Math. Ann. 314, 175–196 (1999)

Mathematische Annalen

Zeros of Eisenstein series, quadratic class numbers and supersingularity for rational function fields

Gunther Cornelissen

Max-Planck-Institut für Mathematik, Gottfried-Claren-Straße 26, D-53225 Bonn, Germany
University of Gent, Deptartment of Pure Mathematics, Galglaan 2, B-9000 Gent, Belgium
(e-mail: gc@cage.rug.ac.be)

Received: 3 June 1998 / in final form: 2 November 1998

Mathematics Subject Classification (1991): 11G09, 11F03

Introduction

In the ample theory of classical modular forms, little attention seems to have been paid to their zeros. As is well known, the (suitably counted) number of zeros of a modular form for a congruence subgroup of $SL(2,\mathbf{Z})$ on the corresponding modular curve can be expressed in solely geometric terms, *e.g.*, the weight multiplied by a normalized hyperbolic volume of the modular curve ([25], 2.16 & 2.20).

In a different vein (following prior work of Wohlfahrt, R.A. Rankin and A.O.L. Atkin) F.K.C. Rankin and Swinnerton-Dyer [19] have used methods of classical analysis to show that zeros of Eisenstein series of integer weight for $SL(2,\mathbf{Z})$ in the fundamental domain are located on the complex unit circle. R.A. Rankin [20] has subsequently generalized the result.

Complementary to this, one can fix a point z in the upper half plane and consider the *weight* s of such Eisenstein series as a variable complex number; the resulting functions behave very much like zeta-functions. For a study of their zeros, see J. Hoffstein [16] and the references therein.

Now assume that $f(z)$ is a holomorphic modular form for a congruence group Γ of level N in $SL(2,\mathbf{Z})$, and that it can be defined over a finite extension $L/\mathbf{Q}$ of the rationals. By this we mean that f admits Fourier expansions in $L((e^{2\pi iz/N}))$. Assume also that L is big enough for the modular curve X_Γ to be uniformized by modular functions defined over L. From these two assumptions it follows that the points in the support of the divisor of f are defined over a finite extension of L. Hence also the j-invariants of

the zeros of f, *i.e.*, the images of the zeros under the (L-rational) projection $X_\Gamma \to X(1)$, are algebraic numbers. Then a famous corollary of the Gelfond-Schneider theorem implies that *zeros in the upper half plane of any modular form defined over a finite extension of* $\mathbf{Q}$*, are either transcendental over* $\mathbf{Q}$*, or points of complex multiplication.*

In order to pursue a meaningful *algebraic* study of the zeros of f, one is led to focus on the field extension of L generated by the points in the support of the divisor of f, denoted by $L(\mathrm{div}(f))$.

Example. Let

$$E_l(z) = 1 - \frac{2l}{B_l} \sum_{n \geq 1} \sum_{d|n} d^{l-1} e^{2\pi i n z},$$

be the Eisenstein series of even weight $l > 2$ for $SL(2, \mathbf{Z})$, normalized in such a way that it is defined over $\mathbf{Q}$ (where B_l is the l-th Bernoulli number). Set $l = 4d + 6e + 12m$ with $d \in \{0, 1, 2\}$ and $e \in \{0, 1\}$. Let $1728 \cdot \Delta = E_4^3 - E_6^2$ and $j = E_4^3/\Delta$ be the normalized discriminant Δ and the j-invariant j respectively. Then

$$E_l(z) E_4(z)^{-d} E_6(z)^{-e} \Delta(z)^{-m} = P_l(j(z))$$

for some polynomial P_l of degree m, and the divisor of E_l on the j-line $X(1)$ is given by

$$\mathrm{div}(E_l) = \frac{d}{3} \cdot 0 + \frac{e}{2} \cdot 1728 + \mathrm{div}(P_l).$$

(As usual, this divisor takes into account the order of the stabilizers in $SL(2, \mathbf{Z})$, and lies in $\mathrm{Div}(X(1)) \otimes \mathbf{Q}$, see [25]). One recognizes $j = 0$ and $j = 1728$ as the two elliptic points of $SL(2, \mathbf{Z})$. One can make the following, partially empirical, observations:

E1. The theorem of Rankin and Swinnerton-Dyer is equivalent to the fact that the roots of P_l are real and belong to the interval $(0, 1728)$.

E2. Assume that $l + 1$ equals a prime number p. Weights of this form seem to be especially relevant to arithmetic due to Deligne's observation that E_{p-1} is congruent to the Hasse invariant modulo p. A bit of computation shows that for $l < 90$, $\mathrm{div}(P_l)$ is irreducible over $\mathbf{Q}$. Furthermore, one computes that

$$\mathrm{Gal}(\mathbf{Q}(\mathrm{div}(E_l))/\mathbf{Q}) = S_m$$

for the same such l. Thus, whereas the j-invariants of the zeros of E_l are algebraic, their algebraic *relations* are "without affect", *i.e.*, like the roots of the general polynomial.

E3. For $l < 90$ as in (E2), the discriminant of P_l is a highly composite number, divisible by all primes $< \frac{p+1}{2}$, with the possible exception of 11. As an example of this,

$$\mathrm{Disc}(P_{31}) = 2^{21} \cdot 3^9 \cdot 5^5 \cdot 7^4 \cdot 13^2 \cdot 39468318601.$$

The aim of this work is to prove that the situation of the example persists for an infinity of different weights, *albeit* in the corresponding theory of modular forms for rational function fields (Eisenstein series for GL_2 over a polynomial ring over a finite field acting on the Drinfeld upper half plane). We will also see how the analogue of Rankin's and Swinnerton-Dyer's theorem fits into this algebraic way of thinking. The main results will be stated after introducing some notations in the next section.

One of the reasons for having a closer look at *zeros* of modular forms seems to be the following qualitative observation. Assume f is a modular form defined over a number field L with ring of integers $\mathcal{O}$ and assume that f is congruent modulo some prime $\mathfrak{B}$ of $\mathcal{O}$ to an arithmetical function H whose zeros z in the upper half plane are important (like invariants of elliptic curves). Assume that $f(z) \in \mathcal{O}$. Then a (hopefully meaningful) inequality results as follows:

$$H(z) = 0 \Rightarrow f(z) = 0 \text{ or } |N_{\mathbf{Q}}^{L} f(z)| \geq |N_{\mathbf{Q}}^{L} \mathfrak{B}|.$$

The Γ-orbits of the zeros z of f form a finite set of "exceptional" values, and for all other values the inequality holds.

This somewhat vague principle can be applied in our situation, as we consider weights corresponding to the case where Deligne's congruence is valid: the modular form "Eisenstein series" is congruent to the arithmetical object "Hasse invariant". This also means that there will be an intimate connection to supersingularity and hence quadratic class numbers (or equivalently, type numbers of quaternion algebras). Indeed, on the way we will encounter a class number problem for certain hyperelliptic function fields, and finally we will be able to present an application to supersingular reduction of Drinfeld modules in the aforementioned sense: if a j-invariant j is supersingular modulo some prime $\mathfrak{B}$, then either it belongs to a finite list of $\mathfrak{B}$-exceptions (corresponding to the zeros), or an inequality between the degrees of $\mathfrak{B}$ and j results. Actually, the number of such $\mathfrak{B}$ of degree $\leq k$ is bounded in terms of j and k for non-exceptional j. The technical result is again stated in the next section.

I expect that most of these results obtained in the setting of a rational function field should carry through for classical Eisenstein series on $SL(2, \mathbf{Z})$ too, but I have not carried out such a programme.

1. Notations and statements

Let q be a power of an *odd* prime p and $A = \mathbf{F}_q[T]$ the polynomial ring over the finite field $\mathbf{F}_q$ of q elements. Let K be the quotient field of A, and $|\cdot|$ the absolute value on K given by $|q| = q^{\deg a}$ for $a \in A$. Let K_∞ and C be respectively the completion of K and the completion of an algebraic closure of K_∞. The space $\Omega := C - K_\infty$ is called *Drinfeld's upper half space*, and carries a structure as a rigid analytic space, on which the group $GL(2, A)$ acts through fractional transformations. With respect to this action and this notion of analyticity, the function

$$E_l(z) : \Omega \to C : z \mapsto \sum_{(0,0)\neq(a,b)\in A^2} (\frac{1}{az+b})^l, \quad \text{where } l \in \mathbf{Z}_{>0},$$

turns out to be a modular form of weight l. It is called the *Eisenstein series* of weight l, and it is non-trivial only if $q-1$ divides l. For an introduction to this circle of ideas, we refer to [6], [10], [13], and [15].

