Frans Oort
Mathematisch Instituut
Universiteit Utrecht
f.oort@uu.nl

Geschiedenis

The Weil conjectures

As of 2003, the Abel Prize has been awarded yearly to one or more mathematicians. Up to 2014, fourteen laureates have received this prize, which has often been described as the mathematician's 'Nobel prize'. In 2013 it was awarded to Pierre Deligne. This event was celebrated by a presentation during a WONDER meeting in Delft, in December 2013. The present note of Frans Oort aims to give a part of that presentation, in particular a contemplation on the 'flow of mathematics' which led to this great success: the main topic will be on the 'pre-history' of the Weil conjectures.

The fundamental problem in number theory is surely how to solve equations in integers. Since this question is still largely inaccessible, we shall content ourselves with the problem of solving polynomial congruences modulo p. Nick Katz in [20]

The Riemann Hypothesis (RH) has been in the focus of mathematical research ever since Bernhard Riemann stated this conjecture in 1859. However, this problem will not be considered here. From 1924 onward an analogue of the RH has been studied, usually called *the characteristic p formulation*. In order to avoid any confusion we will refer to this by pRH (although this is not standard). Basically, this problem concerns solving equations over finite fields. We will see that the pRH answers the question of counting the number of solutions to polynomial equations over all finite fields of the same characteristic at one stroke. This will be illustrated by an easy example, to be followed throughout the paper.

After fifty years Pierre Deligne placed the crown on this impressive series of developments by proving the pRH in its full generality. Below, we will discuss the history of this flow of ideas.

Remark. Does this provide any progress for the solution of the classical RH? The answer is negative in the strict sense: there is no implication pRH ⇒ RH (and also no argument the reverse way). However, it may give us confidence of being on the right track. Moreover, tools have been developed, several technical steps have been made, and above all the deep insight in arithmetic aspects of geometry have proved to be a powerful aspect of modern mathematics.

We discuss:

- Formulation of the (equivalent of the) RH by Emil Artin, and results by F.K. Schmidt, Hasse and Weil proving this conjecture in special cases (algebraic curves and abelian varieties defined over finite fields).
- We indicate how this motivated André Weil to formulate his conjectures.
- In short sections we give references for results proved by Grothendieck with many of his co-workers, and finally by Deligne, proving the Weil conjectures.

I expect that the first four pages can be understood by a general audience; the next two pages will convey some of the thrill of this daring conjecture by Weil; the last two pages give ample references about recent work on the Weil conjectures. Excellent surveys are [20, 26, 33, 40], also see [8].

Counting points on varieties over finite fields
This was considered by Gauss, DA 357 (*Disquisitiones Arithmeticae*), and in his famous 'Last Entry' 146 in 1814 in his Tagebuch: the

Photo: IHES

Pierre Deligne during his time at IHES

number of rational points on several elliptic curves (in our terminology) over a prime field $\mathbb{F}_p$ were computed [11–12]. Also other mathematicians considered such cases.

Let me take one simple example, which we will follow throughout our journey. Try to solve the equation

$$Y^2 - Y = X^3 - X^2, \quad \text{with } x, y \in \mathbb{F}_{2^m}.$$

It is clear that over $\mathbb{F}_2$ there are exactly four solutions given by $x = 0, 1$ and $y = 0, 1$; note that $-1 = +1 \in \mathbb{F}_2$. We can embed the affine plane into the projective plane by $(x, y) = [x{:}y{:}1]$. We know that, adding the 'point at infinity' [0:1:0] (the unique point at 'infinity' on the line $X = 0$) we obtain an elliptic curve $D \subset \mathbb{P}^2_K$ defined over $K = \mathbb{F}_2$ by the homogeneous equation

$$Y^2Z - YZ^2 = X^3 - X^2Z.$$

We write our modest result as

$$\#(D(\mathbb{F}_2)) = 5.$$

How do we compute $N_m := \#(D(\mathbb{F}_{2^m}))$ for all $m \in \mathbb{Z}_{>0}$? We will show that abstract theory gives a complete (and easy) answer to this question (and in fact, the same method answers this question over any finite field).

Explanation. A *finite field* is a field with a finite number of elements. An example is the residue class ring $\mathbb{Z}/p$, where p is a prime number (and indeed, as is easily proved, this is a field). However $\mathbb{Z}/4$ is not a field: it has zero-divisors, the element $2 \bmod 4$ does not have an inverse. General theory says that for any prime power $q = p^n$, where p is a prime number and $n \in \mathbb{Z}_{>0}$, there exists a finite field with q elements, and this field is unique up to isomorphism; it will be denoted by $\mathbb{F}_q$, in particular $\mathbb{F}_p = \mathbb{Z}/p$.

