一.单选题 (共16题,16.0分)

1 构建RSA公钥密码系统。首先随机选取两个大素数p,q,并计算$n=pq$,其次随机选取$e,(e,\varphi(n))=1$,再次求d,最后将(e,n)公开作为加密密钥,将d保密作为解密私钥,这时加密算法为( )。 (1.0分)

A、 $de\equiv 1(mod\ \varphi(n))$

B、 $de\equiv 1(mod\ n)$

C、 $c\equiv m^e(mod\ n)$

D、 $c\equiv m^e(mod\ \varphi(n))$

E、 $c\equiv m^e(mod\ q)$

我的答案: C 得分: 1.0分 ✔

2 2010年1月13日是星期三,第$2^{20100113}$天是( )。 (1.0分)

A、 星期一

B、 星期三

C、 星期四

D、 星期日

我的答案: D 得分: 1.0分 ✔

3 ( )是模23的最小正原根。 (1.0分)

A、 2

B、 4

C、 3

D、 5

我的答案: D 得分: 1.0分 ✔

4 二次同余方程$x^2\equiv 137\ (mod\ 227)$是( )。 (1.0分)

A、 可解的

B、 无解的

C、 无法判断是否有解

我的答案: B 得分: 1.0分 ✔

5 $2^{200}(mod\ 47)\equiv$( )。 (1.0分)

A、 1

B、 12

C、 18

D、 31

我的答案: C 得分: 1.0分 ✔

6 ( )是素数。 (1.0分)

A、 739

B、 749

C、 779

D、 799

我的答案: A 得分: 1.0分 ✔

7 最大公因数(666,1414) =( )。 (1.0分)

A、 12

B、 222

C、 6

D、 2

我的答案：D 得分：1.0分

8 设p是奇素数,则下列结论错误的是( )。 (1.0分)

A、 $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$

B、 $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

C、 设$(a,p)=1$,则$\left(\frac{a^2}{p}\right)=1$

D、 $\left(\frac{a+b}{p}\right)=\left(\frac{a}{p}\right)+\left(\frac{b}{p}\right)$

我的答案：D 得分：1.0分

9 运用广义Euclid除法求整数s,t,使得$sa+tb=(a,b)$,其中$a=2947,b=3772$,则s,t分别为( )。 (1.0分)

A、 $951,-753$

B、 $951,-743$

C、 $851,-753$

D、 $851,-743$

我的答案：B 得分：1.0分

10 $2^{2010}(mod\ 107)\equiv$( )。 (1.0分)

A、 85

B、 86

C、 87

D、 88

我的答案：C 得分：1.0分

11 一次同余方程组$\begin{cases}x=2(mod\ 5)\\x=3(mod\ 7)\\x=4(mod\ 9)\end{cases}$的解为( )。 (1.0分)

A、 155

B、 156

C、 157

D、 158

我的答案：C 得分：1.0分

12 如果a是整数,则a^3-a被( )整除。 (1.0分)

A、 3

B、 4

C、 5

D、 7

我的答案：A 得分：1.0分

13 一次同余方程$24x \equiv 7(mod 59)$的解为( )。 (1.0分)

A、 47

B、 57

C、 67

D、 77

我的答案：A 得分：1.0分

14 设a,b是任意两个不全为零的整数,m为任意正整数,则下列等式成立的是( )。 (1.0分)

A、 $[am,bm]=(a,b)m$

B、 $[am,bm]=[a,m]b$

C、 $[am,bm]=[a,b]m$

D、 $[am,bm]=abm$

我的答案：C 得分：1.0分

15 下列结论正确的是( )。 (1.0分)

A、 $(a,b)[a,b]>ab$

B、 $(a,b)[a,c]=a(b,c)$

C、 $(a,[b,c])=[(a,b),(a,c)]$

D、 $(a,[b,c])=([a,b],[a,c])$

我的答案：C 得分：1.0分

16 构建RSA公钥密码系统。首先随机选取两个大素数p,q,并计算$n=pq$,其次随机选取$e,(e,\varphi(n))=1$,再次求( ),最后将(e,n)公开作为加密密钥,将d保密作为解密私钥。 (1.0分)

A、 $de \equiv 1(mod\ \varphi(n))$

B、 $de \equiv 1(mod\ n)$

C、 $c \equiv m^e(mod\ n)$

D、 $c \equiv m^e(mod\ \varphi(n))$

E、 $c \equiv m^e(mod\ q)$

我的答案：A 得分：1.0分

1 设p是奇素数,$(a_1,p)=1,(a_2,p)=1$。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。()(1.0分)

我的答案: √ 得分: 1.0分

2 设p是奇素数,$(a_1,p)=1,(a_2,p)=1$。如果a_1,a_2都是模p的平方非剩余,则a_1a_2是模p的平方非剩余。()(1.0分)

