

# 第8章椭圆曲线&第7章有限域

## 计算证明

1. (15分)已知  $E_{11}(1,6)$  上一点  $G(2,7)$ , 求  $2G$  到  $13G$  的所有值.
2. (15分)已知  $E_{17}(3,1)$  上一点  $Q = (15, y_Q)$ , 求  $Q$  坐标及  $Q$  的阶.
3. 由多项式  $p(x) = x^4 + x + 1$  定义的域  $\mathbb{F}_{2^4}$ , 选取生成元  $g = (0010)$  (表示多项式  $x$ ):
  - (1) (15分) 求  $\mathbb{F}_{2^4}$  上椭圆曲线:  $y^2 + xy = x^3 + g^4x^2 + 1$  上的所有点;
  - (2) (10分) 验证  $P_1 = (g^6, g^8)$ ,  $P_2 = (g^3, g^{13})$  是椭圆曲线上的点, 并求  $P_1 + P_2$  和  $2P_1$ .
4. (1) (5分)求  $\mathbb{F}_2$  上的三次本原多项式, 并据此给出域  $\mathbb{F}_8$  的矩阵表示;  
(2) (5分)验证对其加法和乘法运算满足域结构的定义;  
(3) (5分)计算  $\mathbb{F}_8$  上所有元素的阶.

## 编程练习(基于C/C++)

(30分)实现基本的  $Z_p$  上的椭圆曲线  $E_p(a,b)$  的计算, 平台可以是Windows/Linux/macOS, 具体如下:

### 1. 功能要求:

- 给定参数  $p, a, b$ , 判断  $E_p(a,b)$  是否为椭圆曲线;
- 判断给定的点  $P, Q$  是否在椭圆曲线  $E_p(a,b)$  上;
- 对在椭圆曲线  $E_p(a,b)$  上的两点  $P, Q$ , 计算  $P + Q$ ;
- 对在椭圆曲线  $E_p(a,b)$  上的点  $P$ , 使用倍加-和算法计算  $mP$ ;
- 对在椭圆曲线  $E_p(a,b)$  上的点  $P$ , 计算阶  $\text{ord}(P)$ ;
- 对在椭圆曲线  $E_p(a,b)$ , 计算阶  $\#E$ ;
- 对在椭圆曲线  $E_p(a,b)$ , 计算所有点;
- 其他功能的进一步扩展.....

### 2. 编程要求:

- 不允许使用第三方的库;
- 按照面向对象的编程思想, 封装类, 调用公有接口实现;
- 符合一定的编程规范;
- 利用之前的知识模块解耦实现: 如扩展Euclid算法求逆、二次互反律求Legendre符号、群的一些基础知识等;
- 在实现功能的基础上, 尽可能提高计算的效率等.

### 3. 示例演示:

```
ubuntu@ubuntu: ~/course/ecc
ubuntu@ubuntu:~/course/ecc$ ls
ecc_base.cpp  ecc_base.h  main.cpp  makefile
ubuntu@ubuntu:~/course/ecc$ make
g++ -c ./ecc_base.cpp
g++ -c ./main.cpp
g++ -o ecc_base ./*.o
ubuntu@ubuntu:~/course/ecc$ make clean
rm -f *.o
ubuntu@ubuntu:~/course/ecc$ ls
ecc_base  ecc_base.cpp  ecc_base.h  main.cpp  makefile
ubuntu@ubuntu:~/course/ecc$ ./ecc_base -t
TEST 1
> E_p(a,b): p=11, a=0, b=0
[ERROR] E_11(0,0) is not elliptic curve.
> E_p(a,b): p=19, a=3, b=7
[ OK ] E_19(3,7) is elliptic curve.
> P(1,2)
[ERROR] P(1,2) is not on E_19(3,7).
> P(1,7)
[ OK ] P(1,7) is on E_19(3,7).
> Q(3,9)
[ OK ] P(3,9) is on E_19(3,7).
> P(1,7) + Q(3,9)
[ OK ] (16,16)
> 7P(1,7)
[ OK ] (15,11)
> ord(P(1,7))
[ OK ] 11
> #E_19(3,7)
[ OK ] 22
> all points on E_19(3,7)
[ OK ] Total: 22
[ OK ] 0,
[ OK ] ( 0, 8), ( 0,11), ( 1, 7), ( 1, 12)
[ OK ] ( 3, 9), ( 3,10), ( 4, 8), ( 4, 11)
[ OK ] ( 8, 7), ( 8,12), (10, 7), (10, 12)
[ OK ] (12, 2), (12,17), (13, 1), (13, 18)
[ OK ] (14, 0), (15, 8), (15,11), (16, 3)
[ OK ] (16,16)
TEST 2
```

### 4. 提交要求:

- 源码文件: \*.cpp、\*.h
- PE文件: .exe等
- 演示说明视频: <3min, 包含对写好的测试样例的演示和对核心部分的讲解说明
- 实验报告: 2123456张三椭圆曲线编程练习报告.doc 或 2123456张三椭圆曲线编程练习报告.pdf