arXiv:2303.00346v1 [math.NT] 1 Mar 2023

使用 Charlap-Coley-Robbins 多项式计算同源

FRANC.OIS MORAIN

Abstract. SEA 算法用于计算许多特征下有限域上椭圆曲线的阶，并使用模多项式。这些多项式有不同的形式，计算方法也得到了蓬勃发展。一旦获得了关于素数 ℓ 的一些模多项式，就可以使用代数公式计算一条曲线 $\mathcal{E}^*/\mathbb{F}_q$，使其与所研究的曲线 ℓ-同源 $\mathcal{E}$。这些公式涉及模多项式的导数，而导数有时可能会消失。为克服这一问题，可以使用 Charlap、Coley 和 Robbins 引入的其他三元多项式 U_ℓ、V_ℓ 和 W_ℓ，以解决 Elkies 方法最初版本中的一些困难。我们给出这些多项式的性质，以及由 Atkin 概述的用于计算同源曲线的公式。此外，我们还研究了 Atkin 提出的另一种建议，即使用与 Dedekind η 函数的幂乘积相关联的模多项式。

1. 引言

计算同源是 Schoof-Elkies-Atkin（SEA）算法的核心环节，该算法用于计算大特征有限域上椭圆曲线的基数 [20, 2, 10]，此外还用于 [4]。近年来，它还应用于后量子密码学 [8, 13, 6, 12] 等领域，以及密码系统 [9, 19, 11]。

给定一条曲线 $\mathcal{E}/\mathbb{F}_q$，我们需要从 $X = j(\mathcal{E})$ 中某个 $\ell+1$ 次模多项式$\Psi_\ell(X,Y)$ 的一个根出发，计算对应于（较小）素数 ℓ 的 ℓ-同源曲线。通过 $\Psi_\ell(X,Y)$ 的偏导数，可以计算出同源曲线 $\mathcal{E}^*/\mathbb{F}_q$ 以及该同源的核多项式的系数。除非其中一个导数为零，否则该方法均有效。这既是理论问题，也是实际问题。对此的一种替代方法是采用 Elkies 的原始方法 [10], ，即使用关于 A^* 和 B^*的代数关系。另一种选择是使用 [7], 中引入的 CCR 多项式（U_ℓ, V_ℓ, W_ℓ），代价是需要求解三个 $\ell+1$ 次多项式的根，而不是一个。[15] 中给出了计算这些多项式以及 A^* 和 B^* 的有理表示的若干方法（本文引用的参考文献中也有相关内容）。

Date: 2023年3月2日。作者目前休假，来自 D´el´egation G´en´erale pourl'Armement。1

我们的工作（与 [15] 密切相关）旨在按照 Atkin 的思路，并遵循 [2] 中的建议，利用 U_ℓ的偏导数，为 Elkies 算法给出计算必要参数的公式。当 $\ell \equiv 11$ 模 12 时，我们也对 Atkin 提出的替代多项式 U^a 进行了相同的工作。

内容如下。我们在第 2 节回顾 SEA 算法，包括埃森斯坦级数的公式，并在第 3 节介绍 CCR 多项式。第 4 节是本文的核心部分，将推导给出同源曲线系数的公式。

2. Schoof/Elkies/Atkin

2.1. 预备知识。

2.1.1. 除法多项式。对于 $\mathcal{E}$： $y^2 = x^3 + Ax + B$，点（X， Y）在 $\mathcal{E}$ 上乘以正整数 n 后可表示为

$$[n](X,Y) = \left(\frac{\phi_n(X,Y)}{\psi_n(X,Y)^2}, \frac{\omega_n(X,Y)}{\psi_n(X,Y)^3}\right)$$

其中多项式满足

$$\phi_n = X\psi_n^2 - \psi_{n+1}\psi_{n-1}, \quad 4Y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$$

并且 ϕ_n、 ψ_{2n+1}、 $\psi_{2n}/(2Y)$ ω_{2n+1}/Y、 ω_{2n} 属于 $\mathbb{Z}[A,B,X]$。通常使用下式对其进行简化

$$f_n(X) = \begin{cases} \psi_n(X,Y) & \text{for } n \text{ odd} \\ \psi_n(X,Y)/(2Y) & \text{for } n \text{ even} \end{cases}$$

其前几项为

$$f_{-1} = -1, \quad f_0 = 0, \quad f_1 = 1, \quad f_2 = 1,$$
$$f_3(X,Y) = 3X^4 + 6AX^2 + 12BX - A^2$$
$$f_4(X,Y) = X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3.$$

f_n的次数在 n 为奇数时是 $(n^2-1)/2$，在 n 为偶数时是 $(n^2-4)/2$。若 X 的权为 1， A 的权为 2， B 的权为 3，则 f_n 中的所有单项式都具有相同的加权次数，等于 f_n的次数。

