一类 $j=0$ 超奇异椭圆曲线的性质及其标量乘算法

翁 江[1],康晓春[2],豆允旗[3],马传贵[4]
(1. 空军工程大学信息与导航学院,陕西西安 710077;2. 中国传媒大学信息工程学院,北京 100024;
3. 数学工程与先进计算国家重点实验室,河南郑州,450001;4. 陆军航空兵学院基础部,北京 101123)

摘 要: 针对非超奇异椭圆曲线上的标量乘算法已经有比较多的研究.与非超奇异曲线不同,超奇异椭圆曲线的自同态环是四元数代数的一个序模,为非交换环.本文主要针对特征大于3的有限域上一类 j 不变量为0的超奇异椭圆曲线,分析了曲线自同态环及其商环的结构.进而研究了此类曲线上整数表示的性质,并基于这种表示方法提出了一种针对此类曲线的标量乘算法.理论上证明了针对此类超奇异曲线,当选择合适系数集合时,此表示实质上为 p-adic 展开.实验结果表明:相较于4-NAF等方法,p-adic 表示方法提高标量乘效率一倍以上.

关键词: 超奇异椭圆曲线;四元数代数;自同态环;Frobenius 自同态;τ-adic 展开
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018)09-2131-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.09.013

Property and Scalar Multiplication Algorithm on Supersingular Elliptic Curves with j Invariant 0

WENG Jiang[1], KANG Xiao-chun[2], DOU Yun-qi[3], MA Chuan-gui[4]
(1. *Information and Navigation College, Air Force Engineering University, Xi'an, Shaanxi* 710077, *China*;
2. *Information Engineering School, Communication University of China, Beijing* 100024, *China*;
3. *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, Henan* 450001, *China*;
4. *Department of Basic, Army Aviation Institution, Beijing* 101123 *China*)

Abstract: The scalar multiplication algorithms for non-supersingular elliptic curves have been widely studied. In contrast, the endomorphism ring of supersingular elliptic curve is an order in a definite quaternion algebra, which is not commutative. This paper focuses on a class of supersingular elliptic curves of j-invariant zero in characteristic greater than 3. We make analysis of the structures of its endomorphism ring and quotient ring. Further we study the properties of integer expansion according to this class of curves. Based on this representation, a scalar multiplication algorithm is proposed. We demonstrate that the representation is essentially the p-adic expansion in theory when a suitable digit set is chosen. The experimental results show that compared with the method of 4-NAF, the p-adic method improves the efficiency of scalar multiplication of more than 100%.

Key words: supersingular elliptic curve; quaternion algebra; endomorphism ring; Frobenius endomorphism; τ-adic expansion

1 引言

在过去的三十年里,椭圆曲线公钥密码(Elliptic Curve Cryptography, ECC)受到了广泛的关注.ECC 算法中耗时最多的操作为标量乘运算,即 $nP=\underbrace{P+P+\cdots+P}_{n\text{个}}$,其中 P 为椭圆曲线上的点,$n\in\mathbb{Z}$.目前提高椭圆曲线标量乘算法的效率主要有以下几个研究方向:直接改进点加和倍点运算公式、利用标量的稀疏

收稿日期:2016-09-19;修回日期:2018-05-10;责任编辑:梅志强
基金资助:国家自然科学基金项目(No. 61379150);数学工程与先进计算国家重点实验室开放基金课题(No. 2016A02);河南省重点科技攻关计划项目(No. 122102210126, No. 092101210502)

表示[1~3]、寻找新的曲线形式使点加和倍点运算更快[4,5]、利用可有效计算自同态进行加速[6~8].

最经典的标量乘算法为倍点-加方法(double-and-add method),首先将整数 n 表示成二进制形式 $n=\sum_{k=0}^{l-1} d_k 2^k$,其中 $d_k \in \{0,1\}$;然后利用 Horner 准则来计算 nP:

$$nP = d_0P + 2(d_1P + 2(d_2P + 2(\cdots + 2(d_{l-1}P)\cdots)))$$

设 $\mathrm{HW}_x(n)$ 为 n 的 x 进制表示中非零项的个数,则倍点-加算法需要 $\mathrm{HW}_2(n)-1$ 个点加与 $l-1$ 个倍点运算. 由于椭圆曲线上点的减法和加法运算类似,可以利用非邻接型(Non-Adjacent Form, NAF)表示[1]、w-NAF 表示[2]等更稀疏的表示方法减少点加运算的个数.

另一方面,从减少倍点运算的计算量考虑,利用可有效计算的自同态,标量 n 还可以表示为关于复数基的展开形式. 对于特征为素数 p 的有限域上的椭圆曲线,存在 Frobenius 自同态 τ,

$$\tau(x,y) = (x^p, y^p)$$

其特征多项式为 $\tau^2 - t\tau + p = 0$. 通常计算 Frobenius 自同态 τ 的计算开销要比倍点运算低很多. Solinas[6]将标量 n 展开为关于基 τ 的表示,开创性地提出了 τ-and-add 方法并用于特征为 2 的 Koblitz 曲线. 这种方法同样可以利用 Horner 准则进行计算,由于利用更快的 Frobenius 自同态替代倍点运算,从而提高标量乘计算的效率. 一般地,可以将整数 n 展开为 $n=\sum_{k=0}^{l-1} d_k\tau^k$,其中 d_k 属于合适的系数集合 S,则可以利用 τ-and-add 方法来计算:

$$nP = d_0P + \tau(d_1P + \tau(d_2P + \tau(\cdots + \tau(d_{l-1}P)\cdots)))$$

对于每个非零系数 $d_i \in S$,需要预计算并存储 d_iP,τ-and-add 方法计算标量乘需要 $\mathrm{HW}_\tau(n)-1$ 个加法和 $l-1$ 次自同态 τ 的计算. 由于计算 τ 只需要对域中两个元素做 p 次方幂的运算,在正规基表示下可以通过循环移位来进行计算,因此是非常有效的. 进一步地,Solinas[6]还将 τ-adic 表示推广到 NAF 表示形式. 考虑将 $\mathbb{Z}[\tau]$ 模 τ^w 剩余类中与 τ 互素的元素作为系数集合 S,则得到的 τ-adic 表示满足 w-NAF 的性质,并且证明每个整数都有唯一的 w-NAFτ-adic 表示. Koblitz[9]提出将 NAFτ-adic 表示用于特征为 3 的超奇异椭圆曲线. 后来文献[10~12]对于 w-NAFτ-adic 表示进行了深入的研究,并对标量乘算法进行了改进. 若选取集合 S 更大,相应地得到的表示中非零项更少,从而需要更少的点加运算. 为了达到最优的性能,通常需要在集合 S 的大小与非零项数之间寻找一个平衡.

