Idoneal Numbers and some Generalizations

Ernst Kani

To Paulo Ribenboim on his 80^{th} Birthday

1 Introduction

Around 1778 Euler discovered a method by which he could use certain numbers to find large primes. However, not every number is suitable for this method and hence he gave the name *numeri idonei* (= suitable, convenient numbers) to those numbers that are suitable. Gauss also considered idoneal numbers from a related but slightly different point of view. After Gauss, many people considered idoneal numbers, often without being aware of the classical connection.

Recently it was discovered that idoneal numbers play an important role in studying certain moduli problems of genus 2 curves [34], and that these questions naturally led to certain generalizations of idoneal numbers [35]. In order to derive these results, it was necessary to take another look at the classical results about idoneal numbers.

In reading over the literature on idoneal numbers, I was surprised to find a multitude of misleading or erroneous statements. While some of these have been discussed in various sources (Grube [22], Steinig [45] or Weil [54]), many others have not been mentioned, but instead were reproduced by other authors. It thus seems worthwhile to give a survey of the main results on idoneal numbers and to address (and to correct) some of these misleading statements; cf. Remarks 7, 13, 21, 24, 26 and §2.5.

In section 3 we present some characterizations of idoneal numbers. One of these (Theorem 32) is due to Weber, and is closely connected with another characterization of idoneal numbers which is mentioned in Frei [17]. Another characterization (Proposition 29) was suggested by the connection between idoneal numbers and genus 2 curves (cf. §4) and can be used to (partially) repair an error in Swift [46].

Some generalizations of idoneal numbers are explored in §5. Some of these were studied by Weinberger [55], Miyada [39], Watson [48] and others, but other generalizations such as Problems 42 and 43 are (as far as I know) new, and were suggested by the study of genus 2 curves, as will be explained in §6. There is a surprising connection between these problems; cf. Theorem 44.

I would like to thank Claude Levesque for his interest and for the helpful comments on this paper. In addition, I would like to gratefully acknowledge receipt of funding from the Natural Sciences and Engineering Research Council of Canada (NSERC).

It is a pleasure to dedicate this paper to my dear colleague (emeritus) Paulo Ribenboim for his 80th birthday, particularly since he discussed idoneal numbers at length in his paper [42].

2 Idoneal numbers: a historical overview

2.1 Euler

As was mentioned in the introduction, idoneal numbers were discovered around 1778 by Euler, who used then as a tool for testing large numbers for primality. One way to define them is as follows (cf. Cox [10], p. 65):

Definition. An integer $n \geq 1$ is called *idoneal* if it has the following property: if m is an odd number prime to n which is properly represented by $q(x, y) = x^2 + ny^2$, and if the equation $q(x, y) = m$ has only one solution with $x, y \geq 0$, then m is a prime number.

While this definition is not identical to the one that Euler gave, it is similar (and equivalent) to it. Indeed, Euler's original definition is somewhat confusing and is often misstated. The problems with Euler's definition and how to correctly interpret it are discussed in detail in Steinig [45]. (See also Weil [54], pp. 222-226.)

Euler discovered that there are precisely 65 idoneal numbers $n \leq 10,000$, the largest being $n = 1848$. More precisely, he proved (by direct computation):

Theorem 1 *If* $1 \leq n \leq 10,000$*, then* n *is idoneal if and only if* n *is one of the following* 65 *numbers:*

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15,
16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45,
48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112,
120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280,
312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848

The fact that he could not find any other idoneal numbers came as a complete surprise to him: *"J'ai donc été bien surpris de me voir arrêté au dernier 1848"*, as he wrote Béguelin in [14]. Later he referred to this phenomenon as a "paradox" in [16]. However, he was convinced that there are no others, for he asserted at the end of [15]: *"Quia autem usque ad decies mille nulli allia se mihi obtulerunt, multo magis verisimillimum videtur, post hunc terminum nullos praetera existere…"*. In other words, we have:

Conjecture 2 (Euler) *The largest idoneal number is* $n = 1848$.

In order to convince himself of the validity of this conjecture, Euler [15] stated and proved ten theorems about idoneal numbers. Many of these show that if we impose extra conditions on n, then there are only finitely many such idoneal numbers. These ten theorems are the following:

Theorem 3 (Euler) 1. *If n is an idoneal number which is a square, then $n = 1, 4, 9, 16$, or 25.*

2. *If $n \equiv 3 \pmod 4$ is idoneal, then $4n$ is also idoneal.*

3. *If $n \equiv 4 \pmod 8$ is idoneal, then so is $4n$.*

4. *If $\lambda^2 n$ is idoneal, then so is n.*

5. *If $n \equiv 2 \pmod 3$ is idoneal, then so is $9n$.*

6. *If $n \equiv 1 \pmod 4$ is idoneal and $n \neq 1$, then $4n$ is not idoneal.*

7. *If $n \equiv 2 \pmod 4$ is idoneal, then so is $4n$.*

8. *If $n \equiv 8 \pmod{16}$ is idoneal, then $4n$ is not idoneal.*

9. *If $n \equiv 16 \pmod{32}$ is idoneal, then $4n$ is not idoneal.*

10. *If n is idoneal and if there is a prime p with $p^2 < 4n$ such that $n + a^2 = p^2$, for some $a \in \mathbb{Z}$, then $4n$ is not idoneal.*

The above numbering scheme follows Euler's; thus, part 1. above is *Theorema 1* in [15], etc. Note that although the assertions are all correct, Euler's proofs of these results were not; they were criticized and corrected by Grube [22].

Euler himself realized that the property of being idoneal is really a property of quadratic forms, and so he generalized this concept to other binary quadratic forms (of discriminant $-4n$). However, Euler noticed that one doesn't really get anything new this way, for he proves in [15], p. 276, that a form f of discriminant $-4n$ is idoneal if and only if n is idoneal.

2.2 Gauss

As is well-known, Gauss [20] studied binary quadratic forms in his *Disquisitiones Arithmeticae* in great depth. For the convenience of the reader (and to introduce some notation) we briefly recall some of his main results. Here we shall not completely follow Gauss's terminology but instead use current terms (cf. [7] or [10]).

1) Following Lagrange, Gauss says in Article 158 that two binary quadratic forms q_1 and q_2 are (properly) *equivalent* (notation: $q_1 \sim q_2$) if there is a linear coordinate transformation $T \in \mathrm{SL}_2(\mathbb{Z})$ which transforms q_1 into q_2, i.e. if we have $q_1(T(x, y)) = q_2(x, y)$. It is easy to see that the *discriminant* $\Delta(q) := b^2 - 4ac$ of a form $q(x, y) = ax^2 + bxy + cy^2$ does not change under such transformations. (Note that Gauss always assumed that b is even and called $\frac{\Delta}{4}$ the *determinant* of the form, but this restriction is not necessary (nor desirable) for the theory.)

In Articles 175 and 191 he uses Lagrange's reduction theory to prove Lagrange's fundamental theorem that there are only finitely many equivalence classes of forms with fixed discriminant Δ. The number $h(\Delta)$ of equivalence classes of *primitive* forms of discriminant Δ is now called the *class number* of Δ.

2) In Article 231 he introduces the important (new) notion of the *genus* of a binary quadratic form q: this set consists of those forms q' whose values have the same quadratic characters (and the same signature) as q. (A nice discussion of this concept can be found in Cox [10], pp. 58-59; see also Buell [7], ch. 4.) The key point here is that the primes $p \nmid \Delta$ which are represented by some form in a fixed genus can be characterized by congruence conditions modulo Δ.

It is immediate from the definition (and from the finiteness of $h(\Delta)$) that the genus of q consists of finitely many equivalence classes of forms. We denote this set of equivalence classes by $\mathrm{gen}(q)$ and write $c(q) = \#(\mathrm{gen}(q))$.

3) In Articles 234–249, Gauss introduces a composition of quadratic forms and shows that this makes the set $Cl(\Delta)$ of equivalence classes of primitive quadratic forms of discriminant Δ into (what we now call) an abelian group. Its identity is (the class of) the *principal form* 1_Δ which is defined by $1_\Delta(x,y) := x^2 - \frac{\Delta}{4}y^2$, if Δ is even, and by $1_\Delta(x,y) = x^2 + xy + \frac{1-\Delta}{4}y^2$, if Δ is odd.

From this it follows easily that the *principal genus* $\mathrm{gen}(1_\Delta)$ is a subgroup of $Cl(\Delta)$, and that each genus $\mathrm{gen}(q) = \mathrm{gen}(1_\Delta)q$ is a coset in $Cl(\Delta)$. Thus, each genus has the same number of elements, so $c(q) = c(1_\Delta) =: c(\Delta)$, for all $q \in Cl(\Delta)$; cf. Article 252.

4) In Article 256 Gauss notes that there is an explicit relation between the class numbers $h(\Delta)$ and $h(t^2\Delta)$. In the case that $t = p$ is a prime (and $\Delta < 0$), we have

$$h(p^2\Delta) \;=\; \frac{1}{c_\Delta}\left(p - \left(\frac{\Delta}{p}\right)\right)h(\Delta), \tag{1}$$

where $c_\Delta = 1$ if $\Delta < -4$ (and $c_{-4} = 2$, $c_{-3} = 3$) and $\left(\frac{\Delta}{p}\right)$ denotes the Kronecker-Legendre symbol. Note that this formula is also correct if Δ is an odd discriminant or if $p = 2$; cf. Cox [10], p. 148.

4) In Articles 266–285 he develops a theory of *ternary forms*, which he then uses in Article 286 to prove the fundamental result that a binary quadratic form q lies in the principal genus if and only if q is a square in $Cl(\Delta)$, i.e.

$$\mathrm{gen}(1_\Delta) \;=\; Cl(\Delta)^2. \tag{2}$$

From this it follows that the number $g(\Delta)$ of genera of primitive forms of discriminant Δ is $g(\Delta) = [Cl(\Delta) : Cl(\Delta)^2] = |Cl(\Delta)[2]|$, where $Cl(\Delta)[2]$ denotes the subgroup of *ambiguous* classes, i.e. $Cl(\Delta)[2] = \{q \in Cl(\Delta) : q^2 \sim 1_\Delta\}$. The order of this subgroup is easily computed (cf. Article 257), and so Gauss obtains the formula

$$g(\Delta) \;=\; 2^{\omega(\Delta)-1+\varepsilon(\Delta)}, \tag{3}$$

where $\omega(\Delta)$ denotes the number of distinct prime divisors of Δ and $\varepsilon(\Delta) = 1$ if $\Delta \equiv 0 \pmod{32}$, $\varepsilon = -1$ if $\Delta \equiv 4 \pmod{16}$ and $\varepsilon(\Delta) = 0$ otherwise. (Again, this formula is also true for odd discriminants; cf. [10], p. 52.)

5) In Article 303, Gauss presents a table of 103 even negative discriminants $\Delta < 0$ which he groups into 9 lists according to their *type* $(g(\Delta), c(\Delta))$. (His term for this pair is "classification".) The 9 types that he considers are: $(2^r, 1)$ with $0 \leq r \leq 4$, $(2, c)$ with $c = 2, 3, 7$ and $(1, 5)$. In his discussion of this table he states:

"Since the table from which we drew these examples has been extended far beyond the largest determinants that occur here and since it furnishes no others belonging to these classes, there seems to be no doubt that the preceding series do in fact terminate, and by analogy it is permissible to extend the same conclusion to any other classifications. [...] *However,* rigorous *proofs of these observations seem to be very difficult."*

Thus, since $h(\Delta) = g(\Delta)c(\Delta)$ has only finitely many factorizations, this statement is equivalent to the following two conjectures:

Conjecture 4 (Gauss) (a) *For each $n \geq 1$, there are only finitely many discriminants $\Delta < 0$ such that $h(\Delta) = n$.*

(b) *For each of the* 9 *types (g, c) listed is the table we have $|\frac{\Delta}{4}| \leq 1848$.*

It is interesting to note that while the first conjecture was proved by Heilbronn [27] in 1934, the second was only established a few years ago. (It follows from Watkin's classification [50] of all (fundamental) discriminants $\Delta < 0$ with $h(\Delta) \leq 100$.)

