第十四章 椭圆曲线
2015年12月14日

信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

14.1 椭圆曲线基本概念

设K 是一个域. 域K 上的Weierstrass 方程是

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

其中$a_1, a_2, a_3, a_4, a_6 \in \mathbf{K}$.
当域K 的特征不为2 时, 上述方程可变形为

$$(y + \frac{1}{2}a_1x + \frac{1}{2}a_3)^2 = x^3 + (\frac{1}{4}a_1^2 + a_2)x^2 + (\frac{1}{2}a_1a_3 + a_4)x + \frac{1}{4}a_3^2 + a_6$$

或 $(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$
其中

$$\begin{cases} b_2 = a_1^2 + 4a_2, \\ b_4 = a_1a_3 + 2a_4, \\ b_6 = a_3^2 + 4a_6. \end{cases} \tag{2}$$

当域K 的特征不为2, 3 时, 方程可继续变形, 有

$$(2y+a_1x+a_3)^2 = 4(x+\frac{1}{12}b_2)^3+(-\frac{1}{12}b_2^2+2b_4)(x+\frac{1}{12}b_2)+(\frac{1}{216}b_2^3-\frac{1}{6}b_2b_4+b_6),$$

或 $108^2(2y + a_1x + a_3)^2 = 36^3(x + \frac{1}{12}b_2)^3 - 27c_4 \cdot 36(x + \frac{1}{12}b_2) - 54c_6,$

其中

$$\left\{\begin{array}{rcl} c_4 & = & b_2^2 - 24b_4 = {a_1}^4 + 8\,{a_1}^2a_2 - 24\,a_1a_3 + 16\,{a_2}^2 - 48\,a_4 \\ c_6 & = & -b_2^3 + 36b_2b_4 - 216b_6 \\ & = & -{a_1}^6 - 12\,{a_1}^4a_2 + 36\,{a_1}^3a_3 - 48\,{a_1}^2{a_2}^2 + 72\,{a_1}^2a_4 + 144\,a_1a_2a_3 \\ & & -64\,{a_2}^3 + 288\,a_2a_4 - 216\,{a_3}^2 - 864\,a_6 \end{array}\right. \tag{3}$$

并作变换

$$\left\{\begin{array}{l} X = 36(x + \frac{1}{12}b_2) \\ Y = 108(2y + a_1x + a_3) \end{array}\right. \quad 或 \quad \left\{\begin{array}{l} x = \frac{1}{36}X - \frac{1}{12}b_2 \\ y = \frac{1}{216}Y - \frac{1}{2}a_1(\frac{1}{36}X - \frac{1}{12}b_2) - \frac{1}{2}a_3, \end{array}\right.$$

我们得到

$$Y^2 = X^3 - 27c_4X - 54c_6. \tag{4}$$

其判别式为 $1728\Delta = c_4^3 - c_6^2.$

定义14.1.1 当$\Delta \neq 0$, 域K 上的点集

$$E := \{(x, y) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}, \quad (5)$$

其中$a_1,\ a_2,\ a_3,\ a_4,\ a_6 \in$ **K**,$\{O\}$ 为无穷远点, 叫做域K 上的**椭圆曲线**.

这时, $j = c_4^3/\Delta$ 叫做椭圆曲线E 的j-**不变量**, 记作$j(E)$.

我们将Weierstrass 方程写成齐次形式:

$$Y^2Z + a_1XYZ + a_3Y = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \quad (6)$$

其中$a_1,\ a_2,\ a_3,\ a_4,\ a_6 \in$ **K**. 则定义1 中的无穷远点O 就是齐次坐标点$[0 : 1 : 0]$.

在对域K 上椭圆曲线E 的研究中，我们通常取如下形式的Weierstrass 方程:

(i) 当域K 的特征不为2，3 时，Weierstrass 方程为

$$y^2 = x^3 + a_4x + a_6, \quad \Delta = -16(4a_4^3 + 27a_6^2), \quad j = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

(ii) 当域K 的特征为2，且$j(E) \neq 0$ 时，Weierstrass 方程为

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad \Delta = a_6, \quad j = 1/a_6.$$

(iii) 当域K 的特征为2，且$j(E) = 0$ 时，Weierstrass 方程为

$$y^2 + a_3y = x^3 + a_4x + a_6, \quad \Delta = a_3^4, \quad j = 0.$$

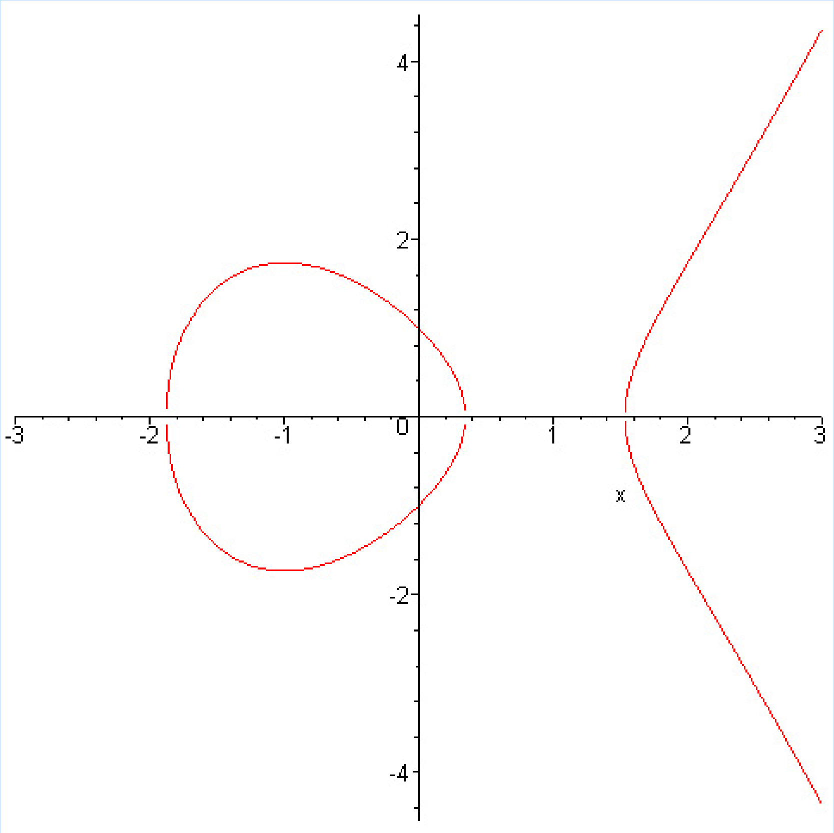
(iv) 当域K 的特征为3，且$j(E) \neq 0$ 时，Weierstrass 方程为

$$y^2 = x^3 + a_2x^2 + a_6, \quad \Delta = -a_2^3a_6, \quad j = -a_2^3/a_6.$$

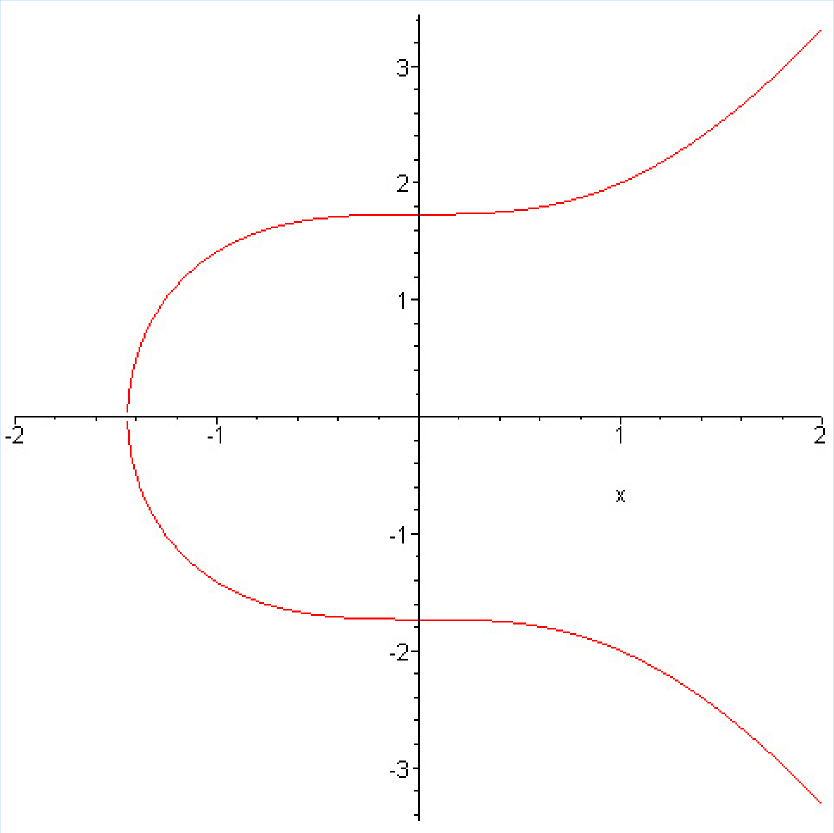
(v) 当域K 的特征为3，且$j(E) = 0$ 时，Weierstrass 方程为

$$y^2 = x^3 + a_4x + a_6, \quad \Delta = -a_4^3, \quad j = 0.$$

例14.1.1 实数域R 上的椭圆曲线$y^2 = x^3 - 3x + 1, \ -3 \le x \le 3$ 的图示为



例14.1.2 实数域R 上的椭圆曲线$y^2 = x^3 + 3,\ -2 \le x \le 2$ 的图示为



14.2 加法原理

设E 是由Weierstrass 方程(5) 定义的域K 上椭圆曲线, 我们定义E 上的运算法则, 记作$\oplus$.

