

武汉大学国家网络安全学院
2019-2020 学年度第 2 学期
《信息安全数学基础》期末考试试卷 A 卷（开卷）

专业：_____ 学号：_____ 姓名：_____

说明：答案请全部写在答题纸上，写在试卷上无效。

未经主考教师同意，考试试卷、答题纸、草稿纸均不得带离考场，否则视为违规。

题号	一	二	三	四	五		总分
分值							100

一. 计算题（共 6 小题，每小题 10 分，共 60 分）

1. 已知 $a = 527, b = 1411$ ，求最大公因子 (a, b) 和最小公倍数 $[a, b]$ 。

2. 利用勒让德符号判断同余方程 $x^2 \equiv 30 \pmod{41}$ 是否有解？

3. 求乘法群 \mathbb{F}_{23}^* 的所有生成元。

4. 求解同余式组

$$\begin{cases} x \equiv 2 \pmod{3} \\ 3x \equiv 4 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$$

5. 求解同余式 $f(x) = 3x^4 + 17x^3 - 5x + 23 \pmod{25}$ 。

6. 假设椭圆曲线 $y^2 = x^3 + 5x + 3 \pmod{11}$ 上的两点 $P = (x_1, y_1), Q = (x_2, y_2)$ 之和为

$P_3 = (x_3, y_3) = P + Q \neq O$ 的计算公式为

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = (x_1 - x_3)\lambda - y_1$$

其中① $x_1 \neq x_2$ 时， $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ ，② $x_1 = x_2$ ，且 $Q \neq -P$ 时， $\lambda = \frac{3x_1^2 + 5}{2y_1}$

若 $P = (3, 1)$ ，试求 $3P$ 。

二、证明题（共 10 分）

假定 a 和 b 是一个群 G 的两个元，并且 $ab = ba$ 。又假定 a 的阶是 m ， b 的阶是 n ，并且 $(m, n) = 1$ 。证明： ab 的阶是 mn 。

三、应用题（每小题 15 分，共 30 分）

1. 构造有限域 $GF(16) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$ （其中模多项式为 $m(x) = x^4 + x + 1$ ）的加法表和乘法表。（填表即可）

加法表

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0																
1																
2																
3																

乘法表

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0																
1																
2																
3																

2.著名 RSA 公钥密码加密系统如下:

- ① 随机选择两个大素数 p 和 q , 而且保密;
- ② 计算 $n = pq$, 将 n 公开;
- ③ 计算欧拉函数 $\varphi(n) = (p-1)(q-1)$, 并对 $\varphi(n)$ 保密;
- ④ 随机选取正整数 $e \in (1, \varphi(n))$ 且有 $(e, \varphi(n)) = 1$, 并将 e 公开;
- ⑤ 根据 $ed \equiv 1 \pmod{\varphi(n)}$, 求出 d , 并对 d 保密;
- ⑥ 加密运算: $C = M^e \pmod{n}$;
- ⑦ 解密运算: $M = C^d \pmod{n}$ 。

现令公钥 $n = 133, e = 101$ 。 问: (1) 若待加密的明文 $M = 83$, 求相应的密文 C ; (2) 若待解密的密文 $C = 131$, 求相应的明文 M 。