arXiv:2302.05217v1 [math.NT] 10 Feb 2023

计算 CHARLAP-COLEY-ROBBINS 模多项式

FRANC.OIS MORAIN

Abstract. 设 $\mathcal{E}$ 是域 K 上的一条椭圆曲线，ℓ 是一个素数。当且仅当 $X(j(\mathcal{E})) = 0$ 时，存在一条椭圆曲线 $\mathcal{E}^*$，它与 $\mathcal{E}$ 之间存在次数为 ℓ 的同源（既是有理映射，也是群同态）Φ_ℓ，其中 $\Phi_\ell(X,Y)$ 是传统模多项式。此外，模多项式给出了 $\mathcal{E}^*$ 的系数，以及显式构造该同源所需的参数。由于传统模多项式的系数很大，因此可以改用许多系数较小的模多项式族，Elkies、Atkin 等人对此有所阐述。本文重点研究 Charlap、Coley 和 Robbins 引入的模多项式族的计算。该族的优点是能直接将 $\mathcal{E}^*$ 的系数表示为这些多项式的根。我们回顾并改进了用于计算模多项式的已知算法。在介绍级数计算的用法后，我们探讨了基于艾森斯坦级数快速数值求值、使用浮点数的快速算法。我们还说明了如何将同源火山用作另一种方法。

1. Introduction

计算同源是 Schoof-Elkies-Atkin（SEA）算法的核心组成部分，该算法用于计算大特征有限域上椭圆曲线的基数 [38, 1, 20]，也用于 [6]。近来，它也应用于后量子密码学 [14, 26, 11, 25] 等领域，以及密码系统 [17, 37, 24]。

设 K 是一个特征不为 2 或 3 的域。两个椭圆曲线 $\mathcal{E}/\mathrm{K}: Y^2 = X^3 + AX + B$ 和 $\mathcal{E}^*/\mathrm{K}: Y^2 = X^3 + A^*X + B^*$ 之间的同源是一个群态射，同时也是次数为 ℓ 的有理映射（其核的基数）。处理这些同源有两种方法。当次数 ℓ 较小时，可以预先计算 A^*、B^* 以及核多项式的公式。当 ℓ 较大时，关键组成部分之一是模多项式；另一部分则是利用 A、B 和模多项式，求出 A^* 和 B^* 的有理表达式。本文重点讨论前一个问题。第二个问题见 [32]。请注意，也可以采用一种纯代数方法，即使用三角集 [35, §7]。

可供使用的模多项式族有很多，各自具有不同的性质。非常一般地说，模多项式是一个二元

Date: 2023年2月13日。

多项式 $\Phi(X, J)$，其中 J对应椭圆曲线 $\mathcal{E}$ 的 j-不变量，而 X 表示 $\Gamma_0(\ell)$ 上的某个模函数。其原型是$j(\mathcal{E}^*)$（更精确的表述见下文），由此得到传统模多项式。 X 也有其他选择。它们都导出高度为（推测） $O((\ell+1)\log\ \ell)$ 的多项式，但常数较小。

Charlap-Coley-Robbins（CCR）模多项式 [12] 提供了另一种选择，即由三元多项式组（U_ℓ、V_ℓ、W_ℓ）构成，并具有以下性质（以及其他性质）：A^* （分别为 B^*）是 V_ℓ （分别为 W_ℓ）的根。它们可以与前述模多项式结合使用（适用于某个偏导数为零的情况）。

本文旨在介绍 CCR 多项式的性质（第 4 节），说明如何计算它们（第 5 节），并将其用于同源计算。我们改编了经典方法：针对小素数，使用 $\mathbb{Z}$ 或 $\mathbb{F}_p$ 上的级数展开和中国剩余定理，采用浮点数进行求值/插值，以及使用同源火山。为此，我们需要以高精度求值第 2 节介绍的艾森斯坦级数，并在第 3 节介绍相应算法，包括一种同时求值多个级数的方法。我们给出数值示例，并比较模多项式的高度。最后，我们将 A^* 和 B^* 的代数表达式计算为有理分式（见 [33]）。

2. Classical functions

令 $q_1 = \exp(i\pi\tau)$ 和 $q = q_1^2$。根据作者的不同，公式会用不同参数表示，有时不太方便。对于某些级数，我们不加区分地写作 $f(\tau)$ 或 $f(q)$。

2.1. 雅可比 θ 函数。

经典的 θ 函数为:

$$\theta_2(q_1) = \sum_{n\in\mathbb{Z}} q_1^{(n+1/2)^2},\ \theta_3(q_1) = \sum_{n\in\mathbb{Z}} q_1^{n^2},\ \theta_4(q_1) = \sum_{n\in\mathbb{Z}} (-1)^n q_1^{n^2}.$$

其中有许多性质，例如

$$\theta_3^4(q_1) = \theta_4^4(q_1) + \theta_2^4(q_1).$$

后一个公式使我们能够像 [18] 中那样，专注于计算 $\theta_{3,4}(q_1)$。

另请注意以下命题 [18, Prop. 4]

命题 2.1。

$$\lim_{\mathrm{Im}(\tau)\to+\infty} \theta_3(\tau) = 1,\ \lim_{\mathrm{Im}(\tau)\to+\infty} \theta_4(\tau) = 1,\ \lim_{\mathrm{Im}(\tau)\to+\infty} \theta_2(\tau) = 0.$$

2.2. 艾森斯坦级数。

2.2.1. 定义与基本性质。我们考虑的经典艾森斯坦级数[1] 为

$$E_2(q) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n,$$

$$E_4(q) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n,$$

$$E_6(q) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n,$$

其中 $\sigma_r(n)$表示 n的因数的 r次幂之和。还可以为 $k > 3$定义其他级数 E_{2k}。理论表明， E_{2k} 是 $k > 1$的权为 $2k$ 的模形式。因此， $k > 3$ 的级数可以表示为 E_4 和 E_6的多项式。判别式 Δ也值得关注:

$$\Delta(q) = (E_4(q)^3 - E_6(q)^2)/1728 = \eta(q)^{24}$$

其中 $\eta(q) = q\prod_{n=1}^{\infty}(1-q^n)$是戴德金函数。最后，模不变量为

$$j(q) = \frac{E_4(q)^3}{\Delta(q)} = \frac{1}{q} + 744 + \cdots.$$

这些量（见 [23, §13.20]）

$$a = \theta_2(q_1), b = \theta_3(q_1), c = \theta_4(q_1)$$

满足以下恒等式（以及其他恒等式）

(1) $E_4 = (a^8 + b^8 + c^8)/2,\ E_6 = (a+b)(b+c)(c-a)/2,\ \Delta = (abc/2)^8.$

由此我们推得

$$\lim_{\mathrm{Im}(\tau)\to+\infty} E_4(\tau) = 1, \quad \lim_{\mathrm{Im}(\tau)\to+\infty} E_6(\tau) = 1.$$

2.2.2. E_2的特殊情形。级数 E_2 不是模形式，因为（见[36]）：

定理 2.2. 对于 $\mathrm{SL}_2(\mathbb{Z})$ 的所有矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$，有

$$E_2((a\tau+b)/(c\tau+d)) = (c\tau+d)^2E_2(\tau) + \frac{6c}{\pi i}(c\tau+d).$$

利用拉马努金的乘子，我们可以轻松构造一个模形式。令 n为整数，并令 $\mathcal{F}_n$表示乘子 $E_2(\tau) - nE_2(n\tau)$。

命题 2.3。函数 $\mathcal{F}_n$ 是权为 2、具有平凡乘子系的模形式，属于 $\Gamma_0(n)$。

[1] Ramanujan used $L = P = E_2$, $M = Q = E_4$, $N = R = E_6$.

