arXiv:2303.03270v1 [math.AG] 6 Mar 2023

K3曲面上的二次剩余模式与点计数

VALENTINA KIRITCHENKO[1,2], MIKHAIL TSFASMAN[2,3], SERGE VL ˘ADUŢ[4], 以及 ILYA ZAKHAREVICH[5]

谨以此文纪念 Lydia Goncharova。

Abstract. 早在19世纪，人们就开始研究模素数的二次剩余模式。我们陈述 Lydia Goncharova 最后一项未发表的结果，用代数几何的语言重新表述该结果及此前的相关结果，并给出证明。该定理的核心是 K3 曲面上的点的数量与复乘椭圆曲线上的点的数量之间一种出人意料的联系。

1. Introduction

自19世纪以来，人们一直在研究模素数的二次剩余与非剩余所形成的模式 [A, St, J]，当代数学家仍对此兴趣不减 [C, MT]。即便是关于二次（非）剩余分布的最基本问题，也会引出数论中的难题和深刻结果。例如，给定一个正整数 ℓ，是否存在一个素数 p 以及一个 ℓ-元连续整数组，其取值介于 1 和 $p-1$ 之间，使得该ℓ-元组中的数模 p全为二次非剩余（或二次剩余）？ 模 p的最小二次非剩余又有多大?

在本文中，我们提出一个关于已故友人 Lydia（Lida）Goncharova 所得二次（非）剩余模式的新结果（定理 2.2）。我们从她与第一作者于 2019 年 12 月的谈话，以及她早期的笔记和电子邮件往来中，部分还原了这一结果。我们感谢 David Kazhdan 帮助我们还原定义 2。遗憾的是，Lida 没有写下其定理的完整证明，但我们成功找到了这一结果的证明。

作为附带结果，我们得到一个具有如下性质的 K3 曲面 X。在含有 p 个元素的有限域 X 上进行点计数，可归结为对具有复乘的椭圆曲线进行点计数。

在第 2 节中，我们按照 Lida 的原文方式陈述她的结果。在第 3 节中，我们从几何视角重新表述她的结果，将其置于更一般的背景下，并给出证明。

关键词和短语：二次剩余、椭圆曲线、K3 曲面。

2. Quadratic residue patterns

设 p 是奇素数。考虑数列 1, 2, . . . , $p-1$。如果数列中的每个数 i 是模 p 的二次剩余，就将其替换为字母 R ；否则替换为字母 N。将所得的词记作 W_p。

定义 1. 设 S 是一个长度为 $\ell \le p-1$ 的词，其中仅包含 R 和 N。定义 $n_p(S)$ 为 W_p 中与 S 相同、且由 W_p 的 ℓ 个连续元素构成的子词数量。

例 2.1. 设 $p = 17$。则 $W_p = RRNRNNNRRNNNRNRR$。若 $\ell = 3$，则对于所有长度为 3 的词 S （ $S = RRR$ 除外），均有 $n_p(S) = 2$，而 $n_p(RRR) = 0$。

注意，若 $\ell = 1$，则 $n_p(S) = \frac{p-1}{2}$。事实上， $n_p(R) = n_p(N)$，因为二次剩余的数量等于非剩余的数量；并且 $n_p(R)+n_p(N) = p-1$。对于 $\ell = 2$，也有一些显式公式可以用初等技巧证明[A，定理 1]。对于 $\ell = 3$，4，某些线性组合有简单的显式公式，例如 $n_p(RRR) + n_p(NNN)$ [A，St]。若 $p = 4k+3$ 且 $\ell = 3$，则 $n_p(S)$ [J，第三部分，公式 I]也有简单公式。然而，若 $p = 4k+1$，则 $n_p(RRR)$ 的公式涉及一个更复杂的要素。具体而言，按以下公式定义函数 $J(k)$

$$J(k) = \sum_{i=1}^{4k-2} \left(\frac{i(i+1)(i+2)}{p}\right),$$

其中 $\left(\frac{a}{p}\right)$ 表示勒让德符号。

若 $p = 4k+1$ 且 $\ell = 3$，那么所有八个函数 $n_p(S)$ 都可以很容易地用 $J(k)$ [J, 第三部分，公式 II] 表示。这与高斯最后一项密切相关（参见 [M]，其中有简短的初等论述）。Jacobstahl 还证明，$J^2(k)$ 4 是将 p 分解为两个平方数之和时的一个加项 [J, 第二部分]。特别是，Jacobstahl 对 $n_p(S)$ 公式的证明也可视为高斯最后一项的第一个证明。从更几何的角度看， $n_p(S)$ 可以通过对一条具有复乘（CM）的椭圆曲线进行点计数来计算。我们将在例 3.1 中重新讨论这一方法。

