第3章　椭圆曲线方法与技术

椭圆曲线应用于密码学开始于 Koblitz 和 Miller。这两位学者几乎同时提出了椭圆曲线密码体制的概念。椭圆曲线密码体制的安全性基于椭圆曲线的 Mordell-Weil 群上离散对数的计算困难性。

椭圆曲线密码体制有许多优点。首先是密钥短，密钥长度为 106 比特的椭圆曲线密码体制的安全强度相当于密钥长度为 512 比特的 RSA 密码体制的安全强度；其次是计算速度快，密码学中所用的椭圆曲线是定义在有限域上的代数曲线，因此它有代数和几何两方面的性质。在椭圆曲线上，点的逆元素容易计算，同时椭圆曲线上的加法群有模结构，因此可供选择的算法就比较多，计算速度也比较快；还有就是定义在同一个有限域上的椭圆曲线有许多条，因此需更换密码体制时只要更换一条定义在同一个有限域上的椭圆曲线，从而有限域的算法还可以继续使用。所以与基于有限域上离散对数问题的密码体制相比，椭圆曲线密码体制中涉及有限域算法的芯片可以重复使用，也就是说通用性比较好。

由于以上这些特点，椭圆曲线密码体制特别适合于应用到计算资源有限的环境中。另外，椭圆曲线上可以定义双线性对（Weil 对和 Tate 对，称之为“对子”），对子把椭圆曲线上离散对数问题转化为有限域上离散对数问题，这种优秀的密码学性质，被用来构造新型的密码体制。

本章主要围绕椭圆曲线在信息安全中的应用，将介绍椭圆曲线的一些基本概念和基本原理。最后，作为这些椭圆曲线理论的应用，还将介绍一些典型的密码体制。

3.1　基本概念

本节重点介绍一些椭圆曲线的基本概念。

3.1.1　椭圆曲线的定义

设 K 是一个域（为了便于理解，不妨把 K 看成实数域 R，但是在密码学应用中，K 一般是有限域）。从平面解析几何的角度来说，定义在 K 上的椭圆曲线 E 是一条由 Weierstrass 方程

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K, i = 1,2,3,4,6 \quad (3.1)$$

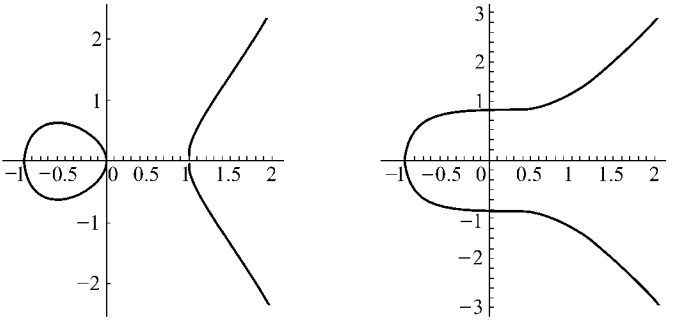
定义的非奇异（即处处光滑，或者不严格地说自己和自己没有交点）的 3 次曲线，再“人为地”添加一个无穷远点（用 ∞ 表示）所得到的曲线，记为 E/K。有时说起由方程(3.1)定义的椭圆曲线时，并不特意指出包含无穷远点，但都默认它自然包含了一个无穷远点。

由此可见，椭圆曲线 E/K 是 $K \times K$ 平面上由方程(3.1)的全体解构成的图形。

设 $L \supset K$ 是 K 的扩域，方程(3.1)在 $L \times L$ 平面上的解称为椭圆曲线 E 的 L 有理点。E 的全体 L 有理点记为 $E(L)$。根据椭圆曲线的定义，无穷远点必须包含在 $E(L)$ 内：

$$E(L) = \{(x,y) \in L \times L \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

例 3.1.1 两条椭圆曲线如图 3.1 所示。



(a) $y^2=x^3-x$ (b) $y^2=x^3+1$

图 3.1 两条椭圆曲线

设 E 是一条由 Weierstrass 方程(3.1)定义的曲线，则可以定义以下参数：

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= 2a_4 + a_1a_3 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j(E) &= c_4^3/\Delta
\end{aligned}$$

其中 Δ 称为这个 Weierstrass 方程的判别式。如果 $\Delta \neq 0$，则 $j(E)$ 有定义，称为这个方程的 j 不变量。判别式和 j 不变量是椭圆曲线的重要参数。

