The Refined Humbert Invariant for Abelian Product Surfaces with Complex Multiplication

Ernst Kani

1 Introduction

The *refined Humbert invariant* is a positive quadratic form $q_{(A,\theta)}$ which is intrinsically attached to a principally polarized abelian surface $(A,\theta) \in \mathcal{A}_2(K)$, where K is an algebraically closed field; cf. [K1], [K3] and §6 below. This invariant is closely related to Humbert's invariant [Hu], as was explained in [K1].

It is of considerable interest to classify the quadratic forms which are equivalent to some refined Humbert invariant $q_{(A,\theta)}$. In the case that A is isogenous to a product $E \times E$, where E is an elliptic curve with $\mathrm{End}(E) = \mathbb{Z}$, such a classification was given in Theorems 1 and 3 of [K5].

The purpose of this article is to give a similar classification in the case that A is isogenous to $E \times E$, where E is a complex multiplication curve, and $q_{(A,\theta)}$ is a primitive form.

To this end, let us consider positive ternary forms $f(x,y,z)$ satisfying the following two conditions.

$$(1) \qquad f(x,y,z) \equiv 0 \text{ or } 1 \pmod 4, \quad \text{for all } x,y,z \in \mathbb{Z};$$

$$(2) \qquad f(x_0,y_0,z_0) = n^2, \text{ for some } x_0,y_0,z_0,n \in \mathbb{Z} \text{ with } \gcd(n,\mathrm{disc}(f)) = 1.$$

Note these conditions are very similar to those characterizing the refined Humbert invariant in the non-CM case which was studied in [K5]. However, condition (2) is more restrictive because it immediately implies that f is a primitive form.

For the CM-case it was shown in [K4] that $q_{(A,\theta)}$ is *genus-equivalent* to a ternary form $f_q(x,y,z) = x^2 + 4q(y,z)$, where $q(y,z)$ is a positive binary quadratic form which is closely related to the intersection form q_A on A. It is easy to see that any such f_q satisfies conditions (1) and (2), and hence the same is true for $q_{(A,\theta)}$ itself. If $\mathrm{char}(K) = 0$, then the converse holds, as will be shown in this article:

Theorem 1 *Let K be an algebraically closed field of characteristic 0, and let f be a positive, primitive ternary quadratic form. Then the following conditions are equivalent:*

(i) *f satisfies conditions (1) and (2);*

(ii) *f is genus-equivalent to f_q, for some positive binary quadratic form q;*

(iii) *f is equivalent to a form $q_{(A,\theta)}$, for some $(A,\theta) \in \mathcal{A}_2(K)$.*

There is a similar (but more complicated) statement for fields of positive characteristic; see Theorem 28 below. Note also that Theorem 20 below gives further information about the ternary forms satisfying conditions (i) and (ii) of Theorem 1.

It is worthwhile to mention that an analogue of Theorem 1 for ternary forms that are not primitive is given by H. Kir in [Kir].

The following result can be viewed as a partial refinement of Theorems 1 and 28.

Theorem 2 *Let E/K and E'/K be two isogenous elliptic curves with complex multiplication over an algebraically closed field K, and let $q = q_{E,E'}$ denote the* degree form *on* $\mathrm{Hom}(E, E')$ *which is defined by $q_{E,E'}(h) = \deg(h)$, for $h \in \mathrm{Hom}(E, E')$. If f is a quadratic form which is genus-equivalent to f_q, then there exists a principal polarization θ on $A = E \times E'$ such that $q_{(A,\theta)}$ is equivalent to f.*

This theorem has an interesting application, for it can be used to prove a *mass-formula* for the set of isomorphism classes of principal polarizations of (certain) CM abelian product surfaces $A = E \times E'$, as is shown in [K6].

The most interesting (and difficult) part of Theorem 1 is the implication (ii) $\Rightarrow$ (iii), so we sketch its proof here. Given a ternary form f which is genus-equivalent to f_q, where q is some positive binary quadratic form, we first find a binary quadratic form ϕ which is properly represented by the form f and which has a suitable discriminant. For this, we need some facts about the existence of (certain) primes which are represented by a ternary form; these facts are derived in §2.

The next step is to show that ϕ can be chosen to be a primitive form, and this requires a refinement (Proposition 10) of a criterion given in Dickson's book[D].

If ϕ is such a primitive form, then one can show that it lies in the principal genus (see Theorem 22) and that it is in fact a form of the type studied in [K3]. Moreover, one can show that $|\operatorname{disc}(\phi)|/16$ is represented by some form $\tilde{q}$ which is genus-equivalent to q (see Corollary 21). Using these facts, and the constructions of [K3], one can construct a CM abelian product surface $A = E \times E'$ and a principal polarization θ on A such that its refined Humbert invariant $q_{(A,\theta)}$ also properly represents ϕ. This information and the above constructions suffice to conclude in §6 that f is equivalent to $q_{(A,\theta)}$.

Note that the above proof can be made into an algorithm which constructs a principally polarized abelian variety (A, θ) such that $q_{(A,\theta)} \sim f$; see Algorithm 27.

The implication (i) $\Rightarrow$ (ii) of Theorem 1 is somewhat simpler, but uses ideas similar to the implication (ii) $\Rightarrow$ (iii), as can be seen in the proof of Theorem 20 below.

Finally, by using a small trick (see Proposition 29), one can refine the previous argument of the proof of the implication (ii) $\Rightarrow$ (iii) to prove Theorem 2; see §6.

Acknowledgment. I thank Harun Kir for his comments on this paper. In addition, I gratefully acknowledge receipt of funding from the Natural Sciences and Research Council of Canada (NSERC).

2 Prime numbers represented by ternary forms

The following result is a slight sharpening of Dirichlet's celebrated result on the existence of primes represented by positive binary forms; cf. Cox[C], Theorem 9.12.

Theorem 3 *Let $q(x,y) = ax^2 + bxy + cy^2$ be a primitive positive binary quadratic form of discriminant $D = b^2 - 4ac$, and let $D_1 < 0$ be a fundamental discriminant. Suppose that there is a prime divisor of D_1 which does not divide D. Then q represents infinitely many primes p with Legendre symbol $\left(\frac{D_1}{p}\right) = 1$, and q also represents infinitely many primes p' with $\left(\frac{D_1}{p'}\right) = -1$.*

Before proving this result, we observe that the following is a special case of this theorem.

Corollary 4 *If $q(x,y)$ is a primitive positive binary quadratic form whose discriminant is odd, then q represents infinitely many primes $p \equiv 1 \pmod 4$ and q also represents infinitely many primes p' with $p' \equiv 3 \pmod 4$.*

Proof. Apply Theorem 3 with $D_1 = -4$. Since $2|D_1$ but $2 \nmid D$, the assertion follows since $\left(\frac{-4}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4$, and $\left(\frac{-4}{p}\right) = -1 \Leftrightarrow p \equiv 3 \pmod 4$.

Proof of Theorem 3. Let S be the set of primes represented by q, and let L be the ring class field of the ring $\mathcal{O}_D$. By the proof of Theorem 9.12 of Cox[C], there exists $\sigma_f \in \mathrm{Gal}(L/\mathbb{Q})$ such that

$$S \doteq S' := \{p \text{ prime} : p \text{ is unramified in } L \text{ and } \left(\tfrac{L/\mathbb{Q}}{p}\right) = \mathfrak{c}(\sigma_f)\}, \tag{3}$$

where $\mathfrak{c}(\sigma)$ denotes the conjugacy class of an element σ; cf. equation (9.16) in [C].

Next, let $S_1 = \{p \text{ prime} : \left(\frac{D_1}{p}\right) = 1\}$ and $S_2 = \{p \text{ prime} : \left(\frac{D_1}{p}\right) = -1\}$, and put $K_1 = \mathbb{Q}(\sqrt{D_1})$. Since D_1 is a fundamental discriminant, we have that

$$S_k = \{p \text{ prime: } p \text{ is unramified in } K_1 \text{ and } \left(\tfrac{K_1/\mathbb{Q}}{p}\right) = \sigma_k\}, \quad \text{for } k = 1, 2,$$

where $\sigma_1 = 1$ and $\langle \sigma_2 \rangle = \mathrm{Gal}(K_1/\mathbb{Q})$; cf. [C], Proposition 5.16 (and [Ja], Property 2.5 on p. 128).

We observe that $K_1 \not\subset L$. Indeed, since there exists a prime $p|D_1$ with $p \nmid D$, it follows that p is ramified in K_1 but not in $K = \mathbb{Q}(\sqrt{D})$, so there is a prime $\mathfrak{p}|p$ of KK_1 which is ramified over K. But L/K is unramified outside of $f\mathcal{O}_K$, where $D = f^2 d_K$ (cf. [C], p. 196), so $KK_1 \not\subset L$ and hence $K_1 \not\subset L$.

We thus have an isomorphism $\varphi : \mathrm{Gal}(L_1/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(K_1/\mathbb{Q})$, where $L_1 := LK_1$, and hence there exists $\tilde{\sigma}_k \in \mathrm{Gal}(L_1/\mathbb{Q})$ such that $(\tilde{\sigma}_k)_{|L} = \sigma_f$ and

$(\tilde{\sigma}_k)_{|K_1} = \sigma_k$, for $k = 1, 2$. Using Property 2.4 of [Ja], p. 127, of the Artin Symbol, it thus follows from (3) that

(4) $S \cap S_k \doteq \{p \text{ prime} : p \text{ is unramified in } L_1 \text{ and } \left(\frac{L_1/\mathbb{Q}}{p}\right) = \mathfrak{c}(\tilde{\sigma}_k)\}$, for $k = 1, 2$.

By Chebotarev, the set on the right hand side of (4) has a positive Dirichlet density and hence is infinite, and so the assertion follows.

We now apply this result to primitive ternary forms. Here, a primitive (integral) quadratic form f is defined as in Watson[W] (and in Brandt[B1]), i.e.,

$$f(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$$

is said to be *primitive* if $a_{ij} \in \mathbb{Z}$, for all $1 \le i \le j \le n$, and if $\gcd(\{a_{ij}\}_{1 \le i \le j \le n}) = 1$.

Since we also need to use the results of Smith[Sm] and Dickson[D], we recall the older terminology (which was introduced by Gauss). Thus, a quadratic form f is called *properly primitive* if it is primitive (in the above sense) and if $2|a_{ij}$, for all $i < j$. Moreover, a form f is called *improperly primitive* if $\frac{1}{2}f$ is primitive in the above sense and if there exists some pair (i, j) with $i < j$ such that $\frac{1}{2}a_{ij}$ is odd.

We call a form *G-primitive* (i.e., primitive in the sense of Gauss) if it is either properly primitive or improperly primitive. If f is G-primitive, then it has a *reciprocal* quadratic form F_f as defined on p. 7 of [D]. Note that the reciprocal F_f is G-primitive and that its reciprocal is f, (so $F_{F_f} = f$), as is mentioned there.

Notation. Recall that a binary quadratic form ϕ is said to be *properly represented* by a ternary quadratic form f if $\phi = fT$, for some integral 3×2 matrix T whose 2×2 sub-determinants are relatively prime; cf. [D], p. 25. If this the case, then we will write $f \to \phi$.

We now use Dirichlet's theorem and its refinement to prove the following results about primes represented by positive ternary forms.

