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) $\longrightarrow$ 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 depends only on the nature of the quadratic form

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

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

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

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

By using deep results in number theory (due to Chowla and Heilbronn), it is possible to prove:

Theorem 1: There exist only finitely many equivalence classes of positive definite quadratic forms q in $r \le 2$ variables such that $q \sim q_{E_1,E_2}$, for some reducible pair (E_1, E_2).

Problem 1a: Classify the (finitely many) "exceptional" quadratic forms of Theorem 1.

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. A Conjecture of Gauss

Recall: *If* $K = \mathbb{Q}(\sqrt{-d})$ *is an imaginary quadratic field with* $h_K = 1$*, then* $d \le 163$ *(provided that* d *is squarefree).*

– this was "conjectured" by Gauss (1801)

– the fact that d is bounded was proved by Heilbronn (1934)

– the conjecture was proved by Heegner (1952), Stark (1967),. . .

However: the above conjecture is only a portion of what he actually conjectured in Article 303 of the *Disquisitiones Arithmeticae*. Translated to number fields, his conjecture is:

If $K = \mathbb{Q}(\sqrt{-d})$ *is an imaginary quadratic field whose class group* $Cl(\mathfrak{O}_K)$ *is an elementary abelian 2-group, then* $d \le 5460$.

– the fact that d is bounded was proved by Chowla (1934) by extending Heilbronn's method.

– 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 $d \le 10^7$ (computations were carried out using Lehmer's linear congruence machine)

– Weinberger (1973) proved:

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

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

Note: Chowla is the only person who mentions that this is (essentially) a conjecture of Gauss.

Conjecture of Gauss: If q is a primitive, positive definite binary quadratic form of discriminant $\Delta(q) = -4D$, then

$$c(q) = 1 \Leftrightarrow D \text{ is one of the } 65 \text{ idoneal numbers of Euler.}$$

Here (cf. Watson), $c(q)$ is the class number of the form q, i.e.

$$c(q) = \#(\text{equivalence classes of forms in the genus of } q).$$

Remarks: Watson studied in 1965-80 the "$c(q) = 1$" 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.

Theorem 2 (Non-CM Case). If $r = 1$, then there are either 21 or 22 exceptional forms $q(x) = dx^2$. If Gauss's Conjecture (or if GRH) is true, then q is exceptional $\Leftrightarrow$ either $d = 1$ or d is one of the 20 idoneal numbers $d \equiv 2, 4, 6 \pmod 8$ $\Leftrightarrow d \in L :=$

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

Moreover, to each such d belongs an infinite family of pairs (E_1, E_2); these are parametrized by the (non-CM) points of the modular curve $X_0(d)$.

Theorem 3 (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).

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

3. The Refined Humbert Invariant

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

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

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

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

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

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

Remark: In [ECAS] (1994) I showed how q_θ 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 $A \Leftrightarrow q_\theta(D) \neq 1, \forall D \in \mathrm{Div}(A)$.

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 $\mathrm{NS}(A)$, i.e.

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

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

(2) $(q_A)_\theta$ represents 1, for every $\theta \in \mathrm{NS}(A)$ 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 (2), i.e.

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

Here, following Watson, "$q \to 1$" means "q represents 1", and Q_θ is defined by replacing (the role of) q_A in (1) 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 $E_1 \times E_2$).

4. Gauss's Problem: A Generalization

Note: As was mentioned above, one such generalization was studied (and solved for $r = 3$) by Watson:

Classify the positive definite forms q with $c(q) = 1$.

Here is another generalization:

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

$$q' \to 1, \quad \text{for all } q' \in \text{gen}(q), \tag{3}$$

where $\text{gen}(q)$ denotes the genus of q, i.e. the set of forms which are genus-equivalent to q.

Remarks: 1) Clearly, if $q \to 1$ and $c(q) = 1 \Rightarrow$ (3) holds. Thus, the solutions of Problem 2 include the solutions q of Watson's Problem with $q \to 1$.

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

5. 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_θ is not primitive. In particular, $Q_\theta \not\to 1$, so q is not exceptional.

