第四届（2019）全国高校密码数学挑战赛

赛题一

一、赛题名称：椭圆曲线离散对数问题（ECDLP）

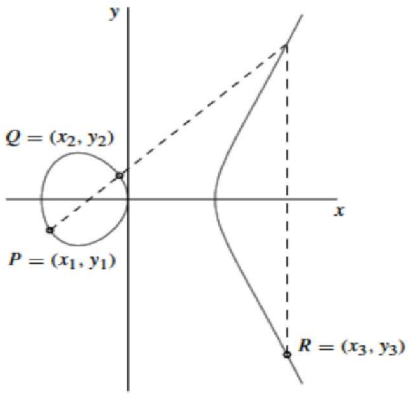
二、赛题描述：

2.1 符号说明

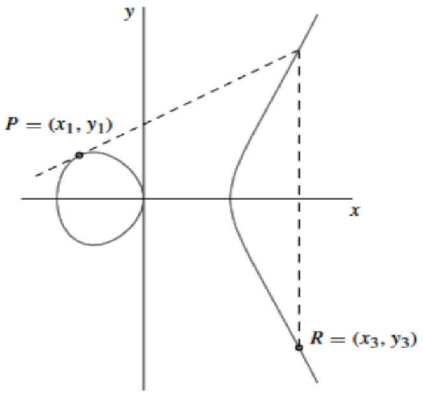
设F_p表示具有p个元素的有限域，其中$p > 3$是一个素数。F_p上的椭圆曲线E是一个点集合$E/F_p = \{(x,y)|y^2 = x^3 + ax + b, a, b, x, y \in F_p\} \cup \{\infty\}$，其中∞表示无穷远点，$4a^3 + 27b^2 \neq 0 \ mod \ p$。

2.2 基础知识

设$P = (x_1, y_1), Q = (x_2, y_2) \in E/F_p$，在$E$上定义“+”运算$P + Q = R$，$R = (x_3, y_3) \in E/F_p$是过$P, Q$的直线与曲线的另一交点关于$x$轴的对称点（当$P = Q$时，$R$是$P$点的切线与曲线的另一交点关于$x$轴的对称点）



(a) Addition: $P + Q = R$.



(b) Doubling: $P + P = R$.

上述计算可用公式表示如下：

1）当$P \neq Q$时（Addition），$R = (x_3, y_3) = (\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1)$；

2）当$P=Q$时（Doubling），$R=(x_3,y_3)=((\frac{3x_1^2+a}{2y_1})^2-2x_1,(\frac{3x_1^2+a}{2y_1})(x_1-x_3)-y_1)$；

此外，对任意$P=(x_1,y_1)\in E/F_p$,定义:

3）$P+\infty=\infty+P=P$；

4）$(x_1,y_1)+(x_1,-y_1)=\infty$,这里$(x_1,-y_1)\in E/F_p$记为$-P$.特别的，$-\infty=\infty$.

可验证E/F_p关于上述定义的“+”运算构成一个交换群，记为$E(F_p)$.

设$P\in E(F_p)$,记$[k]P=P+P+\cdots+P\ (k\ times)$，则[k]P$\in E(F_p)$，该运算称为椭圆曲线标量乘法运算。设$r$为最小的正整数使得$[r]P=\infty$，$r$称为是$P$的阶（order）。令$\langle P\rangle=\{\infty,P,[2]P,\dots,[r-1]P\}$，可验证$\langle P\rangle$关于“+”运算构成$E(F_p)$的一个$r$阶子群。

2.3 问题描述

椭圆曲线离散对数问题（ECDLP）：给定椭圆曲线$E/F_p: y^2=x^3+ax+b, P\in E(F_p), r:=order(P), R\in\langle P\rangle$，计算$1\le k\le r$使得$R=[k]P$.（该问题可形式化地记为$k=log_P R$）

具体参数请见附件：ECDLP 数据文件.txt。

2.4 成绩评判

(1). 本赛题共分 3 类挑战（1-8 小题为第一类，9-16 小题为第二类，17-22 小题为第三类，题目参数请见（五）），在同类挑战中，以选手做出的参数最长的题目得分为该类挑战得分，同类挑战中多做题目不多得分；

(2). 第一类挑战中，第 1-8 小题分值分别为 22，26，30，34，38，42，46，50；第二类挑战中，第 9-16 小题分值分别为 28，34，40，46，52，58，64，70；第三类挑战中，第 17-22 小题分值分别为 30，40，50，60，70，80；

(3). 分数相同的选手依照难度最高的挑战求解时间来排序，求解用时越少者排名越靠前；

(4). 针对每类挑战，给出计算平台和计算结果，并简述求解原理、步骤和实现效率（包括计算需要的时间和空间等），引用前人方法的必须在报告中给出明确引用，否则报告内容作废；

(5). 利用特殊算法求解或求解算法中有创新内容的，酌情加分。

三、密码学背景及相关问题的研究进展

20 世纪八十年代中期，Koblitz 和 Miller 各自独立提出将有限域上椭圆曲线用于建立公钥密码系统（ECC），其安全性基于椭圆曲线上有理点加法群离散对数问题（ECDLP）的难解性[1]。目前一般椭圆曲线上的离散对数问题还没有有效的计算方法，而这也是现代密码学中最具挑战性的问题之一。ECDLP 可简要描述为：已知 G 为曲线上的加法子群且 G 的群阶为大素数 r，P 为 G 的生成元。随机选取 G 中元素 R，计算正整数 k 使得$R = [k]P$，或者表示为 $k = log_P R$。目前计算该问题的方法主要包括通用算法和特殊算法:

通用算法：Pollard's rho 算法，Pollard's kangaroo 算法，以及小步－大步法等均可用于求解一般有限群上的离散对数问题。目前在一般情况下，计算 ECDLP 也只有通用算法奏效，其时间复杂度为 $O(\sqrt{r})$。2009 年 Bailey 等人针对 Certicom 公司提出的 ECC 挑战利用 Pollard's Rho 算法计算 ECC2K-130 上的 ECDLP [2]，目前相关计算仍在进行。

特殊算法：在一些特殊曲线上，可以将 ECDLP 转化到其他群上的离散对数问题弱化其难解性，已有研究主要包括：

（1）将 ECDLP 约化到有限域上的离散对数问题(DLP)。如 SSSA 攻击[3]将异常椭圆曲线(有理点群阶等于有限域大小)上的 ECDLP 约化到有限域加法群的 DLP，MOV 攻击[4] 则利用椭圆曲线上的双线性映射将定义在有限域F_p上的 ECDLP 归约到有限域F_{p^k}乘法群上的离散对数问题，此方法在嵌入次数 k 较小时有效。

（2）利用 Weil 下降等技术将椭圆曲线上的有理点群转化为另一类几何对象（如超椭圆曲线上 Jacobian 或高维 Abel 簇），将 ECDLP 复杂性减弱（目前高亏格 HECDLP 存在比通用算法更有效的算法）。

四、参考文献

[1] Hankerson D., Menezes A.J.,Vanstone S.: Guide to Elliptic Curve Cryptography. Springer, Heidelberg (2004)

[2] Bailey D., Batina L., Bernstein D.J., Birkner P., Bos J.W., et al .: Breaking ECC2K-130. Cryptology ePrint Archive, Report 2009/541 (2009)

[3] Smart N.P.: The discrete logarithm problem on elliptic curves of trace one. J. Cryptol. 12, 193-196 (1999)

[4] Menezes A.J., Okamoto T., Vanstone S.A.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory. 39(5), 1639-1646 (1993)