**信息安全数学基础----习题集二**

一、填空题（把答案写在题目中的横线上。）

1、设a=24、b=78，求a和b的最小公倍数[a,b]= .

2、求欧拉函数= .

3、设p是奇素数，则勒让得符号 .

4、设，则模的最小非负简化剩余系={ }.

5、-5 (mod 11)= （结果要在模11的最小非负剩余系中）

6、设m=5,求2对模5的阶 .

7、设*p*=113，则勒让得符号 .

二、判断题（在题目后面的括号中，对的画“”，错的画“”）

1、设是三个整数, 且. 如果, 则 （ ）

2、是任何整数的倍数 （ ）

3、 设是两个给定的整数, . 那么, 一定存在唯一的一对整数与, 满足, . （ ）

4、设为正整数, 为整数, ，则. （ ）

5、{1,-3,8,4}是模5的一个简化剩余系 （ ）

6、设为正整数, 模的一个简化剩余系中的元素，可以都是奇数或都是偶数 （ ）

7、一次同余方程有解 （ ）

8、设为奇素数, 模的平方剩余和平方非剩余的数量各为个. （ ）

9、设, 则. （ ）

10、设<, o>为群, 则群中任何元素与其逆元具有相同的阶. （ ）

11、设是三个整数, 若, , 且存在整数, 有, 则 （ ）

12、设为素数，*a*为正整数，则欧拉函数. （ ）

13、若用Miller-Rabin素性检测算法，如果该算法判定一个数是素数, 这个数肯定是素数。 （ ）

14、设为正整数, 为整数, 且, 则 （ ）

15、设是素数, 则模的完全剩余系和简化剩余系中元素个数相等 （ ）

16、只有是素数时, 模的原根才存在. （ ）

17、同余方程有解, 因此4叫做模8的平方剩余 （ ）

18、设为奇素数, 模的平方剩余和平方非剩余的数量各为个. （ ）

19、设, 为整数，，若是模的原根，则模的指数等于. （ ）

（ ）

三、单项选择题（把答案写在题目后面的括号中）

1. 关于下面说法描述**错误**的是：

A. 设为素数，则欧拉函数；

B. 设为素数，则欧拉函数；

C. 设素数，*a*为整数，则；

D. 设为素数，*a*为正整数，则欧拉函数。

2. 关于Miller-Rabin素性检测算法，下面描述正确的是：

A. 如果该算法判定一个数是合数, 这个数肯定是合数；

B. 如果该算法判定一个数是素数, 这个数肯定是素数。

C. 该算法常用来求两个整数的最大公因数；

D. 其理论基础是欧几里德除法；

3. 关于下面说法描述**错误**的是：（ ）

A. 设是一个正整数, 满足（*a*,*m*）=1的整数, 如果遍历模的一个完全剩余系, 则也遍历模的一个完全剩余系.

B. 设是正整数, 模的最小非负完全剩余系和绝对值最小完全剩余系中元素个数相等.

C.设为正整数, 整数均与互素,且模m两两不同余，则它们构成模的一个简化剩余系.

D、设是非零整数, 为任意整数. 若为模的一个完全剩余系, 则也是模的一个完全剩余系.

4. 一次同余方程的解数是（ ）

A. 4 B. 3 C. 2 D.1

5. 模11的所有平方非剩余为（ ）

A. 2,6,7,8,10 B. 1,6,7,8,10

C. 2,6,7,8 D. 1,2,6,7,8

6.下面哪个一次同余方程无解？ （ ）

A. B.

C. D.

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. 如果都是模的平方剩余, 则是模的平方剩余.

C. 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.

D. 如果都是模的平方非剩余, 则是模的平方剩余.

8. 下面描述**错误**的是：（ ）

A. 若设, 如果同余方程有解, 则叫做模的平方剩余

B．设为奇素数, 设, 若是模的平方剩余，则

C．设为奇素数, , 则勒让得符号

D. 设为奇素数, , 则勒让得符号

9. 设, 为整数，. 关于原根和指数，下列描述哪个是**错误**的？（ ）

A. 模的指数一定存在；

B. 若是模的原根，则模的指数等于；

C. 若是模的原根，则, …, 构成模的一个完全剩余系；

D. 模的指数整除。

10. 下面哪个一次同余方程组可以直接用孙子定理求解？ （ ）

A. B.

C. D.

11. 关于素数，下面描述**错误**的是： （ ）

A. 设是大于1的整数, 如果除了约数1和它本身外没有其它的约数, 就是素数；

B. 为素数, 是正整数, 当2p且, 则是素数；

C. 素数的个数有无穷多。

D. 互素的两个整数必有一个为素数；

12. 下面关于完全剩余系说法描述**正确**的是：（ ）

A. 模的完全剩余系中，集合1, …, ,m称为最小非负完全剩余系；

B. 设是一个正整数, 满足（a,m）=1的整数, 如果遍历模的一个完全剩余系, 则也遍历模的一个完全剩余系；

C. 设是非零整数, 为任意整数. 若为模的一个完全剩余系, 则也是模的一个完全剩余系；

D. 设为正整数，完全剩余系则恰好由个数组成。

13. 设是素数, 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, 则下面说法不正确的是: （ ）

A. 不是模的平方剩余.

B. 不是模的平方剩余.

C. 不是模的平方剩余.

D. 不是模的平方剩余.

14. 一次同余方程的解数是（ ）

A. 4 B. 3 C. 2 D.1

15. 下面哪个数是模5的原根（ ）

A. 1 B. 4 C. 2 D. 0

16.下面哪个一次同余方程有解？ （ ）

A.