运算法则 设P, Q 是E 上的两个点, L 是过P 和Q 的直线(过P 点的切线, 如果$P = Q$), R 是L 与曲线E 相交的第三点. 设L' 是过R 和O 的直线. 则$P \oplus Q$ 就是L' 与E 相交的第三点.

定理14.2.1 E 上运算法则$\oplus$ 具有如下性质:

(i) 如果直线L 交E 于点P, Q, R (不必是不同的), 则

$$(P \oplus Q) \oplus R = O.$$

(ii) 对任意$P \in E$, $P \oplus O = P$.

(iii) 对任意$P, Q \in E$, $P \oplus Q = Q \oplus P$.

(iv) 设$P \in E$, 存在一个点, 记作$-P$, 使得 $P \oplus (-P) = O$.

(v) 对任意$P, Q, R \in E$, 有

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

这就是说, E 对于运算规则$\oplus$ 构成一个交换群.

更进一步, 如果E 定义在K 上, 则

$$E(\mathbf{K}) := \{(x,y) \in \mathbf{K}\times\mathbf{K} \mid y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6\}\cup\{O\} \tag{7}$$

是E 的子群.

现在我们给出定理14.2.1 中群运算的精确公式.

定理14.2.2 设椭圆曲线E 的一般Weierstrass 方程为:

$$E := \{(x, y) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}.$$

(i) 设$P_1 = (x_1, y_1)$是曲线E 上的点, 则

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3). \tag{8}$$

(ii) 设$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$是E 上的两个点, 且$P_3 = (x_3, y_3) = P_1 + P_2 \neq O$, 则$x_3$, y_3 可以由公式给出

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - a_1x_3 - y_1 - a_3. \end{cases} \tag{9}$$

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

证 设E 是由如下方程

$$F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

定义的椭圆曲线.

(i) 设$P_1 = (x_1, y_1) \in E$, 我们计算点$-P_1$. 设L 是过P_1 和O 的直线, 则该直线为

$$L:\ x - x_1 = 0.$$

将$x = x_1$ 代入到$F(x,y)$ 中, 并求关于y 的两个根y_1, y_1'. 比较下列方程关于一次项y 的系数,

$$F(x_1, y) = (y - y_1)(y - y_1') = y^2 - (y_1 + y_1')y + y_1y_1',$$

我们有$y_1' = -y_1 - a_1x_1 - a_3$, 从而

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3).$$

(ii) 设$P_1=(x_1,y_1)$, $P_2=(x_2,y_2)\in E$. 如果$P_1+P_2\neq O$, 考虑过P_1 和P_2 的直线 $L:\ y=\lambda x+\mu$.

当$x_1\neq x_2$ 时, 直线L 的斜率λ 为 $\lambda=\dfrac{y_2-y_1}{x_2-x_1}$.

当$x_1=x_2$ 时, 直线L 为过点P 的切线, 其斜率λ 为

$$\lambda=\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}.$$

将$y=\lambda x+\mu$ 带入方程$F(x,y)=0$ 中, 有

$$F(x,\lambda x+\mu)=-x^3+(\lambda^2+a_1\lambda-a_2)x^2+(2\lambda\mu+a_1\mu-a_4)x+\mu^2-a_6=0.$$

因为P_1, P_2 和P_3 是E 上三个点, 所以上述方程关于x 有三个解x_1, x_2, x_3.

$$F(x,\lambda x+\mu)=c(x-x_1)(x-x_2)(x-x_3).$$

根据根与系数之间的关系, 我们有$c=-1$ 及

$$x_1+x_2+x_3=\lambda^2+a_1\lambda-a_2.$$

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

14.2.1 实数域R 上椭圆曲线

实数域R 上椭圆曲线及其运算法则的几何意义.

因为实数域R 的特征不为2, 3, 所以实数域R 上椭圆曲线E 的Weierstrass 方程可设为

$$E:\ y^2 = x^3 + a_4x + a_6,$$

其判别式$\Delta = -16(4a_4^3 + 27a_6^2) \neq 0$. E 在R 上的运算规则为:

设$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$是曲线E 上两个点, O 为无穷远点. 则

(1) $O + P_1 = P_1 + O$;

(2) $-P_1 = (x_1, -y_1)$;

(3) 如果$P_3 = (x_3, y_3) = P_1 + P_2 \neq O$,

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1. \end{cases} \quad \text{其中} \quad \begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \dfrac{3x_1^2 + a_4}{2y_1} & \text{如果 } x_1 = x_2. \end{cases} \tag{10}$$

运算法则的几何意义是:

设$P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$是曲线E 上的两个点, O 为无穷远点. 则$-P_1$ 为过点P_1 和点O 的直线L 与曲线E 的交点, 换句话说, $-P_1$ 是点P_1 关于x 轴的对称点.

而点P_1 与点P_2 的和$P_1+P_2=P_3=(x_3,y_3)$ 是过点P_1 和点P_2 的直线L 与曲线E 的交点R 关于x 轴的对称点$P_3=-R$.

例14.2.1 设$P=(0,1)=(x_1,y_1)$ 是**R** 上椭圆曲线$E:\ y^2=x^3+3x+1$ 的点. 求$2P=(x_2,y_2)$, $3P=(x_3,y_3)$, $4P=(x_4,y_4)$, $5P=(x_5,y_5)$, $6P=(x_6,y_6)$, $7P=(x_7,y_7)$, $8P=(x_8,y_8)$.

解 根据公式(10), 我们有

$$\lambda_2=\frac{3x_1^2+a_4}{2y_1}=\frac{3}{2},$$

$$x_2=\lambda_2^2-2x_1=\frac{9}{4},\quad y_2=\lambda_2(x_1-x_2)-y_1=\frac{-35}{8}$$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=\frac{-43}{18},$$

$$x_3=\lambda_3^2-x_1-x_2=\frac{280}{81},\quad y_3=\lambda_3(x_1-x_3)-y_1=\frac{5291}{729}$$

$$\lambda_4=\frac{y_3-y_1}{x_3-x_1}=\frac{2281}{1260},$$

$$x_4=\lambda_4^2-x_1-x_3=\frac{-3519}{19600},\quad y_4=\lambda_4(x_1-x_4)-y_1=\frac{-1852129}{2744000}$$

$$\lambda_5 = \frac{y_4 - y_1}{x_4 - x_1} = \frac{510681}{54740},$$

$$x_5 = \lambda_5^2 - x_1 - x_4 = \frac{13333320}{152881}, \quad y_5 = \lambda_5(x_1 - x_5) - y_1 = \frac{-48696013549}{59776471}$$

$$\lambda_6 = \frac{y_5 - y_1}{x_5 - x_1} = \frac{-348255643}{37238058},$$

$$x_6 = \lambda_6^2 - x_1 - x_5 = \frac{2257258249}{9070276644}, \quad y_6 = \lambda_6(x_1 - x_6) - y_1 = \frac{1146658401987805}{863835007021272}$$

$$\lambda_7 = \frac{y_6 - y_1}{x_6 - x_1} = \frac{723333490963}{549812688282},$$

$$x_7 = \lambda_7^2 - x_1 - x_6 = \frac{49390057276560}{33327979295521},$$

$$y_7 = \lambda_7(x_1 - x_7) - y_1 = \frac{-567521666143702121879}{192403724264235258319}$$

例14.2.2 设$P=(0,1)=(x_1,y_1)$ 是**R** 上椭圆曲线$E:\ y^2=x^3+3x+7$ 的点. 求$2P=(x_2,y_2)$, $3P=(x_3,y_3)$, $4P=(x_4,y_4)$, $5P=(x_5,y_5)$, $6P=(x_6,y_6)$, $7P=(x_7,y_7)$, $8P=(x_8,y_8)$.