另一方面,在某些情况下 $d_k \in S$ 还可以选作一些自同态,从而减少甚至不需要预计算标量乘. 对于某些定义在有限域上的椭圆曲线,在 $\mathbb{Z}[\tau]$ 中存在一些单位根,利用这些单位根生成 τ-adic 表示中的系数集合 S,可以加速标量乘运算并且减少一些预计算. Avanzi 和 Heuberger[13,14]研究了特征为 3 有限域上的超奇异曲线 $E_{3,\mu}: y^2 = x^3 - x - \mu, \mu \in \{\pm 1\}$ 上的标量乘算法. 对单位群 $\left(\frac{\mathbb{Z}[\tau]}{\tau^w\mathbb{Z}[\tau]}\right)^*$ 的结构进行分析得到

$$\left(\frac{\mathbb{Z}[\tau]}{\tau^w\mathbb{Z}[\tau]}\right)^* = \langle\zeta\rangle \times \langle 1+\mu\tau^3\rangle \times \langle -2\rangle \cong (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/3^a\mathbb{Z}) \times (\mathbb{Z}/3^b\mathbb{Z})$$

其中 $\zeta \in \mathbb{Z}[\tau]$ 为六次单位根. 利用 6 次单位根来加速了椭圆曲线标量乘运算,同时减少了存储需求. 文献[15]针对特征为 5 有限域上的椭圆曲线进行了研究,利用 4 次单位根构造的系数集合不需要进行预计算. 文献[16]研究了两类定义在有限域 F_p 上的非超奇异曲线 $E_A: y^2 = x^3 + Ax$(其中 $p \equiv 1 \bmod 4$)和 $E_B: y^2 = x^3 + B$(其中 $p \equiv 1 \bmod 3$)上标量乘算法. 同样考虑 w-NAFτ-adic 表示,利用 4 次和 6 次单位根作为自同态,通过对自同态环 $\mathrm{End}(E)$ 模 τ 剩余类单位群的分解,设计了不需要预计算的标量乘算法.

对于非超奇异椭圆曲线,利用 w-NAFτ-adic 表示计算标量乘已经有比较多的研究. 由于超奇异椭圆曲线的自同态环为非交换环,本文主要考虑一类 j 不变量为 0 的超奇异椭圆曲线自同态环的性质,分析了商环 $\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau]$ 的结构,并对此情况下 w-NAFτ-adic 表示的性质进行研究. $\mathbb{Z}[\sigma,\tau]/\tau\mathbb{Z}[\sigma,\tau]$ 作为系数集合 S 时,证明了 $\mathbb{Z}[\sigma,\tau]$ 中的每个元素都有有限的 S-τ-adic 展开,且对于每个整数所得到的 τ-adic 展开为 2-NAF 表示. 最后讨论了不变量 $j=0$ 超奇异椭圆曲线上的标量乘算法,通过实验对比说明了利用 p-adic 表示,标量乘算法具有最优的效率.

2 基础知识

本节给出一些与本文相关的基础知识,详细内容可以参考文献[17,18].

2.1 超奇异椭圆曲线的定义和性质

设 F_p 为特征为 p 的有限域,$E: y^2 = x^3 + Ax + B$ 为定义在 F_p 上的椭圆曲线,则对于任意定义在 F_p 上的椭圆曲线上都有 Frobenius 自同态 τ 满足

$$\tau(x,y) = (x^p, y^p)$$

由 Hasse 定理[17]可知,设 $t = p + 1 - \#E(F_p)$,则 Frobenius 自同态 τ 满足特征方程 $\tau^2 - t\tau + p = 0$ 且 $|t| \le 2\sqrt{p}$,其中 t 称为 Frobenius 自同态的迹. 自同态 τ 还可以利用特征多项式的根来表示

$$\tau = \frac{t \pm \sqrt{t^2 - 4p}}{2}.$$

对于椭圆曲线 E,曲线的 j 不变量定义为 $j(E)=1728\dfrac{4A^3}{4A^3+27B^2}$. 两条椭圆曲线同构当且仅当其具有相同的 j 不变量.

定义 1　若对于特征 p 有限域上的椭圆曲线 E 有 $E[p]=\mathbb{Z}_p$,则称曲线为正常曲线(ordinary curve);若 $E[p]=\{O\}$,则称曲线为超奇异曲线(supersingular curve).

下面命题给出了一种判定有限域上的椭圆曲线是否为超奇异曲线的简单方法.

定理 1[18]　设 E 为定义在有限域 F_q 上的椭圆曲线,其中 $q=p^n$. 令 $t=q+1-\#E(F_q)$,则椭圆曲线 E 为超奇异曲线当且仅当 $t\equiv 0 \bmod p$.

2.2　自同态环与自同构群的性质

下面考虑两类特殊的椭圆曲线:$E_B:y^2=x^3+B$ 和 $E_A:y^2=x^3+Ax$,其 j 不变量分别为 0 和 1728.