证明：对于 $ad-bc=1$，记其值为

$$E_2\left(n\frac{a\tau+b}{c\tau+d}\right)=E_2\left(\frac{a(n\tau)+nb}{(c/n)(n\tau)+d}\right)$$

$$=((c/n)n\tau+d)^2E_2(n\tau)-\frac{6c}{n\pi i}((c/n)n\tau+d)$$

这导致

$$nE_2\left(n\frac{a\tau+b}{c\tau+d}\right)=n(c\tau+d)^2E_2(n\tau)-\frac{6c}{\pi i}(c\tau+d).$$

减去 $E_2((a\tau+b)/(c\tau+d))$，我们得到

$$\mathcal{F}_n((a\tau+b)/(c\tau+d))=(c\tau+d)^2\mathcal{F}_n(\tau).\square$$

对于较小的 n，已有一些恒等式，例如 [29] 当$n\in\{2,4\}$时； [2] 当 $n=3$ 和 11 时； [7, 定理 6.2], [3, 定理 3.7] 当 $n\in\{5,7\}$时。一个非常漂亮的关系是 [3,定理 6.3]

$$\mathcal{F}_7(q)=6\left(\sum_{m,n=-\infty}^{\infty}q^{m^2+mn+2n^2}\right)^2.$$

3. Fast evaluations

3.1. 对于 $k\geq 1$，快速计算 $E_{2k}(q)$。θ 函数可以在精度为 N 时，通过 q_1 展开（见 [22]）在 $O(\mathsf{M}(N)\sqrt{N})$ 时间内计算，或者借助 [18]，并且 [30], 以更快的 $O(\mathsf{M}(N)\log N)$ 时间计算。因此，量 E_{2k}（当 $k\geq 2$ 时）可以通过 $O(\mathsf{M}(N)\log N)$ 次运算，以精度 N 计算。由此可知， $j(q)$ 也可以用相同的复杂度计算。

求值 E_2 并不那么显而易见。不过，在 [28, Thm4] 的证明中（感谢 [29] 指出了这一点），我们发现

$$\frac{E_2E_4}{E_6}=\frac{{}_2F_1\left(\frac{13}{12},\frac{5}{12};1;\frac{1728}{j}\right)}{{}_2F_1\left(\frac{1}{12},\frac{5}{12};1;\frac{1728}{j}\right)}=1+\frac{720}{j}+\cdots$$

其中高斯超几何函数定义为

$${}_2F_1\left(a,b;c;x\right)=\sum_{k=0}^{\infty}\frac{(a)_k(b)_k}{(c)_k\,k!}x^k,|x|<1$$

其中 $(a)_k=a(a+1)\cdots(a+k-1)$。根据 [40, 41, 31] 以及 [9],，该函数可在 O 中用 N 精度经 $\mathsf{M}(N)(\log N)^2$ 次运算计算得到。实际计算请参见 [27]。

还可以探讨与超几何函数的其他联系（A .Bostan，私人通信）。

此外，请注意，实际上我们需要计算 $\mathcal{F}_\ell$ 素数 ℓ。有时，我们可以使用上文所示的特殊公式。

3.2. 多值方法。实践中，一种更简单的方法可以基于 [22]，在 $O(\mathrm{M}(N)\sqrt{N})$ 的时间内，求出许多 k 的 E_{2k} 值，其中 $k \geq 1$。其代价可降至一次级数求值的代价。

由 [4]，得到

$$(q;q)_\infty = \exp(-2i\pi\tau/24)\eta(q),$$

且对于 $k \geq 0$:

$$T_{2k}(q) = 1 + \sum_{n=1}^{\infty}(-1)^n \left\{(6n-1)^{2k} q^{n(3n-1)/2} + (6n+1)^{2k} q^{n(3n+1)/2}\right\}.$$

注意，$(q;q)_\infty = T_0(q)$。

定理 3.1（第 6 节）。

$$\frac{T_2(q)}{T_0(q)} = E_2,\ \frac{T_4(q)}{T_0(q)} = 3E_2^2 - 2E_4,\ \frac{T_6(q)}{T_0(q)} = 15E_2^3 - 30E_2E_4 + 16E_6.$$

文献中给出了 $T_{2k}(q)/T_0(q)$ 的一般公式。

如果需要计算 E_2、E_4 和 E_6，我们可以看到，只需计算 T_{2k} 在 $k \in \{0,1,2,3\}$ 处的级数，再按照前述定理进行少量乘法和除法即可。此外，我们可以通过共享 q 的幂来计算这些级数。使用 [22, 算法2]可以以较低的成本计算这些幂。我们将修改后的过程列为算法 1。在步骤 3.2.3 中，我们在每个 T[i] 中加入了 $(6n \pm 1)^{2i}$ 的贡献。我们假设乘以这些小量的成本可以忽略不计。若非如此，我们可以增量计算多项式 $(6n \pm 1)^{2i}$。该算法的成本可降至计算其中一个级数的成本，从而节省一个因子 $kmax$。

算法 1 使用算法 2 中的基本操作。第 4 步的原因是，当 q 较小时，$T[k]$ 会接近 1，因此我们可能不想一开始就加上 1，甚至可能在这个函数中也不想加。

3.3. 虚参数的情形。实际上，考虑实数 $\rho \geq 1$ 下的 $\tau = \rho i$ 更容易。在这种情况下，$1 > q_0 = \exp(-2\pi) \geq q = \exp(-2\pi\rho) > 0$。函数 E_2 和 E_6 从 $E_{2k}(q_0)$ 单调递增至 1（注意，$E_6(q_0) = 0$，且 $E_2(q_0) = 3/\pi$ 从 [19] 开始）；E_4 从 $E_4(q_0)$ 单调递减至 1。需要注意这一点，以免计算结果失控。还要记住，$j(i) = 1728$。

接下来讨论计算函数 T_{2k} 所需的精度。令 N 为一个整数，$T_{2k,\ N}$ 为截至 $n = N-1$ 的截断和。由于该级数是交错级数，我们可以用以下方式界定误差:

$$\begin{aligned}&|T_{2k}(q) - T_{2k,N}(q)|\\ &\leq \left\{(6N-1)^{2k}\, q^{N(3N-1)/2} + (6N+1)^{2k}\, q^{N(3N+1)/2}\right\}\\ &\leq \left((6N-1)^{2k} + (6N+1)^{2k}\right) q^{N(3N-1)/2}.\end{aligned}$$

由于 $0 < q < 1$，这给出了一个二次收敛级数。

算法 1： $T_{2k}(q)$ 的组合求值。

函数 EvaluateManyT(q, N, kmax)
- 输入： q, N, $kmax$
- 输出：$(T_{2k}(q))$， 其中 $0 \le k \le kmax$
- 1. 对于 $k := 0$ 到 $kmax$， 执行
  - $T[k] \leftarrow 0$
- 2. $s \leftarrow 1$； $A \leftarrow \{1\}$； $Q[1] \leftarrow \{q\}$； $c \leftarrow 0$
- 3. 对于 $n := 1$ 当 $n(3n+1)/2 \le N$ 执行
  - $s \leftarrow -s$
  - // $s = (-1)^n$
  - 3.1 $c \leftarrow c + 2n - 1$
  - 3.2 对于 $r := 1$ 到 2 执行
    - 3.2.1 如果 $r = 2$ 那么
      - $c \leftarrow c + n$
      - // $c = n(3n+1)/2$
    - 3.2.2 $q' \leftarrow$ FindPowerInTable(A, Q, c)
    - 3.2.3 $C \leftarrow (6n + (-1)^r)^2$
    - 3.2.4 对于 $k := 0$ 到 kmax 执行
      - $T[k] \leftarrow T[k] + sq'$
      - 如果 $k < kmax$， 则
        - $q' \leftarrow Cq'$
- 4. 对于 $k := 0$ 到 kmax 执行
  - $T[k] \leftarrow T[k] + 1$
- 5. 返回 T。

4. The polynomials of Charlap-Coley-Robbins

4.1. 除法多项式。对于 $\mathcal{E}$： $y^2 = x^3 + Ax + B$， 将点 (X, Y) 乘以正整数 n 后，在 $\mathcal{E}$ 上得到