2.1.2. 模函数及相关内容。令 $q = \exp(2i\pi\tau)$，定义

$$E_2(q) = 1 - 24\sum_{n=1}^{\infty}\delta_1(n)q^n,$$
$$E_4(q) = 1 + 240\sum_{n=1}^{\infty}\delta_3(n)q^n,$$
$$E_6(q) = 1 - 504\sum_{n=1}^{\infty}\delta_5(n)q^n,$$

其中 $\delta_r(n)$表示 n的因子的 r次幂之和。级数 E_4 和 E_6 分别是权 4 和权 6 的模形式。

函数 E_2不是模形式，但请注意， $\mathcal{F}_n(\tau) = E_2(\tau) - nE_2(n\tau)$是 $\Gamma_0(n)$的一个权 2 模形式，且具有平凡乘子（参见 [18] 和[3]）。

当 $F(q) = \sum_{n\geq n_0} a_n q^n$ 时，我们引入算子

$$F'(q) = \frac{1}{2i\pi}\frac{dF}{d\tau} = q\frac{dF}{dq} = \sum_{n\geq n_0} n a_n q^n. \tag{1}$$

以下几个恒等式是经典结果：

$$\Delta = \frac{E_4^3 - E_6^2}{1728}, \quad j = \frac{E_4^3}{\Delta}, \quad j - 1728 = \frac{E_6^2}{\Delta}, \tag{2}$$

$$\frac{j'}{j} = -\frac{E_6}{E_4}, \quad \frac{j'}{j-1728} = -\frac{E_4^2}{E_6}, \quad j' = -\frac{E_4^2 E_6}{\Delta}, \quad \frac{\Delta'}{\Delta} = E_2, \tag{3}$$

此外，我们还引入拉马努金微分系统：

$$3{E_4}' = E_4E_2 - E_6, \quad 2{E_6}' = E_6E_2 - E_4^2, \quad 12{E_2}' = E_2^2 - E_4. \tag{4}$$

2.2. Schoof 的方法。设 $\mathcal{E}/\mathbb{F}_q$ 是一条基数为 $m = p+1-t$ 的椭圆曲线，根据哈斯定理，$|t| \leq 2\sqrt{q}$。Schoof 提出了首个确定性多项式时间算法来计算 m。其思路是利用弗罗贝尼乌斯在 $\mathcal{E}$ 的 ℓ-除点上的作用，通过模 (f_ℓ, ℓ) 的特征方程 $\phi^2 - [t]\phi + [q] = 0$ 求出 t 。

2.3. 使用同源。Elkies 和 Atkin 随后提出改进，使 Schoof 算法更高效（且具有概率性），并能在实践中使用。Elkies 介绍了如何利用同源，在有限域上求出 $f_\ell(X)$ 的小次数因子，前提是弗罗贝尼乌斯方程模 ℓ 分裂。借助模多项式，Elkies 推导出一套流程，可计算构造从 $\mathcal{E}: Y^2 = X^3 + AX + B$ 到某条曲线 $\mathcal{E}^*: Y^2 = X^3 + A^*X + B^*$ 的次数为 ℓ 的同源所需的所有参数，以及该同源的核多项式，从而得到我们需要的因子。Atkin 则设计了另一种实现同一目标的方法，重点在于使用更多关于 $X_0(\ell)$ 及其商的模方程。

（重新归一化后）可得：

$$A = -3E_4(q), B = -2E_6(q).$$

采用相容的缩放后，我们得到

$$A^* = -3\ell^4 E_4(q^\ell), \quad B^* = -2\ell^6 E_6(q^\ell).$$

更重要的是，令 σ_r 表示 U_ℓ 的根的幂和，则有

$$\sigma_1 = \frac{\ell}{2}(\ell E_2(q^\ell) - E_2(q)) = -\frac{\ell}{2}\mathcal{F}_\ell(q).$$

此外，Elkies 证明了

$$A - A^* = 5(6\sigma_2 + 2A\sigma_0),$$
$$B - B^* = 7(10\sigma_3 + 6A\sigma_1 + 4B\sigma_0),$$

再加上其他 σ_k 对 $k>3$ 满足的递推关系。因此，由于 σ_2 和 σ_3 属于 $\mathbb{Q}[\sigma_1,A,B]$， A^* 和 B^* 也属于 $\mathbb{Q}[\sigma_1,A,B]$。

给定这些量，有几种算法可以求出同源。关于这一点，请参见 [5] 。

3. The polynomials of Charlap-Coley-Robbins

3.1. 理论。我们从椭圆曲线 $\mathcal{E}$： $Y^2=X^3+AX+B$ 出发，并固定一个奇素数 ℓ，令 $d=(\ell-1)/2$。我们的目标是求出一条 ℓ-同源曲线 $\mathcal{E}^*$ 的方程：$Y^2=X^3+A^*X+B^*$。