若 $\ell \ge 4$，情况就更加复杂了。例如， $n_p(RRRR)$ 的一个（非显式）公式涉及对非复乘椭圆曲线进行点计数（参见第 3 节）。现在我们考虑一个关于剩余四元组的不同问题，它仍然可以用 $J(k)$ 来求解。

令 $A = (a_1, a_2, a_3, a_4)$ 为模 p 的两两不同的剩余类四元组。我们不再假设它们是连续的。若 $p = 4k+1$，则可按照以下规则为 A 赋予一个图 Γ_A。考虑四个顶点 $v_1, \ldots, v_4$，当且仅当差值 $a_i - a_j$ 是模 p 的二次剩余时，连接 v_i 和 v_j 之间的一条边（由于 -1 是二次剩余，关于 $a_i - a_j$ 的这一条件对于 i 和 j 是对称的）。下文中，我们将可以通过彼此获得的四元组视为相同

即通过置换或加性平移获得的四元组；换言之，我们不区分 (a_1, a_2, a_3, a_4) 和 $(a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, a_{\sigma(4)})$，其中 $\sigma \in S_4$，也不区分 (a_1, a_2, a_3, a_4) 和 $(a_1 + a, a_2 + a, a_3 + a, a_4 + a)$，其中 a 是模 p的一个剩余类。

定义 2. 设 Γ 是一个有四个顶点的图。定义 $n_p(\Gamma)$ 为所有满足 Γ_A 与 Γ 在拓扑上等价的四元组 A 的数量。

由于有四个顶点的简单图有 11 种拓扑类型，因此对于每个 p，都有 11 个数 $n_p(\Gamma)$。

定理 2.2（Goncharova）。假设 $p = 4k + 1$。所有函数 $n_p(\Gamma)$（视为 k 的函数）都可以显式表示为 k 和 $d(k)$ 的多项式，其中

$$d(k) = \frac{J(k)^2 - 4}{32}.$$

特别地，如果 Γ 是一个有四个顶点的完全图，那么

$$n_p(\Gamma) = \frac{k(k-1)(k-4) + 2kd(k)}{24}. \tag{1}$$

Goncharova 曾给出该定理的一个初等证明，但我们无法从她的笔记中还原出这个证明。看来，[BE].中证明了类似性质的结果。

我们使用计算机检验了公式 (1) 对所有奇素数 $p < 20000$是否成立（见下文第 3 节中的公式 (2)）。在下一节中，我们将证明，可以通过计算 K3 曲面上的点来计算 $n_p(\Gamma)$。

3. Number of points on elliptic curves and K3 surfaces

现在我们解释数值 $n_p(S)$ 和 $n_p(\Gamma)$ 的几何意义。为简单起见，我们重点讨论以下情形：

$$S = \underbrace{RR \dots R}_{\ell}$$

并且 Γ 是一个有 ℓ 个顶点的完全图（其他情形完全类似）。

设 $\mathbb{F}_p$ 为含有 p 个元素的有限域。考虑曲线 $C \subset \mathbb{F}_p^{\ell}$ 由 $\ell - 1$ 个二次曲面相交得到：

$$x_2^2 - x_1^2 = 1, \quad x_3^2 - x_2^2 = 1, \dots, \quad x_\ell^2 - x_{\ell-1}^2 = 1.$$

