

# Curves of Genus 2 and a Conjecture of Gauss

## 1. Introduction

Let  $E_1$  and  $E_2$  be two elliptic curves over  $K = \overline{K}$ .

**Question:** Is there a (smooth, irreducible) genus 2 curve  $C$  on the product surface  $E_1 \times E_2$ ?

**Equivalent Question:** Is there a curve  $C$  such that its Jacobian  $J_C$  is isomorphic to  $E_1 \times E_2$ ?

**Definition:** The pair  $(E_1, E_2)$  is called **irreducible** if such a curve exists, and is called **reducible** if no such curve exists.

**Problem 1:** Classify the reducible pairs  $(E_1, E_2)$ .

**Remarks:** 1) This problem was studied by:

Hayashida(1965), Hayashida/Nishi(1965)  $\rightarrow$  partial results

Ibukiyama/Katsura/Oort (1986) If  $E_1, E_2$  are **supersingular**, then  $(E_1, E_2)$  is reducible  $\Leftrightarrow \text{char}(K) = 2$  or  $3$ .

2) If  $E_1$  is not isogenous to  $E_2$ , then  $(E_1, E_2)$  is reducible.

**Assume henceforth:**  $E_1 \sim E_2$  and  $E_1$  is not supersingular.

**Basic Observation:** The irreducibility of  $(E_1, E_2)$  depends only on the nature of the **quadratic form**  $q_{E_1, E_2}$  on  $\text{Hom}(E_1, E_2)$  which is defined by

$$q_{E_1, E_2}(f) := \deg(f) \quad \text{for } f \in \text{Hom}(E_1, E_2) \simeq \mathbb{Z}^r.$$

Here  $r = 2$  if  $E_1$  has *CM* and otherwise  $r = 1$ .

**Notes:** 1) Thus, by choosing a basis of  $\text{Hom}(E_1, E_2)$ , the map  $q_{E_1, E_2}$  defines an equivalence class of **positive definite** quadratic forms in  $r \leq 2$  variables.

2) Conversely, it can be shown that every positive definite quadratic form  $q$  in  $r \leq 2$  variables is equivalent to  $q_{E_1, E_2}$ , for some pair  $(E_1, E_2)$  of elliptic curves.

Due to this observation, we can split **Problem 1** into two **sub-problems**:

**Problem 1a:** Classify the “**exceptional**” quadratic forms  $q$  such that  $q \sim q_{E_1, E_2}$ , where  $(E_1, E_2)$  is a **reducible** pair (i.e. there is no genus 2 curve on  $E_1 \times E_2$ ).

**Problem 1b:** For each exceptional quadratic form  $q$ , classify the pairs  $(E_1, E_2)$  of elliptic curves with  $q_{(E_1, E_2)} \sim q$ .

**Note:** While **Problem 1b** is relatively simple, **Problem 1a** is quite difficult, for it is closely connected to a **Conjecture of Gauss**.

## 2. Main Results

**Theorem 1 (Non-CM Case).** (a) The form  $q(x) = dx^2$  is exceptional if and only if  $d \not\equiv 3(4)$  and  $4d$  is an idoneal (or suitable or convenient) number.

Thus, if Gauss's Conjecture (or if GRH) is true, then  $q$  is exceptional  $\Leftrightarrow$  either  $d = 1$  or  $d$  is one of the 20 known idoneal numbers  $d \equiv 2, 4, 6 \pmod{8} \Leftrightarrow d \in L :=$

$\{1, 2, 4, 6, 10, 12, 18, 22, 28, 30, 42, 58, 60, 70, 78, 102, 130, 190, 210, 330, 462\}$ .

(b) Given an integer  $d \geq 1$  (exceptional or not), the pairs  $(E_1, E_2)$  with  $q_{E_1, E_2} \sim dx^2$  are parametrized by the (non-CM) points of the modular curve  $X_0(d)$ .

**Remark:** It follows from the work of Weinberger (1973) that there are either 21 or 22 exceptional  $q$ 's.

**Theorem 2 (CM Case).** If  $r = 2$ , then there are precisely 15 exceptional forms, and these come from 46 (distinct) pairs of CM-curves  $(E_1, E_2)$ .

**Remarks:** 1) If we restrict attention to those CM-curves for which  $\text{End}(E_i)$  is a maximal order, then there are only 4 pairs of curves/forms, as was proven by Hayashida and Nishi (1965).

2) The proof of Theorem 2 uses Theorem 1 and Weinberger's "at most one more" theorem, but does not involve any unproven hypotheses.