定理 2[17]　设 E 为定义在 F_q 上的椭圆曲线,则其自同构群 $\mathrm{Aut}(E)$ 为有限群且其阶整除 24. 更准确地,

表 1　椭圆曲线自同构群的结构

$\#\mathrm{Aut}(E)$	$j(E)$	$\mathrm{Char}(F_q)$
2	$j(E)\neq 0,1728$	-
4	$j(E)=1728$	$p\neq 2,3$
6	$j(E)=0$	$p\neq 2,3$
12	$j(E)=1728,0$	$p=3$
24	$j(E)=1728,0$	$p=2$

设 $p\neq 2,3$,则对于定义在 F_q 上的椭圆曲线 E,有

$$\mathrm{Aut}(E_A)\cong\mu_4,\mathrm{Aut}(E_B)\cong\mu_6$$

对于其他的椭圆曲线只有平凡的自同构群 $\mathrm{Aut}(E)\cong\mu_2$.

定理 3[18]　设 $A,B\in F_p^*$,则

(1)E_A 是非超奇异曲线当且仅当 $p\equiv 1 \bmod 4$;E_B 是非超奇异曲线当且仅当 $p\equiv 1 \bmod 3$;

(2)E_A 是超奇异曲线当且仅当 $p\equiv 3 \bmod 4$;E_B 是超奇异曲线当且仅当 $p\equiv 2 \bmod 3$.

若 ζ 为 m 阶的自同构,则 ζ 作用在椭圆曲线的点上为

$$\zeta(x,y)=(u^2x,u^3y)$$

其中 $u\in\overline{F}_p$ 为 m 阶元素,$\overline{F}_p$ 为 F_p 的代数闭包.

若 $\phi\in\mathrm{End}(E)$ 的系数属于 F_p,称 ϕ 定义在 F_p 上. 若 $u\in F_p$,则自同构 $\zeta(x,y)=(u^2x,u^3y)$ 定义在有限域 F_p 上当且仅当 $p\equiv 1 \bmod \mathrm{ord}(\zeta)$. 因此 E_A 的 4 阶自同构定义在 F_p 上当且仅当 E_A 为非超奇异曲线. 同样地,E_B 的 3 阶或者 6 阶自同构定义在 F_p 上当且仅当 E_B 为非超奇异曲线. 另外不难看出:当 E_A 和 E_B 为超奇异曲线上,它们的自同构定义在 F_{p^2} 上.

考虑高斯整环 $\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}\}$ 和 Eisenstein 整环 $\mathbb{Z}[w]=\{a+b\sigma\mid a,b\in\mathbb{Z}\}$,其中 $\sigma=(-1+\sqrt{-3})/2$ 是一个三次本原单位根,则 $\mathbb{Z}[i]$ 包含 4 次本原单位根,$\mathbb{Z}[\sigma]$ 包含 6 次本原单位根. 事实上,$\zeta=-\bar{\sigma}=(1+\sqrt{-3})/2$ 是一个六次本原单位根,则 $\mathbb{Z}[\sigma]=\mathbb{Z}[\zeta]$.

定理 4[16] 设 p 为素数且满足 $p\equiv 1 \bmod 4$,$A\in F_p^*$,则曲线 E_A 的自同态环同构于 $\mathbb{Z}[i]$;设 p 为素数且满足 $p\equiv 1 \bmod 3$,$B\in F_p^*$,则曲线 E 的自同态环同构于 $\mathbb{Z}[\zeta]$.

由 4 次和 6 次单位根定义的自同态可以很容易的计算,只需要一个域乘.

(1)对于曲线 E_A:设 u 为 F_p 中的 4 阶元,4 次单位根 i 定义的自同态为

$$i(x,y)=(-x,-uy)$$

(2)对于曲线 E_B:设 u 为 F_p 中的 3 阶元,则 6 次单位根 ζ 及其复共轭 $\bar{\zeta}$ 定义的自同态为

$$\zeta(x,y)=(u^2x,-y),\bar{\zeta}(x,y)=(ux,-y)$$

定义 2[17]　(四元数代数)四元数代数是一个形如 $K=\mathbb{Q}+\mathbb{Q}\alpha+\mathbb{Q}\beta+\mathbb{Q}\alpha\beta$ 的代数,其中乘法满足

$$\alpha^2,\beta^2\in\mathbb{Q},\alpha^2<0,\beta^2<0\text{ 且 }\beta\alpha=-\alpha\beta.$$

定理 5[17,18]　设 E 为定义在域 K 上的椭圆曲线,则自同态环 $\mathrm{End}(E)$ 为 $\mathbb{Z}$,或者虚二次域的序模,或者为四元数代数的序模. 若域 K 的特征为 0,则只有前两种可能性.

E 为超奇异椭圆曲线当且仅当其自同态环为四元数代数的一个序模(order),此时 $\mathrm{End}(E)$ 为非交换环.

3　$\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau]$ 的结构

设 p 为大于等于 5 的素数,本文主要考虑一类定义在 F_p 上的超奇异椭圆曲线 $E_B:y^2=x^3+B$,其中 $p\equiv 2 \bmod 3$,其自同态环是非交换环. 由定理 1 知 $p\mid t$,由 Hasse 定理知 $|t|\leq 2\sqrt{p}$,则可知 $t=0$. τ 作为代数整数,其特征多项式为 x^2+p.

设 $u\in F_{p^2}$ 为 6 阶元,则 6 阶自同构 ζ 和 $\bar{\zeta}$ 分别为:

$$\zeta(x,y)=(u^2x,-y),\bar{\zeta}(x,y)=(u^{2p}x,-y)$$

可以验证:$\tau\zeta(x,y)=(u^{2p}x^p,-y^p)=\bar{\zeta}\tau(x,y)$,故 $\tau\zeta=\bar{\zeta}\tau$.

设 $u\in F_{p^2}$ 为 3 阶元,则 3 阶自同构 σ 和 $\bar{\sigma}$ 分别为:

$$\sigma(x,y)=(u^2x,y),\bar{\sigma}(x,y)=(u^{2p}x,y)=(ux,y).$$

可以验证:$\tau\sigma(x,y)=(ux^p,y^p)=\bar{\sigma}\tau(x,y)$,故 $\tau\sigma=\bar{\sigma}\tau$.