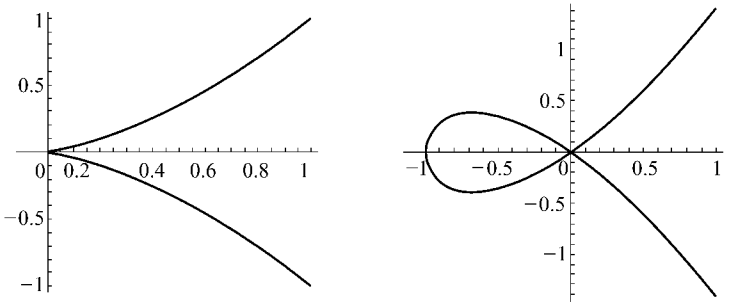
定理 3.1.1 由方程(3.1)定义的曲线是一条非奇异曲线的充分必要条件是 $\Delta \neq 0$。

证明：把方程(3.1)写成形如 $F(x,y)=0$ 的隐函数形式。根据多元微积分中的定理可知，由 $F(x,y)=0$ 定义的曲线是非奇异曲线当且仅当方程组 $\begin{cases} F(x,y)=0 \\ F_x(x,y)=0 \\ F_y(x,y)=0 \end{cases}$ 没有解；用 Δ 的定义直接验证可得定理。

定理 3.1.2 定义在 K 上的两条椭圆曲线 E_1/K 和 E_2/K 同构，则 $j(E_1)=j(E_2)$；如果 K 是一个代数封闭域，则由 $j(E_1)=j(E_2)$ 也可以得到 E_1/K 和 E_2/K 同构。

这里同构的意思是两条曲线之间的方程可以通过一个有理变换互相转化，而且这个有理变换把无穷远点变到无穷远点。

例 3.1.2 因为判别式 $\Delta=0$，所以由图 3.2 所示的两条曲线是奇异曲线，因而不是椭圆曲线：



(a) $y^2=x^3$(γ曲线) (b) $y^2=x^3+x^2$(α曲线)

图 3.2 两条奇异曲线

椭圆曲线的 Weierstrass 方程在形式上是复杂的，但总可以通过坐标变换把它变成相对比较简单的形式，这是一个标准过程，请参考文献[4]。

(1) $\mathrm{char}(K)\neq 2,3$，则 E/K 的方程可以化成以下形式：

$$E:\ y^2 = x^3 + ax + b \quad a,b \in K \tag{3.2}$$

(2) $\mathrm{char}(K)=2$，则 E/K 的方程可以化成以下两种形式：

① $j(E)\neq 0, E:\ y^2+xy=x^3+a_2x^2+a_6 \quad a_2,a_6\in K$ (3.3)

② $j(E)=0, E:\ y^2+a_3y=x^3+a_4x+a_6 \quad a_3,a_4,a_6\in K$ (3.4)

(3) $\mathrm{char}(K)=3$，则 E/K 的方程可以化成以下两种形式：

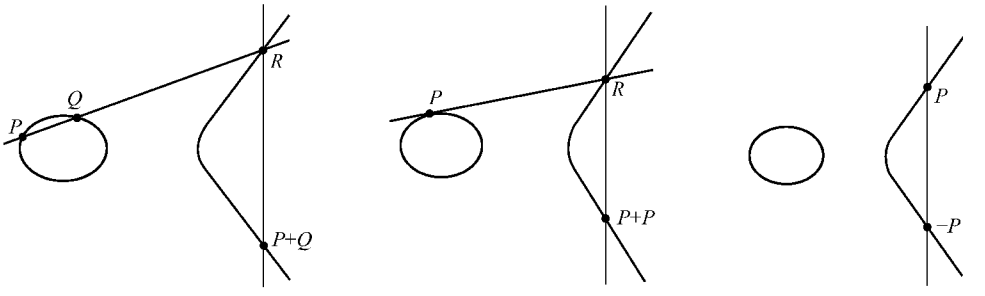
① $j(E)\neq 0, E:\ y^2=x^3+a_2x^2+a_6 \quad a_2,a_6\in K$ (3.5)

② $j(E)=0, E:\ y^2=x^3+a_4x+a_6 \quad a_4,a_6\in K$ (3.6)

