A HYPERELLIPTIC SMOOTHNESS TEST, II

H. W. LENSTRA Jr, J. PILA *and* CARL POMERANCE

[Received 28 June 1999]

Contents

1. *Introduction*

This is our second paper devoted to the description and analysis of the *hyperelliptic curve method*. The hyperelliptic curve method is a probabilistic algorithm for factoring integers. It is well suited to finding small prime factors of an integer and, in particular, to recognizing smooth integers, that is, integers built from small prime numbers.

The hyperelliptic curve method is closely related to the elliptic curve method [**8**]. We refer the reader to the introduction to our first paper [**9**] for a discussion of the provenance of the hyperelliptic curve method, its relation to the elliptic curve method, and comparison of run times with other algorithms.

The hyperelliptic curve method uses the Jacobian varieties of curves of genus 2 over finite fields in the same way that the elliptic curve method uses elliptic curves over finite fields. Let k be a finite field of odd characteristic, and let q be its cardinality. Let $f \in k[X]$ be a sextic or quintic polynomial with non-vanishing discriminant. Let C_f be the smooth projective curve over k whose function field is the field of fractions of $k[X, Y]/(Y^2 - f)$, so that the genus of C_f equals 2. Denote by J_f the Jacobian variety of C_f, and by $J_f(k)$ the set of k-rational points of J_f, which is a finite Abelian group. Since C_f has genus 2, the Riemann Hypothesis for Abelian varieties over finite fields, proved by Weil [**22**], implies that

$$\#J_f(k) \in [(\sqrt{q} - 1)^4, (\sqrt{q} + 1)^4],$$

where # denotes cardinality. So $\#J_f(k)$ resides in an interval of length $\sim 8q^{3/2}$ centered at $\sim q^2$ as $q \to \infty$. (We use the notation $A(q) \sim B(q)$ as $q \to \infty$ to mean that $A(q)/B(q) \to 1$ as $q \to \infty$.) The number of sextic and quintic polynomials

The authors acknowledge the support of the National Science Foundation under grant numbers DMS 9224205, DMS 9104316 and DMS 9701101.

2000 *Mathematics Subject Classification*: 11Y05, 11G10, 11M20, 11N25.

over k with non-vanishing discriminants is $\sim q^7$ as $q \to \infty$. Therefore, the assignment

$$f \mapsto \#J_f(k)$$

has fibres whose *average* size is $\sim \frac{1}{8} q^{11/2}$ as $q \to \infty$. If we restrict to quintic polynomials then the fibres have average size $\sim \frac{1}{8} q^{9/2}$ as $q \to \infty$.

The main results of the present paper concern the size of the fibres over the integers z in a subinterval of $[(\sqrt{q}-1)^4, (\sqrt{q}+1)^4]$. This subinterval is of the form $[q^2 - cq^{3/2}, q^2 + cq^{3/2}]$, where c is positive and explicit. Excluding a small set of values for z, we show that the size of each fibre is not much smaller than the average value that we just computed. Thus, the assignment $f \mapsto \#J_f(k)$ distributes the polynomials f fairly evenly over a substantial subinterval of $[(\sqrt{q}-1)^4, (\sqrt{q}+1)^4]$.

Our first result restricts to prime fields and to quintic polynomials. Prime fields are the only ones that arise in the analysis of the hyperelliptic curve method. Curves C_f with quintic polynomials f are attractive to use, since their Jacobians are particularly easy to construct and to operate in.

THEOREM 1.1. *Let p be a prime number with $p \geqslant 8100$, and let $\mathbb{F}_p$ denote the prime field of cardinality p. Then for all but at most p integers z in the interval $[p^2 - \frac{1}{2} p^{3/2}, p^2 + \frac{1}{2} p^{3/2}]$ there are at least*

$$\frac{p^{9/2}}{24{,}000 \cdot (\log p)^2 \cdot (\log\log p)^2}$$

quintic polynomials $f \in \mathbb{F}_p[X]$ with non-vanishing discriminants such that $\#J_f(\mathbb{F}_p) = z$.

If we do not insist that the curves have quintic models, we can prove a result valid for all finite fields of odd characteristic, with a smaller exceptional set. This result is not needed for our analysis of the hyperelliptic curve method.

THEOREM 1.2. *Suppose that k is a finite field, and suppose that the cardinality q of k is odd and at least 14,400. Then for all but at most $28\sqrt{q}$ integers z in the interval $[q^2 - \frac{1}{9} q^{3/2}, q^2 + \frac{1}{9} q^{3/2}]$ there are at least*

$$\frac{q^{11/2}}{48{,}000 \cdot (\log q)^2 \cdot (\log\log q)^2}$$

sextic polynomials $f \in k[X]$ with non-vanishing discriminants such that $\#J_f(k) = z$.

No great significance should be attached to the constants 24,000 and 48,000 occurring in the theorems beyond the fact that they are explicit. They are definitely open to improvement.

We briefly explain the role that Theorem 1.1 plays in the analysis of the hyperelliptic curve method. The success of the hyperelliptic curve method depends on $\#J_f(\mathbb{F}_p)$ being sufficiently smooth – that is, built up entirely of sufficiently small prime factors – with reasonable probability when f is selected at random. The precise sense of 'sufficiently smooth' and 'reasonable probability' in our situation is discussed in [**9**].

To prove that $\#J_f(\mathbb{F}_p)$ is sufficiently smooth with reasonable probability, one

first shows that an interval of the form $[x - cx^{3/4}, x + cx^{3/4}]$ contains reasonably many numbers that are sufficiently smooth. Such a result is contained in our first paper, [**9**], in which we proved various theorems about the density of smooth numbers in short intervals. Taking $x = p^2$ and $c = \frac{1}{2}$ one finds that the interval $[p^2 - \frac{1}{2}p^{3/2}, p^2 + \frac{1}{2}p^{3/2}]$ contains a fair number of sufficiently smooth integers z. Next one applies Theorem 1.1 to these values of z to see that there is a reasonably large number of quintics f for which $\#J_f(\mathbb{F}_p)$ is sufficiently smooth. This is the required result. For more details, and for an application of our result to primality testing, we refer to the forthcoming third paper in this series.

Our main theorems provide only a lower bound for the number of f such that $J_f(k)$ has order z. For elliptic curves an upper bound of the same form – up to powers of logarithms – is given in [**8**, Proposition 1.9]. One may believe that in the case of hyperelliptic curves there is also an upper bound of the same form, but the arguments that we give do not suffice to prove this.

Adleman and Huang [**1**, Chapter 4, Proposition 1] prove a result similar to Theorem 1.2. However, their argument is restricted to prime numbers z, which does not suffice for our purposes. Their result also admits a much larger set of exceptions.

The structure of the proof of Theorems 1.1 and 1.2, and of the paper, is as follows. In § 2 the proofs are reduced to the proof of four auxiliary propositions. The first of these (Proposition 2.1) estimates the number of f for which C_f is isomorphic to a given curve C of genus 2. The proof is elementary, and it is given in § 3. The second (Proposition 2.2) concerns the reconstruction of C from its Jacobian, viewed as a principally polarized Abelian variety. The only new feature of this result is a sufficient condition, in terms of the Jacobian, for C to possess a quintic model; the details are given in § 3. Our third auxiliary result (Proposition 2.3) estimates the number of two-dimensional principally polarized Abelian varieties with a given 'Weil polynomial'. The proof occupies five sections. In § 4 we use the arguments of Stark [**19**] to obtain an effective lower bound for certain quotients of class numbers (Proposition 4.2). In § 5 we prove the integrality of a suitable quotient of zeta functions of finite rings. Combining these results, we obtain in § 6 an effective lower bound for appropriately defined class numbers of certain orders in number fields. Section 7 contains generalities concerning fourth degree Weil polynomials. Once all these ingredients are available, we give the proof of Proposition 2.3 in § 8. It is based on a result of Deligne [**4**] that establishes an equivalence of categories between the category of *ordinary* Abelian varieties over finite fields, and a certain category of free $\mathbb{Z}$-modules with additional structure. We also employ results of Howe [**6**] on the translation of the notion of polarization of ordinary Abelian varieties under Deligne's equivalence. Abelian varieties that are ordinary are the only ones that we use; thus, Theorems 1.1 and 1.2 remain valid if the additional condition that J_f be ordinary is imposed on f. The final result of § 2 (Proposition 2.4) asserts that for most z in our target interval an appropriate Weil polynomial can be constructed. The proof, which is given in § 10, is completely elementary but somewhat involved; it makes use of a result on non-uniqueness of factorization in short intervals that is presented in § 9. It may be of interest to pursue the latter subject for its own sake.

Fields of characteristic 2 are excluded in Theorems 1.1 and 1.2, not only because we use models of the form $y^2 = f(x)$ for hyperelliptic curves, but also because certain parts of our proof admit a larger set of exceptions when the

characteristic equals 2. In § 11 we state separately some results valid in characteristic 2.

Throughout this paper, a 'curve' will mean a smooth absolutely irreducible projective variety of dimension 1. All maps between varieties will be rational over the base field, unless the contrary is explicitly stated. All rings are supposed to be commutative with unit element, and the unit element is supposed to be respected by ring homomorphisms and to be contained in subrings. The group of units of a ring R is denoted by R^*. By $\mathbb{Z}$ we denote the ring of integers, and by $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ the fields of rational, real and complex numbers, respectively.

Acknowledgement. The authors thank J. Cremona, E. W. Howe, N. M. Katz, S. Louboutin and P. Sarnak for their assistance.

2. *Articulation of the proofs*

Let k be a finite field and q its cardinality. Theorems 1.1 and 1.2 are statements about the fibres of the map from the set of sextic or quintic polynomials over k with non-vanishing discriminants to $\mathbb{Z}$, sending f to $\#J_f(k)$. In the present section we write this map as the composition of four maps. We formulate auxiliary results, to be proved in later sections, about the fibres of each of these maps. At the end of the section we deduce Theorems 1.1 and 1.2 from these results.

From polynomials to curves. The first map goes from the set of sextic or quintic polynomials over k with non-vanishing discriminants to the set of isomorphism classes of curves of genus 2 over k. It is defined only if q is *odd*, and it sends f to the curve C_f whose function field is the field of fractions of $k[X, Y]/(Y^2 - f)$; it does have genus 2, by [**20**, Proposition VI.2.3(b)]. If C is a curve of genus 2 over k, then we call a sextic or quintic polynomial f a *representative* of C if $C \cong C_f$.

PROPOSITION 2.1. *Let k be a finite field of odd cardinality q, and let C be a curve of genus 2 over k. Then the number of representatives of C equals*

$$\frac{(q^2-1)(q^2-q)}{\#\operatorname{Aut} C}.$$

Also, there exists an integer $r(C)$ satisfying

$$0 \leqslant r(C) \leqslant 6, \quad r(C) \equiv \#C(k) \mod 2,$$

such that C has exactly

$$\frac{r(C)(q-1)(q^2-q)}{\#\operatorname{Aut} C} \quad \textit{and} \quad \frac{(q+1-r(C))(q-1)(q^2-q)}{\#\operatorname{Aut} C}$$

quintic and sextic representatives, respectively.

The proof of this proposition is routine. It is given in § 3.

From curves to principally polarized Abelian varieties. A *principally polarized Abelian variety* over k is a pair (A, ξ) consisting of an Abelian variety A over k and a principal polarization $\xi\colon A \to \check{A}$ of A over k; here $\check{A}$ denotes the dual

Abelian variety. An isomorphism $\psi\colon (A,\xi)\to(B,\eta)$ of principally polarized Abelian varieties is an isomorphism $\psi\colon A\to B$ of Abelian varieties satisfying $\xi=\check{\psi}\eta\psi$. For all these terms, see [**11**].

The second map goes from the set of isomorphism classes of curves of genus 2 over k to the set of isomorphism classes of principally polarized two-dimensional Abelian varieties over k. It takes C to the pair (J_C,ξ_C), where J_C is the Jacobian variety of C (see [**12**]) and ξ_C is the canonical principal polarization of J_C induced by the theta divisor (see [**12**, 6.11]).

An Abelian variety over k is called *absolutely simple* if it has, after base extension to an algebraic closure of k, exactly two Abelian subvarieties, namely $\{0\}$ and the Abelian variety itself. For the definition of the *trace* of the Frobenius endomorphism of an Abelian variety A over k we refer to [**11**, §§ 12 and 19].

PROPOSITION 2.2. *Let k be any finite field, and q its cardinality. Let (A,ξ) be a principally polarized absolutely simple Abelian variety of dimension 2 over k. Then (A,ξ) is isomorphic to the canonically polarized Jacobian variety of some curve C of genus 2 defined over k, and for any such C we have $\operatorname{Aut} C\cong\operatorname{Aut}(A,\xi)$. If, in addition, both q and the trace of the Frobenius endomorphism of A are odd, then any curve C of genus 2 with $(J_C,\xi_C)\cong(A,\xi)$ possesses a quintic representative.*

The proof of this proposition is given in § 3. The first part of Proposition 2.2 is well known.

From Abelian varieties to Weil polynomials. By a *Weil q-polynomial* we mean a polynomial $h\in\mathbb{Z}[X]$ of even degree, with leading coefficient 1, all of whose complex zeros have absolute value $\sqrt{q}$, and which satisfies $h(0)>0$ (and therefore $h(0)=q^{(\deg h)/2}$). If A is an Abelian variety over k, then we denote by h_A the characteristic polynomial of the Frobenius endomorphism of A (see [**11**, §§ 12 and 19]); this is a Weil q-polynomial of degree $2\dim A$, by [**11**, Theorem 19.1] (the property $h_A(0)>0$ follows from $h_A(1)=\#A(k)>0$ and the absence of zeros of h_A in the interval $[0,1]$; see [**11**, Theorem 19.1(b) and (c)]).

The third map goes from the set of principally polarized two-dimensional Abelian varieties over k to the set of Weil q-polynomials of degree 4. It sends (A,ξ) to h_A.

As we shall see in Proposition 7.1, the Weil q-polynomials of degree 4 are exactly the polynomials h of the form

$$h=(X^2+q)^2-aX(X^2+q)+bX^2,$$

where a and b are integers satisfying

$$2|a|\sqrt{q}-4q\leqslant b\leqslant\tfrac{1}{4}a^2\leqslant 4q.$$

Moreover, a and b are uniquely determined by h. We say that such a polynomial h is *ordinary* if b is not divisible by the characteristic of k, that h has *odd trace* if a is odd, that h is *regular* if neither of the numbers a^2-4b and $(b+4q)^2-4qa^2$ is an integer square (see Remark 7.6 for an interpretation of these conditions), and we define

$$c(h)=(a^2-4b)^{1/2}\cdot((b+4q)^2-4qa^2)^{1/2}.$$

By the *weighted number* of principally polarized Abelian varieties (A, ξ) in a class S we mean $\sum 1/\#\mathrm{Aut}(A, \xi)$, the sum ranging over the isomorphism classes of pairs (A, ξ) in S. Note that $\mathrm{Aut}(A, \xi)$ is finite, by [**11**, Proposition 17.5(a)].

PROPOSITION 2.3. *Let k be a finite field, and suppose that the cardinality q of k is at least* 8100. *Let h be an ordinary regular Weil q-polynomial of degree* 4. *Then the weighted number of principally polarized two-dimensional Abelian varieties (A, ξ) over k with $h_A = h$ is at least*

$$\frac{c(h)}{95{,}000 \cdot (\log q)^2 \cdot (\log\log q)^2}.$$

Each such A is absolutely simple, and if h has odd trace, then the trace of the Frobenius endomorphism of any such A is odd.

The proof of Proposition 2.3 is given in § 8.

From Weil polynomials to integers. The fourth map goes from the set of Weil q-polynomials of degree 4 to $\mathbb{Z}$, and it sends h to $h(1)$. If A is an Abelian variety over k, then we have $h_A(1) = \#A(k)$ (see [**11**, Theorem 19.1(b)]). Hence the composition of the four maps does map a sextic or quintic polynomial $f \in k[X]$ with non-vanishing discriminant to $\#J_f(k)$.

PROPOSITION 2.4. (a) *Let $q \geqslant 14{,}400$ be an odd prime power. Then for all but at most $28\sqrt{q}$ integers z in the interval*

$$[q^2 - \tfrac{1}{9}q^{3/2}, q^2 + \tfrac{1}{9}q^{3/2}]$$

there is an ordinary regular Weil q-polynomial h of degree 4 *such that $h(1) = z$ and $c(h) \geqslant 2q^{3/2}$.*

(b) *Let $p \geqslant 8100$ be a prime number. Then for all but at most p integers z in the interval*

$$[p^2 - \tfrac{1}{2}p^{3/2}, p^2 + \tfrac{1}{2}p^{3/2}]$$

there is an ordinary regular Weil p-polynomial h of degree 4 *with odd trace such that $h(1) = z$ and $c(h) \geqslant 4p^{3/2}$.*

This result is proved in § 10.

Proof of Theorem 1.2. Suppose that q is odd and that $q \geqslant 14{,}400$. Let $z \in [q^2 - \frac{1}{9}q^{3/2}, q^2 + \frac{1}{9}q^{3/2}]$ be an integer that does not belong to the set of cardinality at most $28\sqrt{q}$ that is excepted in Proposition 2.4(a). It suffices to prove that the conclusion of Theorem 1.2 holds for z. By the choice of z and Proposition 2.4(a), we can choose an ordinary regular Weil q-polynomial h of degree 4 with $c(h) \geqslant 2q^{3/2}$ and $h(1) = z$. Applying Proposition 2.3 we find that the weighted number of principally polarized, absolutely simple two-dimensional Abelian varieties (A, ξ) with $h_A = h$ is at least

$$\frac{2 \cdot q^{3/2}}{95{,}000 \cdot (\log q)^2 \cdot (\log\log q)^2}.$$

By Proposition 2.2, the same lower estimate holds for the weighted number of curves C of genus 2, defined over k, with $h_{J_C} = h$; here the isomorphism class of C is counted with weight $1/\#\mathrm{Aut}\, C$. Each such curve C has, by Proposition 2.1, at least $(q-5)(q-1)(q^2-q)/\#\mathrm{Aut}\, C$ sextic representatives f. Thus the number of sextic $f \in k[X]$ with $h_{J_f} = h$ is at least

$$\frac{2 \cdot q^{3/2}(q-5)(q-1)(q^2-q)}{95{,}000 \cdot (\log q)^2 \cdot (\log\log q)^2}.$$

The conclusion of Theorem 1.2 now follows from the inequality

$$\frac{2 \cdot (q-5)(q-1)(q^2-q)}{95{,}000} \geqslant \frac{q^4}{48{,}000} \quad \text{for } q \geqslant 14{,}400,$$

and the observation that each of the sextic polynomials f with $h_{J_f} = h$ satisfies $\#J_f(k) = h(1) = z$. This proves Theorem 1.2.

Proof of Theorem 1.1. The proof of Theorem 1.1 follows the same lines as the proof of Theorem 1.2. One uses Proposition 2.4(b) instead of Proposition 2.4(a), and employs only Weil polynomials that have odd trace. Likewise, when applying Propositions 2.3, 2.2 and 2.1, one considers only Abelian varieties for which the trace of the Frobenius endomorphism is odd, and curves that possess a quintic representative; the last assertions of these three propositions are now invoked. This proves Theorem 1.1.