Proposition 5 *If f and its reciprocal $F = F_f$ are both positive properly primitive ternary forms, then f properly represents some properly primitive binary form ϕ. Thus, f represents infinitely many primes.*

Proof. The first assertion follows from Theorem 17 of [D]. Since ϕ represents infinitely many primes by Dirichlet's theorem (cf. [C], Theorem 9.12), so does f.

Proposition 6 *If f is a positive improperly primitive ternary form, then f properly represents some improperly primitive binary form ϕ. Thus $\frac{1}{2}f$ represents infinitely many primes $p \equiv 1 \pmod 4$ and also infinitely many primes $p' \equiv 3 \pmod 4$.*

Proof. The first assertion follows from Theorem 19 of [D]. Since ϕ is improperly primitive, we see that $\frac{1}{2}\phi$ is a primitive form whose discriminant is odd, and so by Corollary 4 we have that $\frac{1}{2}\phi$ represents infinitely many primes $p \equiv 1 \pmod 4$ and also infinitely many primes $p' \equiv 3 \pmod 4$. Since $\frac{1}{2}f \to \frac{1}{2}\phi$, it follows that the same is true for $\frac{1}{2}f$.

Corollary 7 *If f is a positive properly primitive ternary form whose reciprocal $F = F_f$ is improperly primitive, then $\frac{1}{2}F$ represents infinitely many primes $p \equiv 1 \pmod 4$ and also infinitely many primes $p' \equiv 3 \pmod 4$.*

Proof. Apply Proposition 6 to F in place of f.

Remark 8 In the situation of Corollary 7 it is also true that f represents infinitely many primes, but this is a bit harder to prove; cf. Corollary 12 below.

3 A primitivity criterion

Let f be a positive G-primitive ternary form which properly represents a binary form ϕ, so $f \to \phi$. In his book[D], Dickson gives a criterion which ensures that ϕ is G-primitive. To state this criterion, recall that f comes equipped with two invariants Ω_f and Δ_f; see [D], p. 7. Then by Theorem 37 of [D] we have:

Proposition 9 *If f is a positive G-primitive ternary form and if $f \to \phi$, where $\phi(x,y) = ax^2 + 2txy + by^2$ has discriminant $-4\Omega_f C$ with $\gcd(C, \Omega_f\Delta_f) = 1$, then ϕ is G-primitive.*

The problem with this criterion is that it is not applicable when F_f is improperly primitive because in that case we have that always $2|\gcd(C, \Omega_f\Delta_f)$. The following result addresses this situation.

Proposition 10 *Let f be a positive properly primitive ternary form whose reciprocal F is improperly primitive. If $f \to \phi$, where $\phi(x,y) = ax^2 + 2txy + by^2$ has discriminant $-4\Omega_f C$ with $\gcd(C, 2\Omega_f\Delta_f) = 2$, then $\tau := \gcd(a,t,b)|2$ and $\mathrm{cont}(\phi) := \gcd(a,2t,b) = \tau^2$. Furthermore, if in addition*

$$C \not\equiv \Omega_f + 4 \pmod 8, \tag{5}$$

then ϕ is properly primitive.

Proof. By replacing f by suitable equivalent form we may assume (as in the proof of Theorem 37 of [D]) that $\phi(x,y) = f(x,y,0)$ and that

$$F_f \;=\; Ax^2 + By^2 + Cz^2 + 2Ryz + 2Sxz + 2Txy.$$

Write $f = ax^2 + by^2 + cz^2 + 2ryz + 2sxz + 2txy$. Then we have the relations

$$(6) \quad BC - R^2 = \Delta a, \quad RS - TC = \Delta t, \quad AC - S^2 = \Delta b, \quad \text{and} \quad AB - T^2 = \Delta c,$$

where $\Delta = \Delta_f$; see equations (70) and (77) of Part I of [D]. From these equations Dickson derives the relation

$$(7) \qquad \Delta(Aa + 2Tt + Bb) \;=\; \Omega\Delta^2 + Cc\Delta,$$

where $\Omega = \Omega_f$; see equation (79) of Part I of [D]. Multiplying (7) by $\frac{\Omega}{\Delta}$ and using the fact that $ab - t^2 = -\operatorname{disc}(\phi)/4 = \Omega C$ yields the relation

$$(8) \qquad \Omega(Aa + 2Tt + Bb) \;=\; \Omega^2\Delta + c(ab - t^2).$$

From this we see that $\tau = \gcd(a, b, t) \mid \Omega^2\Delta$. Since $\tau \mid (ab - t^2) = \Omega C$, it follows that $\tau \mid \gcd(\Omega^2\Delta, \Omega C) = \Omega \gcd(\Omega\Delta, C) \mid \Omega \gcd(2\Omega\Delta, C) = 2\Omega$ by our hypothesis.

We next show that $\tau \mid \Omega$. For this we note that $2 \mid \Omega$ (and $2 \nmid \Delta$) because F_f is improperly primitive. (This follows either from [Sm], p. 459 or from [B2], p. 316 because we are in Case III here.) Thus, $C' := \frac{C}{2}$ is odd because $\gcd(C', \Omega\Delta) = 1$. Suppose that $2^r || \tau$ and $2^s || \Omega$. Then $2^{2r} | (ab - t^2) = 2\Omega C'$, so $2r \leq s + 1$ and hence $r \leq s$, and so $\tau \mid \Omega$. This implies that $\gcd(\tau, C') = 1$.

Put $\tau' := \frac{\tau}{\gcd(2,\tau)}$, so $\tau' | \frac{\Omega}{2}$. From (7) we obtain the relation

$$(9) \qquad \frac{A}{2}a + Tt + \frac{B}{2}b \;=\; \frac{\Omega}{2}\Delta + C'c.$$

Since $2|A$ and $2|B$ (because F_f is improperly primitive), this implies that $\tau' \mid c$.

Next we observe that the following relations hold:

$$(10) \qquad aS + tR + sC \;=\; 0 \quad \text{and} \quad tS + bR + rC \;=\; 0;$$

see [D], p. 33. Since $\tau|a$ and $\tau|t$, we see that $\tau|sC = 2sC'$, and so $\tau|2s$ and $\tau'|s$. Similarly, we obtain that $\tau|rC = 2rC'$, and so $\tau'|r$. Thus, $\tau' | \gcd(a, b, t, c, s, r) = 1$ because f is G-primitive, so $\tau|2$. This proves the first assertion.

To prove the second assertion, note first that clearly $\operatorname{cont}(\phi)|2\tau$. Consider first the case that $\tau = 1$ and suppose that $2|a$ and $2|b$. Since $2|\Omega$ and $2|C$, we see that $t^2 = ab - \Omega C \equiv 0 \pmod 4$, so $2|t$ and hence $2|\tau$, contradiction. Thus either $2 \nmid a$ or $2 \nmid b$, so $2 \nmid \gcd(a, 2t, b)$ and hence $\operatorname{cont}(\phi) = 1 = \tau^2$ in this case.

Next, suppose that $\tau = 2$, so $2|a$, $2|b$ and $2|t$. Thus, since $2|B$ and $2|C$, we have by (6) that $\Delta a = BC - R^2 \equiv -R^2 \pmod 4$, so $R \equiv 0 \pmod 2$ and $a \equiv 0 \pmod 4$ because $2 \nmid \Delta$. Similarly, since $2|A$ and $2|C$, we obtain that $S \equiv 0 \pmod 2$ and $b \equiv 0 \pmod 4$. Thus, $4 | \gcd(a, 2t, b) | 2\tau = 4$, and so $\operatorname{cont}(\phi) = 4 = \tau^2$. This proves the second assertion.

Now assume that (5) holds, and suppose that $\tau = 2$. Then by what was shown above we know that $4|a$ and $4|b$. This implies that $t \equiv 2 \pmod 4$ because otherwise $4|\tau$. Moreover, we have that $T \equiv 1 \pmod 2$ because F_f is improperly primitive and $2|R$ and $2|S$. Thus, since $aA \equiv bB \equiv 0 \pmod 8$ and $2Tt \equiv 4 \pmod 8$, and $2 \nmid \Delta$, we obtain that $\Delta(Aa + 2Tt + Bb) \equiv 4 \pmod 8$.

Next, by (6) we see that $\Delta c = AB - T^2 \equiv -T^2 \equiv -1 \pmod 4$, so $2\Delta c \equiv -2 \pmod 8$, and hence $\Omega\Delta^2 + Cc\Delta \equiv \Omega + C'2c\Delta \equiv \Omega - 2C' \pmod 8$. Thus, by the above and (7) we obtain that $\Omega - C \equiv 4 \pmod 8$, which contradicts the hypothesis (5). Thus, $\tau = 1$, and hence ϕ is properly primitive because we also have that $\mathrm{cont}(\phi) = 1$.

As an application of the results so far, we can now prove that a properly primitive ternary form f always properly represents primitive binary forms of a certain type.

To avoid case distinctions, it is useful to use the invariants $I_1(f)$ and $I_2(f)$ introduced by Brandt[B1], [B2]. In addition, we will use the reciprocal of f as defined by Brandt; this is denoted by F_f^B. These invariants are related to those of Dickson[D] and Smith[Sm] by the following rules. If f is a positive, properly primitive ternary form, then

$$I_1(f) = -4\Omega_f, \quad I_2(f) = -4\Delta_f \quad \text{and} \quad F_f^B = F_f, \tag{11}$$

if the reciprocal F_f of f is properly primitive, whereas

$$I_1(f) = -8\Omega_f, \quad I_2(f) = -\Delta_f \quad \text{and} \quad F_f^B = F_f/2, \tag{12}$$

if F_f is improperly primitive. Note that the first case is Case II of Brandt[B2], and the second case is Case III of [B2], and that the relations (11) and (12) are given on p. 316 of [B2].

Theorem 11 *If f is a positive properly primitive ternary form, then there exist infinitely many primes $p \nmid I_1(f)I_2(f)$ which are represented by F_f^B such that $f \to \phi_p$, where ϕ_p is a G-primitive binary quadratic form of discriminant $I_1(f)p$. Moreover, if $8|I_1(f)$, then ϕ_p is properly primitive.*

Proof. Suppose first that the reciprocal $F = F_f$ is properly primitive, so $F = F_f^B$. Then by Proposition 5 (applied to F, with reciprocal $f = F_F$), we know that F represents infinitely many primes p with $p \nmid I_1(f)I_2(f) = 16\Omega_f\Delta_f$. For any such p we have by Theorem 38 of [D] that there is a binary form $\phi_p = ax^2 + 2txy + by^2$ with $t^2 - ab = -\Omega_f p$ which is properly represented by f, and by Proposition 9 we know that ϕ_p is G-primitive. This proves the first assertion in this case because $\mathrm{disc}(\phi) = (2t)^2 - 4ab = -4\Omega_f p = I_1(f)p$ by (11).

Moreover, if $8|I_1(f)$, then $2|\Omega_f$ by (11), so ϕ_p is properly primitive because otherwise we would have that $-\Omega_f p = t^2 - ab \equiv 1 \pmod 4$, contradiction.

