The Legacy of Bernhard Riemann
After One Hundred and Fifty Years
ALM 35, pp. 595–631

Early History of the Riemann Hypothesis in Positive Characteristic

Frans Oort*, Norbert Schappacher†

Abstract

The classical Riemann Hypothesis RH is among the most prominent unsolved problems in modern mathematics. The development of Number Theory in the 19^{th} century spawned an arithmetic theory of polynomials over finite fields in which an analogue of the Riemann Hypothesis suggested itself. We describe the history of this topic essentially between 1920 and 1940. This includes the proof of the analogue of the Riemann Hyothesis for elliptic curves over a finite field, and various ideas about how to generalize this to curves of higher genus. The 1930ies were also a period of conflicting views about the right method to approach this problem.

The later history, from the proof by Weil of the Riemann Hypothesis in characteristic p for all algebraic curves over a finite field, to the Weil conjectures, proofs by Grothendieck, Deligne and many others, as well as developments up to now are described in the second part of this diptych: [44].

2000 Mathematics Subject Classification: 14G15, 11M99, 14H52.

Keywords and Phrases: Riemann Hypothesis, rational points over a finite field.

Contents

1 From Richard Dedekind to Emil Artin **597**

2 Some formulas for zeta functions. The Riemann Hypothesis in characteristic p **600**

3 F.K. Schmidt **603**

*Department of Mathematics, Utrecht University, Princetonplein 5, 3584 CC Utrecht, The Netherlands, Email: f.oort@uu.n

†IRMA, 7 rue René Descartes, 67084 Strasbourg cedex, France; Email: schappacher@math.unistra.fr

4 The Last Entry **604**

5 Hasse's first proof **606**

6 Elliptic curves **608**

7 Hasse's second proof **614**

8 Rational points over a field **614**

9 Deuring's idea and its reception in 1936 **615**

10 The Deuring lifting theorem **621**

11 Reflections on the place of the classical Riemann Hypothesis **622**

Introduction

In 1859, Riemann [52] called a certain behaviour of a certain function "very likely." This conjecture is known today as the "*Riemann Hypothesis*," or RH for short. For details and references see [9], [56].

Historically as well as mathematically, the real conundrum is: where do the Riemann Hypothesis and its avatars belong in the vast and changing landscape of mathematics? The day we will see a proof of the Riemann Hypothesis, this will root and place the statement for the first time. In the meantime, as long as such a mathematical rooting is not available, we may turn to history for help, and investigate where the authors of the last two-and-a-half centuries have placed the Riemann Hypothesis (cf. Section 11 below), and also which analogous statements have been proposed and investigated.

In this note, our main concern is with the arithmetico-geometric avatar of the Riemann Hypothesis which came into focus only in the 20^{th} century, for the first time in Emil Artin's thesis [1], even though, as we will see, it was directly inherited from one of the principal lines of development of Number Theory during the 19^{th} century. This variant of RH is the *Riemann Hypothesis in characteristic p*, or pRH for short (to avoid confusion with Riemann's original RH). The general pRH concerns the zeros of the zeta function attached to a function field over a finite field of constants, or to an algebraic variety over a finite field $\mathbb{F}_q$.

The 40 some cases where Artin [1] computed these zeros and thus checked pRH, first gave substance to this analogue of Riemann's conjecture. After the PhD-thesis of Emil Artin we see F.K. Schmidt [60] in 1931 generalizing and renormalizing the theory of the new zeta function. In 1933, Helmut Hasse managed to prove the first general theorem (see [27]): under certain conditions, he proved pRH for an elliptic curve over a finite field. In the following years, Hasse gave another, more general proof of the elliptic curve case and worked towards a proof for curves of arbitrary genus, using a seminal idea of Max Deuring's. But the breakthrough was achieved by A. Weil—see Milne's chapter [44] in this book.

Our paper will concentrate on these adventurous quests before Weil entered the scene, i.e., on aspects of the developments around pRH in the period 1921–1940; see also the series of papers [54], as well as [58]. We will not touch upon the generalizations of Artin's original questions, nor the more general *Weil Conjectures* of which (a generalized form) of pRH is an important element.

In this paper we present a historical sketch, without any pretense to being complete, and we give remarks from today's point of view, on the mathematical developments of the 1920ies and thirties around pRH.

1 From Richard Dedekind to Emil Artin

While the first half of the 19$^{\text{th}}$ century had been marked by an industrious domain of research which took pride in combining higher arithmetic—specifically the content of C.F. Gauss's *Disquisitiones Arithmeticae* of 1801—with the theories of algebraic integers, of elliptic functions, and with applications of analysis to Number Theory—specifically Dirichlet series—the sun started setting on this *Arithmetic Algebraic Analysis* soon after 1850 (see [23]; cf. Section 11 below). This change is also illustrated by a paper which the young Richard Dedekind—a former student of Dirichlet's, just like Riemann—published two years before Riemann came out with his famous conjecture: in [10], Dedekind showed that the theory of polynomials with integer coefficients which are read modulo a prime[1] allows a self-contained, purely arithmetic treatment that runs parallel to Gauss's presentation of the arithmetic of the rational integers in the first sections of the *Disquisitiones*: unique factorization, quadratic residues, etc. He also derives results peculiar to polynomials, like the factorization of $x^{p^r} - x$ modulo p. Dedekind was not the first to work out these theorems. They had been established earlier by Serret and Schönemann, but appealing to Galois' *irrationnels de la théorie des nombres*, whereas Dedekind derived them in complete analogy with the arithmetic of rational integers. And what is more: as all the perusers of the *Disquisitiones* knew, it was with Gauss's blessing that this arithmetic theory of polynomials modulo a prime could be considered as belonging to Higher Arithmetic, even though Gauss had only announced, and never published his sequel to the *Disquisitiones*, and even though also Dedekind had not yet seen, when he was writing his paper [10], the preliminary version of this theory in the manuscripts that Gauss left behind when he died in 1855.[2]

In other words, the arithmetic theory of polynomials with coefficients modulo p had been in the air for more than half a century; and Dedekind's presentation in 1857 did everything to establish this part of Number Theory as perfectly self-contained, not owing anything to analytic or geometric considerations. In the following decades he would famously coin the notions of *field* and *ideal*, and build a theory of algebraic number fields via ideals, in three successive versions of the XI$^{\text{th}}$ supplement to his edition of Dirichlet's *Lectures on Number Theory*. Dedekind did

[1] 26 year old Dedekind was still under the spell of Gauss and did not yet dare to speak directly of polynomials whose coefficients were residue classes modulo p.

[2] See [16], p. 168, for four convincing arguments to this effect.

not use his 1857 paper [10] as a toolkit for Algebraic Number Theory, for reasons he explained in [11]. The theory of Algebraic Number Fields also had an analytic part, handed down and generalised from Dirichlet, especially from his analytic class number formulas for the theory of quadratic forms. A central function in this analytic part of the theory was what we call today the *Dedekind zeta function* of an algebraic number field which Dedekind, however, wrote

$$\Omega(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{a}^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{p}^s}} \qquad (\Re(s) > 1).$$

Here $\mathfrak{a}$ runs through all ideals, and $\mathfrak{p}$ through all prime ideals, of the ring of integers of the given number field.

1.1. The goal of Emil Artin's thesis (finished in 1921, published in 1924, see [1]) was to extend Dedekind's 1857 theory from the field K of rational functions with rational integer coefficients modulo p, to quadratic extensions $K\big(\sqrt{D(t)}\big)$ of this field, where $D(t)$ is a squarefree polynomial in $\mathbb{F}_p[t]$. The case $p = 2$ is always excluded by Artin. Organising things in conspicuous analogy with the theory of quadratic number fields, Artin first presents the purely arithmetic theory: divisibility, ideals, class number, units, all the way to the quadratic reciprocity law. Then follows the second, analytic part which involves in particular the analogue of the Dedekind zeta function of an algebraic number field, which Artin writes:

$$\mathrm{Z}(s) = \mathrm{Z}_D(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{a}^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{p}^s}} \qquad (\Re(s) > 1),$$

where $\mathfrak{a}$ runs through the integral ideals of $K\big(\sqrt{D}\big)$, and $\mathfrak{p}$ through all prime ideals, which may be grouped according to the underlying prime polynomials of $\mathbb{F}_p[t]$ and their decomposition type in the quadratic extension:

$$\mathrm{Z}(s) = \frac{1}{1 - p^{-(s-1)}} \sum_{F} \Big[\frac{D}{F}\Big] \frac{1}{|F|^s} \qquad (\Re(s) > 1),$$

the summation being over all irreducible polynomials of $\mathbb{F}_p[t]$ which are relatively prime to D and have leading coefficient 1,

$$\Big[\frac{D}{F}\Big] \quad \text{is the quadratic residue symbol,}$$

and $|F| = p^{\deg F}$. This sum, which Artin simply writes down as such, is of course the (analogue of the) Dirichlet L-function for the non-trivial character of the quadratic extension $K\big(\sqrt{D(t)}\big)/K$. Artin then arranges according to

$$\sigma_\nu = \sum_{|F| = p^\nu} \Big[\frac{D}{F}\Big],$$

and thus obtains

$$\mathrm{Z}(s) = \frac{1}{1 - p^{-(s-1)}} \sum_{\nu=0}^{\infty} \frac{\sigma_\nu}{p^{\nu s}} \qquad (\Re(s) > 1).$$

Artin discovers "remarkable reciprocity relations" ([1], p. 209) between the σ_i, linked to the functional equation. Supposing naturally D of degree $n > 0$ (and in fact $n \geq 3$, excluding only trivial cases) one finds $\sigma_\nu = 0$ for $\nu \geq n$, and the study of the zeros of $\mathrm{Z}(s)$ reduces via $z = p^s$ to studying the zeros of the polynomial:

$$z^{n-1} + \sigma_1 z^{n-2} + \sigma_2 z^{n-3} + \cdots + \sigma_{n-1} = \prod_{\nu=1}^{n-1} (z - \beta_\nu).$$

In other words, we have

$$\mathrm{Z}(s) = \frac{1}{1 - p^{-(s-1)}} \prod_{\nu=1}^{n-1} \Big(1 - \frac{\beta_\nu}{p^s}\Big) \qquad (\Re(s) > 1).$$

Artin uses this expression to deduce a precise formula for the number of primes up to a given bound which is "more or less in analogy with the Riemann-Mangoldt formula" ([1], p. 229). And he goes on to show that **assuming** pRH for all "imaginary quadratic fields"—i.e., for fields $K(\sqrt{D})$ where the squarefree polynomial D of degree at least 3 has odd degree or leading coefficient which is not a square modulo p—there are only finitely many such fields with given class number.

Note that the β_ν are not exactly the zeros of the polynomial one usually writes nowadays to formulate pRH, just as the degree $n - 1$ is not necessarily $2g$, for g the genus of the function field $K\big(\sqrt{D(t)}\big)$. In fact, as Artin explains ([1], p. 228), the zeros ρ of $\mathrm{Z}(s)$ are given by $\beta_\nu = p^\rho$, and this includes trivial zeros on the imaginary axis which occur whenever n is even. Once the trivial zeros are eliminated, the analogue pRH of the Riemann Hypothesis for $\mathrm{Z}(s)$ amounts to the statement that $|\beta_\nu| = \sqrt{p}$ for all $\nu = 1, \ldots, n-1$.

1.2. The 40 **examples by E. Artin.** Let us show some of the examples from the tables calculated by Artin, see [1], p. 232–233. They can be checked by counting the number of points on the various curves. We use σ_1 as explained by Artin. We write $\beta = \pi + \overline{\pi}$, and

$$N = N_1 = \#(E(\mathbb{F}_p)) = 1 - \beta + p$$

(notation explained in the next section). We have:

Table I, $\sigma_1 = -\beta$, one point at infinity;

Table II, "komplexe Körper", $\sigma_1 - 1 = -\beta$, see page 234, and no $\mathbb{F}_p$-rational points at infinity;

Table III, "reelle Körper", see page 234, and two $\mathbb{F}_p$-rational points at infinity; in this case $\sigma_1 + 1 = -\beta$: on page 231 we find $\sigma_3 = -p$ and $\sigma_2 = p - 1 - \sigma_1$ and then

$$z^3 + \sigma_1 z^2 + \sigma_2 z + \sigma_3 = (z^2 - \beta z + p)(z - 1), \quad \text{hence} \quad \sigma_1 = -\beta - 1.$$

I, $p = 3$**.** On line 6 of the first table on page 232 for $y^2 = t^3 - t^2 - 1$ and $p = 3$ we find $N = 2, \beta = -\sigma_1 = 1 - N + p = 2$.