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

其中多项式满足

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

并且 ϕ_n、 ψ_{2n+1}、 $\psi_{2n}/(2Y)$ ω_{2n+1}/Y、 ω_{2n} 属于 $\mathbb{Z}[A, B, X]$。通常会利用以下内容将其简化

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

具有首批值

$$f_{-1} = -1,\ f_0 = 0,\ f_1 = 1,\ f_2 = 1,$$

算法 2：将 c 表示为已知值的组合。

函数 FindPowerInTable(A, Q, c)

输入 ： $A = \{a_1, \ldots, a_z\}$, Q，使得对所有 i, $Q[a_i] = q^{a_i}$, c
输出： q^c； A 和 Q 已更新
如果 $c = 1$，则
  $q' \leftarrow Q[1]$
否则，如果 $c = 2a$ 且 $a \in A$，则
  $q' \leftarrow Q[a]^2$
否则，如果 $c = a + b$ 且 a、$b \in A$，则
  $q' \leftarrow Q[a] \cdot Q[b]$;
否则，如果 $c = 2a + b$ 且 a、$b \in A$，则
  $q' \leftarrow Q[a]^2 \cdot Q[b]$
$A \leftarrow A \cup \{c\}$
$Q[c] \leftarrow q'$
返回 q'。

$$f_3(X, Y) = 3X^4 + 6AX^2 + 12BX - A^2$$

$$f_4(X, Y) = X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3.$$

f_n的次数为奇数 n 时的（$n^2 - 1$）/2，偶数 n时的（$n^2 - 4$）/2。若 X的权重为 1、 A 的权重为 2、 B 的权重为 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。

4.2. Elkies 的工作。同源与其核相关联，也可以用多项式来描述（称为核多项式）。给定 $\mathcal{E}$的某个有限子群 F，可以利用 V´elu 公式构造一条同源曲线 $\mathcal{E}^*$ 及相应的同源。在点计数中，我们通过传统模多项式的根，利用其 j-不变量，发现一条与 $\mathcal{E}$ 具有 ℓ-同源关系的曲线 $\mathcal{E}^*$ ； 同时还需要求出$\mathcal{E}^*$的系数以及相应的同源。Elkies 的思路是在与椭圆曲线 $\mathcal{E}$ 和 $\mathcal{E}^*$相关联的Tate曲线上研究同样的问题。

简而言之， $\mathcal{E}$ 在某个参数 q 下有一个方程，而与之同源的 $\mathcal{E}^*$ 对应于参数 q^ℓ，其中 ℓ 是同源的次数；在我们的情形中，该同源对应于一个基数为 ℓ 的有限子群 F。更准确地说，我们认为 $\mathcal{E}$ 的方程为 $Y^2 = X^3 + AX + B$，其中

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

采用相容缩放后，我们得到关于 $\mathcal{E}^*$ 的方程： $Y^2 = X^3 + A^*X + B^*$其中

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

更重要的是，令 σ_r 表示核多项式的根的幂和，我们有

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

此外，Elkies 证明了 [20, 公式（66）至（69）]

命题 4.1。

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

以及其他 σ_k 所满足的归纳关系 $k > 3$。

这可以改述为，(σ_1、A^*、B^*) 足以描述一个同源。此外，A^* 和 B^* 属于 $\mathbb{Q}[\sigma_1, A, B]$，因为 σ_2 和 σ_3 也属于该域。σ_1 的最小多项式是一个模多项式，我们可以将 A^* 和 B^* 表示为域 $\mathbb{Q}[\sigma_1, A, B]$中的元素，下面将使用这一点。换言之，$E_4(q^\ell)$ 和 $E_6(q^\ell)$ 是我们需要表示为已知模形式的模形式。有关这一主题的更多细节，请参见 [20] 。

给定这些量，有几种算法可以求得该同源。关于这一点，我们参见 [8] 。

4.3. CCR 多项式。

4.3.1. 重新诠释 Elkies 的结果。理解 Elkies 的工作（摘自 [12]）的一种方式是认识到，我们试图将定义在次数为 $\ell+1$ 的子域上的次数为（ℓ^2-1）/2 的多项式f_ℓ（假设 ℓ 为奇数）分解。

$$\begin{array}{c} \mathbb{Q}(A,B)[X]/(f_\ell(X,A,B)) \\ | \, (\ell-1)/2 \\ \mathbb{Q}(A,B)[X]/(U_\ell(X,A,B)) \\ | \, \ell+1 \\ \mathbb{Q}(A,B) \end{array}$$

一种经典做法是使用元素在$\mathbb{Q}(A,B)[X]/(f_\ell(X,A,B))$中的迹 t_1 。令 x_1 表示一个 ℓ 阶除点 $P = (x_1, y_1) \neq O_E$ 的（形式）横坐标。其他点 $P_j = [j]P = (x_j, y_j)$ 和 x_j 可以用除法多项式表示。对于 $0 \leq k \leq \ell+1$, 我们定义

$$t_k = \sum_{j=1}^{d} x_j^k = \sum_{j=1}^{d} \left(x_1 - \frac{\psi_{j-1}(x_1)\psi_{j+1}(x_1)}{\psi_j(x_1)^2} \right)^k \tag{2}$$

因此 $t_1 = x_1 + \cdots + x_d$ 和 $t_0 = d = (\ell-1)/2$。t_1 的最小多项式$U_\ell(X)$ $= X^{\ell+1} + u_1 X^\ell + \cdots + u_0$ 定义了下层扩张。给定幂和 t_k，牛顿恒等式使我们能够重构中间扩张上的最小多项式 $\prod_{i=1}^{d}(X - x_i)$ $= X^d - t_1 X^{d-1} + \cdots$。综合以上各项，$t_1$ 与上文所列的 σ_1 一致。

直接应用 (2)，我们可以计算 $U_3(X,Y,Z) = X^4+2YX^2+4ZX-Y^2/3$（这只是 ψ_3 的伪装形式）。更大的 ℓ 值需要更多工作。

4.3.2. 理论。我们从一条椭圆曲线 $\mathcal{E}$： $Y^2 = X^3+AX+B$ 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 $\mathcal{E}^*$： $Y^2 = X^3+A^*X+B^*$ 的方程。

定理4.2。存在三个多项式 U_ℓ、 V_ℓ、 W_ℓ，属于 $\mathbb{Z}[X,Y,Z,1/\ell]$，其关于 X 的次数为 $\ell+1$，使得 $U_\ell(\sigma_1,A,B)=0$，以及 $V_\ell(A^*,A,B)=0$、$W_\ell(B^*,A,B)=0$。

下面我们来讨论这些多项式的性质。

定理4.3. 当 $\ell>3$时，多项式 U_ℓ、 V_ℓ、 W_ℓ 属于 $\mathbb{Z}[X,Y,Z]$。

命题4.4. 将权重1、2、3分别赋给 X、 Y、 Z，则多项式 U_ℓ、 V_ℓ 和 W_ℓ 是权重为 $\ell+1$的齐次多项式。

命题4.5. $U_\ell(X,A(q)\ B(q))$的根为 $-\ell\mathcal{F}_\ell(q)/2$ 和 $\mathcal{F}_\ell(w\zeta_\ell^k)/2$，其中 $0\le k<\ell$；这里 $w^\ell=q$ 和 ζ_ℓ 是单位根。

我们沿用 [12,§8]。

命题 4.6. U_ℓ 的高度（分别为 V_ℓ、 W_ℓ）约为 $2k(\ell+1)\log\ell$，其中 $k=1$、2、3分别对应 U、 V、 W。

证明：令 $\lambda_k(u)=\sum_{n=1}^\infty \delta_{2k-1}(n)u^n$，这是求和中的重要项。使用

$$\delta_{2k-1}(n)\le n^{2k-1}\sum_{d\mid n}\frac{1}{d^{2k-1}}\le\zeta(2k-1)n^{2k-1},$$

