第八章 椭圆曲线

计算证明

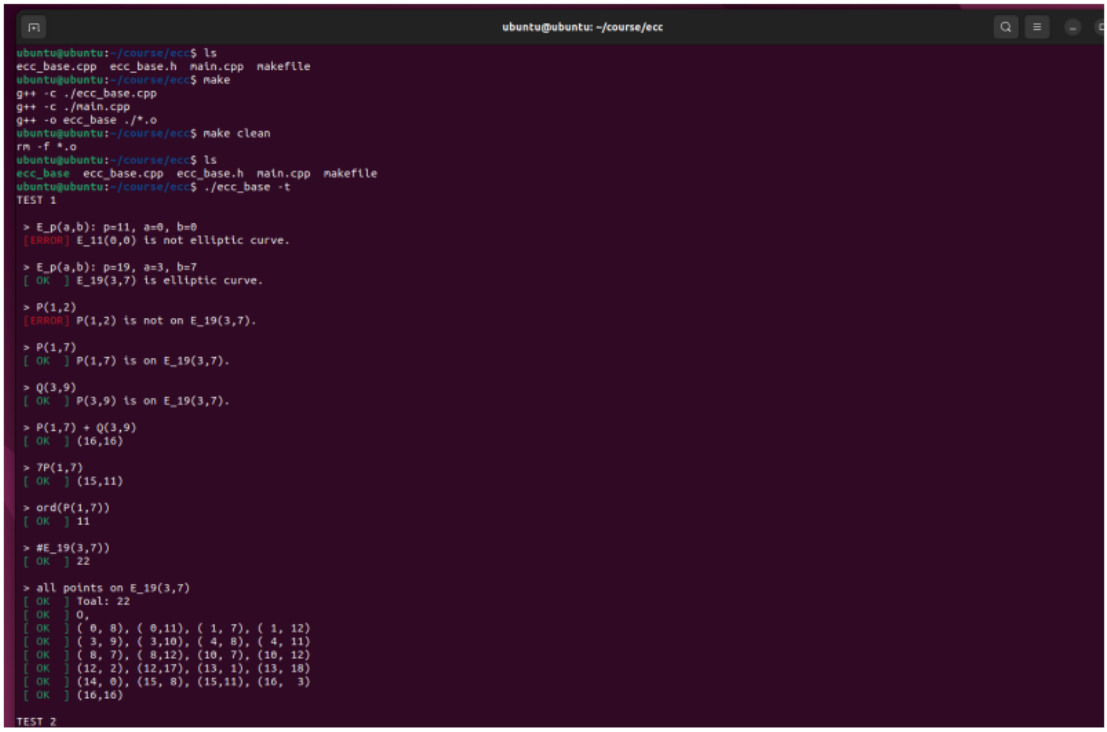
1. 证明：若点 $P=(x,0)$ 是椭圆曲线上的点，则 $2P=O$。
2. 证明：若 P,Q,R 是椭圆曲线上的点，则 $P+Q+R=O$ 的充要条件是 P,Q,R 共线。
3. 设 E 是 Z_7 上的椭圆曲线，$E:y^2\equiv x^3+3x+2(mod\ 7)$。
   (1) 求 $\#E$;
   (2) 已知点 $A=(0,3)$ 在 E 上，求 $ord(A)$;
   (3) 验证 $ord(A)|\#E$。
4. 已知 $E_{11}(1,6)$ 上一点 $G(2,7)$，求 $2G$ 到 $13G$ 所有的值。
5. 已知 $E_{17}(3,1)$ 上一点 $Q(15,y_Q)$，求 Q 坐标以及 Q 的阶。

编程练习（基于C/C++）

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$\mathrm{ord}(P)$;
   - 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：



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