定理 3.1。存在三个多项式 U_ℓ、 V_ℓ、 W_ℓ，它们属于 $\mathbb{Z}[X,Y,Z,1/\ell]$，且在 X 中的次数为 $\ell+1$，使得 $U_\ell(\sigma_1,A,B)=0$，并且 $V_\ell(A^*,A,B)=0$、$W_\ell(B^*,A,B)=0$。

现在让我们来关注这些多项式的性质。

定理 3.2. 当 $\ell>3$ 时，多项式 U_ℓ、 V_ℓ、 W_ℓ 属于 $\mathbb{Z}[X,Y,Z]$。

命题 3.3. 分别赋予 X、 Y、 Z 权重 1、2、3，则 U_ℓ、 V_ℓ 和 W_ℓ 中的单项式具有广义次数 $\ell+1$。

3.2. 在有限域上计算同源曲线。使用 U_ℓ、V_ℓ、 W_ℓ 时，我们需要求三个次数为 $\ell+1$ 的多项式的根，而不是求次数为 1 的多项式的根。一般而言，如果 U_ℓ 有有理根（它应为 1、2 或 $\ell+1$），那么 V_ℓ、 W_ℓ 也都是如此。对于每组三元解 $(\sigma_1$、 z_1、 $z_2)$，我们需要检验它是否会导出一个同源。为了加快计算，我们可以按照 [16] 中的说明，计算 A^* 和 B^* 的有理分式（另见 [17, §7]）。Atkin 在 [2], 中勾勒了另一种方法，接下来我们将对此进行介绍。

4. 按照 Revisiting CCR ` Atkin

其思路是将 [1, 2, 14], 中的方法推广，即利用 q-级数恒等式求得参数 (σ,A^*,B^*)；从现在起，我们用 σ 表示 σ_1 。

4.1. U_ℓ 的性质。为便于阅读，我们记 $U=U_\ell$ ，并且

$$\partial_\sigma=\frac{\partial U}{\partial\sigma},\partial_4=\frac{\partial U}{\partial E_4},\partial_6=\frac{\partial U}{\partial E_6}.$$

并将这一记法推广到二阶导数。

多项式 U 是关于权重的齐次多项式，因此

$$(\ell+1)U=\sigma\partial_\sigma+2E_4\partial_4+3E_6\partial_6. \tag{5}$$

注意， U 的偏导数也是齐次多项式，因此我们得到

$$\ell\partial_\sigma = \sigma\partial_{\sigma\sigma}+2E_4\partial_{\sigma4}+3E_6\partial_{\sigma6}, \tag{6}$$

$$(\ell-1)\partial_4 = \sigma\partial_{\sigma4}+2E_4\partial_{44}+3E_6\partial_{46}, \tag{7}$$

$$(\ell-2)\partial_6 = \sigma\partial_{\sigma6}+2E_4\partial_{46}+3E_6\partial_{66}. \tag{8}$$

4.2. 从 CCR 多项式求得同源曲线。

˜4.2.1. 求取 E_4。

˜命题4.1。 E_4 的值为

$$-\frac{4\ell(3E_4^2\partial_6+2E_6\partial_4)-\partial_\sigma(\ell^2E_4+4\sigma^2)}{\ell^4\partial_\sigma}.$$

证明：对 $U(\sigma,E_4,E_6)=0$ 求导（使用 (1)），得到

$$\sigma'\partial_\sigma+E_4'\partial_4+E_6'\partial_6=0. \tag{9}$$

˜对 $\sigma=\ell/2(\ell E_2-E_2)$ 求导，得到

$$\sigma'=\frac{\ell}{2}\left(\ell^2\tilde{E}_2'-E_2'\right)=\frac{\ell}{24}\left(\ell^2(\tilde{E}_2^2-\tilde{E}_4)-(E_2^2-E_4)\right).$$

˜将 ℓE_2 替换为 $2\sigma/\ell+E_2$，得到

$$\sigma'=\frac{\ell}{24}\left(\frac{4\sigma^2}{\ell^2}+\frac{4\sigma}{\ell}E_2-(\ell^2\tilde{E}_4-E_4)\right),$$

将（9）与方程（4）中 E_4' 和 E_6' 的表达式代入，可得到一个关于 E_2 的次数为 1 的多项式，其 E_2 的系数为

$$\sigma\partial_\sigma+2E_4\partial_4+3E_6\partial_6,$$

我们在（5）中认出了这一点。因此，我们得到

$$(\ell+1)UE_2+\frac{\ell\,\partial_\sigma}{4}\left(\frac{4\sigma^2}{\ell^2}-(\ell^2\tilde{E}_4-E_4)\right)-2E_6\partial_4-3E_4^2\partial_6=0 \tag{10}$$

