arXiv:2302.00568v1 [math.NT] 1 Feb 2023

椭圆曲线上点的二分公式

Lorenz Halbeisen数学系，苏黎世联邦理工学院中心，R¨amistrasse 101，8092 Z¨urich，瑞士 lorenz.halbeisen@math.ethz.ch

Norbert Hungerb¨uhler

数学系，苏黎世联邦理工学院中心，R¨amistrasse 101，8092 Z¨urich，瑞士
norbert.hungerbuehler@math.ethz.ch

关键词：椭圆曲线、二分公式、有限域

2020年 数学主题分类：11G05 94A60 11R16

摘要

设 P 是复数域上椭圆曲线上的任意一点，该曲线具有 $y^2 = x^3 + a_4\,x + a_6$ 或 $y^2 = x^3 + a_2\,x^2 + a_4\,x$ 的形式。我们给出计算点 $P/2$ 的显式公式，即满足 $2 * Q = P$ 的点 Q。

1 引言

尽管椭圆曲线上的点加倍方法众所周知，但关于点减半的结果却鲜有报道。我们在推论2中得到的少数结果之一是：椭圆曲线 $P = (x_0,\ y_0)$ 上的有理点 $E:\quad y^2 = (x - e_0)(x - e_1)(x - e_2)$（其中$e_i \in \mathbb{Q}$）属于 $2E(\mathbb{Q})$，当且仅当 $x_0 - e_0$、$x_0 - e_1$、$x_0 - e_2$ 都是有理数的平方数（参见[2, 第 I 章，§9，命题 20]）。有关相关结果，请参阅 [1, 4, 5, 6]。

求点的二分公式，一个自然的方法是对加倍公式求逆。然而，这通常会导出难以求解的四次方程。另一种方法是先扩张基本域，使方程成为双二次方程，这正是我们下文所做的。

下一节中，我们将分别给出复数域 C 上形如 $y^2 = x^3 + a_4\,x + a_6$ 和形如 $y^2 = x^3 + a_2\,x^2 + a_4\,x$ 的椭圆曲线上点的二分显式公式。请注意，由于每条椭圆曲线都可以变换为这种形式，因此任意椭圆曲线上点的二分也存在类似公式。此外，将复数域 C 替换为某个有限域时，这些公式同样适用。作为示例，我们将展示如何对正整数 n 对应的曲线 $y^2 = x^3 - n^2 + x$ 以及素域上形如 $y^2 = x^3 + a_2x + a_6$ 的曲线上的点进行二分。

2 $P/2$ 的公式

Theo注 1. 设 E_{a_4,a_6} 和 E_{a_2,a_4} 是由下式定义在复数域上的非奇异椭圆曲线

$$E_{a_4,a_6}:\ y^2 = x^3 + a_4\,x + a_6 \qquad and \qquad E_{a_2,a_4}:\ y^2 = x^3 + a_2\,x^2 + a_4\,x$$

其中 $a_2, a_4, a_6 \in$属于复数域，且令 $P = (x_0, y_0)$ 为 E_{a_4,a_6} 或 E_{a_2,a_4}上的一个点。若 $P \in E_{a_4,a_6}$，令

$$r = -9\,a_6 + \sqrt{3}\sqrt{4\,a_4^3 + 27\,a_6^2}, \qquad d = -a_4\left(\frac{2}{3r}\right)^{\frac{1}{3}} + \left(\frac{r}{18}\right)^{\frac{1}{3}}, \qquad k = -(a_4 + 3d^2),$$

and

$$e_0 = d, \qquad e_1 = \frac{-d + \sqrt{9d^2 + 4k}}{2}, \qquad e_2 = \frac{-d - \sqrt{9d^2 + 4k}}{2}.$$

若 $P \in E_{a_2,\ a_4}$，则令

$$e_0 = 0, \qquad e_1 = \frac{-a_2 + \sqrt{a_2^2 - 4a_4}}{2}, \qquad e_2 = \frac{-a_2 - \sqrt{a_2^2 - 4a_4}}{2}.$$

最后，在两种情况下均令

$$\gamma = \sqrt{x_0 - e_0}, \qquad \alpha = \sqrt{x_0 - e_1}, \qquad \beta = \sqrt{x_0 - e_2}.$$

