

# The Watermark and Double Ladder Theorems

The discriminant group of the Néron–Severi lattice of a Fermat surface of prime degree

Rafael Amichis Luengo

Madrid, Spain · tretoef@gmail.com · 14 October 2026

## Abstract

Let  $S_m \subset \mathbb{P}^3$  be the complex Fermat surface  $x_0^m + x_1^m + x_2^m + x_3^m = 0$  of prime degree  $m \geq 5$ . Its Néron–Severi lattice  $\text{NS}(S_m)$  is generated by the classes of the  $3m^2$  lines on  $S_m$  (Schütt–Shioda–van Luijk, Degtyarev). We prove that

$$|\text{disc NS}(S_m)| = m^{3(m-3)^2} \quad (\text{the Watermark Theorem}),$$

which answers, for prime degree, the determinant question asked by Shioda in 1987, and we determine the discriminant group itself:

$$\text{NS}(S_m)^* / \text{NS}(S_m) \cong \begin{cases} (\mathbb{Z}/m)^{3m^2-24m+59} \times (\mathbb{Z}/m^2)^{3m-16}, & m \geq 7, \\ (\mathbb{Z}/5)^{10} \times \mathbb{Z}/25, & m = 5 \end{cases}$$

(the Double Ladder Theorem). The transcendental lattice of  $S_m$  has the same discriminant group. Both proofs work with the explicit integer intersection matrix  $G$  of the lines and use only elementary lattice arithmetic: the action of  $G$  on functions pulled back along the  $m+1$  pencils of directions of  $(\mathbb{Z}/m)^2$ , an explicit sublattice of  $\ker G$  of index  $m^{12}$ , and two index computations for the order; an integer identity  $GYG = 6m^2G$  for the exponent, and a factorization of  $G$  modulo  $m$  through twelve one-variable “shadows” for the number of cyclic factors of order  $m^2$ . The lattice statements of both theorems are checked in the proof assistant Lean 4 with the Mathlib library, with no axiom beyond the three standard ones; the identification of  $G$  with the intersection matrix of the lines is proved by hand and checked by computer. This work has not been refereed by a human expert.

## 1 Introduction

The Néron–Severi lattice of the Fermat surface has been a test case for the theory of algebraic cycles since Shioda’s work on Fermat varieties [11, 2, 13]. Let  $m \geq 5$  be prime and let  $S_m \subset \mathbb{P}^3(\mathbb{C})$  be the Fermat surface of degree  $m$ . It contains exactly  $3m^2$  lines. For  $m \leq 4$  or  $\gcd(m, 6) = 1$  their classes span  $\text{NS}(S_m) \otimes \mathbb{Q}$  [12] (see [10, §3]), and for  $\gcd(m, 6) = 1$  they generate  $\text{NS}(S_m)$  over  $\mathbb{Z}$ : Schütt, Shioda and van Luijk proved this for  $m \leq 100$  [10], and Degtyarev for every such  $m$  [4]. For prime  $m \geq 5$  the rank is  $\rho(S_m) = 3(m-1)(m-2) + 1$  [12, 2].

At the end of [13] (§7, pp. 133–134) Shioda asked whether  $|\det \text{NS}| = m^{3(m-3)^2}$  for the Fermat surface of prime degree  $m$ : Question 7.2 in characteristic  $p \equiv 1 \pmod{m}$ , and Question 7.4, formula (7.10), for the complex surface. Schütt, Shioda and van Luijk computed the determinant of the intersection form on their basis of lines for every odd  $m \leq 81$  and found  $m^{3(m-3)^2}$  [10, end of §4]. In 2015 Shioda still used the formula as expected, inside Conjecture 23 of [14]. Aljovin, Movasati and Villaflor computed by machine the elementary divisors of the lattice of the lines for  $3 \leq m \leq 14$  [1, Table 1]; for  $m = 5, 7, 11, 13$  their rows are

$$1^{26} 5^{10} 25, \quad 1^{48} 7^{38} 49^5, \quad 1^{96} 11^{158} 121^{17}, \quad 1^{120} 13^{254} 169^{23},$$

whose products are  $m^{3(m-3)^2}$ . We did not find a proof of the formula for general prime  $m$ , nor a description of the group for general  $m$ , in the literature that we read (§11).

**Theorem 1** (The Watermark Theorem). *For every prime  $m \geq 5$ , the lattice  $V$  spanned by the classes of the  $3m^2$  lines of  $S_m$ , with the intersection form, is free of rank  $3(m-1)(m-2) + 1$  and the Gram matrix of every  $\mathbb{Z}$ -basis of  $V$  has determinant  $m^{3(m-3)^2}$ . Hence  $|\text{disc NS}(S_m)| = m^{3(m-3)^2}$ .*

**Theorem 2** (The Double Ladder Theorem). *For every prime  $m \geq 7$ ,*

$$V^*/V \cong (\mathbb{Z}/m)^{3m^2-24m+59} \times (\mathbb{Z}/m^2)^{3m-16},$$

*and  $V^*/V \cong (\mathbb{Z}/5)^{10} \times \mathbb{Z}/25$  for  $m = 5$ . Here  $V^* = \text{Hom}(V, \mathbb{Z})$ , and  $V \subset V^*$  through the form.*

Since  $V = \text{NS}(S_m)$ , Theorem 2 is the discriminant group of the Néron–Severi lattice; Theorem 1 gives its order. The sign of the determinant in Theorem 1 is +: the form has signature  $(1, \rho - 1)$  and  $\rho - 1 = 3(m - 1)(m - 2)$  is even.<sup>1</sup> The four rows of [1, Table 1] quoted above are Theorem 2 at  $m = 5, 7, 11, 13$ .

**Corollary 3.** *For every prime  $m \geq 5$  the transcendental lattice  $T_m = \text{NS}(S_m)^\perp \subset H^2(S_m, \mathbb{Z})$  has rank  $(m - 1)(m - 3)^2$  and  $T_m^*/T_m \cong V^*/V$ ; in particular  $|\text{disc } T_m| = m^{3(m-3)^2}$ .*

*Proof.*  $H^2(S_m, \mathbb{Z})$  is torsion free and unimodular, since  $S_m$  is simply connected (Lefschetz) and by Poincaré duality, and  $\text{NS}(S_m) = H^2(S_m, \mathbb{Z}) \cap H^{1,1}$  is a primitive sublattice, so the discriminant groups of  $\text{NS}(S_m)$  and of its orthogonal complement are isomorphic [9, Prop. 1.6.1]. The second Betti number of a smooth surface of degree  $m$  in  $\mathbb{P}^3$  is  $m^3 - 4m^2 + 6m - 2$ , and  $m^3 - 4m^2 + 6m - 2 - (3m^2 - 9m + 7) = (m - 1)(m - 3)^2$ .  $\square$

**The proofs.** Everything is proved for an explicit integer matrix  $G$  of size  $3m^2$ , defined in §2; that  $G$  is the intersection matrix of the lines is the classical configuration, proved in §3. Theorem 1 is proved in §§4–8. The kernel  $K$  of  $G$  contains an explicit sublattice SAT with  $mK \subseteq \text{SAT}$  and  $[K : \text{SAT}] = m^{12}$  (the number 12 is a count of relations modulo  $m$ , Lemma 12); and  $A = \mathbb{Z}^{3m^2}$  contains an explicit sublattice  $F$ , the orthogonal direct sum of  $N_0$  and  $3(m - 2)$  blocks, whose image in  $V$  has index  $m^{3(m^2+m+2)/2-12}$ . Theorem 2 is proved in §9: the order is Theorem 1, the exponent divides  $m^2$  by an explicit integer identity  $GYG = 6m^2G$ , and the rank of  $G$  modulo  $m$  is  $12(m - 3)$  (and 26 at  $m = 5$ ).

**Lean.** The lattice statements of Theorems 1 and 2, for the matrix  $G$  of §2, are checked in Lean 4 with Mathlib (§10). The geometric identification of §3, the equality  $V = \text{NS}(S_m)$  [10, 4] and Corollary 3 are not formalized.