We will set $\langle i \rangle = T^{q^i} - T$ for any natural number i. The symbol $\langle i \rangle$ equals the product of all monic irreducibles polynomials in A whose degree divides i. Define two modular forms g and Δ of respective weights $q-1$ and q^2-1 by

$$g = \langle 1 \rangle E_{q-1}, \quad \Delta = \langle 1 \rangle E_{q-1}^{q+1} - \langle 2 \rangle E_{q^2-1}.$$

The *j-invariant* $j = g^{q+1}/\Delta$ induces an isomorphism of rigid analytic spaces j-line $= GL(2, A)\backslash\Omega \to C$. Note that we have not normalized the E_l such that they are "defined over K" in the sense of the introduction. But subsequent formulas will be written in such a form that all possible transcendentals factor out.

As will become apparent, the role played by the pair (E_{p-1}, p) for a prime p in the example above is taken over by $(E_{q^k-1}, \mathfrak{p})$ for primes $\mathfrak{p} \in A$ of degree k. We will now formulate the main theorems on the arithmetic of the divisors of these Eisenstein series.

First of all, in [4] it was proved that the divisor of the Eisenstein series E_{q^k-1} on the j-line is given by

$$\text{div}(E_{q^k-1}) = \frac{\chi(k)}{q+1} \cdot 0 + \text{div}(P_k(j)),$$

where P_k is a polynomial in j, and χ is the characteristic function of the odd integers, *i.e.* $\chi(2\mathbf{Z}+1) = 1, \chi(2\mathbf{Z}) = 0$. Note that $j = 0$ is the unique elliptic point for $GL(2, A)$ (*i.e.*, whose stabilizer for the action of $GL(2, A)$

on Ω is $\mathbf{F}_{q^2}^*$ rather then the usual center $\mathbf{F}_q^*$ of $GL(2,A)$). The degree of P_k is

$$m(k) = \deg P_k = \frac{q^k - q^{\chi(k)}}{q^2 - 1}.$$

Theorem E1 ([4], compare (2.3)). *Non-zero j-invariants of zeros of Eisenstein series E_{q^k-1} (i.e., the roots of P_l) have absolute value q^q.*

Theorem E2. *For all k, P_k is irreducible over K. For even k, the Galois group of P_k is alternating or symmetric of degree $m(k)$. If we fix p, then there exists a constant $C_{k,p}$ such that for all $q > C_{k,p}$,*

$$\mathrm{Gal}(P_k/K) = \mathrm{Gal}(K(j(z) : E_{q^k-1}(z) = 0)/K) = S_{m(k)}.$$

Theorem E3 (Gekeler, [12]). *A prime of A ramifies in the splitting field of P_k if and only if its degree is less than k.*

These theorems should be compared to the similarly numbered statements in the example from the introduction. The main task of this paper is to prove theorem E2, and then apply our "vague principle" from the introduction. Consequently the *Leitfaden* is as follows. In section two, the polynomials P_k will be introduced, a theorem of Rankin & Swinnerton-Dyer type will be derived, and properties of reductions of P_k will be related to supersingularity of Drinfeld modules and class numbers of hyperelliptic function fields. The third paragraph will contain auxiliary results from the theory of primitive permutation groups and local Galois theory. In the fourth paragraph, a proof of the main theorem will be presented: a "big" cycle in $\mathrm{Gal}(P_k)$ is produced by consideration of certain inertia groups. Then transitivity is proved by combining a counting argument on these cycles with the analogue of Rankin's & Swinnerton-Dyer's result. A group theoretic lemma subsequently implies primitivity, and using results of Jordan-Marggraff and Wielandt, the Galois group is alternating or symmetric. In the fifth section, a link with 8-divisibility of class numbers is exploited to produce an even element in the Galois group. There, we prove the following incongruence result for class numbers of imaginary quadratic extensions of function fields:

Notation. For $\mathfrak{a} \in A$, we denote by $h(\mathfrak{a})$ the class number of $A[\sqrt{\mathfrak{a}}]$.

Theorem H. *(i) Fix a non-square $e \in \mathbf{F}_q$. For a prime $\mathfrak{p}$ of A, the class number $h(e\mathfrak{p})$ is even if and only if $\deg \mathfrak{p}$ is, and is divisible by 4 if and only if $\deg \mathfrak{p}$ is.*

(ii) Fix a characteristic $p > 0$. If k is a fixed integer divisible by 4, then there exists a constant $C_{k,p}$ such that for all $q > C_{k,p}$ there exist two primes $\mathfrak{p}$ and $\mathfrak{p}'$ of degree k in A and non-squares e, e' in $\mathbf{F}_q^*$ such that $h(e\mathfrak{p})$ and $h(e'\mathfrak{p}')$ are incongruent modulo 8.

To the extension $K(\sqrt{e\mathfrak{p}})$ corresponds a hyperelliptic curve $X : y^2 = e\mathfrak{p}(x)$, and the $\mathbf{F}_q$-rational points of its Jacobian are related to the class group of $A[\sqrt{e\mathfrak{p}}]$. Theorem H is proved using the action of Galois on the 2- and 4-torsion of this Jacobian. Part (ii) follows from a specialization argument on the generic such hyperelliptic curve using Chebotarëv's density theorem and some linear algebra in $J[4]$ as a $\mathbf{Z}/4$-module.

Finally, an application to supersingular reduction of Drinfeld modules is given in section six, generalizing [5]. Assume that F is a field equipped with an A-algebra structure $i : A \to F$. Denote the endomorphisms of the additive group scheme over F by additive polynomials in the variable X. Let

$$\phi : A \to \mathrm{End}(\mathbf{G}_a(F))$$

be a rank two A-Drinfeld module defined over F, *i.e.* a ring morphism such that $\phi(a)$ has (1) linear part $i(a)X$ and (2) degree $q^{2\deg(a)}$ in X. The second of these requirements says that ϕ has "rank two"; since this will hold for all Drinfeld modules we consider, we will omit references to the rank from now on. An endomorphism of ϕ is by definition an element $u \in \mathrm{End}(\mathbf{G}_a(\bar{F}))$ such that $u \circ \phi = \phi \circ u$. If F is finite, ϕ (or its j-invariant $j(\phi) = g^{q+1}/\Delta$) is said to be supersingular if its ring of endomorphisms is non-commutative.

Let L be a finite extension of K with ring of integers $\mathcal{O}$ (*i.e.*, the integral closure of A in L), and ϕ a Drinfeld module over L. Assume that $\phi(T) = TX + gX^q + \Delta X^{q^2}$ for certain $g, \Delta \in \mathcal{O}$. For a prime $\mathfrak{B}$ of $\mathcal{O}$ not dividing Δ it makes sense to consider the reduction of ϕ mod $\mathfrak{B}$ as a Drinfeld module over the finite field $\mathcal{O}/\mathfrak{B}$, and $\mathfrak{B}$ is said to be a prime of supersingular reduction of ϕ if its reduction is supersingular.

Definition. A non-zero algebraic integer j over K is said to be (k, L)-*lifting* for an integer k and a finite extension L of K if $j \in L$ and $j = j(z)$ for some zero z of E_{q^k-1}.

Theorem S. *Let L/K be a Galois extension of degree $[L : K]$ with ring of integers $\mathcal{O}$. Assume that $\phi(T) = TX + gX^q + \Delta X^{q^2}$ is a Drinfeld module with $g, \Delta \in \mathcal{O}$. If $j = j(\phi) \in \mathcal{O}$ is integral non-zero, then for any $k \geq 1$, either j is (k, L)-lifting, or*

$$\sum_{\deg(\mathfrak{p}) \leq k} f(\mathfrak{p}) \deg(\mathfrak{p}) s(\mathfrak{p}) \leq m(k) \cdot \max\{q[L : K], \log_q |\mathcal{O}/j|\},$$

where $\mathfrak{p}$ runs over the primes of A, $f(\mathfrak{p})$ is the residue degree of $\mathfrak{p}$, and $s(\mathfrak{p})$ is the number of supersingular primes of $\mathcal{O}$ which lie above $\mathfrak{p}$, but do not divide g nor Δ.