An *elliptic curve* E over a field K is a non-singular algebraic curve $E \subset \mathbb{P}^2_K$ given by a cubic equation having at least one K-rational point. The curve $D \subset \mathbb{P}^2$ given by the homogeneous equation $ZY^2 - Z^2Y = X^3 - ZX^2$ (over a field in which $11 \neq 0$) is an example of an elliptic curve.

Side remark: This equation considered over $\mathbb{F}_{11}$ defines a curve on which ($x = 8 \bmod 11, y = 6 \bmod 11$) is the (only) singular point (a node).

First, we will follow a different line of development in history.

Euler series and the Riemann zeta function

Euler studied in 1740 infinite series defined as an infinite sum of positive numbers, and later Chebyshev studied this as a function of a real variable s:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}, \quad s \in \mathbb{R},$$

where p runs through the set of all prime numbers. Both sides converge for $s > 1$.

Riemann, who knew work by Euler and who knew the relation of this function with the theory of prime numbers, wrote in 1859 his masterpiece *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* [31]. Riemann considered the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}, \quad s \in \mathbb{C},$$

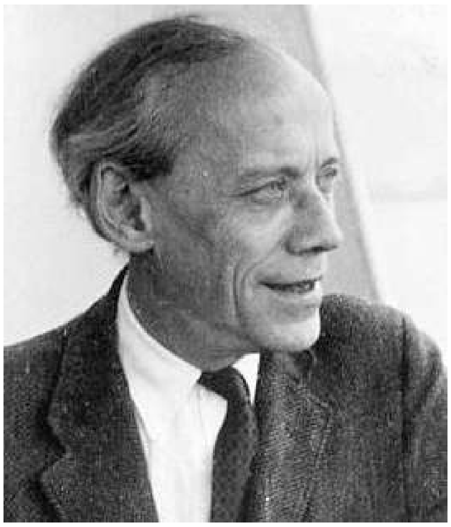
convergent for the real part of s greater than one, and he proved that this complex function has an analytic continuation. He showed that (the analytic continuation of) this function has zeros at all negative, even, integral values of s (the 'trivial zeros'). Riemann then stated his famous conjecture that for this function (called the *zeta function* by Riemann) (continued across the pole at $s = 1$) all 'non-trivial zeros' should have real part with absolute value equal to $\frac{1}{2}$ (in this case 'non-trivial zeros' can be understood as zeros with imaginary part not equal to zero). It is impressive to read this paper by Riemann: concise, a masterpiece of technical skill. This conjecture, if true, would give a insight in the distribution of prime numbers. His idea, his conjecture, now indicated by RH, has had an enormous impact on mathematics, and it still has this influence.

Remark. These series were considered by Euler, already in 1740, for positive integral values of s. As far as I know Euler did not consider this as a 'function' in s, therefore I will not use the terminology 'the Euler zeta-function'. Dirichlet and Chebyshev studied such series as a function (of a complex or a real variable).

The Dedekind and E. Artin zeta functions

At the moment we have no idea how to prove (or disprove?) the Riemann Hypothesis for the Riemann zeta function.

Remarkably enough, it might help to study a generalization. Let R be an *algebra of finite type over* $\mathbb{Z}$. This means that there is an ideal $I \subset \mathbb{Z}[T_1, \ldots, T_m]$ such that $R \cong \mathbb{Z}[T_1, \ldots, T_m]/I$. Here are some examples: $\mathbb{Z}$, $\mathbb{Z}[T]$, $\mathbb{F}_p$ (where $\mathbb{F}_p = \mathbb{Z}/p$), $\mathbb{F}_p[T]$, etc.


Emil Artin (1898–1962)

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 [38].

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

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

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 [39]. Later, these definitions and questions where 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.” [48]

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 proposed in 1924 in his PhD thesis [1] a definition of the zeta function for an algebraic curve over a finite field and he proposed a RH for this kind of zeta function. The definition and properties of such zeta functions were further studied by F.K. Schmidt [34] and by H. Hasse [18–19]. Rationality was proved by F.K. Schmidt and Hasse proved the (analogue pRH of the) RH for elliptic curves over a finite field.

From now on all varieties are defined over a finite field of characteristic p, and we study the pRH, an analog/special case of the extended Riemann Hypothesis (below we give formulas).

Proof of the pRH by Hasse

In 1934 Hasse proves the pRH for elliptic curves over finite fields.

Reminder. We write RH for the classical Riemann Hypothesis (and generalizations in characteristic zero). In order to avoid confusion we write pRH for the equivalent of the RH about solving equations in positive characteristic.

Here we set up notation. As base field we choose $K = \mathbb{F}_q$, where q is a power of p. For any $m \in \mathbb{Z}_{>0}$ we write $K_m := \mathbb{F}_{q^m}$, i.e. $K \subset K_m$ is the extension of degree m (unique up to a K-isomorphism).