我们可以看到， $\lambda_k(u)$ 被 $\zeta(2k-1)\sum_{n=1}^\infty n^{2k-1}u^n$ 支配

$$(2k-1)!\,\zeta(2k-1)\sum_{n=1}^\infty\binom{n+2k-2}{2k-1}u^n=C_ku(1-u)^{-2k}.$$

因此， λ_k^m被 $C_k^m(1-u)^{-2km}$ 支配，而最高次项近似为$u^{m^2/2}$。 λ^m 的最大系数近似为

$$C_k^m\binom{m^2/2+2km-1}{2km-1}\approx C_k^m\frac{(m^2/2+2km)^{2km}}{(2km/e)}$$

$$=C_k^m\left(\frac{e}{4k}\right)^{2km}(m+4k)^{2km}.$$

取 $m=\ell+1$ 即可得出结果。 □

传统模多项式 Φ_ℓ^t 的高度约为 $6(\ell+1)\log\ell$ [15, 39]。我们发现 U_ℓ 和 V_ℓ 较小，但 W_ℓ 却和 Φ_ℓ^t一样大。部分表格见附录。

4.3.3. 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，而不是传统情况下的 1。一般来说，如果 U_ℓ 有有理根（其值应为 1、2 或 $\ell+1$），那么 V_ℓ和 W_ℓ也都如此。对于每组三元解 (σ_1, z_1, z_2)，我们需要检验它是否导出一个同源。关于这项任务的技巧，见 [8]。

5. Computing CCR polynomials

利用上一节的结果，可以将这些多项式写成

$$U_\ell(X,Y,Z) = X^{\ell+1} + \sum_{i_1+2i_2+3i_3=\ell+1} u_{i_1,i_2,i_3} X^{i_1} Y^{i_2} Z^{i_3},$$
$$V_\ell(X,Y,Z) = X^{\ell+1} + \sum_{2i_1+2i_2+3i_3=\ell+1} v_{i_1,i_2,i_3} X^{i_1} Y^{i_2} Z^{i_3},$$
$$W_\ell(X,Y,Z) = X^{\ell+1} + \sum_{3i_1+2i_2+3i_3=\ell+1} w_{i_1,i_2,i_3} X^{i_1} Y^{i_2} Z^{i_3}.$$

所述的所有方法都适用于 U_ℓ、 V_ℓ 和 W_ℓ。为简化说明，下面我们假设 $\ell > 3$，并专注于 U_ℓ，同时指出对于 V_ℓ （分别为 W_ℓ）需要进行哪些修改。我们改写为

$$U_\ell(X,Y,Z) = X^{\ell+1} + \sum_{r=0}^{\ell} X^r \sum_{2i_2+3i_3=\ell+1-r} c_{r,i_2,i_3} Y^{i_2} Z^{i_3}.$$

由此可见， $r=\ell$ 不存在任何可能的项。

我们首先计算单项式的数量。我们从 [16,p. 110] 中取出以下内容。

命题 5.1。正整数中满足$i_1+2i_2+3i_3=n$ 的解的个数 $\mathbf{N}_{1,2,3}(n)$ 是 $(n+3)^2/12$ 的最接近整数。

使用相同的方法

命题 5.2。正整数中满足$2i_2+3i_3=n$ 的解的个数 $\mathbf{N}_{2,3}(n)$ 为

$$\mathbf{N}_{2,3}(n) = \frac{n+1}{6} + \frac{(-1)^n}{4} - \frac{1}{12} + \begin{cases} \frac{2}{3} & \text{if } n \equiv 0 \bmod 3, \\ \frac{1}{3} & \text{if } n \equiv 2 \bmod 3. \end{cases}$$

我们将计算许多形如 $Y^{i_2}Z^{i_3}$ 的乘积，其中 Y 和 Z 是较大的浮点数或级数。为此，我们使用 Pippenger 算法 [34, 第 247–249] 页（感谢 [5]）。

[12] 的作者给出了三种计算多项式 U_ℓ 的方法。第一种基于等式 (2)，可用于非常小的 ℓ。另外两种方法则通过对有理数域上的级数进行 q-展开，或在小素数模下计算后利用命题 4.6 中的界，通过中国剩余定理恢复结果。

5.1. 使用 q 展开。注意

$$\sigma_1(q) = -\frac{\ell \mathcal{F}_\ell(q)}{2} = \frac{\ell(\ell-1)}{2} + 12\ell \sum_{n=1}^{\infty} \sigma_1'(n) q^n$$

其中， $\sigma_1'(n)$ 是与 ℓ 互素的 n 的因数和。

第二种方法是将级数 $\sigma_1(q)$、 $A(q)$ 和 $B(q)$ 截断至次数 $\mathrm{N}^{1,2,3}(\ell+1) = O(\ell^2)$（命题 5.1），代入 $U_\ell(X,Y,Z) = 0$，并通过有理数域上的线性方程组求出多项式的未知系数（对于 $\ell > 3$，实际上是在整数中进行）。对于较小的 ℓ，可以使用任何数学系统完成这一过程。请注意，代数运算的次数（在 $\mathbb{Q}$ 或有限域上的乘法）将接近 $O(\ell^{2\omega})$，其中 ω 是矩阵乘法的常数，矩阵乘法的次数为 $2 \le \omega \le 3$，因此通常为 $O(\ell^6)$，这是一个很大的数。

第三种方法利用了这样一个事实：幂和 $\sigma_r(q)$（当 $1 \le r \le \ell+1$ 时）是模形式，并且可以表示为关于 $A(q)$ 和 $B(q)$（或 $E_4(q)$、 $E_6(q)$）的多项式

$$\sigma_r(q) = \sum_{2i_2+3i_3=r} u_{r,i_2,i_3} A(q)^{i_2} B(q)^{i_3}.$$

这将得到一个关于 $u_{r,\,i_2,\,i_3}$ 的线性方程组 $\mathcal{S}_r$（独立于 ℓ）。根据命题 5.2，该系统的规模为 $\mathrm{N}^{2,3}(r) \times \mathrm{N}^{2,3}(r) \approx (r/6)^2$，并且该线性方程组可用 $O(r^\omega)$ 次 $\mathbb{Z}$ 上的运算求解，因此总计通常需要 $O(\sum_r r^\omega) = O(\ell^{\omega+1}) = O(\ell^4)$。注意，所有这些系统都可以并行求解。

[12] 的作者建议使用更适配的基。当 $r = 2m$ 时，使用 $\{E_4^{m-3j}\Delta^k, 0 \le k \le \lfloor m/3 \rfloor\}$；当 $r = 2m+3$ 时（记住 $r = 1$ 的系数为 0），使用 $\{E_6 E_4^{m-3k}\Delta^k, 0 \le k \le \lfloor m/3 \rfloor\}$。注意，在所有情况下，指标为 k 的级数都以 q^k 开头，并且这些基呈三角形形状，换句话说，相应的系统 $\mathcal{S}_r$ 是三角形的。此外，由于首项系数为 1，系统的所有解都将是整数。

求出所有 r 后，我们使用牛顿恒等式来恢复 U_ℓ 的系数。需要利用中间表达式计算级数 $\sigma_r(q)$，其中具有单位根 ζ_ℓ 的 $w = q^{1/\ell}$ 会暂时出现，随后消失。详见 [21, §2.2]，其中还给出了更详细的说明和复杂度分析。具体而言，如果记 $\mathrm{M}_q(d)$ 为在 $\mathbb{Z}$ 中将含有 d 项的两个稠密 q 展开的乘法所需的算术运算次数，那么级数计算的总复杂度为 $O(\ell \mathrm{M}_q(\ell d))$，在我们的情形下为 $O(\ell \mathrm{M}_q(\ell^2))$。如果 H 是该多项式高度的一个上界，那么比特复杂度为 $O(\ell^3(\log \ell)\mathrm{M}(H))$。根据命题 4.6，假设 $H \in O(\ell \log \ell)$，则其为 $O(\ell^4 \log^{3+\epsilon} \ell)$。