3.1.2 椭圆曲线上的 Mordell-Weil 群

椭圆曲线上的点在“弦切律”下构成一个群。

定义 3.1.1 椭圆曲线上点的加法(弦切律) 如图 3.3(a)、(b)所示，设 P、$Q\in E$，ℓ 是过 P、Q 两点的直线(如果 $P=Q$，则取 ℓ 为过 P 点的切线)，则由于椭圆曲线是一条 3 次曲线，因此 ℓ 必和 E 相交于第三点 R。令 ℓ' 为过 R 和无穷远点的直线(即过 R 且与 x 轴垂直的直线)，则 ℓ' 与 E 的第三个交点即为 P 与 Q 的“和”记为 $P+Q$。



(a) $P+Q$ (b) $2P=P+P$ (c) $-P$

图 3.3 实数域上椭圆曲线弦切律的几何表示

P 点的逆 $-P$ 即为过 P 且与 x 轴垂直的直线与曲线的交点，如图 3.3(c)所示。

图 3.3 所示为实数域上椭圆曲线的弦切律的几何表示，如果要考虑其他域上的椭圆曲线的弦切律，也可以甚至必须借助这些图形思考问题。

由于在平面解析几何的范围内考虑椭圆曲线问题，因此无穷远点在上面的图中表示不出来，但理解加法时要默认它是存在的。比如在定义中垂直于 x 轴的直线 ℓ' 和曲线的交点在图中只显示出有两个，但是理论上 3 次曲线和直线的交点应该有 3 个，那么第三个点就是在无穷远点。这从另外一个方面说明，在定义椭圆曲线时“人为”引入的那个无穷远点是实际存在的，在引入射影几何后，这个无穷远点就自然出现了。

还有一点需要注意的是，如果 E/K 是一条定义在 K 上的椭圆曲线，L 是 K 的扩域，P、Q 是 E 的 L-有理点，则过 P、Q 的直线和 E 的第三个交点一定是 E 的 L 有理点。这是因为直线和曲线的联立方程组的系数都取自域 L，而方程组有 3 个解，其中两个解就是 P 和 Q，那么第三个解一定是 L-有理点。

定理 3.1.3 设 E/K 是一条定义在域 K 上的椭圆曲线，$L\supset K$ 是 K 的扩域，则 E 的全体有理点 $E(L)$ 在弦切律下构成一个交换群，其中单位元就是无穷远点，即用弦切律定义的加法符合以下规律：

(1) 结合律 $(P+Q)+R=P+(Q+R)$，$\forall P,Q,R\in E(L)$；

(2) 存在零元素 $P+\infty=\infty+P$，$\forall P\in E(L)$；

(3) 存在逆元素 $P+(-P)=(-P)+P$，$\forall P\in E(L)$；

(4) 交换律 $P+Q=Q+Q$，$\forall P,Q\in E(L)$。

定理的证明除第一条结合律外都是平凡的。利用代数几何理论给出的结合律的证明可以在文献[4]中找到；也可以通过弦切律的定义直接进行验证，但是那样的话计算量会比较大，而且需要有耐心才可以；Knapp 在文献[3]中给出了一个只利用初等解析几何和线性代数的证明，有兴趣的读者可以参考。

需要指出的是，以上用弦切律定义的群被称为 Mordell-Weil 群。其实发现这是个群结构的时间比 Mordell 和 Weil 要早，可以追溯到 Poincare 甚至 Abel。这个群之所以被称为 Mordell-Weil 群，是因为 Mordell 最早给出了有理数域上椭圆曲线 Mordell-Weil 群的有限生成定理，而 Weil 推广了他的结果。

对于密码学工作者来说，工作的域一般是有限域，在某些情况下也会涉及一些 p-adic 域和复数域。有限域上椭圆曲线和 p-adic 域上椭圆曲线没有直观的图示，复数域上椭圆曲线的图形是个三维空间中的环面。在这些情况下思考问题会缺乏直观的感觉，此时最好借用实数域上椭圆曲线的图形来支持我们的直觉。

点加的表达式：设 E 是由方程(3.1)定义的一条椭圆曲线，则由弦切律定义的加法的表达式可以通过平面解析几何中求曲线和直线的交点的方法推导出来。这个推导的工作量不大，难度也小，把详细推导过程留给读者，这里只是把结果列出来。

