信息安全数学基础----习题集一

一、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φ(3000)=______________________.

3、设$m=9$，则模m的最小非负简化剩余系= {____________________}.

4、设$m=11$，则模m的所有平方剩余=______________________________.

5、设$m=22$ ，则模m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 $m \nmid a$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$a \in Z, (a, m) = 1$，如果同余方程$x^2 \equiv a(\bmod m)$__________，则a叫做模m的平方剩余.

10. 设$a, m \in Z, m > 1, (a, m) = 1$，则使得$a^e \equiv 1(\bmod m)$成立的最小正整数$e$叫做$a$对模$m$的__________.

二、判断题（在题目后面的括号中，对的画“√”，错的画“×”）

1、若k是任意正整数，则$(ak, bk) = (a, b)$. （ ）

2、设$a_1, a_2, \ldots, a_n$是n个不全为零的整数，则$a_1, a_2, \ldots, a_n$与$a_1, |a_2|, |a_3|, \ldots, |a_n|$的公因数相同 （ ）

3、设m是正整数，若$m \mid ab$，则$m \mid a$或$m \mid b$. （ ）

4、设m为正整数，a, b为整数，$a \equiv b(\bmod m)$，$d \mid b$ 且$d > 0$， 则 $\frac{a}{d} \equiv \frac{b}{d}(\bmod \frac{m}{d})$. （ ）

5、{1,-3,8,4,-10}是模 5 的一个完全剩余系. （ ）

6、设m是素数，模m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$p = 17$为奇素数，模p的平方剩余和平方非剩余的数量各为 8. （ ）

8、一次同余方程 $9x \equiv 1(\bmod 24)$有解. （ ）

9、设p是素数，g是模p的原根，若$g^x \equiv 1(\bmod p)$，则x是$p-1$的整数倍.

（　）

10、设$m>1, (a,m)=1$，则$1=a^0, a, a^2$，⋯，$a^{\mathrm{ord}_m(a)-1}$构成模m的简化剩余系.　（　）

11. $b \neq 0$，则$(0,b)=|b|$.　（　）

12. 设a,b是两个互素正整数，那么$a \mid m, b \mid m$，则 $ab \mid m$.　（　）

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m为正整数, a 是满足$(a,m)=1$ 的整数，b 为整数. 若$r_1, r_2, \ldots, r_{\varphi(m)}$为模$m$的一个简化剩余系，则$ar_1+b, ar_2+b, \ldots, ar_{\varphi(m)}+$b 也为模$m$的一个简化剩余系.　（　）

15. p 为素数,n 为整数且与 p 互素，则 n^2 为模 p 的平方剩余.　（　）

16. 设p为正整数，设$a \in Z, (a,p)=1$，则a是模p的平方剩余的充要条件是：$a^{\frac{p+1}{2}} \equiv 1(\bmod p)$.　（　）

17. 3 是模 7 的原根。　（　）

18. 设$a, m \in Z, m>1, (a,m)=1, d$为正整数，若$a^d \equiv 1(\bmod m)$，则$\mathrm{ord}_m(a) | d$.　（　）

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a与b是两个整数，则存在整数s,t，使得$(a,b)=sa+tb$，下面关于a与b线性组合描述**错误**的是：（　）

A. 整数s,t的取值仅有一组唯一的值；

B. 整数a,b的线性和所能表示的最小的正整数是a,b最大公因数，即$sa+tb=(a,b)$；

C. (a,b)的倍数也可以用a,b的线性和表示；

D. 整数s,t，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$a, b \in Z$（整数集合），c $\neq 0$ $c|b$, $c|a$, 则$c|a \pm b$；

C. 0 是任何整数的倍数；

D. 设$a, b \in Z$, 若 $b|a$, $b \neq 0$，则$b|-a$, $-b|-a$。

3、下面的说法**正确**的是：（　　）

A. 给定一个正整数m和两个整数a, b，若$a \equiv b(\bmod m)$，则$(a-b)|m$

B. 设 a, b 为整数，若 $a \equiv b(\bmod m_i), (i=1,2,\ldots,k)$，则 $a \equiv b(\bmod [m_1, m_2, \ldots, m_k])$；

C. 设m_1, m_2是两个正整数，若x_1, x_2分别遍历m_1, m_2的完全剩余系，则$m_2 x_1 + m_1 x_2$遍历模$m_1 m_2$的完全剩余系；

D. 设p为素数，a为任意正整数，则$a^{p-1} \equiv 1(\bmod p)$。

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$3^{1000}x \equiv 9(\bmod 27)$的解数是　　　（　　）