At the end of Article 303, Gauss augments his previous remarks by the following two observations:

(i) The discriminants of type $(2^r, 1)$ that are listed in his table (i.e. $r \leq 4$) are precisely those of the form $-4n$, where n is one of the 65 idoneal numbers of Euler.

(ii) The discriminants of type $(2^r, 1)$ for $r > 4$ do not seem to exist.

Thus, in view of his earlier Conjecture 4(b), these statements amount to the following conjecture:

Conjecture 5 (Gauss) *If $c(-4n) = 1$, then $n \leq 1848$.*

This conjecture has not yet been completely settled (even though Buell [7] claims the opposite on p. 81). However, due to the work of Chowla and Weinberger, this statement has "almost" been proved, as will be explained in §2.6 below.

It is perhaps useful to observe that Gauss, in referring to Euler's work, only quotes Euler's letter [14] because, as R. Fueter points out in the introduction to Euler's Collected Works (*Opera Omnia*, Ser. I, v. 4), Gauss did not have access to Euler's papers [15] and [16] since they were only published after 1801. Gauss says:

"The illustrious Euler (Nouv. mém. Acad. 1776, p. 338) has already singled out these 65 numbers (under a slightly different aspect and with a criterion that is easy to demonstrate; we will mention it later on.)"

In Article 334 he explains this parenthetic comment in more detail and presents a variant of Euler's method on how to use the 65 idoneal numbers for finding primes.

2.3 Grube

In his beautiful but often overlooked paper, Grube [22] analyses Euler's results on idoneal numbers by using Gauss's theory of binary quadratic forms. In particular, it follows from his work that Euler's Conjecture 2 and Gauss's Conjecture 5 are, in fact, equivalent. More precisely, he establishes the following fundamental connection between idoneal numbers and discriminants with one-class genera:

Theorem 6 (Grube) *An integer $n \geq 1$ is an idoneal number if and only if $c(-4n) = 1$, i.e. if and only if each genus of forms of discriminant $-4n$ consists of a single class.*

Proof. Cox [10], pp. 61–62.

Remark 7 (a) In his paper, Frei [17] attributes this theorem to Gauss and calls it "Gauss's criterion". He asserts that *"Gauss certainly had a proof of this theorem"*, but does not explain why he believes this. Perhaps he is following R. Fueter, who expresses a similar sentiment in the introduction to Euler's *Opera Omnia*, I, 4.

What is clear from [20] is that Gauss had a proof of the easy implication "$c(-4n) = 1 \Rightarrow n$ is idoneal". Indeed, this is the basis of his primality test in Article 334, and this certainly suffices for his purposes since he knew that the lists agree for $n \leq 10,000$.

However, the other implication is less obvious. Grube himself uses Schering's extension of Dirichlet's Theorem that a primitive binary quadratic form represents infinitely many primes (which Dirichlet had proved in 1840 only for quadratic forms with prime determinant). Grube's proof was criticized by Keller [36] because Schering did not prove his asserted extension, and suggests that this result still is unproved. It is curious that Keller was not aware that this gap had already been filled by Weber [51] in 1882, or that Briggs [5] gave an "elementary" proof in 1954, or that it follows nowadays from the Chebotarev density theorem; cf. [10], p. 188. Note that the Dirichlet/Schering/Weber Theorem is also used by Cox [10] in the above-mentioned proof of Grube's Theorem.

(b) There are several equivalent ways of stating the condition $c(\Delta) = 1$; these are listed in Theorem 3.22 of [10], p. 59. For example, by Gauss's result (2) we see that $c(\Delta) = 1 \Leftrightarrow Cl(\Delta)^2 = \{1\} \Leftrightarrow Cl(\Delta)$ is an elementary abelian 2-group $\Leftrightarrow$ every class in $Cl(\Delta)$ is ambiguous.

Grube points out in §7 of his paper [22] that it is easy to see that if $c(-4n) = 1$ and $n \equiv 3 \pmod 4$, then $n = 3, 7$, or 15, and uses this fact in the proof of his theorem. We thus obtain:

Corollary 8 *If $n \equiv 3 \pmod 4$ is idoneal, then $n = 3, 7$ or 15.*

In his paper, Grube [22] uses the above theorem to give correct and shorter proofs of the ten assertions of Euler about idoneal numbers. In addition, he gives extensions of many of Euler's results. The basic principle in all these is to compare $c(\Delta)$ with $c(t^2\Delta)$, for $t > 1$. Since $c(\Delta) = h(\Delta)/g(\Delta)$, the relations (1) and (3) for $h(\Delta)$ and $g(\Delta)$ yield such a result.

For example, by taking $p = 2$ in (1) and using (3), we obtain (as in [34]) the following result:

Proposition 9 *If $n > 1$, then*

$$c(-16n) = \begin{cases} 2c(-4n), & \text{if } n \equiv 1\,(mod\ 4) \text{ or } n \equiv 0\,(mod\ 8), \\ c(-4n), & \text{otherwise.} \end{cases} \tag{4}$$

Note that this formula contains many of Euler's results, for we have:

Corollary 10 (Euler) (a) *If $n \equiv 0\,(\mathrm{mod}\ 8)$ or $n \equiv 1\,(\mathrm{mod}\ 4)$, $n > 1$, then $4n$ is not idoneal. Thus, if $n \equiv 0\,(\mathrm{mod}\ 32)$ or if $n \equiv 4\,(\mathrm{mod}\ 16)$ and $n > 4$, then n is not idoneal.*

(b) *If $n \equiv 2, 3\,(\mathrm{mod}\ 4)$ or $n \equiv 4\,(\mathrm{mod}\ 8)$, then n is idoneal if and only if $4n$ is idoneal.*

Proof. (a) By (4) we have $c(-16n) = 2c(-4n) \geq 2$, so $4n$ is not idoneal (by Grube's Theorem). The second statement is a restatement of the first.

(b) Here (4) gives $c(-16n) = c(-4n)$, so $4n$ is idoneal if and only if n is.

Remark 11 Note that Corollary 10(a) is actually the combination of Grube's extensions $6'$, $(7 \text{ und } 8)'$ ([22], p. 514) of Euler's *Theoremae* 6, 8 and 9, whereas Corollary 10(b) is equivalent to the combination of Euler's *Theoremae* 2, 3, and 7.

By a similar method Grube proves the following important extension of Euler's *Theorema* 1:

Theorem 12 (Grube) *If n is idoneal and $t^2|n$, then $t^2 = 1, 4, 9, 16$ or 25. Moreover:*

(a) *If n is idoneal and $9|n$, then $n = 9, 18, 45, 72$.*

(b) *If n is idoneal and $25|n$, then $n = 25$.*

(c) *If n is idoneal and $4||n$, then $n = 4, 12, 28, 60$.*

(d) *If n is idoneal and $16|n$, then $n = 16, 48, 112, 240$.*

Remark 13 (a) Note that the above classification does not deal with the case that $8||n$, for by Corollary 10(b) this case is essentially the same as the case $n \equiv 2\,(\mathrm{mod}\ 4)$. Thus, Frei's assertion (cf. [17], p. 58) that *"Grube determined all convenient numbers which are divisible by a square $k^2 \neq 1$"* is not quite correct.

(b) In connection with the above theorem we should note that if n is idoneal and $t^2|n$, then n/t^2 is also idoneal; cf. Euler's *Theorema* 4. By Theorem 6 above, this follows immediately from the more general fact that we always have that $c(\Delta)|c(t^2\Delta)$ which in turn follows in view of (2) immediately from the fact that there is a surjective group homomorphism $Cl(t^2\Delta) \to Cl(\Delta)$, and hence a surjection $Cl(t^2\Delta)^2 \to Cl(\Delta)^2$.

The above results lead to the following classification of large idoneal numbers:

Corollary 14 *If $n > 288$ is an idoneal number, then $n \not\equiv 3 \pmod 4$. Moreover, if $n \equiv 1, 2 \pmod 4$, then n is squarefree, whereas otherwise $\frac{n}{4}$ is a squarefree idoneal number.*

Proof. The first assertion follows from Corollary 8. If $n \equiv 1, 2 \pmod 4$, then n is squarefree by Theorem 12 (a), (b). Now suppose $4|n$, and put $m = \frac{n}{4}$. By Theorem 12 (c), (d) we have $8||n$, i.e. $m \equiv 2 \pmod 4$. Since $m > \frac{288}{4} = 72$, it follows from Theorem 12 (a), (b) that m is squarefree.

Grube also discusses Euler's criterion for testing whether or not a given number n is idoneal, and proposes two variants. In all these criteria, one considers the factorization of the numbers $n + k^2$, for $k = 1, \ldots, [\sqrt{\frac{n}{3}}]$. Euler's criterion is the following:

Criterion 15 (Euler) *An integer $n \geq 1$ is idoneal if and only if for every $k = 1, \ldots, [\sqrt{\frac{n}{3}}]$ with $(k, n) = 1$ we have that $n + k^2 = p$, p^2, $2p$ or 2^s, for some odd prime p and some integer $s \geq 1$.*

Remark 16 Euler states this criterion in the above form in his letter [14], but not in his paper [15] where he leaves out the hypothesis $(k, n) = 1$. Grube [22] points out that this hypothesis cannot be dropped by providing counterexamples; cf. [22], p. 503. He also criticizes Euler's proof of his criterion, and gives a partial correction. Frei [17], p. 57, points out that Grube only proved one direction of this criterion and says, *"whether* [this criterion] *is also sufficient is still an open problem"*.

In order to correct the problems with Euler's criterion, Grube offers the following two variants:

Proposition 17 (a) *An integer $n \geq 1$ is idoneal if and only if for every $b = 1, \ldots, [\sqrt{\frac{n}{3}}]$, and every factorization*

$$n + b^2 = ac \quad \text{with } c \geq a \geq 2b \tag{5}$$

we have that either $a = c$ or $a = 2b$.

(b) *Suppose $n \geq 1$ is squarefree and $n \neq 3, 7, 15$. Then n is idoneal if and only if for every $k = 1, \ldots, [\sqrt{\frac{n}{3}}]$ we have that $n + k^2 = tp$, tp^2, or $2tp$, where $t|n$ and p is an odd prime.*

Remark 18 (a) As Grube remarks, part (a) follows immediately from the classification of (reduced) ambiguous classes ([20], Article 171). More precisely, if there is a factorization $n + b^2 = ac$ with $c > a > 2b$, then $q(x, y) = ax^2 + 2bxy + cy^2$ is a reduced form of discriminant $-4n$ which is not ambiguous, so $c(-4n) > 1$. (Note that if $t := \gcd(a, 2b, c) > 1$, then q/t is a primitive reduced form of discriminant $-4n/t^2$, so $c(-4n/t^2) > 1$ and hence also $c(-4n) > 1$ by Remark 13(b).) Conversely, if $c(-4n) > 1$, then reduction theory and Article 171 show that there exist positive integers a, b, c (with $\gcd(a, 2b, c) = 1$) such that $c > a > 2b$ and $n + b^2 = ac$.

(b) Note that the above proof shows that the condition of part (a) has to be verified only for those factorizations (5) for which $\gcd(a, 2b, c) = 1$.

2.4 Weber and Frobenius

In 1889 Weber [52] pointed out that the class-fields of imaginary quadratic fields pertaining to idoneal numbers play a very special role in this theory (cf. Theorem 32 below). For this reason, he computes all such fields (for the known idoneal numbers). In a footnote on p. 391 he remarks that the fact that there are only 65 idoneal numbers was found by Euler and Gauss *"by induction"* (i.e. by computation) and that it has not yet been completely proved (*"streng bewiesen"*).