(1) 逆元素：$P=(x,y)\in E$，则 $-P=(x,-y-a_1x-a_3)$。

(2) 加法：记 $P_3=P_1+P_2$，其中 $P_i=(x_i,y_i)$，$i=1,2,3$。

1) 若 $P_1=-P_2$，即 $x_1=x_2$，$y_1+y_2+a_1x_1+a_3=0$，则 $P_1+P_2=\infty$。

2) 若 $P_1 \neq -P_2$，令

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & x_1 = x_2 \end{cases}$$

则 P_3 的坐标由下式给出：

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3. \end{cases}$$

如果采取曲线方程的简化形式(3.6)，则以上加法的表达式有更简单的形式，这在实践中有重要的作用。

例 3.1.3 椭圆曲线 E：$y^2 = x^3 + ax + b$，$(a, b \in K, \mathrm{char}(K) \neq 2, 3)$ 上点加的表达式。

(1) 逆元素：设 $P = (x, y)$，则 $-P = (x, -y)$。

(2) 一般加法：设 $P_3 = P_1 + P_2$，其中 $P_i = (x_i, y_i)$，$i = 1, 2, 3$。

1) 若 $P_1 = -P_2$，即 $x_1 = x_2$，$y_1 = -y_2$，则 $P_1 + P_2 = \infty$。

2) 若 $P_1 \neq -P_2$，令

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1} & x_1 = x_2 \end{cases}$$

则 P_3 的坐标由下式给出：

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

例 3.1.4 椭圆曲线 E：$y^2 + xy = x^3 + a_2x^2 + a_6$，$(a_2, a_6 \in K, \mathrm{char}(K) = 2)$ 上点加的表达式。

(1) 逆元素：设 $P = (x, y)$，则 $-P = (x, y + x)$。

(2) 一般加法：设 $P_3 = P_1 + P_2$，其中 $P_i = (x_i, y_i)$，$i = 1, 2, 3$。

1) 若 $P_1 = -P_2$，即 $x_1 = x_2$，$y_1 = y_2 + x_2$，则 $P_1 + P_2 = \infty$。

2) 若 $P_1 \neq -P_2$，且 $P_1 \neq P_2$ 时，P_3 的坐标由下式给出：

$$\begin{cases} x_3 = \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)^2 + \dfrac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a_2 \\ y_3 = \left(\dfrac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + x_3 + y_1. \end{cases}$$

3) 若 $P_1 \neq -P_2$，且 $P_1 = P_2$ 时，P_3 的坐标由下式给出：

$$\begin{cases} x_3 = x_1^2 + \dfrac{a_6}{x_1^2} \\ y_3 = x_1^2 + \left(x_1 + \dfrac{y_1}{x_1}\right)x_3 + x_3 \end{cases}$$

例 3.1.5 椭圆曲线 E：$y^2 + a_3y = x^3 + a_4x + a_6$，$(a_2, a_3, a_6 \in K, \mathrm{char}(K) = 2)$ 上

点加的表达式。

(1) 逆元素：设 $P=(x,y)$，则 $-P=(x,y+a_3)$。

(2) 一般加法：设 $P_3=P_1+P_2$，其中 $P_i=(x_i,y_i)$，$i=1,2,3$。

1) 若 $P_1=-P_2$，即 $x_1=x_2$，$y_1=y_2+a_3$，则 $P_1+P_2=\infty$。

2) 若 $P_1\neq -P_2$，且 $P_1\neq P_2$ 时，P_3 的坐标由下式给出：

$$\begin{cases} x_3=\left(\dfrac{y_1+y_2}{x_1+x_2}\right)^2+x_1+x_2 \\ y_3=\left(\dfrac{y_1+y_2}{x_1+x_2}\right)(x_1+x_3)+y_1+a_3. \end{cases}$$

3) 若 $P_1\neq -P_2$，且 $P_1=P_2$ 时，P_3 的坐标由下式给出：

$$\begin{cases} x_3=\dfrac{x_1^4+a_4^2}{a_3^2} \\ y_3=\left(\dfrac{x_1^2+a_4}{a_3}\right)(x_1+x_3)+y_1+a_3 \end{cases}$$

特征 3 的情形请读者自己补齐或参见文献[1,4]。

3.2 射影坐标和 Jacobi 坐标

椭圆曲线上的点有几种不同的坐标表示，此前使用的平面解析几何中的坐标平面被称为仿射平面，所以仿射坐标平面上的点的坐标表示也称为仿射坐标，通常记为 (x,y)，而无穷远点没有相应的坐标表示，用∞或者 O 表示。