A. 3　　B. 2　　C. 1　　D. 0

6、下面的说法**正确**的是：　　　　（　　）

A. 一次同余方程 $21x \equiv 55(\bmod 77)$有解；

B、一次同余方程$x \equiv 6(\bmod 15)$，等价于求解一次同余方程组:
$\begin{cases} x \equiv 2(\bmod 3) \\ x \equiv 3(\bmod 5) \end{cases}$ 的解；

C、一次同余方程组 $\begin{cases} x \equiv 5 \ (\bmod 13) \\ x \equiv 20 \ (\bmod 23) \end{cases}$有且仅有唯一的解；

D. 设b_i, m_i是正整数，对于一次同余方程组$x \equiv b_i(\bmod m_i), i=1,2,3$，若$(b_i, m_i)=1$，则同余方程组一定有解。

7、设p是奇素数, $(a_1, p)=1$, $(a_2, p)=1$,则下列说法**错误**的是:　（　　）

A. 如果a_1是模p的平方剩余，a_2是模p的平方非剩余，则$a_1 a_2$是模p的平方剩余.

B. 如果a_1是模p的平方剩余，a_2是模p的平方非剩余，则$a_1 a_2$是模p的平方非

剩余.

C. 如果a_1, a_2都是模p的平方剩余，则$a_1 a_2$是模p的平方剩余.

D. 如果a_1, a_2都是模p的平方非剩余，则$a_1 a_2$是模p的平方剩余.

8、下面说法，**错误**的是（　　　）

A、设 p 为奇素数，设$a \in Z, (a,p)=1$，若$a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p)$，方程 $x^2 \equiv a(\mathrm{mod}\, p)$方程肯定无解；

B、设p, q是奇素数，整数a, b, p, q两两互素. 若a既是模p的平方剩余也是模q的平方剩余，则a不是模pq的平方剩余；

C、设p, q是奇素数，整数a, b, p, q两两互素. 若a既是模p的平方剩余也是模q的平方剩余，b既不是模p的平方剩余也不是模q的平方剩余，则ab不是模p的平方剩余；

D、设p, q是奇素数，（ab, pq）$=1$，只有$x^2 \equiv ab(\mathrm{mod}\, p)$)和$x^2 \equiv ab(\mathrm{mod}\, q)$同时有解，对于二次方程$x^2 \equiv ab(\mathrm{mod}\, pq)$才有解。

9、已知 5 对模 17 的阶为 16, 5×5≡8(mod17)，求$\mathrm{ord}_{17}(8)$的值是（　）

A、2　　B、4　　C、6　D、8

10、下面说法**错误**的是（　　）

A、设n是一个正合数，$Z_n=\{0,1,2,3,\ldots,n-1\}$，则集合$Z_n\setminus\{0\}$对于乘法:

$$a \otimes b = a \times b (\mathrm{mod}\, n)$$

构成一个交换群；

B、设n是一个正整数，令$Z=\{\ldots,-n,\ldots,-2,-1,0,1,2,\ldots,n,\ldots\}$，即$Z$是所有整数的集合. 对于通常意义的加法(+)，$Z$是一个交换群；

C、设p是一个素数，$F_p = Z/pZ = \{0,1,2,3,\ldots,p-1\}$，$F^* = F_p \setminus \{0\}$，$F^*$是模$p$的最小非负简化剩余系. 则集合$F^*$对于乘法:

$$a \otimes b = a \times b (\mathrm{mod}\, p)$$

构成一个交换群；

D、设n是一个奇素数，$Z_n=\{0,1,2,3,\ldots,n-1\}$，则集合$Z_n\setminus\{0\}$对于乘法:

$$a \otimes b = a \times b (\mathrm{mod}\, n)$$

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⊗：$a \otimes b = a \times b (\mathrm{mod}\ 12)$，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/计算题

1. 设$a = 15, b = 101$,求整数s,t，使得$as + tb = (a,b)$.（给出具体求解过程）

2. 计算 7^{1005}(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 $\mathrm{ord}_{26}(7)$，并给出所有模 26 的阶为 $\mathrm{ord}_{26}(7)$的整数 g（1<g<26）。（给出具体求解过程）

4. 判断同余方程 $x^2 \equiv 3(\mathrm{mod}\ 11)$的解的情况。（给出具体求解过程）

5. $F_2[x]$中多项式$g(x) = x^2 + x + 1$，$f(x) = x^5 + x^3 + x^2 + x + 1$，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 6^{2025}（mod41）

8. 写出模 17 的所有平方剩余。

9. 计算 5 模 19 的指数 $\mathrm{ord}_{19}(5)$。

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).