Now suppose that F is improperly primitive, so $2|\Omega_f$, as was mentioned in the proof of Proposition 10. Then by Corollary 7 there exist infinitely many primes p represented by $\frac{1}{2}F = F_f^B$ such that $p \nmid I_1(f)I_2(f) = 8\Omega_f\Delta_f$ and also such that $p \not\equiv \frac{\Omega_f}{2} + 2 \pmod 4$. For any such p we have that $C = 2p$ is properly represented by F, so by Theorem 38 of [D] there is a binary form $\phi_p = ax^2 + 2txy + by^2$ with $t^2 - ab = -\Omega_f C$ which is properly represented by f. Since $\gcd(2\Omega_f\Delta_f, C) = 2$ and $C \not\equiv \Omega_f + 4 \pmod 8$, we can conclude from Proposition 10 that ϕ_p is properly primitive. Since $\mathrm{disc}(\phi_p) = -4\Omega_f C = -8\Omega_f p = I_1(f)p$, this proves the assertion in all cases.

Corollary 12 *If f is a primitive positive ternary quadratic form, then f represents infinitely many primes.*

Proof. Suppose first that f is properly primitive. If F_f is also properly primitive, then the assertion follows from Proposition 5. If F_f is improperly primitive, then $8|I_1(f)$ by (12), and so by Theorem 11 we see that $f \to \phi$, where ϕ is a properly primitive binary quadratic form. Since ϕ represents infinitely many primes by Dirichlet's theorem (cf. [C], Theorem 9.12), so does f.

If f is not properly primitive, then $g := 2f$ is an improperly primitive form, and then $f = \frac{1}{2}g$ represents infinitely many primes by Proposition 6.

4 Special ternary quadratic forms

In this section we study properties of primitive positive ternary quadratic forms f satisfying properties (1) and (2) of the introduction; these will be called *special ternary quadratic forms.*

Proposition 13 *If f is a positive primitive ternary quadratic form which satisfies property (1), then f is a properly primitive form. Moreover, we have that*

$$I_1(f) \equiv 0 \pmod{16} \quad \textit{and} \quad I_2(f) \equiv 0 \textit{ or } 1 \pmod 4. \tag{13}$$

Thus $\mathrm{disc}(f) = 16d$, *where* $d < 0$ *and* $d \equiv 0, 1 \pmod 4$.

Proof. By hypothesis, $f(x, y, z) = ax^2 + by^2 + cz^2 + ryz + sxz + txy$, where a, b, c, r, s, t are integers with $\gcd(a, b, c, r, s, t) = 1$.

Consider the binary quadratic form $q(x, y) = f(x, y, 0) = ax^2 + txy + by^2$. Since f satisfies (1), $q(x, y) \equiv 0, 1 \pmod 4$, for all $x, y \in \mathbb{Z}$, and so by Corollary 6 of [K5] we know that $\mathrm{disc}(q) = t^2 - 4ac \equiv 0 \pmod{16}$. This shows that $2|t$. Similarly, by considering the quadratic forms $f(x, 0, z)$ and $f(0, y, z)$ we see that $2|s$ and $2|r$, and so f is properly primitive.

Let F be the reciprocal of f. Then we have two cases:

Case 1: F is improperly primitive.

Here we are in Case III of Brandt[B2], so $16|I_1(f)$ and $I_2(f) = -\Delta_f$ is odd; cf. [B2], p. 316. Since f is properly primitive, we have that one of a, b or c is odd, so f represents an odd number x. Since f satisfies property (1), it follows that $x \equiv 1 \,(\mathrm{mod}\ 4)$. Since Case III is the same as Case C of Smith[Sm], we have by the relation listed in Table I, part C, on p. 459 of [Sm] that

$$(-1)^{(\Delta_f - 1)/2} \;=\; -(-1)^{(x-1)/2} \;=\; -1.$$

Thus, $\Delta_f \equiv 3 \,(\mathrm{mod}\ 4)$ and hence $I_2(f) = -\Delta_f \equiv 1 \,(\mathrm{mod}\ 4)$, which shows that (13) holds in this case.

Case 2: F is properly primitive.

By (11) we have that $I_2(f) = -4\Delta_f \equiv 0 \,(\mathrm{mod}\ 4)$, so it remains to show that $16|I_1(f) = -4\Omega_f$.

Now since F is properly primitive, F represents an odd number C. Thus, by Theorem 38 of [D] there exists a binary form ϕ of discriminant $-4\Omega_f C = I_1(f)C$ which is properly represented by f. Thus, $\phi(x, y) \equiv 0, 1 \,(\mathrm{mod}\ 4)$, for all $x, y \in \mathbb{Z}$, because f satisfies (1). By Corollary 6 of [K5] we thus have that $16|\operatorname{disc}(\phi) = I_1(f)C$, so $16|I_1(f)$, and hence (13) holds in both cases.

To prove the last assertion, note that $16 \operatorname{disc}(f) = I_1(f)^2 I_2(f)$; cf. [B2], p. 316. Thus, if we put $t := I_1(f)/16$, then $\operatorname{disc}(f) = 16t^2 I_2(f)$, and so the assertion follows from (13) with $d = t^2 I_2(f)$ because $t \in \mathbb{Z}$.

We next observe that properties (1) and (2) are shared by all forms f in the genus $\mathrm{gen}(g)$ of f, if g is a special form. The condition $f \in \mathrm{gen}(g)$ means that f is *semi-equivalent* to g in the terminology of Watson[W], p. 72. Other equivalent definitions of genus equivalence are given in [Jo], p. 107. In particular, f is genus-equivalent to g if and only if f is *p-adically equivalent* to g (notation: $f \sim_p g$), for all primes p and for $p = \infty$. The latter was the definition used in [K4].

To prove the above assertion, we note the following (well-known) result concerning the set $R(f) = \{f(x, y, z) : x, y, z \in \mathbb{Z}\}$ of values represented by f.

Proposition 14 *Let $f \in \mathrm{gen}(g)$, where g is an integral quadratic form. Then for every integer $d \geq 1$ there exists an integer $n = n(d)$ with $\gcd(n, d) = 1$ such that*

$$n^2 R(f) \;\subset\; R(g). \tag{14}$$

Proof. As in Watson[W], p. 2, let $A(f)$ be the $r \times r$ matrix associated to $f(x_1, \ldots, x_r)$, so $f(x_1, \ldots, x_r) = \frac{1}{2} x^t A(f) x$, if $x = (x_1, \ldots, x_r)^t$.

Since $f \in \mathrm{gen}(g)$, we have by Theorem 50 of [W] that there exists $T \in \mathrm{GL}_r(\mathbb{Q})$ with $\det(T) = \pm 1$ such that

$$T^t A(g) T \;=\; A(f). \tag{15}$$

Moreover, T can be chosen in such a way that its denominator n is prime to a given d. Put $S = nT \in M_r(\mathbb{Z})$. Then $S^t A(g) S = n^2 A(f)$.

Thus, if $m \in R(f)$, then there exists $x \in \mathbb{Z}^r$ such that $m = \frac{1}{2} x^t A(f) x$, and hence by(15) we obtain that $n^2 m = \frac{1}{2} x^t n T^t A(g) T n x = \frac{1}{2}(Sx)^t A(g)(Sx)$. Since $Sx \in \mathbb{Z}^r$, we see that $n^2 m \in R(g)$, and so (14) follows.

Corollary 15 *Let g be an integral ternary form, and let $f \in \mathrm{gen}(g)$. Then f satisfies property* (1) *if and only if g satisfies property* (1)*. Similarly, f satisfies property* (2) *if and only if g satisfies property* (2)*.*

Proof. Suppose first that g satisfies (1). By Proposition 14 with $d = 2$ we see that there exists an odd n such that (14) holds. Let $m \in R(f)$. Then $n^2 m \in R(g)$, so $n^2 m \equiv 0, 1 \pmod 4$, and hence $m \equiv 0, 1 \pmod 4$. Thus f satisfies (1).

Conversely, if f satisfies (1), then a similar argument with f and g interchanged shows that also g satisfies (1). (Note that $f \in \mathrm{gen}(g)$ if and only if $g \in \mathrm{gen}(f)$.)

Next, suppose that f satisfies (2), so there exists $m^2 \in R(f)$ with $\gcd(m, \mathrm{disc}(f)) = 1$. By Proposition 14 with $d = \mathrm{disc}(f)$ we see that there exists an integer $n \geq 1$ with $\gcd(n, \mathrm{disc}(f)) = 1$ such that (14) holds. Then $(nm)^2 \in R(g)$ and $\gcd(nm, \mathrm{disc}(f)) = 1$. Since $\mathrm{disc}(f) = \mathrm{disc}(g)$, we see that g satisfies property (2).

Conversely, if g satisfies (2), then a similar argument with f and g interchanged shows that also f satisfies (2).

Recall from the work of Smith[Sm], §12, that the genus equivalence of two positive ternary forms f_1 and f_2 can be tested by comparing the values of the *assigned characters* of f_1 and F_{f_1} with those of f_2 and F_{f_2}, respectively. This generalizes the genus theory of Gauss for positive binary quadratic forms.

It turns out that there is a close relation between the assigned characters of ternary forms and those of binary forms. More precisely, we have:

Proposition 16 *Let f be a positive primitive ternary quadratic form which satisfies property* (1)*, and let ϕ_1 be a positive primitive binary quadratic form with* $\mathrm{disc}(\phi_1) = I_1(f)$*. Then f and ϕ_1 have the same assigned characters, i.e., $X(f) = X(\phi_1)$. Similarly, if ϕ_2 is a primitive binary form with* $\mathrm{disc}(\phi_2) = I_2(f)$*, then F_f and ϕ_2 have the same assigned characters, so $X(F_f^B) = X(\phi_2)$.*

Proof. Since $16 | I_1(f)$ by (13), we know by Brandt[B1], §19, that χ_{-4} is an assigned character, where, as in [B1], $\chi_{-4}(x) = \left(\frac{-4}{x}\right) = (-1)^{(x-1)/2}$, if x is odd. Moreover,

if $32|I_1(f)$, then by [B1], loc. cit., we know that also χ_8 is an assigned character, where $\chi_8(x) = \left(\frac{8}{x}\right) = (-1)^{(x^2-1)/8}$. Furthermore, for any odd prime $\ell|I_1(f)$, we know that $\chi_\ell = \left(\frac{\cdot}{\ell}\right)$ is an assigned character of f. Thus $X(f) = \{\chi_{-4}, \chi_8, \chi_\ell : \ell|I_1(f), \ell \neq 2 \text{ prime}\}$, if $I_1(f) \equiv 0 \,(\mathrm{mod}\ 32)$, and $X(f) = \{\chi_{-4}, \chi_\ell : \ell|I_1(f), \ell \neq 2 \text{ prime}\}$, if $I_1(f) \equiv 16 \,(\mathrm{mod}\ 32)$. But these are precisely the assigned characters for a primitive binary form with discriminant $I_1(f)$; cf. Cox [C], p. 55, who writes $\delta = \chi_{-4}$ and $\varepsilon = \chi_8$. This proves the first assertion.

To prove the second assertion, suppose first that $I_2(f)$ is odd. Then by Brandt[B1], §19, we have that $X(F_f^B) = \{\chi_\ell : \ell|I_2(f)\} = X(\phi_2)$.

Now suppose that $I_2(f)$ is even. Then by Proposition 13 we are in Case II of Brandt[B1], so $F_f^B = F_f$ and $I_2(f) = -4\Delta_f$; cf. equation (11).