下面来确定四元数代数:首先自同态 σ 满足特征方程 $x^2+x+1=0$,然后考虑同源映射(isogeny)$\phi=[1]-\sigma$,其对偶同源(dual isogeny)为 $\hat{\phi}=[1]-\sigma^2$,则 ϕ 的次数 d 满足 $[d]=\phi\hat{\phi}=(1-\sigma)(1-\sigma^2)=1-\sigma-\sigma^2+1=$

3. ϕ 的次数为 3,ϕ 的迹为 $t=1+\deg(\phi)-\deg(1-\phi)=3$. 可以验证 $(\sigma\phi)^2=[-3]$,所以四元数代数为 $\mathbb{Z}[\alpha,\beta]$,其中 α,β 满足 $\alpha^2=-3,\beta^2=-p$ 和 $\alpha\beta=-\beta\alpha$.

定义自由 $\mathbb{Z}$-模 $\mathbb{Z}[\sigma,\tau]=\{a+b\sigma+c\tau+d\sigma\tau\mid a,b,c,d\in\mathbb{Z}\}$. 令 $\alpha=a_0+a_1\sigma+a_2\tau+a_3\sigma\tau$,其中 $a_0,a_1,a_2,a_3\in\mathbb{Z}$,简写为 $\alpha=(a_0,a_1,a_2,a_3)$,定义 α 的共轭为 $\alpha^*=a_0+a_1\bar{\sigma}-a_2\tau-a_3\sigma\tau$. 定义 α 的范数为

$$N(\alpha)=\alpha\alpha^*=a_0^2+a_1^2+pa_2^2+pa_3^2-a_0a_1-pa_2a_3$$

特别地,$N(\tau)=-\tau^2=p,N(\sigma)=\sigma\bar{\sigma}=1,N(\sigma\tau)=p$. 容易验证:$(\alpha\beta)^*=\beta^*\alpha^*$. 若 α 为 $\mathbb{Z}[\sigma,\tau]$ 中的可逆元,则 $\alpha^{-1}=\alpha^*/N(\alpha)$,则 $\mathbb{Z}[\sigma,\tau]$ 中的可逆元是范数为 1 的元素.

为了在 $\mathbb{Z}[\sigma,\tau]$ 中构造系数集合,必须对每个模 τ^w 剩余类选择一个代表元,其中 $w\in\mathbb{N}$ 且 $w\geq1$. 本节研究商环 $\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau]$ 的结构,首先给出 $\mathbb{Z}[\sigma,\tau]$ 中元素被 τ 整除的条件.

定义 3 设 $\alpha,\beta\in\mathbb{Z}[\sigma,\tau]$,如果存在 r_1 使得 $\alpha=r_1\beta$,记作 $\beta\mid_R\alpha$,则称 β 右整除 α;如果存在 r_2 使得 $\alpha=\beta r_2$,记作 $\beta\mid_L\alpha$,则称 β 左整除 α.

由于 $\mathbb{Z}[\sigma,\tau]$ 中乘法非交换,则上述定义中 r_1 和 r_2 通常不相等.

定理 6 设 $\alpha=(a_0,a_1,a_2,a_3)\in\mathbb{Z}[\sigma,\tau]$,则 $\tau\mid_R\alpha$ 当且仅当 $p\mid a_0$ 且 $p\mid a_1$;类似地,$\tau\mid_L\alpha$ 当且仅当 $p\mid a_0$ 且 $p\mid a_1$.

证明 若 $\tau\mid_R\alpha$,则存在 $\beta=(b_0,b_1,b_2,b_3)$,使得 $\alpha=\beta\tau$,即

$$\alpha=b_0\tau+b_1\sigma\tau+b_2\tau^2+b_3\sigma\tau^2$$

又由于 $\tau^2=-p$,则

$$\alpha=b_0\tau+b_1\sigma\tau-b_2p-b_3p\sigma=(-b_2p,-b_3p,b_0,b_1)$$

故 $p\mid a_0$ 且 $p\mid a_1$. 反过来,若 $p\mid a_0$ 且 $p\mid a_1$,则存在 b_0,b_1 使得 $a_0=b_0p,a_1=b_1p$. $\alpha=(a_0,a_1,a_2,a_3)=b_0p+b_1p\sigma+a_2\tau+a_3\sigma\tau$. 同样地,由于 $\tau^2=-p$,则

$$\alpha=(-b_0\tau-b_1\sigma\tau+a_2+a_3\sigma)\tau$$

故 $\tau\mid_R\alpha$. 对于 $\tau\mid_L\alpha$ 的情况可以类似地证明.

所以 $\tau\mid_R\alpha$ 当且仅当 $\tau\mid_L\alpha,\tau$ 生成的左理想与右理想相同.

定理 7 $\dfrac{\mathbb{Z}[\sigma,\tau]}{\tau\mathbb{Z}[\sigma,\tau]}\cong\dfrac{\mathbb{Z}[\sigma]}{p\mathbb{Z}[\sigma]}$.

证明 定义环同态

$$\phi:\mathbb{Z}[\sigma,\tau]\to\mathbb{Z}[\sigma]/p\mathbb{Z}[\sigma]$$
$$(a_0,a_1,a_2,a_3)\mapsto\bar{a}_0+\bar{a}_1\sigma$$

其中 $\bar{a}_0\equiv a_0 \bmod p,\bar{a}_1\equiv a_1 \bmod p$ 且 $0\leq\bar{a}_0,\bar{a}_1<p$. 明显地,$\phi$ 为满射. 另一方面,由于 $(a_0,a_1,a_2,a_3)\in\mathrm{Ker}\phi$ 当且仅当 $a_0\equiv0 \bmod p,a_1\equiv0 \bmod p$,即为 (a_0,a_1,a_2,a_3) 被 τ 整除. 故由同态基本定理得证.

为了证明下面推论 1,需要用到代数数论中有关理想分解的结论(定理 8),详细内容可以参考文献[19].