于是，椭圆曲线 $E_{a_4,\ a_6}$ 和 $E_{a_2,\ a_4}$ 均具有如下形式

$$y^2 = (x_0 - e_0)(x_0 - e_1)(x_0 - e_2)$$

并且满足 $2 * Q_i = P$ 的四个点 Q_1、Q_2、Q_3、Q_4 的 x 坐标为

$$\begin{aligned} x_{11} &= x_0 + \alpha\beta + \gamma(\alpha + \beta), \\ x_{12} &= x_0 + \alpha\beta - \gamma(\alpha + \beta), \\ x_{21} &= x_0 - \alpha\beta + \gamma(\alpha - \beta), \\ x_{22} &= x_0 - \alpha\beta - \gamma(\alpha - \beta). \end{aligned}$$

证明。对于曲线 $E_{a_2,\ a_4}$，显然有 $-e_0 - e_1 - e_2 = a_2$、$e_0e_1 + e_1e_2 + e_2e_0 = a_4$ 和 $-e_0e_1e_2 = 0$。

对于曲线 $E_{a_4,\ a_6}$，我们需要证明 $-e_0 - e_1 - e_2 = 0$（这显然成立）、$e_0e_1 + e_1e_2 + e_2e_0 = a_4$ 以及 $-e_0e_1e_2 = a_6$。

我们有

$$e_0\,e_1 + e_1\,e_2 + e_2\,e_0 \;=\; -d^2 + \frac{d^2 - 9d^2 - 4k}{4} = -3\,d^2 - k$$

and

$$-e_0\,e_1\,e_2 \;=\; -d\,\frac{d^2 - 9d^2 - 4k}{4} = d(2\,d^2 + k).$$

因此，我们必须证明

$$a_4 = -(3\,d^2 + k) \qquad \text{and} \qquad a_6 = d(2\,d^2 + k).$$

根据 k 的定义，我们有

$$-(3d^2 + k) = -(3d^2 - a_4 - 3d^2) = a_4$$

and

$$d(2d^2+k) = 2d^3 - d\,a_4 - 3d^3 = -d^3 - d\,a_4 =$$

$$\left(a_4^3\left(\frac{2}{3r}\right)\underbrace{-a_4^2\left(\frac{2}{3r}\right)^{\frac{1}{3}} + a_4\left(\frac{r}{18}\right)^{\frac{1}{3}}}_{=da_4} - \frac{r}{18}\right) - d\,a_4 = a_4^3\,\frac{2}{3r} - \frac{r}{18} =$$

$$\frac{12\,a_4^3 - r^2}{18\,r} = \frac{12\,a_4^3 - 81\,a_6^2 - 12\,a_4^3 - 81\,a_6^2 + 18a_6\sqrt{4\,a_4^3+27\,a_6^2}}{-162\,a_6 + 18\sqrt{4\,a_4^3+27\,a_6^2}} =$$

$$\frac{a_6\big(-162\,a_6 + 18\sqrt{4\,a_4^3+27\,a_6^2}\,\big)}{-162\,a_6 + 18\sqrt{4\,a_4^3+27\,a_6^2}} = a_6.$$

通过平移曲线，我们可以假设 $e_0 = 0$。特别地，我们可以假设椭圆曲线为 $E_{a_2,\ a_4}$。要证明 $x_{11}, x_{12}, x_{21}, x_{22}$ 是满足条件 $2 * Q = P$ 的点$Q \in E_{a_2,\ a_4}$ 的 x 坐标，只需证明点Q_{ij}:$=(x_{ij}, y)$ 的 x 坐标等于 x_0，其中 $i, j \in \{1, 2\}$ 和 $y = \sqrt{x_{ij}^3 + a_2\,x_{11}^2 + a_4\,x_{11}}$。现在，点 $2 * Q_{ij}$ 的 x 坐标 x_{2ij} 由公式给出

$$x_{2ij} = \frac{x_{ij}^4 - 2a_4\,x_{ij}^2 + a_4^2}{4(x_{ij}^3 + a_2\,x_{11}^2 + a_4\,x_{11})} = \frac{(x_{ij}^2 - a_4)^2}{4x_{ij}(x_{ij}^2 + a_2\,x_{ij} + a_4)}.$$

