北京邮电大学2019——2020学年第一学期

《信息安全数学基础》期中考试试题

姓名：_____ 班内序号：_____ 学号：_____ 班级：_____ 专业：_____

线 封 密

考试注意事项	一、学生参加考试须带学生证或学院证明，未带者不准进入考场。学生必须按照监考教师指定座位就坐。 二、书本、参考资料、书包等物品一律放到考场指定位置。 学生不得另行携带、使用稿纸，要遵守《北京邮电大学考场规则》，有考场违作弊行为者，按相应规定严肃处理。 四、学生必须将答题内容做在试题答题处，做在草稿纸上无效。 五、学生的姓名、班级、学号、班内序号等信息由教材中心统一印制。

考试课程	信息安全数学基础			考试时间		2019 年 11 月 14 日			
题号	一	二	三	四	五	六	七	八	总分
满分	15	30	35	20					
得分									
阅卷教师									

一. 名词解释（15分，5个小题，每小题3分）

1）因数

2）算术基本定理

3）同余

4）平方

5）指标

二. 填

1）设$a=$

2）请写出

3）2019年

4）模30的

5）设$m=5$

6）计算13^{45}

7）同余方程

8）$\left(\frac{438}{593}\right)=$

9）求$\mathrm{ord}_{41}(3$

10）求模7的

4）平方剩余

5）指标

二. 填空题（30 分，10 个小题，每小题 3 分）

1）设$a = 379, b = 19$，则a被b除所得的不完全商是_____。

2）请写出两个任意整数a和b的贝祖等式_____。

3）2019 年 11 月 14 日是星期四，则其后第2^{2019}天是_____。

4）模 30 的简化剩余系为_____。

5）设$m = 5^4 \times 7$，则$\varphi(m) =$_____。

6）计算$13^{45}(mod\ 23) =$_____。

7）同余方程$6x \equiv 3\ (\mathrm{mod}9)$的解是_____。

8）$\left(\frac{438}{593}\right) =$_____。

9）求$\mathrm{ord}_{41}(3) =$_____。

10）求模 7 的所有原根_____。

三、 计算题（35分，5个小题，每个题7分）

1）使用模重复平方法计算$201^{227} \pmod{2309}$。

3）求解同余式$x^2 \equiv 13(mod 101)$。

4）求模$p = 41$的所有原根。

5) 求解同余方程$x^8 \equiv 38(mod\ 11)$，已知模 11 以 2 为底的指数表为:

a	1	2	3	4	5	6	7	8	9	10
inda	0	1	8	2	4	9	7	3	6	5

四. 证明题（20分，4个小题，每小题5分）

1) 同余式组 $a \equiv b \pmod{m_j}, j = 1,2,\cdots,k$ 同时成立的充要条件是 $a \equiv b \pmod{[m_1, m_2, \cdots, m_k]}$。

2) 设a,b是任意两个正整数，则$(a,b) = r_n$，其中r_n是广义欧几里得除法中最后一个非零数。

3)

4)

3) 设$m > 1$是整数，$(a, m) = 1$，证明：若$\mathrm{ord}_m(a) = st$，那么$\mathrm{ord}_m(a^s) = t$。

4) 设p, q是两个不同的奇素数，$n = pq, a$是与n互素的整数。如果整数e满足$1 < e < \varphi(n), (e, \varphi(n)) = 1$，那么存在整数$d, 1 \leq d < \varphi(n)$，使得$ed \equiv 1 (\mathrm{mod}\ \varphi(n))$，证明：对于整数$a^e \equiv c (\mathrm{mod}\ n), 1 \leq c < n$，有$c^d \equiv a (\mathrm{mod}\ n)$。