There are sporadic references to idoneal numbers (and their equivalents) in textbooks on number theory which were published around 1890. For example, Mathews [38] devotes most of ch. IX to a presentation, based on Gauss, of Euler's primality test. Following Gauss, he gives on p. 263 a table of the 65 known idoneal numbers (sorted according to $g(\Delta)$). Similary, Bachmann [2], p. 253, repeats the assertion of Gauss that there seem to be only 65 (even) discriminants $\Delta < 0$ with $c(\Delta) = 1$. It is interesting to note that Bachmann introduces the notation $H(D)$, $G(D)$ and $K(D)$ for the class number $h(4D)$, the number of genera $g(4D)$ and the number $c(4D)$ of classes in the principal genus, respectively.

In an interesting paper Frobenuis [19] studied, among other things, idoneal numbers n for which $h(-4n) = 2$. His motivation for this was an observation of Euler [13] that for $p = 3, 5, 11, 29$, the numbers $2x^2 + p$ are primes for $|x| < p$. He says that he was not able to find a hint on how Euler proved his results, but is convinced that Euler's starting point for this was given by his idoneal numbers. (*"Über den Weg, der Euler zu seinen Ergebnissen geführt hat, habe ich keine Andeutung gefunden (auch nicht die Angabe über* $2x^2 + 29$*). Aber ohne Zweifel bilden seine* Numeri idonei *für ihn den Ausgangspunkt.*)

Proposition 19 (Frobenius) *Let $n = 2p$, where p is an odd prime, and put $\varphi(x, y) = x^2 + ny^2$, $\psi(x, y) = 2x^2 + py^2$. Then the following conditions are equivalent:*

(i) *$k^2 + n$ is a prime or twice a prime, for all integers k with $0 < k < \sqrt{\frac{n}{3}}$;*

(ii) *$h(-4n) = 2$;*

(iii) *The number* $q := \varphi(x,y)$ *is prime whenever* q *is odd and* $1 < q < \varphi(p,1) = p(p+2)$*, and similarly,* $q' = \psi(x,y)$ *is prime whenever* q' *is odd and* $q' < \psi(p,1) = p(2p+1)$*.*

If these conditions hold, then we have that $2x^2+p$ *is prime, for all integers* $|x| < p$*.*

Remark 20 (a) Note that (i) can be viewed as a sharpening of Grube's second criterion (Proposition 17(b)) for idoneal numbers, so in particular any number n satisfying (i) is idoneal. Similarly, it is easy to see that any n satisfying (ii) must be idoneal.

As Frobenius remarks, it follows from Euler's list (and Gauss's class number computations) that this proposition applies to the primes $p = 3, 5, 11, 29$ and no other primes $p < 10,000$. In fact, we now know that there can be no others because the (fundamental) discriminants $\Delta < 0$ with $h(\Delta) \leq 2$ are all known; cf. Stark [43], Watkins [50] and the references therein. (Note that Baker's result [3] is not quite strong enough to be able to make this assertion.)

(b) The implication (iii) ⇒ (i) is not explicitly formulated (nor proved) in [19], but it is easy to verify it as follows. Let $k < \sqrt{\frac{n}{3}}$. If $k \equiv 1 \pmod 2$, then $k^2 + n = \varphi(k,1)$ is prime by the criterion in (iii). If $k = 2x$, then $\psi(x,1)$ is prime by the criterion in (iii) and so $k^2 + n = 2\psi(x,1)$ is twice a prime. Thus (i) holds.

(c) Frobenius also has a statement similar to Proposition 19 in the case that $n = p$ is prime and $p \equiv 1 \pmod 4$. In this case $\psi(x,y) = 2x^2 + 2xy + py^2$ and the bounds in (iii) are slightly different. As he points out, this case applies to $p = 5, 13, 37$.

(d) Frobenius also considers the polynomial $x^2 + x + p$, where $p \equiv 3\ (4)$ is prime and shows that $f(x)$ is prime for $|x| < p$ if $h(-p) = 1$. This statement is often cited; cf. Ribenboim [41], p. 137, for a discussion of its history.

In addition, motivated by some (unpublished) work of Remak, Frobenius also studies the indefinite form $x^2 + xy - py^2$ and the associated prime-producing polynomial $x^2 + x - p$.

2.5 Dickson and Hall

In his *History of Number Theory*, Dickson [12] discusses the history of idoneal numbers (up to 1919) on pp. 361–365. Steinig [45], p. 86, calls this "a rather confused account" of idoneal numbers and explains the mistake in Dickson's definition of an idoneal number. In addition, I feel that Dickson's discussion of Grube's paper on p. 363 of [12] is substandard. Not only are Grube's most important results (Theorems 6 and 12) not mentioned, but he also makes the following very puzzling statement in connection with Euler's criterion: *"Grube could only prove the following modification: Let* Ω *be the set of numbers* $D + n^2 \leq 4D$ *in which* n *is prime to* D*. According as all or not all numbers of* Ω *are of the form* q*,* $2q$*,* q^2 *or* 2^λ *(*q *a prime),* D *is or is not an* *idoneal number."* I fail to see in what way this "modifies" Euler's (original) criterion (as stated above and on p. 361 of [12]), except that Dickson's error (as analyzed by Steinig [45]) has been corrected. On the other hand, he does not mention that Grube could only prove one direction of this criterion; cf. Remark 16.

In his textbook on number theory (published 1929), Dickson [11] devotes Chapter V to binary quadratic forms. His main interest in that chapter is to determine the number of represention of positive definite quadratic forms, and to this end he presents a section (§55) entitled *Positive forms with a single class in each genus* because *"it is only for forms of such discriminants that we can find a simple expression for the number of representations"*, as he states (without proof) on p. 88.

Here he considers not only even discriminants, but odd (negative) discriminants as well. For the latter he introduces on p. 88 a criterion to test whether a given Δ has the property that $c(\Delta) = 1$; this criterion is similar to those of Euler and Grube for even discriminants.

Using this criteron, he gives on p. 85 a table of all (equivalence classes of) forms with discriminant Δ for $-400 < \Delta < 0$, and on p. 89 he lists further discriminants with this property in the range $-23000 < \Delta < -400$. He also remarks that if Δ is even, then these discriminants correspond to the idoneal numbers of Euler, but as in his other book [12], he does not give the correct definition of an idoneal number.

A decade later N. Hall takes up this theme again in his thesis (cf. Hall [24]) and writes down an explicit formula for the number of representations for a positive binary quadratic form of discriminant Δ when $c(\Delta) = 1$. This motivates him to study in [23] the question of *"whether the known discriminants as given by Dickson* [in his book] *comprise all for which there is a single class in each genus."*

Although he knows of Chowla's article [8], which refers to Gauss, he seems to be unaware of the earlier work by Euler, Gauss and Grube, and bases his work solely on Dickson [11].

He begins his article by stating a criterion for the condition $c(\Delta) = 1$ which is exactly the same as Grube's first variant of Euler's criterion (Proposition 17(a)), except that he adds the hypothesis that $\gcd(a, 2b, c) = 1$ and that he also allows odd discriminants.

He then proceeds to transport Dickson's criterion (for odd discriminants) to even discriminants, and thus arrives at a weak version of Euler's criterion. Nevertheless, he says (on p. 86): *"A search of the literature fails to disclose the corresponding rather evident tests for even discriminants."*

More precisely, if $\Delta = -4n$ and $c(\Delta) = 1$, then he investigates the factorization of the numbers $S_k = n + k^2$, for $k = 1, \ldots, 5$. Here he obtains results similar (but not identical) to those of Euler and Grube. (For example, for $k = 2$ he obtains that $S_2 = p, p^2, 2p, 4p, 2^4, 2^5$ or 2^6, where p is some prime.) He then uses these results to derive two theorems which are (for even discriminants) completely contained in Grube's results (specifically, in Corollary 8 and Theorem 12).

2.6 Chowla and Weinberger

Already in 1918 Hecke and Landau observed that the *Generalized Riemann Hypothesis* (GRH) for quadratic characters gives effective lower bounds for the class number $h(\Delta)$ and that this leads to a (conditional) proof of Gauss's Conjecture 5(a). This observation was written up by Landau [37]. Here Hecke and Landau restrict their attention to *fundamental* discriminants $\Delta < 0$, i.e. to those discriminants that are attached to the rings of integers of imaginary quadratic fields. (Thus, Δ is fundamental if and only if either Δ is odd and squarefree, or if $\frac{\Delta}{4} \not\equiv 1 \pmod 4$ and is squarefree.) More precisely, Hecke's result (cf. [28]) is the following: there exists a (computable) constant $c > 0$ such that for every fundamental discriminant $\Delta < 0$ we have

$$(6) \qquad L(s, \chi_\Delta) := \sum_{n=1}^{\infty} \left(\frac{\Delta}{n}\right) n^{-s} \neq 0 \text{ for } s > 1 - \frac{1}{\log|\Delta|} \quad \Rightarrow \quad h(\Delta) > c\frac{\sqrt{|\Delta|}}{\log|\Delta|}.$$

Note that it is still unknown whether the hypothesis (on the left hand side) of (6) holds for every Δ. This would follow from GRH (for quadratic characters) which conjectures that $L(s, \chi_\Delta) \neq 0$ for $\mathrm{Re}(s) > \frac{1}{2}$.

In 1934 Heilbronn [27], inspired by work of Deuring (and others), showed that if GRH is *false*, then one can still conclude that $h(\Delta) \to \infty$, if $-\Delta \to \infty$ (where $\Delta \equiv 0, 1 \pmod 4$), and so Gauss's Conjecture 5(a) (and its extension to odd discriminants) is unconditionally true. This proof is non-effective, and an effective proof was found only in 1986. (For more information, see Stark's essay [44].)

In the same year, Chowla [8] modified Heilbronn's argument to show that $c(\Delta) \to \infty$, if $-\Delta \to \infty$; in fact, his article appears right after Heilbronn's in the same journal. Thus, there are only finitely many idoneal numbers. Although Chowla does not mention idoneal numbers explictly, he does refer to this as a conjecture of Gauss.

Later that year Heilbronn and Linfoot [28] refined the argument of [27] to prove that besides the 9 known fundamental discriminants $\Delta < 0$ with $h(\Delta) = 1$, there can be at most one more. It was not until 1952 that Heegner showed that no such tenth discriminant exists. (At first it was thought that Heegner's proof contains a gap, but it was later found that his proof is correct; cf. Stark [44] and/or Cox [10], p. 271, for more information and references, and Cox [10], §12E, for a nice presentation of Heegner's proof.)

In 1954 Chowla and Briggs [9] proved a similar result for fundamental discriminants $\Delta < 0$ with $c(\Delta) = 1$: there is at most one more such discriminant with $|\Delta| > 10^{60}$. (There is an annoying typo in the statement of their Lemma 4: $k^{1/27}$ should be replaced by $k^{-1/27}$.) They also show that GRH (or a somewhat weaker hypothesis) implies that no such example exists for $|\Delta| > 10^{14}$.

This last result was improved by Grosswald [21] who showed that GRH, together with certain computer computations, implies that the *extended* Conjecture of Gauss and Euler is true, i.e. that $c(\Delta) > 1$ if $\Delta < (-4)1848$ for all discriminants $\Delta \equiv 0, 1 \pmod 4$.

Remark 21 In his Theorem 1, Grosswald [21] classifies the non-fundamental discriminants $\Delta < 0$ for which $c(\Delta) = 1$, thereby extending Grube's result (cf. Theorem 12) to odd discriminants. Unfortunately, his theorem, as stated, is incorrect: the cases listed in Theorem 12(a)–(c) give counterexamples to his assertion. (Here one should exclude the 5 counterexamples that are squares because Grosswald excludes the case that $|\Delta|$ is a square.) Thus, one should add the hypothesis $d > 315$ to the statement of Grosswald's Theorem 1, for this is what he assumes in his proof.