那么，每个坐标均非零的点$(x_1, \dots, x_\ell) \in C$都会产生模 p的 ℓ元组$(x_1^2, x_2^2, \dots, x_\ell^2)$，其中各项为连续的二次剩余。考虑到$x_i$ 和 $-x_i$ 产生相同的二次剩余 x_i^2，我们得到

$$n_p(S) = \frac{\#C^\circ(\mathbb{F}_p)}{2^\ell},$$

其中 $C^\circ \subset C$ 由坐标均非零的点组成。根据伴随公式，C的亏格等于 $2^{\ell-2}(\ell - 3) + 1$。特别地，当$\ell = 2$时，C的亏格为 0。因此，$n_p(RR)$有一个简单的显式公式。

例 3.1. 若 $\ell = 3$，则 C 是三维仿射空间中两个二次曲面的交集。 C 的亏格为 1，也就是说， C 的射影闭包是一条椭圆曲线。利用二次曲面的有理参数化：

$$x_2 + x_1 = u, \quad x_2 - x_1 = u^{-1}; \quad x_3 + x_2 = v, \quad x_3 - x_2 = v^{-1},$$

由此可得， C 的射影闭包与由以下方程给出的平面曲线的射影闭包 E 同构：

$$u(v^2 - 1) = v(u^2 + 1).$$

由于这条曲线在 $\mathbb{C}$上有一个 4 阶自同构：

$$(u, v) \mapsto (iv, iu)$$

由此可得， E 是一条复乘椭圆曲线，且 End(E) = $\mathbb{Z}[i]$。事实上，若将$E(\mathbb{C})$表示为 $\mathbb{C}$除以格 L的商，则 L 有一个 4 阶自同构。因此， L 的基本平行四边形是正方形，且 $\mathbb{C}/L \simeq \mathbb{C}/\mathbb{Z}[i]$ (另见[S，例 III.4。4] 此处采用更代数化的方法)。

E 与具有以下魏尔斯特拉斯形式的椭圆曲线之间存在一个（在有理数上定义的）同构：

$$y^2 = x^3 - x.$$

同一条曲线在 [E] 上的爱德华兹形式 $\mathbb{C}$ 为

$$x^2 + y^2 = 1 - x^2y^2.$$

请注意，这与高斯最后一项中的方程完全相同。历史上，人们曾在研究椭圆 lemniscate 函数时研究该方程。如今，爱德华兹形式广泛应用于椭圆曲线密码学，因为它能让加法律的实现具有更高的计算效率。

根据高斯， E 在 $\mathbb{F}_p$ 模$p = 4k + 1$ 下爱德华兹形式的点的数量等于 $(a_p - 1)^2 + b_p^2$，其中 $a_p + b_pi$ 是 p 在高斯整数环 $\mathbb{Z}[i]$中的一个素因子。该素因子由条件 $a_p - 1 + b_pi$ 能被 $2 + 2i$ 整除而唯一确定。高斯的这一发现对复乘理论的发展至关重要（历史概述见 [V，第 3 节1]）。

注 3.2。利用 $n_p(RRR)$ 的公式（见 [J，第三部分] ），我们可以通过计算 $J(k)$（定义见上一节）在（魏尔斯特拉斯形式的）E 模 $\mathbb{F}_p$ （当 $p = 4k + 1$时）的点的数量，如下所示：

$$J(k) = \#E(\mathbb{F}_p) - p - 1.$$

另请注意， J（k）和 $2a_p$ 仅相差一个符号。它们之间的精确关系由[J，第二部分]确定：

$$2a_p = (-1)^{k+1}J(k).$$

特别是， E 的爱德华兹形式与魏尔斯特拉斯形式在有理数域上并不同构。

如果 $\ell = 4$，那么 C 的亏格为 5；不过，一个简单的技巧 [C，即定理 2 的证明。1]将 $n_p(S)$ 的计算化为对以下形式的 $(2^\ell - 1)$ 求和：

$$\sum_{a\in\mathbb{F}_p}\left(\frac{f_I(a)}{p}\right)$$

对于所有多项式 $f_I(a) = (a + i_1)\cdots(a_i + i_r)$，其中 $0 \le i_1 < \ldots < i_r \le \ell - 1$。因此，只需对由方程 $y^2 = f_I(x)$ 给出的所有曲线 $C_I \subset \mathbb{F}_p^2$ 进行点计数，其中 $I = (i_1, \ldots, i_r) \subset (0, \ldots, l - 1)$。对于 $\ell \le 4$，我们得到五条亏格1曲线（其余曲线的亏格为0）：