3. *Curves of genus* 2 *and their Jacobians*

Proof of Proposition 2.1. Let k be a finite field of odd cardinality q, and let C be a curve of genus 2 over k. By [**20**, Lemma VI.2.2(b) and Proposition VI.2.4(a)], the function field $k(C)$ of C has a unique subfield K with $[k(C) : K] = 2$ for which there exists $x \in K$ with $K = k(x)$; and by [**20**, Proposition VI.2.3(a)], there is a sextic or quintic polynomial $f \in k[x]$ with non-vanishing discriminant such that $k(C) = k(x, y)$ with $y^2 = f$. For such f we have $C \cong C_f$. This shows that C has at least one representative.

We shall denote the unique non-trivial automorphism of $k(C)$ that is the identity on K by τ, and refer to it as the *hyperelliptic involution*.

We next investigate isomorphisms between two curves C_f and C_g of genus 2. Write $k(C_f) = k(x, y)$ with $y^2 = f(x)$ and $k(C_g) = k(x', y')$ with $y'^2 = g(x')$, and suppose that we have an isomorphism $C_f \to C_g$, inducing a k-isomorphism $\sigma\colon k(C_g) \to k(C_f)$. The uniqueness of the subfield $k(x)$ implies that σ induces an isomorphism $k(x') \to k(x)$, so $\sigma(x') = (ax+b)/(cx+d)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in the group $\mathrm{GL}(2, k)$ of invertible 2×2 matrices over k. Also, $y/\sigma(y')$ is fixed under the hyperelliptic involution, so we have $\sigma(y') = h(x)y$ for some $h(x) \in k(x)^*$. We have

$$g((ax+b)/(cx+d)) = h(x)^2 f(x),$$

and since g is square-free we find that $h(x) = e/(cx+d)^3$ for some $e \in k^*$, and that

$$f(x) = e^{-2}(cx+d)^6 g((ax+b)/(cx+d)).$$

Conversely, if the latter equality holds for a pair

$$\left(e, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \in k^* \times \mathrm{GL}(2, k),$$

then

$$x' \mapsto (ax + b)/(cx + d), \quad y' \mapsto ey/(cx + d)^3$$

gives an isomorphism $C_f \to C_g$.

The group $G = k^* \times \mathrm{GL}(2, k)$ acts (on the right) on the set of square-free sextic or quintic polynomials in $k[X]$ by

$$g(X) \circ \left(e, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = e^{-2}(cX + d)^6 \cdot g((aX + b)/(cX + d)).$$

By the above, we have $C_f \cong C_g$ if and only if f and g belong to the same orbit under G. Hence, if we fix f, then the number of g for which $C_f \cong C_g$ equals $\#G$ divided by the order of the stabilizer of f in G. We have $\#G = (q-1) \cdot (q^2-1)(q^2-q)$. A pair $\left(e, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right)$ belongs to the stabilizer of f if and only if it gives an automorphism of C_f. The pairs that give the trivial automorphism are those that belong to the subgroup $\left\{\left(a^3, \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)\right) : a \in k^*\right\}$ of order $q-1$ of G. Hence the order of the stabilizer equals $(q-1) \cdot \mathrm{Aut}\, C_f$. This proves that the number of representatives of C_f equals $(q^2-1)(q^2-q)/\#\mathrm{Aut}\, C_f$. Since each C is of the form C_f, this implies the first assertion of Proposition 2.1.

To prove the second assertion, we let $r(C)$ be the number of elements of $C(k)$ that are fixed under τ. These elements are precisely the k-rational points of C that ramify under the map $C \to \mathbb{P}^1$ corresponding to the field extension $k(C) \supset k(x)$, and by [**20**, Proposition VI.2.3(c)] they correspond to the set of zeros of f in k, including one zero 'at infinity' if $\deg f = 5$. From $\deg f \leqslant 6$ it follows that $0 \leqslant r(C) \leqslant 6$. Also, since the points of $C(k)$ that are not fixed under τ come in pairs $\{P, \tau P\}$, we have $r(C) \equiv \#C(k) \bmod 2$. It remains to prove the statement about the number of quintic models.

Let us first consider isomorphism classes of pairs (C, P), where C is a curve of genus 2 over k and P is a point on $C(k)$ that is fixed under τ; here we call (C, P) and (C', P') isomorphic if there is an isomorphism $C \to C'$ mapping P to P'. When $f \in k[X]$ is a square-free quintic polynomial, then the rational function x on C_f has exactly one pole on C_f, which we call P_f. We have $P_f \in C_f(k)$, and P_f is fixed under τ, so the pair (C_f, P_f) is one of the pairs under consideration. Conversely, for every pair (C, P) there are exactly $(q-1)(q^2-q)/\#\mathrm{Aut}(C, P)$ square-free quintic polynomials f in $k[X]$ for which (C, P) is isomorphic to (C_f, P_f). To prove this, one mimics the part of the proof already given, with a few minor changes. The first change is that one needs to choose the element $x \in K$ such that it has a pole at P; this is possible, since the image of P in $\mathbb{P}^1$ belongs to $\mathbb{P}^1(k)$. Secondly, one should consider only isomorphisms $C_f \to C_g$ that map P_f to P_g, which is equivalent to the restriction $c = 0$ on the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ that one works with. Since the group of those matrices has order $(q-1)(q^2-q)$, one arrives at the formula $(q-1)(q^2-q)/\#\mathrm{Aut}(C, P)$ that we have just stated.

To count the number of quintic representatives one considers the map that sends the isomorphism class of a pair (C, P) to the isomorphism class of C. Let C be a curve of genus 2 over k. If $P, P' \in C(k)$ are fixed under τ, then the pairs (C, P)

and (C, P') are isomorphic if and only if P and P' belong to the same orbit under $\mathrm{Aut}\, C$. Thus the number of quintic representatives for C equals

$$\sum_P \frac{(q-1)(q^2-q)}{\#\mathrm{Aut}(C,P)},$$

the summation ranging over a set of orbit representatives for the action of $\mathrm{Aut}\, C$ on $\{P \in C(k)\colon \tau P = P\}$. We may also extend the sum to include *all* $P \in C(k)$ with $\tau P = P$ provided that each term is given a weight equal to the inverse of the orbit size of P under $\mathrm{Aut}\, C$. This orbit size equals $(\#\mathrm{Aut}\, C)/\#\mathrm{Aut}(C,P)$, which yields the formula stated in Proposition 2.1. Subtracting the number of quintic representatives from the total number of representatives one obtains the final formula in Proposition 2.1.

This proves Proposition 2.1, with the added information that $r(C)$ is the number of $\mathbb{F}_q$-rational points of C that are fixed under the hyperelliptic involution.

REMARK. It follows from Proposition 2.1 that C has at least one quintic model if and only if $r(C) > 0$, and that C has at least one sextic model unless and only unless $r(C) = q+1$. Also, the equality $r(C) = q+1$ can occur only if q equals 3 or 5. It is not hard to show that in those two cases one has $r(C) = q+1$ if and only if $C \cong C_f$ with $f = X^5 - X$.

Proof of Proposition 2.2. Let A be an absolutely simple Abelian variety of dimension 2 over $\mathbb{F}_q$, with dual $\check{A}$, and let $\xi\colon A \to \check{A}$ be a principal polarization. Let D be a positive divisor on A that is defined over k and belongs to the divisor class determining ξ; such a divisor exists since k is finite (see [**11**, Remark 13.2]). By [**11**, Theorem 13.3(b)], the self-intersection number of D equals $(D, D) = 2\sqrt{\deg \xi} = 2$. A theorem of Weil [**23**, Satz 2] (or see [**14**]) implies that this divisor is either a curve C of genus 2 or, over an algebraic closure $\overline{k}$ of k, equal to the sum of two positive divisors. In the first case, (A, ξ) is isomorphic to the principally polarized Jacobian of C; in the second case, A is, over $\overline{k}$, isomorphic to the product of two elliptic curves (see [**23**, **14**]). The latter alternative is excluded by our assumption that A be absolutely simple. Hence we have $(A, \xi) \cong (J_C, \xi_C)$.

Torelli's theorem (see [**12**, Corollary 12.2]) implies that C is uniquely determined, up to isomorphism, by the property that $(A, \xi) \cong (J_C, \xi_C)$. Also, the proof of Torelli's theorem, as given in [**12**], shows that for every $\beta \in \mathrm{Aut}(J_C, \xi_C)$ there is a unique $\alpha \in \mathrm{Aut}\, C$ that maps to β under the natural map $\mathrm{Aut}\, C \to \mathrm{Aut}(J_C, \xi_C)$ (cf. [**12**, Proposition 6.1]). Therefore we have $\mathrm{Aut}\, C \cong \mathrm{Aut}(A, \xi)$.

Next suppose that q and the trace t of the Frobenius endomorphism of A are odd. By [**12**, Theorem 11.1], we have $\#C(k) = 1 - t + q$, which is odd. Hence the number $r(C)$ from Proposition 2.1 is also odd. Therefore we have $r(C) \geqslant 1$, and by Proposition 2.1 the curve possesses a quintic model. This proves Proposition 2.2.

4. *Estimates for zeta functions*

Let K be an algebraic number field of finite degree n over the field $\mathbb{Q}$ of rational numbers. We write ζ_K for the zeta function of K, which is defined on

$\{s \in \mathbb{C}: \operatorname{Re} s > 1\}$ by

$$\zeta_K(s) = \prod_P \frac{1}{1 - N(P)^{-s}};$$

here P ranges over the set of maximal ideals of the ring of integers of K, and $N(P)$ is the cardinality of the residue class field of P. Denote by Δ the absolute value of the discriminant of K over $\mathbb{Q}$, by r_1 the number of real places of K, and by r_2 the number of complex places of K. For $s \in \mathbb{C}$, $\operatorname{Re} s > 1$, we define

$$\xi_K(s) = s(s-1) \cdot \Delta^{s/2} \cdot \left(\frac{\Gamma(s/2)}{2\pi^{s/2}}\right)^{r_1} \cdot \left(\frac{\Gamma(s)}{(2\pi)^s}\right)^{r_2} \cdot \zeta_K(s),$$

where Γ denotes Euler's gamma function. Note that for $s \in \mathbb{R}$ with $s > 1$, both $\zeta_K(s)$ and $\xi_K(s)$ are real and positive.

LEMMA 4.1. (a) *The function ξ_K can be analytically extended to an entire function satisfying the functional equation $\xi_K(s) = \xi_K(1-s)$.*

(b) *All zeros ρ of ξ_K satisfy $0 < \operatorname{Re}\rho < 1$, and one has*

$$\frac{\xi_K'(s)}{\xi_K(s)} = \frac{1}{2} \sum_\rho \left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}}\right)$$

for each $s \in \mathbb{C}$ with $\xi_K(s) \neq 0$; the sum ranges over all zeros ρ of ξ_K, counted with multiplicities, and it is absolutely convergent.

(c) *For $s \in \mathbb{R}$ with $s > 1$ one has*

$$0 < \frac{\xi_K'(s)}{\xi_K(s)} < \frac{1}{s} + \frac{1}{s-1} + \frac{\log\Delta}{2} + \frac{r_1}{2}\left(\frac{\Gamma'(s/2)}{\Gamma(s/2)} - \log\pi\right) + r_2\left(\frac{\Gamma'(s)}{\Gamma(s)} - \log(2\pi)\right).$$

(d) *If $K \neq \mathbb{Q}$, then there is at most one zero β of ξ_K that satisfies $\operatorname{Re}\beta \geqslant 1 - (4\log\Delta)^{-1}$ and $|\operatorname{Im}\beta| \leqslant (4\log\Delta)^{-1}$, and if there is one then it is real and simple.*

(e) *For $K \neq \mathbb{Q}$ and $s \in \mathbb{R}$ with $1 \leqslant s \leqslant 1 + 2(n-1)/\log\Delta$, one has*

$$\xi_K(s) \leqslant 2^{-r_1-r_2} \cdot \pi^{-r_2} \cdot \left(\frac{e \cdot \log\Delta}{2(n-1)}\right)^{n-1} \cdot \sqrt{\Delta}.$$

(f) *One has $\xi_K(1) = h \cdot \operatorname{reg}/w$, where h and* reg *denote the class number and regulator of K, respectively, and w is the number of roots of unity in K.*

Proof. For (a), see [**7**, Chapter XIII]. For (b), see [**7**, Chapter XV, Theorem 3 and Chapter XVII, § 1], as well as [**19**, Lemma 1]. For (f), one uses [**7**, Chapter VIII, Theorem 5] and the fact that $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ (see [**24**, 12.14]).

(c) From the definition of ζ_K one sees that $\zeta_K'(s)/\zeta_K(s) < 0$ for real $s > 1$. Combining this with the definition of ξ_K we find the upper bound in (c). The lower bound follows from the expression given in (b) (see [**19**, Lemma 3]).

(d) This is proved in [**19**, Lemma 3], as a consequence of (b) and (c).

(e) We follow [**10**, proof of Theorem 1]. For a real number $s \geqslant 1$ we define

$$g(s) = s^{1-r_1-r_2} \cdot \xi_{\mathbb{Q}}(s)^n \cdot \left(\frac{2 \cdot \Gamma((s+1)/2)}{\sqrt{\pi} \cdot s \cdot \Gamma(s/2)}\right)^{r_2}.$$

The logarithm of each of the three factors on the right is convex on $[1, \infty)$; for the first factor this is obvious, and for the last two factors it is the content of [**10**, Lemma 9]. It follows that $\log g$ is convex on $[1, \infty)$.

Put $\sigma = 1 + 2(n-1)/\log \Delta$. We claim that

$$g(\sigma) \leqslant g(1) = 2^{-r_1 - r_2} \cdot \pi^{-r_2}.$$

The equality is readily verified. We prove the inequality. From Minkowski's inequality $\sqrt{\Delta} \geqslant (\frac{1}{4}\pi)^{r_2} \cdot n^n/n!$ (see [**7**, Chapter V, § 4]) one finds in a routine manner that $\log \sqrt{\Delta} \geqslant \frac{1}{3}(n-1)$. Therefore we have $\sigma \leqslant 4$, and by convexity it follows that $g(\sigma) \leqslant \max(g(1), g(4))$. Now one deduces the claim from

$$g(4) = 4 \cdot \left(\frac{\xi_{\mathbb{Q}}(4)}{4}\right)^{r_1 + r_2} \cdot \left(\frac{2 \cdot \xi_{\mathbb{Q}}(4) \cdot \Gamma(5/2)}{\sqrt{\pi} \cdot 4 \cdot \Gamma(2)}\right)^{r_2}$$

$$= 4 \cdot \left(\frac{\pi^2}{60}\right)^{r_1 + r_2} \cdot \left(\frac{\pi^2}{40}\right)^{r_2} < \frac{1}{2^{r_1 + r_2}} \cdot \frac{1}{\pi^{r_2}},$$

except if $r_1 + r_2 = 1$. In the exceptional case K is imaginary quadratic, and one has $\Delta \geqslant 3$, $\sigma \leqslant 3$, and $g(\sigma) \leqslant \max(g(1), g(3))$; the inequality $\zeta_{\mathbb{Q}}(3)^2 < \zeta_{\mathbb{Q}}(2)$ (obtained from the Euler product) implies then that $g(3) = 3\zeta(3)^2 \pi^{-3} < (2\pi)^{-1} = g(1)$. This proves the claim.

Let s be real, $s > 1$. From the duplication formula [**24**, 12.15]

$$\frac{\Gamma(s/2)}{2\pi^{s/2}} \cdot \frac{\Gamma((s+1)/2)}{\pi^{(s+1)/2}} = \frac{\Gamma(s)}{(2\pi)^s}$$

for the gamma function, and from the elementary inequality $\zeta_K(s) \leqslant \zeta_{\mathbb{Q}}(s)^n$, one sees that

$$\xi_K(s) = s(s-1) \cdot \Delta^{s/2} \cdot \left(\frac{\Gamma(s/2)}{2\pi^{s/2}}\right)^n \cdot \left(\frac{\Gamma((s+1)/2)/\pi^{(s+1)/2}}{\Gamma(s/2)/(2\pi^{s/2})}\right)^{r_2} \cdot \zeta_K(s)$$

$$\leqslant \frac{\Delta^{s/2}}{(s-1)^{n-1}} \cdot \left(s(s-1) \cdot \frac{\Gamma(s/2)}{2\pi^{s/2}} \cdot \zeta_{\mathbb{Q}}(s)\right)^n \cdot \left(\frac{2 \cdot \Gamma((s+1)/2)}{\sqrt{\pi} \cdot s \cdot \Gamma(s/2)}\right)^{r_2} \cdot s^{1 - r_1 - r_2}$$

$$= \frac{\Delta^{s/2}}{(s-1)^{n-1}} \cdot g(s).$$

Substituting $s = \sigma$, which minimizes $\Delta^{s/2}/(s-1)^{n-1}$, we find that

$$\xi_K(\sigma) \leqslant \frac{\Delta^{(n-1)/\log \Delta} \cdot \Delta^{1/2}}{(2(n-1)/\log \Delta)^{n-1}} \cdot g(\sigma) \leqslant \left(\frac{e \cdot \log \Delta}{2(n-1)}\right)^{n-1} \cdot \Delta^{1/2} \cdot 2^{-r_1 - r_2} \cdot \pi^{-r_2},$$

which proves (e) for $s = \sigma$. To prove (e) for $1 \leqslant s \leqslant \sigma$ it now suffices to observe that ξ_K' is positive on $[1, \infty)$, by (c). This completes the proof of Lemma 4.1.

Combining (e) and (f) we find an upper bound for $h \cdot \mathrm{reg}/w$ that is due to Louboutin [**10**, equation (2)]. It improves an upper bound obtained by Siegel [**18**, Satz 1].

We now come to the main result of this section, which in substance is due to Stark [**19**]. We let h, reg, w be as in Lemma 4.1(f), and by h_+, reg_+ and w_+ we denote the corresponding quantities for the field K_+ appearing in Proposition 4.2.

Likewise, we denote by Δ_+ the absolute value of the discriminant of K_+ over $\mathbb{Q}$.

PROPOSITION 4.2. *Let K be a totally imaginary quadratic extension of a totally real algebraic number field K_+, and suppose that K does not contain a subfield that is imaginary quadratic over $\mathbb{Q}$. Let M be a Galois closure of K_+ over $\mathbb{Q}$. Write $d = [K_+ : \mathbb{Q}]$ and $m = [M : \mathbb{Q}] \cdot \max(1, 4/d)$. Then we have*

$$\frac{h \cdot \mathrm{reg}/w}{h_+ \cdot \mathrm{reg}_+/w_+} > \frac{1}{4\pi \cdot e^{21/40} \cdot (m+1)} \cdot \left(\frac{2(d-1)}{\pi e \cdot \log \Delta_+}\right)^{d-1} \cdot \frac{1}{\log \Delta} \cdot \frac{\sqrt{\Delta}}{\sqrt{\Delta_+}}.$$

The proposition implies that

$$\frac{h \cdot \mathrm{reg}/w}{h_+ \cdot \mathrm{reg}_+/w_+} > \frac{(d-1)^{d-1}}{21.243 \cdot (4.270)^{d-1} \cdot (m+1)} \cdot \frac{\sqrt{\Delta}/\sqrt{\Delta_+}}{(\log \Delta_+)^{d-1} \cdot \log \Delta},$$

where $m+1$ may be replaced by 5, 9 or $d!+1$, according as $d = 2$, $d = 3$ or $d \geqslant 4$, respectively.