定理 8[19] 设 $K=\mathbb{Q}(\sqrt{d})$,p 为素数. 若 $p\geq3$,并且 $p\mid d(K)$,则当 $\left(\dfrac{d}{p}\right)=1$ 时,$pO_K=p_1p_2,p_1\neq p_2,N(p_1)=N(p_2)=p$,即 p 在 K 中完全分裂;而当 $\left(\dfrac{d}{p}\right)=-1$ 时,$pO_K=p,N(p)=p^2$,即 p 在 K 中惯性,其中 $\left(\dfrac{d}{p}\right)$ 表示 Legendre 符号.

推论 1 $\dfrac{\mathbb{Z}[\sigma,\tau]}{\tau\mathbb{Z}[\sigma,\tau]}\cong F_{p^2}$.

证明 由定理 7,只需考虑 $\dfrac{\mathbb{Z}[\sigma]}{p\mathbb{Z}[\sigma]}$. 令 $K=Q(\sqrt{-3})$,则域 K 的代数整数环为 $O_K=\mathbb{Z}\left[\dfrac{1}{2}(1+\sqrt{-3})\right]=\mathbb{Z}[\sigma]$,域 K 的判别式 $d(K)=-3$. 由于 $p\equiv2 \bmod 3$,则 $p\mid d(K)$. 下面说明 $\left(\dfrac{-3}{p}\right)=-1$.

由二次互反律[20],即 $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$,则 $\left(\dfrac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\dfrac{p}{3}\right)$. 由二次剩余的定义知:由于 $p\equiv2 \bmod 3$,则 $\left(\dfrac{p}{3}\right)=\left(\dfrac{2}{3}\right)=-1$. 故

$$\left(\frac{-3}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}}\cdot(-1)=-1.$$

则由定理 8 知:p 在 $\mathbb{Z}[\sigma]$ 中仍是素的,则 $\langle p\rangle$ 为素理想,$\mathbb{Z}[\sigma]/\langle p\rangle$ 为特征为 p 的有限域且 $N(p)=p^2$,故 $\mathbb{Z}[\sigma,\tau]/\langle p\rangle\cong F_{p^2}$.

当 $w\geq2$ 时,商环 $\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau]$ 没有很简单的结构,例如 $w=2$ 时,$\dfrac{\mathbb{Z}[\sigma,\tau]}{\tau^2\mathbb{Z}[\sigma,\tau]}=\dfrac{\mathbb{Z}[\sigma,\tau]}{p\mathbb{Z}[\sigma,\tau]}$. 然而由第 4 节定理 11 知,考虑在环 $\mathbb{Z}[\sigma,\tau]/\tau\mathbb{Z}[\sigma,\tau]$ 中选择系数集合与在环 $\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau]$ 中选择系数集合,每个整数所得到的 S-τ-adic 展开是相同的,所以这里不需要再研究 $w\geq2$ 的情况.

4 $\mathbb{Z}[\sigma,\tau]$ 中元素的 τ-adic 表示

定义 4(τ-adic 表示) 元素 $\eta\in\mathbb{Z}[\sigma,\tau]$ 的右 τ-adic 表示为 $\eta=\sum_{k=0}^{l-1}d_k\tau^k$,其中 d_j 属于适当的系数集合 $S\subseteq\mathbb{Z}[\sigma,\tau]$. 类似地,元素 $\eta\in\mathbb{Z}[\sigma,\tau]$ 的左 τ-adic 表示为 $\eta=\sum_{k=0}^{l-1}\tau^kd_k$,其中 d_k 属于适当的系数集合 $S\subseteq\mathbb{Z}[\sigma,\tau]$.

由于左 τ-adic 表示与右 τ-adic 表示的相似性,下文的证明中主要针对右 τ-adic 表示的情况进行说明.

定义 5(w-NAFτ-adic 表示) 令 $w\in\mathbb{N},w\geq1$,系数

集合为 $S\subseteq\mathbb{Z}[\sigma,\tau]$. 元素 $\eta\in\mathbb{Z}[\sigma,\tau]$ 的右 w-NAFτ-adic 表示为 $\eta=\sum_{k=0}^{l-1}d_k\tau^k, d_k\in S$,满足:对于任意 w 个连续数字中至多有一个非零.

下面给出了计算右 w-NAFτ-adic 表示的算法.

算法 1　计算 $\eta\in\mathbb{Z}[\sigma,\tau]$ 的右 w-NAFτ-adic 表示

输入:$\eta\in\mathbb{Z}[\sigma,\tau]$,系数集合 S,基 τ

输出:$\eta=\sum_{k=0}^{l-1}d_k\tau^k, d_k\in S$

1. $z\leftarrow\eta$
2. $l\leftarrow0$
3. while $z\neq0$ do
4. if $z\equiv0\bmod\tau$ then
5. $d_l\leftarrow0$
6. else
7. 选择 $d_l\in S$ 使得 $d_l\equiv z\bmod\tau^w$
8. end if
9. 设 α 满足 $z-d_l=\alpha\tau$
10. $z\leftarrow\alpha$
11. $l\leftarrow l+1$
12. end while
13. return$(d_0,\cdots,d_l)$

为了得到左 w-NAFτ-adic 表示,只需将算法 1 中 step 9 改为 $z-d_l=\tau\alpha$.

令 $(\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau])^*$ 为商环 $\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau]$ 的单位群,通常利用 $(\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau])^*\cup\{0\}$ 作为 w-NAFτ-adic 表示中系数集合 S. 在第 3 节中已经对商环 $\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau]$ 的结构进行了研究,为了便于描述,下文中主要针对 $w=1$ 的情况进行说明. 由上面推论 1 知,S 可选择为 $\frac{\mathbb{Z}[\sigma,\tau]}{\tau\mathbb{Z}[\sigma,\tau]}$,即

$$S=\{(a,b)\in\mathbb{Z}\times\mathbb{Z}\mid0\leq a,b<p\}.$$

进一步,为了得到对称的系数集合,可以利用一个更方便的表示方法

$$S=D\times D$$

其中 $D=\{a\in\mathbb{Z}\mid-(p-1)/2\leq a\leq(p-1)/2\}$.