˜由此我们推得 E_4，因为 $U(\sigma,E_4,E_6)=0$。 □

˜4.2.2. 求 E_6。

˜命题4.2。 E_6 的值可写为

$$\tilde{E}_6=-\frac{N}{\ell^6\,\partial_\sigma^3}$$

其中 N 是关于 ℓ 的次数为 3 的某个多项式，并在证明末尾给出。

证明：对式（9）求导。

$$\sigma''\partial_\sigma+\sigma'(\sigma'\partial_{\sigma\sigma}+E_4'\partial_{\sigma 4}+E_6'\partial_{\sigma 6}) \tag{11}$$

$$+\quad E_4''\partial_4+E_4'(\sigma'\partial_{4\sigma}+E_4'\partial_{44}+E_6'\partial_{46}) \tag{12}$$

$$+\quad E_6''\partial_6+E_6'(\sigma'\partial_{6\sigma}+E_4'\partial_{64}+E_6'\partial_{66})=0 \tag{13}$$

我们依次计算

$$12E_2''=2E_2E_2'-E_4'=E_2(E_2^2-E_4)/6-(E_2E_4-E_6)/3,$$

$$12\tilde{E}_2''=2\tilde{E}_2\tilde{E}_2'-\tilde{E}_4'=\tilde{E}_2(\tilde{E}_2^2-\tilde{E}_4)/6-(\tilde{E}_2\tilde{E}_4-\tilde{E}_6)/3,$$

由此得到值

$$\sigma'' = \frac{\ell}{2}\left(\ell^3 \tilde{E}_2'' - E_2''\right)$$

用于式 (11)。对式 (4) 的关系式求导，可得

$$E_4'' = \frac{1}{3}\left(E_2' E_4 + E_2 E_4' - E_6'\right), \quad E_6'' = \frac{1}{2}\left(E_2' E_6 + E_2 E_6' - 2E_4 E_4'\right),$$

˜分别用于第 (12) 行和第 (13) 行。我们将 E_4 替换为其在˜ ˜
(10) 中的值，并使用 $\sigma = (\ell/2)(\ell E_2 - E_2)$替换 E_2。最终得到一个关于 E_2 的多项式表达式:

$$C_2 E_2^2 + C_1 E_2 + C_0 = 0.$$

˜未知量 E_6 只需在 C_0 中求得。
幸运的是（？）

命题 4.3。对于满足$U_\ell(\sigma, E_4, E_6) = 0$的三元组，系数 C_1 和 C_2 均为零。

证明思路：两种情形下的证明策略相同。将 $\partial_{\sigma\sigma}$、 ∂_{44} 和 ∂_{66} 替换为它们在 (6) 中的值。对所得表达式进行因式分解后，会得到相同的因子 $\sigma\partial_\sigma + 2E_4\partial_4 + 3E_6\partial_6$，它与 C_1 和 C_2 相消。为方便读者，我们在本文附录中添加了一个 SageMath 脚本。 □

剩下

$$\tilde{E}_6 = -\frac{N}{\ell^6\,\partial_\sigma^3}$$

其中 N 是关于 ℓ 的三次多项式

$$N = -E_6\partial_\sigma^3\ell^3 + c_2\ell^2 + 12\partial_\sigma^2\sigma(3E_4^2\partial_6 + 2E_6\partial_4)\ell - \partial_\sigma^3\sigma^3.$$

系数 c_2 看起来很复杂，我们将其稍作因式分解，写成关于 E_4 的多项式:

$$\begin{aligned} c_2 \;=\; & 18(\partial_6^2\partial_{\sigma\sigma} - 2\partial_6\partial_\sigma\partial_{\sigma 6} + \partial_{66}\partial_\sigma^2)E_4^4 \\ & +(24E_6\partial_4(\partial_6\partial_{\sigma\sigma} - \partial_\sigma\partial_{\sigma 6}) + 24E_6\partial_\sigma(\partial_{46}\partial_\sigma - \partial_6\partial_{\sigma 4}) + 10\partial_4\partial_\sigma^2)E_4^2 \\ & +3\partial_\sigma^2(7E_6\partial_6 - \sigma\partial_\sigma)E_4 + 8E_6^2(\partial_4^2\partial_{\sigma\sigma} - 2\partial_4\partial_\sigma\partial_{\sigma 4} + \partial_{44}\partial_\sigma^2). \square \end{aligned}$$

4.2.3. 数值示例。考虑 E： $Y^2 = X^3 + X + 3$ （在 $\mathbb{F}_{1009}$ 上）和 $\ell = 5$。使用

$$U_5(X) = X^6 + 20X^4A + 160X^3B - 80X^2A^2 - 128XAB - 80B^2,$$

我们选取 $\sigma = 584$ 并计算

$$\partial_\sigma = 905, \partial_4 = 779, \partial_6 = 140$$

˜由此可得 $E_4 = 497$, $A^* = 441$。经过繁琐的计算，我们发现$B^* = 997$。

4.3. $\ell \equiv 11$ 模 12 的情形。在这种情况下，Atkin 建议将 σ 替换为$f(q) = (\eta(q)\eta(q^\ell))^2$, ，其中 η 是 Dedekind 函数。相应的模多项式 U_ℓ^a可以使用[15]中描述的技术计算。例如（使用满足 E_4, E_6 和 Δ的基）：

$$U_{11}^a(X) = X^{12} - 990\,\Delta\,X^6 + 440\,E_4\,\Delta\,X^4 - 165\,E_6\,\Delta\,X^3 + 22\,E_4^2\,\Delta X^2 \\ -E_6\,E_4\,\Delta\,X - 11\,\Delta^2,$$