**Earlier versions.** Both theorems were first stated and proved in June 2026 by a different route, through the characters of  $(\mathbb{Z}/m)^3$ , trace lattices and a large determinant [15, 5]. Four steps of the June proof of Theorem 2 were confirmed by computation at three or four primes and not written for general  $m$ ; the proof printed here does not use them. The proof printed here is the integral route, without characters, along which the theorems were formalized in Lean; every step is written for general  $m$ .

**Notation.** Throughout,  $m \geq 5$  is prime,  $\mathbb{F}_m = \mathbb{Z}/m$ , and  $P = \mathbb{F}_m^2$ ; its elements are written  $(k, l)$ . For a function  $u : \mathbb{F}_m \rightarrow \mathbb{Z}$  write  $\Sigma u = \sum_{x \in \mathbb{F}_m} u(x)$ ;  $Z_0$  is the group of  $u$  with  $\Sigma u = 0$ , free of rank  $m - 1$ . For a commutative ring  $R$  and  $u : \mathbb{F}_m \rightarrow R$  put  $u^\pm(x) = u(x \pm 1)$ ; for  $c \in \mathbb{F}_m$ ,  $\delta_c : \mathbb{F}_m \rightarrow \mathbb{Z}$  is the indicator of  $c$ .

## 2 The configuration and the lattice

The set of *lines* is  $I = \{0, 1, 2\} \times P$ , so  $|I| = 3m^2$ ; the first coordinate is the *family*. Let  $A = \mathbb{Z}^I$  and define the symmetric matrix  $G \in \mathbb{Z}^{I \times I}$  by the following entries, for lines  $p = (j, k, l)$  and  $q = (j', k', l')$ :

<sup>1</sup>The row (2, 7) of [1, Table 1] (arXiv:1711.02628v2) prints the sign  $-$ ; the signature argument and a direct computation of the determinant both give  $+7^{48}$ .

- same family ( $j = j'$ ):  $G_{pp} = 2 - m$ ; for  $(k, l) \neq (k', l')$ ,  $G_{pq} = 1$  if  $k = k'$  or  $l = l'$ , and 0 otherwise;
- families 0 and 1 ( $j = 0, j' = 1$ ):  $G_{pq} = 1$  if  $k - l = k' - l'$ , else 0;
- families 1 and 2 ( $j = 1, j' = 2$ ):  $G_{pq} = 1$  if  $k + l = k' + l'$ , else 0;
- families 0 and 2 ( $j = 0, j' = 2$ ):  $G_{pq} = 1$  if  $k' - l' = k + l + 1$ , else 0;
- the remaining entries by symmetry,  $G_{qp} = G_{pq}$ .

All equalities are in  $\mathbb{F}_m$ . Let  $K = \ker G \subseteq A$  and  $V = A/K$ , with the form induced by  $B(x, y) = x^T G y$ ; it is well defined because  $G$  is symmetric. The group  $V$  is torsion free (if  $cx \in K$  with  $c \neq 0$  then  $x \in K$ ), hence free.

For  $j \in \{0, 1, 2\}$  let  $N_j \in A$  be the indicator of family  $j$ , and  $\mathbf{1} = N_0 + N_1 + N_2$ . For  $x \in A$  write  $x_j : P \rightarrow \mathbb{Z}$  for its restriction to family  $j$  and  $\text{aug}(x_j) = \sum_{p \in P} x_j(p)$ .

**Rows of  $G$ .** The row of  $G$  at  $p = (j, k, l)$  has  $2 - m$  at  $p$ , 1 at the  $2(m - 1)$  lines of family  $j$  that share  $k$  or  $l$  with  $p$ , and, in each other family  $j'$ , the value 1 exactly on an *incidence set*  $S_{j'}(p) \subset P$ :

$$\begin{array}{ll}
\text{family of } p & \\
0 : & S_1(p) = \{k' - l' = k - l\}, \quad S_2(p) = \{k' - l' = k + l + 1\}, \\
1 : & S_0(p) = \{k' - l' = k - l\}, \quad S_2(p) = \{k' + l' = k + l\}, \\
2 : & S_0(p) = \{k' + l' = k - l - 1\}, \quad S_1(p) = \{k' + l' = k + l\}.
\end{array}$$

Each incidence set is a “− set”  $\{k' - l' = c\}$  or a “+ set”  $\{k' + l' = c\}$ ; it has  $m$  points.

**Lemma 4.**  $GN_j = m\mathbf{1}$  for every  $j$ , and  $G\mathbf{1} = 3m\mathbf{1}$ .

*Proof.* At a line of family  $j$  the row sum over family  $j$  is  $(2 - m) + 2(m - 1) = m$ . At a line of another family the row meets family  $j$  in an incidence set, of  $m$  points.  $\square$

### 3 The geometry

This section identifies  $G$  with the intersection matrix of the lines on  $S_m$  and  $V$  with  $\text{NS}(S_m)$ . It is not used in §§4–9.

Put  $\varepsilon = e^{\pi i/m}$  and  $\zeta = \varepsilon^2 = e^{2\pi i/m}$ , so that  $\varepsilon^m = -1$ . For  $(a, b) \in \mathbb{F}_m^2$  the following lines lie on  $S_m$ :

$$\begin{array}{ll}
\text{family 0 :} & x_0 = \varepsilon \zeta^a x_1, \quad x_2 = \varepsilon \zeta^b x_3; \\
\text{family 1 :} & x_0 = \varepsilon \zeta^a x_2, \quad x_1 = \varepsilon \zeta^b x_3; \\
\text{family 2 :} & x_0 = \varepsilon \zeta^a x_3, \quad x_1 = \varepsilon \zeta^b x_2.
\end{array}$$

For instance on a line of family 0,  $x_0^m + x_1^m = (\varepsilon^m + 1)x_1^m = 0$  and likewise  $x_2^m + x_3^m = 0$ . These are the  $3m^2$  lines of  $S_m$  [10]; the line of family  $j$  with parameters  $(a, b)$  is the line  $(j, a, b) \in I$ .

**Proposition 5.** *The intersection number of the lines  $(j, a, b)$  and  $(j', c, d)$  on  $S_m$  is the entry of  $G$ .*

*Proof.* By adjunction a line  $L$  on  $S_m$  has  $L^2 = -2 - K_{S_m} \cdot L = -2 - (m - 4) = 2 - m$ . Two distinct lines on a smooth surface meet in at most one point, transversally, so their intersection number is 1 if they meet and 0 otherwise; they meet if and only if their four linear equations have a common non-zero solution. Two lines of one family meet if and only if they share  $a$  or  $b$ : for instance the lines of family 0 with the same  $a$  and different  $b$  meet at  $(\varepsilon \zeta^a : 1 : 0 : 0)$ , and if  $a \neq a'$  and  $b \neq b'$  the equations force  $x = 0$ . For families 0 and 1, with parameters  $(a, b)$  and  $(c, d)$ , a common point has  $x_3 \neq 0$  (otherwise all coordinates vanish) and

$x_0 = \varepsilon \zeta^a x_1 = \varepsilon^2 \zeta^{a+d} x_3$ ,  $x_0 = \varepsilon \zeta^c x_2 = \varepsilon^2 \zeta^{c+b} x_3$ ; so the lines meet if and only if  $a - b = c - d$ . In the same way families 1 and 2, with  $(c, d)$  and  $(e, f)$ , meet if and only if  $c + d = e + f$ . For families 0 and 2, with  $(a, b)$  and  $(e, f)$ , again  $x_3 \neq 0$  and  $x_0 = \varepsilon \zeta^a x_1 = \varepsilon^2 \zeta^{a+f} x_2 = \varepsilon^3 \zeta^{a+f+b} x_3$  and  $x_0 = \varepsilon \zeta^e x_3$ , so the lines meet if and only if  $\varepsilon^2 \zeta^{a+b+f} = \zeta^e$ , that is,  $e - f = a + b + 1$ . These are the entries of  $G$ ; the  $+1$  of the last case is  $\varepsilon^2 = \zeta$ .  $\square$

**Corollary 6.** *The lattice spanned by the classes of the lines in  $H^2(S_m, \mathbb{Z})$ , with the intersection form, is isometric to  $V$ . For prime  $m \geq 5$  it is  $\text{NS}(S_m)$ .*

*Proof.* The classes of the lines span  $\text{NS}(S_m) \otimes \mathbb{Q}$  for  $\gcd(m, 6) = 1$  [12] (see [10, §3]),  $H^2(S_m, \mathbb{Z})$  is torsion free, as  $S_m$  is simply connected, and the intersection form on  $\text{NS}(S_m)$  is non-degenerate (Hodge index theorem). So a combination  $x \in A$  of lines has class 0 if and only if it pairs to zero with every line, that is,  $Gx = 0$ , by Proposition 5. Hence the lattice of the lines is  $A/\ker G = V$  with the form of  $G$ . For  $\gcd(m, 6) = 1$  the lines generate  $\text{NS}(S_m)$  [10, 4].  $\square$

The proof of Proposition 5 was also checked by computer: for  $m = 5, 7, 11$  the lines were built numerically and every pair of distinct lines was tested for a common point (rank of a  $4 \times 4$  complex matrix); all 2775, 10731 and 65703 such pairs agree with  $G$  (the diagonal entries  $2 - m$  come from adjunction), and the same test with  $k + l - 1$  in place of  $k + l + 1$  in the last case disagrees on 250, 686 and 2662 pairs.