现在，若 $e_0 = 0$，则 $x_0 = \gamma^2$，于是得到

$$\begin{aligned} x_{11} &= (\alpha+\gamma)(\beta+\gamma), \\ x_{12} &= (\alpha-\gamma)(\beta-\gamma), \\ x_{21} &= (\alpha+\gamma)(-\beta+\gamma), \\ x_{22} &= (\alpha-\gamma)(-\beta-\gamma). \end{aligned}$$

此外，我们有 $a_2 = \alpha^2 + \beta^2 - 2\gamma^2$ 和 $a_6 = (\alpha^2 - \gamma^2)(\beta^2 - \gamma^2)$；若将 x_{ij}、a_2、a_4 用 γ、α、β 表示，不难验证

$$(x_{ij}^2 - a_4)^2 = 4x_{ij}\gamma^2(x_{ij}^2 + a_2\,x_{ij} + a_4),$$

这表明 $x_{2ij} = x_0$。

证毕。

注。（a）事实上，我们想指出，分别经过坐标为 x_{11}、x_{12} 和 x_{21}、x_{22} 的点对的直线交于曲线 E 上的一点 $S = (x_S, y_S)$，且

$$x_S = d + \frac{k}{d - x_0} \text{ for } E = E_{a_4,a_6} \quad \text{and} \quad x_S = \frac{a_4}{x_0} \text{ for } E = E_{a_2,a_4} \text{ (i.e., } d = 0,\ k = -a_4).$$

(b) 如果 E 是形如 $E_{a_4,\ a_6}$ 或 $E_{a_2,\ a_4}$ 的椭圆曲线，定义在域 F 上，且 P、$Q \in E(\mathrm{F}) - 0$ 满足 $2 * Q = P$，那么当且仅当群 $(E(\mathrm{F})\ +)$ 中不存在 2 阶元素时，Q 是唯一的。

(c) 如果我们令 $t = x_0^2 + dx_0 - 2d^2 - k$，并且

$$w = \sqrt{t}, \qquad w_1 = \sqrt{(x_0 - d)(d + 2w + 2x_0)}, \qquad w_2 = \sqrt{(x_0 - d)(d - 2w + 2x_0)},$$

那么，对于 $E_{a_4,\ a_6}$，我们有

$$x_{11} = x_0 + w + w_1, \quad x_{12} = x_0 + w - w_1, \quad x_{21} = x_0 - w + w_2, \quad x_{22} = x_0 - w - w_2.$$

由定理1 可得以下结论

推论 2. 椭圆曲线上的有理点 $P = (x_0, y_0)$

$$E:\ y^2 = (x - e_0)(x - e_1)(x - e_2) \quad with\ e_0, e_1, e_2 \in \mathbb{Q}$$

等于 $2 * Q$ 某个有理点 Q 在 E上，当且仅当 $x_0 - e_0$、$x_0 - e_1$、$x_0 - e_2$都是有理数的平方数。

证明. 首先注意到，由于对于任意有理点 $P = (x_0, y_0)$， $E(\mathbb{Q})$ 的挠群同构于 $\mathbb{Z}_2 \times \mathbb{Z}_2$, ，因此满足 $2 * Q_i$ 的四个点 Q_i要么全都不是有理点，要么全都是有理点。现在，由于我们有 $y_0 = -\lambda x_0 + \lambda x_{ij} - y_{ij}$，其中

$$\lambda = \frac{3x_{ij}^2 + 2a_2 x_{ij} + a_4}{2y_{ij}},$$

并且 y_0 是有理的，y_{ij} 是有理的当且仅当 x_{ij} 是有理的。特别地，四个值 x_{11}、x_{12}、x_{21}、x_{22} 要么全都不是有理数，要么全都是有理数。因此，只需证明 x_{11} 是有理的当且仅当 $x_0 - e_0$、$x_0 - e_1$、$x_0 - e_2$ 都是有理数的平方数。

通过平移曲线 E，我们可以假设 $e_0 = 0$，从而得到

$$x_{11} = (\alpha + \gamma)(\beta + \gamma).$$

($\Leftarrow$) 如果 $x_0 = \gamma^2$、$x_0 - e_1 = \alpha^2$、$x_0 - e_2 = \beta^2$ 分别是有理数 γ、α、β的平方数，那么 x_{11} 显然是一个有理数。