$$\text{(a) } y^2 = x(x+1)(x+2); \quad \text{(b) } y^2 = x(x+1)(x+3); \quad \text{(c) } y^2 = x(x+2)(x+3);$$

$$\text{(d) } y^2 = (x+1)(x+2)(x+3); \quad \text{(e) } y^2 = x(x+1)(x+2)(x+3).$$

曲线 (a) 和 (d) 在 $\mathbb{Q}$ 上同构，而曲线 (b) 和 (c) 在 $\mathbb{C}$ 上同构。虽然 (a) 和 (d) 是复乘曲线，但 (b)、(c) 和 (e) 不是。特别是，要描述数 $n_p(RRRR$ 随素数 p 变化时的统计规律，需要用到数论中的一个深刻结果，即萨托–泰特猜想（参见 [S，C 节。21]）。

简要回顾一下相应的结果。设 $E/\mathbb{Q}$ 为一条椭圆曲线，那么对于任意在 p 模 $E_p/\mathbb{F}_p$ 下具有良约化 p 的素数 p，我们有 $\#E(\mathbb{F}_p) = p+1-a_p(E)$，$a_p(E)$ $|a_p(E)| < 2\sqrt{p}$ 是 p-Frobenius 算子的迹。分为两种情况：

A. E 是一条 CM 曲线，即 $\mathrm{End}(E) \neq \mathbb{Z}$；B. $\mathrm{End}(E) = \mathbb{Z}$，也就是说，$E$ 不具有复乘。

我们可以考虑归一化迹 $t_E(p) := {}^{a_p(E)}{}_{2\sqrt{p}} \in I :=]-1, 1[$。它在情形 A 和 B 中的表现截然不同：

A. 序列

$$T(E) := \{t_E(p) : E \text{ 在 } p\} = \{Primes \setminus S(E)\} \text{ 模 } p\} = \{Primes \setminus S \text{ 下具有良约化}$$

对于一个有限素数集 $S(E)$，其关于勒贝格测度 dt 在 I 上是均匀分布的。

B. 序列 $T(E)$ 关于 I 上的“半圆”$d\mu$测度均匀分布，

$$d\mu(t) := \frac{2\sqrt{1-t^2}}{\pi}dt.$$

情形 A 的结果可由类域论、海克关于 E 通过 L-级数与 Grössencharakter 表示（全局）ζ函数的经典结果，以及由池原定理导出的标准分布结果得到，参见 Lang《数论》的最后一章 [La]。

情形 B 中的结果正是约 1960 年提出、并由[HSBT]完全证明的 Sato-Tate 猜想。

因此，对于 $n_p(RRRR)$，我们得到（在公式中各项相互独立这一非常合理的条件下）：

$$n_p(RRRR) = \frac{p-1}{16} + 2\sqrt{p}\xi + o(\sqrt{p})$$

对于 $\xi := b\lambda + c\lambda_{ST}$，其中 a、b、c、$b+c = 1-a$ 为有理正数，且 λ（分别地，λ_{ST} 是在 $]-1$ 上均匀分布的随机变量，$1[$（分别地，按照 ST 测度分布）。

如果 $\ell = 5$，那么同样的方法可以得到一条亏格为 2 的曲线（此外还能得到亏格更小的曲线）：

$$y^2 = x(x+1)(x+2)(x+3)(x+4).$$

然而，对这条曲线进行点计数可以归约为对椭圆曲线进行点计数。事实上，这条曲线有一个非双曲对合 σ： $x+2 \mapsto -(x+2)$ $y \mapsto iy$。因此，$n_p(S)$ 的统计仍可用椭圆曲线的 Sato–Tate 分布来计算。如果 $\ell = 6$，那么就存在无法化简的“实”亏格 2 曲线，也就是说，$n_p(S)$ 的统计将依赖于关于亏格 2 曲线的猜想性 Sato–Tate 分布（见 [Su，定理 4。8]），且无法归约到椭圆曲线的情形。对于 $\ell \geq 7$，当前数论工具甚至无法对 $n_p(S)$ 的统计给出猜想性的描述。