## 4 Pencils and pullbacks

For  $t \in \mathbb{F}_m$  let  $\pi_t(k, l) = k + tl$ , and let  $\pi_\infty(k, l) = l$ . These are the  $m + 1$  *pencils*: the linear forms on  $P$  up to scalars. We call  $\pi_0 = k$  and  $\pi_\infty = l$  the *axis pencils*,  $\pi_1 = k + l$  and  $\pi_{-1} = k - l$  the *overlap pencils*, and the  $m - 3$  others the *live pencils*. For a family  $j$ , a pencil  $\pi$  and  $u : \mathbb{F}_m \rightarrow \mathbb{Z}$ , the *pullback*  $\text{pb}_j^\pi(u) \in A$  is  $u \circ \pi$  on family  $j$  and 0 elsewhere. For  $y : P \rightarrow \mathbb{Z}$  the *fibre sums* are  $\text{fib}_\pi(y)(v) = \sum_{\pi(p)=v} y(p)$ . (The names R.1, R.2 and C given below to three lemmas are those of the Lean project, §10.)

**Lemma 7.** *Let  $\pi \neq \pi'$  be pencils and  $u, v : \mathbb{F}_m \rightarrow \mathbb{Z}$ . Then  $\sum_{p \in P} u(\pi(p))v(\pi'(p)) = (\sum u)(\sum v)$  and  $\sum_{p \in P} u(\pi(p))v(\pi(p)) = m \sum_x u(x)v(x)$ . In particular every fibre of  $\pi$  meets every fibre of  $\pi'$  in exactly one point.*

*Proof.* Two non-proportional linear forms on  $\mathbb{F}_m^2$  give a bijection  $p \mapsto (\pi(p), \pi'(p))$  of  $P$  onto  $\mathbb{F}_m^2$ ; every fibre of one pencil has  $m$  points.  $\square$

**Lemma 8** (Lemma R.1). *For every  $y : P \rightarrow \mathbb{Z}$  and every family  $j$ ,*

$$m \cdot y|_{\text{family } j} = \sum_{\pi} \text{pb}_j^\pi(\text{fib}_\pi(y)) - \left( \sum_p y(p) \right) N_j,$$

*the sum running over the  $m + 1$  pencils (here  $y|_{\text{family } j} \in A$  is  $y$  on family  $j$  and 0 elsewhere).*

*Proof.* At  $(j, p)$  the right side is  $\sum_{\pi} \sum_{\pi(q)=\pi(p)} y(q) - \sum_q y(q)$ . A point  $q \neq p$  lies on the same fibre as  $p$  for exactly one pencil, the one containing the direction  $q - p$ ; the point  $p$  does so for all  $m + 1$ . So the double sum is  $(m + 1)y(p) + \sum_{q \neq p} y(q)$ .  $\square$

**Lemma 9** ( $G$  on pullbacks). *Let  $u \in Z_0$ .*

- (a) *Axis pencils:  $G \text{ pb}_j^{\pi_0}(u) = G \text{ pb}_j^{\pi_\infty}(u) = 0$  for every  $j$ .*
- (b) *Live pencils:  $G \text{ pb}_j^{\pi_t}(u) = -m \text{ pb}_j^{\pi_t}(u)$  for  $t \notin \{0, 1, -1\}$  and every  $j$ .*

(c) *Overlap pencils:*

$$\begin{aligned} G \text{pb}_0^{\pi^{-1}}(u) &= -m \text{pb}_0^{\pi^{-1}}(u) + m \text{pb}_1^{\pi^{-1}}(u), & G \text{pb}_1^{\pi^{-1}}(u) &= -m \text{pb}_1^{\pi^{-1}}(u) + m \text{pb}_0^{\pi^{-1}}(u), \\ G \text{pb}_1^{\pi_1}(u) &= -m \text{pb}_1^{\pi_1}(u) + m \text{pb}_2^{\pi_1}(u), & G \text{pb}_2^{\pi_1}(u) &= -m \text{pb}_2^{\pi_1}(u) + m \text{pb}_1^{\pi_1}(u), \\ G \text{pb}_0^{\pi_1}(u) &= -m \text{pb}_0^{\pi_1}(u) + m \text{pb}_2^{\pi_1}(u^-), & G \text{pb}_2^{\pi_1}(u) &= -m \text{pb}_2^{\pi_1}(u) + m \text{pb}_0^{\pi_1}(u^+). \end{aligned}$$

*Proof.* Let  $v = \text{pb}_j^\pi(u)$  and look at  $(Gv)(q)$ .

*Lines  $q = (j, k, l)$  of family  $j$ .* If  $\pi$  is an axis pencil, say  $\pi = \pi_0$ , the entry is  $(2 - m)u(k) + (m - 1)u(k) + \sum_{k' \neq k} u(k') = \Sigma u = 0$ ; likewise for  $\pi_\infty$ . If  $\pi = \pi_t$  with  $t \neq 0$ , the row  $\{k' = k\}$  and the column  $\{l' = l\}$  each meet every fibre of  $\pi$  once, so with  $x = \pi(k, l)$  the entry is  $(2 - m)u(x) + 2(\Sigma u - u(x)) = -mu(x)$ .

*Lines  $q$  of another family.* The entry is the sum of  $u \circ \pi$  over an incidence set  $S$ . On a  $-$  set  $\{k' - l' = c\}$ ,  $\pi_t$  takes the values  $(1 + t)l' + c$ , a bijection onto  $\mathbb{F}_m$  unless  $t = -1$ ; on a  $+$  set  $\{k' + l' = c\}$ ,  $\pi_t$  takes the values  $(1 - t)k' + tc$ , a bijection unless  $t = 1$ ;  $\pi_0 = k'$  and  $\pi_\infty = l'$  are bijections on both kinds. A bijection gives  $\Sigma u = 0$ . In the two remaining cases ( $\pi_{-1}$  on a  $-$  set,  $\pi_1$  on a  $+$  set)  $\pi$  is constant on  $S$  and the entry is  $m u(\text{value})$ . Reading the value off the table of incidence sets gives the six formulas; for example, for  $v = \text{pb}_0^{\pi_1}(u)$  and  $q = (2, k, l)$  the set is  $S_0(q) = \{k' + l' = k - l - 1\}$ , so the entry is  $m u(k - l - 1) = m u^-(k - l)$ ; for  $v = \text{pb}_2^{\pi_1}(u)$  and  $q = (0, k, l)$  it is  $S_2(q) = \{k' - l' = k + l + 1\}$ , giving  $m u^+(k + l)$ .  $\square$

The three *overlap pairs* are  $(\text{pb}_0^{\pi^{-1}}, \text{pb}_1^{\pi^{-1}})$ ,  $(\text{pb}_1^{\pi_1}, \text{pb}_2^{\pi_1})$  and  $(\text{pb}_0^{\pi_1}, \text{pb}_2^{\pi_1})$ , the last one with a shift by one.