By using results by Tazutawa and other ideas, Weinberger [55] was able to improve the results of Grosswald and Chowla/Briggs to prove:

Theorem 22 (Weinberger) (*a) There is at most one fundamental discriminant* $\Delta < -5460 = (-4)1365$ *with* $c(\Delta) = 1$*.*

(b) *If* GRH *is true, then* $c(\Delta) > 1$ *if* Δ *is a fundamental discriminant with* $\Delta < -5460$*.*

As a consequence, we obtain:

Corollary 23 *There is at most one* squarefree *idoneal number* $n^* > 1848$*. If* n^* *is even, then* $4n^*$ *is also idoneal, and hence there are at most* 67 *idoneal numbers. If* GRH *holds, then there are precisely* 65 *idoneal numbers.*

Proof. Suppose $n^* > 1848$ is idoneal and squarefree. Since $n^* \not\equiv 3 \pmod 4$ by Corollary 8, it follows that $-4n$ is fundamental discriminant, and so by Theorem 22(a) there is at most one such n^*. If n^* is even, then $4n^*$ is also idoneal by Euler's *Theorema* 7; cf. Corollary 10(b).

Now suppose that $n > 1848$ is an arbitrary idoneal number. If n is squarefree, then $n = n^*$. If not, then $n \equiv 0 \pmod 4$ by Corollary 14. Since by Theorem 1 there are no idoneal numbers in the range $1848 < n \leq 5460$, we many assume that $n > 5460$. Then by Corollary 14 we have that $m = \frac{n}{4}$ is a squarefree idoneal number, so $m = n^*$ and hence $n = 4n^*$. This proves that there are at most 67 idoneal numbers.

The last assertion follows directly from Theorem 22(b).

Remark 24 (a) Frei [17] claims that Weinberger's result implies that there is at most *one* idoneal number $n > 1848$, and this assertion is frequently repeated in the literature; cf. e.g. [42], p. 339, 340. However, as was mentioned above, this cannot be true unless we could show that there are *no even* idoneal numbers for $n > 1848$. It is likely that Frei's error is due to his earlier wrong assertion mentioned in Remark 13.

(b) Weinberger's proof uses the assertion that $c(\Delta) > 1$ for $-5400 > \Delta > -d_{11}$, where $d_{11} = 2 \cdot 3 \cdot 5 \cdots 31 = 200,560,490,130$ is the product of the first 11 primes. (Thus, $2 \times 10^{11} < d_{11} < 2.1 \times 10^{11}$.) Here he mentions that this follows from (undocumented) machine computations of Lehmer.

(c) In Weinberger's statement of his theorem [55], he uses in place of the hypothesis "$c(\Delta) = 1$" the equivalent hypothesis "$E(Cl(\Delta)) \leq 2$", where $E(A)$ denotes the exponent of an abelian group A. (The equivalence of these two hypotheses follows from Remark 7(b) because $E(A) \leq 2 \Leftrightarrow A$ is an elementary abelian 2-group.) This allows him to generalize his method to prove that there are only finitely many fundamental discriminants $\Delta < 0$ for which $E(Cl(\Delta)) \leq 3$.

2.7 Numerical computations

By using his criterion of Proposition 17(a), Euler found in 1778 (by hand) that there are precisely 65 idoneal numbers less than 10,000. Similarly, around 1800 Gauss calculated the types (g, c) of all even discriminants Δ with $0 > \frac{\Delta}{4} > -10,000$ and found that there are precisely 65 even discriminants in this range for which $c(\Delta) = 1$.

It is mentioned in [12], p. 365, that in 1901 Cunningham and Cullen checked that there are no idoneal numbers n with $1848 < n < 50,000$, and that they found in 1919 that this is also true for $n < 100,000$.

In his textbook, Dickson [11] lists on p. 85 and p. 89 all discriminants Δ with $c(\Delta) = 1$ and $0 > \Delta > -4 \cdot 100,000$. (On p. 85 he lists more precisely all reduced forms q with $c(q) = 1$ and $0 > \Delta(q) > -400$.) Thus, aside from the 65 even discriminants found by Gauss (and Euler), there are also 36 odd discriminants; the last in this range is $\Delta = -3,315$ (as was found by Townes).

In 1948 Swift used Lehmer's "linear congruence machine" to determine that there are no discrimimants Δ with $c(\Delta) = 1$ and $4 \cdot 1848 < -\Delta < 10^7$. (Note that the lower bound of 3315 given in [46] is clearly incorrect.) To do this efficiently, he used a new criterion for finding idoneal numbers which will be discussed in more detail in the next section. Although this criterion is incorrect as stated (cf. Remark 26), this does not affect the validity of his computations.

In his 1962 paper, Grosswald [21] asserts that J. Selfridge, M. Atkinson and C. MacDonald extended Swift's results up to $-\Delta < 10^{9.12919}$, but it seems that their paper (which is announced in [21] as "to appear in Math. Comp.") never appeared. However, I have checked this is correct for $-\Delta \leq 4 \times 10^9$ (when $\Delta = -4n$ and $n \equiv 2 \pmod 4$): using MAPLE, this took 4.15 hours on my laptop computer.

Similarly, in his 1973 paper, Weinberger uses machine computations (which he says were done by D. H. Lehmer) which extend Swift's work up to $-\Delta \leq d_{11} \approx 2 \times 10^{11}$. Unfortunately, no documentation of these computations seems to exist.

Recently, Jacobson, Ramachandran and Williams [31] computed $h(\Delta)$ and the structure of the class group $Cl(\Delta)$ for all fundamental discriminants $\Delta < 0$ with $|\Delta| < 10^{11}$. From their tables (which took $1501 + 2242$ days of CPU time to compile), one could check the validity of Lehmer's computations for slightly less than half the cases, for we need it up to 2.1×10^{11}. However, this gap should be filled soon, for the authors state in [31] that they hope to extend their tables to 10^{12} in the near future.

3 Characterizations of Idoneal Numbers

We have already encountered several characterizations of idoneal numbers: 1) the criteria of Grube given in Proposition 17 and 2) the characterization in terms of the condition $c(-4n) = 1$ (cf. Theorem 6), which leads to several other characterizations (cf. Remark 7(b) and/or Cox [10], p. 59). Here is another test which is very useful for computations:

Proposition 25 *If n is an idoneal number, then the Legendre symbol*

$$\left(\frac{-n}{p}\right) \neq 1, \quad \textit{for all odd primes } p < \sqrt{n}. \tag{7}$$

Proof. If not, then there exists an odd prime $p < \sqrt{n}$ with $\left(\frac{-n}{p}\right) = 1$, and hence the congruence $b^2 \equiv -n \pmod{p}$ has a solution b with $0 < b < \frac{p}{2}$. Write $b^2 + n = cp$ for some $c > 0$. Since $p^2 < n$, we see that $c = \frac{b^2+n}{p} > \frac{b^2+p^2}{p} > p > 2b$. Since $b < \frac{p}{2} < \sqrt{\frac{n}{4}} < \sqrt{\frac{n}{3}}$, we thus see that $b^2 + n = pc$ is a factorization which violates Grube's criterion of Proposition 17(a), and hence n cannot be idoneal.

Remark 26 (a) This proposition can be viewed as a correction of the test used by Swift [46] in his computations. In his test he asserts that if n is idoneal, then (7) holds for $p^2 < n + \frac{1}{4}(p-1)^2$. This, however, is *false* if n has the form $n = p^2 - 1$, where p is an odd prime, for then clearly $p^2 = n + 1 \leq n + \frac{1}{4}(p-1)^2$ and $(\frac{-n}{p}) = (\frac{1}{p}) = 1$. Thus, the idoneal numbers $n = 8, 24, 48, 120, 168, 840$ and 1848 (with $p = 3, 5, 7, 11, 13, 29$ and 43, respectively) show that the bound $p < \sqrt{n}$ is quite sharp and that Swift's assertion is false unless we make further assumptions on n. Indeed, as will be shown below (cf. Corollary 30), if we assume that $n \equiv 2, 4,$ or $6 \pmod{8}$, then Swift's criterion is true, even for $p^2 < 4n + 1$.

Note that this error does not affect the validity of Swift's calculations because if n is not idoneal, then in practice one can find already a very small prime p which violates (7). Swift remarks that for $|\Delta| < 10^7$ the largest prime needed was $p = 79$, and in my computations for $n < 10^9$ (and $n \equiv 2 \pmod{4}$) the largest prime was $p = 103$.

(b) This test can be extended to odd discriminants as well; i.e. we have that if $c(\Delta) = 1$, $(\Delta < 0)$, then $(\frac{\Delta}{p}) \neq 1$ for all primes $p < \frac{1}{2}\sqrt{|\Delta|}$. Indeed, such a statement (for fundamental discriminants) constitutes one part of the proof of Weinberger's Theorem 1; cf. [55], p. 119.

A natural question is whether the converse of Proposition 25 holds. Strictly speaking, the answer is no: the numbers $n = 19$ and $n = 43$ satisfy (7), yet are not idoneal by Corollary 8. Thus, extra conditions have to be imposed. We begin with the following partial converse to Proposition 25. Since there is no extra work involved, we also include the case of odd discriminants:

Proposition 27 *Let $\Delta < 0$ be a fundamental discriminant. If $(\frac{\Delta}{p}) \neq 1$ for all primes p with $p^2 < \frac{1}{3}|\Delta|$, then $c(\Delta) = 1$.*

Proof. By Remark 7(b) it is enough to show that $Cl(\Delta)$ is an elementary 2-group. Since Δ is a fundamental discriminant, we have that $Cl(\Delta)$ is isomorphic to the class group $Cl(\mathfrak{O}_K)$ of the ring of integers $\mathfrak{O}_K$ of $K = \mathbb{Q}(\sqrt{\Delta})$; cf. e.g. [10], p. 137. The hypothesis implies:

(8) $\quad \mathfrak{p} \subset \mathfrak{O}_K$ prime ideal with $N\mathfrak{p} < \sqrt{|\Delta|/3} \;\Rightarrow\; \mathfrak{p}^2 = (\alpha)$ is a principal ideal.

Indeed, if $\mathfrak{p}$ is such a prime ideal, then $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime p. If $(\frac{\Delta}{p}) = -1$, then $\mathfrak{p} = (p)$ (cf. [10], p. 103), and the assertion is trivial. If $(\frac{\Delta}{p}) \neq -1$, then $N\mathfrak{p} = p$. But the hypothesis forces that $(\frac{\Delta}{p}) = 0$, i.e. $p|\Delta$, and so $\mathfrak{p}^2 = (p)$, which proves (8).

From (8) it follows $Cl(\mathcal{O}_K)$ is an elementary abelian 2-group because its generators have order at most 2. Here we have used the following well-known fact:

(9) $\quad Cl(\mathfrak{O}_K)$ is generated by the classes of prime ideals $\mathfrak{p}$ with $N\mathfrak{p} < \sqrt{|\Delta|/3}$.

For convenience of the reader, we sketch the proof of (9); cf. [6], p. 196. By combining the reduction theory of quadratic forms with the isomorphism $Cl(\Delta) \simeq Cl(\mathfrak{O}_K)$, we see that each ideal class of $Cl(\mathfrak{O}_K)$ contains an ideal $\mathfrak{a}$ with $N\mathfrak{a} < \sqrt{|\Delta|/3}$; cf. [6], p. 195. Since we can write $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ as a product of prime ideals (and then $N\mathfrak{p}_i \leq N\mathfrak{a}$), the assertion follows.

Remark 28 (a) If we specialize Proposition 27 to the case $\Delta = -4n$, then we get: if $n \not\equiv 3 \pmod 4$ is squarefree and $(\frac{-n}{p}) \neq 1$ for all odd primes $p < \sqrt{\frac{4}{3}n}$, then n is idoneal. Thus, aside from the restriction that n be squarefree, the hypothesis of Proposition 27 is stronger than the conclusion (7) of Proposition 25.

(b) It is clear from the above proof that this criterion could be improved if we had a better estimate for the norms of generators of $Cl(\mathfrak{O}_K)$ in (9). Such (unconditional) improvements, however, seem to be very difficult. In 1990 Bach [1], p. 376, proved that GRH implies that (9) holds if we replace $\sqrt{|\Delta|/3}$ by $6(\log|\Delta|)^2$, and [31] shows that this agrees with numercial evidence up to $|\Delta| < 10^{11}$. See also [6], p. 196ff, and [31], where algorithms for determining $Cl(\Delta)$ are discussed.

