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$a \equiv b(\bmod m)$且$c \equiv d(\bmod m)$，则存在整数h和k，使等式$a = b + hm$且$c = d + km$成立.

故 $a + c = (b + hm) + (d + km) = b + d + (h + k)m,$

$ac = (b + hm)(d + km) = bd + (hd + kb + hkm)m.$

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：$\varphi(\varphi(19)) = \varphi(18) = \varphi(3^2 \times 2) = 18 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 6$

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2^d,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：

$2^1 \equiv 2$,　$2^5 \equiv 13$,　$2^7 \equiv 14$,　$2^{11} \equiv 15$,　$2^{13} \equiv 3$, $2^{17} \equiv 10 \pmod{17}$.

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

$54^{\frac{101-5}{2}} \equiv 54^{50} (\mathrm{mod}\ 101)$

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$54^{50} \equiv 1 (\mathrm{mod}\ 101)$，方程有解

4、解：

75=21×3+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× 12-21=2× $(75 - 21 \times 3) - 21$

=$2 \times 75 - 7 \times 21$

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：$\varphi(\varphi(13)) = \varphi(12) = \varphi(2^2 \times 3) = 12 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$

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2^d,其中 d 为模 12 的简化剩余系{1,5,7,11}。

模 13 的所有原根为：

$2^1 \equiv 2$,　$2^5 \equiv 6$,　$2^7 \equiv 11$,　$2^{11} \equiv 7 \pmod{13}$

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$(f(x), g(x))$.

① x^4+x+1=$x^2\times x^2$+ $(x+1)$

即: (x^4+x+1, x^2)=($x^2, x+1)$

② x^2=$(x+1)$ $(x+1)$+1

即: ($x^2, x+1)$= ($x+1$, 1)=1

故$(f(x), g(x))$=1.

7、解：(6,247)=1，根据欧拉定理可知 $6^{\varphi(247)}\equiv 1(\mathrm{mod}\ 247)$.

$$\varphi(247)=\varphi(13\times 19)=216$$

$$6^{1084}\equiv 6^{5*216+4}\equiv 6^4\equiv 61(\ \mathrm{mod}\ 247\ )$$

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 $12x\equiv 9\times 5^{127}$(mod 27).

解：φ(27)=18, 5^{127}(mod 27)= 5^{18*7+1}(mod 27)=5

同余方程 $12x\equiv 9\times 5^{127}$(mod 27) 等价于 $12x\equiv 9*5=18$ (mod 27)

（12,27）=3, 因为 3|18，因此方程有解，有三个解

首先求解 $4x\equiv 1$(mod 9)

求解为： $x\equiv 7$(mod 9)

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