## 5 The sublattice SAT of the kernel

**Definition 10.** Let  $R$  be a commutative ring. A *datum* over  $R$  consists of functions  $a_j, b_j : \mathbb{F}_m \rightarrow R$  ( $j = 0, 1, 2$ ),  $w_0, w_1, w_2 : \mathbb{F}_m \rightarrow R$ , and scalars  $\varepsilon_1, \varepsilon_2 \in R$ . It is *admissible* if each of the nine functions  $a_j, b_j, w_i$  has sum zero; the admissible data form a free  $R$ -module  $\text{Src}_R$  of rank  $9(m - 1) + 2 = 9m - 7$ . The map  $s_R : \text{Src}_R \rightarrow R^I$  sends a datum to the vector with values

$$\begin{aligned} (0, k, l) &\mapsto a_0(k) + b_0(l) + w_0(k - l) + w_2(k + l) + \varepsilon_1, \\ (1, k, l) &\mapsto a_1(k) + b_1(l) + w_0(k - l) + w_1(k + l) + \varepsilon_2 - \varepsilon_1, \\ (2, k, l) &\mapsto a_2(k) + b_2(l) + w_1(k + l) + w_2(k - l - 1) - \varepsilon_2. \end{aligned}$$

Put  $\text{SAT} = s_{\mathbb{Z}}(\text{Src}_{\mathbb{Z}}) \subseteq A$ .

In terms of pullbacks,  $s_{\mathbb{Z}}$  of a datum is

$$\begin{aligned} \sum_j (\text{pb}_j^{\pi_0}(a_j) + \text{pb}_j^{\pi_\infty}(b_j)) &+ (\text{pb}_0^{\pi^{-1}} + \text{pb}_1^{\pi^{-1}})(w_0) + (\text{pb}_1^{\pi_1} + \text{pb}_2^{\pi_1})(w_1) \\ &+ \text{pb}_0^{\pi_1}(w_2) + \text{pb}_2^{\pi_1}(w_2^-) + \varepsilon_1(N_0 - N_1) + \varepsilon_2(N_1 - N_2). \end{aligned}$$

**Lemma 11.**  $\text{SAT} \subseteq K$ .

*Proof.* By Lemma 9(a),  $G$  kills the axis pullbacks. For the first overlap pair, Lemma 9(c) gives

$$G(\text{pb}_0^{\pi^{-1}} + \text{pb}_1^{\pi^{-1}})(w_0) = (-m + m) \text{pb}_0^{\pi^{-1}}(w_0) + (m - m) \text{pb}_1^{\pi^{-1}}(w_0) = 0,$$

and likewise for the second. For the third,  $G \text{pb}_0^{\pi_1}(w_2) = -m \text{pb}_0^{\pi_1}(w_2) + m \text{pb}_2^{\pi_1}(w_2^-)$  and  $G \text{pb}_2^{\pi_1}(w_2^-) = -m \text{pb}_2^{\pi_1}(w_2^-) + m \text{pb}_0^{\pi_1}(w_2)$ , since  $(w_2^-)^+ = w_2$ ; the sum is 0. Finally  $G(N_0 - N_1) = G(N_1 - N_2) = 0$  by Lemma 4.  $\square$

**Lemma 12** (Lemma C: the count of relations). *The kernel of  $s_{\mathbb{F}_m} : \text{Src}_{\mathbb{F}_m} \rightarrow \mathbb{F}_m^I$  has dimension 12; hence its image has dimension  $9m - 19$ .*

*Proof.* Let  $\Theta$  be an admissible datum over  $\mathbb{F}_m$  with  $s_{\mathbb{F}_m}(\Theta) = 0$ , so that the three displayed functions of  $(k, l)$  vanish identically. For  $\Phi : P \rightarrow \mathbb{F}_m$  put  $(\square\Phi)(k, l) = \Phi(k+1, l+1) - \Phi(k+1, l) - \Phi(k, l+1) + \Phi(k, l)$ , and for  $w : \mathbb{F}_m \rightarrow \mathbb{F}_m$  put  $(\Delta^2 w)(z) = w(z+2) - 2w(z+1) + w(z)$ . The operator  $\square$  kills functions of  $k$  alone, of  $l$  alone, and constants, and a direct computation gives  $\square[w(k-l)] = -(\Delta^2 w)(k-l-1)$  and  $\square[w(k+l)] = (\Delta^2 w)(k+l)$ .

Applying  $\square$  to the three identities gives, for all  $k, l$ :

$$\begin{aligned} (\Delta^2 w_2)(k+l) &= (\Delta^2 w_0)(k-l-1), & (\Delta^2 w_1)(k+l) &= (\Delta^2 w_0)(k-l-1), \\ (\Delta^2 w_1)(k+l) &= (\Delta^2 w_2)(k-l-2). \end{aligned}$$

Since  $m$  is odd,  $(k, l) \mapsto (k+l, k-l)$  is a bijection of  $P$ , so each of these says that both sides are one and the same constant. Hence  $\Delta^2 w_0 = \Delta^2 w_1 = \Delta^2 w_2 = 2c$  for one  $c \in \mathbb{F}_m$ . As  $\Delta^2(x^2) = 2$ , the function  $w_i - cx^2$  has zero second difference, so its first difference is a constant  $\alpha_i$  and  $w_i(x) = cx^2 + \alpha_i x + \beta_i$  for all  $x \in \mathbb{F}_m$ .

With these  $w_i$  the cross terms cancel,  $(k-l)^2 + (k+l)^2 = 2k^2 + 2l^2$  and  $(k+l)^2 + (k-l-1)^2 = 2k^2 + 2l^2 - 2k + 2l + 1$ , so each identity reads  $a_j(k) + b_j(l) = p_j(k) + q_j(l)$  with explicit quadratic polynomials  $p_j, q_j$ . Its solutions are exactly  $a_j = p_j + t_j$ ,  $b_j = q_j - t_j$  with  $t_j \in \mathbb{F}_m$  (put  $l = 0$ , then  $k = 0$ ).

Conversely every such choice is admissible: a quadratic function on  $\mathbb{F}_m$  has sum zero, because  $\sum_x 1 = m$ ,  $\sum_x x = m(m-1)/2$  and  $\sum_x x^2 = (m-1)m(2m-1)/6$  vanish in  $\mathbb{F}_m$  ( $\gcd(m, 6) = 1$ ). So the kernel is the image of the injective linear map from  $\mathbb{F}_m^{12}$  sending  $(c, \alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, \beta_2, \varepsilon_1, \varepsilon_2, t_0, t_1, t_2)$  to the datum just described. Injectivity:  $c, \alpha_i, \beta_i$  are read off the  $w_i$ ,  $t_j$  off  $a_j(0)$ , and  $\varepsilon_1, \varepsilon_2$  are coordinates of the datum.  $\square$

*Remark 13.* At  $m = 3$  the count drops to 11 because  $\sum_{x \in \mathbb{F}_3} x^2 \neq 0$ ; this is one of the places where  $m \geq 5$  is used.