### 3. A Conjecture of Gauss

**Definition:** An idoneal number is an integer  $d \geq 1$  such that  $Cl(-4d) = \text{Pic}(\mathbb{Z}[\sqrt{-d}])$  is an elementary abelian 2-group.

Note that by Gauss's genus theory we have that

$$d \text{ is idoneal} \quad \Leftrightarrow \quad c(x^2 + dy^2) = 1,$$

where  $c(f)$  denotes the number of equivalence classes of forms in the genus of  $f$ . (Watson calls  $c(f)$  the class number of  $f$ .)

**Notes:** 1) The term idoneal was introduced by Euler (1772), who used such numbers to find large primes. It is a non-trivial fact that his definition is equivalent to the one above; cf. Cox's book, *Primes of the form  $x^2 + ny^2$* , p. 61.

**Conjecture (Gauss, DA, Art. 303):**  $d$  is an idoneal number if and only if it is one of the 65 numbers found by Euler. In particular, if  $d$  is idoneal, then  $d \leq 1848$ .

– the fact that  $d$  is bounded was proved by Chowla (1934) by extending Heilbronn's method (to show that  $h(-d) \rightarrow \infty$ ).

– in the 1930's, the conjecture was studied by Dickson and his students (e.g. N. Hall), who obtained useful partial results.

– Swift (1948): conjecture is true for  $d \leq 10^7$  (computations were carried out using Lehmer's linear congruence machine)

– Weinberger (1973) proved:

1) there is at most one fundamental counterexample (this requires Lehmer's computations for  $d < 2.1 \times 10^{11}$ )

2) GRH (Generalized Riemann Hypothesis)  $\Rightarrow$  there are no counterexamples, i.e. the conjecture is true.

## 4. Gauss's Problem: Generalizations

**Note:** As will be explained below, **Problem 1a** for **non-CM** curves naturally leads to classifying **idoneal** numbers, i.e. to Gauss's Conjecture. For **CM** curves, however, we need a **generalization** of this to **ternary forms**. One such generalization is:

**Watson's Problem:** Classify the positive definite forms  $q$  with  $c(q) = 1$ .

In **1965-80**, **Watson** studied this problem for  $r \geq 3$  variables (and stated that the case  $r = 2$  is impossible):

- 1) There exist only **finitely many** classes of positive definite primitive forms with  $c(q) = 1$  (and **none** for  $r \geq 11$ ).
- 2) For  $r = 3$ ,  $\exists$  precisely **790** classes of such forms.

Here is another generalization:

**Problem 2.** Classify the positive definite quadratic forms  $q$  in  $r \geq 2$  variables which satisfy the property:

$$(1) \quad q' \rightarrow 1, \quad \text{for all } q' \in \text{gen}(q),$$

where  $\text{gen}(q)$  is the **genus** of  $q$  (i.e. the set of forms which are **genus-equivalent** to  $q$ ) and  $q' \rightarrow 1$  means that  $q$  represents 1.

**Remarks:** 1) Clearly, if  $q \rightarrow 1$  and  $c(q) = 1 \Rightarrow$  (1) holds. Thus, the solutions of **Problem 2** include those solutions  $q$  of **Watson's Problem** for which  $q \rightarrow 1$ .

2) If  $r = 2$ , then **Problem 2** is essentially equivalent to **Gauss's Problem** (or Conjecture) and to **Watson's Problem** (because  $q \rightarrow 1 \Leftrightarrow q \sim 1_\Delta$ ).

## 5. The Refined Humbert Invariant

**Aim:** Translate the **existence** of genus 2 curves into a problem about **quadratic forms**.

**Let**  $A$  be an abelian surface ( $\dim(A) = 2$ ),  
 $\text{NS}(A) = \text{Div}(A)/\equiv$  its **Néron-Severi group**.

**Observation:** If  $C \subset A$  is a (smooth) curve of genus 2, then  $C^2 = 2$  and so its class  $\theta_C = cl(C) \in \text{NS}(A)$  is a **principal polarization** on  $A$ .

The **converse** is false: not every  $\theta \in \mathcal{P}(A) := \{\text{principal polarizations on } A\}$  comes from an irreducible genus 2 curve.

**Definition:** The **refined Humbert invariant** of a principally polarized abelian surface  $(A, \theta)$  is the (positive definite) quadratic form  $q_\theta$  on  $\text{NS}(A, \theta) := \text{NS}(A)/\mathbb{Z}\theta$  defined by

$$(2) \quad q_\theta(D) = (D.\theta)^2 - 2D^2, \quad \text{for } D \in \text{Div}(A).$$

**Remark:** In [ECAS] (1994) I showed how  $q_\theta$  is related to (and refines) the classical **Humbert invariant**  $\Delta(A, \theta) \in \mathbb{N}$ .