Reminder. In a basic course on algebra we learn that for every prime power $q = p^n$ there exists, up to an isomorphism, exactly one field K with q elements; this field we denote by $K = \mathbb{F}_q$. Note that $\mathbb{F}_p \cong \mathbb{Z}/p$, however for $n > 1$ the field F_q is not isomorphic with $\mathbb{Z}/p^n$.

From now on all base fields will be in characteristic $p > 0$.

This theory, started by Emil Artin, gives rise to the following definition, in analogy with the Dedekind zeta function for number fields. Let V be a non-singular, projective variety defined over K, i.e. an algebraic variety defined as a closed set in some projective space $\mathbb{P}^d_K$. For a field L containing K we write $V(L)$ for the set of points on V with coordinates in L, the set of points ‘rational over L’. We write

$$N_m = N_m(V/\mathbb{F}_q) := \#(V(K_m)),$$

the number of points on V with coordinates in $K_m := K_{q^m}$. This results in the (Hasse–Weil) zeta function

$$\begin{aligned} Z(T) = Z(V,T) &= Z_{V/K}(T) \\ &= \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} T^m\right). \end{aligned}$$

Below we will see that this definition generalizes the notion of zeta functions $\zeta_R(s)$ as in the previous section from rings to varieties. In fact, Emil Artin introduced this zeta functions over a finite field, only for curves.

Example. Let V be just one point, rational over $K = \mathbb{F}_q$, hence $N_m = 1$ for every $m > 0$. We see:

$$Z(T) = \exp\left(\sum_{m=1}^{\infty} \frac{1}{m} T^m\right) = \frac{1}{1-T}.$$

Example. Let us consider $V = \mathbb{A}^d_K$, the affine space of dimension d over K; this is defined by: for any ring R containing K we have $\mathbb{A}^d_K(R) = R^d$. We see

$$N_m = \#((\mathbb{F}_{q^m})^d) = q^{md}.$$

We can show:

$$Z_V(T) = \frac{1}{1-q^dT}.$$

Example. For $V = \mathbb{P}^1_K$, the projective line, we have $N_j = q^j + 1$ and we see that

$$Z(\mathbb{P}^1_K, T) = \exp\left(\sum_{j=1}^{\infty} \frac{q^j+1}{j} T^j\right).$$

This can be rewritten as

$$Z(\mathbb{P}^1_K, T) = \frac{1}{(1-T)(1-qT)}.$$

Surprisingly, the above examples give a rational function in the variable T. In an analogous way we can easily show:

$$Z(\mathbb{P}^n_K, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}$$

for all $n \in \mathbb{Z}_{>0}$ and all $K = \mathbb{F}_q$. Note that $\mathbb{P}^n$ can be written as disjoint union of $\mathbb{A}^0, \ldots, \mathbb{A}^n$; from this observation the formula follows. A survey can be found in [25, Chapter 6].

Theorem (F.K. Schmidt, 1931). *For a* (non-singular, irreducible, projective) *algebraic curve C over a finite field $\mathbb{F}_q$, its zeta function $Z(C,T)$ is a rational function in T, having the precise form*

$$Z(C,T) = \frac{P}{(1-T)(1-qT)},$$

where $P \in \mathbb{Z}[T]$ is a polynomial of degree $2g$, where g = genus(C), and

$$P = P(T) = \prod_{i=1}^{2g}(1-\alpha_iT), \quad \alpha_i \in \mathbb{C}.$$

The map $\alpha \mapsto q/\alpha$ is a permutation of $\{\alpha_1, \ldots, \alpha_{2g}\}$.

F.K. Schmidt proved in [34] the Riemann–Roch theorem for curves in positive characteristic, and in the second part of that paper Schmidt uses this to prove the theorem above, in particular the rationality of the zeta function of a complete, nonsingular curve of genus g over $\mathbb{F}_q$, with numerator a polynomial of degree $2g$.

Remark. We see that $Z(C,T)$ admits an analytic continuation. The substitution $T = q^{-s}$ gives

$$Z_E(T) = Z_E(q^{-s}) =: \zeta_E(s).$$

We see that $\alpha \mapsto q/\alpha$ yields $s \mapsto 1-s$, and this is the (analogue of the) 'functional equation'.

Theorem (Hasse, 1934). *For an elliptic curve E over $K = \mathbb{F}_q$ the algebraic integers $\alpha, \beta \in \mathbb{C}$, defined by*

$$Z(E/K,T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

satisfy

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

Hasse proves in [18, §11] the Riemann Hypothesis for elliptic curves over a finite field, see also [19, III, §4].