其比 $U_{11}(X)$ 更稀疏。

4.3.1. U_ℓ^a 的一些性质。令 v_2 （分别为 v_3）表示我们通过实验发现的 $U_\ell^a(X)$ 的系数中 $1/2$ （分别为 $1/3$）的最大幂

ℓ	v_2	v_3
11	16	12
23	32	24
47	64	48
59	80	60
71	96	72

看起来， $f/12$应该是更合理的选择，这会使 $12^{\ell+1}U_\ell^a(X/12)$ 的系数为整数。

由于相应的齐次性质，我们有与 (6) 类似的公式。

$$\ell\partial_f = f\partial_{ff} + 2E_4\partial_{f4} + 3E_6\partial_{f6}, \tag{14}$$

$$(\ell-1)\partial_4 = f\partial_{f4} + 2E_4\partial_{44} + 3E_6\partial_{46}, \tag{15}$$

$$(\ell-2)\partial_6 = f\partial_{f6} + 2E_4\partial_{46} + 3E_6\partial_{66}. \tag{16}$$

~ ~4.3.2. 计算 σ、 E_4 和 E_6。

命题 4.4。 σ 的值为

$$\sigma = \frac{\ell\,\left(3\,\partial_6\,E_4^2 + 2\,\partial_4\,E_6\right)}{f\partial_f}.$$

证明：注意到 $f^{12} = \Delta(z)\Delta(\ell z)$，因此我们可以推出同源曲线的判别式 $\tilde{\Delta} = f^{12}/\Delta$ 。此外，我们还有（利用 (3)）：

$$12\,\frac{f'}{f} = \frac{\Delta'}{\Delta} + \ell\frac{\tilde{\Delta}'}{\tilde{\Delta}} = E_2 + \ell\tilde{E}_2,$$

由此我们推出 f'。同样， U_ℓ^a 是权重为 $\ell+1$ 的齐次式，因此我们有与 σ 相似的恒等式。特别地，

$$(\ell+1)U_\ell^a = f\partial_f + 2E_4\partial_4 + 3E_6\partial_6. \tag{17}$$

从 $f'\partial_f + E_4'\partial_4 + E_6'\partial_6 = 0$ 出发，并代入已知值，可得

$$\left(f\partial_f + 4E_4\partial_4 + 6E_6\partial_6\right)E_2 + f\ell\tilde{E}_2\partial_f - 6E_4^2\partial_6 - 4E_6\partial_4 = 0,$$

即

$$f\partial_f(\ell\tilde{E}_2 - E_2) - 6E_4^2\partial_6 - 4E_6\partial_4 = 0,$$

由此便得到了结果。 □

˜命题 4.5。 E_4 的值由下式给出：

$$\tilde{E}_4 = -\frac{M}{\ell^2 f^2 E_4 E_6 \partial_f^3}$$

其中， M 是一个在证明末尾给出的多项式。

证明：对 f' 求导，得到：

$$\begin{aligned} f'' &= \frac{1}{12}\left(f'(\ell\tilde{E}_2 + E_2) + f(\ell^2\tilde{E}_2' + E_2')\right) \\ &= \frac{f}{12^2}\left((\ell\tilde{E}_2 + E_2)^2 + \ell^2(\tilde{E}_2^2 - \tilde{E}_4) + (E_2^2 - E_4))\right). \end{aligned}$$

˜将这些结果以及式 (14) 和 $E_2 = (E_2 + 2\sigma/\ell)/\ell$ 的对角导数代入

$$f''\partial_f + f'(f'\partial_{ff} + E_4'\partial_{f4} + E_6'\partial_{f6}) \tag{18}$$

$$+ \quad E_4''\partial_4 + E_4'(f'\partial_{4f} + E_4'\partial_{44} + E_6'\partial_{46}) \tag{19}$$

$$+ \quad E_6''\partial_6 + E_6'(f'\partial_{6f} + E_4'\partial_{64} + E_6'\partial_{66}) = 0 \tag{20}$$