**Lemma 14.** *Reduction modulo  $m$  maps  $\text{Src}_{\mathbb{Z}}$  onto  $\text{Src}_{\mathbb{F}_m}$ , and  $s_{\mathbb{F}_m}(\Theta \bmod m) = s_{\mathbb{Z}}(\Theta) \bmod m$  for  $\Theta \in \text{Src}_{\mathbb{Z}}$ .*

*Proof.* The second statement holds because reduction is a ring map. For the first, lift a sum-zero  $f : \mathbb{F}_m \rightarrow \mathbb{F}_m$  to any  $y : \mathbb{F}_m \rightarrow \mathbb{Z}$ ;  $m$  divides  $\Sigma y$ , and  $y - (\Sigma y)\delta_0$  is a sum-zero lift of  $f$  (it changes  $y$  only at 0, by a multiple of  $m$ ). The scalars  $\varepsilon_1, \varepsilon_2$  lift trivially.  $\square$

## 6 The kernel

**Lemma 15** (Lemma R.2). *For  $x \in K$ :  $\text{aug}(x_0) + \text{aug}(x_1) + \text{aug}(x_2) = 0$ , and  $m$  divides each  $\text{aug}(x_j)$ .*

*Proof.* By Lemma 4,  $0 = N_0^T Gx = (GN_0)^T x = m \sum_p x(p)$ , which is the first statement. For the second, let  $y$  be the indicator of the fibre  $\{\pi_t = c\}$  of family 0, so that  $my = \text{pb}_0^{\pi_t}(m\delta_c - 1) + N_0$  with  $m\delta_c - 1 \in Z_0$ . By Lemmas 9 and 4:

$$\begin{aligned} Gy &= 2N_0 + N_1 + N_2 - my & (t \notin \{0, \pm 1\}), \\ Gy &= 2N_0 + N_1 + mz - my & (t = 1), \\ Gy &= 2N_0 + N_2 + mz' - my & (t = -1), \end{aligned}$$

with  $z, z' \in A$  fibre indicators. Pairing with  $x \in K$  gives  $0 = y^T Gx$ , hence, with  $s_j = \text{aug}(x_j)$ :  $2s_0 + s_1 + s_2 \equiv 0$ ,  $2s_0 + s_1 \equiv 0$  and  $2s_0 + s_2 \equiv 0 \pmod{m}$ . A live pencil exists because  $m \geq 5$ . Subtracting,  $s_1 \equiv s_2 \equiv 0$  and  $2s_0 \equiv 0$ , so  $s_0 \equiv 0$  as  $m$  is odd.  $\square$

**Lemma 16** (the census of the kernel). *Let  $x \in K$  and write  $f_{j,\pi} = \text{fib}_{\pi}(x_j)$ . Then  $f_{j,\pi_t}$  is constant for every  $j$  and every live  $t$ , and the functions  $f_{0,\pi_{-1}} - f_{1,\pi_{-1}}$ ,  $f_{1,\pi_1} - f_{2,\pi_1}$  and  $v \mapsto f_{0,\pi_1}(v) - f_{2,\pi_{-1}}(v+1)$  are constant.*

*Proof.* For every  $w \in A$ ,  $x^\top Gw = (Gx)^\top w = 0$ , and  $x^\top \text{pb}_j^\pi(u) = \sum_v u(v)f_{j,\pi}(v)$ . A function  $f : \mathbb{F}_m \rightarrow \mathbb{Z}$  with  $\sum_v u(v)f(v) = 0$  for every  $u \in Z_0$  is constant (take  $u = \delta_a - \delta_b$ ). Apply this with  $w = \text{pb}_j^{\pi_t}(u)$  for live  $t$ , and with  $w = \text{pb}_0^{\pi_0^{-1}}(u)$ ,  $\text{pb}_1^{\pi_1}(u)$ ,  $\text{pb}_0^{\pi_1}(u)$ , using Lemma 9; in the last case  $\sum_z u(z-1)f_{2,\pi_0^{-1}}(z) = \sum_v u(v)f_{2,\pi_0^{-1}}(v+1)$ .  $\square$

**Proposition 17.**  $mK \subseteq \text{SAT}$ .

*Proof.* Let  $x \in K$ , put  $\mu_j = \text{aug}(x_j)/m \in \mathbb{Z}$  (Lemma 15, which also gives  $\mu_0 + \mu_1 + \mu_2 = 0$ ), and  $\tilde{f}_{j,\pi} = f_{j,\pi} - \mu_j$ ; since  $\Sigma f_{j,\pi} = \text{aug}(x_j)$ , each  $\tilde{f}_{j,\pi}$  has sum zero. By Lemma 8,

$$m \cdot x_j|_{\text{family } j} = \sum_{\pi} \text{pb}_j^\pi(\tilde{f}_{j,\pi}) + (m+1)\mu_j N_j - m\mu_j N_j = \sum_{\pi} \text{pb}_j^\pi(\tilde{f}_{j,\pi}) + \mu_j N_j.$$

By Lemma 16,  $\tilde{f}_{j,\pi_t}$  is constant with sum zero, hence 0, for every live  $t$ ; and the three overlap differences, constant with sum zero, vanish:  $\tilde{f}_{0,\pi_0^{-1}} = \tilde{f}_{1,\pi_0^{-1}}$ ,  $\tilde{f}_{1,\pi_1} = \tilde{f}_{2,\pi_1}$ ,  $\tilde{f}_{2,\pi_0^{-1}} = \tilde{f}_{0,\pi_1}^-$ . Hence  $m x = s_{\mathbb{Z}}(\Theta)$  for the admissible datum  $\Theta$ :  $a_j = \tilde{f}_{j,\pi_0}$ ,  $b_j = \tilde{f}_{j,\pi_\infty}$ ,  $w_0 = \tilde{f}_{0,\pi_0^{-1}}$ ,  $w_1 = \tilde{f}_{1,\pi_1}$ ,  $w_2 = \tilde{f}_{0,\pi_1}$ ,  $\varepsilon_1 = \mu_0$ ,  $\varepsilon_2 = -\mu_2$  (note  $\varepsilon_2 - \varepsilon_1 = \mu_1$ ).  $\square$

## 7 The sublattice $F$ and two indices

Let  $F \subseteq A$  be spanned by  $N_0$  and by the  $3(m-2)$  blocks  $\text{pb}_j^{\pi_t}(Z_0)$  for  $j \in \{0, 1, 2\}$  and  $t$  live, together with  $\text{pb}_0^{\pi_0^{-1}}(Z_0)$ ,  $\text{pb}_1^{\pi_1}(Z_0)$  and  $\text{pb}_0^{\pi_1}(Z_0)$  (one member of each overlap pair).

**Lemma 18.** *Distinct blocks are  $B$ -orthogonal, and  $N_0$  is  $B$ -orthogonal to every block. Inside a block,  $B(\text{pb } u, \text{pb } v) = -m^2 \sum_x u(x)v(x)$ ; and  $B(N_0, N_0) = m^3$ .*

*Proof.* By Lemma 9,  $G$  applied to a block vector is  $-m$  times it, plus, for the three overlap members,  $m$  times a pullback along an overlap pencil of another family: of family 1 along  $\pi_{-1}$ , of family 2 along  $\pi_1$ , and of family 2 along  $\pi_{-1}$ . None of these three is a block of  $F$ , so that term pairs with a block of  $F$  either through disjoint supports or through two different pencils of one family, which gives  $(\Sigma u)(\Sigma v) = 0$  by Lemma 7. Two blocks of one family and different pencils are orthogonal for the same reason, and blocks of different families have disjoint supports. Inside a block, Lemma 7 gives  $-m \cdot m \sum_x u(x)v(x)$ . Finally  $B(N_0, w) = (GN_0)^\top w = m \sum_p w(p)$ , which is 0 on pullbacks of sum-zero functions, and  $m \cdot m^2$  for  $w = N_0$ .  $\square$

**Corollary 19.**  $F \cap K = 0$ , and  $F$  is free of rank  $3(m-2)(m-1) + 1$ .

*Proof.* Write  $x \in F$  as  $cN_0 + \sum_{\beta} \text{pb}(u_{\beta})$ , one term per block. If  $x \in K$  then  $0 = B(x, \text{pb}(u_{\beta})) = -m^2 \sum u_{\beta}^2$ , so every  $u_{\beta} = 0$ , and  $0 = B(x, N_0) = cm^3$ . The same argument shows that the blocks and  $N_0$  are independent; each block is isomorphic to  $Z_0$  because  $\pi$  is surjective.  $\square$

Let  $L_{\text{fam}} \subseteq \mathbb{Z}^P$  be spanned by the constant 1 and all  $u \circ \pi$ ,  $u \in Z_0$ ,  $\pi$  a pencil; and let  $L \subseteq A$  consist of the  $x$  with  $x_j \in L_{\text{fam}}$  for every  $j$ .