The theorem should be contrasted with the asymptotic results of Brown ([2]). The inequality in theorem S imposes restrictions on the number of

supersingular invariants of a *fixed* degree. The point is that theorems E1-E3 show that j is only very rarely (k, L)-lifting. Theorem E1 implies that such liftings have degree q. Theorem E2 (or rather, (4.2)) implies in particular that the only (k, K)-lifting j-invariant is $j = T^q - T$ for $k = 2$ (this is the case considered in [5]). More generally, if $[L : K] < m(k)$, then there are no (k, L)-lifting elements in L.

One can also combine theorem S and theorem E2 for families of j-invariants. If $\{j_1, ..., j_n\}$ is a set of distinct j-invariants in L which do not satisfy the bound in theorem S for a certain even k, then forcedly

$$n \leq m(k) \text{ and } [K(j_1, ..., j_n) : K] \geq n!/2.$$

For example, making a few crude estimates shows that there are at most $q^2 + 1$ integral j-invariants for which the number of supersingular primes $\mathfrak{B}$ in $\mathcal{O}$ that lie above a prime of degree 4 in A is larger then $q^5/4$.

Let us finally remark that a Drinfeld module can (by definition) have good reduction at a prime $\mathfrak{B}$ dividing the global discriminant Δ, namely if it does not divide the $\mathfrak{B}$-local minimal discriminant. Hence there can be more supersingular primes then the ones considered above. If ϕ admits a global minimal model (*e.g.* if the class number of L is one), we can apply the theorem to it, and the problem does not occur. We will not pursue this topic any further here (but compare [5], (1.4)).

2. The polynomials P_k

This section presents a short reminder on the polynomials P_k as they were introduced in [4]. It is our policy to give brief indications of the proofs, and refer to that reference for details. It follows from the theory of Drinfeld modules that g has a simple zero at the elliptic point $j = 0$ and nowhere else, and that Δ has a simple zero at the cusp of $GL(2, A)$ and is non-zero on Ω. The modular *function*

$$f_k(z) = (-1)^{k-1} \prod_{i \leq k} \langle i \rangle g(z)^{-\chi(k)} \Delta(z)^{-m(k)} E_{q^k-1}(z)$$

has no poles on Ω, and hence is a polynomial in $j(z)$. This turns out to be our polynomial P_k: $f_k(z) = P_k(j(z))$. There exists a recursion formula connecting the Eisenstein series E_{q^k-1}, and by retranslating it we find:

(2.1) Recursion Formula. *$P_k(j) \in A[j]$ is a polynomial satisfying the recursion $P_0 = P_1 = 1$ and for $k \geq 2$:*

$$P_k(j) = j^{d(k)} P_{k-1} - \langle k-1 \rangle P_{k-2}, \text{ with } d(k) = \frac{q^{k-1} + (-1)^k}{q+1}. \square$$

(2.2) Examples.

$$\begin{aligned}
P_2(j) &= j - \langle 1\rangle,\\
P_3(j) &= j^q - \langle 1\rangle j^{q-1} - \langle 2\rangle,\\
P_4(j) &= j^{q^2+1} - \langle 1\rangle j^{q^2} - \langle 2\rangle j^{q^2-q+1} - \langle 3\rangle j + \langle 1\rangle\langle 3\rangle,\\
P_5(j) &= j^{q^3+q} - \langle 1\rangle j^{q^3+q-1} - \langle 2\rangle j^{q^3} - \langle 3\rangle j^{q^3-q^2+q}\\
&\quad + \langle 1\rangle\langle 3\rangle j^{q^3-q^2+q-1} - \langle 4\rangle j^q + \langle 1\rangle\langle 4\rangle j^{q-1} + \langle 2\rangle\langle 4\rangle.
\end{aligned}$$

(2.3) Theorem E1. *The roots of P_k have absolute value q^q. The zeros of E_{q^k-1} in the domain $\{z \in \Omega : |z| = \inf\{|z-a| : a \in A\} \geq 1\}$ (to which any point of Ω can be mapped by $GL(2,A)$) are on the "unit circle" $|z| = 1$. They are simple and transcendental over K.*

Sketch of proof. The first statement follows from the fact that the Newton polygon of P_k for the valuation $-\deg$ is a straight line of slope q: if we write

$$P_k(j) = \sum_{i=0}^{m(k)} c_i^{(k)} j^{m(k)-i},$$

then

$$|c_i^{(k)}| = q^{qi} \text{ if } c_i^{(k)} \neq 0. \tag{2.3.1}$$

(This is verified inductively using the recursion formula.) The second statement follows from estimates relating $|j(z)|$ and $|z|$. A theorem of Yu [27] implies that non-transcendental zeros of E_{q^k-1} have complex multiplication. An estimate for the j-invariants of such CM-points by Brown ([2], (2.8.2)) shows that they never have absolute value q^q. Finally, the proof that the zeros are simple is a generalization of the one given for $k = 1$ by Gekeler ([10], VII.3.3). It will also follow independently from (4.2). □

The next proposition shows that the case $k = 3$ is special compared to theorem (E2), apparently because all supersingular invariants in degree 3 are rational (*cf.* (2.7)).

(2.4) Proposition. *The Galois group of P_3 is the affine group $AGL(1, \mathbf{F}_q)$.*

Proof. Taking derivatives in (2.2), we see that P_3 is separable. Substituting $Y = j^{-1}$ in P_3, we find

$$-\langle 2\rangle^{-1} j^{-q} P_3(j) = f(Y) = Y^q + aY + b,$$

with $a = \langle 1\rangle/\langle 2\rangle, b = -1/\langle 2\rangle$. P_3 (hence f) is irreducible over K, since it is an Eisenstein polynomial for the prime T of A. Consider the polynomial

$g(X) = X^{q-1} + a$; it is also irreducible over K, since if we substitute $X = Z^{-1}$, we get $\langle 1\rangle Z^{q-1} + \langle 2\rangle$, and this is an Eisenstein polynomial for any prime of degree two in A. Let α be a root of g in an algebraic closure of K. Since K contains all $(q-1)$-th roots of unity, $K(\alpha)/K$ is cyclic with Galois group $G := \mathrm{Gal}(K(\alpha)/K) \cong \mathbf{F}_q^*$. Let y be a root of f in an algebraic closure of K. Then

$$f = \prod_{x\in\mathbf{F}_q} (Y - y - x\alpha),$$

so the splitting field of f is $L := K(y + x\alpha | x \in \mathbf{F}_q) = K(y, \alpha)$. The extension $L/K(\alpha)$ is of Artin-Schreier type of degree q, with Galois group $H := \mathrm{Gal}(L/K(\alpha)) \cong \mathbf{F}_q$. The group G is normal in $\mathrm{Gal}(L/K)$, and $G \cap H = \{1\}$. Hence the semi-direct product $G \rtimes H \cong AGL(1, \mathbf{F}_q)$ belongs to $\mathrm{Gal}(L/K)$ and is of order $q(q-1)$. Since

$$|\mathrm{Gal}(L/K)| = [L : K] = [L : K(\alpha)][K(\alpha) : K] = q(q-1),$$

we find the desired result. □

(2.5) Proposition. *Let $\mathfrak{p}$ be a prime of degree n in A. Then the following congruences hold:*

$$\forall k \geq 0 : \quad P_{k+n} = j^{\chi(k)d(n+1)} P_k^{q^n} P_n \ \mathit{mod}\ \mathfrak{p}.$$

Proof. Using recursion and the fact that $\langle k+n-1\rangle \equiv \langle k-1\rangle^{q^n} \bmod \mathfrak{p}$.□

(2.6) Proposition (Gekeler [11] Sect. 5). *Let $\mathfrak{p}$ be a prime of degree k in A. Then $j^{\chi(k)} P_k(j)$ mod $\mathfrak{p}$ is the supersingular polynomial for rank 2-Drinfeld modules modulo $\mathfrak{p}$, i.e., its roots are the supersingular j-invariants over $A/\mathfrak{p}$.* □

(2.7) Proposition (Gekeler [9] (5.6), [10] (3.7), (6.4)). *The supersingular polynomial modulo $\mathfrak{p}$ has simple roots, factorizes over $A/\mathfrak{p}$ into the product of linear and quadratic factors, and for k even, the number $Q_\mathfrak{p}$ of quadratic factors of the supersingular polynomial satisfies*

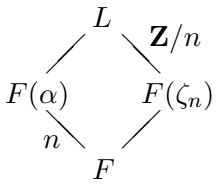
$$4Q_\mathfrak{p} = 2m(k) - h(e\mathfrak{p}),$$

where e is some non-square in $\mathbf{F}_q$. □

3. Resources from group theory and Galois theory

(3.1) Proposition. *Let F be a local field of residual characteristic p, f an Eisenstein polynomial over F of degree n, coprime to p. Then the inertia group of the splitting field of f is generated by an n-cycle.*

Proof. Let α be a root of f. The extension $F(\alpha)/F$ is totally ramified of degree n, and since $(n,p)=1$ we have $F(\alpha)=F(\sqrt[n]{\pi})$ for some uniformizing element $\pi \in F$. The normal closure of $F(\alpha)$ is $L := F(\alpha)(\zeta_n)$, where ζ_n is a primitive n-th root of unity.



