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$\varphi(125)$=_____.

3、设 p 是奇素数，则勒让得符号$\left(\frac{1}{p}\right)=$ _____.

4、设$m=6$，则模m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$\mathrm{ord}_5(2)=$_____.

7、设 p=113，则勒让得符号$\left(\frac{1}{p}\right)=$ _____.

二、判断题（在题目后面的括号中，对的画“√”，错的画“×”）

1、设a,b,c是三个整数，且$c\neq 0$. 如果$c|ab,(a,c)=1$，则$c|b$ （ ）

2、0 是任何整数的倍数 （ ）

3、 设a,b是两个给定的整数，$b>0$. 那么，一定存在唯一的一对整数q与r，满足$a=qb+r,\ \ 0<r<b$. （ ）

4、设m为正整数，a,b,d为整数，$ad\equiv bd(\mathrm{mod}\,m)$，则$a\equiv b(\mathrm{mod}\,m)$.

（ ）

5、{1,-3,8,4}是模 5 的一个简化剩余系 （ ）

6、设m为正整数，模m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$12x\equiv 1(\mathrm{mod}\ 15)$有解 （ ）

8、设p为奇素数，模p的平方剩余和平方非剩余的数量各为$\frac{p-1}{2}$个. （ ）

9、设$a,m\in Z,m>1$，则$\mathrm{ord}_m(a)|m$. （ ）

10、设$<G, o>$为群，则群中任何元素a与其逆元a^{-1}具有相同的阶. （ ）

11、设$a, b, c \neq 0$是三个整数，若$c|a, c|b$，且存在整数s, t，有$m = sa + tb$，则$c|m$ （ ）

12、设p为素数，a为正整数，则欧拉函数$\varphi(p^a) = (p-1)p^{a-1}$. （ ）

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 m 为正整数，a, b 为整数，$a \equiv b(\bmod m)$且$d \mid m$，则$a \equiv b(\bmod d)$ （ ）

15、设 p 是素数，则模 p 的完全剩余系和简化剩余系中元素个数相等 （ ）

16、只有 m 是素数时，模 m 的原根才存在. （ ）

17、同余方程$x^2 \equiv 4(\bmod 8)$有解，因此 4 叫做模 8 的平方剩余 （ ）

18、设p为奇素数，模p的平方剩余和平方非剩余的数量各为$\frac{p-1}{2}$个. （ ）

19、设a，m为整数，$m > 1$，$(a, m) = 1$，若a是模m的原根，则a模m的指数等于$\varphi(\varphi(m))$. （ ）

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p为素数，则欧拉函数$\varphi(p) = p - 1$；

B. 设p, q为素数，则欧拉函数$\varphi(pq) = (p-1)(q-1)$；

C. 设p素数，a为整数，则$a^{p-1} \equiv 1(mod\ p)$；

D. 设p为素数，a为正整数，则欧拉函数$\varphi(p^a) = (p-1)p^{a-1}$。

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m是一个正整数, a满足(a,m)=1 的整数, 如果x遍历模m的一个完全剩余系, 则ax也遍历模m的一个完全剩余系.

B. 设 m 是正整数, 模 m 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 m 为正整数, 整数$r_1, r_2, ..., r_{\varphi(m)}$均与 m 互素,且模 m 两两不同余, 则它们构成模 m 的一个简化剩余系.

D、设 a 是非零整数, b 为任意整数. 若$r_0, r_1, ..., r_{m-1}$为模 m 的一个完全剩余系, 则$ar_0 + b, ar_1 + b, ..., ar_{m-1} + b$ 也是模 m 的一个完全剩余系.

4. 一次同余方程 $12 \times 7^{168}x \equiv 9(\mathrm{mod}\,27)$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. $22x \equiv 55(\mathrm{mod}\,77)$ B. $33x \equiv 55(\mathrm{mod}\,66)$
C. $66x \equiv 33(\mathrm{mod}\,99)$ D. $55x \equiv 44(\mathrm{mod}\,66)$

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_1a_2是模 p 的平方剩余.

B. 如果a_1, a_2都是模 p 的平方剩余, 则a_1a_2是模 p 的平方剩余.

C. 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_1a_2是模 p 的平方非剩余.

D. 如果a_1, a_2都是模 p 的平方非剩余, 则a_1a_2是模 p 的平方剩余.

8. 下面描述**错误**的是：（ ）

A. 若设 $a \in Z, (a, m) = 1$, 如果同余方程$x^2 \equiv a \pmod m$有解, 则 a 叫做模 m 的平方剩余

B. 设 p 为奇素数, 设 $a \in Z, (a, p) = 1$, 若 a 是模 p 的平方剩余，则$a^{\frac{p-1}{2}} \equiv 1 \pmod p$

C. 设 p 为奇素数, $a \in Z, (a, p) = 1$, 若 a 是模 p 的非平方剩余，则勒让得符号$\left(\frac{a}{p}\right) = -1$

D. 设 p 为奇素数, $a \in Z, (a, p) = 1$, 若 a 是模 p 的平方剩余，则勒让得符号$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}$

9. 设a, m为整数，$m > 1$，$(a, m) = 1$. 关于原根和指数，下列描述哪个是**错误**的？（ ）

A. a模m的指数一定存在；

B. 若a是模m的原根，则a模m的指数等于$\varphi(m)$；

C. 若a是模m的原根，则 $1 = a^0, a, a^2, \cdots, a^{\mathrm{ord}_m(a)-1}$ 构成模m的一个完全剩余系；

D. a模m的指数整除$\varphi(m)$。

10. 下面哪个一次同余方程组可以直接用孙子定理求解？ （ ）

A. $\begin{cases} x \equiv 5 \pmod{13} \\ x \equiv 20 \pmod{23} \end{cases}$ B. $\begin{cases} x \equiv 3 \pmod{13} \\ x \equiv 5 \pmod{26} \end{cases}$