得到一个关于 E_2 的二次多项式，其中二次项和一次项的系数最终都为零。剩下

$$\tilde{E}_4 = -\frac{M}{\ell^2 f^2 E_4 E_6 \partial_f^3}$$

其中

$$\begin{aligned} M &= 24(3E_6\partial_6^2\partial_{f4} + \partial_{46}\partial_f^2 f)E_4^6 \\ &\quad +12(9E_6^2\partial_6^2\partial_{f6} - 3E_6\partial_6^2\partial_f\ell + 6E_6\partial_6\partial_f\partial_{f6}f - \partial_6\partial_f^2\ell f + \partial_f^2\partial_{f6}f^2 \\ &\qquad -6E_6\partial_6^2\partial_f + 2\partial_6\partial_f^2 f)E_4^5 + 96E_4^4E_6^2\partial_4\partial_6\partial_{f4} \\ &\quad +4E_6(36E_6^2\partial_4\partial_6\partial_{f6} - 12E_6\partial_4\partial_6\partial_f\ell + 12E_6\partial_4\partial_f\partial_{f6}f - 12E_6\partial_{46}\partial_f^2 f \\ &\qquad +12E_6\partial_6\partial_f\partial_{f4}f - 24E_6\partial_4\partial_6\partial_f - 5\partial_4\partial_f^2 f)E_4^3 \\ &\quad +E_6(32E_6^2\partial_4^2\partial_{f4} - 42E_6\partial_6\partial_f^2 f + \partial_f^3 f^2)E_4^2 \\ &\quad +16E_6^3\partial_4(3E_6\partial_4\partial_{f6} - \partial_4\partial_f\ell + 2\partial_f\partial_{f4}f - 2\partial_4\partial_f)E_4 \\ &\quad +24E_6^4\partial_{46}f\partial_f^2 - 8E_6^3\partial_4\ell f\partial_f^2 + 8E_6^3\partial_{f4}f^2\partial_f^2 + 8E_6^3\partial_4 f\partial_f^2. \quad \square \end{aligned}$$

最后，我们指出， B^* 满足

$$B^{*2} + 6912\tilde{\Delta} - 4A^{*3}/27 = 0, \quad U_\ell^a(-\ell f, A^*, B^*) = 0, \tag{21}$$

后一关系是对 σ_1 对应的模形式应用 Atkin-Lehner 对合得到的。这两个多项式的最大公因式应能揭示 B^*。在极少数情况下，如果这个最大公因式的次数为 2（这意味着有两条椭圆

曲线与 E 同源），我们就不得不使用高阶微分，这看起来会是一项艰巨的任务。

4.3.3. 数值示例。考虑 E： $Y^2 = X^3 + X + 3$ 在 $\mathbb{F}_{1009}$ 上。多项式 U_{11}^a 有两个根：65 和 333。我们取 $f = 65$。首先，我们˜计算 $\sigma = 75$。然后 $E_4 = 532$。(21) 中两个多项式的最大公因式次数为 1，根为 $B^* = 460$。

5. Conclusions

我们已经完成了 Atkin 提出的任务，即使用 CCR 多项式构造同源。所有这些公式都需要在基域中进行 $O(\ell^2)$ 次乘法，这是因为需要计算次数为 $O(\ell)$ 的多项式的偏导数。请注意，这与使用给出 A^* 和 B^* 的有理分式所需的计算量相同，但存储需求较少。

因此，我们有多种算法和公式可供使用，具体取决于要解决的实际问题。

References

[1] A. O. L. Atkin. 素数模意义下椭圆曲线上的点数。草稿，1988 年。[2] A. O. L. Atkin. 素数模意义下椭圆曲线上的点数（II）。草稿。可通过 http://listserv.nodak.edu/archives/nmbrthry.html 获取，1992 年。[3] Bruce C. Berndt. Ramanujan 关于埃森斯坦级数的公式。载于 *Number theory and related topics (Bombay, 1988)* 12 *Tata Inst. Fund. Res. Stud. Math.*，第 卷，23–29 页。Tata 基础研究所，孟买，1989 年。[4] I. Blake、G. Seroussi 和 N. Smart。*Elliptic curves in cryptography*，第 *London Math. Soc. Lecture Note Ser.* 卷（第 265 卷），剑桥大学出版社，1999 年。[5] A. Bostan、F. Morain、B. Salvy 和 ´E. Schost。计算椭圆曲线之间同源的快速算法。*Math. Comp.*，77(263):1755–1778，2008 年。[6] Wouter Castryck、Tanja Lange、Chloe Martindale、Lorenz Panny 和 Joost Renes。CSIDH：一种高效的后量子交换群作用。载于 Thomas Peyrin 和 Steven D. Galbraith 编，*Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Informa-tion Security, Brisbane, QLD, Australia, December 2-6*，2018 年，*Proceedings, Part III*，第 *Lecture Notes in Computer Science* 卷（第 11274 卷），395–427 页。施普林格，2018 年。[7] L. S. Charlap、R. Coley 和 D. P. Robbins。有限域上椭圆曲线有理点的枚举。草稿；副本可从 http://www.lix.polytechnique.fr/Labo/Francois.Morain/Introuvables/Drafts/cc 获取

r.pdf,

1991年。[8] Denis Xavier Charles、Kristin E. Lauter 和 Eyal Z. Goren。基于扩展图的密码学哈希函数。*J. Cryptol.*，22(1):93–113，2009年。[9] Jean-Marc Couveignes。困难齐次空间。密码学电子印本文库，报告 2006/291，2006年。http://eprint.iacr.org/2006/291。[10] N. D. Elkies。有限域上的椭圆曲线与模曲线及相关计算问题。载于 D. A. Buell 和 J. T. Teitelbaum 编，*Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin* 7，