Since $\Delta := \Delta_f = -\frac{I_2(f)}{4}$, the assigned characters of $F = F_f$ are the χ_ℓ's with $\ell|I_2(f)$, $\ell > 2$ prime, together with the "supplementary characters" of F at 2 which are given in Smith's table ([Sm], p. 458). Since $\Omega_f = -I_1(f)/4 \equiv 0 \,(\mathrm{mod}\ 4)$, only the last 2 columns of Smith's table are relevant.

To analyze the entries of this table, recall from what proven above that χ_{-4} is always an assigned character of f. This implies that $\chi_{-4}(f) := \chi_{-4}(n)$ has the same value for every odd n which is represented by f. But since f satisfies condition (1), this means that any such n is $\equiv 1 \,(\mathrm{mod}\ 4)$, so $\chi_{-4}(f) = 1$.

Now in Smith's table there are characters which exist only if a certain condition * or † holds. More precisely, the condition * holds if $\chi_{-4}(f) = \chi_{-4}(\Delta')$, where Δ' denotes the odd part of Δ, and condition † holds if $\chi_{-4}(f) = -\chi_{-4}(\Delta')$. Now since $\chi_{-4}(f) = 1$, the condition * reduces to $\chi_{-4}(\Delta') = 1$, i.e., the condition * means that $\Delta' \equiv 1 \,(\mathrm{mod}\ 4)$. Similarly, the condition † means here that $\Delta' \equiv 3 \,(\mathrm{mod}\ 4)$.

Suppose first that $\Omega := \Omega_f \equiv 4 \,(\mathrm{mod}\ 8)$. Then by using the information given in the 3rd column of Smith's table, we obtain the following assigned characters of F:

(16)

Condition	Assigned character	Reason
$\Delta \equiv 1 \,(\mathrm{mod}\ 4)$	χ_{-4}	$\Delta' = \Delta \equiv 1 \,(\mathrm{mod}\ 4)$
$\Delta \equiv 3 \,(\mathrm{mod}\ 4)$	$-$	
$\Delta \equiv 2 \,(\mathrm{mod}\ 8)$	$\chi_{-4}\chi_8$	$\Delta' = \frac{\Delta}{2} \equiv 1 \,(\mathrm{mod}\ 4)$
$\Delta \equiv 6 \,(\mathrm{mod}\ 8)$	χ_8	$\Delta' = \frac{\Delta}{2} \equiv 3 \,(\mathrm{mod}\ 4)$
$\Delta \equiv 4 \,(\mathrm{mod}\ 8)$	χ_{-4}	
$\Delta \equiv 0 \,(\mathrm{mod}\ 8)$	χ_{-4}, χ_8	

Similarly, if $\Omega \equiv 0 \,(\mathrm{mod}\ 8)$, then by looking at the 4th column of Smith's table we get *exactly* the same list for the assigned characters of F.

Since $\frac{-I_2(f)}{4} = \Delta$, we see that the above list is exactly the same as the list of supplementary characters of ϕ_2; cf. [C], p. 55. We thus have in all cases that $X(\phi_2) = X(F)$, where $X(F)$ denotes the list of assigned characters which are associated to F. This proves the second assertion.

A key feature of an assigned character $\chi \in X(f)$ is that $\chi(n_1) = \chi(n_2)$, for all $n_i \in R(f)$ with $\gcd(n_i, I_1(f)) = 1$. This common value is denoted by $\chi(f)$. Similarly, if $\psi \in X(F_f^B)$, then $\psi(m_1) = \psi(m_2)$, for all $m_i \in R(F_f^B)$ with $\gcd(m_i, I_2(f)) = 1$, and this common value is denoted by $\psi(F_f^B)$; see Brandt[B1].

From the proof of the above proposition we can deduce the following useful fact which will be used below.

Corollary 17 *Let f_1 be a positive primitive ternary form satisfying* (1)*, and let $f_2 \in \mathrm{gen}(f_1)$. Put $I_k = I_k(f_1)$, for $k = 1, 2$. If $n_i \in R(f_i)$ with $\gcd(n_i, I_1) = 1$, and if $m_i \in R(F_{f_i}^B)$ with $\gcd(m_i, 2I_2) = 1$, for $i = 1, 2$, then we have that*

$$\left(\frac{I_1}{n_1}\right) = \left(\frac{I_1}{n_2}\right) \quad \text{and} \quad \left(\frac{I_2}{m_1}\right) = \left(\frac{I_2}{m_2}\right). \tag{17}$$

Proof. Since the content of a form is a genus invariant, we see that f_2 is also primitive, and by Corollary 15 we know that f_2 also satisfies (1). Since I_k is a genus invariant, we have that $I_k(f_2) = I_k$, for $k = 1, 2$, so $X(f_1) = X(f_2)$ and $X(F_{f_1}^B) = X(F_{f_2}^B)$.

To prove the identities of (17), we will use the fact that values $\chi(f_i) = \chi(n_i)$ for $\chi \in X(f_1) = X(f_2)$ are genus invariants (cf. [B2]), so $\chi(n_1) = \chi(n_2)$, for all $\chi \in X(f_1)$. Similarly, the values $\psi(F_{f_i}^B) = \psi(m_i)$ for $\psi \in X(F_{f_1}^B) = X(F_{f_2}^B)$ are genus invariants, so $\psi(m_1) = \psi(m_2)$, for all $\psi \in X(F_{f_1}^B)$. Thus, to prove (17), it suffices to show that the $\left(\frac{I_k}{n_i}\right)$'s are products of values of assigned characters.

For this, note first that since n_i is odd, it follows that $n_i \equiv 1 \pmod 4$ because f_i satisfies (1). Thus, if we write $I_1 = -2^r\Omega'$ with $2 \nmid \Omega'$, then by quadratic reciprocity we obtain that

$$\left(\frac{I_1}{n_i}\right) = \left(\frac{-1}{n_i}\right)\left(\frac{2}{n_i}\right)^r\left(\frac{\Omega'}{n_i}\right) = \left(\frac{2}{n_i}\right)^r\left(\frac{n_i}{\Omega'}\right) = \chi_8(n_i)^r\chi_{\Omega'}(n_i), \tag{18}$$

where $\chi_{\Omega'}(n_i) := \left(\frac{n_i}{\Omega'}\right) = \prod_{\ell|\Omega'} \chi_\ell(n_i)^{v_\ell(\Omega')}$.

Since $\{\chi_\ell : \ell|\Omega'\} \subset X(f_i)$, it follows from what was said above that $\chi_{\Omega'}(n_1) = \chi_{\Omega'}(n_2)$. Thus, the first equation of (17) follows from (18), except when $r \equiv 1 \pmod 2$. But if this is the case, then $I_1 \equiv 0 \pmod{32}$ because $r \geq 4$ by (13), and then $\chi_8 \in X(f_i)$ (cf. the proof of Proposition 17). Thus $\chi_8(n_1) = \chi_8(n_2)$, and so the first equation of (17) holds in all cases.

To prove the second formula, write $I_2 = -2^s\Delta'$, where $2 \nmid \Delta'$. Note that in view of (11) and (12), this Δ' is the same as that of (16).

We now prove an analogue of (18). For this, we observe that if $\Delta' \equiv 1 \pmod 4$, then by quadratic reciprocity we have that $\left(\frac{\Delta'}{m_i}\right) = \left(\frac{m_i}{\Delta'}\right)$, and if $\Delta' \equiv 3 \pmod 4$, then $\left(\frac{-\Delta'}{m_i}\right) = \left(\frac{m_i}{\Delta'}\right)$ because $\left(\frac{-\Delta'}{m_i}\right) = \left(\frac{-1}{m_i}\right)\left(\frac{\Delta'}{m_i}\right) = \left(\frac{-1}{m_i}\right)\left(\frac{m_i}{\Delta'}\right)(-1)^{(m_i-1)/2} = \left(\frac{m_i}{\Delta'}\right)$.

Thus:

$$\left(\frac{I_2}{m_i}\right) \;=\; \left(\frac{-1}{m_i}\right)^{\varepsilon}\left(\frac{2}{m_i}\right)^{s}\left(\frac{m_i}{\Delta'}\right) \;=\; \chi_{-4}(m_i)^{\varepsilon}\chi_8(m_i)^s\chi_{\Delta'}(m_i), \tag{19}$$

where $\varepsilon = 1$, if $\Delta' \equiv 1 \,(\mathrm{mod}\ 4)$, and $\varepsilon = 0$, if $\Delta' \equiv 3 \,(\mathrm{mod}\ 4)$.

Since $\{\chi_\ell : \ell | \Delta'\} \subset X(F_{f_i}^B)$, it follows by a similar argument as before that $\chi_{\Delta'}(m_1) = \chi_{\Delta'}(m_2)$, and so it remains to show that $\chi_{-4}(m_1)^{\varepsilon}\chi_8(m_1)^s = \chi_{-4}(m_2)^{\varepsilon}\chi_8(m_2)^s$. For this, we need to distinguish some cases.

If I_2 is odd, then $\Delta' = -I_2 \equiv 3 \mod 4$ by (13), so $\varepsilon = 0$ and $s = 0$, and the assertion is clear. Thus, assume that I_2 is even, so $I_2 = -4\Delta = -2^s\Delta'$. If $\Delta \equiv 3 \,(\mathrm{mod}\ 4)$, then $\varepsilon = 0$ and $s = 2$, in which case the assertion is clear. Suppose next that $\Delta \equiv 1 \,(\mathrm{mod}\ 4)$, so $\varepsilon = 1$ and $s = 2$. Then by (16) we see that $\chi_{-4} \in X(F_{f_i}^B) = X(F_{f_i})$, so $\chi_{-4}(m_1) = \chi_{-4}(m_2)$, and hence the assertion follows in this case because $\chi_{-4}(m_i)^{\varepsilon}\chi_8(m_i)^s = \chi_{-4}(m_i)$, for $i = 1, 2$. If $\Delta \equiv 2 \,(\mathrm{mod}\ 4)$, then $s = 3$ and by (16) we know that $\chi_{-4}^{\varepsilon}\chi_8 \in X(F_{f_i}^B)$, so $\chi_{-4}(m_1)^{\varepsilon}\chi_8(m_1) = \chi_{-4}(m_2)^{\varepsilon}\chi_8(m_2)$, and hence the assertion follows because $\chi_{-4}(m_i)^{\varepsilon}\chi_8(m_i)^s = \chi_{-4}(m_i)^{\varepsilon}\chi_8(m_i)$, for $i = 1, 2$. Finally, if $\Delta \equiv 0 \,(\mathrm{mod}\ 4)$, then $\chi_{-4} \in X(F_{f_i}^B)$ by (16), so the assertion follows provided that s is even. If s is odd, then $\Delta \equiv 0 \,(\mathrm{mod}\ 8)$, and then also $\chi_8 \in X(F_{f_i}^B)$ by (16), and hence the assertion holds in all cases. This proves the second equation of (17).

5 Quadratic forms in $\mathrm{gen}(f_q)$

Let $q(x, y) = ax^2 + bxy + cy^2$ be a positive binary quadratic form. As in [K4], let

$$f_q(x, y, z) \;:=\; x^2 + 4q(y, z) \;=\; x^2 + 4ay^2 + 4byz + 4cz^2,$$

so f_q is a properly primitive positive ternary quadratic form. Moreover, let

$$d := -\operatorname{disc}(q) = 4ac - b^2, \quad t := \operatorname{cont}(q) := \gcd(a, b, c) \quad \text{and} \quad d' = d/t^2. \tag{20}$$

We now consider forms f which are genus-equivalent to f_q, i.e., $f \in \mathrm{gen}(f_q)$.