Since $(n,p)=1$, the extension $F(\zeta_n)/F$ is unramified, and hence $F(\zeta_n)$ and $F(\alpha)$ are linearly disjoint. Hence $[L:F(\zeta_n)]=[F(\alpha):F]=n$, so f is irreducible over $F(\zeta_n)$. But $\mathrm{Gal}(L/F(\zeta_n))$ is the inertia group of L/F, and hence cyclic of order n since $(n,p)=1$ (*e.g.* [21], IV.2 Cor. I). Since f is irreducible over $F(\zeta_n)$, this cyclic group is also transitive on the n roots of f. Hence it is generated by an n-cycle. □

(3.2) Proposition. *A transitive permutation group of degree n, containing a subgroup that acts transitively on $d > \frac{n}{2}$ letters, and stabilizes the other letters, such that d and n are coprime, is primitive.*

Proof. Assume that G acts transitively on $\Omega = \{1,...,n\}$ as a permutation group, and H is a subgroup of G acting transitively on $D = \{1,...,d\}$, where $d > \frac{n}{2}$, but fixes $\Omega - D$. Let B be a non-trivial block for G. We can assume that $|B| \leq \frac{n}{2}$.

Assume that $\{i,j\} \in B$ for some $i \leq d$ and $j > d$ (such $j > d$ exists since $d < n$). Then for all $h \in H : hj = j \in B \cap hB$, so $H \cdot B = B$ (since B is a block). But $D = H \cdot \{i\} \subseteq H \cdot B = B$, so $d < |B| \leq \frac{n}{2}$, a contradiction.

Hence either $B \subseteq D$ or $B \subseteq \Omega - D$. Since G is transitive, translates of B are blocks that cover Ω. Finally, $|B|$ has to divide both $|D| = d$ and $|\Omega| = n$. □

(3.3) Proposition (Jordan). *A primitive permutation group of degree n containing an m-cycle ($m > 1$) is at least $(n-m+1)$-transitive.*

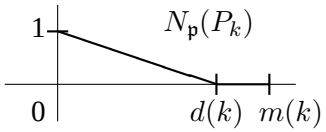
Remark. This theorem is frequently attributed to Marggraff, although it appears to have been stated first by Jordan. For some history and an up-to-date proof, one can consult [18], *pp.* 273-274. □

(3.4) Proposition (Wielandt [26]). *The degree of transitivity t of a permutation group of degree n not containing A_n is bounded by $t < 3 \log n$.*

Remark. Alternatively, it follows from the classification of finite simple groups that $t < 6$. □

4. Proof of theorem E2

(4.1) $\mathrm{Gal}(P_k)$ *contains a* $d(k)$*-cycle.* Let $\mathfrak{p}$ be a prime of degree $k-1$ in A. The Newton polygon of P_k over the completion $K_\mathfrak{p}$ consists of a segment from $(0,1)$ to $(d(k),0)$ and a segment from $(d(k),0)$ to $(m(k),0)$.



As the first segment contains no lattice points, P_k must factor as $P_k = fg$ over $K_\mathfrak{p}$, where f is an Eisenstein polynomial of degree $d(k)$. Since $P_k = j^{d(k)}P_{k-1}$ mod $\mathfrak{p}$, it follows that g mod $\mathfrak{p}$ is the supersingular polynomial for $\mathfrak{p}$ for even k, and the supersingular polynomial divided by j for odd k. Hence it has no multiple roots by (2.7). So elements of the inertia group $I(P_k/\mathfrak{p})$ of P_k over $K_\mathfrak{p}$ act trivially on the roots of g. Hence $I(P_k/\mathfrak{p}) \cong I(f/\mathfrak{p})$.

Since $d(k)$ and q are coprime, lemma (3.1) on local fields implies that the inertia group of f at $\mathfrak{p}$ is cyclic, generated by a $d(k)$-cycle. By the above, we find it in the inertia group of P_k at $\mathfrak{p}$, and *a fortiori* in the Galois group of P_k.

(4.2) *Irreducibility.* Suppose that $P_k = fg$ for two factors $f, g \in A[j]$. In the previous paragraph, we have already found an irreducible factor of P_k of degree $d(k)$ over the completion of K at a prime of degree $k-1$, and hence one can assume that $\deg f \geq d(k)$. For any prime $\mathfrak{p}$ of degree $k-1$ in A, there is a factorization $P_k = f_\mathfrak{p} g_\mathfrak{p}$ over $K_\mathfrak{p}$, with $f_\mathfrak{p}$ irreducible of degree $d(k)$. For reasons of degree, g divides $g_\mathfrak{p}$, and since $g_\mathfrak{p} = P_{k-1}$ mod $\mathfrak{p}$, one finds that g divides P_{k-1} mod $\mathfrak{p}$. Let α be a root of g; it follows that

$$P_{k-1}(\alpha) = \mathfrak{a} \prod \mathfrak{p}$$

holds in $A[\alpha]$, for some integral element $\mathfrak{a}$, where the product runs over all irreducible $\mathfrak{p}$ of degree $k-1$ in A.

Assume that $\mathfrak{a} \neq 0$. Since $P_k(\alpha) = 0$, it follows from (2.3) that $|\alpha| = q^q$, and by (2.3.1), the coefficient of $j^{m(k-1)-i}$ in P_{k-1}, if it is non-zero, has absolute value q^{qi}. Hence we see that all terms of $P_k(\alpha)$ have absolute value $q^{qm(k-1)}$. Finally,

$$\log_q |\mathfrak{a}| + \log_q |\prod \mathfrak{p}| = \log_q |P_{k-1}(\alpha)| \leq qm(k-1).$$

On the other hand,

$$\log_q |\mathfrak{a}| \geq 0, \;\; \log_q |\prod \mathfrak{p}| = (k-1)N_{k-1},$$

where N_{k-1} is the number of primes of degree $k-1$ in A. We claim that

$$qm(k-1) < (k-1)N_{k-1}.$$

It is equivalent to

$$q^{k-2} + q^{k-4} + ... + q^{2-\chi(k)} < \sum_{d|k-1} \mu(\frac{k-1}{d}) q^d = q^{k-1} + ...,$$

(where μ is the Möbius function). This, however, is clear from considering the numbers in the inequality as q-adic expansions (On the right hand side, the only q-adic digits occurring are ± 1, and $q > 2$).

In conclusion, $\mathfrak{a} = 0$, so α is a root of both P_{k-1} and P_k. Hence by using the recursion (2.1) in the opposite direction, one finds inductively that $P_1(\alpha) = 0$, a contradiction. So g has no root, *i.e.* it is constant. □

(4.3) *Group theory, revisited.* By (4.2), the Galois group of P_k is transitive as a permutation group on the roots, and the $d(k)$-cycle of (4.1) generates a cyclic subgroup which acts transitively on $d(k) > \frac{m(k)}{2}$ roots and leaves the rest fixed. For k even, since $qd(k) + (1-q)m(k) = 1$, $d(k)$ and $m(k)$ are coprime. By (3.2), we conclude that $\mathrm{Gal}(P_k)$ is primitive. Since it also contains a $d(k)$-cycle, one obtains from (3.3) that it is $(m(k) - d(k) + 1) = (m(k-1) + 1)$-transitive. Since $m(k-1) + 1 \geq 3 \log m(k)$ for $k > 3$, it follows from (3.4) that $\mathrm{Gal}(P_k)$ contains the alternating group of degree $m(k)$.