*AMS/IP Studies in Advanced Mathematics*卷，21–76 页。美国数学会、国际出版社，1998年。

[11] Luca De Feo、Jean Kieffer 和 Benjamin Smith。面向基于普通同源图的实用密钥交换。载于 Thomas Peyrin 和 Steven D. Galbraith 编, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia December 2-6 2018 Proceedings Part III* 11274 *Lecture Notes in Computer Science* 365 394 2018 , , , , 卷, 页 – 。施普林格, 。[12] Luca De Feo 、 David Kohel 、 Antonin Leroux 、 Christophe Petit 和 Benjamin Wesolowski。SQIsign：基于四元数和同源的紧凑型后量子签名。载于 Shiho Moriai 和 Huaxiong Wang 编, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11,* 2020年, *Proceedings Part I* 12491 *Lecture Notes in Computer Science* 64 93 , , 卷, 页 – 。施普林格, 2020年。[13] David Jao 和 Luca De Feo。基于超奇异椭圆曲线同源的抗量子密码系统。载于 Bo-Yin Yang 编, *Post-Quantum Cryptography - 4th International Workshop PQCrypto 2011 Taipei Taiwan November 29 - December 2 2011. Proceedings* 7071 *Lecture Notes in Computer Science* , , , , , 卷, 19–34 页。施普林格, 2011 年。[14] F. Morain。有限域上椭圆曲线点数的计算：算法方面。 *J. Théor. Nombres Bordeaux*, 7:255–282, 1995年。[15] Fran.cois Morain。Charlap-Coley-Robbins 模多项式的计算, 2023年。[16] Masayuki Noro、Masaya Yasuda 和 Kazuhiro Yokoyama。利用 V´élu 公式对椭圆曲线同源进行符号计算。 *Comment. Math. Univ. St. Pauli*, 68 93 130, 2020年: – 。[17] Adrien Poteaux 和 ´Eric Schost。模三角集的模合成及其应用。 *Comput. Complexity*, 22(3):463–516, 2013年。[18] S. Ramanujan。模方程及对 π的逼近。 *Quarterly J. Math.*, XLV:350–372, 1914年。[19] A. Rostovtsev 和 A. Stolbunov。基于同源的公钥密码系统。密码学电子印本文库, 报告 2006/145, 2006年。http://eprint.iacr.org/。[20] R. Schoof。有限域上椭圆曲线的点计数。 *J. Théor. Nombres Bordeaux* 7 219 254, 1995 , : – 。
[21] Sage 开发者。 *SageMath the Sage Mathematics Software System (Version 9.2)* 2020 , , 。 https://www.sagemath.org。

Appendix A. A script to check the computations

此 SageMath [21] 脚本也可以从作者的网页下载。

```
# 本脚本旨在使用预印本中的记号，计算并验证若干与 CCR 多项式相关的恒等式

# 一环统御众环 R.<ell、E2、E4、E6、sigma、E4t、E6t、d4、d6、s、ds、ds4、ds6、d46、f、df、df4、d f6>=PolynomialRing(Rationals(),18)

########## CCR c 作为 e

# returns ell^-4 * ds^-1 * (-12*ell*E4^2*d6 + ...)
```

定义 c h e c k E 4 t ( ): E4p=(E2*E4 −E6) / 3 E6p=(E2*E6−E4 ^ 2) / 2 E2p=(E2^ 2−E4) / 1 2 E2t=(E2+2*sigma / e l l) / e l l s i g p=e l l / 24*(4*sigma ^2/ e l l ^ 2+4*sigma / e l l *E2−(e l l ^2*E4t−E4)) tmp=s i g p *d s+E4p*d4+E6p*d6 tmp=tmp。n u merator ( ) 打印 (" d e g r e e (tmp, E2)=" , tmp。d e g r e e (E2)) # 检查 tmp 中 E2 的系数是否为零 c1=tmp。c o e f f i c i e n t ({E2 : 1}) # 是 (2*E4*d4 + 3*E6*d6 +f *d f) 的倍数, 因此为 0 打印 (" c1=" , c1。f a c t o r ( )) # 求 sigma, 使其成为常数系数 e 4 t=tmp。c o e f f i c i e n t ({E2 : 0}) e 4 t=− e 4 t。c o e f f i c i e n t ({E4t: 0}) / e 4 t。c o e f f i c i e n t ({E4t : 1}) # s i g 中包含 sigma 的值 返回 e 4 t。f a c t o r ( )

r e t u r n s # e l l ^−6 *ds ^−3 *sigma^−1 *E6^−1 *E4^−1 *(−18*e l l ^3*E4^5*E6*d6 ^ 2*ds +.

