华东师范大学期中试卷

2019-2020第一学期

课程名称： 网络安全数学基础

学生姓名： 学 号:

专 业： 年级/班级：

课程性质：公共必修、公共选修、**专业必修**、专业选修

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 总分 | **阅卷人姓名** |
|  |  |  |  |  |  |  |  |  |  |

……………………………………………………………………………

一、计算题

1. 已知a =666，b = 1515，求整数s,t，使得sa + tb = (a, b)。
2. 求解同余方程组
3. 求模37原根个数及全部原根
4. 求解同余式x2 = 631 (mod 2310)

二、证明题

1、证明形如4n-1 的素数有无穷多个。

2、证明相邻两个整数的立方之差不能被5整除。

3、令 ，是不相同的奇素数，证明：



4、

设p和q是满足的两个不同的奇素数，令。在中选取阶是n的倍数的元素。定义Paillier置换函数如下：

1. 证明集合和的大小相等。
2. 是对任意满足的最小正整数。证明对任意的，都有

（3）这部分，我们要证明函数是双射的。

1. 试论述为什么是单射的等同于它是双射的。
2. 证明：

.

1. 证明是单射的。（提示：证明.）

答案：

计算题：

1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| i | qi | ri-1 | ri | ti-1 | ti | si-1 | si |
| 0 |  | 1515 | 666 |  | 1 |  | 0 |
| 1 | 2 | 666 | 183 | 1 | 0 | 0 | 1 |
| 2 | 3 | 183 | 117 | 0 | 1 | 1 | -2 |
| 3 | 1 | 117 | 66 | 1 | -3 | -2 | 7 |
| 4 | 1 | 66 | 51 | -3 | 4 | 7 | -9 |
| 5 | 1 | 51 | 15 | 4 | -7 | -9 | 16 |
| 6 | 3 | 15 | 6 | -7 | 11 | 16 | -25 |
| 7 | 2 | 6 | 3 | 11 | -40 | -25 | 91 |
| 8 | 2 | 3 | 0 | -40 | 91 | 91 | -207 |

所以s = -207, t = 91, (666,1515) = 3

2. m1 = 3, M1=56, M1-1

m2 = 8, M2=21, M2-1

m3 = 7, M1=24, M1-1

解为

­­­

3. 12个，



4.化简得 ，解得

由中国剩余定理，

则[211, 251, 449, 559, 629, 911, 1021, 1091, 1219, 1289, 1399, 1681, 1751, 1861, 2059, 2099](mod 2310)

证明题：

1.证：假设有有限个这样的素数，设p为最大的一个.考虑整数 N=4×3×7…×p - 1 其中3×5×…×p表示所有不大于p的奇素数的乘积.因为N是4n-1形式的,且N>p,由p为最大的形如4n-1的素数得N不为素数.显然,N的所有素因数必大于p.由于N的因数只能是4n+1成4n-1形的.而两个4n+1形的数相乘仍有4n+1形式的.因此N至少有一个4n-1形的素因数.设为q,而q>p，与p最大矛盾.故得证.

2.证明：



3.证明：



4.证明:





1. Fg定义域与值域大小相同，Fg单射又满射，则显然双射

b)



c)

