**信息安全数学基础----习题集一**

1. 填空题

1、设a=18、b=12，c=27，求a、b、c的最小公倍数[a,b,c]= .

2、求欧拉函数= .

3、设，则模的最小非负简化剩余系 { }.

4、设，则模的所有平方剩余= .

5、设 ，则模的所有原根个数= .

6. 设m，n是互素的两个正整数，则*φ*(mn)=\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

7. 设m是正整数，a是满足的整数，则一次同余式：ax≡b (mod m)有解的充分必要条件是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 。

8. 设 m 是一个正整数，a是满足\_\_\_\_\_\_\_\_\_\_\_\_的整数，则存在整数a’，1≤a’＜m ，使得aa’≡1 (mod m)。

9. 设, 如果同余方程\_\_\_\_\_\_\_\_\_\_, 则叫做模的平方剩余.

**10.** 设, 则使得成立的最小正整数叫做对模的\_\_\_\_\_\_\_\_\_\_.

二、判断题（在题目后面的括号中，对的画“”，错的画“”）

1、若是任意正整数, 则. （ ）

2、设是个不全为零的整数，则与, ||, ||,…, ||的公因数相同 （ ）

3、设是正整数, 若, 则或. （ ）

4、设为正整数, 为整数, , 且, 则 . （ ）

5、{1,-3,8,4,-10}是模5的一个完全剩余系. （ ）

6、设是素数, 模的最小非负完全剩余系和最小非负简化剩余系中元素个数相等. （ ）

7、设为奇素数, 模的平方剩余和平方非剩余的数量各为8. （ ）

8、一次同余方程有解. （ ）

9、设是素数, 是模的原根, 若, 则是的整数倍. （ ）

10、设, 则, …, 构成模的简化剩余系. （ ）

11. , 则. （ ）

12. 设是两个互素正整数, 那么, 则 . （ ）

13. 设m是一个正整数, a,b,d都不为0，若ad≡bd(modm)。则a≡b(mod m)。

（ ）

14. 设为正整数, a是满足的整数，b为整数. 若为模的一个简化剩余系, 则也为模的一个简化剩余系. （ ）

15. p为素数,n为整数且与p互素，则n2为模p的平方剩余. （ ）

16. 设为正整数, 设, 则是模的平方剩余的充要条件是: . （ ）

17. 3是模7的原根。 （ ）

18. 设为正整数, 若，则. （ ）

19. 整数集关于整数的乘法构成群。 （ ）

20. 适当定义加法和乘法，集合{0,1}可以构成一个有限域。 （ ）

三、单项选择题（把答案写在题目后面的括号中）

1. 设与是两个整数, 则存在整数, 使得，下面关于与线性组合描述**错误**的是：（ ）

A. 整数的取值仅有一组唯一的值；

B. 整数的线性和所能表示的最小的正整数是最大公因数，即；

C. 的倍数也可以用的线性和表示；

D. 整数，可以使用辗转相除法(欧几里得算法)反推得到。

2、下面关于整除的描述**错误**的是：（ ）

A. ±1是任何整数的因子；

B. 设（整数集合）, , , 则；

C. 0是任何整数的倍数；

D. 设, 若, ，则,

3、下面的说法**正确**的是：（ ）

A. 给定一个正整数和两个整数，若，则

B. 设为整数, 若，则；

C. 设是两个正整数, 若分别遍历的完全剩余系, 则遍历模的完全剩余系；

D. 设为素数, 为任意正整数, 则

4. 下面哪个集合是模12的简化剩余系？ ( )。

A. 1,3,5,7 B. 1,5,7,9,

C. 1,5,7,11 D. 3,5,7,11。

5. 一次同余方程的解数是 （ ）

A. 3 B. 2 C. 1 D. 0

6、下面的说法**正确**的是： （ ）

A. 有解；

B、一次同余方程，等价于求解一次同余方程组:

的解；

C、一次同余方程组 有且仅有唯一的解；

D. 设是正整数, 对于一次同余方程组, 若, 则同余方程组一定有解。

7、设是奇素数, , ,则下列说法**错误**的是: （ ）

A. 如果是模的平方剩余, 是模的平方非剩余, 则是模的平方剩余.

B. 如果是模的平方剩余, 是模的平方非剩余, 则是模的平方非剩余.

C. 如果都是模的平方剩余, 则是模的平方剩余.

D. 如果都是模的平方非剩余, 则是模的平方剩余.

8、下面说法，**错误**的是（ ）

A、设p为奇素数，设, 若， 方程 方程肯定无解；

B、设是奇素数, 整数两两互素. 若既是模的平方剩余也是模的平方剩余，则不是模的平方剩余；

C、设是奇素数, 整数两两互素. 若既是模的平方剩余也是模的平方剩余, 既不是模的平方剩余也不是模的平方剩余，则不是模的平方剩余；

D、设是奇素数, , 只有)和同时有解，对于二次方程才有解。

9、已知5对模17的阶为16, 5×5≡8(mod17), 求的值是（ ）

A、2 B、4 C、6 D、8

10、下面说法**错误**的是（ ）

A、设是一个正合数, , 则集合对于乘法:

构成一个交换群；

B、设是一个正整数, 令, 即是所有整数的集合. 对于通常意义的加法(+)，是一个交换群；

C、设是一个素数, , , 是模的最小非负简化剩余系. 则集合对于乘法:

构成一个交换群；

D、设是一个奇素数, , 则集合对于乘法:

构成一个有限域。

11．设a, b, c是三个整数，c≠0且c|a，c|b，如果存在整数s, t, 使得sa＋tb＝1，则 ( ) 。

A. (a, b)= c B. c＝1

C. c＝sa＋tb D. c＝±1

12. 设a, b, c是三个不全为零的整数。如果 a = bq + c, 其中q是整数，则有( )。

A. (a, b) = (q, c) B. (a, b) = (b, c)

C. (a, b) = c D. (a, b) = (a, c)

13. 下面哪个集合不是模5的一个完全剩余系？ ( ) 。

A. 1, 3, 5, 7,9 B. 2,4,6,8,10

C. 0, 1, 2,11,13 D. 0, 1, 2, 13, 19。

14. 下面哪个集合是模18的简化剩余系？ ( )。

A. -1, 5, 7, 11, 13, 17

B. -1, 5, 9, 11, 13, 15,17

C. -5, 1, 5, 7, 11,17

D. 1, 3, 5, 7, 9.11, 13, 17。

15. 满足56≡18 (modm)的正整数m(m>2)的个数是( )。

A. 1 B. 2

C. 4 D. 5

16. 30模23的逆元是 ( ) 。

A. 23 B. 19

C. 10 D. 4

17. 下列一次同余式无解的是( )。

A. 12x≡3（mod 16）

B. 8x≡9（mod 19），

C. 78x≡30（mod 98）

D. 111x≡6（mod 51）。

18. 下面哪个是模13的平方剩余? ( )。

A. 5 B. 10

C. 11 D. 7

19．下面各组数中，均为模14的原根的是( )。

A. 2, 3, 4, 5 B. 3, 6, 8, 10

C. 9, 11, 13 D. 3, 5

20. 定义运算：, 下面哪个集合构成一个群.（ ）

A. {1,2,3,4} B. {1,3,5,7}

C. {1,,5,7,9} D. {1,5,7,11}

四、简答题

1. 设,,求整数,, 使得. （给出具体求解过程）

2. 计算71005(mod 15)。（给出具体求解过程，提示：可用欧拉定理）

3. 求7模26的阶ord26(7)，并给出所有模26的阶为ord26(7)的整数g（1<g<26）。（给出具体求解过程）

4. 判断同余方程*x*2≡3(mod 11)的解的情况。（给出具体求解过程）

5. 中多项式, , 给f（x）除以g（x）的商和余式

6. a＝42，b＝164，求a和b的最大公因子（a，b）及整数x和y，使

（a, b）＝ax＋by.