解 根据公式(10), 我们有

$$\lambda_2=\frac{3x_1^2+a_4}{2y_1}=\frac{3}{2},$$

$$x_2=\lambda_2^2-2x_1=\frac{9}{4},\quad y_2=\lambda_2(x_1-x_2)-y_1=\frac{-35}{8}$$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=\frac{-43}{18},$$

$$x_3=\lambda_3^2-x_1-x_2=\frac{280}{81},\quad y_3=\lambda_3(x_1-x_3)-y_1=\frac{5291}{729}$$

$$\lambda_4=\frac{y_3-y_1}{x_3-x_1}=\frac{2281}{1260},$$

$$x_4=\lambda_4^2-x_1-x_3=\frac{-3519}{19600},\quad y_4=\lambda_4(x_1-x_4)-y_1=\frac{-1852129}{2744000}$$

$$\lambda_5 = \frac{y_4 - y_1}{x_4 - x_1} = \frac{510681}{54740},$$

$$x_5 = \lambda_5^2 - x_1 - x_4 = \frac{13333320}{152881}, \quad y_5 = \lambda_5(x_1 - x_5) - y_1 = \frac{-48696013549}{59776471}$$

$$\lambda_6 = \frac{y_5 - y_1}{x_5 - x_1} = \frac{-348255643}{37238058},$$

$$x_6 = \lambda_6^2 - x_1 - x_5 = \frac{2257258249}{9070276644}, \quad y_6 = \lambda_6(x_1 - x_6) - y_1 = \frac{1146658401987805}{863835007021272}$$

$$\lambda_7 = \frac{y_6 - y_1}{x_6 - x_1} = \frac{723333490963}{549812688282},$$

$$x_7 = \lambda_7^2 - x_1 - x_6 = \frac{49390057276560}{33327979295521},$$

$$y_7 = \lambda_7(x_1 - x_7) - y_1 = \frac{-56752166614370212879}{192403724264235258319}$$

14.2.2 素域$\mathbf{F}_p$ $(p > 3)$ 上椭圆曲线E

因为素域$\mathbf{F}_p$ 的特征不为2, 3, 所以素域$\mathbf{F}_p$ 上椭圆曲线E 的Weierstrass 方程可设为

$$E:\ y^2 = x^3 + a_4 x + a_6,$$

其判别式$\Delta = -16(4a_4^3 + 27a_6^2) \neq 0$. E 在$\mathbf{F}_p$ 上的运算规则为:

设$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$是曲线E 上的两个点, O 为无穷远点. 则

(1) $O + P_1 = P_1 + O$;

(2) $-P_1 = (x_1, -y_1)$;

(3) 如果$P_3 = (x_3, y_3) = P_1 + P_2 \neq O$,

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1. \end{cases} \quad \text{其中} \quad \begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \dfrac{3x_1^2 + a_4}{2y_1} & \text{如果 } x_1 = x_2. \end{cases} \tag{11}$$

$\mathbf{F}_p$ 上椭圆曲线E 的阶为

$$\#(E(\mathbf{F}_p)) = 1 + \sum_{x=0}^{p-1}\left(1 + \left(\frac{x^3 + a_4 x + a_6}{p}\right)\right) = p + 1 + \sum_{x=0}^{p-1}\left(\frac{x^3 + a_4 x + a_6}{p}\right). \tag{12}$$

访问主页
标题页
目录页
第 21 页 共 81 页
返回
全屏显示
关闭
退出

例14.2.3 设$\mathbf{F}_{17}$ 上椭圆曲线$E: \ y^2 = x^3 + 2x + 3$, 求出该椭圆曲线的全部点以及阶.

解 根据公式(11), 对$x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$, 分别求出$y$.

$x = 0, \ y^2 = 3 \pmod{17}$, 无解,

$x = 1, \ y^2 = 6 \pmod{17}$, 无解,

$x = 2, \ y^2 = 15 \pmod{17}$, $y = 7, \ 8 \pmod{17}$,

$x = 3, \ y^2 = 2 \pmod{17}$, $y = 6, \ 11 \pmod{17}$,

$x = 4, \ y^2 = 7 \pmod{17}$, 无解,

$x = 5, \ y^2 = 2 \pmod{17}$, $y = 6, \ 11 \pmod{17}$,

$x = 6, \ y^2 = 10 \pmod{17}$, 无解,

$x = 7, \ y^2 = 3 \pmod{17}$, 无解,

$x = 8, \ y^2 = 4 \pmod{17}$, $y = 2, \ 15 \pmod{17}$,

$x = 9, \ y^2 = 2 \pmod{17}$, $y = 6, \ 11 \pmod{17}$,

$x = 10, \ y^2 = 3 \pmod{17}$, 无解,

$x=11,\ y^2=13\ (\mathrm{mod}\ 17),\quad y=8,\ 9\ (\mathrm{mod}\ 17),$
$x=12,\ y^2=4\ (\mathrm{mod}\ 17),\quad y=2,\ 15\ (\mathrm{mod}\ 17),$
$x=13,\ y^2=16\ (\mathrm{mod}\ 17),\quad y=4,\ 13\ (\mathrm{mod}\ 17),$
$x=14,\ y^2=4\ (\mathrm{mod}\ 17),\quad y=2,\ 15\ (\mathrm{mod}\ 17),$
$x=15,\ y^2=8\ (\mathrm{mod}\ 17),\quad y=5,\ 12\ (\mathrm{mod}\ 17),$
$x=16,\ y^2=0\ (\mathrm{mod}\ 17),\quad y=0\ (\mathrm{mod}\ 17).$

椭圆曲线的阶为

$$\#(E(\mathbf{F}_{17}))=17+1+\sum_{x=0}^{17-1}\left(\frac{x^3+2x+3}{17}\right)=22.$$

例14.2.4 设$\mathbf{F}_{17}$ 上椭圆曲线$E: \ y^2 = x^3 + 2x + 3$ 上的点$P = (2,7)$, $Q = (11,8)$. 求$P + Q = (x_3, y_3)$, $2P = (x_4, y_4)$, $4P = (x_5, y_5)$, $8P = (x_6, y_6)$, $10P = (x_7, y_7)$, $11P = (x_8, y_8)$, $22P$.

解 令$x_1 = 2,\ y_1 = 7, x_2 = 11,\ y_2 = 8$, 则

$$\lambda_1 = \frac{y_2 - y_1}{x_2 - x_1} = 2, \quad x_3 = \lambda_1^2 - x_1 - x_2 = 8, \qquad y_3 = \lambda_1(x_1 - x_3) - y_1 = 15$$

$$\lambda_2 = \frac{3x_1^2 + a_4}{2y_1} = 1, \quad x_4 = \lambda_2^2 - 2x_1 = 14, \qquad y_4 = \lambda_2(x_1 - x_4) - y_1 = 15$$

$$\lambda_3 = \frac{3x_4^2 + a_4}{2y_4} = 14, \quad x_5 = \lambda_3^2 - 2x_4 = 15, \qquad y_5 = \lambda_3(x_4 - x_5) - y_4 = 5$$

$$\lambda_4 = \frac{3x_5^2 + a_4}{2y_5} = 15, \quad x_6 = \lambda_4^2 - 2x_5 = 8, \qquad y_6 = \lambda_4(x_5 - x_6) - y_5 = 15$$

$$\lambda_5 = \frac{y_6 - y_4}{x_6 - x_4} = 0, \quad x_7 = \lambda_5^2 - x_4 - x_6 = 12, \qquad y_7 = \lambda_5(x_4 - x_7) - y_4 = 2$$

$$\lambda_6 = \frac{y_7 - y_1}{x_7 - x_1} = 8, \quad x_8 = \lambda_6^2 - x_1 - x_7 = 16, \qquad y_8 = \lambda_6(x_1 - x_8) - y_1 = 0$$

因为过点$11P = (x_8, y_8) = (16, 0)$ 的切线垂直于x轴, 所以$22P = 2(11P) = O$ (无穷远点).

例14.2.5 上椭圆曲线$E: y^2 = x^3 + 3x + 1$, 求出该椭圆曲线的全部点以及阶.

解 根据公式(11), 对$x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16$, 分别求出$y$.

$x = 0,\ y^2 = 1 \pmod{17}$, $y = 1,\ 16 \pmod{17}$,

$x = 1,\ y^2 = 5 \pmod{17}$, 无解,

$x = 2,\ y^2 = 15 \pmod{17}$, $y = 7,\ 8 \pmod{17}$,

$x = 3,\ y^2 = 3 \pmod{17}$, 无解,

$x = 4,\ y^2 = 9 \pmod{17}$, $y = 3,\ 14 \pmod{17}$,

$x = 5,\ y^2 = 5 \pmod{17}$, 无解,

$x = 6,\ y^2 = 14 \pmod{17}$, 无解,

$x = 7,\ y^2 = 8 \pmod{17}$, $y = 5,\ 12 \pmod{17}$,

$x = 8,\ y^2 = 10 \pmod{17}$, 无解,

$x = 9,\ y^2 = 9 \pmod{17}$, $y = 3,\ 14 \pmod{17}$,

$x = 10,\ y^2 = 11 \pmod{17}$, 无解,

$x=11,\ y^2=5 \pmod{17}$,　无解,

$x=12,\ y^2=14 \pmod{17}$,　无解,

$x=13,\ y^2=10 \pmod{17}$,　无解,

$x=14,\ y^2=16 \pmod{17}$,　$y=4,\ 13 \pmod{17}$,

$x=15,\ y^2=4 \pmod{17}$,　$y=2,\ 15 \pmod{17}$,

$x=16,\ y^2=14 \pmod{17}$,　无解.