现在我们转向数 $n_p(\Gamma)$。为了从几何上诠释 $n_p(\Gamma)$，定义簇 $X_\Gamma \subset \mathbb{F}_p^\ell \times \mathbb{F}_p^d$，其中 $d := {}^{\ell}_{(\ell-1)\ 2}$。定义方程为

$$x_j - x_i = y_{i,j}^2, \quad 1 \leq i < j \leq \ell,$$

其中 $(x_1, \ldots, x_\ell)$ 是 $\mathbb{F}_p^\ell$ 中的坐标，而 $(y_{i,j})_{1\leq i<j\leq \ell}$ 是 $\mathbb{F}_p^d$ 中的坐标。考虑由所有坐标两两不同的点组成的子簇 $X_\Gamma^\circ \subset X_\Gamma$。由于置换群 S_ℓ 和加法群 $\mathbb{F}_p$ 在 X° 上有自然的自由作用，因此我们得到

$$n_p(\Gamma) = \frac{\#X^\circ(\mathbb{F}_p)}{\ell! 2^d p}.$$

注意，乘法群 $(\mathbb{F}_p^*)^2 \subset \mathbb{F}_p^*$ 也在 $X_\Gamma^\circ(\mathbb{F}_p)$ 上自由作用。对 $\mathbb{F}_p$ 和 $(\mathbb{F}_p^*)^2$ 的作用取商后，我们可以通过计算 $Y_\Gamma(\mathbb{F}_p)$ 上的点数来计算 $X_\Gamma^\circ(\mathbb{F}_p)$ 上的点数，其中 $Y_\Gamma \subset \mathbb{F}_p^\ell \times \mathbb{F}_p^d$ 由以下方程给出：

$$x_1 = 0,\ x_\ell = 1; \quad x_j - x_i = y_{i,j}^2, \quad 1 \leq i < j \leq \ell.$$

当 $\ell = 2$ 时，情形显然。若 $\ell = 3$，则 Y_Γ 是一对圆锥曲线，因此有一个关于 $n_p(\Gamma)$ 的简单公式。

定理 2.2 的证明 令 $\ell = 4$，则 Y_Γ 由两个 K3 曲面 S 的副本组成；该曲面是在 $\mathbb{F}_p^5$ 中三个二次曲面的交集：

$$y_{1,2}^2 + y_{2,3}^2 = y_{1,3}^2; \quad y_{2,3}^2 + y_{3,4}^2 = y_{2,4}^2; \quad y_{1,2}^2 + y_{2,3}^2 + y_{3,4}^2 = 1.$$

特别 特别地，如果 $p = 4k+1$，那么公式 (1) 等价于下面的公式 ：

$$\#S(\mathbb{F}_p) = (p-1)^2 + J(k)^2 + 4. \tag{2}$$

引理 3.3. 公式 (2) 等价于下面的公式 (5)。

证明。我们使用以下有理参数化来参数化定义 S 的前两个二次曲面:

$$y_{1,2} = (x^2-1)s, y_{2,3} = 2xs, y_{1,3} = (x^2+1)s,$$
$$y_{3,4} = (y^2-1)t, y_{2,3} = 2yt, y_{2,4} = (y^2+1)t,$$

若令 $z := ys^{-1}, s := ytx^{-1}$，则 $s = z/y, t = x/z, t/s = y/x$，第三个方程为

$$z^2 = (x^2y^2+1)(x^2+y^2),$$

该方程在一个 3 维空间中定义了一个奇异 K3 曲面 X。由此得到双有理映射

$$\phi : X \longrightarrow S, \psi : S \longrightarrow X,$$

由下式给出

$$y_{1,2} = (x^2-1)z/y, y_{2,3} = 2xsz/y, y_{1,3} = (x^2+1)z/y$$
$$y_{3,4} = (y^2-1)x/z, y_{2,3} = 2yx/z, y_{2,4} = (y^2+1)x/z,$$

对于 ϕ，以及

$$x = \frac{y_{2,3}}{y_{1,3}-y_{1,2}}, y = \frac{4y_{2,3}}{(y_{1,3}-y_{1,2})^2(y_{2,3}-y_{3,4})}, z = \frac{2y_{2,3}}{(y_{1,3}-y_{1,2})(y_{2,3}-y_{3,4})}$$