Remark. The numerator $P_1(T)$ of $Z(E/K,T)$ in case of an elliptic curve E is the eigenvalue polynomial of the action of the Frobenius $\pi \in \mathrm{End}(E)$, as Hasse remarked and used. We will see that this insight will be generalized.

Explanation. As already has been noted, we write RH for the *classical Riemann Hypothesis*, and we write pRH for the special case of a generalization, studying an *equivalent question over finite fields*. The property $|\alpha| = \sqrt{q} = |\beta|$ above implies that the zeros of $\zeta_E(s)$ have their real part equal to $\frac{1}{2}$ here we see the resemblance with the classical RH.

We have seen that $Z_V(T)$ encodes the sequence $\{N_m \mid m \in \mathbb{Z}_{>0}\}$. Conversely these numbers can be retrieved via the logarithmic derivative (f'/f):

$$\frac{TZ'(T)}{Z(T)} = \sum_{m>0} N_m T^m.$$

The Hasse bound

It follows that for any elliptic curve E over $\mathbb{F}_q$ we have

$$\begin{aligned} N_m(E/\mathbb{F}_q) &:= \#(E(\mathbb{F}_{q^m})) \\ &= 1 - (\alpha^m + \beta^m) + q^m. \end{aligned}$$

We see that such a theorem gives the number of rational points over all finite extensions of K, once α and β are known. This proves that for any elliptic curve E over $\mathbb{F}_q$ we have the 'Hasse bound':

$$|\#(E(\mathbb{F}_q)) - 1 + q| = |\alpha + \beta| \leq 2\sqrt{q}.$$

See below.

Remark. As an elliptic curve is a double cover of the projective line (ramified in at least one point) for an elliptic curve E over $\mathbb{F}_q$ we immediately see the bound

$$\#(E(\mathbb{F}_q)) \leq 2q + 1.$$

As $2\sqrt{q} < q+1$ for all q and $2\sqrt{q} < q$ for $4 < q$ we see the Hasse bound agrees with this bound and in many cases it is sharper.

Elliptic curve

We return to our example $D \subset \mathbb{P}^2_K$, the elliptic curve given by the equation

$$Y^2Z - YZ^2 = X^3 - X^2Z$$
$$\text{over the field } K = \mathbb{F}_2.$$

As we have seen we have $\#(D(\mathbb{F}_2)) = 5$ (an easy computation, solving an equation modulo 2). By

$$\#(D(\mathbb{F}_2)) = 5 = 1 - (\alpha + \beta) + 2,$$
$$\beta = \frac{2}{\alpha}, \quad \alpha + \frac{2}{\alpha} = 2,$$

we see

$$\alpha, \beta = -1 \pm \sqrt{-1}.$$

We conclude that for every $m \in \mathbb{Z}_{>0}$ we have

$$\begin{aligned} \#\left(D(F_{2^m})\right) = 1 - \Big((-1 \pm \sqrt{-1})^m \\ + (-1 \pm \sqrt{-1})^m\Big) + 2^m. \end{aligned}$$

(I find it astonishing that this theory after an easy computation gives this complete result.)

Let us see how this works out in simple examples. As the group $D(\mathbb{F}_4)$ has $D(\mathbb{F}_2) \cong \mathbb{Z}/5$ as a subgroup, and $\#(D(\mathbb{F}_4)) \leq 2 \cdot 4 + 1 = 9$ we conclude $\#(E(\mathbb{F}_4)) = 5$ (this can also be seen by an easy computation), and indeed:

$$\alpha^2, \beta^2 = \mp 2\sqrt{-1},$$
$$\#(E(\mathbb{F}_4)) = 1 - (\alpha^2 + \beta^2) + 4 = 5.$$

Something you would not like to compute without the preceding theory ($\alpha^{10}, \beta^{10} = 15 \mp 8\sqrt{-1}$):

$$\#(D(\mathbb{F}_{1024})) = 1 - 30 + 1024 = 995.$$

I hope this convinces the reader that for any elliptic curve E over $\mathbb{F}_q$ after computing $\#(E(\mathbb{F}_q))$ this theory gives access to all $\#(E(\mathbb{F}_{q^m}))$.

An amusing example: we see that $\alpha^4, \beta^4 = (2\sqrt{-1})^2 = -4$; we obtain:

$$\#(D(\mathbb{F}_{16})) = 1 - (-4-4) + 16 = 25.$$

Here $|\#(D(\mathbb{F}_{16})) - 1 - 16| = 8 = 2\sqrt{16}$, a case where the Hasse bound is reached.

However, note that any result of the type pRH, the Riemann hypothesis in characteristic p, does not give any new result for the classical RH, for example:

$$\zeta_{\mathbb{Z}}(s) = \prod_p \zeta_{\mathbb{F}_p}(s) = \prod_p \frac{1}{1-p^{-s}}$$

(and it seems we have gained nothing in the direction of the classical RH).