椭圆曲线的阶为

$$\#(E(\mathbf{F}_{17}))=17+1+\sum_{x=0}^{17-1}\left(\frac{x^3+3x+1}{17}\right)=15.$$

例14.2.6 设$\mathbf{F}_{17}$上椭圆曲线$E:\ y^2 = x^3 + 3x + 1$ 上的点$P = (2, 7)$. 求$2P = (x_2, y_2)$, $3P = (x_3, y_3)$, $4P = (x_4, y_4)$, $5P = (x_5, y_5)$. $6P = (x_6, y_6)$, $7P = (x_7, y_7)$, $8P = (x_8, y_8)$, $9P = (x_9, y_9)$, $10P = (x_{10}, y_{10})$, $11P = (x_{11}, y_{11})$, $12P = (x_{12}, y_{12})$, $13P = (x_{13}, y_{13})$, $14P = (x_{14}, y_{14})$.

解 令$x_1 = 2,\ y_1 = 7$, 则

$$\lambda_2 = \frac{3x_1^2 + a_4}{2y_1} = 12,\quad x_2 = \lambda_2^2 - 2x_1 = 4,\qquad y_3 = \lambda_2(x_1 - x_2) - y_1 = 3$$

$$\lambda_3 = \frac{y_2 - y_1}{x_2 - x_1} = 15,\quad x_3 = \lambda_3^2 - x_1 - x_2 = 15,\qquad y_3 = \lambda_3(x_1 - x_3) - y_1 = 2$$

$$\lambda_4 = \frac{3x_2^2 + a_4}{2y_2} = 0,\quad x_4 = \lambda_4^2 - 2x_2 = 9,\qquad y_4 = \lambda_4(x_2 - x_4) - y_2 = 14$$

$$\lambda_5 = \frac{y_4 - y_1}{x_4 - x_1} = 1,\quad x_5 = \lambda_5^2 - x_1 - x_4 = 7,\qquad y_5 = \lambda_5(x_1 - x_5) - y_1 = 5$$

$$\lambda_6 = \frac{y_4 - y_2}{x_4 - x_2} = 9,\quad x_6 = \lambda_6^2 - x_2 - x_4 = 0,\qquad y_6 = \lambda_6(x_2 - x_6) - y_2 = 16$$

$$\lambda_7 = \frac{y_6 - y_1}{x_6 - x_1} = 4,\quad x_7 = \lambda_7^2 - x_1 - x_6 = 14,\qquad y_7 = \lambda_7(x_1 - x_7) - y_1 = 13$$

$$\lambda_8 = \frac{3x_4^2 + a_4}{2y_4} = 10, \quad x_8 = \lambda_8^2 - 2x_4 = 14, \qquad y_8 = \lambda_8(x_4 - x_8) - y_4 = 4$$

$$\lambda_9 = \frac{y_8 - y_1}{x_8 - x_1} = 4, \quad x_9 = \lambda_9^2 - x_1 - x_8 = 0, \qquad y_9 = \lambda_9(x_1 - x_9) - y_1 = 1$$

$$\lambda_{10} = \frac{y_8 - y_2}{x_8 - x_2} = 12, \quad x_{10} = \lambda_{10}^2 - x_2 - x_8 = 7, \qquad y_{10} = \lambda_{10}(x_2 - x_{10}) - y_2 = 12$$

$$\lambda_{11} = \frac{y_{10} - y_1}{x_{10} - x_1} = 1, \quad x_{11} = \lambda_{11}^2 - x_1 - x_{10} = 9, \qquad y_{11} = \lambda_{11}(x_1 - x_{11}) - y_1 = 3$$

$$\lambda_{12} = \frac{y_8 - y_4}{x_8 - x_4} = 15, \quad x_{12} = \lambda_{12}^2 - x_4 - x_8 = 15, \qquad y_{12} = \lambda_{12}(x_4 - x_{12}) - y_4 = 15$$

$$\lambda_{13} = \frac{y_{12} - y_1}{x_{12} - x_1} = 15, \quad x_{13} = \lambda_{13}^2 - x_1 - x_{12} = 4, \qquad y_{13} = \lambda_{13}(x_1 - x_{13}) - y_1 = 14$$

$$\lambda_{14} = \frac{y_{12} - y_2}{x_{12} - x_2} = 15, \quad x_{14} = \lambda_{14}^2 - x_2 - x_{12} = 2, \qquad y_{14} = \lambda_{14}(x_2 - x_{14}) - y_2 = 10$$

最后, $14P = -P$, $15P = O$ (无穷远点).

下面是群$< P >$中点的分布图:

例14.2.7 设$P=(5,4)=(x_1,y_1)$ 是$\mathbf{F}_{23}$ 上椭圆曲线$E:\ y^2=x^3+3x+1$ 的点. 求点P 生成的群$<P>$.

解 根据公式(12), 我们有

$$\#(E(\mathbf{F}_p))=p+1+\sum_{x=0}^{p-1}\left(\frac{x^3+a_4x+a_6}{p}\right)=23+1-9=15$$

设$kP=(x_k,y_k)$. 根据公式(11), 我们有

$$\lambda_2=\frac{3x_1^2+a_4}{2y_1}=1,\quad x_2=\lambda_2^2-2x_1=14,\quad y_2=\lambda_2(x_1-x_2)-y_1=21$$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=21,\quad x_3=\lambda_3^2-x_1-x_2=8,\quad y_3=\lambda_3(x_1-x_3)-y_1=13$$

$$\lambda_4=\frac{y_3-y_1}{x_3-x_1}=22,\quad x_4=\lambda_4^2-x_1-x_3=11,\quad y_4=\lambda_4(x_1-x_4)-y_1=13$$

$$\lambda_5=\frac{y_4-y_1}{x_4-x_1}=11,\quad x_5=\lambda_5^2-x_1-x_4=13,\quad y_5=\lambda_5(x_1-x_5)-y_1=11$$

$$\lambda_6=\frac{y_5-y_1}{x_5-x_1}=8,\quad x_6=\lambda_6^2-x_1-x_5=0,\quad y_6=\lambda_6(x_1-x_6)-y_1=1$$

$$\lambda_7=\frac{y_6-y_1}{x_6-x_1}=3,\quad x_7=\lambda_7^2-x_1-x_6=4,\quad y_7=\lambda_7(x_1-x_7)-y_1=10$$

$$\lambda_8 = \frac{y_7 - y_1}{x_7 - x_1} = 6, \quad x_8 = \lambda_8^2 - x_1 - x_7 = 4, \quad y_8 = \lambda_8(x_1 - x_8) - y_1 = 13$$

$$\lambda_9 = \frac{y_8 - y_1}{x_8 - x_1} = l, \quad x_9 = \lambda_9^2 - x_1 - x_8 = 0, \quad y_9 = \lambda_9(x_1 - x_9) - y_1 = 22$$

$$\lambda_{10} = \frac{y_9 - y_1}{x_9 - x_1} = 8, \quad x_{10} = \lambda_{10}^2 - x_1 - x_9 = 13, \quad y_{10} = \lambda_{10}(x_1 - x_{10}) - y_1 = 12$$

$$\lambda_{11} = \frac{y_{10} - y_1}{x_{10} - x_1} = 11, \quad x_{11} = \lambda_{11}^2 - x_1 - x_{10} = 11, \quad y_{11} = \lambda_{11}(x_1 - x_{11}) - y_1 = 10$$

$$\lambda_{12} = \frac{y_{11} - y_1}{x_{11} - x_1} = 22, \quad x_{12} = \lambda_{12}^2 - x_1 - x_{11} = 8, \quad y_{12} = \lambda_{12}(x_1 - x_{12}) - y_1 = 10$$

$$\lambda_{13} = \frac{y_{12} - y_1}{x_{12} - x_1} = 21, \quad x_{13} = \lambda_{13}^2 - x_1 - x_{12} = 14, \quad y_{13} = \lambda_{13}(x_1 - x_{13}) - y_1 = 2$$

$$\lambda_{14} = \frac{y_{13} - y_1}{x_{13} - x_1} = 1, \quad x_{14} = \lambda_{14}^2 - x_1 - x_{13} = 5, \quad y_{14} = \lambda_{14}(x_1 - x_{13}) - y_1 = 7$$

$$\lambda_{15} = \frac{y_{14} - y_1}{x_{14} - x_1} = \infty, \quad (x_{15}, y_{15}) = O$$

下面是群$< P >$中点的分布图:

访问主页
标题页
目录页
第 30 页 共 81 页
返回
全屏显示
关闭
退出

例14.2.8 设$P = (5,8) = (x_1, y_1)$ 是$\mathbf{F}_{23}$ 上椭圆曲线$E: \ y^2 = x^3 + 3x + 7$ 的点. 求点P 生成的群$< P >$.