B.

C.

D.

17. 设是奇素数, , 对于二次方程的解的判断, 下面说法正确的是: （ ）

A. 只有和同时有解, 原方程有解. ?

B. 若和中有一个无解, 则原方程无解.

C. 只有和同时无解, 原方程无解.

D. 只有)和同时有解, 原方程有解.

18. 下面描述**错误**的是：（ ）

A. 若设, 如果同余方程无解, 则叫做模的平方非剩余

B．设为奇素数, 设, 若是模的平方非剩余，则

C．设为奇素数, , 则勒让得符号

D. 设为奇素数, , 则勒让得符号

19. 关于原根和指数，下列描述哪个是**正确**的？（ ）

A．设, 为整数， 模的指数一定存在.

B. 根据费马小定理, 26≡1(mod7),故ord7(2)=6；

C. 设是正整数,, 若, 则。

D. 设是素数, 是模的原根, 若, 则是的整数倍.

20. 设是正整数, 对于一次同余方程组,下面说法正确的是: （ ）

A. 若, 则同余方程组一定有解.

B. 如果同余方程组无解, 则不是两两互素的整数.

C. 若是两两互素的整数, 则同余方程组一定有解.

D. 若是两两互素的整数, 则同余方程组有唯一解.

四、简答题

1. 设m为正整数, a,b,c,d为整数, 如果a≡b(mod⁡m), c≡d(mod⁡m), 则

(i) a+c≡b+d(mod m)；

(ii) ac≡bd(mod m). 给出证明。

2. 求模19的原根个数，并给出模19的所有原根。（给出具体求解过程）

3. 判断同余方程*x*2≡54(mod 101)的解的情况。（给出具体求解过程）

4. 设,,求整数,, 使得. （给出具体求解过程）

5. 求模13的原根个数，并给出模13的所有原根。（给出具体求解过程）

6. 已知中多项式, 求.

7. 计算。(给出具体求解过程，提示：可以利用欧拉定理简化计算)

五、综合题（备注，每题必须给出具体求解过程）

1. 解一次同余方程 12*x*≡9×5127(mod 27).

**信息安全数学基础----习题集二答案**

第一题　填空

1、312 2、100 3、1 4、{1,5} 5、6 6、4 7、1

二、判断题

1—5：√×××√ 6-10：××√×√

11—15：√√×√×16-19：× ×√×

三、单项选择题

1—5：CADBA 6-10：BADCA

11—15：DBAAC 16-20：CDBAD

四、简答题

1、证明:

证明: 已知且, 则存在整数和, 使等式且成立.

故 ,

.

两边同mod m，即

(i) a+c≡b+d(mod m)；

(ii) ac≡bd(mod m).

2、解：

已经19是素数，根据定理，必定有原根，故19有原根，则其原根个数必定为

因此模19必定有6个原根。

则首先判断2是否是模19的原根， 2是模19的原根，因此模19的所有原根,其中d为模18的简化剩余系{1,5,7,11,13,17}。

模19的所有原根为：

21≡2, 25≡13, 27≡14, 211≡15, 213≡3, 217≡10 (mod 17).

即模19的所有6个原根为: 2, 13, 14, 15,3,10

3、解：

欧拉判别式进行求解进行判断

可以采用模重复平方或者平方剩余，或者直接分解求模幂运算，最后结果，方程有解

4、解：

75=213+12 21=12+9 12=9+3 9=3\*3+0

因此(a,b)=（3,0）=3

3=12-9=12-(21-12)=2-21=2

=

因此s=2 ，t=-7

5、解：

已经13是素数，根据定理，必定有原根，故13有原根，则其原根个数必定为

因此模13必定有4个原根。

其中2和3是12的素因子，则首先判断2是否是模13的原根， 2是模13的原根，所有原根,其中d为模12的简化剩余系{1,5,7,11}。

模13的所有原根为：

21≡2, 25≡6, 27≡11, 211≡7 (mod 13)

即模13的所有4个原根为: 2,6,11,7

6、解: 由欧几里德算法, 计算.

① =+

即: ()=()

② =+1

即: ()= ()=1

故=1.

7、解：(6,247)=1，根据欧拉定理可知 (mod 247).

五、综合题（备注，每题必须给出具体求解过程）

1. 解一次同余方程 12*x*≡9×5127(mod 27).

解：(27)=18, 5127(mod 27)= 518\*7+1(mod 27)=5

同余方程12*x*≡9×5127(mod 27) 等价于 12*x*≡9\*5=18 (mod 27)

（12,27）=3, 因为3|18，因此方程有解，有三个解

首先求解 4*x*≡1(mod 9)

求解为： *x*≡7(mod 9)

因此方程的三个解为： x≡7\*6+9t ≡15+9t(mod 27) t=0,1,2