C. $\begin{cases} x \equiv 5 \pmod{15} \\ x \equiv 20 \pmod{25} \end{cases}$ D. $\begin{cases} x \equiv 15 \pmod{25} \\ x \equiv 5 \ (15) \end{cases}$

11. 关于素数，下面描述**错误**的是： （ ）

A. 设p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，p就是素数；

B. p为素数，n是正整数，当 2≤p≤ $\sqrt{n}$且 $p \nmid n$，则n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 m 的完全剩余系中，集合 1, …, m − 1,m 称为最小非负完全剩余系；

B. 设 m 是一个正整数, a 满足（a,m）=1 的整数，如果 x 遍历模 m 的一个完全剩余系，则 ax 也遍历模 m 的一个完全剩余系；

C. 设 a 是非零整数, b 为任意整数. 若$r_0, r_1, \ldots, r_{m-1}$为模 m 的一个完全剩余系，则$ar_0 + b, ar_1 + b, \ldots, ar_{m-1} + b$ 也是模 m 的一个完全剩余系；

D. 设 m 为正整数，完全剩余系则恰好由$\varphi(m)$个数组成。

13. 设 p, q 是素数，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，则下面说法不正确的是: （　　）

A. a 不是模 pq 的平方剩余.

B. ab 不是模 p 的平方剩余.

C. ab 不是模 q 的平方剩余.

D. b 不是模 pq 的平方剩余.

14. 一次同余方程 $12x \equiv 8(\mathrm{mod}\,28)$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. $12x \equiv 1(\mathrm{mod}\,24)$

B. $12x \equiv 2(\mathrm{mod}\,15)$

C. $3x \equiv 12(\mathrm{mod}\,24)$

D. $12x \equiv 4(\mathrm{mod}\,15)$

17. 设 p, q 是奇素数，（ab, pq） = 1，对于二次方程$x^2 \equiv ab(\mathrm{mod}\,pq)$的解的判断，下面说法正确的是:（　　）

A. 只有$x^2 \equiv a(\mathrm{mod}\,pq)$和$x^2 \equiv b(\mathrm{mod}\,pq)$同时有解，原方程有解.？

B. 若$x^2 \equiv a(\mathrm{mod}\,pq)$和$x^2 \equiv b(\mathrm{mod}\,pq)$中有一个无解，则原方程无解.

C. 只有$x^2 \equiv ab(\mathrm{mod}\,p)$和$x^2 \equiv ab(\mathrm{mod}\,q)$同时无解，原方程无解.

D. 只有$x^2 \equiv ab(\mathrm{mod}\,p))$和$x^2 \equiv ab(\mathrm{mod}\,q)$同时有解，原方程有解.

18. 下面描述**错误**的是：（ ）

A. 若设$a \in Z, (a, m) = 1$，如果同余方程$x^2 \equiv a(\mathrm{mod}\,m)$无解，则 a 叫做模 m 的平方非剩余

B．设 p 为奇素数，设$a \in Z, (a, p) = 1$，若 a 是模 p 的平方非剩余，则$a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\,p)$

C．设 p 为奇素数, $a \in Z, (a, p) = 1$，若 a 是模 p 的非平方剩余，则勒让得符号$\left(\frac{a}{p}\right) = -1$

D. 设 p 为奇素数, $a \in Z, (a, p) = 1$，若 a 是模 p 的平方剩余，则勒让得符号$\left(\frac{a}{p}\right) = 1$

19. 关于原根和指数，下列描述哪个是**正确**的？（　　）

A．设a，m为整数，$m > 1$，$(a, m) = 1$, a 模 m 的指数一定存在.

B. 根据费马小定理, $2^6 \equiv 1(\mathrm{mod}\,7)$,故 $ord_7(2)=6$；

C. 设 m 是正整数, $m > 1, (a, m) = 1$, 若$a^d \equiv 1(\bmod m)$, 则 d|φ(m)。

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

20. 设b_i, m_i是正整数, 对于一次同余方程组 $x \equiv b_i(\bmod m_i), i = 1,2,3,$下面说法正确的是: （ ）

A. 若$(b_i, m_i) = 1$, 则同余方程组一定有解.

B. 如果同余方程组无解, 则b_1, b_2, b_3不是两两互素的整数.

C. 若b_1, b_2, b_3是两两互素的整数, 则同余方程组一定有解.

D. 若m_1, m_2, m_3是两两互素的整数, 则同余方程组有唯一解.

四、简答题/计算题

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$a = 75, b = 21,$求整数$s,t,$ 使得$as + tb = (a, b)$. （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F_2 [x]中多项式$f(x) = x^4 + x + 1, g(x) = x^2,$ 求$(f(x), g(x))$.

7. 计算$6^{1084}(\bmod 247)$。(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 $12x$≡9×5^{127}(mod 27).