Proof. For $s \in \mathbb{C}$ with $\mathrm{Re}\, s > 1$, we define

$$L(s) = \zeta_K(s)/\zeta_{K_+}(s),$$

$$\Lambda(s) = (\Delta/\Delta_+)^{s/2} \cdot \left(\frac{\Gamma((s+1)/2)}{\pi^{(s+1)/2}}\right)^d \cdot L(s).$$

The function Λ may be analytically extended to an entire function (see [**7**, Chapter VIII and Chapter XIV]). The duplication formula quoted in the proof of Lemma 4.1(e) implies that

$$\xi_K(s) = \xi_{K_+}(s) \cdot \Lambda(s).$$

It follows that Λ satisfies the functional equation $\Lambda(s) = \Lambda(1-s)$.

By Lemma 4.1(f) one has

$$\Lambda(1) = \frac{h \cdot \mathrm{reg}/w}{h_+ \cdot \mathrm{reg}_+/w_+}.$$

We shall estimate this quantity from below.

From Lemma 4.1(b) one obtains

$$\frac{\Lambda'(s)}{\Lambda(s)} = \frac{1}{2} \sum_\rho \left(\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}}\right)$$

for each $s \in \mathbb{C}$ with $\Lambda(s) \neq 0$, the sum ranging over all zeros ρ of Λ, counted with multiplicities; all these zeros are also zeros of ξ_K. Let B be the set of zeros β of Λ that satisfy $\mathrm{Re}\,\beta \geqslant 1 - (4 \log \Delta)^{-1}$ and $|\mathrm{Im}\,\beta| \leqslant (4 \log \Delta)^{-1}$. By Lemma 4.1(d), the set B is either empty or consists of a single simple real zero. We shall need:

$$\beta < 1 - \frac{1}{4m \cdot \log \Delta} \quad \text{for every } \beta \in B, \tag{4.3}$$

with m as defined in Proposition 4.2. We postpone the proof of this assertion until the end of this section. It depends crucially on the assumption that K does not contain an imaginary quadratic subfield.

Let $\sigma_0 = 1 + (4\log\Delta)^{-1}$. If ρ is a zero of Λ that does not belong to B, then as in the proof of [**19**, Lemma 2] one has

$$\frac{1}{s-\rho} + \frac{1}{s-\overline{\rho}} \leqslant 2\left(\frac{1}{\sigma_0-\rho} + \frac{1}{\sigma_0-\overline{\rho}}\right)$$

for every real number s with $1 \leqslant s \leqslant \sigma_0$. Therefore we have

$$\frac{\Lambda'(s)}{\Lambda(s)} \leqslant \sum_{\rho}\left(\frac{1}{\sigma_0-\rho} + \frac{1}{\sigma_0-\overline{\rho}}\right) + \sum_{\beta\in B}\left(\frac{1}{s-\beta} - \frac{2}{\sigma_0-\beta}\right)$$

for the same values of s, where the first sum ranges over the zeros ρ of Λ. We may include the zeros of ξ_{K_+} in that sum, since they give positive contributions. Then the first sum changes to $2\xi_K'(\sigma_0)/\xi_K(\sigma_0)$. Integrating from 1 to σ_0 and exponentiating one finds that

$$\frac{\Lambda(\sigma_0)}{\Lambda(1)} \leqslant \exp\left(2(\sigma_0-1)\,\frac{\xi_K'(\sigma_0)}{\xi_K(\sigma_0)}\right)\cdot E^{-1},$$

where we put

$$E = \prod_{\beta\in B}\left(\frac{1-\beta}{\sigma_0-\beta}\cdot\exp\left(2\,\frac{\sigma_0-1}{\sigma_0-\beta}\right)\right).$$

Using the fact that $\Lambda(\sigma_0) = \xi_K(\sigma_0)/\xi_{K_+}(\sigma_0)$ we now obtain

$$\Lambda(1) \geqslant \exp\left(2(1-\sigma_0)\,\frac{\xi_K'(\sigma_0)}{\xi_K(\sigma_0)}\right)\cdot\xi_K(\sigma_0)\cdot\xi_{K_+}(\sigma_0)^{-1}\cdot E.$$

We estimate the four factors separately.

For the first factor we apply Lemma 4.1(c) to $s = \sigma_0$. Since $\sigma_0 = 1 + (4\log\Delta)^{-1}$ is smaller than the unique positive zero $1.46163\ldots$ of Γ'/Γ (see [**24**, 12.33]), we have $\Gamma'(\sigma_0)/\Gamma(\sigma_0) < 0$, and we find that

$$\frac{\xi_K'(\sigma_0)}{\xi_K(\sigma_0)} < 1 + \frac{1}{\sigma_0-1} + \tfrac{1}{2}\log\Delta - d\log(2\pi).$$

This leads to

$$\begin{aligned}\exp\left(2(1-\sigma_0)\,\frac{\xi_K'(\sigma_0)}{\xi_K(\sigma_0)}\right) &> \exp(-2\sigma_0)\cdot\Delta^{1-\sigma_0}\cdot(2\pi)^{2d(\sigma_0-1)}\\ &= e^{-1/4}\cdot\frac{(2\pi)^{2d(\sigma_0-1)}}{\exp(2\sigma_0)},\end{aligned}$$

which is our estimate for the first factor.

For the second factor, the definition of ξ_K and the obvious inequalities $\zeta_K(\sigma_0) > 1$ and $\sigma_0 > 1$ imply that

$$\xi_K(\sigma_0) > (\sigma_0-1)\cdot\Delta^{\sigma_0/2}\cdot\left(\frac{\Gamma(\sigma_0)}{(2\pi)^{\sigma_0}}\right)^d = \frac{\sqrt{\Delta}}{(2\pi)^d}\cdot\frac{e^{1/8}}{4\log\Delta}\cdot\left(\frac{\Gamma(\sigma_0)}{(2\pi)^{\sigma_0-1}}\right)^d.$$

Let $\gamma \doteq 0.5772157$ denote Euler's constant (see [**24**, 12.1]). From the inequality

$$\frac{\Gamma'(s)}{\Gamma(s)} \geqslant \frac{\Gamma'(1)}{\Gamma(1)} = -\gamma > -\log 2,$$

valid for $s \geqslant 1$ (see [**24**, 12.16]), one deduces that

$$\Gamma(\sigma_0) = \Gamma(\sigma_0)/\Gamma(1) \geqslant \exp(-\gamma(\sigma_0 - 1)) > 2^{1-\sigma_0},$$

which, since $\pi > e$, gives

$$\left(\frac{\Gamma(\sigma_0)}{(2\pi)^{\sigma_0 - 1}}\right)^d > \frac{1}{(4\pi)^{d(\sigma_0-1)}} > \left(\frac{e}{4\pi^2}\right)^{d(\sigma_0-1)} \geqslant \frac{\exp(2\sigma_0 - 2)}{(2\pi)^{2d(\sigma_0-1)}}.$$

In the last inequality we use the fact that $d \geqslant 2$, which follows from the assumption that K does not contain an imaginary quadratic subfield. We obtain

$$\xi_K(\sigma_0) > \frac{\sqrt{\Delta}}{(2\pi)^d \cdot 4e^{15/8} \cdot \log \Delta} \cdot \frac{\exp(2\sigma_0)}{(2\pi)^{2d(\sigma_0-1)}}.$$

This is our estimate for the second factor.

For the third factor we apply Lemma 4.1(e) to the field K_+ and $s = \sigma_0 = 1 + (4 \log \Delta)^{-1}$. The condition $K_+ \neq \mathbb{Q}$ is satisfied, and from $d \geqslant 2$ and $\Delta_+ \leqslant \Delta$ one sees that the condition $\sigma_0 \leqslant 1 + 2(d-1)/\log \Delta_+$ is satisfied as well. We find that

$$\xi_{K_+}(\sigma_0)^{-1} \geqslant 2^d \cdot \left(\frac{2(d-1)}{e \cdot \log \Delta_+}\right)^{d-1} \cdot \frac{1}{\sqrt{\Delta_+}}.$$

The fourth factor, E, is equal to 1 if B is empty. Suppose next that $B = \{\beta\}$. Applying (4.3) we see that E is at least the minimum of

$$(1-x)\exp(2(\sigma_0 - 1)/(\sigma_0 - x))/(\sigma_0 - x)$$

for $1 - (4 \log \Delta)^{-1} \leqslant x \leqslant 1 - (4m \log \Delta)^{-1}$ or, equivalently, the minimum of

$$f(y) = y \exp(2/(1+y))/(1+y)$$

for $1/m \leqslant y \leqslant 1$ (with $y = (4 \log \Delta)(1-x)$). One readily verifies that f is increasing on $[0, 1]$, so the required minimum is $f(1/m)$, which by $m \geqslant 4$ is at least $e^{8/5}/(m+1)$. This is less than 1, so it is in both cases a lower bound for E.

Assembling the four estimates we find that

$$\Lambda(1) > \frac{\sqrt{\Delta}}{(2\pi)^d \cdot 4e^{17/8} \cdot \log \Delta} \cdot 2^d \cdot \left(\frac{2(d-1)}{e \cdot \log \Delta_+}\right)^{d-1} \cdot \frac{1}{\sqrt{\Delta_+}} \cdot \frac{e^{8/5}}{m+1}.$$

Rearranging the right-hand side, and applying Lemma 4.1(f), we obtain the inequality stated in Proposition 4.2. It remains to prove (4.3).

A discriminant formula. The proof of (4.3) makes use of a formula for discriminants that is difficult to locate in the literature. Since it is also useful in other contexts, we state and prove it in the general case of Dedekind domains.

Let A be a Dedekind domain, E its field of fractions, F a finite separable field extension of E, and B the integral closure of A in F. We denote by $\Delta_{B/A}$ the discriminant of B over A, which is a non-zero ideal of A.

Let M be a finite Galois extension of E, with group G, and suppose that M is large enough to contain an E-isomorphic copy of F. We write S for the set of E-embeddings $F \to M$. This is a set of cardinality $[F : E]$, and it is naturally acted upon by G. Denote by C the integral closure of A in M. We assume that for each

maximal ideal P of C the field C/P is separable over $A/(P \cap A)$. This assumption is satisfied in the case of rings of integers in number fields, since in that case all residue class fields are finite.

THEOREM 4.4. *Let the notation and hypotheses be as above, and let I_σ denote the C-ideal generated by $\{\sigma c - c\colon c \in C\}$, for $\sigma \in G$. Then we have*

$$\Delta_{B/A}^{[M:E]} = \prod_{\sigma \in G, \sigma \neq 1} N_{C/A}(I_\sigma)^{\#\{s \in S\colon \sigma s \neq s\}},$$

where $N_{C/A}$ denotes the ideal norm from C to A.

It is only through the exponents $\#\{s \in S\colon \sigma s \neq s\}$ that the formula given in Theorem 4.4 depends on F. This is what accounts for its usefulness. The fact that the formula for $\Delta_{B/A}$ is independent of the choice of M can be proved directly by means of a theorem of Herbrand (see [**16**, Chapter IV, Proposition 3]). One can give a similar formula that is valid when M is an infinite Galois extension of E; it involves a distribution on the Galois group.

Proof. The different $\mathscr{D}_{C/A}$ of C over A is given by

$$\mathscr{D}_{C/A} = \prod_{\sigma \in G,\, \sigma \neq 1} I_\sigma;$$

if C is a complete discrete valuation ring, this is a reformulation of [**16**, Chapter IV, Proposition 4], and the general case then follows from [**16**, Chapter III, Proposition 10].

Let $s \in S$, and let $G_s = \{\sigma \in G\colon \sigma s = s\}$. Then G_s is the Galois group of M over sF, and applying the formula above to the extension $sF \subset M$ we find that

$$\mathscr{D}_{C/sB} = \prod_{\sigma \in G_s, \sigma \neq 1} I_\sigma.$$

The formula $\mathscr{D}_{C/A} = \mathscr{D}_{C/sB} \cdot \mathscr{D}_{sB/A}$ (see [**16**, Chapter III, Proposition 8]) now yields

$$C \cdot \mathscr{D}_{sB/A} = \prod_{\sigma \in G, \sigma s \neq s} I_\sigma.$$

Applying $N_{C/A} = N_{sB/A} \circ N_{C/sB}$ and noticing that

$$N_{sB/A}(N_{C/sB}(C \cdot \mathscr{D}_{sB/A})) = N_{sB/A}(\mathscr{D}_{sB/A})^{[M:sF]} = \Delta_{sB/A}^{[M:sF]} = \Delta_{B/A}^{[M:E]/\#S}$$

one obtains

$$\Delta_{B/A}^{[M:E]/\#S} = \prod_{\sigma \in G, \sigma s \neq s} N_{C/A}(I_\sigma).$$

Taking the product over $s \in S$ we find the formula stated in the theorem. This proves Theorem 4.4.

An alternative proof of Theorem 4.4 can be derived from the theory of conductors (see [**16**, Chapter VI, § 3]).

COROLLARY 4.5. *With the same notation and hypotheses as in Theorem* 4.4, *assume in addition that M is a Galois closure of F over E. Then $\Delta_{C/A}^2$ divides $\Delta_{B/A}^{[M:E]}$.*

Proof. Since M is a Galois closure of F over E, the only element of G that acts as the identity on S is the identity element of G. Hence every $\sigma \in G$ with $\sigma \neq 1$ moves at least two elements of S:

$$\#\{s \in S\colon \sigma s \neq s\} \geqslant 2;$$

or, equivalently,

$$[M : E] \cdot \#\{s \in S\colon \sigma s \neq s\} \geqslant 2 \cdot \#G.$$

We now express each of $\Delta_{B/A}$ and $\Delta_{C/A}$ by means of the formula given in Theorem 4.4. The set that plays the role of S in the formula for $\Delta_{C/A}$ is G itself, on which G acts by left multiplication. For each $\sigma \in G$ with $\sigma \neq 1$, one has $\#\{s \in G\colon \sigma s \neq s\} = \#G$; so the inequality just proved implies that $\Delta_{B/A}^{[M:E]}$ is divisible by $\Delta_{C/A}^2$. This proves Corollary 4.5.

One can deduce from the proof of Corollary 4.5 that equality holds if and only if the inertia group of any maximal ideal of C that is ramified over A is generated by an element of G that acts as a transposition on S.

We now prove (4.3). With a coefficient $16d!$ instead of $4m$, this result is due to Stark [**19**, Lemma 9]. We indicate which change to make in his argument. By Corollary 4.5, the discriminant of the Galois closure M of K_+ over $\mathbb{Q}$ divides $\Delta_+^{[M:\mathbb{Q}]/2}$. The different of $N = M \cdot K$ over M divides the different of K over K_+ (see [**19**, Lemma 6]), so writing Δ_- for the norm from K to $\mathbb{Q}$ of the latter different, we find that the discriminant of N over $\mathbb{Q}$ divides $\Delta_+^{[M:\mathbb{Q}]} \cdot \Delta_-^{[M:K_+]}$. (This replaces Stark's bound $\Delta^{d!}$.) If the field N has a conjugate $N' \neq N$, then the field $L = N \cdot N'$ equals $K \cdot N'$, so the different of L over N' divides the different of K over K_+, and one finds that the discriminant of L over $\mathbb{Q}$ divides $\Delta_+^{2[M:\mathbb{Q}]} \cdot \Delta_-^{4[M:K_+]}$. (This replaces Stark's bound $\Delta^{4d!}$.) From $\Delta = \Delta_+^2 \Delta_-$ and the definition of m (given in Proposition 4.2) one finds that the discriminant of N and the discriminant of L (if it exists) both divide Δ^m. With this bound, Stark's argument leads to (4.3). This completes the proof of Proposition 4.2.

5. *Zeta functions for finite rings*

For a positive integer n, the size of the unit group $(\mathbb{Z}/n\mathbb{Z})^*$ is not much smaller than the size of the full ring $\mathbb{Z}/n\mathbb{Z}$. More precisely, we have $\#(\mathbb{Z}/n\mathbb{Z})^* \geqslant n \cdot e^{-\gamma + o(1)}/\log\log n$ for $n \to \infty$ (see [**5**, Theorem 328] and Remark 5.10 below). In the proof of Proposition 2.3 we shall need similar information for other finite rings. The natural tool for obtaining sharp results is the theory of zeta functions for finite rings, to which the present section is devoted. Ultimately, these results are responsible for the factor $(\log\log q)^2$ appearing in the estimate of Proposition 2.3. The reader who is satisfied with the higher power $(\log\log q)^6$ can skip most of this section (cf. Remark 6.5).

We recall that rings in this paper are assumed to be commutative with unit element, and that the latter is supposed to be respected by ring homomorphisms and to belong to subrings.

Let A be a finite ring. Following [**17**], we define the zeta function ζ_A of A by

$$\zeta_A(s) = \prod_M \frac{1}{1 - \#(A/M)^{-s}},$$

where M ranges over the set of maximal ideals of A and s is a complex variable. Using the fact that A is isomorphic to the product of its localizations A_M (see [**2**, Theorem 8.7]), we find the *special value*

$$\zeta_A(1) = \frac{\#A}{\#A^*}, \tag{5.1}$$

which explains the relevance of zeta functions for our purpose. The nilradical $\mathrm{nil}\,A$ of A is equal to the intersection of all maximal ideals (see [**2**, Corollary 8.2]); so the reduced ring $A_{\mathrm{red}} = A/\mathrm{nil}\,A$ is given by $A_{\mathrm{red}} = \prod_M A/M$. Clearly, we have

$$\zeta_A = \zeta_{A_{\mathrm{red}}}. \tag{5.2}$$

One easily proves the *functional equation*

$$\zeta_A(-s) = (-1)^t \cdot (\#A_{\mathrm{red}})^{-s} \cdot \zeta_A(s),$$

where t denotes the number of maximal ideals of A, which leads to another special value:

$$\zeta_A(-1) = (-1)^t \cdot (\#A^*_{\mathrm{red}})^{-1}. \tag{5.3}$$

For a prime number l, let A_l be the localization of A at l. Writing A as the product of the rings A_l, with l ranging over the set of all prime numbers, one readily finds the *Euler product*

$$\zeta_A(s) = \prod_l \frac{1}{P_l(l^{-s})}, \tag{5.4}$$

where P_l is a polynomial with integer coefficients and constant term 1. One also finds that all zeros of P_l are roots of unity (the *Riemann hypothesis*), and that the degree d_l of P_l is determined by

$$\#A_{\mathrm{red}} = \prod_l l^{d_l}.$$

For all but finitely many l one has $d_l = 0$ and $P_l = 1$. Substituting $s = 1$ we find that

$$\frac{\#A^*}{\#A} = \prod_l P_l(l^{-1}) \geqslant \prod_l \left(1 - \frac{1}{l}\right)^{d_l}, \tag{5.5}$$

which one can also easily prove without using zeta functions.

As we just saw, $1/\zeta_A(s)$ has an Euler product in which the lth factor is a polynomial in l^{-s}. It is not hard to show that the same is true for $\zeta_B(s)/\zeta_A(s)$, where B is any subring of A. We shall prove the following more general result.

THEOREM 5.6. *Let A be a finite ring, let B and C be subrings of A, and put $D = B \cap C$. Then we can write*

$$\frac{\zeta_B(s)\zeta_C(s)}{\zeta_A(s)\zeta_D(s)} = \prod_{l \text{ prime}} Q_l(l^{-s}),$$

where Q_l is a polynomial with integer coefficients, all of whose zeros are roots of unity, with constant term 1, *and with degree* $\deg Q_l$ *determined by*

$$\#(A_{\mathrm{red}}/(B_{\mathrm{red}} + C_{\mathrm{red}})) = \prod_l l^{\deg Q_l}.$$

Note that B_{red} and C_{red} may be viewed as subrings of A_{red}; by $B_{\mathrm{red}} + C_{\mathrm{red}}$ we mean the additive subgroup they generate.