I, $p = 5$**.** On the first line for $p = 5$ in the first table we find $y^2 = t^3 + 1$, and we see: $N = 6, \beta = -\sigma_1 = 1 - N + p = 0$.

I, $p = 7$**.** On the first line for $p = 5$ in the first table we find $y^2 = t^3 + 1$, and we see: $N = 12, \beta = 1 - N + p = \sigma_1 = 1 - N + p = 0$ and $\sigma_1 - 1 = \beta$ gives $\sigma_1 = +1$.

II, complex, $p = 3$**.** On the last line of the following table we find $y^2 = -(t^4 - t^2 - 1)$, and we see: $N = 6$, $\beta = 1 - N + 3 = -2$ and $\sigma_1 - 1 = -\beta = +2$ gives $\sigma_1 = +3$.

III, real, $p = 3$**.** On line 4 of the last table we find $y^2 = t^4 + t^2 - t + 1$, and $N = 6$, $\beta = -2$ and $\sigma_1 = -\beta - 1 = +1$

1.3. Artin submitted his thesis for publication in 1921. A manuscript of his from the same year actually generalises the presentation to arbitrary finite fields as field of constants; see [2], cf. [76]. For more details on Artin's thesis and other, earlier precursors of pRH, we refer the reader to the first part of the series of papers [54], which looks back on Artin's work from the point of view of the general arithmetic of function fields over finite fields of constants, as well as to [16].

2 Some formulas for zeta functions. The Riemann Hypothesis in characteristic p

2.1. Lemma. *Let R be an algebra of finite type over $\mathbb{Z}$. For any maximal ideal $M \subset R$ the residue class ring R/M is a finite field.* □

For a ring R as above we define its "zeta function" by

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

where this (Euler) product ranges over all maximal ideals $M \subset R$, and where s is a complex variable. E.g. see [62].

2.2. Examples. (1) In case $R = \mathbb{Z}$ we have the classical Riemann zeta function

$$\zeta_{\mathbb{Z}}(s) = \zeta(s) :$$

any maximal ideal $M \subset R = \mathbb{Z}$ is of the form $M = (p) \subset \mathbb{Z}$, where p is a prime number, and

$$\zeta_{\mathbb{Z}}(s) = \prod_M \frac{1}{1 - \#(R/M)^{-s}} = \prod_p \frac{1}{1 - p^{-s}} = \sum_1^\infty \frac{1}{n^s} (\mathrm{Re}(s) > 1).$$

(2) For the ring of integers in a number field we obtain what is now called the Dedekind zeta function.
(3) For a ring like $R = \mathbb{Z}[T]$, or $\mathbb{F}_p[T]$, we obtain a new type of zeta function.

For these zeta functions (e.g. where $\mathbb{Z}$ is a subring of R) we hope we can extend classical properties of the Riemann zeta function: they should extend to a meromorphic function over the complex plane and they should satisfy a functional equation similar to that of the classical Riemann zeta function. We can ask for their non-trivial zeros (the extended Riemann hypothesis). See [63]. Later these definitions and questions were considered for L-functions (not discussed here).

In his description of the RH as Millennium Problem Bombieri writes: "*Not a single example of validity or failure of a Riemann hypothesis for an L-function is known up to this date. The Riemann hypothesis for $\zeta(s)$ does not seem to be any easier than for Dirichlet L-functions (except possibly for non-trivial real zeros), leading to the view that its solution may require attacking much more general problems, by means of entirely new ideas.*"
`http://www.claymath.org/millennium/Riemann_Hypothesis/riemann.pdf`

We seem to have made no progress for the classical RH in this way. However, we can derive some hope (or perhaps any hint ?) from studying a *special case of this more general situation*:

Examples. For a given prime number p we study rings of finite type over the finite field $\mathbb{F}_p$ (the prime field of characteristic p).
(4) We take $R = \mathbb{F}_q$, and obtain $\zeta_R = 1/(1-q^s)$.
(5) Emil Artin in his PhD-thesis [1] proposed a definition of the zeta function for certain (affine) algebraic curves over a finite field and Artin proposed a pRH for this kind of zeta functions.

2.3. Let V be a variety over a finite field $\kappa = \mathbb{F}_q$. Write $\kappa_n := \mathbb{F}_{q^n}$. We try to understand

$$\{\#(V(\kappa_n)) \mid n \in \mathbb{Z}_{>0}\}.$$

Therefore we encode this package in a formal power series

$$Z(V,T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#(V(\kappa_n))\cdot T^n}{n}\right),$$

or

$$\frac{d\ \log Z(V,t)}{d\ T} = \sum_{n=1}^{\infty} \#(V(\kappa_n))T^{n-1}.$$

Hasse knew that for an elliptic curve over $\mathbb{F}_q$ the value of π, the Frobenius, determines the number of rational points; moreover Hasse knew what would happen under a finite extension of the finite field, see 5.1. Hence we can say that the knowledge of the zeta function describes the set $\{\#(C(\kappa_n)) \mid n \in \mathbb{Z}_{>0}\}$. However the above formula we did not find in the literature before 1940.

2.4. Suppose $V = C$ is a complete, nonsingular, absolutely irreducible curve over κ of genus g. We write

$$\zeta(C,s) = \prod_{\wp} \frac{1}{1-\#(\kappa(\wp)^{-s}}$$

where the product ranges over all points of C, and $\kappa(\wp)$ stands for the residue class field of such a point. It follows that

$$\zeta(C,s) = Z(C,q^{-s}).$$

F. K. Schmidt [60] proved the Rieman-Roch theorem for C and showed

$$Z(C,T) = \frac{P(C,T)}{(1-T)(1-qT)}, \text{ with } P(C,T) = 1 + c_1T + \cdots + c_{2g}T^{2g} \in \mathbb{Z}[T];$$

see 3.2. We write

$$P(C,T) = \prod_{j=1}^{j=2g} (1 - a_jT), \quad a_i \in \mathbb{C}.$$

The Riemann Hypothesis for this curve over the finite field $\kappa = \mathbb{F}_q$ asserts

$$\mid a_j \mid = \sqrt{q} \qquad \text{(pRH)}.$$

This notation is also explained in [44].

In the literature before 1940 we do find a quest for computing the numbers a_j and their absolute values. For example, let E be an elliptic curve over $\mathbb{F}_q$, and let a_1 and a_2, in the above notation, be equal to π and $\overline{\pi}$ (different or equal). Then for $\#(\kappa_n) = q^n$ we have:

$$\#(E(\kappa_n)) = 1 - (\pi^n + \overline{\pi}^n) + q;$$

we see that Gauss, E. Artin and Hasse after computing the numbers π and $\overline{\pi}$ could have used this once this method would have been known to them for computing $\#(E(\kappa_n))$.

As a simple example, take the curve E (the normalization of the completion of the curve) studied by Gauss in his Last Entry, see Section 4; we know for $p = 5$ that $\pi = -1 \pm 2i$ is the Frobenius on this elliptic curve E; we see that $\pi^4 = -7 \pm 24i$, and $\beta = \pi + \overline{\pi} = -14$, hence

$$\#(E(\mathbb{F}_{625})) = 1 - 14 + 625 = 612,$$

something you would not like to compute by hand without using some theory.

2.5. Remark. There is a small difference between the zeta functions $\zeta_R(s)$ and $\zeta(C,s)$ of an affine curve $C^0 = \mathrm{Spec}(R)$, respectively of a curve C. This was already the difference in the approaches of E. Artin and F. K Schmidt: the first did not include "the places at infinity", whereas the second author did.

For a (complete) elliptic curve E over a finite field $\kappa = \mathbb{F}_q$ we have

$$\#(E(\kappa)) = 1 - S + q, \quad \text{with} \quad S := a_1 + a_2 = \mathrm{Tr}(\pi).$$

As $N(\pi) = a_1 \cdot a_2 = q$ we see that $T^2 - ST + q$ gives these two zeros. Hence a simple calculation of $\#(E(\kappa))$ gives the zeta-function of E.

3 F.K. Schmidt

3.1. Friedrich Karl Schmidt in [60] first provided a theoretical framework for pRH which was not restricted to Artin's quadratic extensions, i.e., not restricted to hyperelliptic curves over finite fields. Also the field of constants is now an arbitrary finite field whose order, unusual to modern eyes, is written p while its characteristic is p_0, see [60]. As we know now, Artin had also written up such a generalization of his quadratic case to arbitrary finite fields of constants, but never published it. More importantly, F.K. Schmidt realized the potential of changing the field of constants for the smooth buildup of the theory.

The method adopted by F.K. Schmidt is the general arithmetic theory of function fields over a finite field of constants. This immediately allows him to take into account places at infinity, i.e., to free Artin's theory from the choice of the variable t. Every place $\mathfrak{p}$ of the function field now contributes its Euler factor $(1-|\mathfrak{p}|^{-s})^{-1}$ to F.K. Schmidt's zeta function. Schmidt realizes the importance of the (analogue of the) theorem of Riemann-Roch[3], in particular for the functional equation of the zeta function which is proved in §9. His proof of Riemann-Roch in §6 of [60] is an arithmetic *tour de force*.

The final section §10 of [60], where Schmidt specializes to Artin's case, shows the generality of Schmidt's setting, but also reminds us of the peculiar arithmetic results Artin had obtained, for instance about the class numbers of his rings, and whose generalisation to arbitrary function fields is not in sight. Indeed, the effect of Schmidt's paper for the immediate successors, and in particular for Hasse, was not only to place the subject within the frame of the arithmetic of function fields, but also to strongly focalize around pRH the "analytic number theory" of these fields, which the title announces as the subject of the article [60].

3.2. Schmidt influenced Hasse not only by the published paper, but also communicated that he could write the zeta function (for an arbitrary finite field of constants $\mathbb{F}_q$) in the form

$$\zeta(s) = \frac{L(T)}{(1-qT)(1-T)} \qquad (T = q^{-s}),$$

where $L(T)$ is a polynomial of degree $2g$ (see [54], Part 1, 6.1). This was published in [27], Section 7 on page 257. We shall write

$$L(T) = \prod_{j=1}^{j=2g} (1 - a_j T), \quad a_i \in \mathbb{C}.$$

3.3. As a precursor for the more extensive Weil conjectures, mathematicians between 1921 (Artin's PhD-thesis) and 1940 (what we see as the beginning of the Weil conjectures) studied three properties of the zeta function of a function field (of an algebraic curve) of genus g over $\mathbb{F}_q$:

1. Functional equation. See [60], Satz 22. Also see [27] , Section 5.

[3] Schmidt always writes Riemann - Roche.

2. Rationality. See 3.2 above.

3. pRH. Every "eigenvalue" of the Frobenius morphism a_j, as above, satisfies

$$| a_j | = \sqrt{q} \qquad \text{(pRH)}.$$

Compare with the general Weil conjectures (W1)-(W5), see [44] at the end of Section 1. Properties (1) and (2) were proved by F. K. Schmidt. The pRH was provided by Hasse for elliptic curves. Between 1921 and 1940, several attempts were made to find a proof for pRH function fields (for curves) of arbitrary genus over $\mathbb{F}_q$.

4 The Last Entry

4.1. The text of The Last Entry. An isolated early gem of Arithmetic Algebraic Analysis survived unknown, hidden until the end of the 19th century in Gauss's mathematical notebook, the *Notizen-Journal* as he called it. Personal items had naturally been divided among the children after Gauss's death in 1855. But in the Summer of 1898, Paul Stäckel persuaded Gauss's grandson Carl August Gauß to let the Göttingen Academy borrow the little notebook for use in the edition of Gauss's Collected papers.

The last entry of the *Notizen-Journal* is dated 9 July 1814. By that time, Gauss was no longer using that notebook very much. In fact, the one but the last dated entry is from 23 October 1813 and records the completion of the *general theory of biquadratic residues* (where *general* is underlined) on the very day that a son was born to him. Completing that theory for Gauss meant first of all a systematic development of the arithmetic of what we call the ring $\mathbb{Z}[i]$; this is what he would finally publish in 1832, see [20]. The last entry records a rule which Gauss convinced himself of by computing examples and which he explicitly acknowledged as a most elegant link between that theory of biquadratic residues on the one hand, and elliptic functions related to the integral measuring the arclength of the lemniscate $\int \frac{1}{\sqrt{1-x^4}}$ on the other:

> *Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta, si* $a+bi$ *est numerus primus,* $a-1+bi$ *per* $2+2i$ *divisibilis, multitudo omnium solutionum congruentiae* $1 = xx+yy+xxyy \pmod{a+bi}$ *inclusis* $x = \infty,\ \ y = \pm i,\ \ x = \pm i,\ \ y = \infty$ *fit* $= (a-1)^2 + bb$.
>
> A most important observation made by induction which connects the theory of biquadratic residues most elegantly with the lemniscatic functions. Suppose, if $a + bi$ is a prime number, $a - 1 + bi$ divisible by $2 + 2i$, then the number of all solutions of the congruence $1 = xx+yy+xxyy \pmod{a+bi}$ including $x = \infty,\ \ y = \pm i;\ \ x = \pm i,\ \ y = \infty$, equals $(a-1)^2 + bb$.