Remark. Instead of the definition given above of $Z_V(T)$ one can give the equivalent definition:

$$Z_V(T) = \sum_\delta \frac{1}{1 - T^{\deg(\delta)}},$$

where δ runs over all effective divisors of V defined over $\mathbb{F}_q$.

What is the structure behind such theorems, and how can these results be generalized to curves of higher genus, and to varieties of higher dimensions?

Gauss

In DA 358 [11] Gauss computes for certain elliptic curve the number of rational points over a prime field $\mathbb{F}_p$; in the last entry in his *Tagebuch* [12], Gauss discusses these results as a conjecture. In [30] on page 73 G.J. Rieger writes: "Diese Tatsache wurde ... übersehen und ist erst in neuere Zeit bemerkt worden. Damit ist auch die Richtigkeit der *Riemannschen Vermutung* für denjenigen Funktionenkörper nachgewiesen." This claim puzzles me; it is not clear how computations by Gauss imply the pRH in case you do not know rationality, functional equation or something like that for the zeta function considered.

Proof of the pRH by Weil

André Weil had the insight for the correct approach to generalizations. He started to write foundations necessary for proofs. In the period 1946–1948 he proved the pRH for *algebraic curves of arbitrary genus* and for *abelian* *varieties*. His proof starts with a simple, but fundamental observation.

For a variety V over $K = \mathbb{F}_q$ with $q = p^n$ the map which sends coordinates x_i of a point to x_i^q is a morphism

$$\mathrm{Frob}_{V/K} = \pi_{V/K} : V \to V.$$

Important (and obvious) remark. Fixed points of the map $\pi^m : V \to V$ are exactly the $K_m = \mathbb{F}_{q^m}$-rational points:

$$\left(V(\overline{\mathbb{F}_q})\right)^{(\text{fix } \pi^m)} = V(\mathbb{F}_{q^m}).$$

Let us compare this with the result (for an elliptic curve) mentioned earlier:

$$\#(E(\mathbb{F}_{2^m})) = 1 - (\alpha^m + \beta^m) + 2^m.$$

What is an 'interpretation' of this formula, and how can we generalize this to arbitrary varieties (defined over a finite field)?

Further explanation. For a projective algebraic curve C over any field K one can define its *genus*, $g(C) \in \mathbb{Z}_{\geq 0}$; for a curve over $\mathbb{C}$ there is a topological definition; in algebraic geometry this can be extended to curves over any base field. A curve of genus zero is called a rational curve; a curve of genus one with a K-rational point is called an elliptic curve.

A projective, irreducible non-singular variety A such that this is a group variety is called an *abelian variety*.

An abelian variety of dimension one is an elliptic curve. Any curve C of genus g gives rise to an abelian variety of dimension g, and many properties of C can be read off from properties of this abelian varieties. This abelian variety is called the Jacobian of C, or the Picard variety of C or the Albanese variety of C; these notions coincide in case C has at least one point rational over the base field. It is not deep (although it requires some work) that proving pRH for all curves amounts to the same as proving pRH for all abelian varieties. An abelian variety A is called simple if there is no non-zero proper sub-abelian variety $0 \neq B \subsetneqq A$.

André Weil (1906–1998)

The terminology 'abelian variety' stems from the fact that Niels Henrik Abel studied values of path-integrals of differentials on a Riemann surface; their values naturally lie in the related abelian variety, once you fix the end points of the path.

Remark. An abelian variety A over K is a group-object, the endomorphism algebra $\mathrm{End}(A)$ is a ring, and the Frobenius $\mathrm{Frob}_{A/K} \in \mathrm{End}(A)$. In case A is simple, this ring has no zero divisors, is of characteristic zero, and is finitely generated as a $\mathbb{Z}$-module: its field of fractions is a number field (a field of finite degree over $\mathbb{Q}$). Hence $\mathrm{Frob}_{A/K}$ is (can be considered) as an algebraic integer. Here we see access to (pRH) in the case of abelian varieties, and hence in the case of algebraic curves.

Here are a version and a corollary of results by Weil (1948):

Theorem. *For a simple* abelian variety A *defined over* $K = \mathbb{F}_q$ *its Frobenius homomorphism*

$$\mathrm{Frob}_{A/K} = \pi : A \to A$$

is an algebraic integer, and under every embedding $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ *we have*

$$|\psi(\pi)| = \sqrt{q}.$$

An amazing result: a 'nature given' endomorphism of a difficult object in positive characteristic turns out to be an algebraic integer having easy properties. It is easy to characterize and to produce such numbers (e.g. any zero of $T^2 + bT + q$ with $b \in \mathbb{Z}$ and $b^2 < 4q$; many more examples can easily be given).