通常并不能保证对于每个 $\eta\in\mathbb{Z}[\sigma,\tau]$ 都有有限的展开,与系数集合有很大的关系. 定理 10 给出了判断系数集合 S 是否可以得到一个有限展开的条件. 为了证明定理 10,需要用到文献[16]中的结论,即定理 9.

定理 9[16]　设 $D_w\subseteq\mathbb{Z}[\tau]$ 为 w-NAFτ-adic 展开的系数集合,其中 $w\geq1$ 为整数. 令 $d_{\max}=\max\{N(d)\mid d\in D_w\}$,则 $\mathbb{Z}[\tau]$ 中的每个元素都有有限的 D_w-τ-adic 展开当且仅当对于每个满足 $N(z)\leq\frac{d_{\max}}{(|\tau^w|-1)^2}$ 的 $z\in\mathbb{Z}[\tau]$ 都有有限的 D_w-τ-adic 展开.

定理 10　利用 $\frac{\mathbb{Z}[\sigma,\tau]}{\tau\mathbb{Z}[\sigma,\tau]}$ 作为系数集合 S,$\mathbb{Z}[\sigma,\tau]$ 中的每个元素都有有限的右 S-τ-adic 展开.

证明　设 $\eta=A+\sigma B\in\mathbb{Z}[\sigma,\tau]$,其中 $A,B\in\mathbb{Z}[\tau]$,则 η 有有限的 S-τ-adic 展开当且仅当 A 和 B 在 $\mathbb{Z}[\tau]$ 中都有有限的 D-τ-adic 展开.

当 $w=1$ 时,D_1 可以选作 $D=\{a\in\mathbb{Z}\mid-(p-1)/2\leq a\leq(p-1)/2\}$. 将定理 9 应用到 D,则 $d_{\max}=(p-1)^2/4$.

$$\frac{d_{\max}}{(|\tau|-1)^2}=\frac{(p-1)^2}{4\cdot(\sqrt{p}-1)^2}=\frac{(\sqrt{p}+1)^2}{4}$$

若 $p\geq5$,则 $\sqrt{p}<\frac{p}{2}$,从而

$$(\sqrt{p}+1)^2=p+2\sqrt{p}+1<2p+1$$

现在需要考察:若 $z=z_0+z_1\tau\in\mathbb{Z}[\tau]$ 满足 $N(z)<(2p+1)/4$,是否 z 具有有限的 D-τ-adic 展开. 若 $z_1\neq0$,则 $N(z)=z_0^2+pz_1^2\geq p$,又由于 $(2p+1)/4<p$,则 $N(z)>(2p+1)/4$,与 z 满足 $N(z)<(2p+1)/4$ 矛盾. 故可假设 $z=z_0\in\mathbb{Z}$ 且 $z_0^2<(2p+1)/4$. 由于 $p\geq5$,则 $4p<p^2$,进一步有 $(2p+1)/4<(p-1)^2/4=d_{\max}$,从而有 $z_0^2<d_{\max}$,则 $z_0\in D$,即 z_0 的 D-τ-adic 展开长度为 1. 所以对于每个 $z=z_0+z_1\tau\in\mathbb{Z}[\tau]$ 满足 $N(z)<(2p+1)/4$,z 都有有限的 D-τ-adic 展开,利用定理 9 的结论可知 $\mathbb{Z}[\tau]$ 中的每个元素都有有限的 D-τ-adic 展开. 故定理成立.

定理 11　利用 $\frac{\mathbb{Z}[\sigma,\tau]}{\tau\mathbb{Z}[\sigma,\tau]}$ 作为系数集合 S,对于每个整数所得到的 S-τ-adic 展开为 2-NAF 表示.

证明　整数 $n\in\mathbb{Z}$ 作为算法 1 的输入,按照算法 1 的描述 z 的初始值为整数 n. 假设在第 i 轮循环中首次出现 $z\neq0 \bmod\tau$ 的情况,则选择 $d_i\in S$ 使得 $d_i\equiv z \bmod\tau$. 而此时必有 $z\in\mathbb{Z}[\tau]$ 且 $d_i\in\mathbb{Z}[\sigma]$,则必定有 $z,d_i\in\mathbb{Z}$ 且 $z-d_i\equiv0 \bmod p$,即存在 $m\in\mathbb{Z}$ 使得 $z-d_i=mp=-m\tau^2$. 在算法 1 第 $i+1$ 轮循环中得到的 α 满足 $z-d_i=\alpha\tau$,则必定有 $\tau\mid\alpha$,故 d_{i+1} 必定为 0. 则在 $i+1$ 轮循环最后得到的 α' 满足 $z-d_i=\alpha'\tau^2$,即 $\alpha'=-m$ 仍然是一个整数. 则上述过程会依次进行下去,直到循环结束.

5　不变量 $j=0$ 超奇异椭圆曲线的标量乘算法

一般地,对于任意 $\eta\in\mathbb{Z}[\sigma,\tau]$,假设 η 存在右 τ-adic 展开

$$\eta=\sum_{k=0}^{l-1}(a_k,b_k)\tau^k=\sum_{k=0}^{l-1}a_k\tau^k+\sum_{k=0}^{l-1}b_k\sigma\tau^k,$$

其中 $(a_i,b_i)\in S$,σ 的具体计算形式在第 3 节已经给出. 令 $A=\sum_{k=0}^{l-1}a_k\tau^k$ 和 $B=\sum_{k=0}^{l-1}b_k\tau^k$,则 $\eta=A+\sigma B$,其中 $A,B\in\mathbb{Z}[\tau]$.