Taking $C = B$ one recovers the earlier statement about $\zeta_B(s)/\zeta_A(s)$. It is not generally true that, for subrings B, C, E of A, the alternating product

$$\frac{\zeta_B(s)\zeta_C(s)\zeta_E(s)\zeta_{B\cap C\cap E}(s)}{\zeta_A(s)\zeta_{B\cap C}(s)\zeta_{B\cap E}(s)\zeta_{C\cap E}(s)}$$

has the same general shape; a counterexample is provided by $A = \mathbb{F}_l \times \mathbb{F}_l \times \mathbb{F}_l$, where l is any prime number, with B, C and E equal to the three subrings of A of order l^2.

Proof of Theorem 5.6. Writing A as the product of the rings A_l we immediately reduce to the case in which $A = A_l$ for a single prime number l. Let this now be assumed. Next we shall replace A by A_{red}, and B and C by their images B_{red} and C_{red} in A_{red}. This replacement is justified by (5.2) and the equality

$$D_{\mathrm{red}} = B_{\mathrm{red}} \cap C_{\mathrm{red}} \tag{5.7}$$

(inside A_{red}), which we proceed to prove. The inclusion $\subset$ is obvious. To prove $\supset$, suppose that $b \in B$ and $c \in C$ have the same image x in A_{red}. One readily shows that $b^l \equiv c^l \bmod (b-c)\mathrm{nil}A$, and, inductively, that $b^{l^n} \equiv c^{l^n} \bmod (b-c)(\mathrm{nil}A)^{n-1}$ for all positive integers n. Now choose n so large that $(\mathrm{nil}A)^n = 0$. Then it follows that $b^{l^n} = c^{l^n}$, which is an element of $B \cap C = D$. Choosing, in addition, n to be divisible by the degree of each field A/M over $\mathbb{F}_l$, one sees that this element of D maps to x in A_{red}. Hence we have $x \in D_{\mathrm{red}}$. This proves (5.7).

We may, and do, now assume that $A = A_l = A_{\mathrm{red}}$, so that A is a product of finite fields of the same characteristic l, and likewise for the three subrings. From (5.4) it is clear that $\zeta_B(s)\zeta_C(s)/(\zeta_A(s)\zeta_D(s))$ is of the form $Q_l(l^{-s})$ for some rational function Q_l. We shall prove that Q_l is actually a polynomial. Evidently, we can write $Q_l = f/g$, where f and g are polynomials with integer coefficients without common factor and with constant coefficients equal to 1. Since f and g are coprime over the field of rational numbers, we can find polynomials u and v with integer coefficients such that $uf + vg = N$ for some positive integer N.

Applying (5.3) to A, B, C and D, and using the fact that $D^* = B^* \cap C^*$, we obtain

$$Q_l(l) = \frac{\zeta_B(-1)\zeta_C(-1)}{\zeta_A(-1)\zeta_D(-1)} = \pm\frac{\#A^* \cdot \#D^*}{\#B^* \cdot \#C^*} = \pm\#(A^*/(B^* \cdot C^*)).$$

This shows that the rational function Q_l assumes an integer value at l.

Let r be any prime number for which $l^r > \#A$, and let $h \in \mathbb{F}_l[X]$ be an irreducible polynomial of degree r. For any $\mathbb{F}_l$-algebra R, write temporarily $R' = R[X]/hR[X]$. The choice of r implies that h is still irreducible over any residue class field A/M of A, so each of the rings $(A/M)'$ is again a field, and A' is the product of these fields. A straightforward computation now shows that $\zeta_{A'}(s) = \zeta_A(rs)$. Since we also have $l^r > \#B$, the corresponding statement for B is true as well, and likewise for C and D. Also, we may view B' and C' as subrings of A', with intersection D'. Hence, applying what we proved above, we find that $Q_l(l^r)$ is an integer.

We have shown that the rational function $Q_l = f/g$ assumes integer values at

infinitely many points l^r. For each of them, $g(l^r)$ divides $f(l^r)$, and therefore it divides $u(l^r)f(l^r) + v(l^r)g(l^r) = N$ as well. Thus, the polynomial g is bounded on an infinite set of integers. This implies that g is constant, and in fact we have $g = 1$ since its constant term is 1. It follows that $Q_l = f$ is a polynomial.

The remaining assertions of the theorem are now immediate. In particular, the statement about $\deg Q_l$ is obtained from the equality

$$\#(A_{\mathrm{red}}/(B_{\mathrm{red}} + C_{\mathrm{red}})) = \frac{\#A_{\mathrm{red}} \cdot \#D_{\mathrm{red}}}{\#B_{\mathrm{red}} \cdot \#C_{\mathrm{red}}},$$

which follows from (5.7). This completes the proof of Theorem 5.6.

REMARK. A more conceptual proof of the fact that Q_l is a polynomial may be sketched as follows. Let l be fixed, and let K be an algebraic closure of $\mathbb{F}_l$. Write S_A for the finite set of ring homomorphisms $A \to K$. The Frobenius automorphism of K induces a permutation of S_A and therefore an automorphism ϕ of the complex vector space $\mathbb{C}^{S_A}$. One shows that the characteristic polynomial of ϕ is equal to P_l. Next, using the fact proven above that $D_{\mathrm{red}} = B_{\mathrm{red}} \cap C_{\mathrm{red}}$, one shows that there is an exact sequence

$$0 \to \mathbb{C}^{S_D} \to \mathbb{C}^{S_B} \oplus \mathbb{C}^{S_C} \to \mathbb{C}^{S_A}$$

of complex vector spaces, the maps respecting the action of ϕ. Now, to prove that Q_l is a polynomial, one observes that it is in fact the characteristic polynomial of the induced action of ϕ on the cokernel of the rightmost map.

COROLLARY 5.8. *Let A, B, C and D be as in Theorem* 5.6*, and let d be a non-negative integer such that the finite abelian group A/B can be generated by d elements. Then we have*

$$\frac{\#A^*/\#C^*}{\#B^*/\#D^*} \geqslant \frac{\#A/\#C}{\#B/\#D} \cdot \prod_{l \mid \#(A/C)} \left(1 - \frac{1}{l}\right)^d,$$

where l ranges over primes.

Proof. Let Q_l be as in Theorem 5.6. For any complex root of unity η and any prime number l we have $|1 - \eta/l| \geqslant 1 - 1/l$. Therefore we have

$$\prod_l Q_l(l^{-1}) \geqslant \prod_l \left(1 - \frac{1}{l}\right)^{\deg Q_l}.$$

If l does not divide the order of A/C, then it does not divide the order of its homomorphic image $A_{\mathrm{red}}/(B_{\mathrm{red}} + C_{\mathrm{red}})$ either; so then we have $\deg Q_l = 0$. The group $A_{\mathrm{red}}/(B_{\mathrm{red}} + C_{\mathrm{red}})$ is a homomorphic image of A/B, so it can be generated by d elements. It is also of square-free exponent, because A_{red} is a product of fields. Therefore $\#(A_{\mathrm{red}}/(B_{\mathrm{red}} + C_{\mathrm{red}}))$ divides $\prod l^d$, the product ranging over the primes dividing its order. This implies that $\deg Q_l \leqslant d$ for all l, and one obtains Corollary 5.8 from the inequality above and (5.1).

By means of the same argument one proves the upper bound

$$\frac{\#A^*/\#C^*}{\#B^*/\#D^*} \leqslant \frac{\#A/\#C}{\#B/\#D} \cdot \prod_{l \mid \#(A/C)} \left(1 + \frac{1}{l}\right)^d.$$

The following lemma provides an explicit bound for the product appearing in Corollary 5.8.

LEMMA 5.9. *Let P be a finite set of prime numbers. Then we have*

$$\prod_{l\in P}\left(1-\frac{1}{l}\right)\geqslant\left(\sqrt{5}\cdot\log\log\max\left\{\prod_{l\in P}l,\,6000\right\}\right)^{-1}.$$

Proof. If the cardinality of P is a given number k, then the product

$$\left(\log\log\max\left\{\prod_{l\in P}l,\,6000\right\}\right)\cdot\prod_{l\in P}\left(1-\frac{1}{l}\right)$$

is minimal when P consists of the first k primes. Hence, for the proof of Lemma 5.9 we may assume that P is the set of prime numbers less than or equal to x for some $x>1$. According to [**13**, 3.16 and 3.30] we have

$$\log\prod_{l\leqslant x}l>x\cdot\left(1-\frac{1}{\log x}\right)\quad\text{for } x\geqslant 41,$$

$$\prod_{l\leqslant x}\left(1-\frac{1}{l}\right)^{-1}<e^{\gamma}\cdot\left((\log x)+\frac{1}{\log x}\right)\quad\text{for } x>1,$$

where l ranges over primes and $\gamma\doteq 0.5772157$ denotes Euler's constant. These inequalities and a small computation imply that for $x\geqslant 79$ we have

$$\left(\log\log\prod_{l\leqslant x}l\right)\cdot\prod_{l\leqslant x}\left(1-\frac{1}{l}\right)\geqslant\tfrac{1}{2}.$$

Explicit computation for small x shows that this inequality holds in fact for $x\geqslant 37$, and that the conclusion of the lemma is valid for all x. This completes the proof of Lemma 5.9.

REMARK 5.10. It is clear from the proof that the conclusion of the lemma holds with $e^{\gamma}+o(1)$ as $\#P\to\infty$ in place of $\sqrt{5}$. We have $e^{\gamma}\doteq 1.7810724$.

6. *The order of a Picard group*

Let K be an algebraic number field, and let $\mathcal{O}$ be its ring of algebraic integers. Let R be an *order* in K, that is, a subring R of $\mathcal{O}$ for which the index $(\mathcal{O}:R)$ of additive groups is finite. By $\Delta(R)$ we denote the discriminant of R over $\mathbb{Z}$, by $\operatorname{Pic}R$ the group of classes of invertible ideals of R, and by $h(R)$ the order of $\operatorname{Pic}R$. The regulator of R is denoted by $\operatorname{reg}R$, the torsion subgroup of R^* by $\mu(R)$, and the order of $\mu(R)$ by $w(R)$. We write $\widehat{\mathbb{Z}}$ for the profinite completion of $\mathbb{Z}$, and $\widehat{A}$ for $A\otimes_{\mathbb{Z}}\widehat{\mathbb{Z}}$ when A is a ring. One readily proves that the index $(\widehat{\mathcal{O}}^*:\widehat{R}^*)$ of multiplicative groups is finite; in fact, it is equal to $((\mathcal{O}/\mathcal{F})^*:(R/\mathcal{F})^*)$ for any non-zero $\mathcal{O}$-ideal $\mathcal{F}$ that is contained in R (for example, $\mathcal{F}=(\mathcal{O}:R)\mathcal{O}$). By a formula of Dedekind, the number $h(R)\cdot\operatorname{reg}R/(w(R)\cdot(\widehat{\mathcal{O}}^*:\widehat{R}^*))$ is the same for all orders R in K, so in fact

$$\frac{h(R)\cdot\operatorname{reg}R}{w(R)\cdot(\widehat{\mathcal{O}}^*:\widehat{R}^*)}=\frac{h(\mathcal{O})\cdot\operatorname{reg}\mathcal{O}}{w(\mathcal{O})};\tag{6.1}$$

see [**15**, Theorem 3.7 and Corollary 4.6].

Next assume that K is a totally imaginary quadratic extension of a totally real field K_+. We denote the non-trivial K_+-automorphism of K by an overhead bar. The degree of K_+ over $\mathbb{Q}$ is denoted by d, and the ring of integers of K_+ by $\mathcal{O}_+$. We assume that $\overline{R} = R$, and we put $R_+ = R \cap \mathcal{O}_+$. Let $K_{+\gg 0}$ be the multiplicative group of totally positive elements of K_+. We define the group $\mathrm{Pic}_* R$ to consist of equivalence classes of pairs (I, β), where $I \subset K$ is an invertible R-ideal and $\beta \in K_{+\gg 0}$ is such that $I\overline{I} = \beta R$; here we define two such pairs (I, β) and (J, γ) to be equivalent if there exists $\alpha \in K^*$ with $\alpha I = J$ and $\alpha\overline{\alpha}\beta = \gamma$. The group multiplication in $\mathrm{Pic}_* R$ is defined by $(I, \beta) \cdot (I', \beta') = (II', \beta\beta')$.

THEOREM 6.2. *With the notation and hypotheses as above, assume moreover that K does not contain an imaginary quadratic subfield. Let δ be the product of the prime numbers dividing $(\mathcal{O} : R)$. Then $\mathrm{Pic}_* R$ is a finite group of order at least*

$$\frac{(d-1)^{d-1} \cdot w(R) \cdot \sqrt{|\Delta(R)|}/\sqrt{\Delta(R_+)}}{m' \cdot (\log \Delta(\mathcal{O}_+))^{d-1} \cdot \log|\Delta(\mathcal{O})| \cdot (20 \log\log \max\{\delta, 6000\})^d}$$

where m' equals 25, 45 or $5d! + 5$, according as $d = 2$, $d = 3$, or $d \geqslant 4$.

The proof of Theorem 6.2 is preceded by two auxiliary results. We keep the notation and hypotheses as above; the special condition on K in Theorem 6.2 is not needed in Lemmas 6.3 and 6.4.

We denote by $\mathrm{Pic}_+ R_+$ the group of *strict* equivalence classes of invertible R_+-ideals, where I and J are called strictly equivalent if there exists $\alpha \in K_{+\gg 0}$ such that $I = \alpha J$. We write N for the norm map $K \to K_+$ defined by $N(x) = x\overline{x}$, and for several maps that it induces. One of these maps is the map $\mathrm{Pic}\, R \to \mathrm{Pic}_+ R_+$; to see that it is defined it suffices to observe that the groups $\mathrm{Pic}\, R$ and $\mathrm{Pic}_+ R_+$ may be identified with $\widehat{K}^*/(\widehat{R}^* K^*)$ and $\widehat{K}_+^*/(\widehat{R}_+^* K_{+\gg 0})$ respectively, the notation $\widehat{\ }$ being as above.

LEMMA 6.3. *The group $\mathrm{Pic}_* R$ is finite of order*

$$\#C \cdot \frac{w(R)}{2^d} \cdot \frac{h(\mathcal{O}) \cdot \mathrm{reg}\mathcal{O} \cdot w(\mathcal{O}_+)}{h(\mathcal{O}_+) \cdot \mathrm{reg}\,\mathcal{O}_+ \cdot w(\mathcal{O})} \cdot \frac{(\widehat{\mathcal{O}}^* : \widehat{R}^*)}{(\widehat{\mathcal{O}}_+^* : \widehat{R}_+^*)},$$

where C denotes the cokernel of the map N: $\mathrm{Pic}\, R \to \mathrm{Pic}_+ R_+$.

Proof. Write $R_{+\gg 0}^* = R^* \cap K_{+\gg 0}$. The map $\mathrm{Pic}_* R \to \mathrm{Pic}\, R$ sending the class of (I, β) to the class of I gives rise to an exact sequence

$$1 \to R_{+\gg 0}^*/NR^* \to \mathrm{Pic}_* R \to \mathrm{Pic}\, R \xrightarrow{N} \mathrm{Pic}_+ R_+ \to C \to 1.$$

It follows that $\mathrm{Pic}_* R$ is finite of order $\#C \cdot h(R) \cdot \#(R_{+\gg 0}^*/NR^*)/\#\mathrm{Pic}_+ R_+$. The exact sequence

$$1 \to R_{+\gg 0}^* \to R_+^* \to K_+^*/K_{+\gg 0} \to \mathrm{Pic}_+ R_+ \to \mathrm{Pic}\, R_+ \to 1,$$

in which the middle group has order 2^d, implies that

$$\#\mathrm{Pic}_+ R_+ = 2^d h(R_+)/\#(R_+^*/R_{+\gg 0}^*);$$

so we find that

$$\#\mathrm{Pic}_*\, R = \#C \cdot \frac{h(R)}{h(R_+)} \cdot \frac{\#(R_+^*/NR^*)}{2^d}.$$

From $\#(R_+^*/R_+^{*2}) = 2^d$ it follows that the last factor on the right equals the inverse of the order of the group NR^*/R_+^{*2}. Since $\mu(R)$ is the kernel of $N\colon R^* \to R_+^*$, there is an exact sequence

$$1 \to \mu(R)R_+^* \to R^* \xrightarrow{N} NR^*/R_+^{*2} \to 1.$$

Hence we have $2^d/\#(R_+^*/NR^*) = \#(NR^*/R_+^{*2}) = (R^* : \mu(R)R_+^*)$, and this is equal to the regulator of the subgroup $\mu(R)R_+^*$ of R^* divided by $\mathrm{reg}\, R$. The former regulator equals $2^{d-1}\,\mathrm{reg}\, R_+$, the factor 2^{d-1} coming from K being totally complex and K_+ being totally real. Thus we obtain

$$\#\mathrm{Pic}_*\, R = \#C \cdot \frac{1}{2^{d-1}} \cdot \frac{h(R)\cdot \mathrm{reg}\, R}{h(R_+)\cdot \mathrm{reg}\, R_+}.$$

Now apply Dedekind's formula (6.1), both to R and to R_+, and use the fact that $w(R_+) = 2$, to conclude the proof of Lemma 6.3.

LEMMA 6.4. *Let δ be as in the statement of Theorem* 6.2. *Then we have*

$$\frac{(\widehat{\mathcal{O}}^* : \widehat{R}^*)}{(\widehat{\mathcal{O}}_+^* : \widehat{R}_+^*)} \geqslant \frac{\sqrt{\Delta(R)/\Delta(\mathcal{O})}/\sqrt{\Delta(R_+)/\Delta(\mathcal{O}_+)}}{(\sqrt{5}\cdot \log\log \max\{\delta, 6000\})^d}.$$

Proof. Let $\mathcal{F} = (\mathcal{O} : R)\mathcal{O}$, which is an $\mathcal{O}$-ideal contained in R. Likewise, $\mathcal{F}_+ = \mathcal{F} \cap \mathcal{O}_+$ is an $\mathcal{O}_+$-ideal contained in $R \cap \mathcal{O}_+ = R_+$. Let A be the finite ring $\mathcal{O}/\mathcal{F}$, and denote its subrings $\mathcal{O}_+/\mathcal{F}_+$ and $R/\mathcal{F}$ by B and C, respectively. Then the ring $D = B \cap C$ is given by $D = R_+/\mathcal{F}_+$. The expression on the left in Lemma 6.4 is now equal to $\#A^* \cdot \#D^*/(\#B^* \cdot \#C^*)$, so we can apply Corollary 5.8; note that A/B can be generated by d elements, since it is a homomorphic image of the group $\mathcal{O}/\mathcal{O}_+$. We find that

$$\frac{(\widehat{\mathcal{O}}^* : \widehat{R}^*)}{(\widehat{\mathcal{O}}_+^* : \widehat{R}_+^*)} \geqslant \frac{\#A/\#C}{\#B/\#D} \cdot \prod_{l \mid \#(A/C)} \left(1 - \frac{1}{l}\right)^d,$$

with l ranging over prime numbers. By Lemma 5.9, the product appearing on the right is bounded below by $(\sqrt{5}\cdot \log\log \max\{\delta, 6000\})^{-d}$. We have

$$\#A/\#C = (\mathcal{O} : R) = \sqrt{\Delta(R)/\Delta(\mathcal{O})},$$

and likewise $\#B/\#D = \sqrt{\Delta(R_+)/\Delta(\mathcal{O}_+)}$. This proves Lemma 6.4.