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

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

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

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) By Gauss we know 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 2. The second part is essentially trivial, for if E_1 has no CM, then

$$q_{E_1,E_2} \sim dx^2 \;\Leftrightarrow\; \exists h : E_1 \to E_2, \mathrm{Ker}(h) \text{ cyclic of degree } d$$
$$\Leftrightarrow\; (h : E_1 \to E_2) \in X_0(d)(K).$$

6. Exceptional Forms: the Case $r = 2$

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

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

$d = b^2 - 4ac$ 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 $q \to a$, where $a \equiv 3 \pmod 4$, then there is a θ with $Q(\theta) = 1$ such that Q_θ is not primitive. In particular, q is not exceptional.

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

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

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 (3) 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′) $q \to n, n < |d| \Rightarrow n \in L^*$.

Using Weinberger's result, this can be sharpened to

(i″) $q \to n, n < |d| \Rightarrow n \in L$.

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, $a, c \le 462$, so $|d| \le 4 \cdot 462^2 < 10^6 < d^*$, 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

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

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

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

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

This proves the Main Theorem and hence also the first part of Theorem 3. For the second part, use:

Proposition 3. Let $E_1 \sim E_2$ be two elliptic curves with CM by the imaginary quadratic field k, so $\mathrm{End}(E_i)$ is an order in k of discriminant $D_i = f_i^2 d_k$, where d_k is the discriminant of k. Then

$$\begin{aligned} \mathrm{disc}(q_{E_1,E_2}) &= -\mathrm{lcm}(D_1, D_2), \\ \mathrm{cont}(q_{E_1,E_2})^2 &= \frac{\mathrm{lcm}(D_1, D_2)}{\mathrm{gcd}(D_1, D_2)}. \end{aligned}$$

Remark: From the above we see that for a given binary form q, there are only finitely many pairs (E_1, E_2) of elliptic curves such that $q_{E_1,E_2} \sim q$. These can be found precisely by using an explicit formula for q_{E_1,E_2} in terms of the ideals "defining" the E_i relative to a common curve E (i.e. such that $E_i = E/I_i$).

7. Connection with Moduli Spaces

Let A_2 denote the moduli space of princ. pol. abelian surfaces, M_2 the moduli space of smooth genus 2 curves; $M_2 \subset A_2$ via the Torelli map: $C \mapsto (J_C, \theta_C)$.

Definition: Let q be a (positive definite) quadratic form. The generalized Humbert variety associated to q is the subset of A_2 defined by

$$H(q) = \{(A,\theta) \in A_2(K) : q_{(A,\theta)} \to q\}$$

Here $q_{(A,\theta)}$ is the refined Humbert invariant of (A,θ), and "$q_{(A,\theta)} \to q$" means that $q_{(A,\theta)}$ primitively represents the form q.

Examples: 1) The classical Humbert surface of discrim. Δ is

$$H_\Delta = H(\Delta x^2), \tag{4}$$

as was explained in [ECAS]. Thus, by the Key Lemma we have

$$H_1 = A_2 \setminus M_2, \tag{5}$$

which (for $K = \mathbb{C}$) is a theorem of Biermann(1886) and Humbert(1901).

2) If m and n are distinct positive integers, then

$$H_m \cap H_n = \bigcup H(q),$$

where the union runs over the (finitely many) equivalence classes of positive definite binary quadratic forms q with $q \to m$ and $q \to n$.

Theorem 5: (a) Let $q \in \mathrm{gen}(1_{-16d}) \cup \mathrm{gen}(4 \cdot 1_{-4d})$ be a positive definite binary quadratic form of discriminant $-16d$ in the principal genus. If $q \not\to 1$, then $H(q)$ is a curve lying completely in M_2, and every $C \in H(q)$ has the property that $J_C \simeq E_1 \times E_2$, for some elliptic curves E_1 and E_2.

(b) Conversely, if C is a curve with $J_C \simeq E_1 \times E_2$, for some elliptic curves E_1 and E_1, then $C \in H(q)$, for some binary form q as in part (a).

(c) If q is in part (a), then there are morphisms $\mu_s : X_0(d) \to H(q)$ which are either of degree 2 or 4. Thus, $H(q) \sim X_0(d)^+$ or to a degree 2 quotient thereof by an Atkin-Lehner involution. Moreover, the latter case occurs if and only if q is an ambiguous form.

Remark: In [Jacobians], a curve which appears in

$$T(d) = \bigcup_{q \in \mathrm{gen}(1_{-16d}) \cup \mathrm{gen}(4 \cdot 1_{-4d})} H(d),$$

is called a curve of type d. Thus, Theorem 2 $\Leftrightarrow$

Theorem 2′: There is no curve of type d $\Leftrightarrow d \in L^*$.

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.