7. 结合欧拉定理和模重复平方算法(或者平方乘算法)计算62025（mod41）

8. 写出模17的所有平方剩余。

9. 计算5模19的指数ord19(5)。

五、综合题（备注，每题必须给出具体求解过程）

1. 求解一次同余方程 84x+1≡64(mod 371).

**信息安全数学基础----习题集一答案**

第一题　填空

1、108 2、800 3、{1,2,4,5,7,8} 4、{1,3,4,5,9 } 5、4

6、*φ*(m)*φ*(n) 7、(a,m)|b 8、(a,m)=1 9、有解 10、阶

二、判断题

1—5：×√××√ 6-10：×√×√×

11—15：√√××√ 16-20：×√√×√

三、单项选择题

1-5：ACBCD 6-10：CABDA

11-15：DBCCB 16-20：CABDD

四、简答题

1、101=156+11 15=11+4 11=42+3 4=31+1

因此(a,b)=（101,15）=1

1=4-3=4-(11-42)=4-11=(15-11)-11=15

=15

因此s=27 ，t=-4

备注：s=27 t=-4不是唯一答案，只要满足 都正确

2、解：71005(mod 15)，

已知（7,15）=1，由欧拉定理，

因此71005 (mod 15)

(mod 15) (mod 15) (mod 15)

因此 71005mod 15)

备注：此计算方法不是唯一，也可以用中国剩余定理化简求解

3、（1）已知26=2， =12。

（2）72≡23，73≡-21 76≡25 ，7是模26的一个原根, ord26(7)=12

因为模12的简化剩余系为{1,5,7,11}, 故模26的所有原根为:

71≡7, 75≡11, 77≡-33≡-7≡19, 711≡-7\*9 ≡-11≡15 (mod 26).

即模26的原根为:7,11,19,15

4、解：判断同余方程*x*2≡3(mod 11)的解的情况

根据欧拉判别式进行求解进行判断

即3是模11的平方剩余，即*x*2≡3(mod 11)方程有解

备注：判断*x*2≡3(mod 11)方程解情况也可采用0,1,…..,5代入方程穷举方法求解。

5、 解：长除法可得

商式，余式

6、164=423+38 42=38+4 38=49+2 4=22

因此(a,b)=（166,42）=2

2=38-49=38-(42-38)9=38-429=(164-423)-429=164

备注：不是唯一答案，只要满足 都正确

7、解：62017（mod41），

已知（6,41）=1，由欧拉定理，

因此62017（mod41）617（mod41）

(mod 41) (mod 41) (mod 41)

(mod 41)

因此 62017mod 41)

8、1,22mod 17), 32mod 17), 42mod 17),

52mod 17), 62mod 17), 72mod 17)，82mod 17)，

模17的所有平方剩余为1，2，4，8，9，13，15，16

9、

52≡6(mod19)，53≡11(mod19)，56≡7(mod19)，59≡1(mod19) (4分)

ord19(5)=9

五、综合题（备注，每题必须给出具体求解过程）

求解一次同余方程 84x+1≡64(mod 371)

由原方程得84x≡63(mod 371)

（84，371）=7|63，故方程有解。

要解84x≡63(mod 371)，需先求12x≡9(mod53) 的解

先解12x≡1(mod53)

53=12×4+5 12=5×2+2 5=2×2+1

1=5-2×2=5-2×（12-5×2）=5×5-12×2

=5×（53-12×4）-12×2=5×53-12×22

故12x≡1(mod53)的解为x≡31（mod53）

12x≡9(mod 49) 的解为x≡14（mod53）

故84x≡63(mod 301)得全部解为x≡14+53t（mod371），t=0,1,2…,6