(4.4) *An odd element in the Galois group.* To decide in favour of $S_{m(k)}$ instead of $A_{m(k)}$, we will produce an odd element in the Galois group by using theorem H.

Assume first of all that k is divisible by 4. By (2.7), primes $\mathfrak{p}$ of degree k in A are unramified in any root field of P_k, and their decomposition group is generated by a product of $Q_{\mathfrak{p}}$ transpositions. Hence there is an odd element in $\mathrm{Gal}(P_k)$ if we can show that $Q_{\mathfrak{p}}$ is odd for some $\mathfrak{p}$. Since $m(k)$ is constant if k is, it suffices (again by (2.7)) to show that there exist non-squares $e, e' \in \mathbf{F}_q$ and primes $\mathfrak{p}, \mathfrak{p}'$ of degree k in A with $h(e\mathfrak{p}) \not\equiv h(e'\mathfrak{p}') \bmod 8$. But for big enough q, this follows from theorem H, which will be proved in the next section.

Finally, assume that $k = 2 \bmod 4$. Then for any prime $\mathfrak{q}$ of degree $k-2$ in A we have that

$$P_k(j) = (j - \langle 1 \rangle)^{q^{k-2}} P_{k-2}(j) \bmod \mathfrak{q},$$

and the corresponding Newton polygon consists of a segment from $(0,1)$ to $(q^{k-2}, 0)$ and a segment from $(q^{k-2}, 0)$ to $(m(k), 0)$. In this case, $k-2$ is divisible by 4. By the previous argument, we can find a $\mathfrak{q}$ such that $Q_{\mathfrak{q}}$ is

odd. The corresponding product $\bar{\tau}$ of $Q_{\mathfrak{q}}$ transpositions in Gal(P_{k-2} mod $\mathfrak{q}$) lifts to an element $\sigma\tau$ of Gal$(P_k/K_{\mathfrak{q}})$ where σ is in the inertia group of $\mathfrak{q}$ by the above congruence (a similar argument was used at the end of (4.1)). Hence also the (odd) element τ belongs to Gal(P_k). □

5. Proof of theorem H

(5.1) *Hyperelliptic curves.* Assume that q is an odd prime power. Let F be a field with exact field of constants $\mathbf{F}_q$, and e a non-square in F. Consider the projective hyperelliptic curve X of which the affine equation is given by

$$y^2 = ef(x), \;\; f(x) = x^k + \sigma_1 x^{k-1} + ... + \sigma_k, \;\; \sigma_1, ..., \sigma_k \in F,$$

for $k > 2$, where f is separable, and has k distinct roots $t_1, ..., t_k$ in a fixed algebraic closure of F. We will assume *throughout* that f is irreducible over F. The above plane model is singular at infinity as soon as $k > 3$, and its genus g satisfies $2g = k - 2$ if k is even and $2g = k - 1$ if k is odd. Let J denote the Jacobian of X (*viz.* of a non-singular projective model of X).

(5.2) *Jacobians and class numbers.* If $F = \mathbf{F}_q$ itself is a finite field, then we have the following exact sequence ([22], II.2.2)

$$1 \to J(\mathbf{F}_q) \to \mathrm{Cl}(\mathbf{F}_q[x, \sqrt{ef(x)}]) \to \mathbf{Z}/d_\infty \mathbf{Z} \to 1,$$

where d_∞ is the degree of a place above $\infty = \frac{1}{x}$ in $F(X)$ and Cl denotes the ideal class group. Since e is not a square, $d_\infty = 2$ if k is even and $d_\infty = 1$ if k is odd. This is why we will study the field of definition of the 2- and 4-torsion of J, but a priori for more general fields F (because we will use a specialization argument afterwards).

(5.3) *The field of definition of* $J[2]$. Assume first of all that k is even, and F again arbitrary as in (5.1). Then for $i = 2, ..., k$ one finds

$$\mathrm{div}(\frac{x - t_i}{x - t_1}) = 2D_i, \text{ where } D_i = (t_i, 0) - (t_1, 0).$$

In the Jacobian J of X we have that $D_i \in J[2]$, and these divisors satisfy the linear relation

$$\sum_{i=2}^{k} D_i = \mathrm{div}(y(x - t_1)^{-\frac{k}{2}}) = 0$$

in J. Furthermore, $\{D_2, ..., D_{k-1}\}$ form a basis for $J[2] \cong (\mathbf{Z}/2)^{2g}$.

On the other hand, if k is odd, then for any $i = 1, ..., k$, we have that

$$\mathrm{div}(x - t_i) = 2D_i, \text{ where } D_i = (t_i, 0) - \infty.$$

Again, $D_i \in J[2]$, these divisors satisfy the linear relation

$$\sum_{i=1}^{k} D_i = \text{div}(y) = 0$$

in J, and $\{D_1, ..., D_{k-1}\}$ form a basis for $J[2]$. (Remark that geometrically, the $(t_i, 0)$ are exactly the Weierstraß points of X.)

We see that the field of definition of the two-torsion in the Jacobian of X (given by adjoining the coordinates of $\{D_i\}$ to F) is contained in the splitting field of f. Assume for a moment that $\text{Gal}(f/F) = S_k$. If $k > 4$, then the alternating group A_k is simple. It is easy to see from the action of S_k on $\{D_i\}$ that $\text{Gal}(F(J[2])/F)$ is not trivial nor cyclic of order two, so we have that $\text{Gal}(F(J[2])/F) = S_k$ too. The same conclusion holds for $k = 3$ by computing the action of S_3 on $\{D_1, D_2, D_3\}$. On the other hand, if $k = 4$, then one sees that the subgroup of $\text{Gal}(f/F)$ generated by the products of two transpositions fixes the divisors D_i (using the linear relation between them), and in that case, $\text{Gal}(F(J[2])/F) = S_3$ is dihedral. In conclusion:

(5.3.1) Lemma. *If, in the setting of (5.1), we assume furthermore that f has Galois group S_k over F, then the same holds for $F(J[2])/F$ if $k \neq 4$. If $k = 4$, then Gal$(F(J[2])/F) = S_3$ instead.*

(5.4) *The Galois representation on $J[2]$.* The action of the absolute (separable) Galois group of F on $J[2] \cong (\mathbf{Z}/2)^{2g}$ induces a faithful representation

$$\rho_1 : \text{Gal}(F(J[2])/F) \hookrightarrow GL(2g, \mathbf{F}_2).$$

We can now prove the following:

(5.5) Proposition. *(i) Let $F = \mathbf{F}_q$ be a finite field, e a non-square in $\mathbf{F}_q$ and $\mathfrak{p}$ irreducible of degree k over $\mathbf{F}_q$. Then the class number $h(e\mathfrak{p})$ is even if and only if k is even, and divisible by 4 if and only if k is divisible by 4.*

(ii) If k is divisible by 4, then $h(e\mathfrak{p})$ is divisible by 8 if and only if $J[4](\mathbf{F}_q)$ contains an element of order 4.

Proof. Let $F = \mathbf{F}_q$ and $f := \mathfrak{p}$ in the setting of (5.1). Since f is irreducible, its (cyclic) Galois group over F is generated by the k-cycle $\sigma = (t_1 t_2 ... t_k)$. If k is even, it follows from (5.2) that $h(e\mathfrak{p})$ is even (since $d_\infty = 2$).

On the other hand, if k is odd, then $h(e\mathfrak{p})$ is even if and only if $J[2](F) \neq 0$. For this to happen, $\rho_1(\sigma)$ has to fix a non-zero vector in $GL(k-1, \mathbf{F}_2)$, *i.e.*, $\det(\rho_1(\sigma) - 1) = 0$. One can compute the action of $\rho_1(\sigma)$ on the basis $\{D_1, ..., D_{k-1}\}$ using the relation given in (5.3):

$$\rho_1(\sigma) = \begin{pmatrix} 0\,0\,\ldots\,0\,0\,1 \\ 1\,0\,\ldots\,0\,0\,1 \\ 0\,1\,\ldots\,0\,0\,1 \\ \vdots\,\vdots\,\ddots\,\vdots\,\vdots\,\vdots \\ 0\,0\,\ldots\,1\,0\,1 \\ 0\,0\,\ldots\,0\,1\,1 \end{pmatrix}, \quad (k-1)\times(k-1)$$

and it is immediate that $\det(\rho_1(\sigma)-1) = 1$. Hence $h(e\mathfrak{p})$ is not even if k is odd.