计算 ηP

$$\eta P = \left(\sum_{k=0}^{l-1} a_k \tau^k\right) P + \sigma\left(\sum_{k=0}^{l-1} b_k \tau^k\right) P$$

若直接进行计算,需要运用两次 τ-and-add 算法计算 $\left(\sum_{k=0}^{l-1} a_k \tau^k\right) P$ 和 $\left(\sum_{k=0}^{l-1} b_k \tau^k\right) P$,标量乘 ηP 总的计算开销为:

(1)计算 $A \cdot P$ 需要 $\mathrm{HW}_\tau(A) - 1$ 个点加与 $l-1$ 个 τ 运算;

(2)计算 $B \cdot P$ 需要 $\mathrm{HW}_\tau(B) - 1$ 个点加与 $l-1$ 个 τ 运算;

(3)计算同态 σ 与一个点加运算.

自同态 τ 和 σ 都可以有效地计算:计算 τ 在正规基表示下只需要两个循环移位,而计算 σ 只需要一个域乘. 若忽略它们在标量乘计算法中的开销,标量乘总的计算开销为 $\mathrm{HW}_\tau(A) + \mathrm{HW}_\tau(B) - 1$ 个点加运算.

此时还可以考虑预计算 $Q = \sigma(P)$ 和 $\{aP + bQ \mid 0 \le a, b < p\}$,然后利用同时多标量乘的技巧进行计算. 进一步地,利用椭圆曲线上点的加法与点的减法的相似性和集合的对称性,可以减少预计算量,即预计算

$$\{aP + bQ \mid |a| \le (p-1)/2, 0 \le b \le (p-1)/2\}$$

5.1 标量乘算法

通常在椭圆曲线密码算法中标量为整数. 由定理 11 的证明可知:对于整数 n,其 S-τ-adic 展开表示的系数全为整数. 事实上,此时整数 n 的 S-τ-adic 表示就是 p-adic 展开

$$n = \sum_{k=0}^{l-1} d_k p^k$$

其中 $0 \le d_i < p$. 此时算法 1 可以简化为算法 2.

算法 2 计算 $n \in \mathbb{Z}$ 的右 NAF τ-adic 展开

输入:$n \in \mathbb{Z}$,系数集合 S

输出:$n = \sum_{k=0}^{l-1} d_k p^k, d_k \in S$

1. $z \leftarrow n$
2. $l \leftarrow 0$
3. while $z \neq 0$ do
4. 选择 $d_l \in S$ 使得 $d_l \equiv z \bmod p$
5. $z \leftarrow z - d_l$
6. $z \leftarrow z/p, l \leftarrow l + 1$
7. end while
8. return$(d_0, \cdots, d_l)$

另外由于 $\tau^2 = -p$,则点 pP 可以通过计算两次 Frobenius 自同态 τ 得到.

计算标量乘 nP

$$nP = \left(\sum_{k=0}^{l-1} d_k (-1)^k \tau^{2k}\right) P = \sum_{k=0}^{l-1} (-1)^k \tau^{2k} d_k P$$

在预计算 $\{dP \mid 2 \le d < p\}$ 情况下,计算标量乘 nP 只需要 $\mathrm{HW}_\tau(n) - 1$ 个点加运算和一些 τ 运算.

5.2 效率比较

本节以定义在特征 5 有限域上超奇异椭圆曲线为例,选取 NAF、4-NAF、{2,3} 双基链和 {2,5} 双基链四种椭圆曲线标量乘算法作为对比. 利用 Magma 软件[21]实现基于 NAF、4-NAF、{2,3} 双基链、{2,5} 双基链与 p-adic 方法标量乘算法,并比较它们的效率. 为了避免求逆运算,实验选择使用 Jacobian 坐标. 表 2 给出了在 Jacobian 坐标下椭圆曲线点运算的计算开销,其中包括二倍点(DBL)、点加(ADD)、三倍点(TPL)和五倍点(QPL),具体的计算公式可以参考文献[22,23]. M 和 S 分别表示域上乘法与平方,忽略域上的加法和减法计算开销,通常假设 1S = 0.8M.

表 2 Jacobian 坐标下各种点运算的计算开销

点运算	域运算个数	计算开销	参考文献
DBL	1M + 8S	7.4M	文献[22]
ADD	11M + 5S	15M	文献[22]
TPL	5M + 10S	13M	文献[22]
QPL	15M + 10S	23M	文献[23]

对于上述每个算法,分别随机生成 10000 个 160 比特和 256 比特的随机数. 然后将每个随机数分别转化为相应的表示形式,并计算每种表示方法下的平均非零项数和计算开销. 表 3 和表 4 分别针对 160 比特标量乘和 256 比特标量乘给出了具体的实验结果,其中 NAF、{2,3}-双基数链和 {2,5}-双基数链方法不需要预计算,4-NAF 和 p-adic 方法需要 3 个预计算. 另外,表 3 和表 4 还针对两种双基数链方法给出了最优的参数选择,其中 B, T, E 分别表示双基数链表示中首项中双基的次数. 实验结果表明:对于 160 比特标量乘,p-adic 方法的效率比 NAF 方法提高了 140.1%,比 4-NAF 方法提高了 100.8%,比 {2,3}-双基数链方法提高 111.5%,比 {2,5}-双基数链方法提高了 131.5%;对于 160 比特标量乘,p-adic 方法的效率比其他方法分别提高了 139.9%、100.8%、111.8% 和 132.2%.

表 3 各标量乘算法下的计算开销(160bit)

算法	预计算	B	T/E	项数	计算开销
NAF[1]	0	–	–	53.8	1987.3M
4-NAF[2]	3	–	–	32.4	1662.0M
{2,3}-双基数链[3]	0	87	47	35.6	1751.1M
{2,5}-双基数链[23]	0	111	22	42.2	1916.2M
p-adic	3	–	–	55.1	827.6M

表 4　各标量乘算法下的计算开销(256bit)

算法	预计算	B	T/E	项数	计算开销
NAF[1]	0	–	–	85.7	3177.8M
4-NAF[2]	3	–	–	51.6	2660.5M
{2,3}-双基数链[3]	0	140	74	56.3	2806.1M
{2,5}-双基数链[23]	0	172	37	66.4	3075.9M
p-adic	3	–	–	88.3	1324.5M

6　结论

本文主要针对定义在有限域 F_p 上一类特殊的超奇异椭圆曲线 $E_B: y^2 = x^3 + B$(其中 $p \equiv 2 \bmod 3$)进行了研究,其特殊性在于自同态环为非交换环. 确定曲线所对应的四元数代数,对商环 $\mathbb{Z}[\sigma,\tau]/\tau^w\mathbb{Z}[\sigma,\tau]$ 的结构进行了分析,研究了此类曲线的 τ-adic 表示性质. 理论上证明了整数 n 的 S-τ-adic 表示本质上是 p-adic 表示,从而利用 Frobenius 自同态可以提高曲线上标量乘的效率. 相比已有的方法,p-adic 表示方法提高标量乘效率 100% 以上. 由于曲线 $E_A: y^2 = x^3 + Ax$(其中 $p \equiv 3 \bmod 4$)与曲线 E_B 的自同态环具有类似的性质,本文的结论可以类似地推广到曲线 E_A.