**Key Lemma:** Let  $\theta \in \mathcal{P}(A)$ . Then  $\theta = cl(C)$ , for some (smooth) genus 2 curve  $C$  on  $A \Leftrightarrow q_\theta(D) \neq 1, \forall D \in \text{Div}(A)$ .

**Proof (Sketch)** ( $\Leftarrow$ ) If not, then by a theorem of Weil(1957),  $\theta = cl(D)$ , where  $D = E_1 + E_2$ , and the  $E_i$ 's are elliptic curves with  $(E_1.E_2) = 1$ . But then  $q_\theta(E_i) = 1$ , contradiction.

( $\Rightarrow$ ) If  $\theta = cl(C)$  but  $q_\theta(D) = 1$ , then by [ECAS] we have that  $D \equiv E_1$  and  $\theta - D \equiv E_2$ , where the  $E_i$  are elliptic curves. Thus  $\theta \equiv E_1 + E_2 \not\equiv C$  (by Riemann-Roch), contradiction.

**Consequence:** The **existence** (or non-existence) of genus 2 curves  $C$  on  $A$  can be translated to a problem about the **quadratic form**  $q_A$  associated to the **intersection pairing** on  $\text{NS}(A)$ , i.e.

$$q_A(D) = \frac{1}{2}D^2, \quad \text{for all } D \in \text{NS}(A).$$

**Corollary:** If  $A$  is an abelian surface, then there is **no** smooth genus 2 curve on  $A$  if and only if

$$(3) \quad (q_A)_\theta \text{ represents } 1, \text{ for every } \theta \in \text{NS}(A) \text{ with } q_A(\theta) = 1.$$

**Note:** If  $A = E_1 \times E_2$ , then

$$q_A \sim xy \perp (-q_{E_1, E_2}),$$

where  $xy$  is the quadratic form defined by the **hyperbolic plane** and  $q_{E_1, E_2}$  is (as above) the quadratic form defined by the degree map.

**Definition:** A positive definite quadratic form  $q$  is called **exceptional** if the form  $Q := xy \perp (-q)$  satisfies (3), i.e.

$$Q_\theta \rightarrow 1 \quad \text{for all } \theta \text{ with } Q(\theta) = 1.$$

Here, following **Watson**, “ $q \rightarrow 1$ ” means “ $q$  represents 1”, and  $Q_\theta$  is defined by replacing (the role of)  $q_A$  in (2) by  $Q$ .

**Note:** By the above Corollary, this definition is **consistent** with the previous use of the term “exceptional” (which was defined only for the quadratic form  $q_{E_1, E_2}$  since its definition used a geometric property of  $E_1 \times E_2$ ).

## 6. Exceptional Forms: the Case $r = 1$

**Proposition 1:** Let  $q(z) = dz^2$ , where  $d > 0$ , and put  $Q(x, y, z) = xy - dz^2$ . Then:

(a) If  $d \equiv 3 \pmod{4}$ , then  $\exists \theta$  with  $Q(\theta) = 1$  such that  $Q_\theta$  is not primitive. In particular,  $Q_\theta \not\rightarrow 1$ , so  $q$  is **not exceptional**.

(b) If  $d \not\equiv 3 \pmod{4}$ , then

$$\{Q_\theta : Q(\theta) = 1\} = \text{gen}(1_{-16d})$$

is the **principal genus** of discriminant  $-16d$ . Thus  $q$  is exceptional  $\Leftrightarrow c(1_{-16d}) = 1 \Leftrightarrow 4d$  is an idoneal number.

**Proof.** Preprint [Jacobians] = Jacobians isomorphic to ...

**Corollary:** The form  $dz^2$  is exceptional  $\Leftrightarrow$

$$d \in L^* := \{d \geq 1 : c(1_{-16d}) = 1 \text{ and } d \not\equiv 3(4)\}.$$

**Remarks:** 1) It is easy to see (**Gauss**) that  $L \subset L^*$ , and that equality holds if **Gauss's Conjecture** is true.

If, however, there is a  $d^* \in L^* \setminus L$ , then  $d^* \equiv 2, 4, 6 \pmod{8}$  and by **Hall (1940)**  $d^*$  is squarefree. Thus  $-4d^*$  is a fundamental discriminant, and then by **Weinberger** it is the unique (fundamental) counterexample to **Gauss's Conjecture**. Thus  $L^* = L \cup \{d^*\}$  in this case.