例。考虑 $\ell = 5$ 的情形。需要求解的系统 $\mathcal{S}_r$ 来自以下方程：

$$\begin{aligned}\sigma_2(q) &= u_{2,0}E_4\\ \sigma_3(q) &= u_{3,0}E_6\\ \sigma_4(q) &= u_{4,0}E_4^2\\ \sigma_5(q) &= u_{5,0}E_6E_4\\ \sigma_6(q) &= u_{6,0}E_4^3 + u_{6,1}\Delta\end{aligned}$$

我们计算

$$\sigma_6(q) = 1000320 + 186071040q + \cdots$$

并记住，$E_4(q) = 1 + 240q + \cdots$, $\Delta(q) = q + \cdots$，因此系统 $\mathcal{S}_6$ 为

$$\left\{\begin{array}{rcl} 1000320 &=& u_{6,0}\\ 186071040 &=& 720\,u_{6,0} + u_{6,1}\end{array}\right.$$

它确实是三角形的，因此很容易求解。其解为整数。

我们也可以模小素数进行计算，并利用中国剩余定理恢复这些多项式。

5.2. 浮点方法。我们将为通常的模方程提出的方法应用于我们的三元多项式组 (U_ℓ, V_ℓ, W_ℓ)。对于多项式的对数高度，我们记为H；根据命题 4.6，我们估计其为$2k(\ell+1)\log\ \ell$。

5.2.1. 求解线性方程组。我们从

$$U_\ell(\sigma_1, A, B) = 0 = \sigma_1(q)^{\ell+1}$$

$$+\sum_{r=0}^{\ell}\sigma_1(q)^r \sum_{2i_2+3i_3=\ell+1-r} c_{r,i_2,i_3}A^{i_2}(q)B^{i_3}(q)$$

出发，计算浮点值，从而得到关于 c_{r,i_2,i_3}的线性方程组；对于 $\ell > 3$，其解应为整数。我们以高精度计算所选 τ in$q = \exp(2i\pi\tau)$ 值处的 $\sigma_1(q)$、$A(q) = -3E_4(q)$ 和 $B(q) = -2E_6(q)$。这需要 $O(\ell^{2\omega})$ 次浮点运算，下一节将介绍更高效的方法。

5.2.2. 使用幂和。文献 [21] 讨论了传统模多项式的情形。我们可以对自己的多项式采用相同的方法。首先，我们需要计算

$$-\frac{\ell}{2}\mathcal{F}_\ell(q), \{\mathcal{F}_\ell(w\zeta_\ell^k)/2, 0 \le k < \ell\}.$$

根据定义

$$\mathcal{F}_\ell(q) = E_2(q) - \ell E_2(q^\ell)$$

and

$$\mathcal{F}_\ell(w\zeta_\ell^k) = E_2(w\zeta_\ell^k) - \ell E_2(q),$$

最后一项相对于 k 是常数。我们首先计算 $E_2(q)$、 $E_2(q^\ell)$，然后通过共享计算来求出其他根：我们需要的所有项都具有 $(w\zeta_\ell^k)^e = w^e\zeta_\ell^{(ke) \bmod \ell}$ 的形式。当 $\ell \mid e$ 时，计算会稍快一些。相应的代码见算法 3。我们还预先计算 $\xi_k = \zeta_\ell^k$。完整代码见算法 4。

算法 3： $T_{2k}(w\zeta_\ell^j)$ 的组合求值。

```
函数 EvaluateConjugateValues(ℓ, w, N, (ξ), kmax)
    输入    : ℓ, w, (ξ), N
    输出: (T_{2k}(wζ_ℓ^j)), 其中 0 ≤ k ≤ kmax, 0 ≤ j < ℓ
    1. 对于 k := 0 至 kmax , 执行
        对于 j := 0 至 ℓ − 1 , 执行
            T[k, j] ← 0
    2. s ← 1;  A ← {1};  W[1] ← {w};  c ← 0
    3. 对于 n := 1 , 当 n(3n + 1)/2 ≤ N 时执行
        s ← −s
        //  s = (−1)^n
        3.1 c ← c + 2n − 1
        3.2 对于 r : = 1 到 2 执行
            3.2.1 如果 r = 2 那么
                c ← c + n
                //  c = n(3n + 1)/2
            3.2.2 w′ ← s·FindPowerInTable(A, W, c)
            3.2.3 C ← (6n + (−1)^r)^2
            3.2.4 对于 k := 0 to kmax do
                T[k, 0] ← T[k, 0] + w′
                对于 j := 1 to ℓ − 1 do
                    T[k, j] ← T[k, j] + ξ[(jc) 模 ℓ] w′
                如果 k < kmax then
                    w′ ← C · w′
    4. 对于 k := 0 to kmax do
        对于 j := 0 至 ℓ − 1 , 执行
            T[k, j] ← T[k, j] + 1
    5. 返回 T。
```

系统 $\mathcal{S}_r$ 的规模为 $N_{2,\ 3}(r)^2 = O(r^2)$，求解需要 $O(r^\omega)$ 次运算，总计 $O(\ell^{\omega+1})$。与级数情形一样，我们可以使用 (E_4, E_6, Δ) 基，因为我们预计系数为整数，这一点由级数计算表明。

算法 4：使用浮点数计算 CCR 多项式 k 。

函数 ComputeUVW(k, ℓ)
输入： $k \in \{1,2,3\}$ 分别对应于 U_ℓ、 V_ℓ 或 W_ℓ ，
ℓ 一个奇素数
输出：阶为 k 的 CCR多项式
0.0 $H \leftarrow 2k(\ell+1)\log \ell$；所有计算均在
精度 H
0.1 计算 $\zeta_\ell \leftarrow \exp(2i\pi/\ell)$
0.2 对于 $j := 0$ 到 $\ell - 1$ 执行
$\xi_j \leftarrow \zeta_\ell^j$
0.3 计算所有系统 $\mathcal{S}_r$ 对于 $2 \le r \le \ell + 1$
0.4 对于 $r := 2$ 到 $\ell + 1$ 执行
$\mathcal{L}_r \leftarrow \emptyset$
0.5 $\rho \leftarrow 1$
1. 当存在尚未求解的系统 $\mathcal{L}_r$ 时，执行
1.0 $\rho \leftarrow \rho + 0.1$
1.1 $w \leftarrow \exp(-2\pi\rho/\ell)$
1.2 $T \leftarrow$ EvaluateConjugateValues(ℓ, w, N, (ξ), $2k$)
1.3. 对来自 T 的所有 q，使用定理 3.1 计算 E_{2k} ，
得到 $r = 0, \ldots, \ell + 1$ 对应的 (γ_r)
1.4 对于 $r := 2$，对 $\ell + 1$ 执行
if $\mathcal{L}_r$ 若未求解，则
1.4.1 用 $\sum \gamma_i^r$ 实例化 $\mathcal{S}_r$， A $_\rho$ 以及 B_ρ; 将其添加到 $\mathcal{L}_r$
1.4.2 如果 $\mathcal{L}_r$ 的方程数量与未知数数量相同，则
求解 $\mathcal{L}_r$ 并存储这些值；声明 $\mathcal{L}_r$ 已求解
2. 对系数进行取整，并使用牛顿公式。

例。再次取 $\ell = 5$，其 $\mathcal{S}_r$ 已给出。我们聚焦于 $\sigma_6(q) = u_{6,0}E_4^3 + u_{6,1}\Delta$ 的情形；从 $\mathcal{L}_6 = \emptyset$ 开始。使用 $\rho = 1.1$ 得到

$$\mathcal{L}_6 = \{1.912407642u_{6,0} + 0.0009726854527956u_{6,1} = 1393450.57337539139\}$$