参考文献

[1] Joye M, Yen S M. Optimal left-to-right binary signed-digit recoding[J]. IEEE Transactions on Computers, 2000, 49(7):740 – 748.

[2] Muir J A, Stinson D R. Minimality and other properties of the width-w nonadjacent form[J]. Mathematics of computation, 2005, 75(253):369 – 384.

[3] Dimitrov V, Imbert L, Mishra P K. Efficient and secure elliptic curve point multiplication using double-base chains [A]. ASIACRYPT 2005 [C]. Chennai, India: Springer, 2005. 59 – 78.

[4] Hisil H, Wong K, Carter G, Dawson E. Jacobi quartic curves Revisited[A]. ACISP 2009[C]. Brisbane, Australia: Springer, 2009. 452 – 468.

[5] Bernstein D J, Lange T. Faster addition and doubling on elliptic curves[A]. ASIACRYPT 2007[C]. Kuching, Malaysia: Springer, 2007. 29 – 50.

[6] Solinas J A. Efficient arithmetic on Koblitz curves[J]. Design, Codes and Cryptography, 2000, 19(2):125 – 179.

[7] Gallant R, Lambert R, Vanstone S A. Faster point multiplication on elliptic curves with efficient endomorphisms[A]. CRYPTO 2001 [C]. Santa Barbara, California, USA: Springer, 2001. 190 – 200.

[8] Galbraith S, Lin X, Scott M. Endomorphisms for faster elliptic curve cryptography on a large class of curves[A]. EUROCRYPT 2009 [C]. Cologne, Germany: Springer, 2009. 518 – 635.

[9] Koblitz N. An elliptic curve implementation of the finite field digital signature algorithm[A]. CRYPTO 1998[C]. Santa Barbara, California, USA: Springer, 1998. 327 – 337.

[10] Blake I F, Murty V K, Xu G. Efficient algorithms for Koblitz curves over fields of characteristic three[J]. Journal of Discrete Algorithms, 2005, 3(1):113 – 124.

[11] Avanzi R M, Heuberger C, Prodinger H. Redundant τ-adic expansions I: Non-adjacentdigit sets and their applications to scalar multiplication[J]. Designs, Codes and Cryptography, 2011, 58(2):173 – 202.

[12] Heuberger C. Redundant τ-adic expansions II: Non-optimality and chaotic behavior[J]. Mathematics in Computer Science, 2010, 3(2):141 – 157.

[13] Avanzi R M, Heuberger C, Prodinger H. Arithmetic of Supersingular Koblitz Curves in Characteristic Three[OL]. https://eprint.iacr.org/2010/436.pdf, 2016-07-29.

[14] Avanzi R, Heuberger C. Faster and lower memory scalar multiplication on supersingular curves in characteristic three[A]. PKC 2011 [C]. Taormina, Italy: Springer, 2011. 109 – 127.

[15] Kleinrahm A. Arithmetic of subfield elliptic curves in small characteristic [D]. Bochum, Germany: Ruhr-Universitat Bochum, 2011.

[16] Heuberger C, Mazzoli M. Symmetric digit sets for elliptic curve scalar multiplication without precomputation[J]. Theoretical Computer Science, 2014, 547(1):18 – 33.

[17] Silverman J H. The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics)[M]. 2 Ed. New York: Springer, 2009.

[18] Washington L C. Elliptic Curves: Number Theory and Cryptography [M]. New York: Chapman & Hall/CRC, 2008.

[19] Murty M R, Esmonde J. Problems in Algebraic Number Theory (Graduate Texts in Mathematics 190)[M]. 2 Ed. New York: Springer, 2005.

[20] Ireland K, Rosen M. A classical introduction to modern number theory (Graduate Texts in Mathematics 84) [M]. New York: Springer, 1990.

[21] The Magma Development Team. MAGMA Computational Algebra System[EB/OL]. http://magma.maths.usyd.edu.au/magma, 2016-06-18.

[22] Bernstein D J, Lange T. Explicit-formulas database[EB/OL]. http://hyperelliptic.org/EFD, 2016-06-18.

[23] Mishra P K, Dimitrov V. Efficient quintuple formulas for elliptic curves and efficient scalar multiplication using multibase number representation [A]. ISC 2007 [C]. Valparaíso, Chile: Springer, 2007. 390 – 406.

作者简介

翁 江 男,1986 年 3 月出生,陕西西安人. 现为空军工程大学信息与导航学院讲师,主要研究方向为网络密码和椭圆曲线密码.
E-mail:wengjiang858@163.com

康晓春 女,1989 年 4 月出生,河南商丘人. 现为中国传媒大学硕士研究生. 主要从事信息安全方面的研究.
E-mail:kangxiaochun0585@khtsc.com.cn

豆允旗 男,1987 年 8 月出生,河南商丘人. 2017 年毕业于信息工程大学,获得博士学位. 研究方向为椭圆曲线密码学.
E-mail:douyunqi@126.com

马传贵(通讯作者) 男,1962 年 4 月出生,山东菏泽人,博士,教授. 主要研究方向为密码学和无线网络安全.
E-mail:cgm20090501@163.com