Proposition 18 *Let $f \in \mathrm{gen}(f_q)$, where q is as above, and let d, t, d' be as in* (20)*. Then we have that*

$$I_1(f) \;=\; -16t \quad \textit{and} \quad I_2(f) \;=\; -d'. \tag{21}$$

Moreover, the reciprocal F_f of f is properly primitive if and only if d' is even.

Proof. For $f = f_q$ this was proved in [K4], p. 167, and so this holds for any $f \in \mathrm{gen}(f_q)$ because $I_1(f)$ and $I_2(f)$ are genus invariants; cf. [B2].

Moreover, it follows from [B2], p. 316, that F_f is improperly primitive if and only if $I_2(f)$ is odd, and so this implies the second assertion.

It is easy to see that f_q satisfies properties (1) and (2), so by Corollary 15 every $f \in \mathrm{gen}(f_q)$ is a special ternary form (in the sense of §4). It is less obvious that the converse holds; this will be proved now. For this, we will use the following result which is essentially Theorem 17 of Dickson[D].

Proposition 19 *Let f be a properly primitive positive ternary form and suppose that $F = F_f$ is also properly primitive, and that C is properly represented by F_f. If $\gcd(C, \Omega_f \Delta_f) = 1$, then f properly represents a properly primitive binary form ϕ with $\mathrm{disc}(\phi) = -4\Omega_f C$.*

Proof. The existence of ϕ follows from Theorem 17 of [D]. The fact that $\mathrm{disc}(\phi) = -4\Omega_f C$ follows from [D], Theorem 27.

Theorem 20 *If f is a positive ternary form, then following conditions are equivalent:*

(i) *f satisfies conditions* (1) *and* (2)*;*

(ii) *$f \in \mathrm{gen}(f_q)$, for some positive binary quadratic form q;*

(iii) *f is primitive and satisfies condition* (1)*. Moreover, $\chi(f) = 1$, for every $\chi \in X(f)$ and $\left(\frac{I_2(f)}{m}\right) = 1$, for some (and hence for any) $m \in R(F_f^B)$ with $\gcd(m, 2I_2(f)) = 1$.*

Proof. (ii) $\Rightarrow$ (i): It is clear that condition (2) holds for f_q because $1 \in R(f_q)$. Moreover, f_q satisfies condition (1) because $f_q(x, y, z) \equiv 1 \pmod 4$ if $x \equiv 1 \pmod 2$, and $f_q(x, y, z) \equiv 0 \pmod 4$ if $x \equiv 0 \pmod 2$. It thus follows from Corollary 15 that conditions (1) and (2) hold for any $f \in \mathrm{gen}(f_q)$.

(i) $\Rightarrow$ (iii): If conditions (1) and (2) hold for f, then f is primitive, for otherwise $\gcd(n, \mathrm{disc}(f)) > 1$ for every $n \in R(f)$, which contradicts (2). Thus, by Proposition 13 we see that f is properly primitive and that (13) holds.

Moreover, since there exists $n^2 \in R(f)$ with $\gcd(n^2, \mathrm{disc}(f)) = 1$ by (2), we see that $\chi(f) = \chi(n^2) = 1$, for all $\chi \in X(f)$, because $\gcd(n^2, \Omega_f) = 1$. (For the latter, note that by (11), (12) and [B2], p. 316, we have that $\Omega_f \mid \frac{I_1(f)}{4} \mid (\frac{I_1(f)}{4})^2 I_2(f) = \mathrm{disc}(f)$.)

It remains to verify the last assertion of (iii). For this, we know by property (2) that there exists $n_1^2 = f(x, y, z) \in R(f)$ with $\gcd(n_1, \mathrm{disc}(f)) = 1$. Put $g = \gcd(x, y, z)$ and $n = \frac{n_1}{g}$. Then $n^2 = f(\frac{x}{g}, \frac{y}{g}, \frac{z}{g})$ is properly represented by f, and $\gcd(n, \mathrm{disc}(f)) = 1$. Thus also $\gcd(n^2, 2I_2) = 1$, where $I_2 := I_2(f)$, because by Proposition 13 and [B2], p. 316, we have that $2I_2 \mid (\frac{I_1(f)}{4})^2 I_2 = \mathrm{disc}(f)$. We now show:

Claim: There exists a primitive binary form ϕ with $F_f^B \to \phi$ and $\mathrm{disc}(\phi) = I_2 n^2$.

Using this claim, the last assertion of (iii) can be verified as follows. For this, note first that since by Corollary 17 we know that $\left(\frac{I_2}{m_1}\right) = \left(\frac{I_2}{m_2}\right)$ for all $m_i \in R(F_f^B)$ with $\gcd(m_i, 2I_2) = 1$, for $i = 1, 2$, it suffices to verify that $\left(\frac{I_2}{m}\right) = 1$ for some $m \in R(F_f^B)$. Now by Dirichlet there exists a prime $p \in R(\phi)$ with $p \nmid I_2 n^2$. Then $\left(\frac{I_2}{p}\right) = \left(\frac{I_2 n^2}{p}\right) = \left(\frac{\mathrm{disc}(\phi)}{p}\right) = 1$, where the last equality follows from Lemma 2.5 of [C] because $p \in R(\phi)$. But since $F_f^B \to \phi$, it follows that $p \in R(\phi) \subset R(F_f^B)$, and so the assertion holds with $m = p$.

To prove the claim, we now distinguish two cases.

Case 1: F_f is properly primitive.

Here we have by (11) that $I_1 := I_1(f) = -4\Omega_f = -4\Delta_{F_f}$ and $I_2 := I_2(f) = -4\Delta_f = -4\Omega_{F_f}$, so $\mathrm{disc}(f) = \frac{I_1^2 I_2}{16} = -4\Omega_f^2 \Delta_f$. Thus $\gcd(n^2, \Omega_{F_f}\Delta_{F_f}) = 1$, and so by applying Proposition 19 to F_f in place of f with $C = n^2 \in R(f) = R(F_{F_f})$, we see that there exists a properly primitive binary form ϕ with $F_f \to \phi$ and $\mathrm{disc}(\phi) = -4\Omega_{F_f} n^2 = -4\Delta_f n^2 = I_2 n^2$. This proves the claim in this case.

Case 2: F_f is improperly primitive.

In this case we have that $I_1 := I_1(f) = -8\Omega_f$ and $I_2 := -\Delta_f$, so $\mathrm{disc}(f) = \frac{I_1^2 I_2}{16} = -4\Omega_f^2 \Delta_f$, and hence $\gcd(n^2, \Omega_{F_f}\Delta_{F_f}) = 1$. Since $n^2 \in R(f) = R(F_{F_f})$, we have by Theorem 38 of [D] that there exists a binary form ϕ' with $F_f \to \phi'$ and $\mathrm{disc}(\phi') = -4\Omega_{F_f} n^2 = -4\Delta_f n^2 = 4I_2 n^2$. Moreover, by Proposition 9 (applied to F_f in place of f) we see that ϕ' is G-primitive, and hence improperly primitive because F_f is improperly primitive. Thus $\phi := \frac{1}{2}\phi'$ is a primitive form with $\mathrm{disc}(\phi) = I_2 n^2$. Moreover, since $F_f^B = \frac{1}{2}F_f$, it follows that $F_f^B \to \phi$, and so the claim holds in all cases. As was explained above, this shows that condition (iii) holds.

(iii) $\Rightarrow$ (ii): If f satisfies the conditions of (iii), then f is primitive and satisfies condition (1). Moreover, there exists $m \in R(F_f^B)$ such that $\left(\frac{I_2}{m}\right) = 1$, where $I_2 = I_2(f)$. Since F_f^B is primitive by construction, there exists by Corollary 12 a prime $p \in R(F_f^B)$ with $p \nmid 2I_2$. Thus, by Corollary 17 we have that $\left(\frac{I_2}{p}\right) = \left(\frac{I_2}{m}\right) = 1$. This means that there is a $b \in \mathbb{Z}$ such that $I_2 \equiv b^2 \pmod{p}$. By replacing b by $p - b$, if necessary, we may assume that $b \equiv I_2 \pmod{2}$, so $b^2 \equiv I_2 \pmod{4}$. (Recall that $I_2 \equiv 0, 1 \pmod{4}$ by (13).) We thus have that $I_2 \equiv b^2 \pmod{4p}$, so $q'(x, y) := px^2 + bxy + \frac{b^2 - I_2}{4p} y^2$ is a positive primitive binary form with $\mathrm{disc}(q') = I_2$.

Next, put $q = tq'$, where $t := -\frac{I_1}{16} \in \mathbb{Z}$ by (13). We claim that $f \in \mathrm{gen}(f_q)$. For this, we first note that since $t = \mathrm{cont}(q)$, it follows from (21) that

$$I_1(f_q) = -16t = I_1(f) \quad \text{and} \quad I_2(f_q) = \mathrm{disc}(q') = I_2(f). \tag{22}$$

Thus, f and f_q have the same basic invariants. It therefore follows from Smith[Sm], §12, (together with [W], Theorem 50) that $f \in \mathrm{gen}(f_q)$ once we have shown that

$$\chi(f) \;=\; \chi(f_q),\ \forall \chi \in X(f_q) \quad \text{and} \quad \psi(F_f^B) \;=\; \psi(F_{f_q}^B),\ \forall \psi \in X(F_{f_q}^B). \tag{23}$$

(Note that although Smith formulates the second equation as $\psi(F_f) = \psi(F_{f_q}), \forall \psi \in X(F_{f_q})$, this condition is equivalent to the one above.)

To verify this, note first that since $1 \in R(f_q)$, we have that $\chi(f_q) = \chi(1) = 1$, for all $\chi \in X(f_q)$. But by hypothesis we have that $\chi(f) = 1$, for all $\chi \in X(f) = X(f_q)$, so the first equation of (23) holds.

To verify the second equation, recall that the above $p \in R(F_f^B)$ satisfies (by construction) that $p \in R(q')$. Now by [K4], equation (44), we know that

$$F_{f_q}^B \;\sim\; td'x^2 + q'(y,z), \quad \text{where } d' = -\operatorname{disc}(q'), \tag{24}$$

so we see that $R(q') \subset R(F_{f_q}^B)$. Thus, $p \in R(F_f^B) \cap R(F_{f_q}^B)$, and so $\psi(F_f^B) = \psi(p) = \psi(F_{f_q}^B)$, for every $\psi \in X(F_{f_q}^B) = X(F_f^B)$. This proves that (23) holds, and hence $f \in \mathrm{gen}(f_q)$, as desired.

The following result, which will be used below, is closely related to the proof of Theorem 20.

Corollary 21 *Let $f \in \mathrm{gen}(f_q)$, where $q = tq'$ is as in* Proposition 18, *and let $p \in R(F_f^B)$ be a prime with $p \nmid d' = -\operatorname{disc}(q')$. Then there exists a form $\tilde{q}' \in \mathrm{gen}(q')$ which represents p. Thus tp is primitively represented by $\tilde{q} := t\tilde{q}' \in \mathrm{gen}(q)$.*

Proof. By Theorem 20 we have that f satisfies the conditions of Theorem 20(iii). From the proof of the implication (iii) $\Rightarrow$ (ii) we know that if $p \in R(F_f^B)$ is any prime with $p \nmid I_2(f) = -d'$, then there exists an integer b such that $\tilde{q}' := px^2 + bxy + \frac{b^2+d'}{4p}y^2$ is a primitive integral form of discriminant $-d'$.