我的答案: × 得分: 1.0分

3 设m_1,m_2是互素的两个正整数。如果x_1,x_2分别遍历模m_1和模m_2的既约剩余系,则$m_2x_1+m_1x_2$遍历模m_1m_2的既约剩余系。()(1.0分)

我的答案: √ 得分: 1.0分

4 设m是一个正整数,a,a',b,b'是四个整数,且$aa'\equiv 1(mod\ m),bb'\equiv 1(mod\ m)$。如果$a\equiv b(mod\ m)$,则$a'\equiv b'(modm)$。()(1.0分)

我的答案: √ 得分: 1.0分

5 设$m>1$是整数,a是与m互素的整数,则$1=a^0,a^1,\dots,a^{ord_m(a)-1}$中必存在两个数模$m$同余。()(1.0分)

我的答案: × 得分: 1.0分

6 设$m>1$是整数,g是模m的原根。设$d\geq 0$为整数,则g^d是模m的原根当且仅当$(d,\varphi(m))=0$。()(1.0分)

我的答案: √ 得分: 1.0分

7 设$m=227$是奇素数,则二次同余式$x^2\equiv 2(mod\ m)$有解。()(1.0分)

我的答案: × 得分: 1.0分

8 设m是一个正整数,$ad\equiv bc(mod\ m)$,则$a\equiv b(mod\ m)$。()(1.0分)

我的答案: × 得分: 1.0分

9 设m是大于1的整数,则对与m互素的整数a,有$a^{\varphi(m)}\equiv 1(mod\ m)$。()(1.0分)

我的答案: √ 得分: 1.0分

10 设m是正整数,a是整数。若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。()(1.0分)

我的答案: × 得分: 1.0分

11 设m是大于1的整数。若有整数a使得$a^{m-1}\equiv 1(mod\ m)$成立,则m是素数。()(1.0分)

我的答案: × 得分: 1.0分

12 设$m_1,\dots,m_k$是k个正整数,$a\equiv b(mod\ m_i),i=1,\dots,k$,则$a\equiv b(mod\ m_1\dots m_k)$。()(1.0分)

我的答案: × 得分: 1.0分

13 设m是一个正整数,则模m同余是等价关系。()(1.0分)

我的答案: √ 得分: 1.0分

14 设p是奇素数,则$\left(\frac{-ab}{p}\right)=\left(\frac{-a}{p}\right)\left(\frac{b}{p}\right)$。()(1.0分)

我的答案: √ 得分: 1.0分

15 设$m_1,\dots,m_k$是k个两两互素的正整数,则对任意的整数$b_1,\dots,b_k$,同余式组$\begin{cases}x\equiv b_1(mod\ m_1)\\ x\equiv b_2(mod\ m_2)\\ \dots\dots\dots\dots\\ x\equiv b_k(mod\ m_k)\end{cases}$一定有解,且解是唯一的。()(1.0分)