用仿射坐标表示椭圆曲线上点在做点加时会涉及有限域的除法，而除法在计算中要消耗较多的计算时间。在椭圆曲线密码体制的应用中，每一次计算都要涉及数百次点加运算，所以能够在做点加时省下一些除法运算，那对于提高系统的效率是有重要意义的。这个时候需要射影坐标和 Jacobi 坐标。

3.2.1 射影坐标

我们把射影坐标理解为仿射坐标通分后把公分母用另一个分量表示的一种坐标表示方法。这样，给射影坐标乘上一个非零常数，那这个坐标和原来的坐标表示的是同一个点。

点 (x,y) 的坐标“通分”以后写为 $(X/Z,Y/Z)$，把公分母写成另一个分量，则这个点的表示为 $[X,Y,Z]$。这里用方括号表示坐标 $[X,Y,Z]$ 和 $[\lambda X,\lambda Y,\lambda Z]$ 当 λ 不等于零时表示同一个点。这是因为，把 $[X,Y,Z]$ 和 $[\lambda X,\lambda Y,\lambda Z]$ 变成仿射坐标就是 $(X/Z,Y/Z)$ 和 $(\lambda X/\lambda Z,\lambda Y/\lambda Z)$，这是同一个点的坐标。

射影平面是在仿射平面的基础上加上一些无穷远点构成的。动用一点灵活性，减少一点严格性，不妨称仿射平面上的点为“有穷远点”，以示对无穷远点的区别。射影平面上的有穷远点的射影坐标 $[X,Y,Z]$ 的特点是 $Z\neq 0$；无穷远点的射影坐标形如 $[X,Y,0]$，其中 X 和 Y 中至少有一个不为零。下面就来计算一下椭圆曲线上无穷远点的射影坐标。

设 E：$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6(a_i\in K)$是一条椭圆曲线，如果 $P=(x,y)$是 E 上一个点，则把 P 的坐标代入上述方程可使方程两边相等。设 P 的射影坐标为 $P=[X,Y,Z]$，则当 $Z\neq 0$ 时有

$$x = X/Z, \quad y = Y/Z$$

代入上述椭圆曲线的方程有

$$\left(\frac{Y}{Z}\right)^2+a_1\frac{XY}{Z^2}+a_3\frac{Y}{Z}=\left(\frac{X}{Z}\right)^3+a_2\left(\frac{X}{Z}\right)^2+a_4\frac{X}{Z}+a_6$$

方程两边各项通分后乘上 Z^3 得

$$Y^2Z+a_1XYZ+a_3YZ^2 = X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$

这个方程称为椭圆曲线的齐次方程。因为无穷远点的坐标的特点是 $Z=0$，把它代入齐次方程后发现方程变成

$$X^3 = 0$$

也就是说，椭圆曲线上无穷远点的坐标一定是$[0,Y,0]$的样子，而点的射影坐标的 3 个分量一定要有一个不为零，因此 $Y\neq 0$。所以椭圆曲线上的无穷远点一定是$[0,1,0]$。

可以看到，用仿射坐标表示椭圆曲线上的点，无穷远点就没有坐标表示；而在射影坐标的情形，无穷远点有一个自然的坐标表示。这说明射影平面比仿射平面更具完备性。

3.2.2 Jacobi 坐标

Jacobi 坐标用$[X,Y,Z]$表示点的坐标。Jacobi 坐标和仿射坐标(x,y)的关系为

$$x = X/Z^2, \quad y = Y/Z^3$$

当域的特征大于 3 时，方程的形式为

$$Y^2 = X^3+aXZ^4+bZ^6$$

当域的特征是 2 时，方程的形式分别是

$$Y^2+XYZ = X^3+a_2X^2Z^2+a_6Z^6, \quad j\neq 0$$

$$Y^2+a_3YZ^3 = X^3+a_4XZ^4+a_6Z^6, \quad j=0$$

在 Jacobi 坐标下，无穷远点的坐标是$[0,1,0]$。仿射坐标(x,y)到 Jacobi 坐标的转换为 $X=x,Y=y,Z=1$。

使用 Jacobi 坐标的点加算法比采取射影坐标更快一些。以下就给出两条曲线的点加运算的公式。

定义在特征大于 3 的曲线 $Y^2=X^3+aXZ^4+bZ^6$ 的点加公式。其中 $P_i=(X_i,Y_i,Z_i)$，$i=1,2,3$，符合 $P_3=P_1+P_2$。