Another line of attack is based on the following criterion which was suggested by the connection with genus 2 curves. This connection will be explained in more detail in the next section.

Proposition 29 *If $n \equiv 2, 4$ or $6 \pmod 8$, then n is idoneal if and only if for every prime $p > 2$ we have that*

(10) $\quad$ *$nt^2 = k(p-k)$ has a solution $t, k \in \mathbb{Z}$ with $t, k > 0$ whenever* $\left(\dfrac{-n}{p}\right) = 1.$

Before giving the proof, we observe that the above result implies that Swift's test (cf. Remark 26) is correct when $n \equiv 2, 4, 6 \pmod 8$. It also implies that the converse of Proposition 27 holds, provided that $\Delta = -4n$, where $n \equiv 2 \pmod 4$.

Corollary 30 (a) *If* $n \equiv 2, 4, 6 \pmod 8$ *is an idoneal number, then* $(\frac{-n}{p}) \neq 1$*, for all odd primes* $p < \sqrt{4n+1}$.

(b) *If* $n \equiv 2 \pmod 4$ *is squarefree, then the following conditions are equivalent:*

(i) n *is idoneal;*

(ii) $(\frac{-n}{p}) \neq 1$*, for all odd primes* $p < \sqrt{\frac{4}{3}n}$*;*

(iii) $(\frac{-n}{p}) \neq 1$*, for all odd primes* $p < \sqrt{4n+1}$.

Proof. (a) Suppose that p is an odd prime with $(\frac{-n}{p}) = 1$. Then by Proposition 29 there exist $t, k \geq 1$ such that $nt^2 = k(p-k)$. Then clearly $k < p$, and by replacing k by $p-k$, if necessary, we can assume that $k \leq \frac{p-1}{2}$. Since the function $k(p-k)$ is increasing in the range $1 \leq k \leq \frac{p-1}{2}$, we obtain that $n \leq nt^2 = k(p-k) \leq (\frac{p-1}{2})(\frac{p+1}{2}) = \frac{1}{4}(p^2-1)$, or $p^2 \geq 4n+1$, and so (a) holds.

(b) The implication (i) $\Rightarrow$ (iii) follows from part (a), that of (iii) $\Rightarrow$ (ii) is trivial, and (ii) $\Rightarrow$ (i) is Proposition 27; cf. Remark 28(a).

Proof of Proposition 29. Recall from Remark 7(b) that n is idoneal if and only if every primitive form of discriminant $-4n$ is ambiguous. Since n is even but not divisible by 8, every ambiguous form is equivalent to $ax^2 + by^2$ (cf. [20], Art. 257-8), so we see that in this situation n is idoneal if and only if we have:

$$(11) \qquad q \in Cl(-4n) \quad \Rightarrow \quad q(x,y) \sim ax^2 + cy^2, \text{ where } ac = n \text{ and } (a,c) = 1.$$

Thus, it is enough to show that (11) is equivalent to (10).

Suppose first that (11) holds, and let p be an odd prime with $(\frac{-n}{p}) = 1$. Then $\exists b \not\equiv 0 \pmod p$ such that $b^2 \equiv -n \pmod p$, so $b^2 + n = pm$, for some m. Consider $q(x,y) = px^2 + 2bxy + my^2$. Then $\Delta(q) = (2b)^2 - 4pm = -4n$, so $q \in Cl(-4n)$. (Note that q is primitive because $(2b, p) = 1$.) Thus, by condition (11) we have that $q \sim ax^2 + cy^2$, for some a, c with $ac = n$ and $(a,c) = 1$. Since q properly represents p (for $p = q(1,0)$), it follows that this is also true for $q' := ax^2 + cy^2$, so there exist $t_1, t_2 \in \mathbb{Z}$ with $(t_1, t_2) = 1$ such that $p = at_1^2 + ct_2$. Clearly $t_1 \neq 0$ (for otherwise $p = ct_2^2 = c|n$, contradiction) and similarly $t_2 \neq 0$. Put $k = at_1^2$. Then $p - k = ct_2^2$ and so $k(p-k) = at_1^2 ct_2^2 = nt^2$, where $t = |t_1 t_2| > 0$. Thus property (10) holds.

Now suppose conversely that (10) holds, and let q be a primitive quadratic form of discriminant $-4n$. By Dirichlet's Theorem ([10], p. 188), q represents infinitely many primes p, so there is a prime $p \nmid 4n$ represented by q. For any such prime we have $(\frac{-n}{p}) = 1$; cf. [10], p. 30.

By hypothesis (10) $\exists k, t \geq 1$ such that $k(p-k) = nt^2$. Put $k_1 = k$, $k_2 = p - k$, and for $i = 1, 2$, put $a_i = (k_i, n)$, $t_i = (k_i, t)$. Since $(k_1, k_2) = 1$ and $n | k_1 k_2$, we see that $a_1 a_2 = n$, and similarly $t_1 t_2 = t$. Thus, $(a_1 t_1^2)(a_2 t_2^2) = nt^2 = k_1 k_2$, and so $k_i = a_i t_i^2$, for $i = 1, 2$, because $(a_1 t_1^2, a_2 t_2^2) = 1$ and $k_i | a_i t_i^2$. This means that if we let $q'(x, y) = a_1 x^2 + a_2 y^2$, then q' is primitive with $\Delta(q') = -4n$, and q' represents p (because $q'(t_1, t_2) = a_1 t_1^2 + a_2 t_2^2 = k_1 + k_2 = p$).

We thus have that q and q' both represent the prime $p \nmid 4n$. From this it follows that either $q \sim q'$ or $q \sim (q')^{-1}$; cf. Piehler [40]. But since q' is ambiguous, we have $(q')^{-1} \sim q'$, and so $q \sim q'$. This shows that (11) holds, and so n is idoneal.

Remark 31 The above proof can be generalized to show that the condition (10) of Proposition 29 is equivalent to the following more general assertion: for every odd integer $m > 1$ we have that

(12) $nt^2 = k(m-k)$ has a solution $t, k > 0$ whenever $(\frac{-n}{p}) = 1$, for all primes $p|m$.

Indeed, clearly (12) implies (10). On the other hand, if m is an odd integer with $(\frac{-n}{p}) = 1$, for all primes $p|m$, then $(m, n) = 1$ and $-n$ is a square mod m; cf. e.g. Hua [29], p. 44. Thus, there are integers b, c such that $b^2 + n = mc$, and then $q = mx^2 + 2bxy + cy^2 \in Cl(-4n)$ primitively represents m. Thus, if n is idoneal, then (the first part of) the proof of Proposition 29 shows that (12) holds.

We now come to the following characterization of idoneal numbers in terms of the modular function $j(\tau)$. As was mentioned above, Weber [52] alludes to this connection in the introduction of his paper, but without giving a precise statement (or proof).

Theorem 32 (Weber) *Let $n \geq 1$ be an integer. Then $\mathbb{Q}(j(\sqrt{-n}))$ is a Galois (and hence an abelian) field extension of $\mathbb{Q}$ if and only if n is idoneal.*

Proof. Put $K = \mathbb{Q}(\sqrt{-n})$. By the First Main Theorem of Complex Multiplication ([10], Theorem 11.1) we know that $L_n := K(j(\sqrt{-n}))$ is an abelian extension of K with $\mathrm{Gal}(L_n/K) \simeq Cl(-4n)$. In addition, we have that L_n is Galois over $\mathbb{Q}$ with Galois group $G = \langle \sigma, H \rangle$, where σ denotes complex conjugation (restricted to L_n) and $H = \mathrm{Gal}(L_n/K)$. Furthermore, σ acts on H by inversion, i.e. $\sigma h \sigma^{-1} = h^{-1}$, for all $h \in H$; cf. [10], Lemma 9.3. Thus $\mathbb{Q}(j(\sqrt{-n}))) = \mathrm{Fix}(\sigma)$ because $j(\sqrt{-n}) \in \mathbb{R}$ (cf. [10], Exercise 11.1).

By Galois theory we therefore see that $\mathbb{Q}(j(\sqrt{-n}))$ is Galois over $\mathbb{Q}$ $\Leftrightarrow$ $\langle \sigma \rangle$ is normal in G $\Leftrightarrow$ $h\sigma h^{-1} = \sigma, \forall h \in H$ $\Leftrightarrow$ $\sigma^{-1} h \sigma = h, \forall h \in H$ $\Leftrightarrow$ $h = h^{-1}, \forall h \in H$ $\Leftrightarrow$ $H \simeq Cl(-4n)$ is an elementary abelian 2-group $\Leftrightarrow$ n is idoneal (cf. Remark 7(b)). This proves the theorem. Note that the above argument also shows that if $\mathbb{Q}(j(\sqrt{-n}))$ is Galois over $\mathbb{Q}$, then $L_n/\mathbb{Q}$ is abelian (with group $G \simeq \mathbb{Z}/2\mathbb{Z} \times H$) and so $\mathbb{Q}(j(\sqrt{-n}))/\mathbb{Q}$ is abelian as well.

Remark 33 In his paper, Weber [52] does not compute $j(\sqrt{-n})$ directly (when n is idoneal), but instead finds expressions for powers of $f(\sqrt{-n})$ (or of $f_1(\sqrt{-n})$, $f_2(\sqrt{-n})$), where f, f_1 and f_2 denote the *Weber functions* (cf. [10], §12.B). From this one gets an expression for $j(\sqrt{-n})$ because $j(\tau)^3 = \gamma_2(\tau) = (f(\tau)^{24} - 16)/f(\tau)^8$; cf. [10], p. 249, 257. As Cox [10] remarks on p. 263, Weber's method is based on the Kronecker Limit Formula. Cox works out the details of the computation in the case that $n = 14$ to obtain $j(\sqrt{-14})^3 = \gamma_2(\sqrt{-14}) = 2(323 + 228\sqrt{2} + (231 + 161\sqrt{2})\sqrt{2\sqrt{2} - 1})$; cf. [10], §12.D. Note that in Table VI at the end of his textbook [53], Weber lists the values of (powers of) the Weber functions for $\tau = \sqrt{-n}$ for $1 \le n \le 52$ and for all the idoneal numbers $n \le 1848$ (together some other values such as $n = 55, 63, 67, \ldots, 163, 193$).

Closely connected with this theorem is the following characterization of idoneal numbers which was mentioned in Frei [17] without proof or reference:

Corollary 34 *Let $n \ge 1$. Then the primes numbers of the form $p = x^2 + ny^2$ with $x, y \in \mathbb{Z}$ can be characterized by congruence relations modulo m for some m if and only if n is an idoneal number.*

Proof. By genus theory (and quadratic reciprocity) we know that the prime numbers p which are represented by some form in the principal genus $\mathrm{gen}(1_\Delta)$ of discriminant $\Delta = -4n$ can be characterized by congruence conditions modulo $|\Delta|$. Thus, if n is idoneal, the assertion holds with $m = 4n$.

To prove the converse, we shall use the following fact (proved in Cox [10], p. 189): the primes p which are represented by $1_\Delta = x^2 + ny^2$ are (up to finitely many exceptions) the primes p which split completely in the ring class field L_n of $\mathbb{Z}[\sqrt{-n}]$. (This is the same field as that of the proof of Theorem 32 by [10], Theorem 11.1).

Suppose now that the primes p represented by 1_{-4n} can be described by congruence conditions modulo m. Then the primes which split completely in L_n are described by the same conditions mod m, and so by class field theory over $\mathbb{Q}$, the field $L_n/\mathbb{Q}$ is abelian. By Theorem 32, this means that n is idoneal.

4 Connections with genus 2 curves

We now turn to the connection between idoneal numbers and curves of genus 2 which was mentioned above. For this, fix an (algebraically closed) field K and consider the following problem.