REMARK 6.5. The weaker lower bound with denominator

$$(\sqrt{5}\cdot \log\log \max\{\delta, 6000\})^{3d}$$

is much easier to obtain. It suffices to apply (5.5) to A and D and to use the trivial upper bounds $\#B^* \leqslant \#B$ and $\#C^* \leqslant \#C$.

Proof of Theorem 6.2. We apply the formula of Lemma 6.3. The factor $\#C$ is obviously at least 1. For the last two factors we use the lower bounds provided by

Proposition 4.2 and Lemma 6.4. Noting that

$$\frac{21.243}{4.270} < 5, \quad 5(m+1) \leqslant m', \quad 2 \cdot 4.270 \cdot \sqrt{5} < 20,$$

we obtain Theorem 6.2.

7. *Fourth degree Weil polynomials*

In this section we denote by q a power of a prime number. We shall study the set of Weil q-polynomials of degree 4, as defined in § 2. For $a, b \in \mathbb{Z}$, we define $h_{a,b} \in \mathbb{Z}[X]$ by

$$h_{a,b} = (X^2 + q)^2 - aX(X^2 + q) + bX^2.$$

PROPOSITION 7.1. *The map sending (a, b) to $h_{a,b}$ is a bijection from the set of pairs of integers a, b satisfying*

$$2|a|\sqrt{q} - 4q \leqslant b \leqslant \tfrac{1}{4}a^2 \leqslant 4q$$

to the set of Weil q-polynomials of degree 4. The polynomial $h_{a,b}$ has a real zero if and only if $(b + 4q)^2 - 4qa^2 = 0$. If $h_{a,b}$ is ordinary then it does not have a real zero.

Proof. First we show that $h_{a,b}$ is a Weil polynomial whenever a and b satisfy the stated inequalities. From $a^2 - 4b \geqslant 0$ it follows that there are real numbers σ and τ such that $X^2 - aX + b = (X - \sigma)(X - \tau)$. The inequality $2|a|\sqrt{q} - 4q \leqslant b$ implies that $(\pm 2\sqrt{q})^2 - a(\pm 2\sqrt{q}) + b \geqslant 0$, and so

$$(2\sqrt{q} - \sigma)(2\sqrt{q} - \tau) \geqslant 0, \quad (2\sqrt{q} + \sigma)(2\sqrt{q} + \tau) \geqslant 0.$$

If $\sigma > 2\sqrt{q}$ then the first inequality implies that $\tau \geqslant 2\sqrt{q}$, which contradicts $\sigma\tau = b \leqslant 4q$. Likewise, $\sigma < -2\sqrt{q}$ contradicts the second inequality. Therefore we have $|\sigma| \leqslant 2\sqrt{q}$, and by symmetry $|\tau| \leqslant 2\sqrt{q}$. This implies that there are complex numbers π and ρ of absolute value $\sqrt{q}$ such that $X^2 - \sigma X + q = (X - \pi)(X - \overline{\pi})$ and $X^2 - \tau X + q = (X - \rho)(X - \overline{\rho})$. From $\sigma + \tau = a$ and $\sigma\tau = b$ it follows that

$$(X - \pi)(X - \overline{\pi})(X - \rho)(X - \overline{\rho}) = (X^2 - \sigma X + q)(X^2 - \tau X + q) = h_{a,b},$$

so that $h_{a,b}$ is a Weil polynomial of degree 4.

Conversely, suppose that h is a Weil polynomial of degree 4. From $h(0) = q^2$ it follows that each real zero of h has even multiplicity, so there are complex numbers π and ρ of absolute value $\sqrt{q}$ such that

$$h = (X - \pi)(X - \overline{\pi})(X - \rho)(X - \overline{\rho}).$$

Let $\sigma = \pi + \overline{\pi}$ and $\tau = \rho + \overline{\rho}$. These are real numbers of absolute value at most $2\sqrt{q}$, and putting $a = \sigma + \tau$ and $b = \sigma\tau$ we have

$$h = (X^2 - \tau X + q)(X^2 - \sigma X + q) = (X^2 + q)^2 - aX(X^2 + q) + bX^2.$$

Since the coefficients of h at X^3 and X^2 are equal to $-a$ and $2q + b$, respectively, we have $a, b \in \mathbb{Z}$, and a, b is the unique pair of integers with $h = h_{a,b}$.

Because σ and τ are in the closed interval $[-2\sqrt{q}, 2\sqrt{q}]$, we have

$$4q - 4a\sqrt{q} + b = (2\sqrt{q} - \sigma)(2\sqrt{q} - \tau) \geqslant 0$$

and

$$4q + 4a\sqrt{q} + b = (2\sqrt{q} + \sigma)(2\sqrt{q} + \tau) \geqslant 0,$$

so $b \geqslant 2|a|\sqrt{q} - 4q$. We have also

$$b = \sigma\tau \leqslant \tfrac{1}{4}(\sigma + \tau)^2 = \tfrac{1}{4}a^2$$

and

$$\tfrac{1}{4}a^2 = \tfrac{1}{4}(\sigma + \tau)^2 \leqslant \tfrac{1}{4}(4\sqrt{q})^2 = 4q.$$

The polynomial $h_{a,b}$ has a real zero if and only if σ or τ is in $\{2\sqrt{q}, -2\sqrt{q}\}$. This is equivalent to one of $\pm 2\sqrt{q}$ being a zero of $X^2 - aX + b$, which occurs if and only if $(b + 4q)^2 - 4qa^2 = 0$. This cannot happen if $\gcd(b, q) = 1$, that is, if h is ordinary.

This proves Proposition 7.1.

PROPOSITION 7.2. *Let $h = h_{a,b}$ be a Weil q-polynomial of degree 4. Then h is irreducible over $\mathbb{Q}$ if and only if $a^2 - 4b$ is not an integer square and $(b + 4q)^2 - 4qa^2 \neq 0$.*

Proof. The condition $(b + 4q)^2 - 4qa^2 \neq 0$ is equivalent to h not having a real zero. Since the numbers $\pm\sqrt{q}$ have degree at most 2 over $\mathbb{Q}$, this condition is satisfied if h is irreducible. Hence we may, in the proof of Proposition 7.2, assume that h does not have a real zero.

As in the proof of Proposition 7.1, we denote by π a complex zero of h, and we put $\sigma = \pi + \overline{\pi}$. From $\overline{\pi} = q/\pi$ we see that $\sigma \in \mathbb{Q}(\pi)$. Since π is not real and $\pi^2 - \sigma\pi + q = 0$, we have $[\mathbb{Q}(\pi) : \mathbb{Q}(\sigma)] = 2$. Hence the irreducibility of h over $\mathbb{Q}$, which is equivalent to $[\mathbb{Q}(\pi) : \mathbb{Q}] = 4$, is also equivalent to $[\mathbb{Q}(\sigma) : \mathbb{Q}] = 2$. Since σ is a zero of $X^2 - aX + b$ this is the case if and only if $a^2 - 4b$ is not an integer square. This proves Proposition 7.2.

In the rest of this section we let $h = h_{a,b}$ be a Weil q-polynomial of degree 4 that is irreducible over $\mathbb{Q}$. We denote by π a zero of h in some extension field of $\mathbb{Q}$, and we put $K = \mathbb{Q}(\pi)$. This is an algebraic number field of degree 4 over $\mathbb{Q}$, and it has an automorphism $\bar{}$ of order 2 for which $\overline{\pi} = q/\pi$. The field K is a totally imaginary quadratic extension of the real quadratic number field $K_+ = \mathbb{Q}(\pi + \overline{\pi})$, and $\bar{}$ generates the Galois group of K over K_+. As in the previous section, we write $\mathcal{O}$ for the ring of integers of K and $\mathcal{O}_+$ for the ring of integers of K_+. Moreover, we put $R = \mathbb{Z}[\pi, \overline{\pi}]$, which is an order in K, and $R_+ = \mathbb{Z}[\pi + \overline{\pi}]$, which is an order in K_+. The hypothesis $\overline{R} = R$ of § 6 is clearly satisfied, and from $R = R_+[\pi] = R_+ + R_+\pi$ one sees that R_+ is indeed equal to the ring $R \cap \mathcal{O}_+$ that we called R_+ in § 6.

PROPOSITION 7.3. *With the notation and hypotheses as above, let* Tr *denote the trace function $K \to \mathbb{Q}$, and let ρ and $\overline{\rho}$ denote zeros of h, different from π and $\overline{\pi}$, in some extension field of K. Then the element $\iota = (\pi - \overline{\pi})(\pi + \overline{\pi} - \rho - \overline{\rho})$ belongs to R, and for $r \in R$ one has $\mathrm{Tr}(rR) \subset \mathbb{Z}$ if and only if $r \in R\iota^{-1}$.*

Proof. From $\pi + \overline{\pi} + \rho + \overline{\rho} = a$ it follows that $\rho + \overline{\rho} \in R$, so $\iota \in R$. Next, let $\mathrm{Tr}' : K \to K_+$ and $\mathrm{Tr}_+ : K_+ \to \mathbb{Q}$ denote the relative traces. A quick computation,

which is based on $R = R_+ + R_+\pi$, shows that for r in R one has $\mathrm{Tr}'(rR) \subset R_+$ if and only if $r \in R(\pi - \overline{\pi})^{-1}$. Likewise, from $R_+ = \mathbb{Z} + \mathbb{Z} \cdot (\pi + \overline{\pi})$ one deduces that for $r' \in R_+$ one has $\mathrm{Tr}_+(r'R_+) \subset \mathbb{Z}$ if and only if $r' \in R_+(\pi + \overline{\pi} - \rho - \overline{\rho})^{-1}$. Combining these two facts with the formula $\mathrm{Tr} = \mathrm{Tr}_+ \circ \mathrm{Tr}'$ and with the R_+-linearity of Tr' one finds the last assertion of Proposition 7.3. This proves Proposition 7.3.

PROPOSITION 7.4. *In addition to the notation and hypotheses above, let the function* Δ *be as in* § 6, *let* δ, *as in Theorem* 6.2, *be the product of the prime numbers dividing* $(\mathcal{O} : R)$, *and put*

$$c(h) = (a^2 - 4b)^{1/2} \cdot ((b + 4q)^2 - 4qa^2)^{1/2}$$

as in § 2. *Then we have*

$$0 < \Delta(\mathcal{O}_+) \leqslant \Delta(R_+) = a^2 - 4b < 16q,$$

$$0 < \Delta(\mathcal{O}) \leqslant \Delta(R) = ((b + 4q)^2 - 4qa^2) \cdot \Delta(R_+)^2 \leqslant 256q^4 = (4q)^4,$$

$$\delta \leqslant c(h) = \sqrt{\Delta(R)}/\sqrt{\Delta(R_+)} \leqslant \frac{32}{3\sqrt{3}} \cdot q^{3/2}.$$

Proof. We may assume that K is a subfield of the field of complex numbers. Let ρ, σ and τ be as in the proof of Proposition 7.1. Since the irreducible polynomial of σ over $\mathbb{Q}$ is $X^2 - aX + b$, the discriminant of the ring $R_+ = \mathbb{Z}[\sigma]$ equals $a^2 - 4b$. This equals $(\sigma - \tau)^2$, so it belongs to the open interval $(0, 16q)$. From $\Delta(R_+) = (\mathcal{O}_+ : R_+)^2 \Delta(\mathcal{O}_+)$ we obtain $0 < \Delta(\mathcal{O}_+) \leqslant \Delta(R_+)$.

We have $\Delta(\mathcal{O}) > 0$ since K has an even number of complex places, and $\Delta(R) = (\mathcal{O} : R)^2 \Delta(\mathcal{O}) \geqslant \Delta(\mathcal{O})$. The irreducible polynomial of π over K_+ is $X^2 - \sigma X + q$, and its discriminant $(\pi - \overline{\pi})^2 = \sigma^2 - 4q$ equals the discriminant of the R_+-basis 1, π for R. By an easy computation, the norm map $K_+ \to \mathbb{Q}$ sends this discriminant to $(b + 4q)^2 - 4qa^2$; so using the $\mathbb{Z}$-basis 1, σ, π, $\sigma\pi$ for R one finds that $\Delta(R) = ((b + 4q)^2 - 4qa^2) \cdot \Delta(R_+)^2$. One obtains the inequality $\Delta(R) \leqslant 256q^4$ by maximizing $((b + 4q)^2 - 4qa^2) \cdot (a^2 - 4b)^2$ as a function of real variables a and b over the domain described by the inequalities in Proposition 7.1; the maximum is assumed at $a = 0$, $b = -2q$.

The equality $c(h) = \sqrt{\Delta(R)}/\sqrt{\Delta(R_+)}$ follows immediately. To obtain the stated upper bound for $c(h)$, one maximizes $c(h)^2$ as a function of real variables a and b over the domain described by the inequalities in Proposition 7.1; the maximum is assumed for $a = 0$, $b = -\frac{4}{3}q$.

It remains to prove the upper bound for δ. From

$$(\mathcal{O} : R) = (\mathcal{O} : \mathcal{O}_+[\pi]) \cdot (\mathcal{O}_+[\pi] : R_+[\pi]) = (\mathcal{O} : \mathcal{O}_+[\pi]) \cdot (\mathcal{O}_+ : R_+)^2$$

it follows that the square of each prime l dividing $(\mathcal{O} : R)$ divides one of the numbers $\Delta(\mathcal{O}_+[\pi])/\Delta(\mathcal{O})$ and $\Delta(R_+)$. We have

$$\frac{\Delta(\mathcal{O}_+[\pi])}{\Delta(\mathcal{O})} = \frac{((b + 4q)^2 - 4qa^2) \cdot \Delta(\mathcal{O}_+)^2}{\Delta(\mathcal{O})},$$

and this divides $(b + 4q)^2 - 4qa^2$ because $\Delta(\mathcal{O})$ is divisible by $\Delta(\mathcal{O}_+)^2$. Therefore

we have

$$\delta^2 \leqslant ((b+4q)^2 - 4qa^2) \cdot \Delta(R_+) = c(h)^2.$$

This proves Proposition 7.4.

PROPOSITION 7.5. *With the notation and hypotheses as above, the field K contains an imaginary quadratic subfield if and only if $(b+4q)^2 - 4qa^2$ is an integer square.*

Proof. Clearly K contains an imaginary quadratic subfield if and only if the Galois group G of a normal closure of K over $\mathbb{Q}$ is isomorphic to the Klein four group. Let G be viewed as a transitive permutation group of the four zeros of h. Since K is a tower of two quadratic extensions, the order of G divides 8. Inspecting the symmetric group of degree 4, one sees that a transitive subgroup of order dividing 8 is isomorphic to the Klein four group if and only if it consists of even permutations only. We conclude that K has an imaginary quadratic subfield if and only if its discriminant over $\mathbb{Q}$ is a square. By the formula for $\Delta(R)$ in Proposition 7.4, this discriminant equals $(b+4q)^2 - 4qa^2$ (modulo $\mathbb{Q}^{*2}$). This proves Proposition 7.5.

REMARK 7.6. In § 2, we defined h to be *regular* if neither of $a^2 - 4b$ and $(b+4q)^2 - 4qa^2$ is an integer square. From Propositions 7.2 and 7.5 we see that h is regular if and only if the ring $\mathbb{Q}[X]/(h)$ is a field that does not have an imaginary quadratic subfield.

The notation $\mathrm{Pic}_* R$ and $w(R)$ in the following result was introduced in § 6.

PROPOSITION 7.7. *Let the notation and hypotheses be as in Proposition* 7.4*, and assume moreover that h is regular. Then we have*

$$\frac{\#\mathrm{Pic}_* R}{w(R)} \geqslant \frac{c(h)}{95{,}000 \cdot (\log q)^2 \cdot (\log\log q)^2}$$

whenever $q \geqslant 8100$.

Proof. By Proposition 7.5, the field K does not contain an imaginary quadratic subfield. Hence we can apply Theorem 6.2 with $d = 2$. Using the equalities and inequalities given in Proposition 7.4 we obtain

$$\frac{\#\mathrm{Pic}_* R}{w(R)} \geqslant \frac{c(h)}{40{,}000 \cdot (\log\log \max\{32(q/3)^{3/2}, 6000\})^2 \cdot \log(16q) \cdot \log(4q)}.$$

Applying the inequalities

$$\frac{32}{3\sqrt{3}} \cdot q^{3/2} \geqslant 6000, \quad \frac{95{,}000}{40{,}000} \cdot \frac{(\log q)^2}{\log(4q) \cdot \log(16q)} \cdot \left(\frac{\log\log q}{\log\log(32(q/3)^{3/2})} \right)^2 \geqslant 1,$$

which are valid for $q \geqslant 8100$, we arrive at Proposition 7.7.

In the final results of this section we make the additional assumption that h be ordinary.

PROPOSITION 7.8. *Let h be an ordinary regular Weil polynomial of degree 4, let π be a zero of h in an extension field of $\mathbb{Q}$, and let $K = \mathbb{Q}(\pi)$. Then for every positive integer n one has $K = \mathbb{Q}(\pi^n)$.*

Proof. From

$$(\pi + \overline{\pi})^2 - a(\pi + \overline{\pi}) = -b, \quad \pi\overline{\pi} = q, \quad \gcd(b, q) = 1$$

it follows that π and $\overline{\pi}$ generate the unit ideal of R. Therefore, for any positive integer n, the elements π^n and $\overline{\pi}^n$ generate the unit ideal as well. Since they are not units, that implies in particular that they are distinct: $\pi^n \neq \overline{\pi}^n$. Therefore π^n does not belong to K_+, and $\mathbb{Q}(\pi^n)$ is not contained in K_+. But since K does, by Proposition 7.5, not have an imaginary quadratic subfield, every proper subfield of K is contained in K_+. It follows that $\mathbb{Q}(\pi^n)$ must be equal to all of K. This proves Proposition 7.8.

PROPOSITION 7.9. *Let h be an ordinary regular Weil polynomial of degree 4, and let π and ρ be zeros of h in an extension field of $\mathbb{Q}$. Then we have $\rho \neq \overline{\pi}$ if and only if the field $\mathbb{Q}(\pi, \rho)$ has an exponential valuation v for which $v(\pi) > 0$, $v(\rho) > 0$, and $v(q) > 0$.*

Proof. As we saw in the proof of Proposition 7.8, the elements π and $\overline{\pi}$ generate the unit ideal of R, and so there is no exponential valuation v of $\mathbb{Q}(\pi)$ with $v(\pi) > 0$ and $v(\overline{\pi}) > 0$. This proves the 'if' part. For the 'only if' part, we assume that $\rho \neq \overline{\pi}$. Suppose that π and ρ are coprime in the ring of algebraic integers $\mathcal{O}'$ of $\mathbb{Q}(\pi, \rho)$. Since ρ divides $\pi\overline{\pi} = q$, it must divide $\overline{\pi}$. Then $\overline{\pi}/\rho$ is an algebraic integer all of whose conjugates in the complex plane have absolute value 1, so it is a root of unity. Then we have $\rho^n = \overline{\pi}^n$ for some positive integer n, while $\rho \neq \overline{\pi}$. Hence the total number of conjugates of π^n is smaller than 4. This contradicts Proposition 7.8. It follows that $\mathcal{O}'$ has a maximal ideal that contains both π and ρ. Then it contains $q = \pi\overline{\pi}$ as well. This maximal ideal gives rise to an exponential valuation v of $\mathbb{Q}(\rho, \pi)$ with $v(\pi) > 0$, $v(\rho) > 0$, and $v(q) > 0$, as required. This proves Proposition 7.9.