The equation given by Gauss is precisely Fagnano's relation between the lemniscatic sine and cosine. This motivates Gauss's four points at infinity.

4.2. Interpretation in modern language. The prime element $a + bi \in \mathbb{Z}[i]$ lies above the rational prime $p = (a + bi)(a - bi) \equiv 1 \pmod 4$ and is the unique generator of the prime ideal $(a+bi)\mathbb{Z}[i]$ that satisfies $a+bi \equiv 1 \pmod{(2+2i)}$. Thus $p = a^2 + b^2$, with $a, b \in \mathbb{Z}$ where a is odd and b is even and $a - 1 \equiv b \pmod 4$. The curve $C \subset \mathbb{P}^2_{\mathbb{F}_p}$ given by the equation $X^2Y^2+X^2Z^2+X^2Z^2 = Z^4$ has two ordinary double points points for $Z = 0$, both rational over $\mathbb{F}_p$ and, because $\sqrt{-1} \in \mathbb{F}_p$ in both points both branches are rational over $\mathbb{F}_p$. The normalization E of C is an elliptic curve. It has two rational points over $\mathbb{F}_p$ above each of those two ordinary double points of C. Let us write

$$N = \#(E(\mathbb{F}_p)) = \#\left(\{(x, y) \in \mathbb{F}_{p^2} \mid 1 = xx + yy + xxyy\}\right) + 4.$$

Gauss expects that

$$N = \mathrm{Norm}(a + bi - 1) = (a - 1)^2 + b^2.$$

Let $\beta = 2a = (a+bi)+(a-bi)$. Then we see in modern terminology that $\pi = a \pm bi$ is the Frobenius on this elliptic curve over $\mathbb{F}_p$, and $T^2 - \beta \cdot T + p$ is its minimal equation.

See the last section of [39] for a hands-on discussion of Gauss's equation, including a numerical example and a proof of Gauss's observation using Jacobi sums.

4.3. Some examples.

***p*=5** Here the $\mathbb{F}_5$-rational points on E are $(x = 0, y = \pm 1), (x = \pm 1, y = 0)$ and the four points at infinity. We obtain $\#(E(\mathbb{F}_5)) = 8$. As $5 = (-1)^2 + 2^2$, with $a - 1 + bi = -2 + 2i$ we see that indeed $\mathrm{Norm}(a - 1 + bi) = 8$. From $\beta = 1 - N + p = -2$ we see that $\pi = -1 \pm 2i$ is a zero of $T^2 + 2T + 5$.

***p*=13** Here the $\mathbb{F}_{13}$-rational points on E are $(x = 0, y = \pm 1), (x = \pm 1, y = 0)$ and the four points at infinity. We obtain $N = 8$, hence $\beta = 1 - N + p = 6$ and $3 \pm 2i$ are the zeros of $T^2 - 6T + 13$.

***p*=17** Here we obtain $\#(E(\mathbb{F}_{17})) = N = 16$, hence $\beta = 1 - N + p = 2$ and $1 \pm 4i$ are the zeros of $T^2 - 2T + 17$.

***p*=29** Here $N = 36$, and $\beta = 1 - N + p = -10$ and $\pi = -5 \pm 2i$ are the zeros of $T^2 + 10T + 29$.

***p*=41** Here $N = 32$, and $\beta = 1 - N + p = 10$ and $\pi = 5 \pm 4i$ are the zeros of $T^2 - 10T + 41$.

4.4. In the introduction to his article [13], Max Deuring has pointed out that if an elliptic function field K_0 with field of constants $k_0 = \mathbb{F}_q$ is defined by the equation $f(x, y) = 0$, then pRH for K_0 is equivalent to the fact that *the norm of* $\pi - 1$*, where* π *is the Frobenius endomorphism, equals the number of solutions of* $f(x, y) = 0$ *over* k_0*, plus the number of prime ideals of* K_0 *of degree one which divide the denominators of* x *or* y*.*

An equivalent reformulation of the Last Entry in modern terminology is as follows:

Let E be given by $Y^2 = X^3 + 4X$ over $\mathbb{F}_p$ with $p \equiv 1 \pmod 4$. Suppose $p = \pi\overline{\pi}$ in $\mathbb{Z}[i]$, $i = \sqrt{-1}$, with $\pi \equiv 1 \pmod{2+2i}$; then

$$\#(E(\mathbb{F}_p)) = 1 - (\pi + \overline{\pi}) + p.$$

See [71], Th. 2.5.

For either model, the curve of which we are counting points over $\mathbb{F}_p$ is the reduction modulo $\pi = a + bi$ of a curve defined over $\mathbb{Q}(i)$ with complex multiplication by $\mathbb{Z}[i]$, of j-invariant 1728. As p is split in $\mathbb{Q}(i)/\mathbb{Q}$ this reduction is an ordinary elliptic curve in characteristic p. What is more, all $\mathbb{F}_p$-rational points on the reduction of the curve are the injective image of the $(\pi - 1)$-division points of the curve in characteristic zero.

Gauss may have seen this. Gotthold Eisenstein in 1850 had all the ingredients to prove it—see [15], cf. [57], §6. But it was Gustav Herglotz who first published a proof of Gauss's Last Entry in 1921, see [35]. In this proof he used the approach just indicated, obtaining the situation over $\mathbb{F}_p$ by reducing modulo π Gauss's curve over $\mathbb{Q}(i)$ which he controls by Weierstrass σ-functions. Herglotz also links the number of points counted to certain quantities that occur in Gauss's first publication on biquadratic residues [19]. This last sort of approach can be used to give other proofs of Gauss's claim. See for instance [8] where the counting of points is translated into properties of sums of Legendre symbols. Cf. the remarks in [42], Chapter 10.

5 Hasse's first proof

5.1. Hasse's strategy. The first proof of pRH for an infinite family of curves over finite fields was given by Hasse in 1933, see [26]. He had followed the budding subject from the very beginning. In his 1924 review of Artin's thesis in the *Jahrbuch Fortschritte der Mathematik* he explicitly noted, rephrasing Artin, that the author had checked pRH in about 40 cases, but that "its proof in general encounters difficulties." Peter Roquette [54] has described in detail how Hasse came to be interested in pRH through the discussion of diophantine questions with Louis Joel Mordell and Harold Davenport, and launched by a remark that Artin made to him in November 1932. Thus embarking on the subject, he naturally relied on the general framework established by F.K. Schmidt.

In [26] on page 257 Hasse notes that in order to give that a proof for pRH for a curve over $\mathbb{F}_q$, it it sufficient to prove the same for that curve E over an extension field $\mathbb{F}_{q^r}$. This is convenient. However in several considerations it seems that q is fixed, that $\pi = \mathrm{Frob}_{\mathbb{F}_q}$, but that other claims, sometimes incorrect for π, do hold for π^r for some r. We will come back to this confusing state of affairs below.

Hasse's crucial idea was to prove the pRH for elliptic curves over finite fields by realizing such a curve as reduction modulo a conveniently chosen prime of a conveniently chosen CM elliptic curve defined over a suitable ring class field of an imaginary quadratic number field. Hasse was helped in this strategy by the fact that in the 1920ies he had worked in depth on the arithmetic theory of complex

multiplication of elliptic curves, i.e., on the explicit class field theory of imaginary quadratic fields, following in particular the work of Teiji Takagi.

Looked at from our vantage point, this first proof which Hasse came up with appears as a direct generalization of Herglotz's argument for the lemniscatic curve which we have briefly sketched in section 4.4 above. Strictly speaking this seems to be wrong on both mathematical and historical grounds. Indeed, for technical reasons, Hasse in [26] excludes extra symmetries working only with CM elliptic curves whose j-invariant is different from 0 and 1728. Furthermore, Roquette [54] has found no evidence that Hasse was aware of Herglotz's article [35].

5.2. Hasse's setup. However that may be, given his elliptic curve over the finite field $\mathbb{F}_q$, where $q = p^f$ and where Hasse assumes that the characteristic p is neither 2 nor 3, he transforms—extending $\mathbb{F}_q$ a bit to $\mathbb{F}_{q^r}$ with r dividing 12, if necessary to adjust the discriminant—the equation of the elliptic curve into Weierstrass normal form

$$2^4 3^3 \eta^2 = \xi^3 - 3\kappa_2 \xi - 2\kappa_3 \qquad \text{with} \quad \kappa_2^3 - \kappa_3^2 = 2^6 3^3, \kappa_2 \neq 0 \neq \kappa_3,$$

and now looks for an imaginary quadratic number field $\Omega = \mathbb{Q}(\sqrt{d})$ and a lattice $\mathfrak{a}$ in Ω such that in its order $o(\mathfrak{a}) = \{\alpha \in \Omega \mid \alpha\mathfrak{a} \subset \mathfrak{a}\}$ one finds a decomposition

$$q^r = \omega \cdot \overline{\omega},$$

and such that in the ring class field of Ω associated to $o(\mathfrak{a})$, for a suitable prime ideal $\mathfrak{P}$ dividing p one has

$$\gamma_2(\mathfrak{a}) \equiv \kappa_2 \pmod{\mathfrak{P}} \quad \text{and} \quad \gamma_3(\mathfrak{a}) \equiv \kappa_3 \pmod{\mathfrak{P}},$$

where γ_2 and γ_3 are given in Weierstrass's notation as

$$\gamma_2(\mathfrak{a}) = 2^2 3 \frac{g_2(\mathfrak{a})}{\sqrt[4]{\Delta(\mathfrak{a})}}, \quad \gamma_3(\mathfrak{a}) = 2^2 3^3 \frac{g_3(\mathfrak{a})}{\sqrt{\Delta(\mathfrak{a})}}.$$

Assuming $\mathfrak{a}$ has been found, Hasse will then adjoin the coordinates of the $\omega - 1$ and the $\omega + 1$ division points of the elliptic curve associated to $\mathfrak{a}$ to the ring class field of $o(\mathfrak{a})$, thus obtaining a certain ray class field of Ω and show that the residue class field modulo a suitable prime $\mathfrak{P}^*$ of this ray class field lying over $\mathfrak{P}$ is precisely $\mathbb{F}_{q^r}$, and that all the elements of this residue class field are precisely swept out by coordinates of the adjoined division points, taken modulo $\mathfrak{P}^*$. This then reduces the counting of points on our initial elliptic curve over $\mathbb{F}_{q^r}$, and therefore pRH for this curve, to an exercise in explicit class field theory of the said ray class field.

Trying to find the CM lattice $\mathfrak{a}$, Hasse encountered difficulties to sort out the eligible j-values, and had to assume that the j-invariant of the initial elliptic curve has odd degree over $\mathbb{F}_p$, which is equivalent to saying that κ_2^3 has odd degree over $\mathbb{F}_p$. Today we know that these were only technical difficulties; in fact, every elliptic curve over $\mathbb{F}_q$ together with an endomorphism can be lifted to characteristic 0. See Section 10 below.

Hasse never came back to remove this technical assumption himself; he soon established pRH for elliptic curves in complete generality by another strategy, see Section 7 below.

Already in 1933 Hasse writes that the number N_1 of rational points of an elliptic curve over $\mathbb{F}_p$ satisfies

$$\mid N_1 - (p+1) \mid < 2\sqrt{p},$$

proved in special cases by Emil Artin, and that this is equivalent to the analogue of the Riemann Hypothesis, see [26], page 253. For an elliptic curve over $\mathbb{F}_q$ in general we have an analogous inequality $\leq$. This is the "Hasse bound", later generalized to curves of higher genus, known under the name of "Hasse-Weil" bound.

6 Elliptic curves

In this section we survey what is known *now* about elliptic curves over finite fields. Several of these results were known and proved by Hasse and Deuring.

6.1. Definition. Let K be a field. An elliptic curve E over K is an absolutely irreducible, nonsingular, complete algebraic curve over K of genus equal to one such that $E(K) \neq \emptyset$.
Equivalent definition. An elliptic curve over a field is an abelian variety of dimension one over that field.
Equivalent definition. An elliptic curve over a field K is a plane cubic nonsingular curve with a rational point over K.

An algebraic curve C over K of genus equal to one such that $C(K) = \emptyset$ should not be called an elliptic curve over K.