解 根据公式(12), 以及对应的legendre 符号,

x	0	1	2	3	4	5	6	7	8	9	10	11
$\left(\frac{x^3+a_4x+a_6}{p}\right)$	-1	-1	-1	-1	-1	1	-1	1	-1	1	1	-1
x	12	13	14	15	16	17	18	19	20	21	22	
$\left(\frac{x^3+a_4x+a_6}{p}\right)$	0	1	-1	0	-1	1	-1	0	-1	1	1	

我们有

$$\#(E(\mathbf{F}_p)) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + a_4x + a_6}{p}\right) = 23 + 1 - 4 = 20$$

以及

$$\begin{aligned} E(\mathbf{F}_p) \ = \ & \{O, (5,3), (5,20), (7,7), (7,16), (9,2), (9,21), (10,5), (10,18), \\ & (12,0), (13,9), (13,14), (15,0), (17,7), (17,16), (19,0), \\ & (21,4), (21,19), (22,7), (22,16), \} \end{aligned}$$

(i) 取$P=(5,3)=(x_1,y_1)$. 设$kP=(x_k,y_k)$. 根据公式(11), 我们有

$$\lambda_2=\frac{3x_1^2+a_4}{2y_1}=13,$$

$$x_2=\lambda_2^2-2x_1=21,\quad y_2=\lambda_2(x_1-x_2)-y_1=19$$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=1,$$

$$x_3=\lambda_3^2-x_1-x_2=21,\quad y_3=\lambda_3(x_1-x_3)-y_1=4$$

$$\lambda_4=\frac{y_3-y_1}{x_3-x_1}=13,$$

$$x_4=\lambda_4^2-x_1-x_3=5,\quad y_4=\lambda_4(x_1-x_4)-y_1=20$$

(ii) 取$P=(7,16)=(x_1,y_1)$. 设$kP=(x_k,y_k)$. 根据公式(11), 我们有

$$\lambda_2=\frac{3x_1^2+a_4}{2y_1}=9,\quad x_2=\lambda_2^2-2x_1=21,\quad y_2=\lambda_2(x_1-x_2)-y_1=19$$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=15,\quad x_3=\lambda_3^2-x_1-x_2=13,\quad y_3=\lambda_3(x_1-x_3)-y_1=9$$

$$\lambda_4=\frac{y_3-y_1}{x_3-x_1}=18,\quad x_4=\lambda_4^2-x_1-x_3=5,\quad y_4=\lambda_4(x_1-x_4)-y_1=20$$

$$\lambda_5=\frac{y_4-y_1}{x_4-x_1}=21,\quad x_5=\lambda_5^2-x_1-x_4=15,\quad y_5=\lambda_5(x_1-x_5)-y_1=0$$

$$\lambda_6=\frac{y_5-y_1}{x_5-x_1}=21,\quad x_6=\lambda_6^2-x_1-x_5=5,\quad y_6=\lambda_6(x_1-x_6)-y_1=3$$

$$\lambda_7=\frac{y_6-y_1}{x_6-x_1}=18,\quad x_7=\lambda_7^2-x_1-x_6=13,\quad y_7=\lambda_7(x_1-x_7)-y_1=14$$

$$\lambda_8=\frac{y_7-y_1}{x_7-x_1}=15,\quad x_8=\lambda_8^2-x_1-x_7=21,\quad y_8=\lambda_8(x_1-x_8)-y_1=4$$

$$\lambda_9=\frac{y_8-y_1}{x_8-x_1}=9,\quad x_9=\lambda_9^2-x_1-x_8=7,\quad y_9=\lambda_9(x_1-x_9)-y_1=7$$

(iii) 取$P=(9,2)=(x_1,y_1)$. 设$kP=(x_k,y_k)$. 根据公式(11), 我们有

$$\lambda_2=\frac{3x_1^2+a_4}{2y_1}=4,\quad x_2=\lambda_2^2-2x_1=21,\quad y_2=\lambda_2(x_1-x_2)-y_1=19$$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=11,\quad x_3=\lambda_3^2-x_1-x_2=22,\quad y_3=\lambda_3(x_1-x_3)-y_1=16$$

$$\lambda_4=\frac{y_3-y_1}{x_3-x_1}=17,\quad x_4=\lambda_4^2-x_1-x_3=5,\quad y_4=\lambda_4(x_1-x_4)-y_1=20$$

$$\lambda_5=\frac{y_4-y_1}{x_4-x_1}=7,\quad x_5=\lambda_5^2-x_1-x_4=12,\quad y_5=\lambda_5(x_1-x_5)-y_1=0$$

$$\lambda_6=\frac{y_5-y_1}{x_5-x_1}=7,\quad x_6=\lambda_6^2-x_1-x_5=5,\quad y_6=\lambda_6(x_1-x_6)-y_1=3$$

$$\lambda_7=\frac{y_6-y_1}{x_6-x_1}=17,\quad x_7=\lambda_7^2-x_1-x_6=22,\quad y_7=\lambda_7(x_1-x_7)-y_1=7$$

$$\lambda_8=\frac{y_7-y_1}{x_7-x_1}=11,\quad x_8=\lambda_8^2-x_1-x_7=21,\quad y_8=\lambda_8(x_1-x_8)-y_1=4$$

$$\lambda_9=\frac{y_8-y_1}{x_8-x_1}=4,\quad x_9=\lambda_9^2-x_1-x_8=9,\quad y_9=\lambda_9(x_1-x_9)-y_1=21$$

注意到$3(7,16)+(9,2)=(13,9)+(9,2)=(17,7)$

(iv) 取$P=(17,7)=(x_1,y_1)$. 设$kP=(x_k,y_k)$. 根据公式(11), 我们有

$$\lambda_2=\frac{3x_1^2+a_4}{2y_1}=3,\quad x_2=\lambda_2^2-2x_1=21,\quad y_2=\lambda_2(x_1-x_2)-y_1=4$$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=5,\quad x_3=\lambda_3^2-x_1-x_2=10,\quad y_3=\lambda_3(x_1-x_3)-y_1=5$$

$$\lambda_4=\frac{y_3-y_1}{x_3-x_1}=20,\quad x_4=\lambda_4^2-x_1-x_3=5,\quad y_4=\lambda_4(x_1-x_4)-y_1=3$$

$$\lambda_5=\frac{y_4-y_1}{x_4-x_1}=8,\quad x_5=\lambda_5^2-x_1-x_4=19,\quad y_5=\lambda_5(x_1-x_5)-y_1=0$$

$$\lambda_6=\frac{y_5-y_1}{x_5-x_1}=8,\quad x_6=\lambda_6^2-x_1-x_5=5,\quad y_6=\lambda_6(x_1-x_6)-y_1=20$$

$$\lambda_7=\frac{y_6-y_1}{x_6-x_1}=20,\quad x_7=\lambda_7^2-x_1-x_6=10,\quad y_7=\lambda_7(x_1-x_7)-y_1=18$$

$$\lambda_8=\frac{y_7-y_1}{x_7-x_1}=5,\quad x_8=\lambda_8^2-x_1-x_7=21,\quad y_8=\lambda_8(x_1-x_8)-y_1=19$$

$$\lambda_9=\frac{y_8-y_1}{x_8-x_1}=3,\quad x_9=\lambda_9^2-x_1-x_8=17,\quad y_9=\lambda_9(x_1-x_9)-y_1=16$$

14.2.3 域$\mathbf{F}_{2^n}$ $(n \geq 1)$ 上椭圆曲线E, $j(E) \neq 0$

因为域$\mathbf{F}_{2^n}$ 的特征为2, 所以域$\mathbf{F}_{2^n}$ 上椭圆曲线E 的Weierstrass 方程可设为

$$E: \ y^2 + xy = x^3 + a_2x^2 + a_6.$$

E 在域$\mathbf{F}_{2^n}$上的运算规则为:

设$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$是曲线E 上的两个点, O 为无穷远点. 则

(1) $O + P_1 = P_1 + O$;

(2) $-P_1 = (x_1, x_1 + y_1)$;

(3) 如果$P_3 = (x_3, y_3) = P_1 + P_2 \neq O$,

$$\begin{cases} x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2, \\ y_3 = \lambda(x_1 + x_3) + x_3 + y_1. \end{cases} \quad \text{其中} \quad \begin{cases} \lambda = \dfrac{y_2 + y_1}{x_2 + x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \dfrac{x_1^2 + y_1}{x_1} & \text{如果 } x_1 = x_2. \end{cases} \tag{13}$$

例14.2.9 设$\mathbf{F}_{2^8} = \mathbf{F}_2[t]/(t^8+t^4+t^3+t^2+1)$. 设$\mathbf{F}_{2^8}$ 上的椭圆曲线

$$E : y^2 + x \cdot y = x^3 + x^2 + 1.$$

设$P_1 = (t^3+1, t^7+t^6+t^5+t^3+t^2+t)$. 计算$-P_1$, $2P_1, 3P_1, 4P_1, 5P_1$.

