密码学基础实验报告实验四

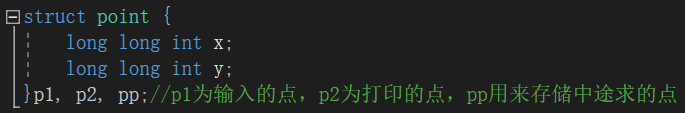
王天行 2011428

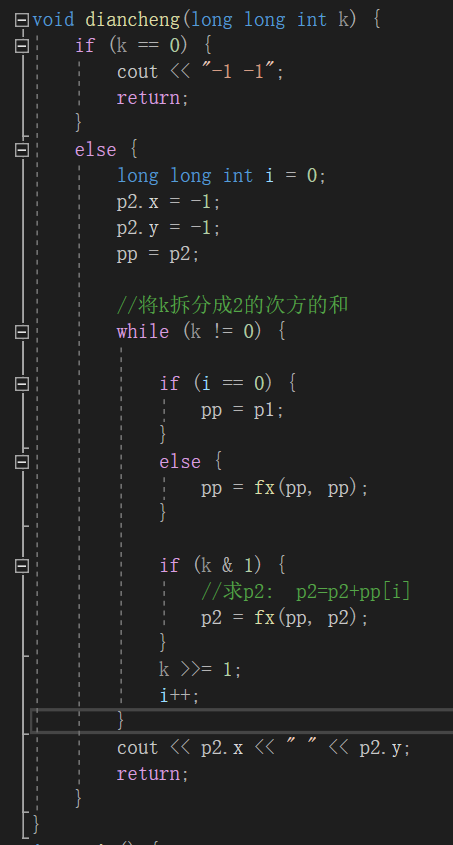
1. 题目要求

请计算定义在有限域Zp上椭圆曲线y^2=x^3+ax+b的点乘kP。 其中p为一个素数，p<2^31; a, b定义在Zp上; 0<=k<2^31, 设P=(x,y)为椭圆曲线上的整点(保证（x,y）为椭圆曲线上的整点), 其中x, y定义在Zp上。同时定义椭圆曲线上的零元(无穷远点)为(-1,-1)。