If k is even, we have w.r.t. the basis $\{D_2, ..., D_{k-1}\}$:

$$\rho_1(\sigma) = \begin{pmatrix} 1\,1\,\ldots\,1\,1\,0 \\ 1\,0\,\ldots\,0\,0\,1 \\ 0\,1\,\ldots\,0\,0\,1 \\ \vdots\,\vdots\,\ddots\,\vdots\,\vdots\,\vdots \\ 0\,0\,\ldots\,1\,0\,1 \\ 0\,0\,\ldots\,0\,1\,1 \end{pmatrix}, \quad (k-2)\times(k-2)$$

and it is easy to see that

$$4|h(e\mathfrak{p}) \iff J[2](F) \neq 0 \iff \det(\rho_1(\sigma)-1) = 0 \iff 4|k.$$

We even see that $\rho_1(\sigma)$ is a Jordan block (its nilpotency order is $k-2$). Hence $\rho_1(\sigma)$ has a unique fixed vector in $J[2]$, *i.e.*, $J[2^\infty](\mathbf{F}_q)$ is a *cyclic* group. From this and (5.2), part (ii) is immediate. □

(5.6) *The field of definition of* $J[4]$. Let F again not necessarily be finite, but from now on, assume that k is divisible by 4. We will compute the extension $F(J[4])/F(J[2])$, and for this it is useful to change the shape of the equation of X, *over* $F(J[2])$. For $k > 4$, the latter field contains the roots of f. Now over a field which contains one root of f, we can find an isomorphism which maps X to

$$\tilde{X}: \ y^2 = \tilde{f}(x), \text{ where } \tilde{f}(x) = (x-u_1)...(x-u_{k-1})$$

over $\tilde{F} := F(t_1, u_1, ..., u_{k-1})$ ([24], I.1.4). To find a basis for the 4-torsion in J we have to find divisors $\tilde{E}_i$ such that $2\tilde{E}_i = \tilde{D}_i$ for each $i = 1, ..., k-1$, where the $\tilde{D}_i$ span the 2-torsion on the Jacobian $\tilde{J}(\cong_{\tilde{F}} J)$ of $\tilde{X}$, as in the odd case of (5.3). By Kummer theory ([23], 4.6), for any field L containing $F(J[2])$ we have an injective group homomorphism

$$\tilde{J}(L)/2\tilde{J}(L) \hookrightarrow (L^*/L^{*2})^k,$$

for which the image of the divisors $\tilde{D}_i$ may be computed explicitly to be

$$\tilde{D}_i \to (u_i - u_1, ..., u_i - u_k),$$

(*see* [3], 11.1). If $\tilde{D}_i = 2\tilde{E}_i$ and $\tilde{E}_i$ is defined over L, then the image of the Kummer map is zero on $\tilde{D}_i$. Hence:

(5.6.1) Lemma. $F(J[4]) = F(J[2])(\sqrt{u_i - u_j};\ i,j = 1,...,k-1)$. □

(5.6.2) *Remark.* For $k = 4$, the above argument shows that $F(J[4],t_1) = F(J[2],t_1)(\sqrt{u_i - u_j};\ i,j = 1,2,3)$ One can check that this does not obstruct the argumentation that follows.

(5.7) *The Galois representations on* $J[4]$. The groups $J[M]$ carry an alternating, Galois-equivariant form, called the Weil-pairing ([17], par. 16).

Convention. To prevent us from too much duplication, we will assume in the main text that the fourth roots of unity are contained in F, and *anything between set delimiters* $\{\ \}$ *is concerned with the case when* $\sqrt{-1} \notin F$.

The action of the absolute Galois group $\mathrm{Gal}(\bar{F}/F)$ of the separable closure $\bar{F}$ of F on the 4-torsion produces an action on $(\mathbf{Z}/4)^{2g}$ which leaves invariant ($\{$scales$\}$) an alternating form, *i.e.*, it is given by symplectic matrices ($\{$symplectic similitudes$\}$). We arrive at the following diagram of representations:

$$\begin{array}{ccc}
 & 1 & 1 \\
 & \downarrow & \downarrow \\
\rho_3 : & \mathrm{Gal}(F(J[4])/F(J[2])) & \hookrightarrow \quad K \\
 & \downarrow & \downarrow \\
\rho_2 : & \mathrm{Gal}(F(J[4])/F) & \hookrightarrow \{G\}Sp(k-2,\mathbf{Z}/4) \\
 & \downarrow & \downarrow \\
\rho_1 : & \mathrm{Gal}(F(J[2])/F) & \hookrightarrow \{G\}Sp(k-2,\mathbf{Z}/2) \\
 & \downarrow & \downarrow \\
 & 1 & 1
\end{array}$$

where K is defined as the kernel of the natural reduction map

$$\{G\}Sp(k-2,\mathbf{Z}/4) \to \{G\}Sp(k-2,\mathbf{Z}/2).$$

(5.8) *Linear algebra over* $\mathbf{Z}/4$. We will assume to have conjugated all matrices in the above diagram such that the Weil pairing takes on the form $S = \mathrm{diag}(J,...,J)$ in the sense of block matrices, where $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (this is possible over $\mathbf{Z}/4$ by copying the classical arguments over fields). An element $\kappa \in \{G\}Sp(k-2,\mathbf{Z}/4)$ is in the kernel K if and only if it is of the form $\kappa = 2m+1$ and $\kappa S \kappa^t = \{\lambda\}S$ for some $m \in \mathrm{Mat}(2g \times 2g)$ ($\{\lambda = \pm 1\}$). The symplectic condition is $2(mS + Sm^t)\{+(1-\lambda)S\} = 0$, which in its turn is equivalent to $mS = Sm^t\{+\frac{1-\lambda}{2}S\}$ mod 2. If we write $m = (M_{ij})$ as a block matrix consisting of g^2 matrices M_{ij} of order 2×2,

then the symplectic condition is equivalent to

$$(*) \quad M_{ji}^t = JM_{ij}J \bmod 2 \text{ and } \mathrm{tr}(M_{ii}) = 0\{+\frac{1-\lambda}{2}\} \bmod 2$$

for all i and all $j \neq i$.

(5.8.1) Lemma. *If $[F(J[4]) : F(J[2])] = 2^{g(2g+1)\{+1\}}$, then ρ_3 is an isomorphism.*

Proof. The same $\kappa \in K$ has two representations $\kappa = 2m+1 = 2m'+1$ if and only if $m = m' \bmod 2$. This allows us to count the number of elements in K. For $i < j$, choose M_{ij} arbitrary modulo 2: this can be done in $(2^4)^{\frac{g(g-1)}{2}}$ ways. Then M_{ji} is completely determined modulo 2 by $(*)$. One can then choose M_{ii} of given trace modulo 2 in $(2^3)^{k-2}$ ways ({resp. in $2 \cdot (2^3)^{k-2}$ ways}). We finally see that $|K| = 2^{g(2g+1)\{+1\}}$. □

(5.8.2) Lemma. *A matrix h in $Sp(k-2, \mathbf{Z}/4)$ does not have a fixed vector of order 4 in $J[4]$ if $\det(h-1) = 2$.*

Proof. If γ^{ad} denotes the classical adjoint of a matrix γ, $(h-1)^{ad}(h-1) = \det(h-1) \cdot 1$, so if v is a fixed vector of h,

$$2v = \det(h-1)v = (h-1)^{ad}(hv - v) = 0,$$

whence v is of order two. □

(5.9) Proposition. *Let k be divisible by 4, and σ the image of the cycle $(t_1 ... t_k)$ in $Gal(F(J[2])/F)$. Assume that ρ_3 is an isomorphism. Then there exist two lifts of σ to $Gal(F(J[4])/F)$ such that one of them has a fixed vector of order 4 in $J[4]$ and the other one does not. {Furthermore, if $\mu_4 \not\subseteq F$, then one can choose such lifts with either action ± 1 on $\sqrt{-1}$.}*

Proof. Since ρ_3 is an isomorphism, it suffices to find matrices $h, h' \in \{G\}Sp(k-2, \mathbf{Z}/4)$ lifting $\rho_1(\sigma)$ having/not having a fixed vector of order 4 {and having determinant ± 1}. The matrix $\rho_1(\sigma)$ has a fixed vector v in $J[2]$, hence any of its lifts to $\{G\}Sp(k-2, \mathbf{Z}/4)$ has the same fixed vector v, which is of order two in $J[4]$, so $v = 2w$ for some w of order 4 in $J[4]$. We fix one such lift $\bar{h}$ ({resp. two such lifts $\bar{h}_\pm$, where the subscript denotes the sign of the determinant of $\bar{h}$}).