Clearly $p \in R(\tilde{q}')$, so it remains to show that $\tilde{q}' \in \mathrm{gen}(q')$. Since $\operatorname{disc}(\tilde{q}') = -d' = \operatorname{disc}(q')$, this is equivalent to the condition that $\chi(\tilde{q}') = \chi(q')$, for all $\chi \in X(q')$; see Cox[C], Lemma 3.20.

By Proposition 16 we know that $X(\tilde{q}') = X(F_f^B)$ because $\operatorname{disc}(\tilde{q}') = -d' = I_2(f)$. Now since $p \in R(\tilde{q}') \cap R(F_f^B)$, we have that $\chi(\tilde{q}') = \chi(p) = \chi(F_f^B)$, for all $\chi \in X(\tilde{q}')$. On the other hand, by (24) we see that $R(q') \subset R(F_{f_q}^B)$, so $\chi(q') = \chi(x) = \chi(F_{f_q}^B)$, for all $\chi \in X(q')$ and any $x \in R(q')$ with $\gcd(x, I_2) = 1$. But since $f \in \mathrm{gen}(f_q)$, we have that $\chi(F_f^B) = \chi(F_{f_q}^B)$, for all $\chi \in X(F_{f_q}^B) = X(q')$, the latter by Proposition 16 again. We thus have that $\chi(\tilde{q}') = \chi(q')$, for all $\chi \in X(q')$, as desired.

We now prove the second main result of this section.

Theorem 22 *Let $f \in \mathrm{gen}(f_q)$, where q is as in* Proposition 18. *If ϕ_p is a properly primitive binary form which is properly represented by f with $\mathrm{disc}(\phi_p) = I_1(f)p = -16tp$, for some prime $p \nmid 16td'$, then $\phi_p \in \mathrm{gen}(x^2+4tpy^2)$, i.e., ϕ_p lies in the principal genus. Thus, ϕ_p is a primitive binary form* of type tp *in the sense of* [K3].

Proof. By Cox[C], Lemma 3.20, it suffices to show that $\chi(\phi_p) = 1$ for all assigned characters $\chi \in X(\phi_p)$. For this, we first observe that

$$X(\phi_p) \;=\; X(f) \;\cup\; \{\chi_p\}. \tag{25}$$

Indeed, if $2|t$, then $32|\,\mathrm{disc}(\phi) = -16tp$, so by Cox[C], p. 55, we have that $X(\phi_p) = \{\chi_{-4}, \chi_8, \chi_\ell : \ell|tp, \ell \neq 2\}$, and by the proof of Proposition 16 we know that $X(f) = \{\chi_{-4}, \chi_8, \chi_\ell : \ell|t, \ell \neq 2\}$. Thus, (25) follows in this case. On the other hand, if $2 \nmid t$, then $\mathrm{disc}(\phi) \equiv 16 \,(\mathrm{mod}\ 32)$, then $X(\phi_p) = \{\chi_{-4}, \chi_\ell : \ell|tp\}$, and $X(f) = \{\chi_{-4}, \chi_\ell : \ell|t\}$, so (25) holds in all cases.

Thus, if x is any integer represented by ϕ_p with $\gcd(x, 16td') = 1$, then x is also represented by f and $\gcd(x, I_1(f)) = 1$, so

$$\chi(\phi) \;=\; \chi(x) \;=\; \chi(f) \;=\; \chi(f_q) \;=\; 1, \quad \text{for all } \chi \in X(f) = X(\phi_p) \setminus \{\chi_p\}.$$

Here the third equality follows because $f \in \mathrm{gen}(f_q)$ and the fourth holds because $1 \in R(f_q)$.

It remains to compute $\chi_p(\phi)$. For this, write $I_1 = I_1(f)$ and let p' be a prime represented by $\phi_p$with $p' \nmid 16tp$. (This exists by Dirichlet's Theorem; cf. Theorem 9.12 of [C].) Then $\left(\frac{I_1 p}{p'}\right) = 1$ by Lemma 2.5 of [C] because $p' \in R(\phi_p)$ and $\mathrm{disc}(\phi_p) = I_1 p$. But by (17) we have that $\left(\frac{I_1}{p'}\right) = \left(\frac{I_1}{1}\right) = 1$ because $p' \in R(f)$ and $1 \in R(f_q)$ and $f \in \mathrm{gen}(f_q)$, and hence $\left(\frac{p}{p'}\right) = 1$. Thus, since $p' \equiv 1 \,(\mathrm{mod}\ 4)$ because f satisfies (1), we see by quadratic reciprocity that $\chi_p(\phi_p) = \chi_p(p') = \left(\frac{p'}{p}\right) = \left(\frac{p}{p'}\right) = 1$, and so $\chi(\phi_p) = 1$, for all $\chi \in X(\phi_p)$, as desired. This means that $\phi_p \in \mathrm{gen}(x^2 + 4tpy^2)$, and so ϕ_p is a primitive binary form of type tp by Theorem 13 of [K3].

The (primitive) binary forms *of type* $\delta = tp$ were classified in [K3]. To state the result, put

$$P(\delta)^{odd} \;:=\; \{(n, m, k) \in \mathbb{Z}^3 : nm - k^2\delta = 1,\, n > 0, m > 0, \text{ and } 2 \nmid \gcd(n, m)\},$$

and for $s = (n, m, k) \in P(\delta)^{odd}$ put

$$q_s(x, y) \;:=\; n^2x^2 + 2k\delta(nm + 2)xy + m^2\delta(nm + 3)y^2.$$

Then by Theorem 13 of [K3] (and its proof) we have the following characterization of the primitive binary forms of type δ.

Proposition 23 *Let $\delta \geq 1$, and let q be a binary form. Then $q \in \mathrm{gen}(x^2 + 4\delta y^2)$ if and only if $q \sim q_s$, for some $s \in P(\delta)^{odd}$.*

In view of this result, we can deduce the following result from Theorem 22.

Corollary 24 *Let $f \in \mathrm{gen}(f_q)$, where q is as in* Proposition 18. *Then there exist infinitely many primes $p \in R(F_f^B)$ such that $f \to q_s$, for some $s \in P(tp)^{odd}$.*

Proof. By Theorem 11 and equation (21) there exist infinitely primes $p \in R(F_f^B)$ with $p \nmid 16td'$ such that $f \to \phi_p$, where ϕ_p is some properly primitive form of discriminant $-16tp$. By Theorem 22 we know that each such ϕ_p is in $\mathrm{gen}(x^2 + 4tpy^2)$, and so it follows from Proposition 23 that $\phi_p \sim q_s$, for some $s \in P(tp)^{odd}$. Then also $f \to q_s$; see [D], Theorem 28.

6 The construction of (A, θ)

Using the above results on ternary forms, we are now in a position to prove that every form $f \in \mathrm{gen}(f_q)$ is equivalent to a refined Humbert invariant $q_{(A,\theta)}$, for a suitable principally polarized abelian surface (A, θ).

For this, recall from [K1], [K3] that the *refined Humbert invariant* is defined as follows. Let A/K be an abelian surface, where K is an algebraically closed field, so the *Néron-Severi group* $\mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$ comes equipped with a canonical bilinear form β_A which is given by the intersection pairing $(D.D')$ on divisors. In fact, the rule $D \mapsto \frac{1}{2}(D.D)$ defines an integral quadratic form $q_A : \mathrm{NS}(A) \to \mathbb{Z}$ whose associated bilinear form is β_A, i.e.,

$$\beta_A(D, D') \;:=\; q_A(D + D') - q_A(D) - q_A(D') \;=\; (D.D'). \tag{26}$$

Now assume that A has a principal polarization $\theta \in \mathcal{P}(A) \subset \mathrm{NS}(A)$. This means that $q_A(\theta) = 1$, and that θ is (the image of) an ample divisor on A. Put

$$\tilde{q}_{(A,\theta)}(D) \;:=\; \beta_A(D, \theta)^2 - 4q_A(D) \;=\; (D.\theta)^2 - 2(D.D), \quad \text{for } D \in \mathrm{NS}(A). \tag{27}$$

It is easy to see (cf. [K1]) that this defines a positive quadratic form $q_{(A,\theta)}$ on the quotient space $\mathrm{NS}(A, \theta) := \mathrm{NS}(A)/\mathbb{Z}\theta$. The form $q_{(A,\theta)}$ is called the *refined Humbert invariant* of the principally polarized abelian surface (A, θ).

In the case that $A = E \times E'$ is an abelian product surface, then we have an isomorphism

$$\mathbf{D} : \mathbb{Z} \times \mathbb{Z} \times \mathrm{Hom}(E, E') \xrightarrow{\sim} \mathrm{NS}(E \times E')$$

such that

$$q_A(\mathbf{D}(x, y, h)) \;=\; xy - \deg(h), \quad \text{for } x, y \in \mathbb{Z}, h \in \mathrm{Hom}(E, E'); \tag{28}$$

cf. [K3], Proposition 23. Thus, $q_A \sim xy - q_{E,E'}$, where $q_{E,E'}(h) = \deg(h)$ is the degree form on $\mathrm{Hom}(E, E')$. Note that if $\theta_{E,E'} := \mathbf{D}(1,1,0)$ is the product polarization of $E \times E'$, then we see from (27) and (28) that

$$q_{(E\times E',\theta_{E,E'})}(\mathbf{D}(x,y,h)) \;=\; (x-y)^2 + 4q_{E,E'}(h), \tag{29}$$

so $q_{(E\times E',\theta_{E,E'})} \sim f_{q_{E,E'}}$. We now recall the following fact which was proven in [K3].

Proposition 25 *Let $A = E \times E'$ be a CM abelian product surface, i.e., $E \sim E'$ are isogenous elliptic curves with complex multiplication. If $\theta \in \mathcal{P}(A)$ is a principal polarization such that $q_{(A,\theta)}$ is a primitive form, then $q_{(A,\theta)} \in \mathrm{gen}(f_q)$, where $q = q_{E,E'}$.*

Proof. Apply Theorem 20 of [K4] to the quadratic module $(\mathrm{NS}(A), q_A)$. By (28) we see that this module satisfies the hypothesis of that theorem, so it follows that $q_{(A,\theta)}$ is primitive if and only if $\theta \in \mathcal{P}(A)^{odd}$. Moreover, since $\theta_{E,E'} \in \mathcal{P}(A)^{odd}$, it follows from the same theorem that $q_{(A,\theta)} \in \mathrm{gen}(q_{(A,\theta_{E,E'})})$, for all $\theta \in \mathcal{P}(A)^{odd}$. Since $q_{E,E'} \sim f_q$ by (29), this proves the assertion.

We are now almost ready to prove Theorem 1 of the introduction. However, we also need part (a) of the following result which was implicitly proven in [K2], Remark 41.

