。

1、 例：Klein群$G = \{ e, a, b, c \}$运算如图所示，每个元素的阶是多少？

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

2、 例：$G = \{1, -1, i, -i\}$，则$(G,\cdot)$是个交换群，那么每个元素的阶是多少？

3、求出$<N_6, \oplus>$关于子群$<\{0,3\}, \oplus>$的所有左陪集和右陪集，其中$N_6 = \{0,1,2,3,4,5\}$。

4、已知置换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$， $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$ ，求 $\tau\sigma$， $\sigma\tau$和σ^{-1}

5、将置换 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$， $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 2 & 6 & 7 & 5 & 3 \end{pmatrix}$ 写成不想交轮换的形式

1、

- e的阶是1
- a,b,c的阶都是2

3、 **解:**令H={0,3},则左陪集:

0H={0,3}=3H

1H={1,4}=4H

2H={2,5}=5H

从中可以看出：{0H,1H,2H}是G的一个划分。

2、

- 1的阶是1
- -1的阶是2
- i的阶是4
- $-i$的阶是4

4、

$$\tau\sigma=\begin{pmatrix}1&2&3&4&5\\5&1&3&4&2\end{pmatrix},\quad \sigma\tau=\begin{pmatrix}1&2&3&4&5\\1&2&5&3&4\end{pmatrix}$$

$$\sigma^{-1}=\begin{pmatrix}5&3&2&1&4\\1&2&3&4&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&3&2&5&1\end{pmatrix}$$

5、 **从σ中分解出来的第一个轮换式 (1 5 2 3 6)；第二个轮换为(4)；第三个轮换为 (7 8). σ的轮换表示式**

σ=(1 5 2 3 6) (4) (7 8)=(1 5 2 3 6) (7 8)

用同样的方法可以得到τ的分解式

τ=(1 8 3 4 2) (5 6 7)