Note, by the Schmidt-Witt theorem, see 8.1, that any curve over a finite field has a rational point. Hence over a finite field any genus one curve is an elliptic curve. However note that over $K = \mathbb{Q}$ there exist curves of genus one with no $\mathbb{Q}$-rational point, Selmer, Shafarevich, see Section 8.

Any elliptic curve can be given as a non-singular cubic curve. Normal forms for such curves are available (Weierstrass, Legendre, etc.).

The facts proved by Deuring for elliptic curves over finite fields later had a great impact. It induced Tate to prove more general results for abelian varieties over finite fields, and eventually it emerged in the Honda-Tate theory, classifying isogeny classes of abelian varieties over finite fields, see [75].

6.2. Deuring proved in [13]:
(1) An elliptic curve E over a field $K \supset \mathbb{F}_p$ such that $\mathrm{End}(E) \supsetneqq \mathbb{Z}$ can be defined over a finite field;

this means: there exists a finite field $\kappa = \mathbb{F}_q$, an elliptic curve E_0 over κ and a field K' containing κ and K and an isomorphism $E \otimes_K K' \cong E_0 \otimes_\kappa K'$.

A little warning: some authors say a variety V defined over a field K can be defined over $\kappa \subset K$ if there exists a variety V_0 over κ such that $V_0 \otimes_\kappa K \cong V$; we will refer to this property by saying that V can be descended to κ; this notion is slightly different from the notion used in this paper.

(2) An elliptic curve E over a finite field $\kappa = \mathbb{F}_q$ has $\mathrm{End}(E) \supsetneqq \mathbb{Z}$. This ring $\mathrm{End}(E)$ does have rank two or four over $\mathbb{Z}$.

(3) Ordinary. For elliptic curve E over a finite field $\kappa = \mathbb{F}_q$ the following are equivalent:

- The group $E(\overline{\kappa})$ contains a point of order p.
- The endomorphism ring $\mathrm{End}(E \otimes \overline{\kappa})$ has rank two over $\mathbb{Z}$.
- The endomorphism algebra $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic field in which p is split.
- The elliptic curve E is an ordinary abelian variety over a finite field.

(4) Supersingular. For an elliptic curve E over a finite field $\kappa = \mathbb{F}_q$ the following are equivalent:

- The group $E(\overline{\kappa})$ contains no points of order p.
- The endomorphism ring $\mathrm{End}(E \otimes \overline{\kappa})$ has rank four over $\mathbb{Z}$.
- The endomorphism algebra $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ either is non-commutative, of rank four over $\mathbb{Q}$, or is an imaginary quadratic field in which p is non-split.
- The elliptic curve E over a finite field is not an ordinary abelian variety.

Moreover, if E is a supersingular elliptic curve, then it can be defined over $\mathbb{F}_{p^2}$.

In the Götingen seminar notes [32] it says on page 104 that the endomorphism ring of an elliptic curve over an algebraically closed field of characteristic p can be $\mathbb{Z}$ "in besonderen Fällen" (but no further details are given).

A remark on terminology. An elliptic curve in characteristic zero with endomorphism ring larger than $\mathbb{Z}$ is said to have a singular j-invariant. When Hasse and Deuring discovered that there exist elliptic curves cover a finite field having a larger endomorphism ring, Deuring did choose the terminology "supersingular"; we should say "an elliptic curve with a supersingular j-invariant", too long, so this has been called now a supersingular elliptic curve. In this case $\mathrm{End}^0(E \otimes \overline{\kappa})$ is a quaternion algebra precisely ramified in ∞ and in p, denoted by Deuring as $\mathbb{Q}_{\infty,p}$.

(5) Deuring computed the number of supersingular j-invariants: this equals the class number h_p of $\mathbb{Q}_{\infty,p}$, see [13], § 10.

(6) Deuring proved that an elliptic curve is supersingular if and only if its j-invariant is either $= 0$ in characteristic $p = 2$, or for $p > 2$ it is in Legendre normal form

$$Y^2 = X(X-1)(X-\lambda)$$

and λ is a zero of the polynomial

$$H_p(T) = \sum_{i=0}^{i=(p-1)/2} \binom{(p-1)/2}{i}^2 T^i;$$

also see [24], 4.4.22. In particular this shows supersingular elliptic curves do appear in every positive characteristic. In [14] it was shown that this class number h_p is given by

$$h_p = \frac{1-(\frac{-3}{p})}{3} + \frac{1-(\frac{-4}{p})}{4} + \frac{p-1}{12},$$

where $(\frac{j}{p})$ denotes the Legendre symbol. Equivalently: $h_2 = 1 = h_3$, and

$$h_p = \frac{p-1}{12}, \qquad p \equiv 1 \pmod{12},$$

$$h_p = \frac{p-5}{12} + 1, \qquad p \equiv 5 \pmod{12},$$

$$h_p = \frac{p-7}{12} + 1, \qquad p \equiv 7 \pmod{12},$$

$$h_p = \frac{p-11}{12} + 2, \qquad p \equiv 11 \pmod{12};$$

see [13], page 200. In [38] this result was proved again by showing that the zeros of the polynomial $H_p(T)$ above are simple for every $p > 2$; the group S_3 acts on $\mathbb{P}^1 - \{0, 1, \infty\}$ by substitutions $\lambda \mapsto$

$$\lambda, \quad 1-\lambda, \quad \frac{1}{\lambda}, \quad \frac{1}{1-\lambda}, \quad \frac{\lambda-1}{\lambda}, \quad \frac{\lambda}{\lambda-1}$$

and curves in Legendre normal form are isomorphic if and only if they correspond to each other under such a transformation; the action of this group on the set of zeros of $H_p(T)$ has exactly h_p orbits, as careful bookkeeping shows; this proves again these formulas giving the number of supersingular elliptic curves in positive characteristic.

These polynomials $H_p(T)$ in connection with the Hasse invariant already can be found in [30], page 81; Hasse conjectures what the degree of polynomials giving the supersingular values in the Legendre normal form should be; if one observes that these degrees are positive one could already conclude there exist supersingular elliptic curves in every characteristic; the precise number of supersinglar j values was determined for the first time by Deuring-Eichler.

6.3. Class number computations and applications in connection with abelian varieties generalizing these results by Deuring have been done in many interesting situations (Hashimoto, Ibukiyama, Katsura, Oort and many others).

We say an elliptic curve E has CM if $\mathrm{End}(E) \supsetneqq \mathbb{Z}$. We have seen that an elliptic curve in positive characteristic has CM if and only if it can be defined over a finite field, hence if and only if $j(E) \in \overline{\mathbb{F}_p}$.

For abelian varieties of dimension larger than one this has been generalized. We say a simple abelian variety A of dimension g is a CM abelian variety if $\mathrm{End}^0(A)$ contains a field $L \subset \mathrm{End}^0(A)$ with $[L : \mathbb{Q}] = 2g$. If A is a CM abelian variety defined over a field of characteristic zero, then it can be defined over $\overline{\mathbb{Q}}$.

Tate showed that any abelian variety over a finite field is a CM abelian variety, [74]; note that this was inspired by the results of Deuring, see [7], page 1. Conversely, Grothendieck showed that a CM abelian variety over a field of positive characteristic is isogenous to an abelian variety defined over a finite field, see [47].

For more information, surveys and references see [7].

In the paper [13] by Deuring elliptic curves over finite fields are considered, but at the same time considered over $\overline{\mathbb{F}_p}$. In this way we miss interesting aspects. Such as, that an elliptic curve E can be defined over $\mathbb{F}_q$, that $j(E) \in \mathbb{F}_r \subsetneqq \mathbb{F}_q$ but that E cannot descended directly down to $\mathbb{F}_r$.

Enlarging a finite field elliptic curves can become isomorphic, but new isomorphic classes of elliptic curves are created, even with j-values in smaller fields. For a survey of the classification of isogeny classes of elliptic curves over finite fields see [78], Th. 4.1 on page 536, see [50], 14.6.

Here is an easy example of an abelian variety A defined over $K = \mathbb{F}_{p^2}$, that can be defined over $K_0 = \mathbb{F}_p \subset K$, but A cannot be descended from K to K_0: take $p \equiv 3 \pmod 4$ and A a simple abelian variety over K with Weil-p^2-number $\pi_A = p \cdot \sqrt{-1}$, see [50], 15.2. In [87], Section 3, we find examples of a supersingular elliptic defined over the transcendental extension $K = \mathbb{F}_{p^2}(t)$ that cannot be descended from K to $\kappa = \mathbb{F}_{p^2}$ (although any supersingular elliptic curve can be defined over $\mathbb{F}_{p^2}$, in our definition of this notion).

6.4. Just a reminder. For an elliptic curve E over a finite field $\kappa = \mathbb{F}_q$ and the related Wei q-number $\pi = \pi_E = \mathrm{Frob}_{E/\kappa}$ one of the three cases holds:

- **ordinary.** The endomorphism algebra $\mathrm{End}^0(E)$ is a quadratic imaginary field $L = \mathbb{Q}(\pi)$ over $\mathbb{Q}$ in which p splits; π is imaginary; for any extension $\kappa \subset K$ we have $\mathrm{End}^0(E) = \mathrm{End}^0(E \otimes K)$. (Here E is called ordinary.)
- **ss2.** The endomorphism algebra $\mathrm{End}^0(E)$ is a quadratic imaginary field $L = \mathbb{Q}(\pi)$ over $\mathbb{Q}$ in which p does not splits; π is imaginary; there exists an integer e such that $\pi^e \in \mathbb{Z}$; in that case $\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(E \otimes \mathbb{F}_{q^e})) = 4$. (A supersingular elliptic curve with not all endomorphisms defined over κ.)
- **ss4.** We have $q = p^{2j}$ and $\pi = \pm p^j$. In this case $\mathrm{End}^0(E) \cong \mathbb{Q}_{\infty,p}$. (A supersingular elliptic curve with all endomorphisms defined over κ.)

Note that $\pi \in \mathbb{R}$ but $\pi \notin \mathbb{Z}$ does not occur for elliptic curves, however it does occur for abelian surfaces, see [75], Example (a) on page 97; in this case π_A is quadratic over $\mathbb{Q}$. It seems Deuring was the first to prove that for every elliptic curve E over a finite field we have $\mathrm{End}(E) \neq \mathbb{Z}$.

We note that Hasse did not know this precise classification. Hasse seems to be the first who observed that (ss4) can occur, see [13], page 198: Hasse shows that the case (ss4) above does show up for $p = 3$ (Type III in his terminology). In [28], III §3 we find the question whether $\mathrm{End}^0(E) \stackrel{?}{=} \mathbb{Q}$ is possible for an elliptic curve over a finite field (Type I in his terminology); Hasse asks for the case $\pi = \overline{\pi}$ (hence $\pi \in \mathbb{R}$): "Es wäre interessant zu enscheiden, von welchem der drei Typen I, II, III der Meromorphismenring M in diesem Falle ist"; we know that in this case $\pi \in \mathbb{Z}$ and (ss4) appears, and we know by Deuring that this occurs for every $p \geq 2$. Also in 1937/38 Hasse did not know whether $\mathrm{End}(E) = \mathbb{Z}$ does occur for an elliptic curve over a finite field, see [32], page 104 where is says that over a finite field rank 1 and rank 4 for $\mathrm{End}(E)$ only occurs "in besonderen Fällen", without further explanation.

As we said earlier, it is better to distinguish a variety V over a field K from the "same" variety $V_L = V \otimes L$ over an extension field $L \supset K$. We try to understand what Hasse says in [31], III, especially § 2 and § 3. In the introduction of this paper we see that an elliptic function field K over $k = \overline{\mathbb{F}_p}$ is considered, and $\mathbb{F}_q = k_0 \subset k$ is a finite field over which this function field can be given as K_0. In our notation: $K_0 = k_0(E_0)$ and $K = k(E)$. Hasse describes $M = \mathrm{End}(E)$, and

$$\pi = \pi_{E_0} = \mathrm{Frob}_{E_0/k_0}.$$

In [31], III, on pp. 204-205 Hasse claims that $A = 0$ (i.e. the Hasse invariant is zero, i.e. E is supersingular in our terminology after Deuring) is equivalent with $\beta^2 \neq 0, 4q$ ("die Grenzfälle"). Indeed if E is not supersingular then $0 < \beta < 4q$. However the converse does not hold. The same flaw we find again in Hasse's 1936 Oslo ICM talk [33], on page 204, and in [31], Part III, page 205. In [54], Part 3, 4.4 the same mistake is not spotted but repeated. Below we give examples in every prime characteristic of a supersingular elliptic curve over a field $\mathbb{F}_q$ with $0 < \beta > 4q$.