($\Rightarrow$) 如果 x_{11}、x_{12}、x_{21}、x_{22} 是有理数，那么它们全都

$$(\alpha + \gamma)(\beta + \gamma), \quad (\alpha - \gamma)(\beta - \gamma), \quad (\alpha + \gamma)(-\beta + \gamma), \quad (\alpha - \gamma)(-\beta - \gamma),$$

都是有理数，这恰好发生在 γ、α、β全都是有理数的情况下。 $q.e.d.$

3 两个例子

例 1. 对于自然数 n，考虑曲线

$$E_n:\ y^2 = x^3 - n^2 x$$

在有理数域 $\mathbb{Q}$ 上。众所周知， n 是全等数，当且仅当 E_n 上存在满足 $y_0 \neq 0$的有理点（x_0, y_0）。此外，已知其挠群

E_n(Q) 同构于 $\mathsf{Z}_2 \times \mathsf{Z}_2$——注意，2 阶的三个点是 (0,0) 和 $(\pm n, 0)$。

现在，对于 $a_4 = -n^2$ 和 $a_6 = 0$，我们有 $e_0 = 0$、$e_1 = n$ 和 $e_2 = -n$。假设 (x_0, y_0) 是 E 上的一个有理点，且满足 $y_0 \neq 0$。特别地，(x_0, y_0) 是一个无穷阶点。于是，我们的二分公式给出

$$\begin{aligned}
x_{11} &= x_0 + \sqrt{x_0^2 - n^2} + \sqrt{x_0}\left(\sqrt{x_0 - n} + \sqrt{x_0 + n}\right),\\
x_{12} &= x_0 + \sqrt{x_0^2 - n^2} - \sqrt{x_0}\left(\sqrt{x_0 - n} + \sqrt{x_0 + n}\right),\\
x_{21} &= x_0 - \sqrt{x_0^2 - n^2} + \sqrt{x_0}\left(\sqrt{x_0 - n} - \sqrt{x_0 + n}\right),\\
x_{22} &= x_0 - \sqrt{x_0^2 - n^2} - \sqrt{x_0}\left(\sqrt{x_0 - n} - \sqrt{x_0 + n}\right).
\end{aligned}$$

对于 $n = 6$、$x_0 = -3$ 和 $y_0 = 9$，点 $P = (x_0, y_0)$ 是一个 E_n 上的无穷阶点；又由于 $\sqrt{x_0^2 - n^2} \notin \mathsf{Q}$，不存在有理点 $Q \in E_n$ 使得 $2 * Q = P$。另一方面，$2 * P = (25/4, -35/8)$，并且对于这四个点

$$Q_1 = (18, -72), \quad Q_1 = (-2, -8), \quad Q_1 = (-3, 9), \quad Q_1 = (12, 36),$$

我们有 $2 * Q_i = 2 * P$。

例 2。设 p 是一个奇素数，满足 $p > \max\{|a_4|, |a_6|\}$，并设 E 是一条形如以下形式的椭圆曲线

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

在域 F_p 上。此外，设 $P = (x_0, y_0)$ 是 $E(\mathsf{F}_p)$ 上的一个点。

假设多项式 $X^3 + a_4\, X + a_6 \in \mathsf{F}_p[X]$ 在 F_p 上不可约，这意味着群 $(E, +)$ 中没有元素的阶为 2。于是存在唯一的 $Q \in E(\mathsf{F}_p)$ 使得 $Q = P/2$，即 $2 * Q = P$。现在考虑域 $\mathsf{F}_{p^3} := \mathsf{F}_p[X]/(X^3 + a_4\, X + a_6)$。那么，对于 $d = X$ 和 $k = -(a_4 + 3\, X^2)$，计算 x_{ij}（对于 $i, j \in \{1, 2\}$）的过程在域 F_{p^3} 中进行，其中 x_{ij} 中恰好有一个属于 F_{p^3}，它就是 $P/2$ 的 x-坐标。我们想指出的是，当 $p \equiv 3$(模 4) 时，对于任意为平方数的 $a \in \mathsf{F}_{p^3}$，都有 $\sqrt{a} = \pm a^{(p^3+1)/4}$（关于 $p \equiv 3$(模 4) 情形下根的计算，见 [3]）。

为了说明该算法，令

$$p = 17000000000000071, \quad E:\ y^2 = x^3 + 17\, x + 71, \quad P = (17071,\ 4145148307074498).$$