**Lemma 20.**  $[\mathbb{Z}^P : L_{\text{fam}}] = m^{(m^2+m+2)/2}$ , hence  $[A : L] = m^{3(m^2+m+2)/2}$ .

*Proof.* The  $(m+1)(m-1) + 1 = m^2$  vectors  $(\delta_x - \delta_0) \circ \pi$  ( $x \neq 0$ ,  $\pi$  a pencil) and 1 span  $L_{\text{fam}}$ . By Lemma 7 their Gram matrix for the standard inner product is block diagonal: inside one pencil it is  $m(I + J)$  of size  $m-1$ , with determinant  $m^{m-1} \cdot m$ ; and  $\langle 1, 1 \rangle = m^2$ . The Gram determinant is  $(m^m)^{m+1} m^2 = m^{m^2+m+2} \neq 0$ ; so the vectors form a basis, and the index of the lattice they span is the square root of the Gram determinant ( $m^2 + m$  is even).  $\square$

**Lemma 21.**  $F + \text{SAT} = L$ , and  $F \cap \text{SAT} = 0$ .

*Proof.* Both  $F$  and  $\text{SAT}$  lie in  $L$ . Conversely  $L$  is spanned by the vectors  $\text{pb}_j^\pi(u)$ ,  $u \in Z_0$ , and  $N_0, N_1, N_2$ . Live blocks lie in  $F$ ; axis pullbacks lie in  $\text{SAT}$ ; for an overlap pair, one member lies in  $F$  and the sum of the pair lies in  $\text{SAT}$  (with a datum having one non-zero  $w_i$ ; for the third pair, the vector  $\text{pb}_2^{\pi^{-1}}(v)$  is reached with  $w_2 = v^+$ ). Finally  $N_0 \in F$ , and  $N_0 - N_1, N_1 - N_2 \in \text{SAT}$ . The intersection is 0 because  $F \cap K = 0$  and  $\text{SAT} \subseteq K$ .  $\square$

**Proposition 22.**  $\text{SAT}$  and  $K$  are free of rank  $9m - 7$ , and  $[K : \text{SAT}] = m^{12}$ .

*Proof.* By Lemmas 20 and 21,  $F \oplus \text{SAT}$  has finite index in  $A$ , so  $\text{rank SAT} = 3m^2 - \text{rank } F = 9m - 7$ . Since  $\text{SAT} \subseteq K$  and  $F \cap K = 0$ , also  $9m - 7 \leq \text{rank } K \leq 3m^2 - \text{rank } F = 9m - 7$ .

By Proposition 17,  $K/\text{SAT}$  is killed by  $m$ , so  $[K : \text{SAT}] = |K/mK|/|\text{SAT}/mK| = m^{9m-7}/|\text{SAT}/mK|$ . Since  $K = \ker G$ ,  $K \cap mA = mK$ , so  $K/mK$  embeds in  $A/mA = \mathbb{F}_m^I$ ; it maps  $\text{SAT}/mK$  onto the reduction of  $\text{SAT}$  modulo  $m$ , which by Lemma 14 is the image of  $s\mathbb{F}_m$ , of dimension  $9m - 19$  (Lemma 12). Hence  $[K : \text{SAT}] = m^{(9m-7)-(9m-19)} = m^{12}$ .  $\square$

**Corollary 23.**  $[A : F + K] = m^{3(m^2+m+2)/2-12}$ .

*Proof.*  $L = F + \text{SAT} \subseteq F + K \subseteq A$ . The map  $K \rightarrow (F + K)/(F + \text{SAT})$  is onto with kernel  $K \cap (F + \text{SAT}) = \text{SAT}$ : if  $k = f + s$  then  $f = k - s \in F \cap K = 0$ . So  $[F + K : L] = [K : \text{SAT}] = m^{12}$ , and  $[A : F + K] = [A : L]/m^{12}$ .  $\square$

## 8 Proof of the Watermark Theorem

$V = A/K$  is free of rank  $3m^2 - (9m - 7) = 3(m - 1)(m - 2) + 1$  (§2 and Proposition 22). The quotient map  $\varphi : A \rightarrow V$  is injective on  $F$  (Corollary 19) and  $V/\varphi(F) \cong A/(F + K)$ , so  $\varphi(F)$  is a sublattice of full rank and index  $N = m^{3(m^2+m+2)/2-12}$  (Corollary 23).

Let  $c$  be the basis of  $\varphi(F)$  formed by  $\varphi(N_0)$  and, for each block, the images of  $\text{pb}(\delta_x - \delta_0)$ ,  $x \neq 0$ . By Lemma 18 its Gram matrix is block diagonal, with  $3(m - 2)$  blocks  $-m^2(I + J)$  of size  $m - 1$  and the block  $(m^3)$ ; since  $m - 1$  is even,

$$\det \text{Gram}_c = (m^{2(m-1)} \cdot m)^{3(m-2)} \cdot m^3 = m^{3(m-2)(2m-1)+3}.$$

For any basis  $b$  of  $V$ ,  $\text{Gram}_c = M^T \text{Gram}_b M$  with  $|\det M| = N$ , so

$$\det \text{Gram}_b = m^{3(m-2)(2m-1)+3-3(m^2+m+2)+24} = m^{3m^2-18m+27} = m^{3(m-3)^2}.$$

With Corollary 6 this proves Theorem 1.  $\square$

## 9 Proof of the Double Ladder Theorem

By Theorem 1,  $D = V^*/V$  is a finite group of order  $m^{3(m-3)^2}$ . Its structure is fixed by two more facts: its exponent divides  $m^2$  (§9.1), and the rank of  $G$  modulo  $m$  (§9.2).

### 9.1 The exponent

For a pencil  $\pi$  let  $P_\pi \in \mathbb{Z}^{I \times I}$  be the block-diagonal matrix with  $(P_\pi)_{pq} = 1$  if  $p, q$  lie in one family and  $\pi(p) = \pi(q)$ , and 0 otherwise. Put

$$Y = P_{\pi_0} + P_{\pi_\infty} + 3P_{\pi_{-1}} + 3P_{\pi_1} - 6m I.$$

**Lemma 24.**  $GYG = 6m^2G$ .

*Proof.* By Lemma 8 (applied to the indicator of one point),  $\mathbb{Q}^I$  is spanned by the pullbacks  $\text{pb}_j^\pi(u)$ ,  $u \in Z_0$ , and the vectors  $N_j$ ; we check the identity on these. By Lemma 7,  $P_\pi \text{pb}_j^{\pi'}(u)$  is  $m \text{pb}_j^\pi(u)$  if  $\pi' = \pi$  and 0 otherwise, and  $P_\pi N_j = mN_j$ . So  $Y$  acts by  $-5m$  on axis pullbacks, by  $-3m$  on overlap pullbacks, by  $-6m$  on live pullbacks, and by  $2m$  on the  $N_j$ . Now use Lemma 9. Axis: both sides vanish. Live:  $(-m)(-6m)(-m) = -6m^3 = 6m^2 \cdot (-m)$ . Each overlap pair spans a  $G$ -stable plane on which  $G = mE$ ,  $E = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$  (for the third pair use the vectors  $\text{pb}_0^{\pi_1}(u)$  and  $\text{pb}_2^{\pi_{-1}}(u^-)$ ), and  $Y = -3m$ ; as  $E^2 = -2E$ ,  $mE(-3m)mE = 6m^3E = 6m^2 \cdot mE$ . On the span of  $N_0, N_1, N_2$ ,  $G = mJ_3$  (Lemma 4) and  $Y = 2m$ ; as  $J_3^2 = 3J_3$ ,  $mJ_3 \cdot 2m \cdot mJ_3 = 6m^3J_3$ .  $\square$

The proof shows that  $G$  is diagonalizable over  $\mathbb{Q}$  with eigenvalues  $0, -m, -2m, 3m$ , so its minimal polynomial is  $x(x+m)(x+2m)(x-3m)$ ; and  $Y$  acts as  $6m^2/\lambda$  on the  $\lambda$ -eigenspace for every  $\lambda \neq 0$ ; the integer 6 is the least common denominator of  $m^2/\lambda$  over  $\lambda \in \{-m, -2m, 3m\}$ .