If we write $\rho_1(\sigma)$ with respect to a new, standard sympletic basis, we may assume that $w = e_i$ for one of the standard vectors e_i of this basis. Indeed, choose i such that w is not orthogonal e_i. Then the symplectic transvection

$$x \mapsto x + \frac{(e_i - w)Sx^t}{e_i S w^t}(e_i - w)$$

preserves S and maps w to e_i (see Artin [1]).

{The rest of the proof applies equally well to $h_\pm$ as it does to h.} There exists a $\kappa = 2m+1 \in K$ {of determinant one} such that the lift $h = \kappa\bar{h}$ to $\{G\}Sp(k-2, \mathbf{Z}/4)$ fixes w. Indeed, since $\bar{h}2w = 2w$, we have $\bar{h}w = w + 2z$ for some vector z. Consequently, $\kappa\bar{h}w = w$ if and only if $(2m+1)(w+2z) = w$, *viz.* $2mw = \bar{h}w - w$. Now $\bar{h}$ and $w = e_i$ being given, this condition only fixes the i-th column of m modulo two, and we can then choose m ({and $\lambda = 1$}) to satisfy the conditions in $(*)$, so that κ is symplectic ({and has determinant one}).

On the other hand, to prove that there exists a lift $h' = \kappa' h$ for some $\kappa' = 2m' + 1$ which does not fix a vector of order 4, it suffices by lemma (5.8.2) to have that $\det(\kappa' h - 1) = 2$, *viz.*, $\det(h - 1 + 2m') = 2$ (since κ' will have determinant one). Since h is constructed such that it fixes e_i, the i-th column of $h-1$ is identically zero.

We introduce the following notation: for a matrix γ and an indexing set $I = \{(i_1, j_1), ..., (i_l, j_l)\}$, we denote by $[\gamma, I]$ the I-th cofactor of γ (*i.e.*, the determinant of the matrix given by deleting the rows and columns going through the elements $\gamma_{i_\alpha, j_\alpha}$ for $\alpha = 1, ..., l$). If $l = 1$, the cofactor is called principal.

From the explicit form of $\rho_1(\sigma) - 1$ given in (5.5), we see that its rank (and that of $h-1$) is $k-3$ (since $[\rho_1(\sigma) - 1, (1, k-2)] \neq 0$). Hence at least one of the principal cofactors of $h-1$ is invertible in $\mathbf{Z}/4$. This implies that one of the cofactors of the i-th row of $h-1$ is a unit, say $[h-1, (i,j)] = \pm 1$ (since all other principal cofactors are zero, as the zero row occurs in them). We then choose m' to have 0-entry everywhere, except $m'_{ij} = 1$, and possibly one more non-zero entry $m'_{k,l}$ to assure that m' satisfies the symplectic conditions $(*)$. Then by multilinearity

$$\det(h - 1 + 2m) = 2 \cdot [h-1, (i,j)] + 4 \cdot [h-1, \{(i,j),(k,l)\}] = 2,$$

and we are done. {Note that since $\det(\kappa) = \det(\kappa') = 1$, the lifts of $\bar{h}_\pm$ have determinant ± 1.} □

(5.10) Proposition. *Fix a characteristic $p > 0$. Let k be a positive integer divisible by 4. For q odd and big enough depending on p and k, there exist non-squares e, e' in $\mathbf{F}_q^*$ and $\mathfrak{p}, \mathfrak{p}'$ irreducible polynomials in $\mathbf{F}_q(x)$ such that the class number $h(e\mathfrak{p})$ is divisible by 8 and the class number $h(e'\mathfrak{p}')$ is not.*

Proof. Consider the condition

$$[F(J[4]) : F(J[2])] = 2^{g(2g+1)\{+1\}}. \tag{5.10.1}$$

It is fulfilled for the "generic" hyperelliptic curve as in (5.1) over the field $\mathcal{F} = \mathbf{F}_p(e, \sigma_1, ..., \sigma_k)$, where e, σ_i are independent transcendental parameters. Indeed, the discriminant of f (and $\tilde{f}$) is then squarefree (modulo constants in $\mathbf{F}_p$), so if $u_\alpha - u_\beta = u_\gamma - u_\delta$ modulo squares, then $\{\alpha, \beta\} = \{\gamma, \delta\}$.

It follows from (5.6.1), that the degree $[\mathcal{F}(J[4]) : \mathcal{F}(J[2])]$ is $\binom{k-1}{2} = g(2g+1)$.

Now let $F := \mathbf{F}_p(t)$ for a transcendental t. Since F is Hilbertian, Hilbert's irreducibility theorem ([8], chapter 12) implies that there exists a specialization $e(t), \sigma_i(t)$ of $e, \sigma_i \in \mathcal{F}$ to F such that (5.10.1) holds, and the corresponding $f \in F(x)$ has Galois group S_k over F. For this F and f, the corresponding ρ_3 is an isomorphism by (5.8.1).

By Chebotarëv's theorem (see the appendix to [14]), for big enough n (bounded below in terms of p and k), there exist primes P, P' of degree n in F whose Frobenius elements act conjugate to h and h' on $J[4]$. Then since h and h' act like a k-cycle σ on the roots of f by construction, $\mathfrak{p} := f \bmod P$ and $\mathfrak{p}' := f \bmod P'$ remain irreducible over $\mathbf{F}_q := \mathbf{F}_p[t]/P = \mathbf{F}_{p^n}$. If n is even or $p \equiv 1 \bmod 4$, then $\mu_4 \subseteq \mathbf{F}_q$; if n is odd and $p \equiv 3 \bmod 4$, then Frob_q acts like -1 on $\sqrt{-1}(\notin \mathbf{F}_q)$, hence we choose h_- then (and similarly for P' and h').

The above constructions apply to any $e(t)$ which is not a square in F, irrespective of its precise form. We choose it to be a non-square modulo P and P', and set $e = e(t) \bmod P$ and $e' = e(t) \bmod P'$.

It then makes sense to consider the reduction of the diagram in (5.7) modulo P and P' respectively. We see that in the first case, $\mathrm{Frob}_q = h$ has a fixed vector of order 4 in $J[4]$, so $h(e\mathfrak{p})$ is divisible by 8 by (5.5), (ii). In the second case, $\mathrm{Frob}_q = h'$ does not have a fixed vector of order 4 in $J[4]$, so $h(e'\mathfrak{p}')$ is not divisible by 8. Also, the resulting Frob_q has the right action on $\sqrt{-1}$ by construction. This finishes the proof of theorem H. □

(5.10.2) *Remark.* The argument of the first paragraph even applies if $k = 4$. Namely, let $d = [F(t_1) : F]$. Then we know that we can choose the specializations of σ_i to satisfy $[F(t_1, J[4]) : F] = 48d$. Since $[F(J[2]) : F] = 6$, $[F(J[4]) : F(J[2])] \leq |K| = 8$ and $[F(t_1, J[4]) : F(J[4])] \leq d$, both these inequalities are actually equalities.

(5.10.3) *Remark.* It might be possible to suppress the dependence of $C_{p,k}$ on p by a good effective version of Hilbert irreducibility over K ([7]).