接下来使用 $\rho = 1.2$ 进行迭代，得到

$$\{1.435895343u_{6,0} + 0.0005247501300701u_{6,1} = 1156054.63606077432\}$$

而 $\mathcal{L}_6$ 的解（四舍五入为整数）为

$$u_{6,1} = -534159360, u_{6,0} = 1000320.$$

5.3. 同源火山。 [13] 中的方法与接下来要介绍的方法有许多相似之处，但复杂度更高。该方法使用超奇异曲线，且需要其完整的显式 ℓ-扭点。

[10] 的工作是 [39] 中的一个基石，在那里，利用中国剩余定理模小素数的显式版本，可以直接计算$\Phi_\ell(X, j(E)) \bmod q$。我们的方法使得这一思路很容易应用于中国剩余定理多项式问题。

5.3.1. 简要介绍。概括而言， [10] 中的算法对满足算术条件的特殊素数 p 进行模运算： $p \equiv 1 \bmod \ell$，且 $4p = t^2 - \ell^2 v^2 D$属于整数 t和 v， v不是 ℓ 的倍数； $D < 0$是某个辅助二次域的判别式。在这些条件下，所谓的类多项式 $H_D(X)$在模 p意义下完全分裂，其根是算法所需的、具有复乘的椭圆曲线的 j不变量。基本上，该算法利用 $H_D(X)$的根对数据进行插值。核心在于计算与 D 模 p相关的同源火山两个层级之间的同源。关于椭圆曲线的更多性质，请参阅原文。就我们的目的而言，只需知道我们已有可用的同源数据，并且这些数据可以帮助我们据此计算多项式 $U_\ell(X, A, B) \bmod p$。关于广义黎曼猜想下的复杂度，请参阅该文，即 $O(\ell^3(\log \ell)^3 \log\log \ell)$，使用 $O(\ell^2 \log(\ell p))$空间，其中p经过适当选择。

5.3.2. 算法。在我们的情形中，我们再次考虑幂和。为简化叙述，我们只考虑 U_ℓ，因为对于 V_ℓ和 W_ℓ，算法相同。

这里我们对 [10] 的简化版算法 2.1 做了少许修改，以满足我们的需求。我们所描述的内容同样适用于 [10] 中的完整版本。对于 $1 \le r \le \ell + 1$，我们将 $\mathcal{P}$ 记作 U_ℓ 的幂和，它被视为一个关于 X 的多项式，其系数属于 $\mathbb{Z}[Y, Z]$。我们可以写作

$$\mathcal{P}_r(Y, Z) = \sum_{2i_2 + 3i_3 = r} c_{r, i_2, i_3} Y^{i_2} Z^{i_3}.$$

这些求和将根据与曲线 $\mathcal{E}_i\colon Y^2 = X^3 + A_i X + B_i$ 相关联的值 $\mathcal{P}_{r,\ i}(A_i, B_i)$ 重建。

步骤 3 按如下方式完成。随机选取 $E_i/\mathbb{F}_p = [A_i, B_i]$ 上一个阶为 ℓ 的点 P。使用 V´elu 公式计算有理同源 $\mathcal{E}_i \to \mathcal{E}_i' = \mathcal{E}_i/\langle P \rangle$。如果 $j(\mathcal{E}_i')$ 是 H_D 的根，那么 $\mathcal{E}_i'$ 位于火山口上，并且是两个邻点之一。如果它不属于火山口，则属于火山底部。一般情形下涉及多个火山时的识别细节见 [10]。

就重构而言，在步骤 5 中将 σ_1 替换为 A^* （分别将 V_ℓ 替换为W_ℓ、将 σ_1 替换为B^*）。

算法5：计算 $U_\ell(X,Y,Z) \bmod p$

函数 ComputeUMod(ℓ, D, $H_D(X)$, p)：

输入： ℓ 一个奇素数， D 一个虚
判别式为 D 、类数为 $\mathcal{O}$ 的虚二次序
$h(D) \geq \ell+2$； H_D 是与.....相关的类多项式
阶 $\mathcal{O}$； p 素数，满足 $p \equiv 1$模 ℓ 且
$4p = t^2 - \ell^2 v^2 D$， $v \not\equiv 0$ 模 ℓ

输出： $U_\ell(X,Y,Z)$ 模 p

1. 构造列表 $\mathcal{J}_D$ ，其中包含模 p下 $H_D(X)$ 的根
2. 对每个 $j_i \in \mathcal{J}_D$，找到一条曲线 $\mathcal{E}_i$ ，其不变量为 j_i 且
基数 $m = p+1-t$；将 $\mathcal{C}_D$ 这个曲线集合称为
3. 对于每个 $\mathcal{E}_i \in \mathcal{C}_D$ ，在火山中找出其所有邻居 $\mathcal{N}(\mathcal{E}_i)$：2
水平同源以及火山底部上的 $\ell-1$ 。这是一组
通过 V´elu 公式得到的 $\ell+1$ 三元组 (σ_1, A^*, B^*)
4. 对于每个 $\mathcal{E}_i$： $Y^2 = X^3 + A_i X + B_i$， 计算幂和
$\mathcal{P}_{r,\ i}(A_i, B_i)$， 对应于 σ_1 在
$(\sigma_1, A^*, B^*) \in \mathcal{N}(\mathcal{E}_i)$， 使用 V´elu 公式
5. 使用 A 和 B 重构 $\mathcal{P}_r(Y,Z)$ 模 p 的幂和
以及 $\mathcal{P}_{r,\ i}(A_i, B_i)$， 求解一个 $N_{2,\ 3}(r) \times N_{2,\ 3}(r)$ 线性方程组
6. 返回 $\mathcal{P}$。

5.3.3. 数值示例。我们为 $\ell = 5$ 给出一个取值。我们选择$D = -71$ ，使得 $h(-71) = 7 \geq 5+2$。考虑 $p = 1811$。$H_{-71}(X)$ 模 p 的根为：

$$\mathcal{J}_D = \{313, 1073, 1288, 1312, 1402, 1767, 1808\}.$$

对于每个 j 值，都有与之关联的曲线和邻点。这些可以在表1中找到。与这些值对应的幂和为：

$\mathcal{E}_i \backslash r$	1	2	3	4	5	6
$[1582, 902]$	0	105	1680	1379	756	772
$[1662, 405]$	0	527	1188	90	748	888
$[1451, 1331]$	0	1723	403	350	293	583
$[1013, 747]$	0	1133	18	1594	1738	105
$[224, 753]$	0	95	760	1790	1603	27
$[1128, 1504]$	0	155	669	1424	1130	522
$[91, 725]$	0	1793	1523	589	1233	134

例如， $\sigma_6 = c_{030} Y^3 + c_{012} Z^2$，我们需要求解

$$\begin{cases} 772 &= c_{030} 1582^3 + c_{012} 902^2 \bmod 1811, \\ 888 &= c_{030} 1662^3 + c_{012} 405^2 \bmod 1811, \\ 583 &= c_{030} 1451^3 + c_{012} 1331^2 \bmod 1811, \\ \cdots & \cdots \quad \cdots \end{cases}$$

也就是 $1565Y^3 + 1218Z^2$。系数为：

$$\begin{aligned}\sigma_2 &= 1771Y \\ \sigma_3 &= 1331Z \\ \sigma_4 &= 1120Y^2 \\ \sigma_5 &= 341YZ \\ \sigma_6 &= 1565Y^3 + 1218Z^2\end{aligned}$$

6. Computing A^* and B^* as rational fractions

由 [33, 定理 3.9], ，存在次数小于 $\ell + 1$ 的多项式 $N_{\ell,\ A}$ 和 $N_{\ell,\ B}$，使得

$$A^* = \frac{N_{\ell,A}(X, A, B)}{U'_\ell(X)},\ B^* = \frac{N_{\ell,B}(X, A, B)}{U'_\ell(X)}$$

（仅在此处： U'_ℓ（X） $= \frac{\partial U_\ell}{\partial X}$。）此外，$N_{\ell,\ A}$ （分别为 $N_{\ell,\ B}$）是整数系数且广义权重为 $2\ell + 4$ （分别为 $2\ell + 6$）的多项式。参考文献的作者使用格罗布纳基计算来求出这两个分子。