**Corollary 25.**  $m^2V^* \subseteq V$ : the exponent of  $D$  divides  $m^2$ .

*Proof.* A functional on  $V$  is given by a vector  $f \in \mathbb{Z}^I$  orthogonal to  $K = \ker G$ ; as  $G$  is symmetric,  $f = Gy$  with  $y \in \mathbb{Q}^I$ . By Lemma 24,  $6m^2f = GYGy = G(Yf)$ , which is the functional of the class of the integer vector  $Yf$ . So  $6m^2V^* \subseteq V$ . The order of  $D$  is a power of  $m$  and  $\gcd(6, m) = 1$ , so  $m^2V^* \subseteq V$ .  $\square$

## 9.2 The rank of $G$ modulo $m$

Use the four pencils  $\pi_0, \pi_\infty, \pi_{-1}, \pi_1$  (that is,  $k, l, k-l, k+l$ ). For each family  $j$  and each of them let  $\text{push}_{j,\pi} : \mathbb{F}_m^P \rightarrow \mathbb{F}_m^{\mathbb{F}_m^m}$  be the fibre sum, and let  $S : \mathbb{F}_m^I \rightarrow U = (\mathbb{F}_m^{\mathbb{F}_m^m})^{12}$  collect these twelve *shadows*. Let  $\Gamma$  be the symmetric matrix on  $U$  that pairs each of the six axis slots  $(j, \pi_0), (j, \pi_\infty)$  with itself by the identity, pairs  $(0, \pi_{-1})$  with  $(1, \pi_{-1})$  and  $(1, \pi_1)$  with  $(2, \pi_1)$  by the identity, and pairs  $(0, \pi_1)$  with  $(2, \pi_{-1})$  by the shift (the value  $v$  of the first slot with the value  $v+1$  of the second). Then  $\Gamma^2 = I$ .

**Lemma 26.**  $G = S^\top \Gamma S - mI$  over  $\mathbb{Z}$  (with  $S$  and  $\Gamma$  read as integer matrices). Hence  $G \equiv S^\top \Gamma S \pmod{m}$  and  $\text{rank}_{\mathbb{F}_m}(G \pmod{m}) = \dim W - \dim(W \cap W^{\perp_\Gamma})$ , where  $W = \text{im } S$  and  $W^{\perp_\Gamma} = \{w : \langle \Gamma w, W \rangle = 0\}$ .

*Proof.* The entry of  $S^\top \Gamma S$  at two lines of one family is  $[k = k'] + [l = l']$  (only the axis slots pair inside a family), which is 2 on the diagonal; at a line of family 0 and one of family 1 it is  $[k - l = k' - l']$ ; at families 1, 2 it is  $[k + l = k' + l']$ ; at families 0, 2 it is  $[k' - l' = k + l + 1]$ . Subtracting  $mI$  gives  $G$ . For the rank:  $S^\top \Gamma Sx = 0$  if and only if  $\Gamma Sx \perp W$ , i.e.  $Sx \in W \cap W^{\perp_\Gamma}$ , so  $\dim \ker = \dim \ker S + \dim(W \cap W^{\perp_\Gamma})$ .  $\square$

**Lemma 27.**  $\dim W = 12m - 18$ . The annihilator  $R$  of  $W$  (for the standard pairing) has dimension 18; family by family it is spanned by the elements placing  $c_\pi x^s$  in the slot  $(j, \pi)$ , with  $s \in \{0, 1, 2\}$  and  $\sum_\pi c_\pi \pi^s = 0$  as a form on  $P$ .

*Proof.*  $W = \bigoplus_j W_j$ . A tuple  $(h_\pi)_\pi$  of functions annihilates  $W_j$  if and only if  $\sum_\pi h_\pi(\pi(k, l)) = 0$  as a function on  $P$ . Write each  $h_\pi$  as a polynomial of degree  $\leq m-1$ ; the sum is a polynomial of total degree  $\leq m-1$ , which vanishes as a function on  $\mathbb{F}_m^2$  if and only if it vanishes as a polynomial, i.e. if and only if  $\sum_\pi c_{\pi,s} \pi^s = 0$  for each  $s$ , where  $c_{\pi,s}$  is the coefficient of  $x^s$  in  $h_\pi$ . For  $3 \leq s \leq m-1$  the four forms  $\pi^s$  are linearly independent: writing  $\pi = ak + bl$ , the coefficient of  $k^t l^{s-t}$  in  $\pi^s$  is  $\binom{s}{t} a^t b^{s-t}$ , the binomial coefficients are units ( $s < m$ ), and the matrix  $(a_\pi^t b_\pi^{s-t})_{\pi,t}$  has rank 4 because evaluation of binary forms of degree  $s \geq 3$  at the four distinct points  $(1:0), (0:1), (1:-1), (1:1)$  of  $\mathbb{P}^1(\mathbb{F}_m)$  is surjective onto  $\mathbb{F}_m^4$ . For  $s \leq 2$  the four forms  $\pi^s$  span all binary forms of degree  $s$  (here  $\text{char} \neq 2$ ), a space of dimension  $s+1$ , so the relations

have dimension 3, 2, 1 for  $s = 0, 1, 2$ ; the relation in degree 2 is  $(k + l)^2 + (k - l)^2 = 2k^2 + 2l^2$ . So  $\dim R_j = 6$  and  $\dim W_j = 4m - 6$ .  $\square$

**Proposition 28.** *For every prime  $m \geq 7$ ,  $\text{rank}_{\mathbb{F}_m}(G \bmod m) = 12(m - 3)$ .*

*Proof.*  $W^{\perp_\Gamma} = \Gamma(W^\perp) = \Gamma R$ . The slot functions of an element of  $\Gamma R$  are polynomials of degree  $\leq 2$ , possibly translated by  $\pm 1$ . Such an element lies in  $W = R^\perp$  if it pairs to zero with  $R$ ; each pairing is  $\sum_{x \in \mathbb{F}_m} p(x)q(x)$  with  $\deg(pq) \leq 4$ , and  $\sum_{x \in \mathbb{F}_m} x^e = 0$  for  $0 \leq e \leq m - 2$ . As  $4 \leq m - 2$  for  $m \geq 7$ ,  $\Gamma R \subseteq W$ , so  $W \cap W^{\perp_\Gamma} = \Gamma R$  has dimension 18 and the rank is  $(12m - 18) - 18$ .  $\square$

At  $m = 5$  the pairings of degree 4 survive, because  $\sum_{x \in \mathbb{F}_5} x^4 = -1$ . Only the three relations of degree 2 pair non-trivially (every other product has degree  $\leq 3 = m - 2$ ): the relation  $r_j$  places  $-2x^2, -2x^2, x^2, x^2$  in the slots  $(j, \pi_0), (j, \pi_\infty), (j, \pi_{-1}), (j, \pi_1)$ , and  $\langle \Gamma r_j, r_{j'} \rangle$  is  $8 \sum_x x^4$  for  $j = j'$  (the two axis slots) and  $\sum_x x^4$  for  $j \neq j'$  (one overlap slot; the shift changes only terms of lower degree). The matrix  $-(7I + J_3) \equiv 3I + 4J_3 \pmod{5}$  has rank 2. So the  $18 \times 18$  matrix of  $\Gamma$ -pairings between the relations has rank 2,  $\dim(W \cap W^{\perp_\Gamma}) = 16$  and  $\text{rank}(G \bmod 5) = 26$ . This value is also checked in Lean by kernel-checked decision procedures (§10), and it agrees with [1, Table 1, row (2, 5)].

### 9.3 Assembly

$K$  is a direct summand of  $A$  (it is saturated), so in a basis of  $A$  adapted to  $A = K \oplus C$  the matrix  $G$  becomes  $0 \oplus \text{Gram}(V)$ . Hence the non-zero elementary divisors of  $G$  are those of  $\text{Gram}(V)$ , whose cokernel is  $D$ . All of them are powers of  $m$  (the order of  $D$  is), and by Corollary 25 none has valuation  $\geq 3$ . Let  $n_0, n_1, n_2$  be the numbers of non-zero elementary divisors 1,  $m$ ,  $m^2$ . Then  $D \cong (\mathbb{Z}/m)^{n_1} \times (\mathbb{Z}/m^2)^{n_2}$  and

$$n_0 + n_1 + n_2 = \text{rank } V = 3m^2 - 9m + 7, \quad n_1 + 2n_2 = 3(m - 3)^2, \quad n_0 = \text{rank}(G \bmod m).$$

For  $m \geq 7$ ,  $n_0 = 12(m - 3)$ , so  $n_1 + n_2 = 3m^2 - 21m + 43$ , and  $n_2 = 3m - 16$ ,  $n_1 = 3m^2 - 24m + 59$ . For  $m = 5$ :  $n_0 = 26$ ,  $n_1 + n_2 = 11$ ,  $n_1 + 2n_2 = 12$ , so  $n_2 = 1$  and  $n_1 = 10$ . This proves Theorem 2.  $\square$

*Remark 29.* The proof also explains the exceptional prime:  $m = 5$  is the only prime  $\geq 5$  with  $4 > m - 2$ , that is, the only one for which  $\sum_x x^4 \neq 0$  in  $\mathbb{F}_m$  enters the count. The integer 6 in Lemma 24 is harmless exactly because  $\gcd(m, 6) = 1$ , the hypothesis under which the lines generate  $\text{NS}(S_m)$ .