Question 35 Let E_1 and E_2 be two elliptic curves over K. *Is there a* (smooth, irreducible) *curve C of genus* 2 *on the product surface $E_1 \times E_2$?*

By the theory of Jacobians of curves, this question is equivalent to: *Is there a curve C/K of genus 2 such that its Jacobian J_C is isomorphic to $E_1 \times E_2$?*

This problem was first studied by Hayashida and Nishi [25], [26] in 1965, who obtained partial results. A complete solution can be found in [35], and will be discussed in section 6. Here we shall focus on a special case of this question by imposing the extra condition that E_1 and E_2 do not have complex multiplication (i.e. that $\mathrm{End}(E_i) = \mathbb{Z}$) and that E_1 and E_2 are isogenous. Note that these two conditions are equivalent to saying that $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, for some $h \neq 0$; we shall refer to this as "the non-CM case".

Definition. A pair (E_1, E_2) of elliptic curves is said to have *type* n if we have $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, where $\deg(h) = n$.

The following result (which is a restatement of Theorem 5 of [34]) gives the connection between certain idoneal numbers and the solution of the above question in the non-CM case:

Theorem 36 *If (E_1, E_2) is a pair of elliptic curves of type n, then the following conditions are equivalent:*

(i) *there is* no *genus* 2 *curve on $E_1 \times E_2$;*

(ii) $n = 1$ *or n is an* even *idoneal number which is not divisible by* 8.

(iii) $n \not\equiv 3 \,(\mathrm{mod}\ 4)$ *and $4n$ is an idoneal number.*

Proof. (Sketch) Note first that conditions (ii) and (iii) are equivalent by Corollary 10. For the other equivalence, we shall outline the main ideas of the proof and refer to [34] for the details.

Let $\mathcal{P}^{irr}(A)$ denote the set of irreducible genus 2 curves C on $A := E_1 \times E_2$. By the adjunction formula, the self-intersection number of C is $C^2 = 2$, so

$$\mathcal{P}^{irr}(A) \subset \mathcal{P}(A) := \{\theta \in \mathrm{Div}(A) : \theta \geq 0, \theta^2 = 2\},$$

where $\mathrm{Div}(A)$ denotes the group of divisors on A. Here the notation $\mathcal{P}^{irr}(A)$ reflects the fact (due to Weil) that if $\theta \in \mathcal{P}(A)$, then $\theta \in \mathcal{P}(A)^{irr}$ if and only if θ is an irreducible curve.

To decide whether or not $\theta \in \mathcal{P}(A)$ is irreducible, we shall use the *refined Humbert invariant q_θ* defined in [34] (which is closely related to the classical Humbert invariant defined by Humbert). This is the quadratic form defined by the formula

$$q_\theta(D) = (D.\theta)^2 - 2D^2, \quad D \in \mathrm{Div}(A), \tag{13}$$

where (.) denote intersection numbers. It is clear that q_θ can be viewed as a quadratic form on the *Néron-Severi group* of A, i.e. on the quotient group $\mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where the equivalence relation $D_1 \equiv D_2$ (numerical equivalence) means that $(D_1.D) = (D_2.D)$, $\forall D \in \mathrm{Div}(A)$. Moreover, a short computation (using the fact that $\theta^2 = 2$)

shows that q_θ is actually a quadratic form on $\mathrm{NS}(A,\theta) := \mathrm{NS}(A)/\mathbb{Z}\theta$, and the Hodge Index Theorem shows that q_θ is positive definite (on $\mathrm{NS}(A,\theta)$).

One of the key properties of q_θ is the following *irreducibility criterion* (cf. [34], Proposition 6):

$$\theta \text{ is irreducible} \quad \Leftrightarrow \quad q_\theta(D) \neq 1, \text{ for all } D \in \mathrm{Div}(A). \tag{14}$$

So far, the above results are true for an arbitrary abelian surface A. We now specialize to the case that $A = E_1 \times E_2$, where (E_1, E_2) has type n. In this case we have a complete classification of the quadratic forms q_θ that can occur. Indeed, by [34], Theorem 2 (or, better, by [34], Propositions 39 and 15), we know that q_θ is a binary quadratic form of discriminant $\Delta(q_\theta) = -16n$ which is either primitive and in the principal genus or is of the form $q_\theta = 4q'$, where q' is primitive of discriminant $-n$ and is in the principal genus. (Note that the last case can occur only if $n \equiv 3 \pmod 4$.) Moreover, up to equivalence, each such form is equivalent to some q_θ, i.e. we have

$$\{cl(q_\theta) : \theta \in \mathcal{P}(A)\} \;=\; \mathrm{gen}(1_{-4n}) \;\cup\; 4\mathrm{gen}(1_{-n}), \tag{15}$$

where $cl(q_\theta)$ denotes the equivalence class(es) defined by q_θ. (Note that q_θ is only defined up to $\mathrm{GL}_2(\mathbb{Z})$-equivalence, and hence gives rise to (possibly) two proper equivalence classes of forms.)

From these facts the equivalence of (i) and (iii) follow easily, for we have that (i) $\Leftrightarrow \mathcal{P}^{irr}(A) = \emptyset \Leftrightarrow q_\theta \sim 1_{-16n}, \forall \theta \in \mathcal{P}(A) \Leftrightarrow n \not\equiv 3 \pmod 4$ and $\mathrm{gen}(1_{-16n}) = \{cl(1_{-16n})\} \Leftrightarrow n \not\equiv 3 \pmod 4$ and $c(-4n) = 1 \Leftrightarrow$ (iii). Here, the second equivalence follows from (14) (together with the fact that a binary form represents 1 if and only if it is equivalent to the principal form) and the third follows from (15), together with the obvious fact that $4q'$ can never represent 1.

A closer study of genus 2 curves on $E_1 \times E_2$ naturally leads to a condition of the form (10). This is obtained by combining two facts. One of these is that such a curve C admits (infinitely) many minimal elliptic subcovers $f : C \to E$ whose degrees are given as the values of a certain binary quadratic form. (A cover $f : C \to E$ is called *minimal* if it does not fact through a non-trivial isogeny of E.) The other is that the *reducibility criterion* of [33] forces certain restrictions on the degrees of such subcovers. More precisely, we have:

Proposition 37 *Let C be a genus 2 curve on $E_1 \times E_2$, where (E_1, E_2) has type n. Then there exist integers z, r, m with $rm = z^2 n + 1$ and $m \geq 2$ such that C has a minimal elliptic subcover $f_d : C \to E_1$ of degree d if and only if*

$$d = nrx^2 - 2nzxy + my^2, \qquad \textit{for some } x, y \in \mathbb{Z} \textit{ with } (nx, y) = 1. \tag{16}$$

Moreover, if $n \not\equiv 3 \pmod 4$, or if $(r, m, 2) = 1$, then there exist infinitely many d's which are prime, and for each such odd prime $p = d$ we have

$$\left(\tfrac{-n}{p}\right) = 1 \quad \textit{and} \quad k(p-k) \neq t^2 n, \ \textit{for all integers } k, t \geq 1. \tag{17}$$

Proof. Since $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, where $\deg(h) = n$, the only cyclic isogenies from E_1 to E_2 are $\pm h$. Thus, by [18], Proposition 6.5, there exist integers z, m such that $z^2 n \equiv -1 \pmod{m}$ and such that (in the notation there) we have $C \simeq C_\psi$, where $\psi = zh_{|E_1[m]}$. Thus, the first assertion follows directly from Corollary 6.6 of [18].

To prove the other assertions, note first that the quadratic form $q(x, y) := nrx^2 - 2nzxy + my^2$ has discriminant $\Delta(q) = 4n^2z^2 - 4nrm = -4n$, and that $(nr, 2nz, m) = (r, m, 2)$. Thus, q is primitive if and only if $(r, m, 2) = 1$. This is always true if $n \not\equiv 3 \pmod 4$, for if $(r, m, 2) \neq 1$, then $z^2 n + 1 \equiv 0 \pmod 4$, so $n \equiv 3 \pmod 4$. If q is primitive, then by Dirichlet's theorem q represents infinitely many primes p, i.e. $p = q(x, y)$. If $p \nmid n$, then also $(nx, y) = 1$, and then $d = p$ is one of the values of (16). Note that since $\Delta(q) = -4n$, we have $(\frac{-n}{p}) = 1$ (if $p \neq 2$); cf. [10], p. 30.

Now fix p and write $p = q(x, y)$. Then the proof of [18], Corollary 6.6, constructs integers r' and z' such that $r'p = (z')^2 n + 1$ and such that $C \simeq C_{\psi'}$, where $\psi' = (z')\psi_{|E_1[p]}$. Suppose the equation $t^2 n = k(p - k)$ had a solution $k, t > 0$. Then $(kz')^2 \equiv -k^2 \equiv t^2 n \pmod p$, and so $t \equiv kz' \pmod p$ (replacing k by $p-k$, if necessary). Thus $k\psi' = h'_{|E_1[p]}$, where $h' = th$. Note that $\deg(h') = t^2 \deg(h) = t^2 n = k(p - k)$. By the reducibilty theorem of [33], Theorem 3, this means C_ψ is a reducible curve, contradiction. Thus, no such solution t, k can exist, and so (17) holds.

Remark 38 Note that the above Proposition 37 combined with Theorem 36 gives a quick proof of the fact that (10) implies that n is idoneal, which is the more difficult direction of Proposition 29. Indeed, if $n \equiv 2, 4, 6 \pmod 8$ were not idoneal, then by Theorem 36 there would exist a genus 2 curve C on $E_1 \times E_2$ (for some pair (E_1, E_2) of type n) and then by Proposition 37 we would have that (17) holds for infinitely many primes p, which violates (10). Thus n is idoneal.

Of course, this proof is much more complicated than the one given in section 3, but it pointed the way to suggest the criterion (10).

5 Generalizations of idoneal numbers

A first generalization of idoneal numbers was already tacitly used above. Indeed, since idoneal numbers are those numbers $n \geq 1$ for which $c(-4n) = 1$ (Theorem 6), the problem of classifying *all* discriminants $\Delta < 0$ which satisfy $c(\Delta) = 1$ constitutes a first generalization of idoneal numbers. (Discriminants with this property are called *idoneal discriminants* in Buell [7], p. 193.)

As was noted by Grube, Chowla and others, the problem of classifying idoneal discriminants reduces to that of classifying those that are fundamental. Thus, as was mentioned above, an equivalent problem is to classify those imaginary quadratic fields K whose class group $Cl(K) := Cl(\mathfrak{O}_K)$ is an elementary 2-group; this was the approach taken by Weinberger [55].

Viewed from this angle, this problem has a natural generalization to other number fields: classify the (totally) imaginary number fields K whose class group $Cl(K)$ is an elementary 2-group. This problem was studied by Miyada [39] who found that under GRH there are precisely 301 *abelian* number fields with this property.

There is another natural generalization of idoneal numbers which is perhaps closer to the original viewpoint of Euler and Gauss. In this generalization we consider (positive definite) quadratic forms in an arbitrary number $r \geq 2$ of variables. As in the case of two variables, there is the concept of genus equivalence of forms in r variables: two forms are *genus-equivalent* if they are p-adically equivalent for all primes p (including $p = \infty$); cf. e.g. Jones [32], p. 106-7 or Watson [47], p. 72. If $\text{gen}(q)$ denotes the set of equivalence classes of forms that are genus-equivalent to q, then one has as before that the number $c(q) = \#\text{gen}(q)$ is finite. Watson [48] calls $c(q)$ the *class number* of the form q. (It should be mentioned, however, that Watson uses $\text{GL}_r(\mathbb{Z})$-equivalence in place of *proper* or $\text{SL}_r(\mathbb{Z})$-equivalence of forms, so in the case that $r = 2$ his $c(q)$ is in general not the same as the $c(q)$ defined above in §2.2. Nevertheless, the condition "$c(q) = 1$" coincides for both definitions.) Note also that contrary to the case of 2 variables, it is no longer true that all (primitive) forms of the same discriminant have the same class number when $r \geq 3$.

In view of these definitions, a natural extension of the problem of determining all idoneal numbers is the following.