解 设点$kP_1 = (x_k, y_k)$, 则

2) $l_2 = (x_1^2+y_1)/x_1 = t^4+t^2+t+1;$

$x_2 = l_2^2 + l_2 + x_1 + x_1 + 1 = t^4+t^3+t^2+t;$

$y_2 = l_2 \cdot (x_1+x_2) + x_2 + y_1 = t^7+t^6+t^5+t^4+t^3;$

3) $l_3 = (y_2+y_1)/(x_2+x_1) = t^6+t^5+t^2+t+1;$

$x_3 = l_3^2 + l_3 + x_1 + x_2 + 1 = t^7+t^6+t^4+t^3+t^2+1;$

$y_3 = l_3 \cdot (x_1+x_3) + x_3 + y_1 = t^7+t^4+t^3+1;$

4) $l_4 = (x_2^2+y_2)/x_2 = t^6+t^5+t^4+t^2;$

$x_4 = l_4^2 + l_4 + x_2 + x_2 + 1 = t^7+t^6+1;$

$y_4 = l_4 \cdot (x_2+x_4) + x_4 + y_2 = t^5+t^3;$

5) $l_5 = (y_4+y_1)/(x_4+x_1) = t^3+1;$

$x_5 = l_5^2 + l_5 + x_1 + x_4 + 1 = 1 + t^7;$

$y_5 = l_5 \cdot (x_1+x_5) + x_5 + y_1 = t^7+t^6+t^4+t+1.$

6) $l_6 = (y_5 + y_1)/(x_5 + x_1) = t^3 + 1;$

$x_6 = l_6^2 + l_6 + x_1 + x_5 + 1 = 1 + t^7;$

$y_6 = l_6 \cdot (x_1 + x_6) + x_6 + y_1 = t^7 + t^6 + t^4 + t + 1.$

7) $l_7 = (y_6 + y_1)/(x_6 + x_1) = t^3 + 1;$

$x_7 = l_7^2 + l_7 + x_1 + x_6 + 1 = 1 + t^7;$

$y_7 = l_7 \cdot (x_1 + x_7) + x_7 + y_1 = t^7 + t^6 + t^4 + t + 1.$

8) $l_8 = (y_7 + y_1)/(x_7 + x_1) = t^3 + 1$

$x_8 = l_8^2 + l_8 + x_1 + x_7 + 1 = 1 + t^7$

$y_8 = l_8 \cdot (x_1 + x_8) + x_8 + y_1 = t^7 + t^6 + t^4 + t + 1$

9) $l_9 = (y_8 + y_1)/(x_8 + x_1) = t^5 + t^4 + t + 1$

$x_9 = l_9^2 + l_9 + x_1 + x_8 + 1 = t^7 + t^6 + t^4 + t^2 + t$

$y_9 = l_9 \cdot (x_1 + x_9) + x_9 + y_1 = t^6 + t^2 + t^7 + t^4 + t + 1$

10) $l_{10} = (y_9 + y_1)/(x_9 + x_1) = t^6 + t^4 + t^3 + t^2 + t + 1$

$x_{10} = l_{10}^2 + l_{10} + x_1 + x_9 + 1 = t^2$

$y_{10} = l_{10} \cdot (x_1 + x_{10}) + x_{10} + y_1 = t^4 + t^2 + t$

$$11)\ l_{11} = (y_{10} + y_1)/(x_{10} + x_1) = t^7 + t^6 + t^3 + t^2 + 1$$

$$x_{11} = l_{11}^2 + l_{11} + x_1 + x_{10} + 1 = t^6 + t^3 + t^2 + t$$

$$y_{11} = l_{11} \cdot (x_1 + x_{11}) + x_{11} + y_1 = t^7 + t^6 + t^4 + t^2$$

$$12)\ l_{12} = (y_{11} + y_1)/(x_{11} + x_1) = t^6 + t^7 + t^5 + t^3$$

$$x_{12} = l_{12}^2 + l_{12} + x_1 + x_{11} + 1 = t^6 + t^2$$

$$y_{12} = l_{12} \cdot (x_1 + x_{12}) + x_{12} + y_1 = t^6 + t^3 + t^2 + t$$

$$13)\ l_{13} = (y_{12} + y_1)/(x_{12} + x_1) = t^7 + t^4 + 1$$

$$x_{13} = l_{13}^2 + l_{13} + x_1 + x_{12} + 1 = t^7 + t^6 + t^4 + t$$

$$y_{13} = l_{13} \cdot (x_1 + x_{13}) + x_{13} + y_1 = t^6 + t + 1$$

$$14)\ l_{14} = (y_{13} + y_1)/(x_{13} + x_1) = t^3 + t^2 + t + 1$$

$$x_{14} = l_{14}^2 + l_{14} + x_1 + x_{13} + 1 = t^7$$

$$y_{14} = l_{14} \cdot (x_1 + x_{14}) + x_{14} + y_1 = t^7 + t^6 + t^3 + t$$

$$15)\ l_{15} = (y_{14} + y_1)/(x_{14} + x_1) = t^7 + t^5 + t^3 + t$$

$$x_{15} = l_{15}^2 + l_{15} + x_1 + x_{14} + 1 = 1$$

$$y_{15} = l_{15} \cdot (x_1 + x_{15}) + x_{15} + y_1 = t^7 + t^6 + t^4 + t^2 + t$$

例14.2.10 设$\mathbf{F}_{2^3} = \mathbf{F}_2[t]/(t^3+t+1)$. 设设$\mathbf{F}_{2^3}$ 上的椭圆曲线

$$E: y^2 + x \cdot y = x^3 + x^2 + 1.$$

设点$P_1 = (t, t^5) = (t, t^2+t+1)$ 是$E(\mathbf{F}_{2^3})$ 的生成元, 求$E(\mathbf{F}_{2^3})$ 上所有点.

解 设点$kP_1 = (x_k, y_k)$, 则

2) $l_2 = (x_1^2 + y_1)/x_1 = t^2$;

$x_2 = l_2^2 + l_2 + x_1 + x_1 + 1 = t + 1$; $y_2 = l_2 \cdot (x_1 + x_2) + x_2 + y_1 = 0$;

3) $l_3 = (y_2 + y_1)/(x_2 + x_1) = t^2 + t + 1$;

$x_3 = l_3^2 + l_3 + x_1 + x_2 + 1 = t^2$; $y_3 = l_3 \cdot (x_1 + x_3) + x_3 + y_1 = t^2 + t + 1$;

4) $l_4 = (x_2^2 + y_2)/x_2 = t + 1$;

$x_4 = l_4^2 + l_4 + x_2 + x_2 + 1 = t^2 + t + 1$; $y_4 = l_4 \cdot (x_2 + x_4) + x_4 + y_2 = 0$;

5) $l_5 = (y_4 + y_1)/(x_4 + x_1) = t^2 + 1$;

$x_5 = l_5^2 + l_5 + x_1 + x_4 + 1 = t^2 + t$; $y_5 = l_5 \cdot (x_1 + x_5) + x_5 + y_1 = t + 1$;

6) $l_6 = (y_5 + y_1)/(x_5 + x_1) = 1$;

$x_6 = l_6^2 + l_6 + x_1 + x_5 + 1 = t^2 + 1$; $y_6 = l_6 \cdot (x_1 + x_6) + x_6 + y_1 = t^2 + 1$;

7) $l_7 = (y_6 + y_1)/(x_6 + x_1) = t + 1;$

$x_7 = l_7^2 + l_7 + x_1 + x_6 + 1 = 0; y_7 = l_7 \cdot (x_1 + x_7) + x_7 + y_1 = 1;$

8) $l_8 = (y_7 + y_1)/(x_7 + x_1) = t + 1;$

$x_8 = l_8^2 + l_8 + x_1 + x_7 + 1 = t^2 + 1; y_8 = l_8 \cdot (x_1 + x_8) + x_8 + y_1 = 0;$

9) $l_9 = (y_8 + y_1)/(x_8 + x_1) = 1;$

$x_9 = l_9^2 + l_9 + x_1 + x_8 + 1 = t^2 + t; y_9 = l_9 \cdot (x_1 + x_9) + x_9 + y_1 = t^2 + 1;$