Remark (details not explained nor discussed here). Conversely, an algebraic integer π with properties as in the theorem determines (an isogeny class of) an abelian variety A over $\mathbb{F}_q$ such that $\mathrm{Frob}_{A/K} = \pi$ (Honda-Tate theory): abelian varieties over a finite field can be constructed by just computing an algebraic integer having easy properties.

This theorem by Weil also proves the pRH for algebraic curves defined over a finite field. Reminder: a proof for the pRH for algebraic curves defined over a finite field implies the pRH for abelian varieties over a finite field.

Weil had two proofs. One proof relies on an analogue of a classical inequality (Castelnuovo-Severi) for correspondences on algebraic curves. Another proof (in this case for abelian varieties) uses the result that the Frobenius $\pi = \pi_{A/K} : A \to A$ for an abelian variety over $\mathbb{F}_q$ and its 'transpose' π^t (the image of π under the Rosati involution) satisfy $\pi \cdot \pi^t = q$. As π^t equals the complex conjugate of π, under any embedding ψ into C, we easily conclude $\mid \psi(\pi) \mid = \sqrt{q}$.

In order to achieve such results Weil developed many aspects of algebraic geometry over an arbitrary field (in this case a field of characteristic p). Note that Pierre Deligne was born in 1944.

Corollary (The Hasse–Weil bound). *For a non-singular, projective* algebraic curve C *of genus* g *over* $K = \mathbb{F}_q$ *we have*

$$|\#(C(\mathbb{F}_q)) - 1 - q| \leq 2g\sqrt{q}.$$

Indeed, $\#(C(\mathbb{F}_q)) - 1 - q = -\sum_i \alpha_i$ and $|\alpha_i| \leq \sqrt{q}$.

Remark. For elliptic curves, $g = 1$, we find this in [19, III, p. 206].

The Weil conjectures

We will especially look into the RH for varieties over finite fields.

Reminder. For a curve C defined over $K = \mathbb{F}_q$, the pRH is just a statement on the asymptotic behavior of $\#(C(\mathbb{F}_{q^m}))$ for $m \to \infty$.

As we have seen, for a variety V over $K = \mathbb{F}_q$, with $q = p^n$, the map which sends coordinates x_i of a point to x_i^q is a morphism

$$\mathrm{Frob}_{V/K} = \pi_{V/K} : V \to V$$

and $V(\mathbb{F}_{q^m})$ is the set of fixed points of $\mathrm{Frob}_{V/K}^m$.

André Weil made in 1949 the following conjecture:

Conjecture. *Let* V *be a non-singular, projective variety of dimension* d *defined over the* *finite field $K = \mathbb{F}_q$ having q elements. Then:*

1. Rationality. *The zeta function is a rational function with coefficients in $\mathbb{Z}$ in $T := q^{-s}$:*

$$Z(V/K,T) = \frac{P_1 \times P_3 \times \cdots \times P_{2d-1}}{P_0 \times P_2 \times \cdots \times P_{2d}}$$

with

$$P_j \in \mathbb{Z}[T], \quad P_0 = 1 - T, \quad P_{2d} = 1 - q^d T.$$

2. Analog of the classical Riemann Hypothesis. *The polynomials $P_1, \cdots, P_{2d-1}$ factor over $\mathbb{C}$ as*

$$\text{(pRH)} \qquad P_k(T) = \prod_j \, (1 - \alpha_{k,j}T), \qquad \text{with} \, |\alpha_{k,j}| = \sqrt{q^k}.$$

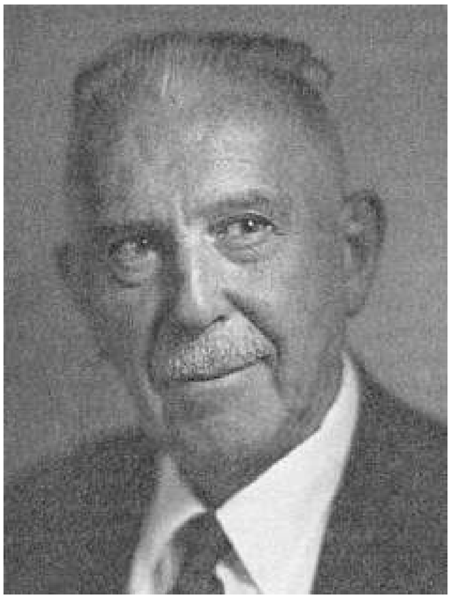
Moreover there should be a functional equation, Poincaré duality and an explanation of the degrees of the polynomials P_k in terms of geometry of V: they should be (the analogues of) the 'Betti numbers'; if V is the reduction mod p of a complex variety, these numbers should be the Betti number in the complex-topological sense. These together are called the 'Weil conjectures'.