Lemma 26 *Let K be an algebraically closed field and let q be a positive binary quadratic form of discriminant D.*

(a) *If $\mathrm{char}(K) = 0$, then there exist two elliptic curves E_i/K, $i = 1, 2$ such that $q_{E_1,E_2} \sim q$.*

(b) *If $\mathrm{char}(K) = p > 0$, then there exist two elliptic curves E_i/K, $i = 1, 2$ such that $q_{E_1,E_2} \sim q$ if and only if $\left(\frac{D}{p}\right) = 1$.*

Proof. (a) Write $q = tq'$, where $t = \mathrm{cont}(q)$, and let $F = \mathbb{Q}(\sqrt{D})$. Then $q' \sim q_L$, for some lattice L of F, where q_L is as defined in [K2], p. 321. Moreover, the index $f_L = [\mathcal{O}_F : R(L)]$ of its order $R(L) \subset \mathcal{O}_F$ satisfies the relation $f_L^2 d_F = D/t^2 = \mathrm{disc}(q')$, where d_F denotes the discriminant of the ring of integers $\mathcal{O}_F$ of F. Thus $R(L) = \mathcal{O}_{D/t^2}$ where $\mathcal{O}_D \subset \mathcal{O}_F$ denotes the (unique) order of F of discriminant D.

By [K2], Proposition 37(a) there exists a CM elliptic curve E_2/K such that $\mathrm{End}(E_2) \simeq \mathcal{O}_D$. Note that $\mathcal{O}_D \subset R(L) = \mathcal{O}_{D/t^2}$, and that $[\mathcal{O}_{D/t^2} : \mathcal{O}_D] = t$, so $f_{E_2} := [\mathcal{O}_F : \mathcal{O}_D] = tf_L$.

Since $R(L) \supset \mathcal{O}_D$, we see that $L \simeq \mathfrak{a}$, for some ideal $\mathfrak{a}$ of $\mathcal{O}_D$. It thus follows from Corollary 21 of [K2] together with equation (54) of [K2] that there is an elliptic curve E_1/K with $E_1 \sim E_2$ such that $I_{E_2}(E_1) \simeq \mathfrak{a} \simeq L$ and that $\mathrm{End}(E_1) \simeq R(L)$, so $f_{E_1} = f_L$. We thus have that $\frac{\mathrm{lcm}(f_{E_1}, f_{E_2})}{\gcd(f_{E_1}, f_{E_2})} = t$. Moreover, since $I_{E_2}(E_2) \simeq \mathcal{O}_D$, we have

by Proposition 40 of [K2] that $q_{E_1,E_2} \sim tq_{L'}$, where $L' = I_{E_2}(E_1)I_{E_2}(E_2)^{-1} \simeq \mathfrak{a} \simeq L$, so $q_{E_1,E_2} \sim tq_L \sim tq' = q$, and so the assertion follows.

(b) Suppose first that $q \sim q_{E_1,E_2}$ for some elliptic curves E_i/K, $i = 1, 2$. Then $\mathrm{rank}(\mathrm{Hom}(E_1, E_2)) = 2$, so $E_1 \sim E_2$ are CM elliptic curves over K. By Deuring (cf. [K2], Proposition 37(b)), this implies that $\left(\frac{\Delta_{E_i}}{p}\right) = 1$, where Δ_{E_i} denotes the discriminant of the order $\mathrm{End}(E_i)$ in $F = \mathrm{End}^0(E_i)$. Thus $p \nmid f_{E_i} = [\mathcal{O}_F : \mathrm{End}(E_i)]$ and $\left(\frac{d_F}{p}\right) = 1$. We thus have that $p \nmid \mathrm{lcm}(f_{E_1}, f_{E_2})$, and so $\left(\frac{D}{p}\right) = 1$ because $D = \mathrm{lcm}(f_{E_1}, f_{E_2})^2 d_F$ by Corollary 42 of [K2].

Conversely, suppose that the discriminant $D = \mathrm{disc}(q)$ satisfies $\left(\frac{D}{p}\right) = 1$. Then by Deuring (cf. [K2], Proposition 37(b)), there exists a CM elliptic curve E_2/K such that $\mathrm{End}(E_2) \simeq \mathcal{O}_D$. Using this fact, we see that the same proof as in part (a) shows that there exists a CM elliptic curve E_1/K such that $q_{E_1,E_2} \sim q$.

Proof of Theorem 1. (i) $\Leftrightarrow$ (ii): This follows from Theorem 20.

(iii) $\Rightarrow$ (ii): Here we assume that $f \sim q_{(A,\theta)}$, for some (A, θ). Since f is a ternary form, it follows that $\mathrm{rank}(\mathrm{NS}(A, \theta)) = 3$, so $\mathrm{rank}(\mathrm{NS}(A)) = 4$. Since $\mathrm{char}(K) = 0$, it is well-known (cf. e.g. [K2]) that this implies that A cannot be simple, and so $A \sim E \times E$, for some elliptic curve E with CM. By the Theorem of Shioda-Mitani (cf. [K2]), this implies that $A \simeq E' \times E''$, for some elliptic curves E' and E'' with $E' \sim E'' \sim E$. Since f is assumed to be primitive, we have by Proposition 25 that $f \in \mathrm{gen}(f_q)$, where $q = q_{E',E''}$.

(ii) $\Rightarrow$ (iii): Suppose that $f \in \mathrm{gen}(f_q)$, for some positive binary quadratic form q. Let $d := -\mathrm{disc}(q)$ and $t = \mathrm{cont}(q)$. Then by Corollary 24 there exists a prime p represented by F_f^B and a triple $s = (n, m, k) \in P(tp)^{odd}$ such that $f \to q_s$. Moreover, by Corollary 21 we know that there exists $\tilde{q} \in \mathrm{gen}(q)$ such that tp is primitively represented by $\tilde{q}$.

Since $\mathrm{char}(K) = 0$, there exist two elliptic curves E, E' with $q_{E,E'} \sim \tilde{q}$; cf. Lemma 26(a). Since $\tilde{q}$ primitively represents tp, it follows that there exists a primitive $h \in \mathrm{Hom}(E, E')$ such that $q_{E,E'}(h) = tp$. Moreover, since h is primitive, there exists an $h' \in \mathrm{Hom}(E, E')$ such that h, h' is a basis of $\mathrm{Hom}(E, E')$.

Put $A = E \times E'$, and put $\theta = D_{s,h} = \mathbf{D}(n, m, kh)$. Then $\theta \in \mathcal{P}(A)$ by [K3], Corollary 25, and by Proposition 29 of [K3] we know that $q_{(A,\theta)} \to q_s$.

Since $s \in P(tp)^{odd}$, it follows that q_s is primitive, and hence by [K4], Theorem 20, we see $\theta \in \mathcal{P}(A)^{odd} = \{\theta' \in \mathcal{P}(A) : \beta_A(D, \theta') \equiv 1 \pmod 2, \text{ for some } D \in \mathrm{NS}(A)\}$. Thus, $q_{(A,\theta)}$ is primitive, and so $q_{(A,\theta)} \in \mathrm{gen}\, f_{\tilde{q}}$ by Proposition 25. Since $\tilde{q} \in \mathrm{gen}(q)$, we have that $\mathrm{gen}(f_q) = \mathrm{gen}(f_{\tilde{q}})$. Thus, f and $q_{(A,\theta)}$ both lie in $\mathrm{gen}(f_q)$, and so they have the same invariants I_k, $k = 1, 2$, and hence also the same invariants Ω and Δ.

From the above constructions we know that both f and $q_{(A,\theta)}$ properly represent q_s, which has discriminant $-16tp = -4\Omega C$, where $C = p$, if d' is even and $C = 2p$,

if d' is odd. It thus follows from Theorem 34 of [D] that $f \sim q_{(A,\theta)}$, which proves the theorem.

It is useful to observe that the above proofs and constructions actually provide an algorithm for constructing a principally polarized abelian surface (A, θ) such that $q_{(A,\theta)} \sim f$, where $f \in \text{gen}(f_q)$, for some q. This algorithm is as follows.

Algorithm 27 *Let f be a primitive positive ternary form. Determine whether there exists a principally polarized abelian surface (A, θ) with $q_{(A,\theta)} \sim f$. If so, then find such an (A, θ).*

Steps of the Algorithm: 1) Check that $f \equiv f_1^2 \pmod 4$, for some linear form f_1. If not, then f does not satisfy condition (1) and hence there is no such (A, θ) by Theorem 1, and the algorithm returns FAIL. Otherwise, f satisfies condition (1), and we continue with the next step.

2) Compute the invariants $I_k = I_k(f)$, for $k = 1, 2$, and check that the conditions of Theorem 20(iii) hold for f. (To check these, use the method of the proof of Theorem 7 of [D] to find integers $n \in R(f)$ and $m \in R(F_f^B)$ with $\gcd(n, I_1) = \gcd(m, 2I_2) = 1$ and check that $\chi(n) = 1$, for all $\chi \in X(f)$, and that $\left(\frac{I_2}{m}\right) = 1$.) If one of these conditions does not hold, then f does not satisfy condition (2) by Theorem 20, and so the algorithm returns FAIL by Theorem 1. If they hold, then such an (A, θ) exists, and we go to the next step.

3) Compute the reciprocal F_f^B of f and find integers x, y, z such that $p := F_f^B(x, y, z)$ is an odd prime with $p \nmid d := -\frac{\text{disc}(f)}{16}$. (If d is odd, then choose p such that also $p \equiv t \pmod 4$, where $t = -\frac{I_1}{16}$. Such a prime exists by Corollary 7.) We can find a suitable p by substituting small values for x, y, z, but it is unclear how long we have to search until such a p is found. (However, if we accept the Generalized Riemann Hypothesis (GRH), then explicit estimates can be given.)

4) Choose an integer b such that $-d' \equiv b^2 \pmod{4p}$, where $d' = d/t^2$. Such a b exists and can be found by the method outlined in the proof of the implication (iii) $\Rightarrow$ (ii) of Theorem 20. Then $q := tpx^2 + tbxy + \frac{t(b^2+d')}{4p}$ is such that $f \in \text{gen}(f_q)$, as was shown in the proof of Theorem 20.

5) By CM-theory, we can construct a CM-elliptic curve E'/K such that the discriminant of $\text{End}(E')$ is equal to $-d$, and by the recipe of Lemma 26 (and the results of [K2]) we can find $E \sim E'$ such that $q_{E,E'} \sim q$. Thus, there exists a (cyclic) $h \in \text{Hom}(E, E')$ such that $\deg(h) = tp$.

6) Use the results from Step 3 and the recipe of the proof of Theorem 38 of [D] to find a binary form ϕ of discriminant $-16tp$ which is properly represented by f. Then ϕ is a properly primitive form by Theorem 11 and Proposition 13.

7) Since $\phi \in \text{gen}(x^2 + 4tpy^2)$ by Theorem 22, we can use the recipe of the proof of Theorem 13 of [K3] to find $s = (n, m, k) \in P(tp)$ such that $\phi \sim q_s$.

8) Put $A = E \times E'$ and $\theta = D_{s,h} = \mathbf{D}(n, m, kh)$. Then θ is a principal polarization on A and $q_{(A,\theta)} \sim f$ by the proof of Theorem 1.

In the case of positive characteristic we have the following result which is analogous to Theorem 1.

Theorem 28 *Let K be an algebraically closed field of characteristic $p > 0$, and let f be a primitive positive ternary quadratic form. Then the following conditions are equivalent:*

(i) *f satisfies conditions* (1) *and* (2)*, and $\left(\frac{-d}{p}\right) = 1$, where $d = -\operatorname{disc}(f)/16$.*

(ii) *$f \in \operatorname{gen}(f_q)$, for some positive binary quadratic form q with $\left(\frac{\operatorname{disc}(q)}{p}\right) = 1$.*

(iii) *f is equivalent to a form $q_{(A,\theta)}$, for some $(A, \theta) \in \mathcal{A}_2(K)$ with $A \sim E \times E$, for some elliptic curve E.*

Proof. (i) $\Leftrightarrow$ (ii): This follows from Theorem 20 because $d = -\operatorname{disc}(q)$, if $f \in \operatorname{gen}(f_q)$.