The difficulty in these considerations is that the ground field is taken algebraically closed, but then E is considered over $\mathbb{F}_q$ and π is taken with that fixed ground field $\mathbb{F}_q$.

6.5. At an early stage Hasse did not know whether an endomorphism of an elliptic curve over a finite field is algebraic or whether it could be transcendental over $\mathbb{Q}$, see [28], the last sentence of § 7.

6.6. Already in 1962 or earlier, Mumford pointed out to Tate that the natural map

$$\mathbb{Z}_\ell \otimes \mathrm{Hom}(A, B) \to \mathrm{Hom}_G(T_\ell(A), T_\ell(B))$$

is an isomorphism for elliptic curves over a finite field, as follows from these results by Deuring (for notation see [74]). It inspired Tate to show this holds for abelian varieties over a finite field, and it inspired Tate also to formulate more general conjectures, see [73]; we see the influence of the seminal paper [13].

6.7. Example. Consider the curve E given over $\mathbb{F}_2$ by $Y^2 + Y = X^3 + X$. This curve is non-singular. We compute $N = \#(E(\mathbb{F}_2)) = 5$ and $\beta = 1 - N + p = -2$. The Frobenius of E is a zero of $T^2 + 2T + 2$, and $\pi = -1 \pm i$. In this case E is supersingular and $0 < \beta^2 < 4p = 8$.

6.8. Example. Consider the curve E given over $\mathbb{F}_3$ by $Y^2 = X^3 - X$. This curve is non-singular. We compute $N = \#(E(\mathbb{F}_3)) = 7$ and $\beta = 1 - N + p = -3$. The Frobenius of E is a zero of $T^2 + 3T + 3$, and $\pi = -(3/2) \pm \sqrt{-3}/2 = \zeta_3 \cdot \sqrt{-3}$. In this case E is supersingular and $0 < \beta^2 < 4p = 12$.

Note that this example is already in Table I of [1], last line of the case $p = 3$; there already we see a supersingular elliptic curve (over $\mathbb{F}_p$) contradicting [27], page 343: "Die Grenzfälle $v = 0$ und $v = \pm 2\sqrt{q}$ sind mit $A = 0$ gleichbedeutend".

6.9. Example. Suppose π is a zero of $T^2 + pT + p^3$. In this case π is not the Frobenius of an elliptic curve over $\mathbb{F}_{p^3}$. See [75], example on page 98.

6.10. Honda-Tate theory. We give $q = p^n$, and we wonder whether for a given $\beta \in \mathbb{Z}$ with $0 \leq \beta^2 \leq 4q$ a zero of $T^2 - \beta \cdot T + q$ can be the Frobenius of an elliptic curve over $\mathbb{F}_q$. This is an exercise in Honda-Tate theory; we will not explain details of this theory, but we refer to [75]; see [50]. This exercise has been explained and solved in [78], Theorem 4.1 on page 536; details have been spelled out in [50], 14.6. Here we give a survey of the answer to the question above. For a given $q = p^n$ and $\beta \in \mathbb{Z}$ with $0 \leq \beta^2 \leq 4q$ (as above) and π a zero of $T^2 - \beta \cdot T + q$ and we look for an elliptic curve over $\mathbb{F}_q$ with $\mathrm{Frob}_{E/\mathbb{F}_q} = \pi$; we have the following possibilities.

- If β is not divisible by p there exists an elliptic curve E over $\mathbb{F}_q$; in this case E is an ordinary elliptic curve.

  Suppose $\beta = ap^j$ with $j \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}$ not divisible by p. The following four cases below give supersingular elliptic curves.

- If $2j \geq n + 2$ then $p = 2$, $a = \pm 1$ and $\beta^2 = 4q = 4p^{2n+2}$.

- If $2j = n+1$ then $p = 2$, or $p = 3$ and $a = \pm 1$ and $0 < \beta^2 < 4q$. We have seen this in examples 6.7 and 6.8. In these cases $\pi^{12} \in \mathbb{Z}$ and $\pi^{12} + \overline{\pi}^{12} = p^{12n}$.

- If $0 < 2j = n$ then $a^2 \leq 4$. If $a = \pm 2$ we have $\beta^2 = 4q$ and $\pi = \pm p^j$.

- Suppose $0 < 2j = n$ and $a = \pm 1$ and $0 < \beta^2 = p^{2j} < 4q$. In this case this is the Frobenius of a supersingular curve over $\mathbb{F}_p$ and $\pi = \zeta_3 \cdot p^j$. This case occurs for every prime number p; in this case $j > 0$ and the curve is supersingular.

- If $0 < 2j < n$ there is no elliptic curve over $\mathbb{F}_q$ with Frobenius a zero of $T^2 + ap^j T + q$; see 6.9.

Conclusion. *There are several cases of a supersingular curve E over a finite field $\mathbb{F}_q$, with $\beta = \pi + \overline{\pi}$ such that $0 < \beta^2 < 4q$. Such cases do appear for every prime*

number p. Note however that in the supersingular case there exists an integer e such that $E \otimes_{\mathbb{F}_q} \mathbb{F}_{q^e}$ has $\pi^e + \overline{\pi}^e = 4q^e$.

If π is imaginary and p is split in $\mathbb{Q}(\pi)/\mathbb{Q}$ and p divides β, a zero of $T^2 - \beta T + q$ is not the Frobenius of an elliptic curve over $\mathbb{F}_q$; in all other cases a zero of $T^2 - \beta T + q$ with $\beta^2 \leq q$ is the Frobenius of an elliptic curve over $\mathbb{F}_q$.

Note that for an elliptic curve over a finite field either β is non-real or $\beta \in \mathbb{Z}$. The real number $\sqrt{p}$ is the Frobenius of an abelian variety, but not of an elliptic curve, see [75], Example (b) on page 97.

In general it is not so easy for a given π as above to determine E. Existence can be proved by analytic parametrization and reduction modulo p, see [36], [75]; an algebraic proof can be found in [6].

7 Hasse's second proof

Already in 1930 Hasse introduced the "Frobenius operator", see [25], see [54], Part 3, 2.5. This endomorphism for an elliptic curve E over $\mathbb{F}_q$ was already by Hasse written as

$$\pi : E \longrightarrow E.$$

In [28], on page 342 we find

$$\pi\overline{\pi} = \mathrm{Norm}(\pi) = q$$

and Hasse shows this implies the pRH; the case $\pi \in \mathbb{Z}$, the case of a supersingular elliptic curve, needed extra care. A crucial aspect is the fact that the anti-involution $\pi \mapsto \overline{\pi}$ comes from complex conjugation in the characteristic zero ring $\mathrm{End}(E)$. For an extensive description, also of Deuring's contribution, see [54], Part 3, Sections 2 and 3.

The anti-involution $z \mapsto \overline{z}$ on $M = \mathrm{End}(E)$ is nowadays called the "Rosati involution", after [55].

An isogeny $E \to E'$ gives an inclusion of function fields $K(E) \supset K(E')$ and conversely. Such concepts were well-know, e.g. see [28], page 125 (but not under the name isogeny). It is unclear to us whether at that time it was known that isogenous elliptic curves give equal zeta functions.

8 Rational points over a field

Theorem 8.1 (F. K. Schmidt 1931, Witt 1934)**.** *Let C be an algebraic curve (complete, non-singular) over a* finite *field $\kappa = \mathbb{F}_q$. Then*

$$C(\kappa) \neq \emptyset.$$

See [60], page 27; [86]; see [54], Part 1, pp. 54–55.

Corollary 8.2. *Let V be a complete, projective variety of positive dimension over a finite field $\kappa = \mathbb{F}_q$. Then*

$$V(\kappa) \neq \emptyset.$$

Proof. For $V \subset \mathbb{P}^n_\kappa$ there exists a hypersurface $H \subset \mathbb{P}^n_\kappa$ such that every irreducible component of $H \cap V$ has dimension equal to $\dim(V) - 1$. Hence for $\dim(V) = d$ there exists hypersurfaces $H_1, \cdots, H_{d-1} \subset \mathbb{P}^n_\kappa$ such that $H_1 \cap \cdots \cap H_{d-1} \cap V$ is a finite union of irreducible (possibly singular) curves. For each of these the normalization has a rational point over κ by the theorem above. Hence $V(\kappa) \neq \emptyset$. □

8.3. Here we consider a curve (complete, non-singular) C over a field K. We define the *exponent* of C, denoted by $f(C, K) = f$ as the smallest degree of an effective divisor on C. We have seen that $f(C, \mathbb{F}_q) = 1$.

For a curve of genus $g > 1$ one can show that over an arbitrary base field $f(C, K)$ divides $2g - 2$.

Theorem (Selmer, 1954). *The curve $C \subset \mathbb{P}^2_{\mathbb{Q}}$ given over $\mathbb{Q}$ as the set zeros of*

$$3X^3 + 4Y^3 + 5Z^3$$

is a non-singular plane curve of genus one, and $C(\mathbb{Q}) = \emptyset$.

In fact, much more is true: this curve has no rational point over any $\mathbb{Q}_p$, and has no rational point over $\mathbb{R}$. See [64], page 205, [65].

Theorem (Shafarevich, 1957). *For every integer b there exists a curve C of genus one over $\mathbb{Q}$ with*

$$f(C, \mathbb{Q}) > b.$$

See [68], see [41], corollary and discussion on page 670, see [72]. In [41] on page 670 we See that Emil Artin conjectured this result that the index is unbounded for an elliptic curve over $\mathbb{Q}$.

9 Deuring's idea and its reception in 1936

At the beginning we have asked where the Riemann Hypothesis is to be situated in the vast and changing landscape of mathematics. It is time to come back to this question, but with respect to the analogue pRH in characteristic p. Of course, the answer to the question may vary according to personal opinions and appreciations of the mathematicians concerned. For Hasse in 1936, after his two proofs for the elliptic case and after the publication of his triptych [31], the arithmetic theory of function fields of one variable over a finite field of constants was the adequate conceptual framework to ground proofs of (special cases of) pRH. He clearly preferred his second proof over the first one, not just because the first proof suffered, at least in [26], from restrictive assumptions, but because *der ganze Aufbau der Theorie hat jetzt rein strukturellen Charakter*, i.e., "the whole setup of the theory is now of a purely structural kind." ([26], p. 55) The natural pride of his considerable achievement would naturally orient his choices for future work on the conjecture which at first remained wide open for curves of higher genus. It is interesting to see how he and others envisaged this future at various junctures. Indeed, it not

only tells us something about Hasse's mathematical orientation, but also about the conditions of doing research at the time.

9.1. How to attack curves of higher genus? Already at the end of his 1933 paper [26], Hasse had pointed out what he called a "formal analogy" of his (first) proof of pRH for (certain) elliptic curves, with Carl Ludwig Siegel's momentous 1929 paper on diophantine approximations [70]:

> To Siegel's principle that at the bottom of algebraic relations between values of power series there is generally a relation between the associated functions, corresponds in my case the principle that at the bottom of the solutions of a congruence there are solutions of a related equation in algebraic numbers. And just as Siegel has solved from there the problem that there are only finitely many quasi-integral solutions of a general binary diophantine equation, via the uniformisation by general abelian functions, it is to be expected that the determination of the number of solutions of *general* binary diophantine congruences can also be performed via the uniformisation by *general* abelian functions, thus proving the analogue of the Riemann Hypothesis for the *general* congruence zeta functions in the sense of F.K. Schmidt. But for this one would have to first develop the complex multiplication for general abelian functions, unless the purely arithmetico-algebraic methods developed by A. Weil in [79] should suffice.

And Hasse repeated the same message at the Oslo ICM in 1936, again with reference to both Siegel and Weil, and then continuing on a much more optimistic note about the immediate future of pRH, see [33], p. 192 :

> The method that I have developed is so general that it also allows to tackle the case of arbitrary genus $g > 1$. It is true that the investigations are not quite finished yet, but very recently Deuring has removed the essential difficulty which still stood in the way of generalizing [my method] from $g = 1$ to $g > 1$, so that the said problem should be completely resolved shortly.

Three questions arise here: What was Deuring's idea? What remained to be done once one had this idea? Why did this research programme not bear quick fruit?

9.2. Deuring's idea. On 9 May 1936, Max Deuring, who at the time was assistant to B.L. Van der Waerden in Leipzig, wrote to Hasse all letters to and from Hasse quoted here are Kept at the manuscript section of staats—and universtiäts — Bibliothek Göttingen):

> In the last few weeks, I have tried to generalize your results for elliptic function fields to fields of higher genus. I have succeeded in doing so, all the way to the construction of the ring of multipliers and the proof that it is algebraic. Since you may already be further ahead in these questions, I enclose the introduction to a projected paper. There the algebraic results are only stated. I have complete proofs of them; but they are still monstrous.