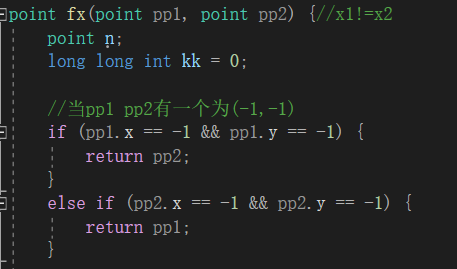
1. 主要代码

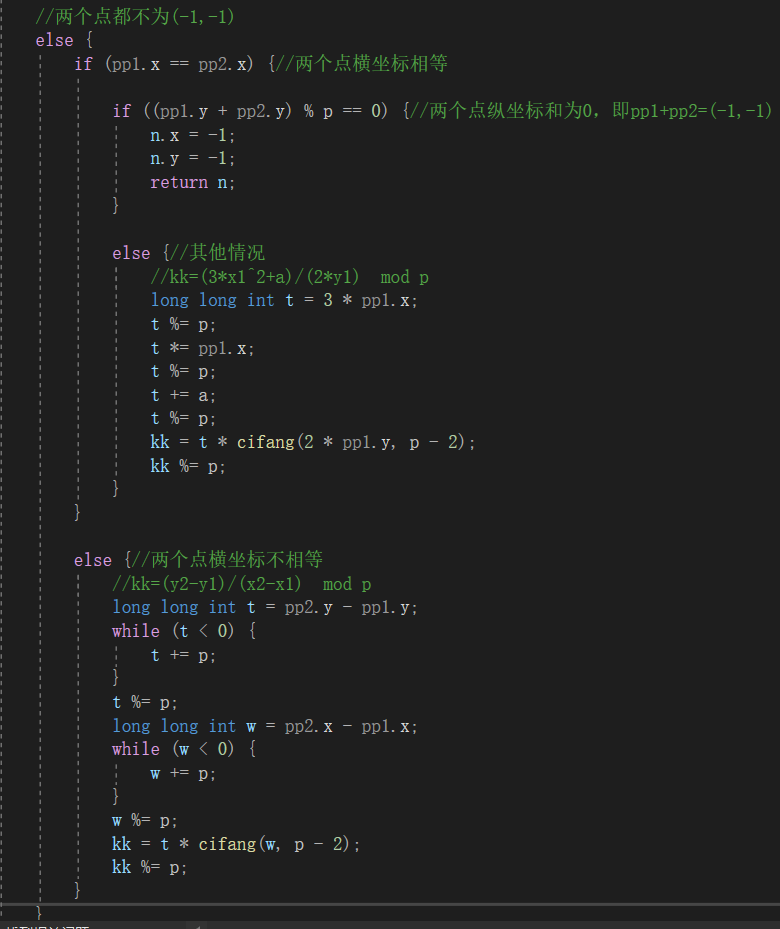
1.整体思路

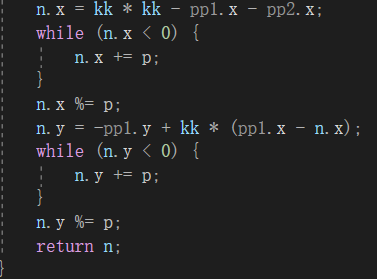




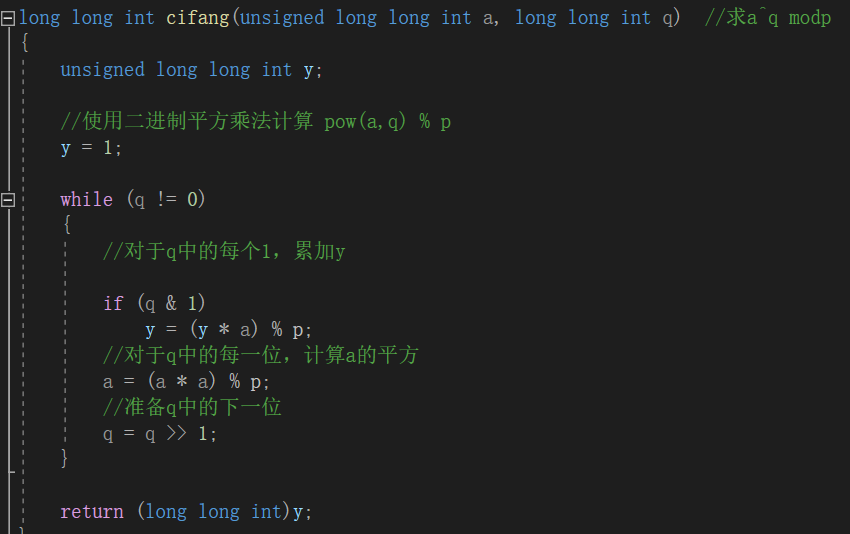
2.点加







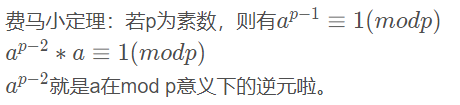
3.模逆运算



1. 输出结果

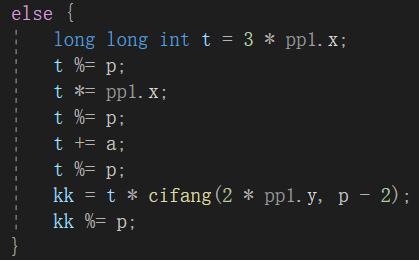


1. 心得体会
   1. 求逆：一开始选择暴力搜索，但当a,p较大时，可能会导致乘积过大，超出限制，而且运行时间过长，从而在oj平台上报错（运行出错），于是考虑更简单的方式求出逆。



考虑到上次写素性检测中有涉及更有效的次方运算的代码，于是根据费马小定理写求逆的代码，于是oj平台上没有报错运行出错。

* 1. 在修改完求逆后，oj平台上报错答案错误。之后发现是在过程中有数据溢出。



该处2\*pp1.y的范围在[0,2^33]，然而在函数cifang中会涉及到平方运算，可能会超过2^64，也就是long long int的范围，因此在cifang函数中，部分参数需要使用unsigned long long int类型。

* 1. 整体来说思路不难，但细节需要注意的地方较多，尤其是数据类型。在此题中，由于大多数数据都是有符号的，不能简单粗暴地直接全部定义为无符号整型，需要根据各处的需要，定义不同的类型。