8. *Abelian surfaces with a given Weil polynomial*

In this section we prove Proposition 2.3. We denote by k a finite field, by q its cardinality, by p its characteristic, and by $\overline{k}$ an algebraic closure of k. An Abelian variety A over k is called *ordinary* if the number of elements of the group $A(\overline{k})$ of order dividing p equals $p^{\dim A}$. By $\mathbb{Q}_p$ we denote the field of p-adic numbers.

We recall Deligne's description, given in [**4**], of the category of ordinary Abelian varieties over k, and the corresponding description of their polarizations given by Howe [**6**].

By a *Deligne q-module*, or briefly a *Deligne module*, we mean a pair (T, F), where T is a finitely generated free $\mathbb{Z}$-module and F is an endomorphism of T satisfying the following conditions:

(a) the endomorphism of $T \otimes_{\mathbb{Z}} \mathbb{Q}$ induced by F is semi-simple, in the sense that $H(F) = 0$ for some square-free polynomial $H \in \mathbb{Q}[X]$, and all eigenvalues of F in $\mathbb{C}$ have absolute value $q^{1/2}$;

(b) at least half of the zeros of the characteristic polynomial of F in an algebraic closure of $\mathbb{Q}_p$, counting multiplicities, are p-adic units;

(c) there is an endomorphism V of T such that $FV = q$.

If (T, F) and (T', F') are Deligne modules, then a *morphism* from (T, F) to (T', F') is a group homomorphism $\psi\colon T \to T'$ such that $\psi \circ F = F' \circ \psi$.

Every Deligne module (T, F) has a *dual* Deligne module $(\check{T}, \check{F})$, defined by $\check{T} = \mathrm{Hom}(T, \mathbb{Z})$ and $(\check{F}u)(t) = u(Vt)$ for $u \in \check{T}$ and $t \in T$. Any morphism $\psi\colon (T, F) \to (T', F')$ of Deligne modules induces a dual morphism $\check{\psi}\colon (\check{T}', \check{F}') \to (\check{T}, \check{F})$, by $\check{\psi}(u)(t) = u(\psi(t))$ for $u \in \check{T}'$ and $t \in T$.

For any Deligne module (T, F), the subring $R = \mathbb{Z}[F, V]$ of the algebra of endomorphisms of (T, F) that is generated by F and V has the following two properties: first, its additive group is finitely generated and free as a $\mathbb{Z}$-module; and second, $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a product of finitely many totally imaginary algebraic number fields, each of which is a quadratic extension of a totally real number field. Let, generally, R be a ring satisfying these two conditions. By a *CM-type* for R we mean a set Φ of ring homomorphisms $\phi\colon R \to \mathbb{C}$ with the property that for each ring homomorphism $\psi\colon R \to \mathbb{C}$ there exist a unique element $\phi \in \Phi$ and a unique element c of the Galois group of $\mathbb{C}$ over $\mathbb{R}$ such that $\psi = c \circ \phi$. If Φ is a CM-type for R, then an element $\iota \in R$ is called Φ-*positive* if for each $\phi \in \Phi$ the number $\phi(\iota)/i$ is real and positive; here $i \in \mathbb{C}$ denotes a fixed square root of -1. Such elements ι exist for every Φ.

With this terminology, we call a morphism $\lambda\colon (T, F) \to (\check{T}, \check{F})$ a *polarization* of (T, F) with respect to a CM-type Φ for $R = \mathbb{Z}[F, V]$, if the $\mathbb{Z}$-bilinear map $T \times T \to \mathbb{Z}$ that sends (s, t) to $\lambda(t)(\iota s)$ is symmetric and positive definite. (This does not depend on the choice of ι; cf. [**6**, (4.10)]. The other conditions mentioned in [**6**, (4.10)] are automatic.) A polarization λ is called *principal* if it is an isomorphism $(T, F) \to (\check{T}, \check{F})$. By a *principally polarized Deligne module* we mean a pair consisting of a Deligne module (T, F) and a principal polarization λ of (T, F); this notion is relative to a choice of Φ.

Let W denote the ring of Witt vectors over $\overline{k}$. It is isomorphic to the completion of the ring of integers of a maximal unramified extension of $\mathbb{Q}_p$. Denote by $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ inside $\mathbb{C}$. For a ring homomorphism $\epsilon\colon W \to \mathbb{C}$, we let v_ϵ be the unique exponential valuation on $\overline{\mathbb{Q}}$ that extends the valuation on $\overline{\mathbb{Q}} \cap \epsilon(W)$ coming from W, normalized so that $v_\epsilon(p) = 1$. For any ϵ and any ring $R = \mathbb{Z}[F, V]$ as considered above, the set $\Phi_\epsilon = \{\phi\colon R \to \mathbb{C}\colon v_\epsilon(\phi(F)) > 0\}$ is a CM-type for R.

THEOREM 8.1. *For each ring homomorphism $\epsilon\colon W \to \mathbb{C}$ there exists a category equivalence $\mathscr{D} = \mathscr{D}_{\epsilon,k}$ from the category of ordinary Abelian varieties over k to the category of Deligne q-modules, such that for every ordinary Abelian variety A over k, with $\mathscr{D}(A) = (T, F)$, the following is true:*

(a) *the characteristic polynomial of F on T equals the characteristic polynomial h_A of the Frobenius endomorphism of A;*

(b) *if $\check{A}$ is the Abelian variety over k that is dual to A, then $\check{A}$ is ordinary, and there is an identification $\mathscr{D}(\check{A}) = (\check{T}, \check{F})$, functorial in A, with the property that a morphism $\xi\colon A \to \check{A}$ is a polarization, or a principal polarization, if and only if the map $\mathscr{D}(\xi)\colon (T, F) \to (\check{T}, \check{F})$ is a polarization, or a principal polarization, respectively, with respect to Φ_ϵ;*

(c) *if l is a finite extension of k inside $\overline{k}$, then $\mathscr{D}_{\epsilon,l}(A \otimes_k l)$ is the Deligne $q^{[l:k]}$-module $(T, F^{[l:k]})$.*

Proof. The construction of $\mathscr{D}$ and the proof that it is an equivalence of categories can be found in [**4**]. Properties (a) and (c) are clear from the construction. For (b) we refer to [**6**, § 4]; the functoriality statement, which means that $\mathscr{D}(\check{f}) = \mathscr{D}(f)^{\check{}}$ for any morphism f of Abelian varieties, is obtained from [**6**, proof of (4.5)] combined with [**11**, Lemma 16.2(b)]. This proves Theorem 8.1.

In the following result, we use the notation Pic_* and w introduced in § 6. For the meaning of 'weighted number', see § 2.

PROPOSITION 8.2. *Let h be an ordinary regular Weil polynomial of degree 4, and let $R = \mathbb{Z}[\pi, \overline{\pi}]$ be as defined before Proposition 7.3. Then the weighted number of principally polarized two-dimensional Abelian varieties (A, ξ) over k with $h_A = h$ is at least $(\#\mathrm{Pic}_* R)/w(R)$.*

Proof. There is no harm in assuming that R is actually a subring of $\mathbb{C}$. More specifically, among the two complex zeros of h with positive imaginary part, we let π be the one that has the largest real part. Of the two complex zeros of h different from π and $\overline{\pi}$, let ρ be the one with negative imaginary part. The fourth zero is then $\overline{\rho}$. We define $\iota = (\pi - \overline{\pi})(\pi + \overline{\pi} - \rho - \overline{\rho}) \in R$ as in Proposition 7.3. Let the set Φ consist of the inclusion map $R \to \mathbb{C}$ and the map $R \to \mathbb{C}$ that maps π to ρ and $\overline{\pi}$ to $\overline{\rho}$; the existence of the latter map follows from the irreducibility of h. The set Φ is clearly a CM-type for R, and the labeling of the zeros of h implies that ι is Φ-positive. Since $\rho \neq \overline{\pi}$, there is by Proposition 7.9 an exponential valuation v of $\mathbb{Q}(\pi, \rho)$ such that $v(\pi) > 0$, $v(\rho) > 0$, and $v(p) > 0$, and we can normalize v so that $v(p) = 1$. We may extend v to a valuation of $\overline{\mathbb{Q}}$, which we likewise denote by v, and extend the inclusion of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ to an embedding of its completion $\overline{\mathbb{Q}}_v$ with respect to v into $\mathbb{C}$. Composing that embedding with a continuous embedding $W \to \overline{\mathbb{Q}}_v$ we obtain an embedding $W \to \mathbb{C}$, which we call ϵ. The construction of ϵ implies that v_ϵ equals v. Also, the definition of Φ and the choice of v imply that $\Phi = \Phi_\epsilon$.

The group $\mathrm{Pic}_* R$ was defined, in § 6, to consist of equivalence classes of pairs (I, β), where I is an invertible R-ideal in the field K of fractions of R, and where $\beta \in K_{+\gg 0}$ is such that $I\overline{I} = \beta R$. We show that each such pair (I, β) gives rise to a principally polarized Deligne module. First, denoting the map $I \to I$ sending x to πx simply by π, we claim that (I, π) is a Deligne module. Namely, from $I \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$ one sees that the characteristic polynomial of π on I equals h. Since h is irreducible, this implies property (a) in the definition of Deligne modules. From the 'if'-part of Proposition 7.9 we obtain (b), and to prove (c) we let V be the map sending x to $\overline{\pi} x$. Next we claim that there is an isomorphism $\lambda\colon (I, \pi) \to (\check{I}, \check{\pi})$ with

$$\lambda(t)(s) = \mathrm{Tr}(s\bar{t}(\beta\iota)^{-1}), \tag{8.3}$$

where Tr denotes the trace map $K \to \mathbb{Q}$. To prove this we first note that by the non-degeneracy of the trace map there is, for each group homomorphism $u\colon I \to \mathbb{Q}$, a unique element $\alpha \in K$ such that for all $s \in I$ one has $u(s) = \mathrm{Tr}(s\alpha)$. Let u and α be such. Then $u(I)$ is a subset of $\mathbb{Z}$ if and only if $\mathrm{Tr}(\alpha I) \subset \mathbb{Z}$. This

is equivalent to $\alpha I \subset R\iota^{-1}$, by Proposition 7.3, and to $\alpha \in I^{-1}\iota^{-1} = \overline{I}(\beta\iota)^{-1}$. Thus, for each $t \in I$ the map $\lambda(t)\colon I \to \mathbb{Q}$ defined by (8.3) takes values in $\mathbb{Z}$, and each group homomorphism $I \to \mathbb{Z}$ is of the form $\lambda(t)$ for a unique $t \in I$. It follows that λ is an isomorphism from I to $\check{I} = \mathrm{Hom}(I, \mathbb{Z})$. We have $\lambda(\pi t)(s) = \lambda(t)(\overline{\pi}s)$, so λ is actually a morphism, and hence an isomorphism, of Deligne modules. Finally, we claim that λ is a polarization, and hence a principal polarization, of (I, π). This is equivalent to the expression $\lambda(t)(\iota s) = \mathrm{Tr}(s\overline{t}/\beta)$ being symmetric and positive definite as a function of s and t, which follows from $\beta \in K_{+\gg 0}$.

This concludes the construction of a principally polarized Deligne module $((I, \pi), \lambda)$, starting from a pair (I, β). Let (J, γ) be a second such pair, giving rise to a principally polarized Deligne module $((J, \pi), \mu)$. We investigate all isomorphisms of principally polarized Deligne modules $((I, \pi), \lambda) \to ((J, \pi), \mu)$, that is, group isomorphisms $\sigma\colon I \to J$ with $\sigma\pi = \pi\sigma$ that satisfy $\lambda(t)(s) = \mu(\sigma t)(\sigma s)$ for all $t, s \in I$, or, equivalently, $\lambda = \check{\sigma}\mu\sigma$. The group isomorphisms $\sigma\colon I \to J$ respecting the action of π are given by $x \mapsto \alpha x$, where $\alpha \in K$ satisfies $\alpha I = J$. The condition $\lambda(t)(s) = \mu(\sigma t)(\sigma s)$ amounts to

$$\mathrm{Tr}(s\overline{t}(\beta\iota)^{-1}) = \mathrm{Tr}(\alpha s\overline{\alpha}\overline{t}(\gamma\iota)^{-1}) \quad \text{for all } s, t \in I,$$

which is equivalent to $\alpha\overline{\alpha}\beta = \gamma$. This implies, first, that two pairs (I, β), (J, γ) give rise to isomorphic principally polarized Deligne modules if and only if they define the same element of $\mathrm{Pic}_* R$; so the number of isomorphism classes of principally polarized Deligne modules obtained in this way is equal to $\#\mathrm{Pic}_* R$. Secondly, we find that the automorphism group of each $((I, \pi), \lambda)$ may be identified with the group of all $\alpha \in K^*$ satisfying $\alpha I = I$ and $\alpha\overline{\alpha} = 1$. Clearly any root of unity α in R satisfies these conditions; and no other element $\alpha \in K^*$ does, since the first condition implies that $\alpha R = \alpha I\overline{I}/\beta = I\overline{I}/\beta = R$, so $\alpha \in R^*$, while the second condition gives $\alpha \in \ker(N\colon R^* \to R_+^*) = \mu(R)$. The conclusion is that each $((I, \pi), \lambda)$ has exactly $w(R)$ automorphisms.

We conclude that the 'weighted number' of principally polarized Deligne modules that we constructed equals $(\#\mathrm{Pic}_* R)/w(R)$. The notion of isomorphism of principally polarized Deligne modules that we just used corresponds, under the category equivalence of Theorem 8.1, to the notion of isomorphism of principally polarized Abelian varieties, by Theorem 8.1(b). Thus, the weighted number of principally polarized Abelian varieties (A, ξ) over k that we obtain is also $(\#\mathrm{Pic}_* R)/w(R)$. As we saw above, the characteristic polynomial of π on each I equals h, so by Theorem 8.1(a) each of these A satisfies $h_A = h$. This proves Proposition 8.2.

Proof of Proposition 2.3. The first assertion of Proposition 2.3 follows from Propositions 8.2 and 7.7. For the last two assertions, let A be any Abelian variety over k with $h_A = h$. Then A is ordinary, by [**4**, § 2]. To prove that A is absolutely simple, let B be a non-zero Abelian subvariety of $A \otimes_k l$, for some finite extension l of k in $\overline{k}$; it will suffice to prove that $B = A \otimes_k l$. Let $n = [l : k]$. By Theorem 8.1(c) and 8.1(a), the Weil polynomial of $A \otimes_k l$ over l is the characteristic polynomial of F^n on T, where $\mathscr{D}(A) = (T, F)$. Its complex zeros, counting multiplicities, are the nth powers of the complex zeros of h. Proposition 7.8 now implies that the Weil polynomial of $A \otimes_k l$ over l is irreducible over $\mathbb{Q}$. Therefore the Weil polynomial of B over l, which divides the Weil polynomial of $A \otimes_k l$, is actually equal to it. Hence B has the same dimension as $A \otimes_k l$, and therefore

$B = A \otimes_k l$, as desired. To prove the last assertion of Proposition 2.3, it suffices to remark that the trace of the Frobenius automorphism of A, as defined in [**11**], is equal to the trace of h_A, as defined in § 2. This proves Proposition 2.3.

9. *Non-uniqueness of factorization in short intervals*

In the present section we prove the following result.

PROPOSITION 9.1. *Let q be an integer with $q > 1$. Then there are fewer than $6 \cdot \sqrt{q} + 11$ integers z for which there exist integers r, s, t and u in the interval $[(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$ with $z = rs = tu$ and $\{r, s\} \neq \{t, u\}$.*

In § 10 we shall use Proposition 9.1 in the proof of Proposition 2.4(a). The present section can be skipped by readers who are interested in Proposition 2.4(b) only; the latter result suffices both for our smoothness test and for the application to primality testing alluded to in the introduction.

We deduce Proposition 9.1 from a general result on positive integer solutions to the equation $rs = tu$ that lie in a short interval $[L, U]$. If the length $U - L$ of the interval is at most $2\sqrt{L}$, then all solutions are trivial in the sense that $\{r, s\} = \{t, u\}$ (see Remark 9.3). In the proof of Proposition 9.1 we shall take $U = (\sqrt{q}+1)^2$ and $L = (\sqrt{q}-1)^2$; then $U - L$ is a little larger, but it is still $O(\sqrt{L})$. In that case the number of non-trivial solutions is $O(\sqrt{L})$ (see Remark 9.3).

The number of integers z as in Proposition 9.1 is actually equal to $(\lambda + o(1)) \cdot \sqrt{q}$ for $q \to \infty$, where λ is given by

$$\lambda = 4\log(2+\sqrt{3}) + 6\log(1+\sqrt{2}) + \tfrac{10}{3}\log 3 - 2\sqrt{3} - 3\sqrt{2} - \tfrac{10}{3} \doteq 3.178038436.$$

This can be shown by an elaboration of our argument.

We denote by $[x]$ the greatest integer not exceeding x.

LEMMA 9.2. *Let U and L be real numbers with $U > L > 0$, and let $S = \{x \in \mathbb{Z} : L \leqslant x \leqslant U\}$. Then the following is true.*

(a) *The number $M(L, U)$ of triples r, s, t in S for which $rs = t^2$ and $r > t$ satisfies*

$$M(L,U) \leqslant \sum_d \binom{M_d}{2} < (\sqrt{U}-\sqrt{L})^2 \cdot (\tfrac{3}{2} + \max\{\log(\sqrt{U}-\sqrt{L}), 0\}),$$

the sum ranging over the positive integers d with $d \leqslant (\sqrt{U}-\sqrt{L})^2$, where $M_d = [\sqrt{U/d} - \sqrt{L/d} + 1]$.

(b) *The number $N(L, U)$ of quadruples r, s, t, u in S for which $rs = tu$ and $r > \max\{t, u\}$ satisfies*

$$\begin{aligned} N(L,U) &\leqslant \sum_{a,b} (2(b-a)+1) \\ &\quad \times \left[1 + \frac{1}{b}\sqrt{(\sqrt{U}-\sqrt{L})^2 - ab}\,\sqrt{(\sqrt{U}+\sqrt{L})^2 - ab}\right] \\ &< 2(U-L)(\sqrt{U}-\sqrt{L})^2(1+\max\{\log(\sqrt{U}-\sqrt{L}), 0\}) \\ &\quad + 2(\sqrt{U}-\sqrt{L})^4, \end{aligned}$$

the sum ranging over all pairs of positive integers a, b with $a \leqslant b$ and $ab \leqslant (\sqrt{U} - \sqrt{L})^2$.

REMARK 9.3. The sums appearing in (a) and (b) are empty when $U < (\sqrt{L} + 1)^2$; so in that case there are no non-trivial solutions to $rs = tu$ in S. If $U - L = O(\sqrt{L})$, then $\sqrt{U} - \sqrt{L} = O(1)$, so by (b) the number of non-trivial solutions is $O(\sqrt{L})$, and by (a) the number of non-trivial solutions with $t = u$ is $O(1)$.

Proof of Lemma 9.2. (a) Let r, s and t in S satisfy $rs = t^2$ and $r > t$, and put $d = \gcd(r, s)$. Then there are coprime positive integers a and b with $a > b$ and $r = a^2 d$ and $s = b^2 d$. Hence, if for each positive integer d we denote by N_d the number of positive integers c with $c^2 d \in S$, then we have

$$M(L, U) \leqslant \sum_{d \geqslant 1} \binom{N_d}{2}.$$

We have $N_d \leqslant M_d$, where M_d is as in the statement of the lemma. For $d > (\sqrt{U} - \sqrt{L})^2$ one has $M_d = 1$ so

$$\binom{M_d}{2} = 0.$$

This proves the first inequality in (a). The second, which will not be used in the sequel, follows from the inequalities

$$\sum_d \frac{1}{d} \leqslant 1 + \max\{\log T, 0\}, \quad \sum_d \frac{1}{\sqrt{d}} < 2\sqrt{T}$$

for any $T > 0$, where d ranges over the positive integers less than or equal to T.