The generalization of Hasse's triptych which Deuring was working towards in 1936 was based on the idea to replace the endomorphism ring of the elliptic curves which Hasse was using, by the ring of *correspondences* from the curve to itself in the higher genus case. We unfortunately do not know Deuring's original manuscripts from that period; from the correspondence between Hasse and Deuring it is obvious that the published papers [12] are the result of considerable reworking in direct exchange with Hasse and H.L. Schmid. But the letter quoted shows that Deuring placed himself squarely within Hasse's research programme on the arithmetic of function fields. We will see shortly that this option was not taken for granted by all the colleagues potentially interested in the work. Different views existed about where to place pRH in the mathematical landscape of the time. Hasse, however, was simply delighted by Deuring's idea and replied to him on 11 May 1936:

> At any rate, I am sure that you have laid the foundations, in particular for overcoming the Riemann Hyopthesis in arbitrary function fields. I am convinced that I will be able to give a proof of the Riemann Hypothesis by combining my own ideas, which I have thought about again these past few weeks, with your results. I want to think about this more precisely as soon as possible, also with a view to a more polished presentation of your proofs.

9.3. Correspondences. In Hurwitz's seminal paper [37], the theory of correspondences was an essentially analytic theory. Later on it was at least partially integrated into the Italian Algebraic Geometry, esp. by Francesco Severi. See [66], as well as the later [67], chapter 6, §§2, 3. But when Emmy Noether in 1919 was writing her report on the various existing arithmetic theories of algebraic functions, she pointed out [45]:

> Just as Riemann's theory [of Riemann surfaces] preceded the other theories historically, even if the rigorous proof of the existence theorems only succeeded later, it has also happened later that with the use of its transcendental tools algebraic questions have been settled which even today are not yet amenable to a purely algebraic or arithmetic treatment; one has to mention here above all Hurwitz's theory of singular correspondences.

By 1936, the situation could have appeared a bit different, especially for Max Deuring in Leipzig, insofar as B.L. Van der Waerden was trying to rewrite quite a bit of algebraic geometry in algebraic language, and thus also in a way which in principle would hold over ground fields of arbitrary characteristic. See for instance his paper [77], cf. [59]. But it seems that Deuring was naturally developing his idea in the context of Hasse's approach, i.e., in the language of the arithmetic of function fields.

9.4. Publicizing Deuring's idea. The day before leaving for Oslo to participate in the ICM, on Sunday 12 July 1936, Hasse found the time to write an eight page letter to Weil, in which, among other things, he explained his understanding of Deuring's idea to Weil in some detail.

Lieber Herr Weil,

. . . . . .

Deuring has had the decisive idea which leads to the generalisation of my theory from the elliptic case to genus $g \geq 1$. It resides in the algebraization of the theory of correspondences of two algebraic function fields, and thus not, as I had always thought, in the use of the field of Abelian functions in g variables.

A correspondence of a field $K|k$ to a field $K'|k$ is according to Hurwitz a conformal mapping of a finite covering surface of K to a finite covering surface of K'. In purely algebraic terms this means (provided the covering surfaces are connected):

There is an isomorphism which relates K' to a subfield $\bar{K}_0$ of a finite extension $\bar{K}$ of K; here $\bar{K}$ is normalised in such a way that $\bar{K} = \bar{K}_0 K$ arises by composition of $\bar{K}_0$ and K, i.e., it is chosen to be as small as possible.

This state of affairs can now be transferred to abstract function fields; for this we suppose that k is algebraically closed.

In order to be able to compute with such isomorphisms, and already to be able to survey their totality, one introduces the field $\mathcal{K} = KK'$, where composition is to be understood such that both components K and K' are regarded as algebraically independent over the field of constants; $\mathcal{K}$ therefore has transcendence degree 2 over k. But we regard $\mathcal{K}$ essentially as an algebraic function field of only one variable, i.e., as $\mathcal{K}|K$ with K as formal field of constants.

. . . . . .

Looking now at the totality of all correspondences from $K|k$ to itself . . . , one obtains a ring. This is the precise generalisation of the meromorphism ring [in the elliptic case].

In order to get from here to the proof of the Riemann Hypothesis, two things are still missing:

First a theory of the behaviour of differentials of the first kind under these correspondences.

Second a generalisation of the theory of the norm, which has to do here with the degree of the field extension $|\ \bar{K}\ :\ \bar{K}_0\ |$.

I have not been long enough in possession of Deuring's theory to have had the time to think through these two generalisations. But one can already see approximately that the Riemann Hypothesis will reduce also in the general case to the analogue of the fact that the well-known hermitian form of the period matrix is positive-definite.

The greatest part of Hasse's long letter is devoted to explaining the translation of correspondences into the language of algebraic function fields. As we know today, the second step of the programme which Hasse outlines, i.e., the "generalisation of the theory of the norm" has never been supplied.

Here is Weil's reaction to Hasse's letter, written in German on 17 July 1936:

> *Lieber Herr Hasse,*
>
> I have read your letter and the enclosed communications with the greatest interest. As you can imagine, the generalization of your theory of the elliptic function fields is particularly close to my heart, and it is very nice that thanks to Deuring's idea the solution of this problem is now in sight. I would therefore like to communicate to you a few remarks which occurred to me when I first read your letter.
>
> It is a very fortunate idea to use singular correspondences to generalize the algebraic theorems of complex multiplication. But as far as the execution sketched in your letter is concerned, the remark may not be superfluous, for various (not only historical) reasons, that several of the required ideas already existed ready to be used. For, after Hurwitz had provided the transcendental theory of correspondences on an algebraic curve in his well-known memoir of 1887, the theory was taken up again by the Italians – in the sense of algebraic geometry, it is true, but in an altogether algebraic spirit. This is well presented in Severi's *Trattato* (Severi, *Trattato di Geometria algebrica*, vol. I, chap. VI, in part. §§60–71, and also the historico-bibliographical sketch on p. 240).
> .....
> It is even more remarkable that Severi unequivocally defines the ring of correspondences on a curve (§69, *Prodotto e somma di due corrispondenze*); and since the correspondences with valence 0 obviously form an ideal in this ring, this yields a quotient ring which is completely identical with Deuring's ring (and with your ring of meromorphisms in the elliptic case).
> .....
> Please do not consider these remarks as in any sense polemical. This I leave to Severi (who, incidentally, is not totally unjustified in the polemics that he directed chiefly against Van der Waerden). I know very well how necessary, and how difficult it is sometimes to translate the already existing results in this domain into the language of modern algebra. But I consider it very important in such investigations never to lose sight of the connections with the older theories, and this not only in order to give the former authors their due (although this is only fair), but chiefly in order not to throw away irreplaceable gauges. This, I think, will also prove to be true in the further development of the problem at hand.
> .....

In addition to Severi's *Trattato* of 1926 mentioned by Weil, there was also available at the time a recent voluminous survey written by Berzolari of the algebraic geometric theory of correspondences that had appeared in 1933 in the *Enzyklopädie* in German translation.

From the correspondence between Hasse and Deuring we can gather that Solomon Lefschetz had essentially the same reaction as Weil, pointing to Severi, when confronted with Hasse's Oslo presentation. As a result Deuring, in the introduction [12], will defend the fact that he publishes his function field version of correspondences at all.

Even though a smooth presentation of Deuring's theory in the language of algebraic geometry over a field of characteristic p would certainly not have been easy to write in 1936, Deuring's paper [12] would provoke Weil's unrelenting sarcasm for many years to come. Weil even vented his feelings in a boastful, and historically debatable footnote to the *Note historique* of Bourbaki's *Commutative Algebra*, see [4], where he alludes to:

> the brillant successes obtained by these "non-rigorous" methods [of the Italian geometers], contrasting with the fact that, until about 1940, the orthodox successors of Dedekind showed themselves incapable of formulating with enough flexibility and power the algebraic notions that would have allowed them to give correct proofs for these results.

9.5. A Göttingen Workshop on Algebraic Geometry in 1937. From January 6 to 8, 1937 Hasse organized a small workshop on algebraic geometry in Göttingen with invited instructional lectures by Heinrich Jung, Harald Geppert, Bartel L. Van der Waerden, and of course Deuring. He had surely hoped to be able to orchestrate a collective effort of learning and working, with positive effects on the proof of the Riemann Hypothesis.

This would not materialize for various reasons. Apart from the widely differing ages and mathematical backgrounds of the participants, there was the major problem, which Hasse actually realized even before the event, that every one of the speakers really spoke "his own dialect" of algebraic geometry. Hasse also invited Weil, who declined with the good reason that he was on his way to Princeton for a few months' stay at the IAS during these days. It is hard to know if he would have come otherwise.

At some point, A. Weil did engage in the battle for pRH. This is evident from his letter to his sister written from Rouen prison, [80], and from the Academy Note, see [81], also see [82]. Hasse considered this note as cheating, see [3], for the ensuing war of reviews. But he may have deceived himself about Weil's potential to come up with a proof in the end.

9.6. The German-Italian axis. Hasse's last paper promoting the research programme towards pRH for curves of any genus, based on the arithmetic theory of algebraic function fields and Deuring's idea, was published in Italian [34], in the proceedings of a congress that could not actually take place because of the war. Its explicit aim was to "facilitate for the Italian school of algebraic geometry the access to a field which is being cultivated at various places in Germany, and in which algebra and arithmetic are coming together." ([34], p. 85) There is a fleeting reference to Severi's chapter on congruences in his *Trattato* ([34], p. 94, note (3)), but otherwise no effort is made to render the presentation palatable to a reader who is well-versed in algebraic geometry, but has little experience with

the function-field language. Towards the end ([34], p. 138, note (1)) Hasse briefly comments on other papers of Severi's which the latter had indicated to him in their correspondence.

The paper ends with Hasse recalling his first proof of pRH for certain elliptic curves, which proceeded via lifting to characteristic 0, saying that it appears to him *unfair* by comparison with the straight development of the arithmetic theory of function fields in characteristic p, which will in the end also yield the general pRH.

We know today that he was right about the possiblity of giving such a proof because his student Roquette did it in [53]. But between Hasse's Italian paper and this thesis, a new language and practice of algebraic geometry had been created, not in Europe in the 1930ies and 1940ies—in spite of the seminal ideas published by Van der Waerden—but in the US, under the independent inspirations of André Weil and Oscar Zariski.

10 The Deuring lifting theorem

In this section $\kappa = \mathbb{F}_q$ will be a finite field. In his *first* proof of the pRH Hasse needed the fact that an elliptic curve over a finite field together with an endomorphism could be CM lifted to a field in characteristic zero. Hasse had to make exceptions for his proof to work. That made his proof incomplete.The full CM lifting theorem for elliptic curves was proved by Deuring.

Theorem 10.1 (Deuring, 1941)**.** *Let E_0 be an elliptic curve over κ, and $b \in \mathrm{End}(E_0)$. The pair (E_0, b) can be lifted to characteristic zero.*
By this we mean: there exists an integral domain R of characteristic zero, a homomorphism $R \to \kappa$, an elliptic curve $\mathcal{E}$ over R, and an element $b \in \mathrm{End}(\mathcal{E})$ such that $(\mathcal{E}, b) \otimes_R \kappa \cong (E_0, b)$. This theorem was stated and proved in [13] page 259 and pp. 259–263 over the algebraic closure of a finite field; however once the theorem is proved for the residue class field $\overline{\kappa}$, the result follows for the residue class field κ. Also see [69]. For a modern proof see [46] and [48], Th. 14.6 and pp.192–193.

10.2. Remark. A well-known theorem by Serre and Tate shows that any (A_0, b) where A_0 is an ordinary abelian variety, and $b \in \mathrm{End}(A_0)$ can be lifted to characteristic zero, see [43] Coroll. 1.3 on page 178.

Such a pair (A_0, b) can be lifted to characteristic zero in case the p-rank of A_0 is at least $\dim(A_0) - 1$ (sometimes called "the almost ordinary case"), see [48], Th. 14.6; in particular this covers the case of elliptic curves.

For any $g \geq 2$ there exist (many) examples of pairs (A_0, b), where A_0 is an abelian variety of dimension g and $b \in \mathrm{End}(A_0)$ over an algebraically closed field $k \supset \mathbb{F}_p$ such that the pair (A_0, b) cannot be lifted to characteristic zero; see [49], and for more information see [7].

10.3. Remark. More specifically: any abelian variety over a finite field is a CM abelian variety by [74], and one can ask whether it can be lifted to a CM abelian variety in characteristic zero.