10) $l_{10} = (y_9 + y_1)/(x_9 + x_1) = t^2 + 1;$

$x_{10} = l_{10}^2 + l_{10} + x_1 + x_9 + 1 = t^2 + t + 1; y_{10} = l_{10} \cdot (x_1 + x_{10}) + x_{10} + y_1 = t^2 + t + 1;$

11) $l_{11} = (y_{10} + y_1)/(x_{10} + x_1) = 0;$

$x_{11} = l_{11}^2 + l_{11} + x_1 + x_{10} + 1 = t^2; y_{11} = l_{11} \cdot (x_1 + x_{11}) + x_{11} + y_1 = t + 1;$

12) $l_{12} = (y_{11} + y_1)/(x_{11} + x_1) = t^2 + t + 1;$

$x_{12} = l_{12}^2 + l_{12} + x_1 + x_{11} + 1 = t + 1; y_{12} = l_{12} \cdot (x_1 + x_{12}) + x_{12} + y_1 = t + 1;$

13) $l_{13} = (y_{12} + y_1)/(x_{12} + x_1) = t^2;$

$x_{13} = l_{13}^2 + l_{13} + x_1 + x_{12} + 1 = t; y_{13} = l_{13} \cdot (x_1 + x_{13}) + x_{13} + y_1 = t^2 + 1;$

14) $l_{14} = (y_{13} + y_1)/(x_{13} + x_1) = \infty.$

域$\mathbf{F}_{3^n}$ $(n \geq 1)$ 上椭圆曲线E, $j(E) \neq 0$.

因为域$\mathbf{F}_{3^n}$ 的特征为3, 所以域$\mathbf{F}_{3^n}$ 上椭圆曲线E 的Weierstrass 方程可设为

$$E: \; y^2 = x^3 + a_2 x^2 + a_6.$$

E 在域$\mathbf{F}_{3^n}$上的运算规则为:

设$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$是曲线E 上的两个点, O 为无穷远点. 则

(1) $O + P_1 = P_1 + O$;

(2) $-P_1 = (x_1, -y_1)$;

(3) 如果$P_3 = (x_3, y_3) = P_1 + P_2 \neq O$,

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 - a_2, \\ \\ y_3 = \lambda(x_1 - x_3) - y_1. \end{cases} \quad \text{其中} \quad \begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \dfrac{3x_1^2 + 2a_2 x_2}{2y_1} & \text{如果 } x_1 = x_2. \end{cases} \tag{14}$$

14.3 有限域上的椭圆曲线的阶

设$\mathbf{K} = \mathbf{F}_q$ 是$q = p^n$ 元有限域. 设E 是定义在$\mathbf{F}_q$ 上的椭圆曲线. 当$p > 3$ 时, 其Weierstrass 方程为

$$y^2 = x^3 + a_4 x + a_6.$$

易知, $\mathbf{F}_q$ 上椭圆曲线E 中的点数$\#(E(\mathbf{F}_q)) \le 2q+1$. 事实上, 对每个$x \in \mathbf{F}_q$, 至多有两个$y \in \mathbf{F}_q$ 使得$P(x,y) \in E$, 再加上无穷远点O, 我们有$\#(E) \le 2|\mathbf{F}_q| + 1 = 2q+1$.

现在我们考虑$\mathbf{F}_q$ 上椭圆曲线E 上的映射:

$$\begin{array}{cccc} \varphi: & \overline{\mathbf{F}}_q & \longrightarrow & \overline{\mathbf{F}}_q \\ & (x,y) & \longmapsto & (x^q, y^q) \\ & O & \longmapsto & O \end{array}$$

φ 叫做q 次幂**Frobenius 映射**. 易知, φ 将E 上的点映到E, 且保持群的运算法则. 这就是说, φ 是$\mathbf{F}_q$ 上E 的群同态, 因此, φ 又叫做q 次幂**Frobenius 自同态**.

Frobenius 自同态φ 与其迹(trace) 在椭圆曲线的研究中起着重要作用. 它们由如下方程联系:

$$\varphi^2 - [t]\varphi + [q] = [0],$$

也就是, 对椭圆曲线E 上任意点$P = (x, y)$, 我们有

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = O.$$

此外, 我们有

$$\#(E(\mathbf{F}_q)) = q + 1 - t.$$

第一个关于$E(\mathbf{F}_q)$ 的阶的逼近估计是由下面的Hasse 定理给出.

定理14.3.1 (Hasse). 设E 是定义在$\mathbf{F}_q$ ($q = p^n$, p素数)上的椭圆曲线, φ q 次幂**Frobenius 自同态** 则椭圆曲线E 上的点数$\#(E(\mathbf{F}_q))$ 满足

$$|\#(E(\mathbf{F}_q)) - (q + 1)| \leq 2\sqrt{q}.$$

14.4 重复倍加算法

本节讨论n 倍点nP 的计算

将n 写成二进制:

$$n = n_0 + n_1 2 + n_2 2^2 + \cdots + n_{i-1} 2^{i-1} + n_i 2^i + \cdots + n_{k-2} 2^{k-2} + n_{k-1} 2^{k-1},$$

其中$n_i \in \{0, 1\}$, $i = 0, 1, \ldots, k-1$.

$$nP = n_0 P + n_1 2P + n_2 2^2 P + \cdots + n_{i-1} 2^{i-1} P + n_i 2^i P + \cdots + n_{k-2} 2^{k-2} P + n_{k-1} 2^{k-1} P$$

$$nP = \underbrace{\underbrace{\underbrace{\underbrace{\underbrace{n_0 P_0}_{Q_0} + n_1 P_1}_{Q_1} + n_2 P_2}_{Q_2} + \cdots + n_{k-2} P_{k-2}}_{Q_{k-2}} + n_{k-1} P_{k-1}}_{Q_{k-1}}$$

0). 计算$P_0 = P$, 及$Q_0 = n_0 P_0$.

1). 计算$P_1 = 2P_0$, 及$Q_1 = Q_0 + n_1 P_1$.

2). 计算$P_2 = 2P_1$, 及$Q_2 = Q_1 + n_2 P_2$.

$\ldots\ldots$

i-1). 计算$P_{i-1} = 2b_{i-2}$ 及$Q_{i-1} = Q_{i-2} + n_{i-1} P_{i-1}$

i). 计算$P_i = 2P_{i-1}$ 及$Q_i = Q_{i-1} + n_i P_i$

$\ldots\ldots$

k-2). 计算$P_{k-2} = 2P_{k-3}$ 及$Q_{k-2} = Q_{k-3} + n_{k-2} P_{k-2}$

k-1). 计算$P_{k-1} = 2P_{k-2}$ 及$Q_{k-1} = Q_{k-2} + n_{k-1} P_{k-1}$

令$P_k = 2^k P = (x_k, y_k),\ k = 0, 1, 2, \ldots$, 由$P_k = 2P_{k-1}$, 我们得到

$\lambda_k = \frac{3\,{x_{k-1}}^2 + a_4}{2y_{k-1}}$

$x_k = \lambda_k^2 - 2x_{k-1},\ \ y_k = \lambda_k(x_{k-1} - x_k) - y_{k-1}$

再令$Q_k = Q_{k-1} + n_k P_k = (u_k, v_k),\ k = 1, 2, \ldots$, 我们得到

$\lambda_k = (v_{k-1} - y_k)/(u_{k-1} - x_k)$;

if $(n_k > 0)$ then $u_k = \lambda_k^2 - u_{k-1} - x_k$;

$v_k = \lambda_k(u_{k-1} - u_k) - v_{k-1}$;

else $u_k = u_{k-1}, v_k = v_{k-1}$ end if; end do;

例14.4.1 $p=100823$ 是一个素数, 有限域$\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$ 上的椭圆曲线点群

$$E(\mathbf{F}_p)=\{(x,y)\mid\in\mathbf{F}_p\times\mathbf{F}_p,\ \ y^2=x^3+3x+7\}\cup\{O\}$$

$|E(\mathbf{F}_p)|=100482=2\cdot3\cdot16747.$

$E(\mathbf{F}_p)$ 的生成元为$P_0=(1,8811)$. $\mathrm{ord}(P_0)=100482$. 因而, $P=6P_0=(62046,14962)$ 的阶为素数16747. 计算$1007P$

$n=1007=1+2+2^2+2^3+2^5+2^6+2^7+2^8+2^9$

$n_0=1,n_1=1,n_2=1,n_3=1,n_4=0,n_5=1,n_6=1,n_7=1,n_8=1,n_9=1.$

0). 计算$P_0=P=(62046,14962)$, 及$Q_0=P_0=(62046,14962)$.

1). 计算$P_1=2P_0=(79956,69266)$, 及$Q_1=Q_0+P_1=(10232,99402)$.

2). 计算$P_2=2P_1=(18004,60305)$, 及$Q_2=Q_1+P_2=(77066,35653)$.

3). 计算$P_3=2P_2=(71409,96128)$, 及$Q_3=Q_2+P_3=(98956,33961)$.