(b) Let r, s, t and u in S satisfy $rs = tu$ and $r > \max\{t, u\}$. Define $y = \gcd(s, u)$, $x = s/y$ and $x' = u/y$. Then we have $\gcd(x, x') = 1$, so from $rx = rs/y = tu/y = tx'$ it follows that x divides t. Therefore we have $t = xy'$ and $r = x'y'$ for some integer y'. From $r > \max\{t, u\}$ we see that $x' > x$ and $y' > y$; so we can write $x' = x + a$ and $y' = y + b$ with positive integers a and b. The quadruple r, s, t, u can now be expressed in x, y, a, b:

$$r = (x + a)(y + b), \quad s = xy, \quad t = x(y + b), \quad u = (x + a)y.$$

Hence $N(L, U)$ is at most the number of quadruples of positive integers x, y, a, b satisfying

$$L \leqslant xy, \quad (x + a)(y + b) \leqslant U.$$

(In fact, one easily proves that $N(L, U)$ equals the number of such quadruples satisfying $\gcd(x, a) = 1$, but we shall not use the latter condition.)

For each pair a, b of positive integers, let $R_{a,b}$ denote the plane region

$$R_{a,b} = \{(x, y) \in \mathbb{R}^2 : x > 0, y > 0, L \leqslant xy, (x + a)(y + b) \leqslant U\}.$$

Writing $N_{a,b} = \#(R_{a,b} \cap \mathbb{Z}^2)$, we may express the result just proved by $N(L, U) \leqslant \sum_{a,b} N_{a,b}$, the sum ranging over all pairs of positive integers a, b. Since we have evidently $N_{a,b} = N_{b,a}$, we may rewrite this as

$$N(L, U) \leqslant \sum_{a=b} N_{a,b} + 2 \sum_{a<b} N_{a,b}, \tag{9.4}$$

the sums still ranging over pairs of positive integers.

Let a and b be positive integers for which $R_{a,b}$ is non-empty, and let $(x, y) \in R_{a,b}$. Then we have $ab < (x+a)(y+b) \leqslant U$. To obtain a better upper bound for ab, we remark that $L/x \leqslant y \leqslant U/(x+a) - b$, so that we have

$$bx^2 + (L - U + ab)x + La \leqslant 0.$$

This implies that the zeros ρ_1 and ρ_2 of the quadratic polynomial $bz^2 + (L - U + ab)z + La$ are real, with $\rho_1 \leqslant \rho_2$ (say), and that x lies between them: $\rho_1 \leqslant x \leqslant \rho_2$. The discriminant $\Delta(a, b)$ of the polynomial, which is given by

$$\Delta(a, b) = (L - U + ab)^2 - 4Lab = ((\sqrt{U} - \sqrt{L})^2 - ab) \cdot ((\sqrt{U} + \sqrt{L})^2 - ab),$$

is equal to $b^2 \cdot (\rho_2 - \rho_1)^2$ and therefore non-negative. Since we know already that $ab < U < (\sqrt{U} + \sqrt{L})^2$, this implies that $ab \leqslant (\sqrt{U} - \sqrt{L})^2$. It follows that the sum in (9.4) may be restricted to those pairs a, b for which we have $ab \leqslant (\sqrt{U} - \sqrt{L})^2$.

We claim that for any of these pairs a, b we have

$$N_{a,b} \leqslant \left[1 + \frac{\sqrt{\Delta(a, b)}}{b}\right] + N_{a,b+1}. \tag{9.5}$$

For each $(x, y) \in R_{a,b}$, the number x lies in the interval $[\rho_1, \rho_2]$ of length $\sqrt{\Delta(a, b)}/b$, and the number of integers in this interval is at most the term in square brackets in (9.5). Hence, to prove (9.5), it suffices to show the following: if x is any integer, then the number of integers y with $(x, y) \in R_{a,b}$ is at most 1 more than the number of integers y with $(x, y) \in R_{a,b+1}$. This is clear if no integer y exists with $(x, y) \in R_{a,b}$. In the other case, let y' be the smallest integer with $(x, y') \in R_{a,b}$. Then the definition of $R_{a,b}$ immediately implies that for any integer $y > y'$ with $(x, y) \in R_{a,b}$ one has $(x, y-1) \in R_{a,b+1}$. This proves (9.5).

Repeatedly applying (9.5) one finds that

$$N_{a,b} \leqslant \sum_{b'} \left[1 + \frac{\sqrt{\Delta(a, b')}}{b'}\right],$$

the sum ranging over all integers $b' \geqslant b$ with $ab' \leqslant (\sqrt{U} - \sqrt{L})^2$. Substituting this inequality in (9.4), and collecting terms, we obtain

$$N(L, U) \leqslant \sum_{a,b} (2(b-a)+1) \cdot \left[1 + \frac{\sqrt{\Delta(a, b)}}{b}\right],$$

the sum ranging over all pairs of positive integers a, b with $a \leqslant b$ and $ab \leqslant (\sqrt{U} - \sqrt{L})^2$. By our formula for $\Delta(a, b)$, this is the same as the first inequality in (b). The proof of the second inequality in (b), which will not be used in the sequel, is elementary, and left to the reader. This proves Lemma 9.2.

Proof of Proposition 9.1. The number of integers z as in the statement of Proposition 9.1 is at most the number of quadruples of integers r, s, t, u with

$$rs = tu, \quad (\sqrt{q}+1)^2 \geqslant r > t \geqslant u > s \geqslant (\sqrt{q}-1)^2.$$

That number is, in the notation of Lemma 9.2, equal to $\frac{1}{2}(M(L, U) + N(L, U))$, where $L = (\sqrt{q}-1)^2$ and $U = (\sqrt{q}+1)^2$. We have $(\sqrt{U} - \sqrt{L})^2 = 4$, so the sum in Lemma 9.2(a) ranges over $1 \leqslant d \leqslant 4$, and it gives

$$M(L, U) \leqslant 3 + 1 + 1 + 1 = 6.$$

The sum in Lemma 9.2(b) ranges over $(a, b) \in \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2)\}$. We have $(\sqrt{U} + \sqrt{L})^2 = 4q$, and so we find that

$$N(L, U) \leqslant [1 + \sqrt{3} \cdot \sqrt{4q - 1}] + 3[1 + \tfrac{1}{2}\sqrt{2} \cdot \sqrt{4q - 2}] + 5[1 + \tfrac{1}{3}\sqrt{4q - 3}] + 7 + 1$$

$$< 17 + (2\sqrt{3} + 3\sqrt{2} + \tfrac{10}{3}) \cdot \sqrt{q} < \tfrac{265}{24}\sqrt{q} + 17 < 12\sqrt{q} + 16.$$

It follows that $\frac{1}{2}(M(L, U) + N(L, U)) < 6\sqrt{q} + 11$, as required. This proves Proposition 9.1.

10. *Constructing Weil polynomials*

In this section we prove Proposition 2.4.

In Proposition 7.1 we described all Weil q-polynomials of degree 4 in terms of two integer parameters a and b that satisfy certain inequalities. Writing these inequalities in terms of $\alpha = a/\sqrt{q}$ and $\beta = b/q$, we get a region W that is independent of q:

$$W = \{(\alpha, \beta) \in \mathbb{R}^2 \colon |\alpha| \leqslant 4,\ 2|\alpha| - 4 \leqslant \beta \leqslant \tfrac{1}{4}\alpha^2\}.$$

Figure 10.1 provides a picture of W.

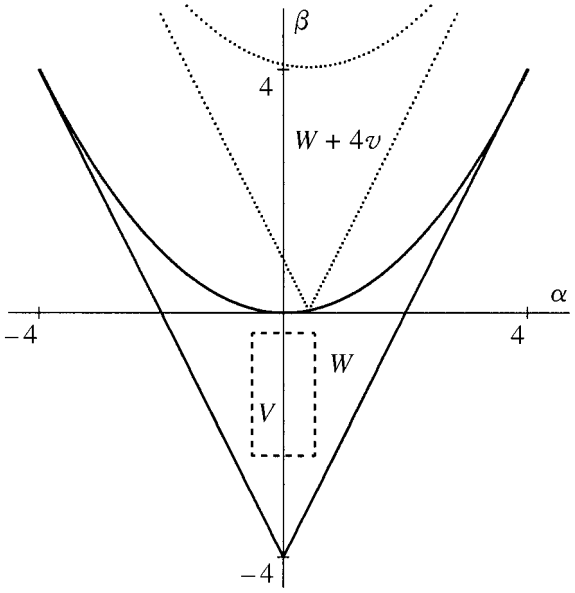

FIGURE 10.1. *The sets W, V and* $W + 4v$ (*for* $q = 101$).

The evaluation map $h \mapsto h(1)$ may be illustrated on this picture. If $h = h_{a,b}$ is an ordinary Weil q-polynomial then we have

$$h(1) = (q + 1)^2 - a(q + 1) + b.$$

If one fixes $h(1)$, one obtains a relation between a and b that determines a line of slope $q + 1$ in the (a, b)-plane; in the (α, β)-plane the slope is $(q + 1)/\sqrt{q}$. More precisely, two integer vectors (a, b) give rise to the same value for $h(1)$ if and only if they differ by an integer multiple of the vector $(1, q + 1)$, and if and only if the corresponding vectors (α, β) differ by an integer multiple of

$v = (1/\sqrt{q}, 1 + 1/q)$. The intersection of $W + 4v$ with W consists of the single point $4v + (0, -4) = (4/\sqrt{q}, 4/q)$, which lies on the parabolic piece of the boundary of W (see Figure 10.1). Since two Abelian varieties over a finite field are isogenous if and only if they have the same Weil polynomial (see [**21**, Theorem 1(c)]), it follows that for any finite field k and any integer z there are at most five isogeny classes of Abelian varieties A over k for which $\#A(k) = z$; and at most four if the single value $z = (\#k - 1)^2$ is excluded, or if only Abelian varieties A for which h_A has no real zero are considered (for example, ordinary Abelian varieties; see Proposition 7.1).

Proposition 2.4 asserts that, for most z in a certain range, there is at least one suitable Weil polynomial h with $h(1) = z$. Here 'suitable' means that h is ordinary and regular, that, in the case of Proposition 2.4(b), the trace of h is odd, and that $c(h)$ is appropriately large. The latter condition is equivalent to the corresponding point (α, β) not being close to the boundary of W.

LEMMA 10.2. *For any prime power q the following is true.*

(a) *The number of ordinary Weil q-polynomials $h = h_{a,b}$ for which $a \neq 0$ and $(b + 4q)^2 - 4qa^2$ is an integer square is less than $14\sqrt{q}$.*

(b) *The number of ordinary Weil q-polynomials $h = h_{a,b}$ for which a is odd and $(b + 4q)^2 - 4qa^2$ is an integer square is less than $4\sqrt{q} + 2$.*

(c) *If $h_{a,b}$ is an ordinary Weil q-polynomial for which $(b + 4q)^2 - 4qa^2$ is an integer square, and both q and a are even, then one has $a = 0$ or $a^2 - 4b = 0$.*

Proof. (a) Suppose that $h = h_{a,b}$ is an ordinary Weil q-polynomial with $a \neq 0$, and that $(b + 4q)^2 - 4qa^2 = c^2$ for some integer c. Then we have $c^2 \equiv b^2 \bmod 4q$. Since h is ordinary, we have $\gcd(b, q) = 1$, and hence we have, both for q even and for q odd, that $c \equiv \pm b \bmod 2q$. Changing the sign of c, if necessary, we may assume that $c \equiv b \equiv b + 4q \bmod 2q$, so that we may write

$$c = b + 4q - 2kq$$

for some integer k. From the inequalities $b + 4q \geqslant 0$ and

$$0 < 4qa^2 = (b + 4q)^2 - (b + 4q - 2kq)^2 = 4kq(b + 4q - kq)$$

we see that $k > 0$, and that

$$b = \frac{a^2}{k} + (k - 4)q.$$

Hence h is determined by a and k. The inequality $b \leqslant \frac{1}{4}a^2$ from Proposition 7.1 may be rewritten as $(k - 4)(k - a^2/(4q)) \leqslant 0$, so k lies in the closed interval with endpoints 4 and $a^2/(4q)$; we have $a^2/(4q) \leqslant 4$, so we obtain

$$a^2/(4q) \leqslant k \leqslant 4.$$

It follows that $k \in \{1, 2, 3, 4\}$. For each of these values of k we have $0 < |a| \leqslant 2\sqrt{kq}$. Also, since b is an integer, a is divisible by k when $k = 2$ or 3, and a is divisible by 2 when $k = 4$. So for $k = 1, 2, 3, 4$ we have respectively

$$2[2\sqrt{q}],\ 2[\sqrt{2q}],\ 2[2\sqrt{q/3}],\ 2[2\sqrt{q}]$$

possibilities for a, where $[x]$ denotes the largest integer not exceeding x. Assertion (a) now follows because $4 + 2\sqrt{2} + 4/\sqrt{3} + 4 \doteq 13.137828 < 14$.

(b) Next let a be odd. Then we have $a \neq 0$, so we can apply the above. Since k divides a^2, it is odd as well, so we have $k = 1$ or 3. For these values we have respectively

$$2[\sqrt{q} + \tfrac{1}{2}], \quad 2[\sqrt{q/3} + \tfrac{1}{2}]$$

possibilities for a. We have $2 + 2/\sqrt{3} \doteq 3.154701 < 4$, and (b) follows.

(c) Finally, let q and a be even, and suppose that $a \neq 0$. Since $h_{a,b}$ is ordinary and q is even, the number b is odd. From $(a^2/k) + (k-4)q = b \equiv 1 \bmod 2$ and $a \equiv 0 \bmod 2$ it follows that $k = 4$ and that $b = \frac{1}{4}a^2$.

This proves Lemma 10.2.

We define the function C on W by

$$C(\alpha, \beta) = (\alpha^2 - 4\beta) \cdot ((\beta + 4)^2 - 4\alpha^2).$$

If $h = h_{a,b}$ is a Weil polynomial of degree 4, corresponding to the point $(\alpha, \beta) = (a/\sqrt{q}, b/q)$ of W, then we have $c(h) = C(\alpha, \beta)^{1/2} \cdot q^{3/2}$.

LEMMA 10.3. *Let α_0, β_1 and β_2 be real numbers with $\alpha_0 \geqslant 0$, and let W_0 be the region*

$$W_0 = \{(\alpha, \beta) \in \mathbb{R}^2 \colon |\alpha| \leqslant \alpha_0, \beta_1 \leqslant \beta \leqslant \beta_2\}.$$

Suppose that $W_0 \subset W$. Then the minimum of C on W_0 is assumed at one of the points $(0, \beta_1)$, $(0, \beta_2)$, (α_0, β_1) and (α_0, β_2).

Proof. First let β be fixed, with $\beta_1 \leqslant \beta \leqslant \beta_2$. Then $C(\alpha, \beta)$ is a quadratic function of α^2 with a negative leading coefficient. The minimum of any quadratic function with a negative leading coefficient on any compact interval is assumed at one of the endpoints; in our case, at $\alpha^2 = 0$ or at $\alpha^2 = \alpha_0^2$. It follows that the minimum value of $C(\alpha, \beta)$ for fixed β and $|\alpha| \leqslant \alpha_0$ is one of $C(0, \beta)$ and $C(\alpha_0, \beta)$. Next fix $\alpha \in \{0, \alpha_0\}$, and consider $C(\alpha, \beta)$ as a function of β. It is a cubic in β, with a negative leading coefficient, and its zeros are $-4 - 2\alpha$, $-4 + 2\alpha$, and $\frac{1}{4}\alpha^2$. These zeros satisfy $-4 - 2\alpha \leqslant -4 + 2\alpha \leqslant \frac{1}{4}\alpha^2$. Since W_0 lies inside W, we have $-4 + 2\alpha \leqslant \beta \leqslant \frac{1}{4}\alpha^2$, and on that interval $C(\alpha, \beta)$ is first increasing and next decreasing. One deduces that the minimum value of $C(\alpha, \beta)$ is assumed at one of the endpoints β_1 and β_2. This proves Lemma 10.3.

Proof of Proposition 2.4(b). Let p be a prime number with $p \geqslant 8100$. Define

$$a_0 = \max\{a \in \mathbb{Z} \colon a \text{ odd}, a \leqslant \tfrac{14}{27}\sqrt{p}\}, \quad b_0 = \min\{b \in \mathbb{Z} \colon b \geqslant -\tfrac{1}{3}p\}.$$

Then we have

$$\tfrac{14}{27}\sqrt{p} - 2 < a_0 \leqslant \tfrac{14}{27}\sqrt{p}, \quad -\tfrac{1}{3}p \leqslant b_0 < -\tfrac{1}{3}p + 1. \tag{10.4}$$

Put

$$Y = \{a \in \mathbb{Z} \colon |a| \leqslant a_0, \ a \text{ odd}\}, \quad Z = \{b \in \mathbb{Z} \colon b_0 - 2p - 1 \leqslant b \leqslant b_0\},$$

$$X = Y \times Z.$$

We begin by showing that for all $(a, b) \in X$ we have $c(h_{a,b}) \geqslant 4p^{3/2}$. Since we have $p \geqslant 8100$, the points $(a/\sqrt{p}, b/p)$ corresponding to $(a, b) \in X$ all lie within the region

$$V = \{(\alpha, \beta) \in \mathbb{R}^2 : |\alpha| \leqslant \tfrac{14}{17},\ -\tfrac{1}{3} - 2 - \tfrac{1}{8100} \leqslant \beta \leqslant -\tfrac{1}{3} + \tfrac{1}{8100}\}$$

(see Figure 10.1). One easily checks that $V \subset W$. Applying Lemma 10.3 to V, we find that the minimum of C on V is equal to the value of C at one of the points

$$(0, -\tfrac{1}{3} - 2 - \tfrac{1}{8100}),\ (0, -\tfrac{1}{3} + \tfrac{1}{8100}),\ (\tfrac{14}{17}, -\tfrac{1}{3} - 2 - \tfrac{1}{8100}),\ (\tfrac{14}{27}, -\tfrac{1}{3} + \tfrac{1}{8100}).$$

These values are computed to be at least 16, so we have $C \geqslant 16$ on V. From $c(h_{a,b}) = C(a/\sqrt{p}, b/p)^{1/2} \cdot p^{3/2}$ it now follows that $c(h_{a,b}) \geqslant 4p^{3/2}$ for $(a, b) \in X$, as asserted.

We next show that the values $h_{a,b}(1)$ for $(a, b) \in X$ include all integers in the interval $[p^2 - \frac{1}{2}p^{3/2}, p^2 + \frac{1}{2}p^{3/2}]$. From $h_{a,b}(1) = (p+1)^2 - a(p+1) + b$ one sees that

$$h_{a,b}(1) - h_{a+2,b}(1) = 2(p+1).$$

Since Z consists of $2(p+1)$ consecutive integers, and

$$Y = \{-a_0, -a_0 + 2, \ldots, a_0 - 2, a_0\},$$

it follows that the assignment $(a, b) \mapsto h_{a,b}(1)$ gives a bijection of X with the set of integers in the interval

$$[(p+1)^2 - a_0(p+1) + b_0 - 2p - 1,\ (p+1)^2 + a_0(p+1) + b_0].$$

Using the inequalities (10.4) and $\sqrt{p} \geqslant 90$ we find that this interval contains the interval $[p^2 - \frac{1}{2}p^{3/2}, p^2 + \frac{1}{2}p^{3/2}]$. Hence for each integer z in the latter interval there exists a unique Weil p-polynomial $h_{a,b}$ with $(a, b) \in X$ and $h_{a,b}(1) = z$. As we proved above, all these $h_{a,b}$ satisfy $c(h_{a,b}) \geqslant 4p^{3/2}$. Also, they have odd trace, since a is odd for all $(a, b) \in X$.