We have seen this conjecture to be true for $\mathbb{P}^d$, for algebraic curves and for abelian varieties. The conjecture above is a daring generalization. How did Weil come to this insight? We will see that methods of algebraic topology have their counterpart in arithmetic geometry.

Cohomology as predicted by Weil

- Weil used in his proofs an interpretation and generalizations of the notion of correspondences as studied in the classical Italian algebraic geometry. Also aspects of the theory of abelian varieties were generalized to properties over arbitrary fields.
- It might very well be that Weil originally had from the beginning a deeper motivation behind his ideas.
- In 1949 Weil stated his famous conjectures,
- and in the ICM in 1954 he describes why these should be true, and what could be a way to prove these.

His idea how to proceed is of a great beauty, of deep insight and of daring courage. Note that Pierre Deligne graduated from high school in Brussels in 1962. This insight by Weil started a new chapter in arithmetic algebraic geometry, a revolution, and a whole new setup of algebraic geometry with new insights and new conjectures.



Solomon Lefschetz (1884–1972)

Here is that idea. We try to compute the number of rational points on a variety V defined over $\mathbb{F}_q$ over any finite field containing $\mathbb{F}_q$. The zeta function encodes

$$N_m = \#(V(\mathbb{F}_{q^m})) \quad \text{for all } m > 0.$$

We have seen that N_m is the number of fixed points under the operator $(\mathrm{Frob}_{V/K})^m$.

In a completely different branch of mathematics Lefschetz has indicated how to compute the number of fixed points of an operator:

The Lefschetz fixed-point theorem (first stated in 1926). *For a continuous map $f : X \to X$ from a compact triangulable space X to itself, such that f has a finite set $\mathcal{F} = X^{(\text{fix } f)}$ of fixed points, and such that the graph of f intersects the diagonal in $X \times X$ transversally the trace formula computes the number of fixed points:*

$$\#(\mathcal{F}) = \sum_{k \geq 0} \, (-1)^k \, \mathrm{Tr}\left(f_* \mid \mathrm{H}_k(X,\mathbb{Q})\right).$$

Let us compare this with the result for an algebraic curve mentioned earlier:

$$\#(C(\mathbb{F}_{q^m})) = 1 - \sum_{i=1}^{2g} \alpha_i^m + q^m.$$

"Je gaat het pas zien als je het doorhebt", as Johan Cruijff says. I would paraphrase: "Once you see it you understand it."

This is *the Lefschetz fixed point formula* in the following disguise:

- Show the graph of Frobenius is transversal to the diagonal (and this is easy).
- Find some (co)homology theory (??!!) such that the traces of $(\mathrm{Frob}_{V/K})^m$ on H^k for all $k \in \{0, 1, \cdots, 2 \cdot \dim(V)\}$ give the zeta-function of V/K. We should have $\mathrm{H}^k = 0$ for $k < 0$ and $k > 2 \cdot \dim(V)$.

In the case of an algebraic curve this should be:

- The trace of the Frobenius on the one-dimensional H^0 should be 1.
- The trace of $(\mathrm{Frob}_{C/K})^m$ on H^1 should be $\sum_{i=1}^{2g} \alpha_i^m$.
- The trace of the Frobenius on the one-dimensional H^2 should be q.

For an algebraic curve of genus g the degree of P_1 should be equal to $2g$. For algebraic varieties of higher dimension the polynomials $P_1, \ldots, P_{2d-1}$ should be given in an analogous way. If so, we conclude (?!):

$$\begin{aligned} \#(C(\mathbb{F}_{q^m})) &= \mathrm{Tr}\left(f^* \mid \mathrm{H}^0\right) - \mathrm{Tr}\left(f^* \mid \mathrm{H}^1\right) \\ &\quad + \mathrm{Tr}\left(f^* \mid \mathrm{H}^2\right) \\ &= 1 - \sum_{i=1}^{2g} \alpha_i^m + q^m \end{aligned}$$

with $\mathrm{H}^k = \mathrm{H}^k(X, ?)$ and $f = \mathrm{Frob}_{C/K}$.

I hope you see that earlier results by E. Artin, Schmidt, Hasse and Weil have a natural, geometric interpretation and generalization once you see this geometric approach, and once you find this elusive cohomology theory.

After this became clear, *once you see it you understand it*, we "only" had to find this mysterious cohomology theory, and prove it has the right properties. Then the Weil conjectures would follow.

Completely independent from these ideas Dwork (1923–1998) proved in 1960 rationality of the zeta function of a variety over a finite field [9]. Also Monsky/Washnitzer and Lubkin contributed.