我的答案: √ 得分: 1.0分

A、 x^2+x+1

B、 x^3+x^2+1

C、 $x+1$

D、 x

我的答案：B 得分：1.0分

2 设$F_{2^8}=F_2[x]/(x^8+x^4+x^3+x^2+1)$是有限域。若$a=x^5+x^3+1$,则$a^{-1}$=( )。（1.0分）

A、 x^3+x^2

B、 $x^7+x^6+x^4$

C、 x^4+x^2+1

D、 x^7+x^6

我的答案：B 得分：1.0分

3 设$q=p^n$,p为素数,$d|q-1$,则( )。（1.0分）

A、 有限域F_q中有阶为d的元素

B、 有限域F_q中没有阶为d的元素

C、 有限域F_q中有阶为2^d的元素

D、 以上说法都不对

我的答案：A 得分：1.0分

4 下列说法正确的是( )。（1.0分）

A、 设p为素数,则存在模p原根

B、 设p为合数,则存在整数g,其幂g^k遍历模p的简化剩余系

C、 设p为合数,则存在模p原根

D、 设p为素数,则存在整数g,其幂g^k遍历模p的完全剩余系

我的答案：A 得分：1.0分

5 设$F_{2^8}=F_2[x]/(x^8+x^4+x^3+x^2+1)$是有限域。若$a=x^5+x^2+1$,则$a^{-1}$=( )。（1.0分）

A、 x^3+x^2

B、 $x^6+x^4+x^2+x$

C、 x^4+x^2+1

D、 x^7+x^6

我的答案：B 得分：1.0分

6 如果a,b是群G的任意元素,则( )。（1.0分）

A、 $(ab)^{-1}=b^{-1}a^{-1}$

B、 $(ab)^{-1}=a^{-1}b^{-1}$

C、 $(ab)^{-1}\neq b^{-1}a^{-1}$

D、 以上说法均不对

我的答案：A 得分：1.0分

7 $f(x)=x^8+x+1$在F_2上有因式( )。（1.0分）

A、 $x+1$

B、 x^2+x+1

C、 x^3+x+1

D、 x^3+x^2+1

我的答案：B 得分：1.0分

8 设H是群G的子群,则下列说法正确的是( )。（1.0分）

A、 $|G|=[G:H]|H|$

B、 $|G|=[G:H]/|H|$

C、 $|H|=[G:H]|G|$

D、 $|G|=[H:G]|H|$

我的答案：A 得分：1.0分

9 群G是交换群的充要条件是( )。（1.0分）

A、 对任意$a,b\in G$,有$(ab)^2=abab$

B、 对任意$a,b\in G$,有$(ab)^2=a^2b^2$

C、 对任意$a,b\in G$,有$(ab)^2=ab^2$

D、 以上说法均不对

我的答案：B 得分：1.0分

10 设R是一个环,则下列说法错误的是( )。（1.0分）

A、 对任意$a\in R$,有$0\cdot a=a\cdot 0=0$

B、 对任意$a,b\in R$,有$(-a)b=a(-b)=-ab$

C、 对任意$a,b\in R$,有$(-a)(-b)=-ab$

D、 对任意$a_i,b_j\in R$,有$(\sum_{i=1}^{n}a_i)(\sum_{j=1}^{m}b_j)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j$

我的答案：C 得分：1.0分

11 设$F_{2^8}=F_2[x]/(x^8+x^4+x^3+x+1)$是有限域。若$a=x^6+x^4+x^2+x+1,b=x^7+x+1$,则$a+b=$( )。（1.0分）

A、 x^6+x^3

B、 $x^7+x^6+x^4+x^2$

C、 $x^7+x^5+x^3+x^2+1$

D、 x^7+x^6+1

我的答案：B 得分：1.0分

12 设$G=\langle a\rangle$是循环群,下列说法正确的是( )。（1.0分）

A、 如果G是无限的,则G的生成元仅为a

B、 如果G具有有限阶m,则a^k是G的生成元当且仅当$(k,m)=1$

C、 如果G是无限的,则G的生成元为$a^i,i=1,2,\ldots$

D、 如果G具有有限阶m,则a^k是G的生成元

我的答案：B 得分：1.0分

13 下列说法错误的是( )。 (1.0分)

A、 每个有限域都有生成元

B、 F_q有$\varphi(q-1)$个生成元

C、 如果g是F_q的生成元,则g^d是F_q的生成元

D、 如果g不是F_q的生成元,则g^d不可能是F_q的生成元

我的答案：C 得分：1.0分

14 设$F_{2^8}=F_2[x]/(x^8+x^4+x^3+x+1)$是有限域。若$a=x^6+x^4+x^2+x+1, b=x^7+x+1$,则$a\cdot b=$( )。 (1.0分)

A、 x^6+x^3

B、 $x^7+x^6+x^4+x^2$

C、 $x^7+x^5+x^3+x^2+1$

D、 x^7+x^6+1

我的答案：D 得分：1.0分

二.判断题 (共12题,12.0分)

1 设H是群G的子群,则对任意$a,b\in G, aH=bH$的充要条件是$ab^{-1}\in H$。 ( ) (1.0分)

我的答案：× 得分：1.0分

2 $\mathbb{Z}$是主理想整环 ( ) (1.0分)

我的答案：×　　得分：1.0分

2 Z是主理想整环。（）(1.0分)

我的答案：√　　得分：1.0分

3 设m是正整数,则对模m乘法运算,$(Z/mZ)\setminus\{0\}$构成一个乘法群。（）(1.0分)

我的答案：×　　得分：1.0分

4 设p是素数,则对模p乘法运算,$(Z/pZ)\setminus\{0\}$构成一个乘法群。（）(1.0分)

我的答案：√　　得分：1.0分

5 设G是一个群,则对任意的$a,b,c\in G$,都有$(ab)c=a(bc)$。（）(1.0分)

我的答案：√　　得分：1.0分

6 多项式x^3-2x-1是Q上的不可约多项式。（）(1.0分)

我的答案：×　　得分：1.0分

7 $f(x)=x^2+1$是F_2上的不可约多项式。（）(1.0分)

我的答案：×　　得分：1.0分

8 实数域R是有理数域Q的扩域,也是复数域C的扩域。（）(1.0分)

我的答案：×　　得分：1.0分

9 $f(x)=x^2+1$是Z上的不可约多项式。（）(1.0分)

我的答案：√　　得分：1.0分

10 复数域C是有理数域Q的扩域,也是实数域R的扩域。（）(1.0分)

我的答案：√　　得分：1.0分

11 设p是素数,则对模p加法和乘法运算,Z/pZ构成一个域。（）(1.0分)

我的答案：√　　得分：1.0分

12 设m是正整数,则mZ是整环Z的理想。（）(1.0分)

我的答案：√　　得分：1.0分