It remains to consider the values z for which the corresponding Weil polynomial $h_{a,b}$ fails to be ordinary and regular. The number of such z is at most the number of pairs $(a, b) \in X$ satisfying at least one of the following conditions:

(10.5) b is divisible by p,

(10.6) $a^2 - 4b$ is an integer square,

(10.7) $(b + 4p)^2 - 4pa^2$ is an integer square.

To finish the proof of Proposition 2.4(b) it suffices to show that there are at most p such pairs.

If (10.5) holds then we have $b = -p$ or $b = -2p$, and the number of $(a, b) \in X$ for which this occurs is

$$2 \cdot \#Y = 4 \cdot [\tfrac{7}{27}\sqrt{p} + \tfrac{1}{2}] \leqslant \tfrac{28}{27}\sqrt{p} + 2.$$

Suppose that (10.6) holds, so that $a^2 - 4b = d^2$ for some positive integer d. The inequalities $|a| \leqslant \frac{14}{27}\sqrt{p}$ and $-\frac{7}{3}p - 1 \leqslant b < -\frac{1}{3}p + 1$ valid for $(a, b) \in X$ imply that $\frac{4}{3}p - 4 \leqslant d^2 \leqslant \frac{7000}{729}p + 4$. With $p \geqslant 8100$ it follows that $\frac{23}{20}\sqrt{p} \leqslant d \leqslant \frac{31}{10}\sqrt{p}$, so that d lies in an interval of length less than $2(\sqrt{p} - 1)$. Also, we have $d \equiv a \equiv 1 \bmod 2$, so there are at most $\sqrt{p}$ possible values for d. Since a and d determine b, it follows that the number of pairs for which (10.6) occurs is at most $\sqrt{p} \cdot \#Y \leqslant \sqrt{p} \cdot (\frac{14}{27}\sqrt{p} + 1)$.

Finally, Lemma 10.2(b) implies that (10.7) occurs for at most $4\sqrt{p}+2$ pairs (a, b).

Thus the total number of pairs $(a, b) \in X$ satisfying (10.5), (10.6) or (10.7) is at most $\frac{14}{27}p + (6+\frac{1}{27})\sqrt{p}+4$, which is less than p since $p \geqslant 8100$. This proves Proposition 2.4(b).

LEMMA 10.8. *Let q be a power of a prime number. Then for all but at most $6\sqrt{q}+11$ integers z there exists at most one fourth degree Weil q-polynomial $h_{a,b}$ for which a^2-4b is an integer square and $h_{a,b}(1)=z$.*

Proof. Let z be an integer. Suppose that $h_{a,b}(1)=z$ and that a^2-4b is an integer square. Then the numbers σ and τ from the proof of Proposition 7.1 are integers in the closed interval $[-2\sqrt{q}, 2\sqrt{q}]$. We have $h_{a,b}=(X^2-\sigma X+q)\cdot(X^2-\tau X+q)$; so $z=h_{a,b}(1)$ has the factorization $z=(1-\sigma+q)\cdot(1-\tau+q)$ into integers in the interval $[(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$. A second such Weil polynomial gives rise to a different set $\{\sigma, \tau\}$ and hence to a different factorization of z. By Proposition 9.1, this occurs for at most $6\sqrt{q}+11$ values of z. This proves Lemma 10.8.

Proof of Proposition 2.4(a). The proof follows the same general lines as the proof of Proposition 2.4(b), with some additional complications.

Let q be a power of an odd prime number p, and assume that $q \geqslant 14{,}400$. Define

$$a_1 = \max\{a \in \mathbb{Z}: a \leqslant \tfrac{1}{8}\sqrt{q}-1\}, \quad b_1 = \min\{b \in \mathbb{Z}: b \geqslant -\tfrac{4}{3}q+2\}.$$

Then we have

$$\tfrac{1}{8}\sqrt{q}-2 < a_1 \leqslant \tfrac{1}{8}\sqrt{q}-1, \quad -\tfrac{4}{3}q+2 \leqslant b_1 < -\tfrac{4}{3}q+3. \tag{10.9}$$

Put

$$Y_1 = \{a \in \mathbb{Z}: |a| \leqslant a_1\}, \quad Z_1 = \{b \in \mathbb{Z}: b_1 - q \leqslant b \leqslant b_1\},$$

$$X_1 = Y_1 \times Z_1,$$

$$X_2 = \{(a+1, b+q+1): (a, b) \in X_1\}, \quad X_3 = \{(a-1, b-q-1): (a, b) \in X_1\},$$

$$X_0 = X_1 \cup X_2 \cup X_3.$$

We begin by showing that for all $(a, b) \in X_0$ we have $c(h_{a,b}) \geqslant 2q^{3/2}$. All pairs $(a, b) \in X_0$ satisfy $|a| \leqslant \frac{1}{8}\sqrt{q}$ and $-\frac{10}{3}q+1 \leqslant b < -\frac{1}{3}q+4$. Since we have $q \geqslant 14{,}400$, the points $(a/\sqrt{q}, b/q)$ corresponding to $(a, b) \in X_0$ all lie within the region

$$V_0 = \{(\alpha, \beta) \in \mathbb{R}^2: |\alpha| \leqslant \tfrac{1}{8}, -\tfrac{10}{3} \leqslant \beta \leqslant -\tfrac{1}{3}+\tfrac{4}{14{,}400}\}.$$

One easily checks that $V_0 \subset W$. Applying Lemma 10.3, we find that the minimum of C on V_0 is equal to the value of C at one of the points

$$(0, -\tfrac{10}{3}), \ (0, -\tfrac{1}{3}+\tfrac{4}{14{,}400}), \ (\tfrac{1}{8}, -\tfrac{10}{3}), \ (\tfrac{1}{8}, -\tfrac{1}{3}+\tfrac{4}{14{,}400}).$$

These values are computed to be at least 4, so we have $C \geqslant 4$ on V_0. From $c(h_{a,b}) = C(a/\sqrt{q}, b/q)^{1/2}\cdot q^{3/2}$ it now follows that $c(h_{a,b}) \geqslant 2q^{3/2}$ for $(a, b) \in X_0$, as asserted.

We next study the map $X_0 \to \mathbb{Z}$ sending (a, b) to $h_{a,b}(1)$. Since Z_1 consists of

$q+1$ consecutive integers, one shows, as in the proof of Proposition 2.4(b), that this map induces a bijection of X_1 with the set of integers in the interval

$$I = [(q+1)^2 - a_1(q+1) + b_1 - q, (q+1)^2 + a_1(q+1) + b_1].$$

Since one has $h_{a,b}(1) = h_{a+1,b+q+1}(1)$, the map also induces bijections $X_2 \to I \cap \mathbb{Z}$ and $X_3 \to I \cap \mathbb{Z}$.

The inequalities (10.9) and $\sqrt{q} \geqslant 120$ imply that I contains the interval $[q^2 - \frac{1}{9}q^{3/2}, q^2 + \frac{1}{9}q^{3/2}]$. Hence for each integer z in the latter interval there are three pairs $(a, b) \in X_0$ for which $h_{a,b}(1) = z$, and these three pairs take the form

$$(a'-1, b'-q-1), \quad (a', b'), \quad (a'+1, b'+q+1).$$

As we proved above, all these $h_{a,b}$ satisfy $c(h_{a,b}) \geqslant 2q^{3/2}$.

It remains to consider the values z for which none of the corresponding polynomials $h_{a,b}$ is ordinary and regular. For such z, each of the three pairs $(a, b) \in X_0$ with $h_{a,b}(1) = z$ satisfies at least one of the following conditions:

(10.10) b is divisible by p,

(10.11) $a^2 - 4b$ is an integer square,

(10.12) $(b+4q)^2 - 4qa^2$ is an integer square, and $a \neq 0$,

(10.13) $a = 0$.

To finish the proof of Proposition 2.4(a) it suffices to show that there are at most $28\sqrt{q}$ values of z with this property.

Since p is an odd prime dividing q, at most one of the three integers $b'-q-1$, b' and $b'+q+1$ is divisible by p, for any integer b'. Hence for each z at most one of the pairs (a, b) satisfies (10.10).

Lemma 10.8 implies that for each z with fewer than $6\sqrt{q}+11$ exceptions, at most one pair (a, b) satisfies (10.11).

By Lemma 10.2, for each z with at most $14\sqrt{q}$ exceptions, it is true that not a single pair (a, b) satisfies (10.12).

Since at most one of $a'-1$, a', $a'+1$ equals 0, there is for each z at most one pair (a, b) satisfying (10.13).

We conclude that the only problematic values of z are those for which one of the corresponding pairs $(a'-1, b'-q-1)$, (a', b'), $(a'+1, b'+q+1)$ satisfies (10.10), another one satisfies (10.11), and the remaining one satisfies (10.13). We shall show that this occurs for at most $\frac{22}{3}\sqrt{q}$ values of z. This will finish the proof of Proposition 2.4(a), since we have $6\sqrt{q} + 11 + 14\sqrt{q} + \frac{22}{3}\sqrt{q} \leqslant 28\sqrt{q}$.

Let z, a' and b' have the properties just described. Since one of $a'-1$, a', $a'+1$ equals 0, we have $|a'| \leqslant 1$. Then for each of the other two pairs (a, b) we have $a \in \{-2, -1, 1, 2\}$. Let now (a, b) be the pair that satisfies (10.11), so that $a^2 - 4b = d^2$ for some integer $d \geqslant 0$. The inequality $-\frac{10}{3}q + 1 \leqslant b < 0$ that is valid in X_0 implies that $0 < d^2 \leqslant \frac{40}{3}q$; so the number of possibilities for d is at most $\sqrt{40q/3}$, which is less than $\frac{11}{3}\sqrt{q}$. Once we know d, the value for a is determined up to sign by the conditions $a \in \{-2, -1, 1, 2\}$ and $a \equiv d \bmod 2$, and the value for b is determined by $b = \frac{1}{4}(a^2 - d^2)$. That gives at most $\frac{22}{3}\sqrt{q}$ pairs (a, b), and consequently at most $\frac{22}{3}\sqrt{q}$ values for $z = h_{a,b}(1)$, as required.

This completes the proof of Proposition 2.4(a).

11. *Characteristic* 2

Our main theorems exclude fields of characteristic 2, not only because they make assertions about models of the form $y^2 = f(x)$ for hyperelliptic curves, but also because our result on the map from the set of Weil polynomials to $\mathbb{Z}$ admits a larger exceptional set in characteristic 2. Here we state a result about isomorphism classes of curves valid in characteristic 2. We begin with a suitable replacement for Proposition 2.4.

PROPOSITION 11.1. *Let $q \geqslant 14{,}400$ be a power of 2. Then for all but at most $\frac{10}{9}q$ integers z in the interval*

$$[q^2 - \tfrac{1}{9}q^{3/2}, q^2 + \tfrac{1}{9}q^{3/2}]$$

there is an ordinary regular Weil q-polynomial h of degree 4 with $c(h) \geqslant 2q^{3/2}$ and $h(1) = z$.

Proof. Let $q \geqslant 14{,}400$ be a power of 2. Define a_1, X_1, X_2 and X_0 as in the proof of Proposition 2.4(a), and put

$$X_4 = X_1 \cup X_2.$$

As in the proof of Proposition 2.4(a), one deduces from $q \geqslant 14{,}400$ that for each integer z in the interval $[q^2 - \frac{1}{9}q^{3/2}, q^2 + \frac{1}{9}q^{3/2}]$ there are two pairs $(a, b) \in X_4$ such that $h_{a,b}(1) = z$, and that these two pairs take the form

$$(a', b'), \quad (a' + 1, b' + q + 1).$$

Precisely one of b', $b' + q + 1$ is odd. Therefore for each z in the target interval there is a unique $(a, b) \in X_4$ such that $h_{a,b}$ is ordinary and $h_{a,b}(1) = z$.

The inequality $c(h_{a,b}) \geqslant 2q^{3/2}$ holds for all $(a, b) \in X_4$, by the same computation as in the proof of Proposition 2.4(a), since $X_4 \subset X_0$.

It remains to estimate the number of integers z for which the corresponding polynomial $h_{a,b}$ is not regular. This is at most the number of pairs $(a, b) \in X_4$ with b odd that satisfy one of the following conditions:

(11.2) $a^2 - 4b$ is an integer square,

(11.3) $(b + 4q)^2 - 4qa^2$ is an integer square, $a \neq 0$, and $a^2 - 4b \neq 0$,

(11.4) $a = 0$.

It suffices to show that there are at most $\frac{10}{9}q$ such pairs.

Let (a, b) be a pair satisfying (11.2), so that $a^2 - 4b = d^2$ for a non-negative integer d. Since b is odd, we have $d \equiv 0 \bmod 2$ and $a \equiv d + 2 \bmod 4$. From $(a, b) \in X_4$ one deduces that

$$\tfrac{4}{3}q - 16 \leqslant d^2 \leqslant \tfrac{1795}{192}q - 8.$$

It follows that $\frac{23}{20}\sqrt{q} \leqslant d < \frac{31}{10}\sqrt{q}$; so d belongs to an interval of length at most $2(\sqrt{q} - 1)$. Since d is even, this leaves at most $\sqrt{q}$ possible values for d. For given d, the value of a is restricted by $-a_1 \leqslant a \leqslant a_1 + 1$ and $a \equiv d + 2 \bmod 4$; the number of possibilities for a is therefore at most $\frac{1}{4}(2a_1 + 4)$, which is at most $\frac{1}{16}\sqrt{q} + \frac{1}{2}$. Since a and d determine b, we conclude that the number of pairs $(a, b) \in X_4$ with b odd for which (11.2) holds is at most $\sqrt{q} \cdot (\frac{1}{16}\sqrt{q} + \frac{1}{2})$, which equals $\frac{1}{16}q + \frac{1}{2}\sqrt{q}$.

By Lemma 10.2(b), (c), there are fewer than $4\sqrt{q}+2$ pairs $(a, b) \in X_4$ with b odd for which (11.3) holds.

Finally, the number of pairs satisfying (11.4) is the number of possible values for b that are odd, which equals $q+1$.

The total number of z that must be excluded is therefore less than $\frac{1}{16}q + \frac{1}{2}\sqrt{q} + 4\sqrt{q} + 2 + q + 1 \leqslant \frac{10}{9}q$. This completes the proof of Proposition 11.1.

THEOREM 11.5. *Suppose that $q \geqslant 14{,}400$ is a power of 2, and that k is a finite field of cardinality q. Then for all but at most $\frac{10}{9}q$ integers z in the interval*

$$[q^2 - \tfrac{1}{9}q^{3/2}, q^2 + \tfrac{1}{9}q^{3/2}],$$

the weighted number of curves C of genus 2 over k with $\#J_C(k) = z$ is at least

$$\frac{q^{3/2}}{47{,}500 \cdot (\log q)^2 \cdot (\log\log q)^2};$$

here the isomorphism class of C is counted with weight $1/\#\mathrm{Aut}\, C$.

Proof. Combine Proposition 11.1, Proposition 2.3 and Proposition 2.2. This proves Theorem 11.5.

References

1. L. M. ADLEMAN and M.-D. A. HUANG, *Primality testing and Abelian varieties over finite fields*, Lecture Notes in Mathematics 1512 (Springer, Berlin, 1992).
2. M. F. ATIYAH and I. G. MACDONALD, *Introduction to commutative algebra* (Addison-Wesley, Reading, MA, 1969).
3. G. CORNELL and J. H. SILVERMAN (eds), *Arithmetic geometry* (Springer, New York, 1986).
4. P. DELIGNE, 'Variétés abéliennes ordinaires sur un corps fini', *Invent. Math.* 8 (1969) 238–243.
5. G. H. HARDY and E. M. WRIGHT, *An introduction to the theory of numbers*, 5th edn (Oxford University Press, 1979).
6. E. W. HOWE, 'Principally polarized ordinary Abelian varieties over finite fields', *Trans. Amer. Math. Soc.* 347 (1995) 2361–2401.
7. S. LANG, *Algebraic number theory*, 2nd edn (Springer, New York, 1994).
8. H. W. LENSTRA JR, 'Factoring integers with elliptic curves', *Ann. of Math.* 126 (1987) 649–673.
9. H. W. LENSTRA JR, J. PILA and C. POMERANCE, 'A hyperelliptic smoothness test, I', *Philos. Trans. Roy. Soc. London Ser. A* 345 (1993) 397–408.
10. S. LOUBOUTIN, 'Explicit bounds for residues of Dedekind zeta functions, values of L-functions at $s = 1$, and relative class numbers', *J. Number Theory* 85 (2000) 263–282.
11. J. S. MILNE, 'Abelian varieties', [**3**, pp. 103–150].
12. J. S. MILNE, 'Jacobian varieties', [**3**, pp. 167–212].
13. J. B. ROSSER and L. SCHOENFELD, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* 6 (1962) 64–94.
14. H.-G. RÜCK, 'Abelian surfaces and Jacobian varieties over finite fields', *Compositio Math.* 76 (1990) 351–366.
15. J. W. SANDS, 'Generalization of a theorem of Siegel', *Acta Arith.* 58 (1991) 47–57.
16. J.-P. SERRE, *Corps locaux* (Hermann, Paris, 1962).
17. J.-P. SERRE, 'Zeta and L functions', *Arithmetical algebraic geometry* (ed. O. F. G. Schilling, Harper and Row, New York, 1965) 82–92; *Œuvres*, Vol. II (Springer, Berlin, 1986) 249–259.
18. C. L. SIEGEL, 'Abschätzung von Einheiten', *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl.* (1969) 71–86; *Gesammelte Abhandlungen*, Vol. IV (Springer, Berlin, 1979) 66–81.
19. H. M. STARK, 'Some effective cases of the Brauer–Siegel theorem', *Invent. Math.* 23 (1974) 135–152.
20. H. STICHTENOTH, *Algebraic function fields and codes* (Springer, Berlin, 1993).
21. J. TATE, 'Endomorphisms of Abelian varieties over finite fields', *Invent. Math.* 2 (1966) 134–144.
22. A. WEIL, *Variétés abéliennes et courbes algébriques* (Hermann, Paris, 1948).

23. A. WEIL, 'Zum Beweis des Torellischen Satzes', *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* (1957) 33–53; *Œuvres scientifiques*, Vol. II (Springer, New York, 1979) 307–327.
24. E. T. WHITTAKER and G. N. WATSON, *A course of modern analysis*, 4th edn (Cambridge University Press, 1927).

H. W. Lenstra Jr
Department of Mathematics #3840
University of California
Berkeley
CA 94720–3840
USA
hwl@math.berkeley.edu

and

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 *RA Leiden*
The Netherlands
hwl@math.leidenuniv.nl

J. Pila
Department of Mathematics
University of Melbourne
Parkville 3052
Australia
pila@ms.unimelb.edu.au
Mail address:
6 *Goldthorns Avenue*
Kew 3101
Australia

Carl Pomerance
Bell Laboratories – Lucent Technologies
600 *Mountain Avenue*
Murray Hill
NJ 07974
USA
carlp@research.bell-labs.com