另外，给定 U_ℓ，我们可以从以下形式开始（对 $N_{\ell,\ B}$也同样如此）：$U'_\ell(X, A, B)A^* = N_{\ell,\ A}(X, A, B)$，然后代入级数，得到

$$U'_\ell(\sigma_1(q), A(q), B(q))(-\ell^4 E_4(q^\ell)) = N_{\ell,A}(\sigma_1(q), A(q), B(q)).$$

我们通过求解一个线性方程组来求出系数（在 $\mathbb{Q}$ 上，或者使用前面所述的小素数）。我们可以预先计算级数 σ_1、 A 和 B 的幂，并注意到 U'_ℓ 和 $N_{\ell,\ A}$ 有许多幂是相同的。此外，级数 $E_4(q^\ell)$相当稀疏，因此与该量相乘的计算速度很快。

我们也可以像上面一样使用浮点数，并从 $N_{\ell,\ A}$的系数值中识别出整数。

同时计算 $N_{\ell,\ A}$ 和 $N_{\ell,\ B}$ 有一个优点：可以尽可能多地共享幂；在我们使用 Pippenger 算法时，这一点尤其有利。数值示例见附录。

7. 实现与数值结果

我们使用 Maple编写了大量程序，其中一些程序后来又用 Magma （2.26-10 版）重写，以提高速度。参见作者的网页。计算 $\ell \leq 100$ 的多项式，在普通笔记本电脑上只需几分钟。按照 [33]中的说明，使用 SEA 对其进行验证。

我们给出我们的对高度的示例 H 对 ℓ 的图。这里 $H(P) = \tilde{H}(P)/((\ell + 1)\log\ \ell)$。注意，这些量似乎会随着 ℓ 增大而趋于稳定。

ℓ	$\tilde{H}(\Phi_\ell^t)$	$\tilde{H}(\Phi_\ell^c)$	$\tilde{H}(\Phi_\ell^*)$	$\tilde{H}(U_\ell)$	$\tilde{H}(U_\ell^*)$
5	11.243	0.762	−−	0.526	−−
7	9.787	0.582	−−	0.640	−−
11	10.130	1.842	1.120	0.670	0.240
13	9.565	0.367	0.941	0.688	−−
17	9.581	0.958	0.714	0.690	−−
19	9.365	0.648	0.630	0.695	−−
23	9.438	1.995	0.419	0.698	0.441
101	−−	1.111	0.159	0.778	−−
103	−−	0.740	0.249	0.779	−−
107	−−	2.218	0.228	0.781	0.493
109	−−	0.379	0.213	0.782	−−

数据是使用 MAGMA 中提供的多项式计算得出的： Φ_ℓ^c 称为典范多项式，Φ_ℓ^* 称为 Atkin 多项式。对于 Φ_ℓ^c，高度取决于 $\ell \bmod 12$。有关这些多项式大小的更多统计信息，请参见附录。

当 $\ell \equiv 11$ 模 12 时，Atkin [1] 建议将 σ 替换为 $f(q) = (\eta(q)\eta(q^\ell))^2$。例如：

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

其高度小于其他备选方案的高度。使用这种方程计算同源需要更多工作，参见 [32]。

8. CONCLUSIONS

我们给出了许多计算 Charlap-Coley-Robbins 多项式的方法，包括将其表示为多项式的分式。在同源密码学中，当 ℓ较小时，它们很有用，只要我们存储 $(U_\ell, N_{\ell,A}, N_{\ell,B})$。若要计算一个同源，只需先计算 U_ℓ的一个根，再实例化三个多项式即可。

Atkin [1], 提出了另一种方法，即使用 U_ℓ的偏导数。这种方法见 [32]。

致谢。作者谨向 A. Bostan 和 F. Chyzak 致谢，感谢他们就本工作的若干方面进行的有益讨论；特别感谢前者提供了一份令人印象深刻的超几何函数快速求值参考文献清单。作者也感谢 L. De Feo 提供有关同源密码学应用的最新进展。

REFERENCES

[1] A. O. L. Atkin。《模素数椭圆曲线上的点数（II）》。草稿。可访问 http://listserv.nodak.edu/archives/nmbrthry.html，1992。

[2] B. C. Berndt。Ramanujan 关于艾森斯坦级数的公式。载于 *Number theory and related topics (Bombay, 1988)* 12 *Tata Inst. Fund. Res. Stud. Math.* ，卷号，第 23–29 页。Tata 基础研究所，孟买，1989年。[3] B. C. Berndt、H. H. Chan、J. Sohn 和 S. H. Son。Ramanujan 遗失的笔记本中的艾森斯坦级数。 *Ramanujan J.*，4(1):81–114，2000年。[4] B. C. Berndt 和 A. J. Yee。Ramanujan 对艾森斯坦级数的贡献，尤其是他遗失的笔记本中的相关内容。载于 *Number theoretic methods (Iizuka, 2001)* 8 *Dev.*，卷号，第 – 页。Kluwer 学术出版社，多德雷赫特，。[5] D. J. Bernstein。Pippenger 幂运算算法。https://cr.yp.to/papers.html，2002年1月。[6] I. Blake、G. Seroussi 和 N. Smart。 *Elliptic curves in cryptography*，第 265 卷，*London Math. Soc. Lecture Note Ser.* 剑桥大学出版社，1999年。[7] J. M. Borwein 和 P. B. Borwein。Jacobi 恒等式和算术几何平均的三次对应式。 *Trans. Amer. Math. Soc.*，323(2):691–701，1991年。[8] A. Bostan、F. Morain、B. Salvy 和 ́E. Schost。计算椭圆曲线间同源的快速算法。 *Math. Comp.*，77(263):1755–1778，2008年。[9] R. Brent 和 P. Zimmermann。 *Modern Computer Arithmetic*。剑桥大学出版社，2010年。[10] R. Br¨oker、K. E. Lauter 和 A. V. Sutherland。通过同源火山计算模多项式。 *Math. Comput.*，81(278):1201–1231，2012年。[11] W. Castryck、T. Lange、C. Martindale、L. Panny 和 J. Renes。CSIDH：一种高效的后量子交换群作用。载于 T. Peyrin 和 S. 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* 395 427 2018，，，，，卷号，第 – 页。施普林格，。[12] 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，1991年。[13] D. Charles 和 K. Lauter。模多项式计算。 *LMS J. Comput. Math.*，8 195: –204，2005年。[14] D. X. Charles、K. E. Lauter 和 E. Z. Goren。基于扩展图的密码哈希函数。 *J. Cryptol.*，22(1):93–113，2009年。[15] P. Cohen。椭圆模函数变换多项式的系数。 *Math. Proc. Cambridge Philos. Soc.*，95:389–402，1984年。[16] L. Comtet。 *Advanced Combinatorics*。D. Reidel 出版公司，1974年。[17] J.-M. Couveignes。困难齐性空间。密码学电子印本档案，报告 2006/291，2006年。http://eprint.iacr.org/2006/291。[18] R. Dupont。利用牛顿迭代和算术几何平均快速求值模函数。 *Math. Comp.*，80(275):1823–1847，2011年。[19] A. El Basraoui 和 A. Sebbar。艾森斯坦级数 E_2 *Proc. Amer. Math. Soc.* 138 7 2289 2299, 2010 的零点。，( ): – 。[20] 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* 第 卷，第 21–76 页。美国数学会、国际出版社，1998年。[21] A. Enge。准线性时间内计算模多项式。 *Math. Comp.*，78 267 1809 1824, 2009 ( ): – 。[22] A. Enge、W. Hart 和 F. Johansson。用于 θ 函数的短加法序列。 *J. Integer Seq.*，21(2):第 18.2.4 条，34，2018年。[23] A. Erd´elyi，编。 *Higher transcendental functions*，第 II 卷。麦格劳-希尔，1953年。[24] L. D. Feo、J. Kieffer 和 B. Smith。迈向基于普通同源图的实用密钥交换。载于 T. Peyrin 和 S. 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, Lecture Notes in Computer Science*第 11274 卷，页码 365–394。施普林格，2018 年。[25] L. D. Feo、D. Kohel、A. Leroux、C. Petit 和 B. Wesolowski。Sqisign：基于四元数和同源的紧凑型后量子签名。载于 S. Moriai 和 H. 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 Proceedings Part I* 12491 *Lecture* , , , , , 卷，*Notes in Computer Science* 64 93 2020 页码 – 。施普林格，。[26] D. Jao 和 L. De Feo。基于超奇异椭圆曲线同源构建抗量子密码系统。载于 B. Yang 编，*Post-Quantum Cryptography - 4th In-ternational Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings* 7071 *Lecture Notes in Computer Science* 19 34 , 卷，页码 – 。施普林格，2011 年。[27] F. Johansson。严格计算超几何函数。*ACM Trans. Math.* , ( ): 。*Softw.* 45 3 30, 2019