Honda and Tate proved that *after extending the base field and choosing an appropriate isogeny such a lift exists*, [75], Th. 2. In [49] we see many examples of abelian varieties over $k = \overline{\mathbb{F}_p}$ that do not admit a CM lift, i.e. in general an isogeny is necessary, even over k. In [7] this question is further studied and we see a complete answer: for an abelian variety A_0 over a finite field κ there exists an isogeny $A_0 \sim B_0$ over κ and a CM lift of B_0 to characteristic zero. After more than 70 years the problem, stated and proved for elliptic curves by Hasse and Deuring, is thus generalized to all abelian varieties over a finite field and their CM liftings.

11 Reflections on the place of the classical Riemann Hypothesis

Riemann's statement of RH—see [52], p. 148 in the *Gesammelte Werke*—to the effect that "very probably" all the roots of the function

$$\xi(t) = \frac{1}{2}s(s-1)\Gamma\big(\frac{s}{2}\big)\pi^{-\frac{s}{2}}\zeta(s), \qquad \text{where} \quad s = \frac{1}{2} + ti,$$

are real, ostensibly belongs to complex function theory, or more precisely to the chapter of it which is often called "Special Functions," because it only concerns a specific function (and its generalisation GRH, a specific class of functions). The *Jahrbuch über die Fortschritte der Mathematik* did not exist yet when Riemann published his seminal paper, but when the first *Jahrbuch* appeared in 1868, it did classify, for instance, a paper by Curtze on Lambert's series and the law of prime numbers under its "Chapter 2. Special series" of "Section five : Series."

This pigeonholing of the conjecture is obviously unsatisfactory, already because when one goes through the list of prominent special functions, just what is special about them has to be found out in each and every single case, and rarely points to a specific subdiscipline of mathematics. Furthermore, there are many equivalent formulations of RH, and there are analogues in different settings. Once we will see a proof of the Riemann Hypothesis, this will root and place the statement for the first time. In the meantime, as long as such a mathematical rooting is not available, we may turn to history for help, and investigate where the authors of the last two-and-a-half centuries have placed the Riemann Hypothesis and its avatars.

When Euler solved the "Basel problem," i.e., when he first evaluated

$$\sum \frac{1}{n^2} = \frac{\pi^2}{6}$$

in 1735, and later proved it, when he obtained the product formula

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1-\frac{1}{p^s}}, \qquad \text{where} \quad \mathrm{Re}(s) > 1,$$

for the function that was not yet called $\zeta(s)$, when he even established a relation which we recognise as a variant of the functional equation for the Riemann zeta

function, all these achievements are in the first place and above all pieces of 18^{th} century real analysis. See the extremely careful reading of Euler's paper **E352** in [40]. Cf. [84] for the early history of "Riemann's" zeta function.

Yet prime numbers, whose distribution would be the explicit subject of Riemann's 1859 paper, are already part of the story. And when Euler started to analytically measure their infinity through the divergence of the sum of their reciprocals, the tabulation of primes was about to develop into one of the important, if often overlooked, sources which would not only make Gauss as a young man fill his odd hours of leisure by counting prime numbers in given intervals of thousands, but which would finally be integrated into the new number theory that was shaped during the long 19^{th} century. See [5], in particular 4.3.

In his informal lecture [83], page 293: André Weil writes: ".. aspects which we now classify as 'analytic number theory', which to me, as I told you, is not number theory at all", famously excluding analytic number theory from what he accepts as Number Theory and bemoans the—indeed surprising, given Riemann's education—fact that "of all the great mathematicians of the last century, [Riemann] is outstanding for many things, but also, strangely enough, for his complete lack of interest in number theory and algebra." One might try to object that not only does the title of Riemann's 1859 paper sound like number theory: *On the number of prime numbers below a given quantity*, but Weil himself in a later paper [85] has suggested that Riemann's treatment of 'his' zeta function may very well have been prompted by the case of a quadratic Dirichlet L-series which Eisenstein may have showed him. Such a connection—whether it was immediately brought about by Eisenstein's influence, as Weil suggests, or whether it only existed by way of a lasting influence of Riemann's education with Dirichlet—would indeed link the 1859 paper, and thus also the Riemann Hypothesis, to the integrated domain of *Arithmetic Algebraic Analysis* which a historical analysis of research activities between the 1820ies and 1850ies establishes as the peculiar hybrid state that Number Theory found itself in during that period—see [23].

Indeed, Riemann's teacher Dirichlet had been one of the protagonists of Arithmetic Algebraic Analysis when he combined his keen reading of Gauss's *Disquisitiones Arithmeticae* with the new analysis he had learned in Paris. His theorem on primes in arithmetic progressions and his analytic theory of quadratic forms, which by the end of the 19^{th} century would be reinterpreted as class number formulae for (quadratic) number fields, initiated the analytic part of what would evolve into Algebraic Number Theory.

But to be sure, Weil is fundamentally right about Bernhard Riemann. The latter does not at all do what practitioners of Arithmetic Algebraic Analysis used to delight in: to combine notions from Gauss's *Disquisitiones* or their analogues for more general rings of algebraic integers, with the theory of elliptic functions, the resolution of algebraic equations, or with analytic techniques like those invented by Dirichlet. The connection of RH with Arithmetic Algebraic Analysis, however much of it can actually be established, is therefore extremely tenuous. Riemann does not engage the functions which he uses to estimate the frequency of primes in any systematic arithmetic theory. As a matter of fact, Riemann's 1859 paper appeared at a time when the integrated domain of Arithmetic Algebraic Analysis

was about to give way to a clearer division of disciplines and labour in and around Number Theory.

In his Berlin lecture course of the Winter term 1876–76, Leopold Kronecker—who in his long career would carry the programme of Arithmetic Algebraic Analysis further than any other mathematician of his century—had this to say about Riemann's 1859 paper (see p. 38 of the notes taken by Hettner of Kronecker's course on *Anwendung der Analysis des Unendlichen auf die Zahlentheorie* in the Library of IRMA, Strasbourg):

> ... From this Riemann has actually exhibited in the Monthly reports of the Berlin Academy (around 1860) a series of functions on which the number of prime numbers depends. These functions are very irregular, they stray all the time along the border of convergence. But in this way Riemann has implicitly given an analytic expression for the number of primes up to a certain bound. This expression is not very satisfactory, however. What is lacking is a precise determination to know the bounds between which the expression is situated. But Riemann's investigation constitutes a progress that has to be marked in the annals of mathematics. It was Riemann's force—however strange the functions may be—to produce their analytic expressions.

We see that Kronecker, and also Weil much later, tended to place the origin of the Riemann Hypothesis outside of the realm of Number Theory. And when Frobenius in his 1901 evaluation of Edmund Landau's second thesis (*Habilitation*) openly criticised Landau's "extremely narrow domain" of research around the RH and admonished the young candidate to turn to "other questions of a more general interest and higher relevance," this also suggests a relative isolation of the Riemann Hypothesis with respect to the rest of mathematics. But not all mathematicians at the turn from the 19^{th} to the 20^{th} century can have shared these opinions because, for instance, a paper by Mangoldt on the distribution of the zeros of $\zeta(s)$ was classified in the 1900 *Jahrbuch über die Fortschritte der Mathematik* in Chapter 2. Number Theory, Section A. General.

Today of course, analytic number theoretic is recognized as an active subdiscipline of mathematics. We just do not know whether it will one day carry by itself a proof of RH.

References

[1] E. Artin – *Quadratische Körper im Gebiet der höheren Kongruenzen, I & II.* Math. Zeitschr. **19** (1924), 153–206, 207–246.

[2] E. Artin – *Quadratische Körper über Polynombereichen Galois'scher Felder und ihre Zetafunktionen.* Abh. Math. Sem. Hamburg **70** (2000), 3–30. [Text aus dem Nachlaß Emil Artin November 1921.]

[3] M. Audin – *La guerre des recensions. Autour d'une note d'André Weil en 1940.* Mathematische Semesterberichte **59** (2012), 243–260.
`arXiv:1109.5230`

[4] N. Bourbaki – *Elements of the history of mathematics*, transl. by J. Meldrum. Berlin, Heidelberg, etc., Springer-Verlag, 1994.

[5] M. Bullynck – *Factor tables 1657–1817, with notes on the birth of Number Theory.* Revue d'historie des mathématiques **16** (2010), 141–224.

[6] C-L. Chai and F. Oort – *An algebraic construction of an abelian variety with a given Weil number.* [To appear in Journ. Algebraic Geometry.]

[7] C-L. Chai, B. Conrad and F. Oort – *Complex multiplication and lifting problems.* Mathematical Surveys and Monographs 195. American Mathematical Society, Providence, RI, 2014.

[8] S. Chowla – *The Last Entry in Gauss's Diary.* Proceedings of the National Academy of Sciences of the United States of America **35** (1949), 244–246.

[9] B. Conrey – *Riemann's hypothesis.* [This volume]

[10] R. Dedekind – *Abriß einer Theorie der höheren Kongruenzen in Bezug auf einen reellen Primzahl-Modulus.* Journal reine und angew. Math. **54** (1857), 1–26. *Gesammelte mathematische Werke I*, pp. 40–67.

[11] R. Dedekind – *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen.* Abhandlungen Kgl. Ges. der Wiss. Göttingen **23** (1878), 1–23. *Gesammelte mathematische Werke I*, pp. 202–232.

[12] M. Deuring – *Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper.* Part I; Journal reine und angew. Math. (Crelle) **177** (1937), 161–191; Part II; Journal reine und angew. Math. (Crelle) **183** (1941), 25–36.

[13] M. Deuring – *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272.

[14] M. Eichler – *Über die Idealklassenzahl total definiter Quaternionenalgebren.* Math. Z. **43** (1938), 102–109.

[15] G. Eisenstein – *Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt.* Journal reine und angew. Math. (Crelle) **39** (1850), 160–179; and the sequel:
Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, nebst Anwendungen derselben auf die Zahlentheorie. Journal reine angew. Math. (Crelle) **39** (1850), 224–287 [= Mathematische Werke, vol. II, pp. 536–619].

[16] G. Frei – *The unpublished Section Eight: On the way to function fields over finite fields.* In [22], chap. II.4, pp. 159–198.

[17] *C.F.Gauss Gedenkband anlässlich des 100 Todestag.* Teubner 1957.
G. Rieger – *Die Zahlentheorie bei C.F. Gauss;* p. 37–77.

[18] C. Gauss – *Disquisitiones Arithmeticae.* Fleischer, Leipzig 1801.
Translation by A. Clarke: *Disquisitiones Aritmeticae.* Yale University Press, 1966.

[19] C. Gauss – *Theoria residuorum biquadraticorum. Commentatio prima.* Commentationes soc. reg. sc. Gotting. recentiores VI, Gottingae 1828. Reprinted in *Werke*, vol. II.

[20] C. Gauss – *Theoria residuorum biquadraticorum. Commentatio secunda.* Commentationes soc. reg. sc. Gotting. recentiores VII, Gottingae 1832. Reprinted in *Werke*, vol. II.

[21] C. Gauss – *Tagebuch,* 1796–1814. Rediscovered (1897) and published (1903) by F. Klein.
C. Gauss, *Mathematisches Tagebuch,* 1796–1814. Edited by K-R. Biermann; Ostwalds Klassiker der Exakten Wissenschaften 256 (Fifth ed.), Verlag Harri Deutsch, Frankfurt am Main, 2005.

[22] C. Goldstein, N. Schappacher, J. Schwermer (eds.) – *The Shaping of Arithmetic after Gauss's* Disquisitiones Arithmeticae. Springer, 2007.

[23] C. Goldstein and N. Schappacher – *A book in search of a discipline.* In [22], chapt. I.1. pp. 3–65.

[24] R. Hartshorne – *Algebraic geometry.* Graduate Texts in Mathematics 52, Springer, 1977.

[25] H. Hasse – *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, II: Reziprozitätsgesetz.* Jahresbericht Deutsche Math.-Verein. **6** (Ergänzungsband), 1930.

[26] H. Hasse – *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktion in gewissen elliptischen Fällen. Vorläufige Mitteilung.* Nachr. Ges. d. Wiss. Göttingen, Math.-Phys. Kl. 1933; pp. 253–262.
Helmut Hasse – Mathematische Abhandlungen. De Gruyter, 1975; Band 2, p. 85–108.

[27] H. Hasse – *Über die Kongruenzzetafunktionen.* Unter Benutzung von Mitteilungen von Prof. Dr. F. K. Schmidt und Prof. Dr. E. Artin. Sitzungsber. Preuss. Akad. Wissenschaften **H17** (1934), 250–263.

[28] H. Hasse – *Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern.* Abh. Math. Sem. Hamburg, **10** (1934), 325–348.
Helmut Hasse – Mathematische Abhandlungen. De Gruyter, 1975; Band 2, pp. 109–132.