Problem 39 *Find all the equivalence classes of positive definite primitive forms q with class number* 1*, i.e. with $c(q) = 1$.*

This problem was studied by Watson in a series of papers in the years 1963–1978; cf. [49] and the references therein. His main results are the following:

Theorem 40 (Watson) (a) *For each $r \geq 3$, the number N_r of equivalence classes of positive primitive quadratic forms q in r variables with $c(q) = 1$ is finite.*

(b) *Such forms exist if and only if $r \leq 10$, i.e. $N_r > 0 \Leftrightarrow 1 \leq r \leq 10$.*

(c) *We have $N_3 = 790$, $N_4 \geq 27$, $N_5 \geq 42$, $N_8 = 36$, $N_9 = 4$ and $N_{10} = 2$.*

Remark 41 Watson does not study the case $r = 2$ except to say that it "seems hopeless" (cf. [48]) and that it is "very difficult" (cf. [49]). It is curious that he does not mention the obvious connection with the work of Euler, Gauss and others.

There is still another generalization of idoneal numbers. This generalization is a variant of Watson's problem and was suggested by the study of genus 2 curves, as will be explained in the next section. It is based on the following observation. If q is *binary* quadratic form, then

$$(18) \qquad q \sim 1_{\Delta(q)} \quad \Leftrightarrow \quad q \to 1 \quad \overset{\text{def}}{\Leftrightarrow} \quad q(x,y) = 1, \text{ for some } x, y \in \mathbb{Z},$$

where, as before, 1_Δ denotes the principal form of discriminant Δ. This, therefore, suggests the following (partial) generalization of Watson's problem.

Problem 42 *Find all the equivalence classes of positive definite primitive forms q in r variables which satisfy:*

$$q' \to 1, \quad \textit{for all } q' \in \mathrm{gen}(q). \tag{19}$$

Indeed, in view of (18), it is clear that for $r = 2$ condition (19) holds for $q = 1_\Delta$ if and only if $c(1_\Delta) = 1$, i.e. if and only if Δ is an idoneal discriminant. Moreover, for any r we see that if $q \to 1$ and $c(q) = 1$, then q satisfies (19). Thus, every solution q of Watson's Problem 39 with $q \to 1$ is a solution of Problem 42. It is not at all obvious that the converse holds, but Theorem 44 below suggests that this is true at least in some special cases.

Before stating the result of Theorem 44, let us look at yet another generalization of idoneal numbers and/or forms. For this, we first introduce the following terminology.

Definition. Let $q(x_1, \ldots, x_r)$ be a positive definite quadratic form in r variables. We say that q is an *idoneal-valued* form if its only (proper) values $\leq |\Delta(q)|$ are idoneal numbers, i.e. if

$$q \to n \leq |\Delta(q)| \quad \Rightarrow \quad n \text{ is an idoneal number;} \tag{20}$$

here, the symbol $q \to n$ means that q *properly represents* n, i.e. that there exist $x_1, \ldots, x_r \in \mathbb{Z}$ with $\gcd(x_1, \ldots, x_r) = 1$ such that $q(x_1, \ldots, x_r) = n$.

In addition, we say that q is a *special idoneal-valued form* if

$$q \to n \leq |\Delta(q)| \quad \Rightarrow \quad 4n \text{ is an idoneal number,} \tag{21}$$

and if in addition we have that $q \not\to n$, for any $n \equiv 3 \pmod 4$ when $\Delta(q) \not\equiv 1 \pmod 4$, and that $q \not\to n$, for any $n \equiv 3 \pmod 4$ with $n < |\Delta(q)|$ when $\Delta(q) \equiv 1 \pmod 4$.

Clearly, the 1-variable form $q(x) = nx^2$ is idoneal-valued if and only if n is an idoneal number because $\Delta(nx^2) = n$ (cf. [48], p. 2) and n is the only value which is primitively represented by q. Moreover, nx^2 is a special idoneal-valued form if and only if n satisfies condition (iii) of Theorem 36. Thus, this concept gives another generalization of idoneal numbers, and hence the following problem generalizes the search for idoneal numbers.

Problem 43 *Classify all the equivalence classes of positive definite quadratic forms which are idoneal-valued.*

At first sight it might seem unlikely that idoneal-valued forms in $r \geq 2$ variables exist at all. However, such forms do exist, as following result shows. It also shows that there is a (perhaps surprising) connection between Problems 39, 42 and 43.

Theorem 44 *Let $q(x,y) = ax^2 + bxy + cy^2$ be a positive-definite binary quadratic form, and let $Q_q(x,y,z) = z^2 + 4q(x,y)$. If either $\Delta := b^2 - 4ac \equiv 1 \pmod 4$ or if $q \not\to n$, for any $n \equiv 3 \pmod 4$, then the following conditions are equivalent:*

(i) *$c(Q_q) = 1$;*

(ii) *Q_q satisfies condition* (19)*;*

(iii) *q is a special idoneal-valued form;*

(iv) *q is equivalent to one of* 15 *forms whose coefficients (a,b,c) are given by following list:*

$$\begin{aligned}\mathcal{L} &= \{k(1,1,1) : k = 1,2,4,6,10\} \cup \{k(1,0,1) : k = 1,2,6\} \cup \{(1,1,2),(1,1,4)\} \\ &\quad \cup \{2(1,1,c) : c = 3,9\} \cup \{2(1,0,c) : c = 2,5\} \cup \{2(2,0,3)\}.\end{aligned}$$

This theorem is proved in [35]. The next section explains its relevance to problems about genus 2 curves and gives a (rough) sketch of its proof.

6 Further connections to genus 2 curves

As was mentioned above, some of the above generalizations of idoneal numbers and forms were directly inspired by considering certain problems about genus 2 curves. We now look at these problems and explain their connection to the Problems 42 and 43 formulated in the previous section.

For this, let us return to Question 35 of section 4. In Theorem 36 we saw that in the non-CM case the non-existence of curves of genus 2 on $E_1 \times E_2$ is closely related to whether or not the type n of (E_1, E_2) is an idoneal number (satisfying certain congruence conditions). This can be generalized by considering the following quadratic form q_{E_1,E_2} attached to the pair (E_1, E_2).

Notation. If E_1 and E_2 are two elliptic curves, let q_{E_1,E_2} denote the positive definite quadratic form on $\mathrm{Hom}(E_1, E_2)$ defined by

$$q_{E_1,E_2}(f) = \deg(f), \quad \text{if } f \in \mathrm{Hom}(E_1, E_2).$$

Thus, by fixing a basis of $\mathrm{Hom}(E_1, E_2)$, we obtain an explicit quadratic form in $r = \mathrm{rank}(\mathrm{Hom}(E_1, E_2))$ variables, and hence (by considering all bases) a $\mathrm{GL}_r(\mathbb{Z})$-equivalence class of forms.

Note that if (E_1, E_2) has type n, then $r = 1$ and $q_{E_1,E_2}(x) = nx^2$. Conversely, if $q_{E_1,E_2}(x) = nx^2$, then (E_1, E_2) has type n.

It turns out that the answer to Question 35 is completely determined by properties of the quadratic form q_{E_1,E_2}. More precisely, we have the following result which contains Theorem 36 as a special case:

Theorem 45 *Let $E_1 \sim E_2$ be two isogenous elliptic curves over K, and assume that E_1 is not supersingular. Then the following conditions are equivalent:*

(i) *there is* no *genus* 2 *curve on $E_1 \times E_2$;*

(ii) *q_{E_1,E_2} is a special idoneal-valued form.*

If this is the case, then either $q_{E_1,E_2}(x) = nx^2$ and $4n$ is idoneal (non-CM case) *or q_{E_1,E_2} is one of the* 15 *binary forms listed in* Theorem 44 (CM case).

Remark 46 Note that if E_1 is not isogenous to E_2, then it is easy to see that there is no genus 2 curve on $E_1 \times E_2$, so this case can be excluded from our considerations. Furthermore, the case that E_1 is supersingular was treated in [30].

The first part of the proof of this theorem is very similar to that of Theorem 36. Let q_A be the integral quadratic form defined by the intersection pairing on the Néron-Severi group $\mathrm{NS}(A)$, i,e.

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

In the case that $A = E_1 \times E_2$, we can choose a basis of $\mathrm{NS}(A)$ such that

$$q_{E_1 \times E_2} \sim xy - q_{E_1,E_2}; \tag{22}$$

cf. [34], Proposition 22. For any $\theta \in \mathrm{NS}(A)$ such that $q_A(\theta) = 1$ we have the associated refined Humbert invariant $q_{A,\theta}$ defined by (13). Then by the same reasoning as in the (first part of the) proof of Theorem 36 we obtain the following result.

Proposition 47 *If $A = E_1 \times E_2$, then condition* (i) *of* Theorem 45 *is equivalent to*

(i′) *$q_{A,\theta} \to 1$, for all $\theta \in \mathrm{NS}(A)$ with $q_A(\theta) = 1$.*

Note that this reduces the *geometric problem* of finding curves on the surface A to a purely *arithmetic problem* involving the quadratic form $q_A \sim xy - q_{E_1,E_2}$.

Before stating the solution to this problem, let us treat a trivial case:

Lemma 48 *If $\Delta(q_{E_1,E_2}) \not\equiv 1 \pmod 4$ and there is an integer $n \equiv 3 \pmod 4$ which is represented by q_{E_1,E_2}, then there is a $\theta \in \mathrm{NS}(A)$ such that $q_{A,\theta}$ is not primitive. In particular, $q_{A,\theta} \not\to 1$.*

Proof. (Sketch) In the non-CM case, this follows immediately from (15). In the CM-case, a similar argument (using (15)) yields the assertion.

In view of this lemma and Theorem 36, Theorem 45 follows from the following result which sharpens Theorem 44:

Theorem 49 *In the situation of* Theorem 44*, put* $\tilde{Q}(x,y,z,w) = xy - q(z,w)$*. Then conditions* (i) – (iv) *of* Theorem 44 *are equivalent to*

(v) $\tilde{Q}_\theta \to 1$*, for all* $\theta \in \mathbb{Z}^4$ *with* $\tilde{Q}(\theta) = 1$*.*

Here $\tilde{Q}_\theta$ *is defined by the analogue of formula* (13)*, i.e. by*

$$\tilde{Q}_\theta(x) = \beta_{\tilde{Q}}(x,\theta)^2 - 4\tilde{Q}(x),$$

where $\beta_{\tilde{Q}}(x,y) = \tilde{Q}(x+y) - \tilde{Q}(x) - \tilde{Q}(y)$ *is the bilinear from associated to* $\tilde{Q}$*.*

Proof. (Sketch) Here we give the main steps of the proof; cf. [35] for the details.

(i) $\Rightarrow$ (ii): trivial.

(ii) $\Rightarrow$ (v): Here one shows (using the conditions that $\Delta(q) \equiv 1 \pmod 4$ or that $q \not\to n \equiv 3 \pmod 4$) that we have the following partial analogue of (15):

$$\{\tilde{Q}_\theta : \theta \in \mathbb{Z}^4 \text{ with } \tilde{Q}(\theta) = 1\} \quad \subset \quad \mathrm{gen}(Q_q).$$

From this, the implication (ii) $\Rightarrow$ (v) follows immediately.

(v) $\Rightarrow$ (iii): Let S denote the set of idoneal numbers satisfying condition (iii) (and/or (ii)) of Theorem 36, i.e.

$$S = \{n \geq 1 : n \not\equiv 3 \pmod 4 \text{ and } 4n \text{ is idoneal}\}.$$

If $q \to n$, and if $n \notin S$, then Propositions 15 and 39 of [34] show that there exists θ with $\tilde{Q}(\theta) = 1$ and a binary quadratic form q' of discriminant $-16n$ such that $q' \not\to 1$ and $\tilde{Q}_\theta \to q'$. (The latter condition means that there exists an injective linear transformation $T : \mathbb{Z}^2 \to \mathbb{Z}^3$ with $\mathbb{Z}^3/\mathrm{Im}(T)$ torsionfree such that $q'(x) = \tilde{Q}_\theta(T(x))$, for all $x \in \mathbb{Z}^2$.) If we have in addition that $n \leq |\Delta(q)|$ (respectively, $n < |\Delta(q)|$ when $n \equiv 3 \pmod 4$), then one can show that it follows that $\tilde{Q}_\theta \not\to 1$, which is contrary to the assumption (v). It thus follows that $n \in S$, and so q is a special idoneal-valued form.