2) This proves the first part of **Theorem 1**. The second part is essentially trivial, for if  $E_1$  has no CM, then

$$\begin{aligned} q_{E_1, E_2} \sim dx^2 &\Leftrightarrow \exists h : E_1 \rightarrow E_2, \text{Ker}(h) \text{ cyclic of degree } d \\ &\Leftrightarrow (h : E_1 \rightarrow E_2) \in X_0(d)(K). \end{aligned}$$

## 7. Exceptional Forms: the Case $r = 2$

**Let**  $q = (a, b, c)$  be a positive definite binary quadratic form, i.e.

$$q(x, y) = ax^2 + bxy + cy^2,$$

$$d = b^2 - 4ac \text{ its discriminant}$$

$$Q(x, y, z, w) = xy - q(z, w)$$

$$1_q(x, y, z) = x^2 + 4q(y, z)$$

**Proposition 2.** (a) If  $d \equiv 0 \pmod{4}$  and  $q \rightarrow a$ , where  $a \equiv 3 \pmod{4}$ , then there is a  $\theta$  with  $Q(\theta) = 1$  such that  $Q_\theta$  is not primitive. In particular,  $q$  is **not exceptional**.

(b) If  $d \equiv 1 \pmod{4}$  or if  $q \not\rightarrow a$ , for any  $a \equiv 3 \pmod{4}$ , then

$$\{Q_\theta : Q(\theta) = 1\} \subset \text{gen}(1_q)$$

Thus, if  $c(1_q) = 1$ , then  $q$  is exceptional.

**Main Theorem.** If  $q$  is as in Proposition 2(b), then **TFAE**:

- (i)  $q$  is exceptional;
- (ii)  $1_q$  satisfies property (1) of Problem 2;
- (iii)  $c(1_q) = 1$ ;
- (iv)  $q \in \mathcal{L} := \{k(1, 1, 1) : k = 1, 2, 4, 6, 10\}$   
 $\cup \{k(1, 0, 1) : k = 1, 2, 6\}$   
 $\cup \{(1, 1, 2), (1, 1, 4)\}$   
 $\cup \{2(1, 1, c) : c = 3, 9\}$   
 $\cup \{2(1, 0, c) : c = 2, 5\}$   
 $\cup \{2(2, 0, 3)\}.$

**Proof (Sketch).** (iii)  $\Rightarrow$  (ii)  $\Rightarrow$  (i): trivial (by Proposition 2(b)).

(i)  $\Rightarrow$  (iv): If  $q$  is exceptional, then using [Proposition 1\(b\)](#), one proves that  $q$  satisfies:

$$(i') \quad q \rightarrow n, n < |d| \Rightarrow n \in L^*.$$

Using [Weinberger's](#) result, this can be [sharpened](#) to

$$(i'') \quad q \rightarrow n, n < |d| \Rightarrow n \in L.$$

Indeed, if  $q = (a, b, c)$  is (wlog) reduced, then by (i') we have  $a, c, a+b+c \in L^*$ . But if  $c \in L^* \setminus L = \{d^*\}$ , then  $a+b+c > c = d^*$ , so  $a+b+c \notin L^*$ , contradiction. Thus,  $a, c \leq 462$ , so  $|d| \leq 4 \cdot 462^2 < 10^6 < d^*$ , and hence (ii'') holds.

We therefore have only [finitely many](#)  $d$ 's to consider, and by a somewhat [tedious](#) argument (using (ii'')) we obtain that  $q \in \mathcal{L}$ .

(iv)  $\Rightarrow$  (iii) For each  $q \in \mathcal{L}$ , apply the [mass formula](#) of [Eisenstein/Smith/Brandt](#) to the ternary form  $1_q$ . This has the form

$$M(1_q) = \frac{-kd'}{6 \cdot 2^\nu} \prod_{p|\delta} \left(1 - \frac{1}{p^2}\right) \prod_{p|kd'} \left(1 + \left(\frac{d'}{p}\right) \frac{1}{p}\right) \left(1 + \left(\frac{-4k^2 d'}{p}\right) \frac{1}{p}\right)$$

where  $k = \text{cont}(q)$ ,  $d' = \frac{d}{k^2}$ ,  $\delta = \text{gcd}(4k^2, d')$ , etc. and

$$M(1_q) = \sum_{f \in \text{gen}(1_q)/\sim} \frac{1}{|\text{Aut}(f)|}.$$

For each  $q \in \mathcal{L}$  one calculates that  $M(1_q) = \frac{1}{|\text{Aut}(q)|} = \frac{1}{|\text{Aut}(1_q)|}$ , and so it follows that  $c(1_q) = 1$ .

## 8. References

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

**[Jacobians]** Jacobians isomorphic to a product of two elliptic curves. Preprint, 39pp.