[29] H. Hasse – *Zur Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit volkommenem Konstantenkörper bei beliebiger Charakteristik.* Journal reine und angew. Math. (Crelle) **175** (1936), 50–54.
Helmut Hasse – Mathematische Abhandlungen. De Gruyter, 1975; Band 2, pp. 218–222.

[30] H. Hasse – *Existenz separabler zyklischer umverzweigter Erweiterungskörper vom Primzahlgrad p über elliptischen Funktionenkörpern der Charakteristik p.* Journal reine und angew. Math. (Crelle) **172** (1934), 77–85.
Helmut Hasse – Mathematische Abhandlungen. De Gruyter, 1975; Band 2, pp. 161–169.

[31] H. Hasse – *Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung.* Journal reine und angew. Math. (Crelle) **175** (1936), 55–62.
H. Hasse – *Zur Theorie der abstrakten elliptischen Funktionenkörper II. Automorphismen und Meromorphismen. Das Additionstheorem.* Journal reine und angew. Math. (Crelle) **175**(1936), 69–88.
H. Hasse – *Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung.* Journal reine und angew. Math. **175** (1936), 193–208.
Helmut Hasse – Mathematische Abhandlungen. De Gruyter, 1975; Band 2, pp. 223–230, 231–250, 251–266.

[32] H. Hasse – *Korrespondenzen algebraischer Funktionenkörper und die Riemannsche Vermutung.* Seminar im Wintersemester 1937/38. Seminar notes, 132 pp. SUB Göttingen, Abteilung für Handschriten und ältere Drucke, Cod MS H. Hasse 11 – 8.

[33] H. Hasse – *Über die Riemannsche Vermutung in Funktionenkörper.* Compt. Rend. ICM Oslo 1936. A.W.Brøgger, Oslo, 1937; pp. 189–206.

[34] H. Hasse – *Punti razionali sopra curve algebriche a congruenze.* Reale Accademia d'Italia, Fondazione Alessandro Volta. Atti dei Convegni vol. 9 (1943), 85–140. Reproduced in *Mathematische Abhandlungen*, Band 2, 295–350.

[35] G. Herglotz – *Zur letzten Eintragung im Gaußschen Tagebuch.* Ber. Math.-Phys. Kl. Sächs. Akad. Wiss. Leipzig **73** (1921), 271–276. Reproduced in *Gesammelte Schriften* (H. Schwerdtfeger, ed.), pp. 415–420.

[36] T. Honda – *Isogeny classes of abelian varieties over finite fields.* Journ. Math. Soc. Japan **20** (1968), 83–95.

[37] A. Hurwitz – *Über algebraische Korrespondenzen und das verallgemeinerte Korrespondenzprinzip.* First published in Berichte Leipziger Akademie 1887; later also in Math. Annalen **28** (1887), 561–581. Reproduced in *Werke*, vol. I, pp. 163–188.

[38] J-I. Igusa – *Class number of a definite quaternion with prime discriminant.* Proc. Nat. Acad. Sci. U.S.A. **44** (1958), 312–314.

[39] K. Ireland, M. Rosen – Elements of number theory, including an introduction to equations over finite fields. Bogden & Quigley Publishers 1972.

[40] E. Landau – *Euler und die Funktionalgleichung der Riemannschen Zetafunktion.* Bibliotheca Mathematica (3) **7** (1906), 69–79. Reproduced in *Collected Works*, vol.2, pp. 335–345.

[41] S. Lang and J. Tate – Principal homogeneous spaces over abelian varieties. Amer. J. Math. **80** (1958), 659–684

[42] F. Lemmermeyer – *Reciprocity Laws, from Euler to Eisenstein.* Springer, 2000.

[43] W. Messing – *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes.* Lecture Notes in Mathematics, Vol. 264. Springer-Verlag, Berlin-New York, 1972.

[44] J. Milne – *The Riemann Hypothesis over finite fields. From Weil to the present day.* This volume.

[45] E. Noether – *Die arithmetische Theorie der algebraischen Funktionen einer Veränderlichen in ihrer Beziehung zu den übrigen Theorien und zu der Zahlkörpertheorie*. Jahresbericht D.M.V. 28 (1919), 182–203. Reproduced in Emmy Noether's *Gesammelte Abhandlungen — Collected Papers* (Springer-Verlag 1983): pp. 271–292, however with incomplete title, and with the last footnote missing.

[46] F. Oort – *Lifting an endomorphism of an elliptic curve to characteristic zero.* Nederl. Akad. Wetensch. Proc. Ser. A 76=Indag. Math. **35** (1973), 466–470.

[47] F. Oort – *The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field.* J. Pure Appl. Algebra **3** (1973), 399–408.

[48] F. Oort – *Lifting algebraic curves, abelian varieties, and their endomorphisms to characteristic zero.* Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), 165–195, Proc. Sympos. Pure Math., 46, Part 2, Amer. Math. Soc., Providence, RI, 1987.

[49] F. Oort – CM-*liftings of abelian varieties.* J. Algebraic Geom. **1** (1992), 131–146.

[50] F. Oort – *Abelian varieties over finite fields.* In: Proceed. NATO Adv. St. Inst. on higher-dimensional geometry over finite fields, Göttingen 2007. NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., Vol. **16**; IOS Press, Amsterdam, 2008; pp. 123–188.

[51] R. Rankin – *Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions.* Math. Proceed. Cambridge Philos. Soc. **35** (1939), 357–372.

[52] B. Riemann – *Über die Anzahl der Primzahlen unter einer gegebenen Grösse.* Monatsberichte der Berliner Akademie, November 1859; 6 pp.

In: Monath. der Kgl. Tm Preuss. Akad. der Wissen. zu Berlin aus dem Jahre 1859 (1860), 671– 680; also, Gesammelte math. Werke und wissensch. Nachlass, 2. Aufl. 1892, 145–155.

[53] P. Roquette – *Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunktionenkrpern beliebigen Geschlechts.* Journal reine und angew. Math. (Crelle) **191** (1953), 199–252.

[54] P. Roquette – *The Riemann hypothesis in characteristic p, its origin and development.* Part I: *The formation of the zeta-functions of Artin and of F. K .Schmidt.* Hamburger Beiträge zur Geschichte der Mathematik. Mitt. Math. Ges. Hamburg **21** (2) (2002), 79–157.
`http://www.rzuser.uni-heidelberg.de/~ci3/rv.pdf`
Part 2: *The first steps by Davenport and Hasse;* **22** (2004), 5–74.
`http://www.rzuser.uni-heidelberg.de/~ci3/rv2.pdf`
Part 3: *The elliptic case;* **25** (2006), 103–176.
`http://www.rzuser.uni-heidelberg.de/~ci3/rv3.pdf`
Part 4: *Davenport-Hasse fields;* **32** (2012), 145–210.
`http://www.rzuser.uni-heidelberg.de/~ci3/rv4.pdf`
manuscripts by P.Roquette:
`http://www.rzuser.uni-heidelberg.de/~ci3/manu.html`

[55] C. Rosati – Sulle corrispondenze algebriche fra i punti di due curve algebriche. Annali di Matematica Pura ed Applicata **3** (28) (1918), 35–60.

[56] M. Rubinstein – *Riemann's influence in number theory from a computational and experimental perspective.* [This volume]

[57] N. Schappacher – *Some Milestones of Lemniscatomy.* In S. Sertöz (ed.) : Algebraic Geometry. Proceedings Bilkent Summer School, Ankara 1995. Lecture Notes in Pure and Applied Mathematics Series 193. New York: M. Dekker 1997; pp. 257–290.

[58] N. Schappacher – *Seventy years ago: The Bourbaki Congress at El Escorial and other mathematical (non)events of 1936.* The Mathematical Intelligencer, Special issue International Congress of Mathematicians Madrid August 2006, 8–15.

[59] N. Schappacher – *A Historical Sketch of B.L. van der Waerden's work on Algebraic Geometry 1926-1946.* In J.J. Gray & K.H. Parshall (eds.) : Episodes in the History of Modern Algebra (1800-1950). History of mathematics series, vol. 32, AMS / LMS (2007) 245–283.

[60] F. K. Schmidt – *Analytische Zahlentheorie in Körpern der Charakteristik p.* Math. Zeitschr. **33** (1931), 1–32. (Habilitationsschrift)

[61] F. K. Schmidt – *Zur arithmetischen Theorie der algebraischen Funktionen I.* Math. Zeitschr. **41** (1936), 415–438.

[62] J-P. Serre – *Zeta and* L *functions.* Arithmetical algebraic geometry (Proc. Conf. Purdue Univ., 1963), pp. 82–92. Harper & Row, New York, 1965.

[63] J-P. Serre – *Facteurs locaux des fonctions zêta des variétés algébriques* (définitions et conjectures). Sém Delange-Pisot-Poitou **11** (1969/70), no. 19.

[64] E. Selmer – *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$. Acta Math. **85** (1951). 203–362.

[65] E. Selmer – *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$. *Completion of the tables.* Acta Math. **92** (1954). 191–197.

[66] F. Severi – *Sul principio della conservazione del numero*. Rendiconti del Circolo Matematico di Palermo **33** (1912), 313–327.

[67] F. Severi – *Trattato di geometria algebrica*. Nicola Zanichelli, Bologna, 1926.

[68] I. Shafarevich – *Exponents of elliptic curves.* (Russian) Doklady. Akad. Nauk SSSR **114** (1957), 714–716.

[69] K. Shiratani – *Über singuläre Invarianten elliptischer Funktionenkörper.* Journal reine und angew. Math. (Crelle) **226** (1967), 108–115.

[70] C.L. Siegel – *Über einige Anwendungen diophantischer Approximationen.* Abh. Preuss. Akad. d. Wiss. 1929, Phys.-Math. Klasse Nr. 1. Reproduced in *Gesammelte Abhandlungen*, vol. I, pp. 209–266.

[71] A. Silverberg – *Group order formulas for reductions of CM elliptic curves.* In: Arithmetic, geometry, cryptography and coding theory 2009. Contemporary Mathematics **521**, AMS 2010, 107–120.

[72] W. Stein – *There are genus one curves over Q of every odd index.* Journal reine und angew. Math. (Crelle) **547** (2002), 139–147.

[73] J. Tate – *Algebraic cycles and poles of zeta functions.* Arithmetical algebraic geometry (Proc. Conf. Purdue Univ., 1963), pp. 93–110. Harper & Row, New York 1965.

[74] J. Tate – Endomorphisms of abelian varieties over finite fields. Invent. Math. **2** (1966), 134–144.

[75] J. Tate – *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*. Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Exp. No. 352, 95–110, Lecture Notes in Math., 175, Springer, Berlin, 1971.

[76] P. Ullrich – *Emil Artins unveröffentlichte Verallgemeinerung seiner Dissertation*. Mitt. Math. Ges. Hamburg **19** (2000), 173–194.

[77] B.L. Van der Waerden – *Zur algebraischen Geometrie VI: Algebraische Korrespondenzen und rationale Abbildungen*. Mathematische Annalen **110** (1934), 134–160.

[78] W. Waterhouse – *Abelian varieties over finite fields*. Ann. Sci. Ecole Norm. Sup. (4) **2** (1969), 521–560.

[79] A. Weil – *L'arithm-métique sur les courbes aléggébriques.* Acta Mathematica 52 (1928), 281–315.

[80] A. Weil – *Une lettre et un extrait de lettre á Simone Weil.* André Weil, Collected papers, Vol. I, [1940a].

[81] A. Weil – *Sur les fonctions algébriques à corps de constantes fini.* C. R. Acad. Sci. Paris **210** (1940), 592–594.

[82] A. Weil – *On the Riemann hypothesis in function-fields.* Proc. Nat. Acad. Sci. U. S. A. **27** (1941), 345–347.
André Weil, Collected papers, Vol. I, [1941].

[83] A. Weil – *Two lectures on number theory, past and present.* Enseignem. Math. **XX** (1974), 87–110.

[84] A. Weil – *Prehistory of the zeta-function.* Sympos. Atle Selberg (1987): Number theory, trace formulas and discrete groups (Editors A. Aubert, E. Bombieri and D. Goldfeld). Acad. Press, 1989.

[85] A. Weil – *On Eisenstein's copy of the Disquisitiones*. Adv. Stud. Pure Math. **17**, Academic Press, Boston, MA, 1989; pp. 463–469.

[86] E. Witt – *Über ein Gegenbeispiel zum Normensatz.* Math. Zeitschr. **39** (1934), 462–467.

[87] C-F. Yu – *A note on supersingular abelian varieties.*
`http://xxx.tau.ac.il/pdf/1412.7107v1.pdf`