对于 ψ。这些映射在 $X \setminus D$ 和 $S \setminus D_1$之间建立了一一对应，其中除子D、D_1 分别由 $\{y = z = 0\}$ 和 $\{y_{1,3} - y_{1,2} = y_{2,3} = 0\}$给出。简单计算可知，$D$ 上有 $6p-4$ $\mathbb{F}_p$个有理点，而 D_1 上有 $2p-1$ 个这样的点，由此证明了所需的等价关系。□

定理 3.4。考虑 3 维空间中的仿射曲面 X，其方程为:

$$z^2 = (x^2y^2+1)(x^2+y^2), \tag{3}$$

以及由下列方程给出的仿射平面曲线 E：

$$y^2 = x^3 - x. \tag{4}$$

令 M_p 和 N_p分别表示方程 (3) 和 (4) 模素数 p的解的个数。则 M_p 和 N_p 满足以下恒等式:

$$M_p = (p+1)^2 + (N_p - p)^2 + 1. \tag{5}$$

证明。作变量代换 $x = x_1$、$y = tx_1$、$z = y_1x_1$ 后，可将曲面 X 替换为曲面 X'；在坐标 (x_1、y_1、t) 下，该曲面的方程为:

$$y_1^2 = (t^2x_1^4+1)(t^2+1). \tag{6}$$

容易验证,

$$\#X(\mathbb{F}_p) = \#X'(\mathbb{F}_p) + p.$$

现在我们分别统计 $X' \setminus X'_0$ 和 X'_0 上满足 $X'_0 := X' \cap (\{x_1 = 0\} \cup \{y_1 = 0\} \cup \{t = 0\})$ 的点。

根据容斥公式，我们得到：若 $p \equiv 1$ （模 4），则

$$\#X'_0(\mathbb{F}_p) = \#[X' \cap \{x_1 = 0\}](\mathbb{F}_p) + \#[X' \cap \{y_1 = 0\}](\mathbb{F}_p) + \#[X' \cap \{t = 0\}](\mathbb{F}_p) -$$

$$- \#[X' \cap \{x_1 = y_1 = 0\}](\mathbb{F}_p) \; - \; \#[X' \cap \{x_1 = t = 0\}](\mathbb{F}_p) \; = \\ = \; (p-1) + (4p-10) + 2p - 2 - 2 \; = \; 7p - 15$$

这里我们用到了 $X' \cap \{y_1 = t = 0\}$ 为空这一事实。

为了计算 $X' \setminus X'_0$ 上的点的数量，我们将 t 视为参数。若固定 t，则方程 (6) 定义了一条椭圆曲线 $X_t \subset X'$。这类曲线上的点的数量由 (t, t^2+1) 形成的二次剩余模式唯一确定。因此，需要考虑四种情形： RR, RN, NR, NN。在每种情形下，分别有四条椭圆曲线E_1, E_2, E_3, E_4，用于参数化点对 (t, t^2+1)。例如，若 (t, t^2+1) 的模式为 RR，则 $t = s^2$ 且 $t^2 + 1 = u^2$，其中 (s, u) 是平面曲线 E_1 上一个坐标均非零的点，该曲线由方程$u^2 = s^4 + 1$给出。显然，点 $(\pm s, \pm u)$ 和 $(\mp s, \pm u)$ 对应于 t的同一个值。因此，使点对 (t, t^2+1) 具有模式 RR 的 t 值的数量等于$_{14}\#E_1^\circ(\mathbb{F}_p)$，其中 E_1° 表示 $E_1 \setminus (\{s = 0\} \cup \{u = 0\})$。其余三种情形也有类似的等式。

有趣的是，对于由 E_i 参数化的所有 t 值，相应的椭圆曲线 X_t 在 $\mathbb{F}_p$ 上都同构于 E_i。例如，如果 t 和 t^2+1 是二次剩余，那么 X_t 通过变量代换 $x = sx_1$、 $y = u^{-1}y_1$ 同构于曲线 $y^2 = x^4 + 1$。因此，我们得到以下恒等式:

$$\#[X' \setminus X'_0](\mathbb{F}_p) = \frac{1}{4} \sum_{i=1}^{4} \#E_i^\circ(\mathbb{F}_p)^2$$

