湖南科技大学考试试题参考答案及评分细则

（ 2022 - 2023 学年度第 二 学期）

课程（A 卷） 信息安全数学基础 上课学院 计算机学院 班级 21 信息安全 123

应试学生人数_____实际考试学生人数_____考试时量_____分钟

命题教师 李志刚 审核人_____考试时间： 年 月 日

一、证明

1. $3m+1\equiv 0(mod\ 5)$ $m\equiv 3(mod\ 5)$ 得证。
2. 由欧拉定理，$2^8\equiv 1\ (\mathrm{mod}\ 15)$ $2^{70}\equiv (2^8)^8 2^6=2^6=64=4\ (\mathrm{mod}\ 15)$

二、综合题

1. $m_1=4,m_2=5$，m_1 =7，$a_1=3,a_2=2$，$a_3=0$，2 分$M_1=35,M_2=28,M_3=20$ 2 分

   $M_1^{-1}=-1,M_2^{-1}=2,M_3^{-1}=-1$ 3 分

   $x\equiv 35\times(-1)\times 3+28\times 2\times 2+20\times(-1)\times 0=7(\mathrm{mod}\ 140)$ 3 分
2. 123= $49\times 2+25$，49= $25\times 1+24$，$25=24\times 1+1$ $\gcd(123,49)=1$ 5 分

   $1=25-24=25-(49-25)=2\times 25-49=2\times(123-49\times 2)-49$

   $=2\times 123-49\times 5$ $49^{-1}=-5=118(mod\ 123)$ 5 分
3. 119 合数 1 分 $\left(\frac{26}{119}\right)=\left(\frac{2}{119}\right)\left(\frac{13}{119}\right)$ $119\equiv 3(\mathrm{mod}\ 4)$ $119\equiv 7(\mathrm{mod}\ 8)$ $\left(\frac{2}{119}\right)=1$ 4 分

   $\left(\frac{13}{119}\right)=\left(\frac{119}{13}\right)=\left(\frac{2}{13}\right)=-1$ $\left(\frac{26}{119}\right)=-1$ 无解。5 分
4. 2^8 的阶 $\frac{18}{(18,8)}=9$ $16^x\equiv 4(mod\ 19)$ 。$2^{4x}\equiv 2^2(mod\ 19)$ $4x\equiv 2(\mathrm{mod}\ 18)$ $x\equiv 5,14(\mathrm{mod}\ 18)$
5. 群的运算的封闭性，结合律，单位元，逆元 每个要点 2 分
6. $q(x)=x^2-1$，$r(x)=x-1$ 5 分

   $q(x)=3x^3+x^2+2x+4$，$r(x)=2x+2$ 5 分
7. $e\oplus b=e+b-1=b$ e=1 零元 $a\oplus b=a+b-1=1$ $a+b=2$ 5 的负元是-3 验证结合律略$(a\odot b)\odot c=a\odot(b\odot c)$
8. $(x+1)(x^2+2)=x^2$ $-(x+2)=2x+1$ $x(x^2+2)+2(x^3+2x+2)=1$

   x的逆元 (x^2+2)