4). 计算$P_4=2P_3=(88114,449)$, 及$Q_4=Q_3=(98956,33961)$.

5). 计算$P_5=2P_4=(83127,15384)$, 及$Q_5=Q_4+P_5=(72985,39118)$.

6). 计算$P_6=2P_5=(74848,74692)$, 及$Q_6=Q_5+P_6=(53181,78296)$.

7). 计算$P_7=2P_6=(32021,39593)$, 及$Q_7=Q_6+P_7=(53704,97059)$.

8). 计算$P_8=2P_7=(78143,43796)$, 及$Q_8=Q_7+P_8=(43906,14791)$.

9). 计算$P_9=2P_8=(94069,18649)$, 及$Q_9=Q_8+P_9=(80726,17229)$.

例14.4.2 $p = 359$ 是一个素数, 有限域$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ 上的椭圆曲线点群

$$E(\mathbf{F}_p) = \{(x, y) \mid \in \mathbf{F}_p \times \mathbf{F}_p,\ \ y^2 = x^3 + 3x + 7\} \cup \{O\}$$

$|E(\mathbf{F}_p)| = 395 = 5 \cdot 79.$

$E(\mathbf{F}_p)$ 的生成元为$P_0 = (1, 27)$. $\mathrm{ord}(P_0) = 395$. 计算$5P, 79P, 395P$

i) 计算$5P$

$n = 79 = 1 + 2^2$

$n_0 = 1, n_1 = 0, n_2 = 1$

0). 计算$P_0 = P = (1, 27)$, 及$Q_0 = P_0 = (1, 27)$.

1). 计算$P_1 = 2P_0 = (162, 354)$, 及$Q_1 = Q_0 = (1, 27)$.

2). 计算$P_2 = 2P_1 = (7, 33)$, 及$Q_2 = Q_1 + P_2 = (352, 340)$.

ii) 计算$79P$

$n = 79 = 1 + 2 + 2^2 + 2^3 + 2^6$

$n_0 = 1, n_1 = 1, n_2 = 1, n_3 = 1, n_4 = 0, n_5 = 0, n_6 = 1$

0). 计算$P_0 = P = (1, 27)$, 及$Q_0 = P_0 = (1, 27)$.

1). 计算$P_1 = 2P_0 = (162, 354)$, 及$Q_1 = Q_0 + P_1 = (92, 194)$.

2). 计算$P_2 = 2P_1 = (7, 33)$, 及$Q_2 = Q_1 + P_2 = (126, 316)$.

3). 计算$P_3 = 2P_2 = (6, 263)$, 及$Q_3 = Q_2 + P_3 = (19, 183)$.

4). 计算$P_4 = 2P_3 = (95, 355)$, 及$Q_4 = Q_3 = (19, 183)$.

5). 计算$P_5 = 2P_4 = (316, 147)$, 及$Q_5 = Q_4 = (19, 183)$.

6). 计算$P_6 = 2P_5 = (290, 146)$, 及$Q_6 = Q_5 + P_6 = (160, 80)$.

iii) 计算$395P$

$n = 395 = 1 + 2 + +2^3 + 2^7 + 2^8$ 1, 1, 0, 1, 0, 0, 0, 1, 1

$n_0 = 1, n_1 = 1, n_2 = 0, n_3 = 1, n_4 = 0, n_5 = 0, n_6 = 0, n_7 = 1, n_8 = 1$

0). 计算$P_0 = P = (1, 27)$, 及$Q_0 = P_0 = (1, 27)$.

1). 计算$P_1 = 2P_0 = (162, 354)$, 及$Q_1 = Q_0 + P_1 = (92, 194)$.

2). 计算$P_2 = 2P_1 = (7, 33)$, 及$Q_2 = Q_1 + P_2 = (92, 194)$.

162, 354, 92, 194 7, 33, 92, 194 6, 263, 298, 180 95, 355, 298, 180

316, 147, 298, 180 290, 146, 298, 180 79, 221, 166, 351

3). 计算$P_3 = 2P_2 = (6, 263)$, 及$Q_3 = Q_2 + P_3 = (298, 180)$.

4). 计算$P_4 = 2P_3 = (95, 355)$, 及$Q_4 = Q_3 = (298, 180)$.

5). 计算$P_5 = 2P_4 = (316, 147)$, 及$Q_5 = Q_4 = (298, 180)$.

6). 计算$P_6 = 2P_5 = (290, 146)$, 及$Q_6 = Q_5 + P_6 = (298, 180)$.

7). 计算$P_7 = 2P_6 = (79, 221)$, 及$Q_7 = Q_6 + P_7 = (166, 351)$.

8). 计算$P_8 = 2P_7 = (166, 8)$, 及$Q_8 = Q_7 + P_8 = O$.

例14.2.* 设$\mathbf{F}_{17}$ 上椭圆曲线$E:\ y^2 = x^3 - 3x + 1$, 求出该椭圆曲线的全部点以及$\#(E(\mathbf{F}_2))$, 以及各个点P 生成的子群$< P >$.

解 根据公式(11), 对$x = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16$, 分别求出$y$.

$x = 0,\ y^2 = 1 \pmod{17},\quad y = 1,\ 16 \pmod{17},$

$x = 1,\ y^2 = 16 \pmod{17},\quad y = 4,\ 13 \pmod{17},$

$x = 2,\ y^2 = 3 \pmod{17},$ 无解,

$x = 3,\ y^2 = 2 \pmod{17},\quad y = 6,\ 11 \pmod{17},$

$x = 4,\ y^2 = 2 \pmod{17},\quad y = 6,\ 11 \pmod{17},$

$x = 5,\ y^2 = 9 \pmod{17},\quad y = 3,\ 14 \pmod{17},$

$x = 6,\ y^2 = 12 \pmod{17}$, 无解,

$x = 7,\ y^2 = 0 \pmod{17}$, $y = 0 \pmod{17}$,

$x = 8,\ y^2 = 10 \pmod{17}$, $y = 6,\ 11 \pmod{17}$,

$x = 9,\ y^2 = 13 \pmod{17}$, $y = 8,\ 9 \pmod{17}$,

$x = 10,\ y^2 = 2 \pmod{17}$, $y = 6,\ 11 \pmod{17}$,

$x = 11,\ y^2 = 7 \pmod{17}$, 无解,

$x = 12,\ y^2 = 10 \pmod{17}$, 无解,

$x = 13,\ y^2 = 0 \pmod{17}$, $y = 0 \pmod{17}$,

$x = 14,\ y^2 = 0 \pmod{17}$, $y = 0 \pmod{17}$,

$x = 15,\ y^2 = 16 \pmod{17}$, $y = 4,\ 13 \pmod{17}$,

$x = 16,\ y^2 = 3 \pmod{17}$, 无解.

椭圆曲线的阶为

$$\#(E(\mathbf{F}_{17})) = 17 + 1 + \sum_{x=0}^{17-1} \left(\frac{x^3 + 3x + 1}{17} \right) = 22.$$

对于点$P_1=(x_1,y_1), x_1=0,\ y_1=7,$ 则$\lambda_2=\dfrac{3x_1^2+a_4}{2y_1}=7,\ \ x_2=\lambda_2^2-2x_1=15,\qquad y_2=\lambda_2(x_1-x_2)-y_1=13$

$$\lambda_3=\frac{y_2-y_1}{x_2-x_1}=11,\ \ x_3=\lambda_3^2-x_1-x_2=4,\qquad y_3=\lambda_3(x_1-x_3)-y_1=6$$

$$\lambda_4=\frac{y_3-y_1}{x_3-x_1}=14,\ \ x_4=\lambda_4^2-x_1-x_3=5,\qquad y_4=\lambda_4(x_1-x_4)-y_1=14$$

$$\lambda_5=\frac{y_4-y_1}{x_4-x_1}=6,\ \ x_5=\lambda_5^2-x_1-x_4=14,\qquad y_5=\lambda_5(x_1-x_5)-y_1=0$$

$$\lambda_6=\frac{y_5-y_1}{x_5-x_1}=6,\ \ x_6=\lambda_6^2-x_1-x_5=5,\qquad y_6=\lambda_6(x_1-x_6)-y_1=3$$

$$\lambda_7=\frac{y_6-y_1}{x_6-x_1}=14,\ \ x_7=\lambda_7^2-x_1-x_6=4,\qquad y_7=\lambda_7(x_1-x_7)-y_1=11$$

$$\lambda_8=\frac{y_7-y_1}{x_7-x_1}=11,\ \ x_8=\lambda_8^2-x_1-x_7=15,\qquad y_8=\lambda_8(x_1-x_8)-y_1=4$$

$$\lambda_9=\frac{y_8-y_1}{x_8-x_1}=7,\ \ x_9=\lambda_9^2-x_1-x_8=0,\qquad y_9=\lambda_9(x_1-x_9)-y_1=16$$

$P_9=-P_1.$