6. Supersingularity

(6.1) Proposition (Gekeler, [9]). *Let ϕ be a Drinfeld module over a finite field F equipped with an A-algebra structure $i : A \to F$. Let $\mathfrak{i} = \ker(i)$. Then ϕ is supersingular if and only if the coefficient of $X^{q^{\deg(\mathfrak{i})}}$ in $\phi(\mathfrak{i})$ is zero.* □

(6.2) Proposition. *Let ϕ be a Drinfeld module over a finite extension L of K, and assume that $\phi(T) = TX + gX^q + \Delta X^{q^2}$ for some $g, \Delta \in \mathcal{O}$, where $\mathcal{O}$ is the ring of integers of L. Set $j = g^{q+1}/\Delta$. Let $\mathfrak{B}$ be a prime ideal of*

$\mathcal{O}$, not dividing Δ, and set $\mathfrak{p} = \mathfrak{B} \cap A$. Let $l_{\mathfrak{p}}(g, \Delta)$ be the coefficient of $X^{q^{\deg(\mathfrak{p})}}$ in $\phi(\mathfrak{p})$. Then:

(i) $\mathfrak{B}$ is a supersingular prime of ϕ if and only if $l_{\mathfrak{p}}(g, \Delta) = 0$ mod $\mathfrak{B}$.
(ii) ("Deligne's congruence") $l_{\mathfrak{p}}(g, \Delta) = P_{\deg \mathfrak{p}}(j)\Delta^{m(k)}g^{\chi(k)}$ mod $\mathfrak{B}$.

Proof. The first part follows immediately from (6.1). For $L = K$, part (ii) is the contents of theorem (11.5) in [11]. The proof is inductive, using the recursion formula for P_k. A careful inspection of the arguments show that they go through in our setting. □

(6.3) *Proof of theorem S.* Let $\phi, g, \Delta, j, L, \mathcal{O}$ be as in the statement of the theorem. Assume S is the set of supersingular primes $\mathfrak{B}$ for ϕ, such that $\mathfrak{B} \cap A$ is of degree $i \leq k$, not dividing g, Δ. Since $\mathfrak{B}$ does not divide g and Δ, we find by (6.2) that

$$P_i(j) = 0 \bmod \mathfrak{B}.$$

Now the congruences in (2.5) also hold modulo $\mathfrak{B}$ (an easy check), so the previous formula implies that $\mathfrak{B}|P_k(j)$. Taking everything together, we find that the following inclusion of ideals holds:

$$P_k(j) \cdot \mathcal{O} \subseteq \prod_{\mathfrak{B} \in S} \mathfrak{B}$$

since the different $\mathfrak{B}$ are coprime. If we define $\deg_{\mathcal{O}}$ by $\deg_{\mathcal{O}}(\mathfrak{A}) = \log_q |\mathcal{O}/\mathfrak{A}|$ (*i.e.*, the extension of the degree-function on $\mathcal{O}$ to the non-zero ideals of $\mathcal{O}$), then the above implies that either $P_k(j) = 0$, so j is (k, L)-lifting, or

$$\deg_{\mathcal{O}}(P_k(j)) \geq \sum_S \deg_{\mathcal{O}}(\mathfrak{B}).$$

Using (2.3.1), we find that

$$\deg_{\mathcal{O}}(c_i^{(k)}) = [L : K] \deg(c_i^{(k)}) = [L : K]qi,$$

and a small computation gives that

$$\deg_{\mathcal{O}}(P_k(j)) \leq m(k) \cdot \max\{q[L : K], \log_q |\mathcal{O}/j|\}.$$

On the other hand,

$$\deg_{\mathcal{O}}(\mathfrak{B}) = f(\mathfrak{B}) \deg(\mathfrak{B} \cap A),$$

where $f(\mathfrak{B}) = [\mathcal{O}/\mathfrak{B} : A/(\mathfrak{B} \cap A)]$ is the residue degree of $\mathfrak{B}$. If we assume that L/K is Galois, and put everything together, we find

$$\sum_{\deg(\mathfrak{p}) \leq k} f(\mathfrak{p}) \deg(\mathfrak{p}) s(\mathfrak{p}) \leq m(k) \cdot \max\{q[L : K], \log_q |\mathcal{O}/j|\},$$

where $f(\mathfrak{p})$ is the residue degree of $\mathfrak{p}$, and $s(\mathfrak{p})$ is the number of supersingular primes $\mathfrak{B}$ not dividing g, Δ and lying above $\mathfrak{p}$ in $\mathcal{O}$. □

Acknowledgements. The author is post-doctoral fellow of the Fund for Scientific Research - Flanders (FWO -Vlaanderen). Part of this work was done while visiting the MPIM. Thanks to Jan Van Geel for his stimulating interest. The original proof of theorem H worked only under more restrictive conditions; the current argument in paragraph 5 was suggested by a referee.

References

1. E. Artin, Geometric algebra, Wiley Classics Library, New York, 1988
2. M.L. Brown, Singular moduli and supersingular moduli of Drinfeld modules, Invent. Math. **110** (1992), 419–439
3. J.W.S. Cassels, E.V. Flynn, Prolegomena to a middlebrow arithmetic of curves of genus 2, LMS Lecture Note Series **230**, Cambridge University Press, Cambridge, 1996
4. G. Cornelissen, Sur les zéros des séries d'Eisenstein de poids $q^k - 1$ pour $GL_2(\mathbf{F}_q[T])$, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), 817–820
5. G. Cornelissen, Deligne's congruence and supersingular reduction of Drinfeld modules, Arch. der Math., to appear
6. V.G. Drinfeld, Elliptic modules, Math. Sb. **94(136)** (1974), 594–627
7. T. Ekedahl, An effective version of Hilbert's irreducibility theorem, in: Séminaire de Théorie des Nombres, Paris 1988–1989 (C. Goldstein, ed.), Progr. Math. **91**, Birkhäuser Boston, 1990, 241–249
8. M.D. Fried, M. Jarden, Field arithmetic, Ergebnisse der Math. und ihrer Grenzgebiete (3), **11**, Springer-Verlag, Berlin-New York, 1986
9. E.-U. Gekeler, Zur Arithmetik von Drinfeld-Moduln, Math. Ann. **262** (1983), 167–182
10. E.-U. Gekeler, Drinfeld modular curves, Lecture Notes in Math., vol. 1231, Springer, Berlin - Heidelberg - New York, 1986
11. E.-U. Gekeler, On the coefficients of Drinfeld modular forms, Invent. Math. **93** (1988), 667–700
12. E.-U. Gekeler, Some new results on modular forms for $GL(2, \mathbf{F}_q[T])$, in: Recent Progress in Algebra (S.G. Hahn, H.C. Myung, E. Zelmanov, eds.), Contemp. Math. **224** (1998), 111–141
13. E.-U. Gekeler, M. Reversat, Jacobians of Drinfeld modular curves, J. Reine Angew. Math. **476** (1996), 27–93
14. W.D. Geyer, M. Jarden, Bounded realization of l-groups over global fields. The method of Scholz and Reichardt, Nagoya Math. J. **150** (1998), 13–62
15. D. Goss, Modular forms for $F_r[T]$, J. Reine Angew. Math. **317** (1980), 16–39
16. J. Hoffstein, Real zeros of Eisenstein series, Math. Z. **181** (1982), no. 2, 179-190
17. J.S. Milne, Abelian Varieties, in: Arithmetic geometry (G. Cornell, J. Silverman, eds.), Springer-Verlag, New York-Berlin, 1986
18. P.M. Neumann, Some primitive permutation groups, Proc. London Math. Soc. (3) **50** (1985), 265–281
19. F.K.C. Rankin, H.P.F. Swinnerton-Dyer, On the zeros of Eisenstein series, Bull. London Math. Soc. **2** (1970), 169–170
20. R.A. Rankin, The zeros of certain Poincaré series, Compositio Math. **46** (1982), 255–272

21. J.-P. Serre, Corps locaux, Actualités scientifiques et industrielles, vol. 1296, Hermann, Paris, 1968
22. J.-P. Serre, Trees, Springer-Verlag, Berlin-New York, 1980
23. J.-P. Serre, Lectures on the Mordell-Weil theorem, Aspects of Mathematics, **E15**, Vieweg, Braunschweig, 1989
24. I.R. Shafarevich, Basic algebraic geometry. 1. Varieties in projective space, Springer-Verlag, Berlin, 1994
25. G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. of the Math. Soc. of Japan, vol. 11, Iwanami Shoten and Princeton University Press, 1971
26. H. Wielandt, Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad, Werke, vol. I, 23–46, de Gruyter, Berlin - New York, 1994
27. J. Yu, Transcendence and Drinfeld modules, Invent. Math. **83** (1986), 507–517

Note added in proof. At the cost of enlarging $C_{p,k}$, one can indeed assume that it is independent of p, as was suggested in remark (5.10.3). For this, let $F = \mathbf{F}_q(t)$ in the proof of (5.10) and find P, P' of degree *one*. One can then also choose $e = e'$ in theorem H.