## 10 Verification in Lean

The lattice statements of Theorems 1 and 2 are proved in Lean 4 [7] with the Mathlib library [8], toolchain `leanprover/lean4:v4.28.0`. The Lean definitions of the lines, of  $G$  (as the case analysis of §2), of  $K = \ker G$ , of  $V = A/K$  with the induced form, and of  $D = V^*/V$  (the dual of  $V$  modulo the range of the form) are printed verbatim in the two certificates [18, 6] and compared there, line by line, with the June papers [15, 5], whose definitions are those of §2. The final theorems are:

- `Watermark.watermark_theorem`: for every prime  $m \geq 5$ ,  
 $V$  is free of rank  $3(m - 1)(m - 2) + 1$ , and for every  $\mathbb{Z}$ -basis  $b$  of  $V$  the Gram determinant is  $m^{3(m-3)^2}$ ;
- `DoubleLadder.double_ladder_theorem`: for every prime  $m \geq 7$ ,  
 $D \cong (\mathbb{Z}/m)^{3m^2 - 24m + 59} \times (\mathbb{Z}/m^2)^{3m - 16}$  as abelian groups;
- `DoubleLadder.double_ladder_five`:  $D \cong (\mathbb{Z}/5)^{10} \times \mathbb{Z}/25$  at  $m = 5$ .

They depend only on the axioms `propext`, `Classical.choice` and `Quot.sound`; the project contains no `sorry`, no `admit` and no `native_decide`. The Lean proof follows §§4–9 with a few differences of detail recorded in the certificates: for instance, the inclusion  $\text{SAT} \subseteq K$  is proved there for every  $m \geq 1$  by a direct computation, the relations of Lemma 27 are identified by mixed second differences instead of polynomials, and the structure of  $D$  is obtained from  $|D|$  and  $|D/mD|$  instead of a Smith form. The Lean proofs were written by the system Aristotle (Harmonic) [3] from statements and proofs prepared by the author, then compiled and checked again on the author’s machine, including a clean rebuild of the whole project. The project, the certificates and the logs are in the Zenodo record [16] and the repository <https://github.com/tretoef-estrella/watermark-theorem>.

Not formalized: the geometry of §3 (Mathlib has no complex algebraic surfaces and no singular cohomology of them), the equality  $V = \text{NS}(S_m)$ , which is cited [10, 4], and Corollary 3, which uses the unimodularity of  $H^2(S_m, \mathbb{Z})$  and [9].

## 11 What was known before, and what is new

We read in the original [13, 10, 4, 14, 1]; a search cannot prove that nothing else exists, it records what we looked at.

- Shioda [13], §7, pp. 133–134, asks for the determinant only (Questions 7.2 and 7.4, prime  $m$ ). In “Added in proof” he notes that the discriminant divides a power of  $m$  for every  $m$ . Theorem 1 answers (7.10) for prime  $m \geq 5$ , and [4] answers (7.11) (the lines span NS).
- Schütt, Shioda and van Luijk [10, end of §4]: for every odd  $m \leq 81$  the Gram determinant of their rational basis  $\mathcal{B}$  of lines is  $m^{3(m-3)^2}$ , by computer, “with exponent as conjectured”;  $\mathcal{B}$  spans  $\text{NS}(S_m)$  when  $\gcd(m, 6) = 1$  and  $m \leq 100$  [10, Theorem 1.1].
- Shioda [14, §6.5, Conjecture 23] still uses the formula as expected in 2015, for every  $m$  prime to 6; the present paper proves it for prime  $m$  only.
- Aljovin, Movasati and Villaflor [1, Table 1]: the elementary divisors for  $3 \leq m \leq 14$ , by machine; for prime  $m$  these are the rows quoted in §1, that is, Theorem 2 at  $m = 5, 7, 11, 13$ . They give no formula for general  $m$ .

New here, as far as we could determine: the proof of the formula  $m^{3(m-3)^2}$  for every prime  $m \geq 5$ ; the structure of the discriminant group for every prime  $m \geq 5$ , with the explanation of the exceptional value at  $m = 5$ ; and the verification of both lattice statements in Lean. The determinant of the lattice of linear cycles of Fermat varieties of prime degree in every even dimension is treated, by other methods and modulo cited results, in [17].

## Use of AI

This work was developed with extensive use of AI systems: Claude (Anthropic) for exploration, computation, writing and auditing, and Aristotle (Harmonic) for writing the Lean proofs. The text of this paper was read before release by a separate reader, also an AI system; its report led to corrections in Lemma 14 and §11 and to changes of presentation, which were applied and checked again, without a second reading. The statements, the choice of what to claim and the responsibility for errors are the author’s. The work has not been refereed by a human expert.

## References

- [1] E. Aljovin, H. Movasati, R. Villafior, *Integral Hodge conjecture for Fermat varieties*, J. Symbolic Comput. **95** (2019), 177–184. arXiv:1711.02628.
- [2] N. Aoki, T. Shioda, *Generators of the Néron–Severi group of a Fermat surface*, in: Arithmetic and Geometry, Vol. I, Progr. Math. **35**, Birkhäuser, Boston (1983), 1–12.
- [3] Harmonic, *Aristotle*, <https://aristotle.harmonic.fun>.
- [4] A. Degtyarev, *Lines generate the Picard groups of certain Fermat surfaces*, J. Number Theory **147** (2015), 454–477. arXiv:1305.3073.
- [5] R. Amichis Luengo, *The Double Ladder Theorem*, version 4 (30 September 2026), in [16].
- [6] R. Amichis Luengo, *The Double Ladder Theorem — Lean certificate*, version 2 (30 September 2026), in [16].
- [7] L. de Moura, S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Comput. Sci. **12699**, Springer (2021), 625–635.
- [8] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM (2020), 367–381.
- [9] V. V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR Izv. **14** (1980), 103–167.
- [10] M. Schütt, T. Shioda, R. van Luijk, *Lines on Fermat surfaces*, J. Number Theory **130** (2010), no. 9, 1939–1963. arXiv:0812.2377.
- [11] T. Shioda, *The Hodge conjecture for Fermat varieties*, Math. Ann. **245** (1979), 175–184.
- [12] T. Shioda, *On the Picard number of a Fermat surface*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1982), no. 3, 725–734.
- [13] T. Shioda, *Some observations on Jacobi sums*, in: Galois Representations and Arithmetic Algebraic Geometry, Adv. Stud. Pure Math. **12**, Kinokuniya / North-Holland (1987), 119–135.
- [14] T. Shioda, *Mordell–Weil lattice of higher genus fibration on a Fermat surface*, J. Math. Sci. Univ. Tokyo **22** (2015), 443–468.
- [15] R. Amichis Luengo, *The Watermark Theorem*, 4 June 2026, with the version note of 30 September 2026, in [16].
- [16] R. Amichis Luengo, *The Watermark and Double Ladder Theorems (Verified in Lean)*, Zenodo (2026), doi:10.5281/zenodo.23062530.
- [17] R. Amichis Luengo, *The Watermark in Every Even Dimension: the Discriminant of the Hodge Lattice of a Fermat Variety of Prime Degree*, Zenodo (2026), doi:10.5281/zenodo.23091046.
- [18] R. Amichis Luengo, *The Watermark Theorem — Lean certificate*, version 2 (30 September 2026), in [16].