(iii) $\Rightarrow$ (ii): Since $q_{(A,\theta)} \sim f$ and f is a ternary form, we know that $\operatorname{rank}(\mathrm{NS}(A)) = 4$. Moreover, since $A \sim E \times E$, we have that $4 = \operatorname{rank}(\mathrm{NS}(A)) = \operatorname{rank}(\mathrm{NS}(E \times E)) = 2 + \operatorname{rank}(\mathrm{End}(E))$, so $\operatorname{rank}(\mathrm{End}(E)) = 2$, and hence E is a CM elliptic curve. Thus, it follows from Theorem 2 of [K2] that $A \simeq E_1 \times E_2$, for some elliptic curves E_1/K, E_2/K with $E \sim E_i$, for $i = 1, 2$.

Since f is assumed to be primitive, we have by Proposition 25 that $f \in \operatorname{gen}(f_q)$, where $q = q_{E_1,E_2}$, and by Lemma 26(b) we know that $\left(\frac{\operatorname{disc}(q)}{p}\right) = 1$.

(i) $\Rightarrow$ (iii): This is similar to the method of Algorithm 27. Indeed, steps 1) - 6) of this algorithm only involve quadratic form theory, so we have the same conclusions. More precisely, the hypotheses of (i) guarantee that steps 1) and 2) are successful, and so by steps 3) - 6) we have a binary form q such that $f \in \operatorname{gen}(f_q)$. Note that $\operatorname{disc}(q) = -d$, as was mentioned above.

In step 7) we observe that since $\left(\frac{\operatorname{disc}(q)}{p}\right) = \left(\frac{-d}{p}\right) = 1$ by hypothesis, we have by Lemma 26(b) that there exists a pair of CM elliptic curve E/K and E'/K such that $q_{E,E'} \sim q$. Putting $A = E \times E'$ and $\theta = D_{s,h}$ as before, we see by the same argument as in the proof of Theorem 1 that $f \sim q_{(A,\theta)}$, as desired.

We now turn to the proof of Theorem 2. For this, we shall use the following general fact.

Proposition 29 *Let A and A' be two abelian surfaces over an algebraically closed field K. If their intersection forms q_A and $q_{A'}$ are equivalent, then there exists an isomorphism*

$$\varphi : (\mathrm{NS}(A), q_A) \quad \tilde{\to} \quad (\mathrm{NS}(A'), q_{A'})$$

of quadratic modules such that $\varphi(\mathcal{P}(A)) = \varphi(\mathcal{P}(A'))$. *Moreover, if* $\theta \in \mathcal{P}(A)$, *then* φ *induces an isomorphism*

$$\varphi_\theta : (\mathrm{NS}(A,\theta), q_{(A,\theta)}) \quad \tilde{\to} \quad (\mathrm{NS}(A', \varphi(\theta)), q_{(A',\varphi(\theta))}). \tag{30}$$

Thus, if $\Theta_A := \{q : q \sim q_{(A,\theta)},\ \textit{for some } \theta \in \mathcal{P}(A)\}/\sim$ *denotes the set of equivalence classes of integral quadratic forms* q *which are equivalent to some* $q_{(A,\theta)}$, *and if* $\Theta_{A'}$ *is defined similarly, then we have that* $\Theta_A = \Theta_{A'}$.

Proof. The hypothesis $q_A \sim q_{A'}$ is equivalent to the assertion that we have an isomorphism φ of quadratic modules as indicated. Thus, if we put $\mathcal{P}(A)^* = \{D \in \mathrm{NS}(A) : q_A(D) = 1\}$, and define $\mathcal{P}(A')^*$ similarly, then it is clear that $\varphi(\mathcal{P}(A)^*) = \mathcal{P}(A')^*$.

Now by [K1], Corollary 2.2(b), we have that

$$\mathcal{P}(A)^* = \mathcal{P}(A) \cup \mathcal{P}(A)^-, \quad \text{where } \mathcal{P}(A)^- = \{-\theta : \theta \in \mathcal{P}(A)\}, \tag{31}$$

so $\mathcal{P}(A)^* = \emptyset \Leftrightarrow \mathcal{P}(A) = \emptyset$. Since the same holds for $\mathcal{P}(A')^*$, we see that the proposition is vacuously true if $\mathcal{P}(A)$ is empty.

Thus, assume that $\theta_0 \in \mathcal{P}(A)$. Then $\varphi(\theta_0) \in \mathcal{P}(A')^*$, so either $\varphi(\theta_0) \in \mathcal{P}(A')$ or $-\varphi(\theta_0) \in \mathcal{P}(A')$. Thus, by replacing φ by $-\varphi$, if necessary, we may assume that $\theta_0' = \varphi(\theta_0) \in \mathcal{P}(A')$.

Now let $\theta \in \mathcal{P}(A)$ be arbitrary. Then $(\theta.\theta_0) > 0$, so also $(\varphi(\theta).\varphi(\theta_0)) = (\theta.\theta_0) > 0$, and hence $\varphi(\theta) \notin \mathcal{P}(A')^-$ because $\varphi(\theta_0) \in \mathcal{P}(A')$. It follows that $\varphi(\theta) \in \mathcal{P}(A')$ because $\varphi(\theta) \in \mathcal{P}(A')^*$, as was mentioned above.

This shows that $\varphi(\mathcal{P}(A)) \subset \mathcal{P}(A')$. A similar argument shows that $\varphi^{-1}(\mathcal{P}(A')) \subset \mathcal{P}(A)$, and so $\varphi(\mathcal{P}(A)) = \mathcal{P}(A')$. This proves the first assertion.

Now suppose that $\theta \in \mathcal{P}(A)$, and let $\pi_{(A,\theta)} : \mathrm{NS}(A) \to \mathrm{NS}(A,\theta) = \mathrm{NS}(A)/\mathbb{Z}\theta$ denote the quotient map. Since $\varphi(\mathrm{Ker}(\pi_{(A,\theta)})) = \mathbb{Z}\varphi(\theta) = \mathrm{Ker}(\pi_{(A',\varphi(\theta))})$, there is a unique isomorphism $\varphi_\theta : \mathrm{NS}(A,\theta) \tilde{\to} \mathrm{NS}(A', \varphi(\theta))$ such that $\varphi_\theta \circ \pi_{(A,\theta)} = \pi_{(A',\varphi(\theta))} \circ \varphi$. Moreover, since $q_{A'}(\varphi(D)) = q_A(D)$ and $\beta_{A'}(\varphi(D), \varphi(\theta)) = \beta_A(D,\theta)$, for all $D \in \mathrm{NS}(A)$, we see by (27) that $\tilde{q}_{(A',\varphi(\theta))} \circ \varphi = \tilde{q}_{(A,\theta)}$, and so it follows that $q_{(A',\varphi(\theta))} \circ \varphi_\theta = q_{(A,\theta)}$. We thus obtain the desired isomorphism (30) of quadratic modules.

It follows from the isomorphism (30) that if $q \sim q_{(A,\theta)}$, for some $\theta \in \mathcal{P}(A)$, then $q \sim q_{(A',\theta')}$ with $\theta' = \varphi(\theta) \in \mathcal{P}(A')$. Thus $\Theta_A \subset \Theta_{A'}$. By interchanging the roles of A and A' we also obtain that $\Theta_{A'} \subset \Theta_A$, so $\Theta_A = \Theta_{A'}$.

Corollary 30 *If* $A \simeq E_1 \times E_2$ *and* $A' \simeq E_1' \times E_2'$ *are two abelian product surfaces such that* $q_{E_1',E_2'} \in \mathrm{gen}(q_{E_1,E_2})$, *then* $q_{A'} \sim q_A$ *and hence* $\Theta_A = \Theta_{A'}$.

Proof. By (28) we know that $q_{A'} \sim xy - q'$ and $q_A \sim xy - q$, where $q' = q_{E_1',E_2'}$ and $q = q_{E_1,E_2}$. Since $q' \in \mathrm{gen}(q)$, it follows that $q_{A'} \sim q_A$; cf. [K4], Remark 27. This proves the first assertion, and the second follows from Proposition 29.

Proof of Theorem 2. Let $f \in \mathrm{gen}(f_q)$. Then by the proofs of Theorems 1 and 28 we see that there exists a binary form $\tilde{q} \in \mathrm{gen}(q)$, elliptic curves $\tilde{E}$ and $\tilde{E}'$ with $q_{\tilde{E},\tilde{E}'} \sim \tilde{q}$ and a principal polarization $\tilde{\theta} \in \mathcal{P}(\tilde{A})$, where $\tilde{A} = \tilde{E} \times \tilde{E}'$, such that $f \sim q_{(\tilde{A},\tilde{\theta})}$. Thus $f \in \Theta_{\tilde{A}}$, and so by Corollary 30 we have that $f \in \Theta_A$. This means that $f \sim q_{(A,\theta)}$, for some $\theta \in \mathcal{P}(A)$, as desired.

References

[B1] H. Brandt, Zur Zahlentheorie der ternären quadratischen Formen. *Math. Ann.* **124** (1952), 334–342.

[B2] H. Brandt, Über das Maß positiver ternärer quadratischer Formen. *Math. Nachr.* **6** (1952), 315–318.

[C] D. Cox, *Primes of the Form* $x^2 + ny^2$. Wiley & Sons, New York, 1989.

[D] L. Dickson, *Studies in the Theory of Numbers.* U Chicago Press, Chicago, 1930. Reprinted by Chelsea Publ. Co., New York, 1957.

[Hu] G. Humbert, Sur les fonctions abéliennes singulières. I. *J. de Math.* (ser. 5) **5** (1899), 233–350 = Œuvres, Gauthier-Villars et Cie., Paris, 1929, pp. 297–401.

[Ja] G. Janusz, *Algebraic Number Fields*. 2nd ed. AMS, Providence, 1996.

[Jo] B. Jones, *The Arithmetic Theory of Quadratic Forms*. Carus Math. Monograph No. 10, MAA, 1960.

[K1] E. Kani, Elliptic curves on abelian surfaces. *Manusc. math.* **84** (1994), 199–223.

[K2] E. Kani, Products of CM elliptic curves.*Collectanea Math.* **62** (2011), 297–339.

[K3] E. Kani, The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Collect. Math.* **67** (2016), 21–54.

[K4] E. Kani, Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. *J. Number Theory* **139** (2014), 138–174.

[K5] E. Kani, Elliptic subcovers of a curve of genus 2 II. The refined Humbert invariant. *J. Number Theory* **193** (2018), 302–335.

[K6] E. Kani, Principal polarizations on $E \times E'$. Preprint, 29 pages.

[Kir] H. Kir, The classification of the refined Humbert invariant for curves of genus 2. *International J. of Number Theory* **21** (2025), 1247–1279.

[Sm] J.H.S. Smith, On the orders and genera of ternary quadratic forms (1867). *Collect. Math. Papers* vol. I, Oxford, 1894, pp. 455–509.

[W] G. Watson, *Integral Quadratic Forms.* Cambridge U Press, Cambridge, 1960.