利用表 1 可知，对于 $p = 8k \pm 1$，右侧等于

$$\frac{1}{4}[(p-7+a)^2 + 2(p-3-a)^2 + (p+1+a)^2] = p^2 - 6p + 17 + a^2.$$

利用表 2 对 $p = 8k \pm 3$ 进行计算，得到相同的结果。还需指出，曲线 E_1 和 E 的弗罗贝尼乌斯迹仅相差一个符号。

曲线	∞ 处的点数	$u = 0$ 或 $s = 0$ 处的点数之和,		弗罗贝尼乌斯迹
$u^2 = s^4 + 1$	2	6	8	a
$\delta u^2 = s^4 + 1$	0	4	4	$-a$
$u^2 = \delta^2 s^4 + 1$	2	2	4	$-a$
$\delta u^2 = \delta^2 s^4 + 1$	0	0	0	a

TABLE 1. 情形 $p = 8k \pm 1$

这里及下文中， $\delta \in \mathbb{F}_p^*$ 表示一个二次非剩余。

□

曲线	∞处的点数	$u=0$ 或 $s=0$ 处的点数	弗罗贝尼乌斯迹之和	
$u^2=s^4+1$	2	2	4	a
$\delta u^2=s^4+1$	0	0	0	$-a$
$u^2=\delta^2 s^4+1$	2	6	8	$-a$
$\delta u^2=\delta^2 s^4+1$	0	4	4	a

TABLE 2. 情形 $p=8k\pm 3$

REFERENCES

[A] N.S. ALADOV,关于素数 ′在数列 $P1$ 中二次剩余与非剩余的分布，
Mat. Sb., 18 (1896), 第1期, 61–75[BE] B.C. BERNDT, R.J. EVANS, 高斯、雅可比与雅各布斯塔尔和, Journal of Number Theory, 11 (1979), 349–398[C] K. CONRAD, 素数模下的二次剩余模式, 预印本, 2014[E] H. M. EDWARDS, 椭圆曲线的一种标准形式, Bull. Amer. Math. Soc. (N.S.), 44 (2007), 第3期, 393–422[J] E. JACOBSTHAL, 二次剩余理论中一个公式的应用, Dissertation, Friedrich-Wilhelms-Universit¨at zu Berlin, 1906[HSBT] M. Harris、N. Shepherd-Barron 和 R. Taylor, 一族卡拉比–丘流形与潜在自守性, Ann. of Math. (2) 171 (2010), 第2期, 779–813[La] S. LANG, 代数数论[M] M.G. MONZINGO, 关于二次剩余与二次非剩余的连续三元组的分布及相关

Fibonacci Quart., 23 (1985), no. 2, 133–138[MT] K. MCGOWN AND E. TREVIÑO, 《最小二次非剩余》, 2019 年预印本[S] J.H. SILVERMAN, 《椭圆曲线算术》, 第 2 版, Springer, 2009 年[St] R. VON STERNECK, 关于素数的二次剩余与二次非剩余的分布, Mat. Sb., 20 (1898), no. 2, 269–284[Su] A.V. SUTHERLAND, 《Sato–Tate 分布》, Contemp. Math. 740 (2019), 197–248[V] S.G. VLĂDUŢ, 《克罗内克青年之梦与模函数》, Gordon and Breach Science Publ., 1991

[1]HSE UNIVERSITY, MOSCOW, RUSSIA [2]INSTITUTE FOR INFORMATION TRANSMISSION PROBLEMS, MOSCOW, RUSSIA
[3]INDEPENDENT UNIVERSITY OF MOSCOW, MOSCOW, RUSSIA [4]AIX MARSEILLE UNIVERSITÉ, CNRS, CENTRALE MARSEILLE, I2M UMR 7373, MAR-SEILLE, FRANCE [5]UNIVERSITY OF CALIFORNIA, BERKELEY, USA

电子邮箱地址：vkiritch@hse.ru 电子邮箱地址：
MTsfasman@yandex.ru 电子邮箱地址：
serge.vladuts@univ-amu.fr 电子邮箱地址：
ilya@math.berkeley.edu