(1) $P_1\neq P_2$：

$$\lambda_1 = X_1Z_2^2$$

$$\lambda_2 = X_2Z_1^2$$

$$\lambda_3 = \lambda_1-\lambda_2$$

$$\lambda_4 = Y_1Z_2^3$$

$$\lambda_5 = Y_2 Z_1^3$$
$$\lambda_6 = \lambda_4 - \lambda_5$$
$$\lambda_7 = \lambda_1 + \lambda_2$$
$$\lambda_8 = \lambda_4 + \lambda_5$$
$$Z_3 = Z_1 Z_2 \lambda_3$$
$$X_3 = \lambda_6^2 - \lambda_7 \lambda_3^2$$
$$\lambda_9 = \lambda_7 \lambda_3^2 - 2X_3$$
$$Y_3 = (\lambda_9 \lambda_6 - \lambda_8 \lambda_3^3)/2$$

(2) $P_1 = P_2$：

$$\lambda_1 = 3X_1^2 + aZ_1^4$$
$$Z_3 = 2Y_1 Z_1$$
$$\lambda_2 = 4X_1 Y_1^2$$
$$X_3 = \lambda_1^2 - 2\lambda_2$$
$$\lambda_3 = 8Y_1^4$$
$$Y_3 = \lambda_1(\lambda_2 - \lambda_3) - \lambda_3$$

定义在特征 2 的曲线 $Y^2 + XYZ = X^3 + a_2 X^2 Z^2 + a_6 Z^6$ 的点加公式。其中 $P_i = (X_i, Y_i, Z_i)$，$i = 1, 2, 3$，符合 $P_3 = P_1 + P_2$。

(1) $P_1 \neq P_2$：

$$\lambda_1 = X_1 Z_2^2$$
$$\lambda_2 = X_2 Z_1^2$$
$$\lambda_3 = \lambda_1 + \lambda_2$$
$$\lambda_4 = Y_1 Z_2^3$$
$$\lambda_5 = Y_2 Z_1^3$$
$$\lambda_6 = \lambda_4 + \lambda_5$$
$$\lambda_7 = Z_1 \lambda_3$$
$$\lambda_8 = \lambda_6 X_2 + \lambda_7 Y_2$$
$$Z_3 = \lambda_7 Z_2$$
$$\lambda_9 = \lambda_9 + Z_3$$
$$X_3 = a_2 Z_3^2 + \lambda_6 \lambda_9 + \lambda_3^3$$
$$Y_3 = \lambda_9 X_3 + \lambda_8 \lambda_7^2$$

(2) $P_1 = P_2$：

$$Z_3 = X_1 Z_2^2$$
$$X_3 = (X_1 + a_6 Z_1^2)^4$$
$$\lambda = Z_3 + X_1^2 + Y_1 Z_1$$
$$Y_3 = X_1^4 Z_3 + \lambda X_3$$

3.3 自同态

本节讨论椭圆曲线 E 上的自同态。

定义 3.3.1 有理映射 $\alpha: E(\overline{K}) \to E(\overline{K})$ 称为椭圆曲线 E 的自同态，如果它符合

$$\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$$

这里 α 是有理映射的意思是，存在有理函数（多项式的商）$R_1(x,y)$，$R_2(x,y)$，使得对任意的 $(x,y) \in E(\overline{K})$，都有 $\alpha(x,y) = (R_1(x,y), R_2(x,y))$。

例 3.3.1 设 $E: y^2 = x^3 + ax + b$ 是一条椭圆曲线，则 $P \mapsto nP$ 是 E 的自同态，因此其形式为 $n(x,y) = (R_1(x,y), R_2(x,y))$。特别地，$n=2$ 时有

$$2(x,y) = \left(\left(\frac{3x^2+a}{2y}\right)^2 - 2x, \left(\frac{3x^2+a}{2y}\right)\left(3x - \left(\frac{3x^2+a}{2y}\right)^2\right) - y\right)$$

为了简单起见，考虑特征不等于 2,3 的域上定义的椭圆曲线 $E: y^2 = x^3 + ax + b$。此时对任意的 $(x,y) \in E(\overline{K})$ 都有 $y^2 = x^3 + ax + b$，因此 E 上的有理函数都可以写成以下形式：