于是 $P \in E(\mathsf{F}_p)$，$p \equiv 3$（模 4），且多项式 $f = X^3 + 17X + 71$ 在 F_p上不可约。为了计算 $P/2$，我们在域 $\mathsf{F}_{p^3} = \mathsf{F}_p[X]/(f)$ 中进行运算，并首先计算 $\pm w$、w_1 和 w_2——见备注 (c)——相对于 $x_0 = 1700000000000071$、$d = X$和 $k = -(17 + 3X^2)$:

$$\begin{aligned}
w &= 14551045313109763\, X^2 + 6554553633085449\, X + 7788921359847751\\
-w &= 2448954686890308\, X^2 + 10445446366914622\, X + 9211078640152320\\
w_1 &= 2448954686890308\, X^2 + 10445446366914622\, X + 9211078640152320\\
w_2 &= 11464660070096309\, X^2 + 3152403672687182\, X + 16599480794424362.
\end{aligned}$$

因此，$w + w_1 = w_1 - (-w) \in \mathbb{F}_p$，且由于 $x_0 \in \mathbb{F}_p$，我们有

$$x_{11} = x_0 + w + w_1 = 4631223433830370 \in \mathbb{F}_p$$

由此得到点

$$P/2 = (4631223433830370,\ 13664114850453464),$$

并且由于 $x_{12}, x_{21}, x_{22} \notin \mathbb{F}_p$，$P/2$ 是 $E(\mathbb{F}_p)$ 上唯一满足性质 $2 * (P/2) = P$ 的点。

事实上，我们还可以先计算 P 在有限群 $(E, +)$ 中的阶，从而得到点 $P/2$：P 的阶为 $m = 16999999816127027$（这与 E 的阶相同）；又因为 2 在 $\mathbb{Z}_m$ 中的乘法逆元是 $\bar{2} = 8499999908063514$，所以我们有 $P/2 = \bar{2} * P$。

备注。借助我们的二分公式，对于有限域上的某些椭圆曲线 E 以及 E 上的点 P，我们可以逆转 Diffi-Hellman 密钥交换算法：如果椭圆曲线 E 的阶是奇数，那么由于群 $(E, +)$ 是有限生成阿贝尔群，对于 E 上的每个点 P，$P/2$ 都是唯一的。现在，Alice 和 Bob 交换了一个共同的密钥 k 后，Alice 可以按如下方式加密一个正整数 T。首先，Alice 将 T 乘以某个整数 10^m，并在 E 上寻找一个点 $Q = (10^m \cdot T + i, y_i)$，使得 $i < 10^m$。然后，Alice 按步骤遍历 k 的二进制表示，每一步从 Q 开始，将该点加倍并加上点 $b_n * P$，其中 b_n 是 k 的二进制表示中的第 n 个条目。Alice 将结果 Q' 发送给 Bob；Bob 可以从 Q' 开始，通过从后往前读取密钥 k 的二进制表示、将加法替换为减去 P，并将点加倍替换为点的二分，来逆转 Alice 的算法。

参考文献

[1] B. M. Bekker 和 Yu. G. Zarkhin. 椭圆曲线上有理点的二除法，Algebra i Analiz，29(4):196–239，2017。[2] Neal Koblitz. 《椭圆曲线与模形式导论》（第 2 版），[《数学研究生教材》第 97], 卷，Springer-Verlag，纽约，1993。[3] Siguna M¨uller. 有限域中平方根的计算，Designs, Codes and Cryptography，31(3):301–312，2004。[4] Mohammad Sadek 和 Tu˘gba Yesin. 椭圆曲线四次模型上的二可除性与有理丢番图 D(q)-五元组，Rev. R. Acad. Cienc. Exactas F ´ıs. Nat. Ser. A Mat. RACSAM，116(3):第 139 号论文（ 17 页），2022。[5] Jeffrey Yelton. 椭圆曲线的 8- 除法域札记，Eur. J. Math.，3(3):603–613，2017。[6] Yu. G. Zarkhin. 奇数次超椭圆曲线及其雅可比簇上的二除法，Izv. Ross. Akad. Nauk Ser. Mat.，83(3):93–112，2019；译文发表于 Izv. Math.，83(3):501–520，2019。