[28] M. Kaneko 和 D. Zagier。超奇异 j-不变量、超几何级数与 Atkin 正交多项式。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，页码 97–126。美国数学会、国际出版社，1998 年。[29] M. Kaneko 和 M. Koike。关于由超几何型微分方程导出的模形式。*Ramanujan J.*, 7(1-3):145–164，2003 年。Rankin 纪念专辑。[30] H. Labrande。准线性时间计算雅可比 theta 函数。*Math. Comp.*, 87 311 1479 1508, 2018 ( ): – 。[31] M. Mezzarobba 和 B. Salvy。p- 递归序列的有效界。*J. Symb.* , ( ): – 。*Comput.* 45 10 1075 1096, 2010

[32] F. Morain。使用 Charlap-Coley-Robbins 多项式计算椭圆曲线之间的同源。准备中，2023 年 2 月。[33] M. Noro、M. Yasuda 和 K. Yokoyama。利用 V´elu 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。[34] N. Pippenger。关于幂和单项式的求值。*SIAM J. Comput.*, 9 2 230 250, 1980 ( ): – 。[35] A. Poteaux 和 ´E. Schost。三角集模下的模复合及其应用。*Comput. Complexity*, 22(3):463–516，2013 年。[36] R. A. Rankin。*Modular forms and functions*。剑桥大学出版社，1977 年。[37] A. Rostovtsev 和 A. Stolbunov。基于同源的公钥密码系统。Cryptology ePrint Archive，报告 2006/145，2006 年。http://eprint.iacr.org/。[38] R. Schoof。有限域上椭圆曲线的点计数。*J. Théor. Nombres* , : – 。*Bordeaux* 7 219 254, 1995

[39] A. V. Sutherland。关于模多项式的求值。载于 *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium* 1 *Open* , 卷，页码 – 。*Book Ser.* 531 555 2013 Math. Sci. Publ.，美国加利福尼亚州伯克利，。[40] J. van der Hoeven。全纯函数的快速求值。*Theor. Comput. Sci.*, 210 1 199 215, 1999 ( ): – 。[41] J. van der Hoeven。正则奇点附近及其中全纯函数的快速求值。*J. Symb. Comput.*, 31(6):717–743，2001 年。

Appendix附录 A. Some values of U_ℓ, etc.

请注意，与 [33] 相比，这里存在符号翻转，这是因为采用了不同于参考文献、但其他文章中使用的归一化方式。

对于 $\ell = 3$, 我们计算

$$V_3(X, A, B) = X^4 - 84AX^3 + 246A^2X^2 + (63756A^3 + 432000B^2)X$$
$$+576081A^4 + 3888000AB^2,$$
$$W_3(X, A, B) = X^4 + 732BX^3 + (25088A^3 + 171534B^2)X^2$$
$$+(1630720A^3B + 11009548B^3)X - 139150592A^3B^2 - 437245479B^4$$
$$-\frac{297493504}{27}A^6;$$
$$N_{3,A}(X, A, B) = 84X^3A - 360X^2B - 76XA^2 + 36AB,$$
$$N_{3,B}(X, A, B) = 732X^3B + \frac{1456}{3}X^2A^2 - 724XAB - \frac{112}{3}A^3 + 108B^2.$$
$$N_{5,A} = 630AX^5 - 9360BX^4 - 8240A^2X^3 + 24480BAX^2$$
$$+(1120A^3 - 28800B^2)X - 3200BA^2,$$
$$N_{5,B} = 15630\,X^5B + 34720\,X^4A^2 - 208240\,X^3AB$$
$$+\left(-76160\,A^3 + 110400\,B^2\right)X^2 + 138720\,XA^2B - 83200\,AB^2.$$

对于 P 具有有理系数的多项式, 我们用各系数绝对值所需位数之和 S 来近似其大小。例如, 按照这一标准, 我们得到 $S(U_5) = 36$。(U_5,$N_{5,\ A}$, $N_{5,\ B}$) 的总和为 $36 + 91 + 117 = 244$, 相比之下, $S(V_5) = 349$, $S(W_5) = 602$; $S(\Phi_5^t) = 2838$, $S(\Phi_5^c) = 55$。我们注意到 $S_{tot}(\ell) = S(U_\ell) + S($ $N_{\ell,\ A}) + S(N_{\ell,\ B})$。

ℓ	$\tilde{H}(V_\ell)$	$\tilde{H}(W_\ell)$	$\tilde{H}(N_{\ell,\ A})$	$\tilde{H}(N_{\ell,\ B})$	$S_{tot}(\ell)$
5	3.266	4.336	1.063	1.268	244
7	3.050	4.207	0.973	1.167	551
11	2.939	3.979	0.896	1.016	1816
13	2.856	3.969	0.864	0.983	2684
17	2.770	3.883	0.831	0.919	5762
19	2.754	3.831	0.820	0.901	7866
23	2.723	3.764	0.799	0.869	13632
101	2.471	3.527	0.801	0.818	1187388
103	2.469	3.517	0.801	0.818	1262059
107	2.466	3.516	0.803	0.819	1422237
109	2.467	3.515	0.803	0.819	1504765

AppendixB. Numerical data for the isogeny volcano algorithm

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

i	$\mathcal{E}_i = [A_i, B_i]$	$\mathcal{E}_i^*$	$\sigma(\mathcal{E}_i^*)$
1	$[1582, 902]$	$[594, 422]$	226
		$[1543, 911]$	1542
		$[937, 1244]$	1283
		$[1333, 561]$	1691
		$[879, 342]$	1212
		$[757, 1578]$	1290
2	$[1662, 405]$	$[1770, 433]$	529
		$[1439, 1411]$	1536
		$[259, 355]$	1810
		$[382, 1793]$	1733
		$[1472, 543]$	433
		$[413, 1603]$	1203
3	$[1451, 1331]$	$[1096, 1433]$	743
		$[1371, 1367]$	98
		$[1105, 1195]$	207
		$[1657, 1699]$	787
		$[811, 812]$	1769
		$[779, 1311]$	18
4	$[1013, 747]$	$[1691, 473]$	1705
		$[509, 342]$	1245
		$[1642, 417]$	1406
		$[127, 765]$	1519
		$[905, 1464]$	145
		$[1277, 254]$	1224
5	$[224, 753]$	$[1485, 892]$	1566
		$[823, 1106]$	908
		$[397, 1451]$	1729
		$[131, 673]$	450
		$[654, 1798]$	1353
		$[1805, 1025]$	1238
6	$[1128, 1504]$	$[1275, 1672]$	1176
		$[1409, 761]$	1362
		$[907, 1757]$	309
		$[824, 1267]$	781
		$[578, 1320]$	1208
		$[1168, 1207]$	597
7	$[91, 725]$	$[1184, 542]$	1284
		$[1753, 297]$	859
		$[1440, 1524]$	1268
		$[421, 410]$	517
		$[1626, 1013]$	245
		$[198, 159]$	1260

TABLE 1. $\ell = 5$ 和 $p = 1811$的取值。