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}$$

进而用 $p_3(x) - p_4(x)y$ 对上式的分母“有理化”后有

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}$$

又因为

$$\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y)$$

故而有

$$R_1(x,-y) = R_1(x,y), \quad R_2(x,-y) = -R_2(x,y)$$

因此有

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

其中 $r_1(x)$、$r_2(x)$ 是 x 的有理函数。

记 $r_1(x) = p(x)/q(x)$，其中 $(p(x), q(x)) = 1$。如果在点 (x,y) 处有 $q(x) = 0$，则令 $\alpha(x,y) = \infty$；如果 $q(x) \neq 0$，则可以证明（留给读者证明）$r_2(x) \neq 0$，因此 α 的定义是良好的。如果 α 是一个非平凡自同态，则定义 α 的次数为

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}$$

规定 $\deg(0) = 0$。如果 $\frac{\mathrm{d}}{\mathrm{d}x} r_1(x) \neq 0$，则称 α 是可分的；否则称 α 为不可分的。

关于椭圆曲线自同态的一个基本定理表明，椭圆曲线上的全体自同态构成一个环，并且同构于下列 3 种环之一[1]：

(1) 整数环；

(2) 虚二次代数数域的子环；

(3) 四元数域的子环。

因此，椭圆曲线 E 的自同态映射 α 在 E 上的作用有以下 3 种情况：

(1) $\alpha(P)=nP$,其中 $n\in\mathbf{Z}$,此时记 $\alpha-n=0$;

(2) $\alpha^2(P)+a\alpha(P)+b=\infty$,其中 $a,b\in\mathbf{Z}$,此时记 $\alpha^2+a\alpha+b=0$;

(3) α 符合一个 4 次多项式。

例 3.3.2 设 E 是定义在 q 元有限域 $\boldsymbol{F}_q$ 上的椭圆曲线,其上的 q-Frobenius 映射 ϕ_q 定义为

$$\phi_q(x,y)=(x^q,y^q)$$

显而易见,ϕ_q 是 E 上的一个次数为 q 的不可分自同态,且有

$$\phi_q^2-a\phi_q+q=0$$

其中 a 的意义将在下一节中给出详细说明。

例 3.3.3 设素数 $p\equiv1(\mathrm{mod}\ 4)$,$i\in\boldsymbol{F}_q$ 是一个乘法 4 阶元素。考虑椭圆曲线 $E/\boldsymbol{F}_q$: $y^2=x^3+ax$ 上的映射

$$\begin{array}{rccc}\phi: & (x,y) & \mapsto & (-x,iy)\\ & \infty & \mapsto & \infty\end{array}$$

则 ϕ 是 E 的一个自同态,且有

$$\phi^2+1=0$$

例 3.3.4 设素数 $p\equiv1(\mathrm{mod}\ 3)$,$\rho\in\boldsymbol{F}_q$ 是一个乘法 3 阶元素。考虑椭圆曲线 $E/\boldsymbol{F}_q$: $y^2=x^3+b$ 上的映射

$$\begin{array}{rccc}\phi: & (x,y) & \mapsto & (\rho x,y)\\ & \infty & \mapsto & \infty\end{array}$$

则 ϕ 是 E 的一个自同态,且有

$$\phi^2+\phi+1=0$$

本节中的例子都是在椭圆曲线密码学中常常要用到的。

3.4 曲线上点的个数

3.4.1 有限域上椭圆曲线上点的个数

设 E/K 是一条椭圆曲线,令 n 是一个正整数,记

$$E[n]=\{P\in E(\overline{K})\mid nP=\infty\}$$

为 E 上 n 阶点全体。如果 K 的特征不整除 n 或者等于 0,则[1]

$$E[n]\cong\mathbf{Z}_n\oplus\mathbf{Z}_n$$

如果域 K 的特征是素数 p,且 $p\mid n$。记 $n=p^rn'$,$p\nmid n'$,则[1]

$$E[n]\cong\mathbf{Z}_{n'}\oplus\mathbf{Z}_{n'}\quad\text{或者}\quad E[n]\cong\mathbf{Z}_n\oplus\mathbf{Z}_{n'}$$

设 F_q 是 q 元有限域,则定义在 F_q 上的椭圆曲线 E/F_q 上点的个数的最基本结果由以下 Hasse 引理给出。

定理 3.4.1(Hasse 引理) $|\#E(F_q)-q-1|\leqslant2\sqrt{q}$。

定理 3.4.1 的证明参见文献[4]。

Hasse 引理表达出这样一个信息:定义在 q 元有限域上的椭圆曲线上点大约有