信息安全数学基础----习题集一答案

第一题　填空

1、108　2、800　3、{1,2,4,5,7,8}　4、{1,3,4,5,9 }　5、4

6、φ(m)φ(n)　7、(a,m)|b　8、(a,m)=1　9、有解　10、阶

二、判断题

1—5：× √ × × √　6-10：× √ × √ ×

11—15：√ √ × × √　16-20：× √ √ × √

三、单项选择题

1-5：ACBCD　6-10：CABDA

11-15：DBCCB　16-20：CABDD

四、简答题

1、101=15×6+11　15=11+4　11=4×2+3　4=3×1+1

因此(a,b)=（101,15）=1

1=4-3=4-(11-4×2)=4× 3-11=(15-11)× 3-11=15× $3-11\times 4$

=15× $3-(101-15\times 6)\times 4=15\times 27-101\times 4$

因此 s=27 ，t=-4

备注：s=27 t=-4 不是唯一答案，只要满足$as+tb=(a,b)$ 都正确

2、解：7^{1005}(mod 15)，

已知（7,15）=1，由欧拉定理$7^{\varphi（15）}\equiv 1(\mathrm{mod}\,15)$，$7^{8}\equiv 1(\mathrm{mod}\,15)$

因此 $7^{1005}\equiv 7^{1005（\mathrm{mod}\,8）}\equiv 7^{5}$ (mod 15)

$7^{2}\equiv 4$ (mod 15)　$7^{4}\equiv 1$ (mod 15)　$7^{5}\equiv 7$ (mod 15)

因此 $7^{1005}\equiv 7$(mod 15)

备注：此计算方法不是唯一，也可以用中国剩余定理化简求解

3、（1）已知 26=2× 13，$\varphi(26)$ =12。

（2）7^2≡23≡$-3(\bmod 26)$，7^3≡-21≡ $5(\bmod 26)$　7^6≡25≡$-1(\bmod 26)$ ，7 是模 26 的一个原根, $ord_{26}(7)$=12

因为模 12 的简化剩余系为{1,5,7,11}, 故模 26 的所有原根为:

7^1≡7,　7^5≡11,　7^7≡-33≡-7≡19,　7^{11}≡-7*9 ≡-11≡15 (mod 26).

即模 26 的原根为:7,11,19,15

4、解：判断同余方程 x^2≡3(mod 11)的解的情况

根据欧拉判别式进行求解进行判断

$$3^{\frac{11-1}{2}} \equiv 3^5 \equiv 12 \equiv 1(\bmod 11)$$

即 3 是模 11 的平方剩余，即 x^2≡3(mod 11)方程有解

备注：判断 x^2≡3(mod 11)方程解情况也可采用 0,1,…..,5 代入方程穷举方法求解。

5、 解：长除法可得 $f(x) = (x^3 + x^2 + x + 1)g(x) + x$

商式$x^3 + x^2 + x + 1$，余式 x

6、164=42×3+38　42=38+4　38=4×9+2　4=2×2

因此(a,b)=（166,42）=2

2=38-4×9=38-(42-38) ×9=38× 10-42×9=(164-42×3)× 10-42×9=164× 10 $- 42 \times 39$

备注：不是唯一答案，只要满足$as + tb = (a, b)$ 都正确

7、解：6^{2017}（mod41），

已知（6,41）=1，由欧拉定理$6^{\varphi(41)} \equiv 1(\bmod 41)$，$6^{40} \equiv 1(\bmod 41)$

因此 6^{2017}（mod41）≡6^{17}（mod41）

$6^2 \equiv -5$ (mod 41)　$6^4 \equiv -16$ (mod 41)　$6^8 \equiv 10$ (mod 41)

$6^{16} \equiv 18$ (mod 41)

因此 $6^{2017} \equiv 18 \times 6 \equiv 26$(mod 41)

8、1,$2^2 \equiv 4$(mod 17), $3^2 \equiv 9$(mod 17), $4^2 \equiv 16$(mod 17),

$5^2 \equiv 8$(mod 17), $6^2 \equiv 2$(mod 17), $7^2 \equiv 15$(mod 17)，$8^2 \equiv 13$(mod 17)，

模 17 的所有平方剩余为 1，2，4，8，9，13，15，16

9、$\varphi(19) = 18$

$5^2 \equiv 6$(mod19)，$5^3 \equiv 11$(mod19)，$5^6 \equiv 7$(mod19)，$5^9 \equiv 1$(mod19) (4分)

$ord_{19}(5)=9$

五、综合题（备注，每题必须给出具体求解过程）

求解一次同余方程 84x+1≡64(mod 371)

由原方程得 84x≡63(mod 371)

（84，371）=7|63，故方程有解。

要解 84x≡63(mod 371)，需先求 12x≡9(mod53) 的解

先解 12x≡1(mod53)

53=12×4+5　　12=5×2+2　　5=2×2+1

1=5-2×2=5-2×（12-5×2）=5×5-12×2

=5×（53-12×4）-12×2=5×53-12×22

故 12x≡1(mod53)的解为 x≡31（mod53）

12x≡9(mod 49) 的解为 x≡14（mod53）

故 84x≡63(mod 301)得全部解为 x≡14+53t（mod371），t=0,1,2…,6