定义 c h e c k E 6 t ( ) : e 4 t=c h e c k E 4 t ( ) E4p=(E2*E4 −E6) /3 E6p=(E2*E6− E4 ^2) / 2 E2p=(E2^2−E4) /12 E2t=(E2+2*sigma / e l l) / e l l s i g p=e l l *(4* sigma ^2/ e l l ^2+4*sigma / e l l *E2−(e l l ^2*e4t −E4)) / 2 4 # 更多导数 E4pp =1/3*(E2p*E4+E2*E4p−E6p) E6pp=1/2*(E2p*E6+E2*E6p−2*E4*E4p) # 关键值 E4tp =1/3*(E2t *e4t −E6t) E2tp=(E2t^2−e 4 t) / 12 E2pp=1/12*(2*E2*E2p− E4p) E2tpp =1/12*(2*E2t *E2tp−E4tp) s i g p p=e l l *(e l l ^3*E2tpp−E2pp) / 2 # 注入对角导数 d s s =(e l l *d s −2*E4*d s4 −3*E6*d s6) / sigma d44 =((e l l −1)*d4−sigma *ds4 −3*E6*d46) / (2*E4) d66 =((e l l −2)*d6−sigma * ds6 −2*E4*d46) / (3*E6) # 起始点

```
tmp=sigpp*ds+sigp*(sigp*dss+E4p*ds4+E6p*ds6)
tmp=tmp +E4pp*d4+E4p*(sigp*ds4+E4p*d44+E6p*d46)
tmp=tmp +E6pp*d6+E6p*(sigp*ds6+E4p*d46+E6p*d66)
tmp=tmp.numerator() c2=tmp.coefficient({E2: 2})
print("E6t.c2=", c2.factor()) c1=tmp.coefficient({E2: 1}) print("E6t.c1=", c1) c0=tmp.coefficient({E2: 0}) e6t=-c0.coefficient({E6t: 0})/c0.coefficient({E6t: 1}) return e6t.factor()
```

########## 模 12 的椭圆曲线情形，Atkin 的变体 def check11sigma(): # R.<ell, E2, E4, E6, sigma, d4, d6, f, df>=多项式环(Rationals(), 9) tmp=2*E4*d4+3*E6*d6+f*df E4p=(E2*E4-E6)/3 E6p=(E2*E6-E4^2)/2 E2p=(E2^2-E4)/12 E2t=(E2+2*sigma/ell)/ell fp=f/12*(ell*E2t+E2) tmp=fp*df+E4p*d4+E6p*d6 tmp=tmp.numerator() # 检查 E2 的系数是否为零 c1=tmp.coefficient({E2: 1}) # 是 (2*E4*d4 + 3*E6*d6 +f*df) 的倍数，因此为 0 print("c1=", c1.factor()) # 求常数项系数的根 sigma s1g=tmp.coefficient({E2: 0}) s1g=-s1g.coefficient({sigma: 0})/s1g.coefficient({sigma: 1}) # s1g 包含 sigma 的值 return s1g.factor()

返回 #(-1) *df^-3*f^-2*ell^-2*E6^-1*E4^-1*(-36*ell*E4^5*E6*d6^2*df +

定义 check_11E4t(): sigma=
check_11sigma() E4p=(E2*E4 -
E6) / 3 E6p=(E2*E6-E4^2) / 2
E2p=(E2^2-E4) / 12 E2t=(E2+2*
sigma / ell) / ell fp=f / 12*(ell *
E2t+E2)

```
fpp=f/12^2*((ell*E2t+E2)^2+ell^2*(E2t^2-E4t)+(E2^2-E4))E4pp=1/3*(E2p*E4+E2*E4p-E6p)E6pp=1/2*(E2p*E6+E2*E6p-2*E4*E4p)# 注入对角导数 dff =(ell*df-2*E4*df4 -3*E6*df6)/fd44 =((ell-1)*d4-f*df4-3*E6*d46)/(2*E4)d66 =((ell-2)*d6-f*df6-2*E4*d46)/(3*E6)tmp=fpp*df+fp*(fp*dff+E4p*df4+E6p*df6)tmp=tmp +E4pp*d4+E4p*(fp*df4+E4p*d44+E6p*d46)tmp=tmp +E6pp*d6+E6p*(fp*df6+E4p*d46+E6p*d66)tmp=tmp.numerator()print("tmp 的次数（E2）=",tmp.degree(E2))c2=tmp.coefficient({E2:2})print("E4t.c2=",c2.factor())c1=tmp.coefficient({E2:1})print("E4t.c1=",c1)c0=tmp.coefficient({E2:0})e4t=-c0.coefficient({E4t:0})/c0.coefficient({E4t:1})return e4t.factor()
```

LIX - Laboratoire d'informatique de l'École polytechnique *and* GRACE - Inria Saclay–Île-de-France*Email address*: morain@lix.polytechnique.fr