(iii) $\Rightarrow$ (iv): Let q be a special idoneal-valued form, i.e. we have that $q \to n$, $n \leq |\Delta(q)| \Rightarrow n \in S$ (with the *proviso* that if $n \equiv 3 \pmod 4$, then $n \neq |\Delta(q)|$).

The *key observation here* is that by using Weinberger's "at most one-more" theorem (Theorem 22(a)) we can replace the (unknown) set S by the *explicit* set

$$\begin{aligned} S^* &= \{n \in S : n \leq 10^5\} \\ &= \{1,2,4,6,10,12,18,22,28,30,42,58,60,70,78,102,130,190,210,330,462\}, \end{aligned}$$

where the latter equality follows from Euler's (and/or Gauss's) computations; cf. Theorem 1. In other words, subject to the above proviso, we have

$$(23) \qquad q \text{ is a special idoneal-valued form } \Leftrightarrow \{n : q \to n, n \leq |\Delta|\} \subset S^*.$$

To verify this observation, note first that by replacing q be an equivalent form, we may assume without loss of generality that q is reduced, i.e. that $|b| \le a \le c$. Since $q \to a, c$ and $B := a + |b| + c$, and $a, c, B \le |\Delta(q)|$, we see that $a, c, B \in S$.

Now if there is a $d^* \in S \setminus S^*$, then by Euler and Grube (Corollaries 10 and 14) we know that d^* is square-free, and so from Weinberger's Theorem 22(a) it follows that $S = S^* \cup \{d^*\}$, where $d^* > 10^8$ (by numerical computations). Thus, if $c \in S \setminus S^* = \{d^*\}$, then $B = a + |b| + c > c = d^*$, so $B \notin S$, contradiction. Thus, $a, c \le 462$, so $|\Delta(q)| = 4ac - b^2 \le 4 \cdot 462^2 < 10^6 < d^*$, and hence (23) holds.

We therefore have that a, b, c can take on only finitely many *explicit* values. By a straight-forward but extremely tedious check (but suitable for a computer) one can show from this that the (reduced) special idoneal-valued q's are precisely the $q \in \mathcal{L}$. In [35] a more intrinsic argument is given, but it still requires the consideration of many cases.

(iv) ⇒ (i): Here we shall apply the *mass formula* of Eisenstein/Smith/Brandt (cf. Brandt [4]) to the ternary form Q_q. This has the form

$$(24)\quad \sum_{f \in \mathrm{gen}(Q_q)} \frac{1}{|\mathrm{Aut}(f)|} = \frac{-kd}{6 \cdot 2^\nu} \prod_{p|\delta} \left(1 - \frac{1}{p^2}\right) \prod_{p|kd} \left(1 + \left(\frac{d}{p}\right)\frac{1}{p}\right)\left(1 + \left(\frac{-4kr}{p}\right)\frac{1}{p}\right),$$

where $k = \gcd(a, b, c)$, $d = \frac{\Delta(q)}{k^2}$, $\delta = \gcd(4k^2, d)$ and r is any integer represented by $q' := \frac{1}{k}q$ with $(r, d) = 1$. In addition, $2^\nu = 4g(-16k)g(d)$, where, as in §2.2, $g(\cdot)$ denotes the number of genera. Calculating the expression on the right hand side of (24) we find that for each $q \in \mathcal{L}$ this expression equals $\frac{1}{|\mathrm{Aut}(q)|} = \frac{1}{|\mathrm{Aut}(Q_q)|}$, and so it follows that $c(Q_q) = 1$, for all $q \in \mathcal{L}$. Thus (i) holds.

References

[1] E. Bach, Explicit bounds for primality testing and related problems. *Math. Comp.* **55** (1990), 355-380.

[2] P. Bachmann, *Die analytische Zahlentheorie.* Teubner, Leipzig, 1894.

[3] A. Baker, Imaginary quadratic fields with class number 2. *Ann. Math.* **94**, 139–152.

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

[5] W. Briggs, An elementary proof of a theorem about the representation of primes by quadratic forms. *Can. J. Math.* **6** (1954), 353–363.

[6] J. Buchmann, U. Vollmer, *Binary Quadratic Forms.* Springer, Berlin, 2007.

[7] D. Buell, *Binary Quadratic Forms.* Springer-Verlag, New York, 1989.

[8] S. Chowla, An extension of Heilbronn's class-number theorem. *Quart. J. Math.* **5** (1934), 304–307.

[9] S. Chowla, W. Briggs, On discriminants of binary quadratic forms with a single class in each genus. *Can. J. Math.* **6** (1954), 463–470.

[10] D. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication.* Wiley, New York, 1989.

[11] L. Dickson, *Introduction to the Theory of Numbers.* U of Chicago Press, Chicago, 1929.

[12] L. Dickson, *History of the Theory of Numbers* vol. I. Carnegie Inst. 1919; Chelsea Reprint, New York, 1971.

[13] L. Euler, Extrait d'une lettre de M. Euler le pere à M. Bernoulli concernant le memoire imprimé parmi ceux de 1771 p. 318. *Nouveaux mém. acad. scien. Berlin* 1772, 1774, Histoire, pp. 35–36 = Leonhardi Euleri Opera Omnia I, v. 3, Teubner, 1917, pp. 335–337.

[14] L. Euler, Extrait d'une lettre de M. Euler à M. Beguelin (en Mai 1778). *Nouveaux mém. acad. scien. Berlin* 1776, 1779, pp. 337–339 = Leonhardi Euleri Opera Omnia I, v. 3, Teubner, 1917, pp. 418–420.

[15] L. Euler, De formulis speciei $mxx + nyy$ ad numeros primos explorandos idoneis earumque mirabilibus proprietatibus. (Presented 16 March 1778). *Nova acta acad. scien. Petropolitonae* **12** (1794), 1801, pp. 22–46 = Leonhardi Euleri Opera Omnia I, v. 4, Teubner, 1916, pp. 269–289.

[16] L. Euler, Illustratio paradoxi circa progressionem numeronum idoneorum sive congruorum. (Presented 20 April 1778). *Nova acta acad. scien. Petropolitonae* **15** (1799/1802), 1806, pp. 29–32 = Leonhardi Euleri Opera Omnia I, v. 4, Teubner, 1916, pp. 395–398.

[17] G. Frei, Leonhard Euler's convenient numbers. *Math. Intell.* **7**, No. 3 (1985), 55-58, 64.

[18] G. Frey, E. Kani, Curves of genus 2 with elliptic differentials and associated Hurwitz spacces. *Inst. Exp. Math.* (IEM) Preprint No. 6 (1008), 50 pp. To appear in *Contemp. Math.*.

[19] G. Frobenius, Über quadratische Formen, die viele Primzahlen darstellen. *Sitzungsber. Preuss. Akad. Wiss. Berlin* 1912, 966– 980 = *Collected papers* III, Springer-Verlag, Berlin, 1986, pp. 573–587.

[20] C.F. Gauss, *Disquisitiones Arithmeticae.* Translated by A.A. Clarke, 1966. Springer-Verlag, New York, 1986.

[21] E. Grosswald, Negative discriminants of binary quadratic forms with one class in each genus. *Acta Arith.* **8** (1963), 295–306.

[22] F. Grube, Ueber einige Euler'sche Sätze aus der Theorie der quadratischen Formen. *Zeitschrift Math. Physik* **19** (1874), 492–519.

[23] N. Hall, Binary quadratic forms with a single class in each genus. *Math. Z.* **44** (1939), 85–90.

[24] N. Hall, The number of representations function for binary quadratic forms. *Am. J. Math.* **62** (1940), 589–598.

[25] T. Hayashida, A class number associated with a product of two elliptic curves. *Natur. Sci. Rep. Ochanomizu Univ.* **16** (1965), 9–19.

[26] T. Hayashida, M. Nishi, Existence of curves of genus two on a product of two elliptic curves. *J. Math. Soc. Japan* **17** (1965), 1–16.

[27] H. Heilbronn, On the class-number of imaginary quadratic fields. *Quart. J. Math.* **5** (1934), 150–160 = Collected Papers, Wiley, New York, 1988, pp. 177–187.

[28] H. Heilbronn, E. Linfoot On the imaginary quadratic corpora of class-number one. *Quart. J. Math.* **5** (1934), 293–301 = Collected Papers, Wiley, New York, pp. 188–196.

[29] Hua Loo Keng, *Introduction to Number Theory.* Springer-Verlag, Berlin, 1982.

[30] T. Ibukiyama, T. Katsura, F. Oort, Supersingular curves of genus two and class numbers. *Compositio Math.* **57** (1986), 127–152.

[31] M. Jacobson, S. Ramachandran, H. Williams, Numerical results on class groups of imaginary quadratic fields. In: *Algorithmic Number Theory*, Lect. Notes in Comp. Sci. **4076** (2006), Springer, Berlin, pp. 87–101.

[32] B. Jones, *The Arithmetic Theory of Quadratic Forms.* Carus Math. Monographs, MAA; Wiley, New York, 1950.

[33] E. Kani, The number of curves of genus 2 with elliptic differentials. *J. reine angew. Math.* **485** (1997), 93–121.

[34] E. Kani, The moduli space of Jacobians isomorphic to a product of two elliptic curves. Preprint, 39pp.

[35] E. Kani, The existence of Jacobians isomorphic to a product of two elliptic curves. Preprint, 36 pages.

[36] O.-H. Keller, Über die "Numeri idonei" von Euler. *Beiträge Alg. Geo.* **16** (1983), 79-91.

[37] E. Landau, Über die Klassenzahl imaginär-quadratischer Zahlkörper. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Klasse* 1918, 285–295.

[38] G. Mathews, *Theory of Numbers I.* Cambridge U Press, London, 1892.

[39] Miyada, On imaginary abelian number fields of type $(2, 2, \ldots, 2)$ with one class in each genus. *Manuscr. math.* **88** (1995), 535-540.

[40] J. Piehler, Über Primzahldarstellungen durch binäre quadratische Formen. *Math. Ann.* **141** (1960), 239-241.

[41] P. Ribenboim, *The Book of Prime Number Records.* 2nd ed. Springer-Verlag, New York, 1989.

[42] P. Ribenboim, Galimatias Arithmeticae. *Math. Mag.* **71** (1998), 331–340.

[43] H. Stark, On complex quadratic fields with class-number two. *Math. Comp.* **29** (1975), 289–302.

[44] H. Stark, The papers on class numbers of imaginary quadratic fields. In: *The Collected Papers of Hans Arnold Heilbronn* (E. Kani, R. Smith, eds.), Wiley, New York, 1988, pp. 571–575.

[45] J. Steinig, On Euler's idoneal numbers. *Elem. Math.* **21** (1966), 73–96.

[46] J.D. Swift, Note on discriminants of binary quadratic forms with a single class in each genus. *Bull. AMS* **54** (1948), 560–561.

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

[48] G.L. Watson, One-class genera of positive quaternary forms. *Acta Arith.* **24** (1974), 461–475.

[49] G.L. Watson, One-class genera of positive quadratic forms in nine and ten variables. *Mathematika* **25** (1978), 57–67.

[50] M. Watkins, Class numbers of imaginary quadratic fields. *Math. Comp.* **73** (2004), 907–938.

[51] H. Weber, Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist. *Math. Ann.* **20** (1882), 301–329.

[52] H. Weber, Zur complexen Multiplication elliptischer Functionen. *Math. Ann.* **33** (1889), 390–410.

[53] H. Weber, *Lehrbuch der Algebra.* Vol. III. Vieweg, Braunschweig, 1908; Chelsea Reprint, New York.

[54] A. Weil, *Number Theory: An approach through history.* Birkhäuser, Boston, 1964.

[55] P. Weinberger, Exponents of the class groups of complex quadratic fields. *Acta Arith.* **22** (1973), 117–124.