Alexandre Grothendieck

In 1958 Grothendieck told us he was putting algebraic geometry on a new footing with the main goal (for the time being) to prove the Weil conjectures, see [13]. I remember I was present at his presentation. I did not understand his explanation, however there was one person in the audience who was very much 'au courant'; then I did not not know yet the influence Serre would have on mathematics and also upon on me. Note that Pierre Deligne was 14 years old at that time.

Serre made several attempts to construct a 'Weil cohomology'. His cohomology with values in the Witt vectors [35], 1958, did not bring this success.

His attempt to use 'étale topology' turned out to be fruitful. In Serre [36], 1958, we find the idea. In order to have the analogue of fiber spaces in algebraic geometry one should introduce a *new notion of covering*. Suppose $G \to H$ is a homomorphism between algebraic groups (e.g. dividing out an elliptic curve $E = G$ by a finite subgroup, $H = E/N$). We see this need not be locally trivial in the Zariski topology (e.g. if G is irreducible and N is a finite group, but $N \neq 0$), but the covering can be trivialized (locally) by an étale map to a Zariski open of H. Objects in this new notion of 'covering' are maps with certain properties onto Zariski open subsets. We see that the search for a proof can give new insights and constructions of radically new concepts.

This opened the way for Grothendieck to define a new notion of topologies, and to construct the sought-for cohomology theory. Grothendieck on page 104 of [13] seemed to be the first who used the term 'Weil cohomology'.

Grothendieck, together with Michael Artin, Giraud, Michel Raynaud, Illusie, Deligne and many others managed to find the earlier elusive 'Weil cohomology'. They were able to pin down basic properties. Here we record just some of these properties: fix the prime number p and choose another prime number $\ell \neq p$. It turned out that the best choice for a ring or field of constants was $\mathbb{Z}_\ell$, the ring of ℓ-adic integers respectively the field $\mathbb{Q}_\ell$ of ℓ-adic numbers.

- For every variety V of dimension d over a field of characteristic p and for every choice of ℓ there exists a cohomology theory $\mathrm{H}^*(V, \mathbb{Z}_\ell)$, the 'étale cohomology'. (As usual, obtained by derived functors in some topology, here in the 'étale topology' of H^0).
- For this cohomology properties like duality and more other vital ingredients were proved.

From these Grothendieck and his co-workers derived:

- Rationality of $Z_V(T)$ and hence analytic continuation of $\zeta_V(s) = Z_V(q^{-s})$.
- A Lefschetz type of fixed point formula for the Frobenius morphism.
- Functional equation.

See [14] for a first description of these results. Proofs were described in various volumes of SGA. For example, see [10, 27–28, 39], [17, Appendix C] and also see [38].

However the property pRH, the characteristic p analogue of the Riemann hypothesis, still escaped proofs:

- (pRH) The eigenvalues of Frob_V on $\mathrm{H}^i(V, \mathbb{Z}_\ell)$ have absolute value $\sqrt{q^i}$. Here the coefficient ring is $\mathbb{Z}_\ell$, the ring of ℓ-adic integers, where ℓ is a prime number different from p.

How to proceed? We see once the general machinery of cohomology developed, most of the aspects of the Weil conjectures followed by 'pure thought'. However the analogue (pRH) of the Riemann Hypothesis seemed out of reach of abstract theory.

It is wonderful to see how various mathematicians did continue in different ways.

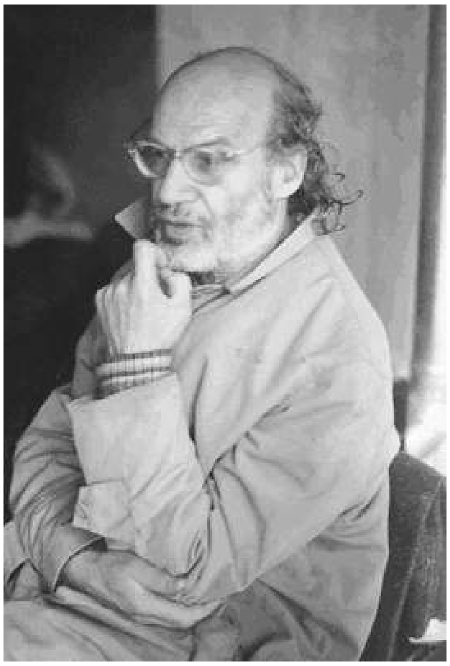


Photo: Archive of Winfried Scharlau

Alexander Grothendieck

Generalization. Grothendieck came with much more general conjectures; a survey of these conjectures can be found in: [16, 21–24]. These 'standard conjectures' on algebraic cycles describe, amongst others, relations between algebraic cycles and the Weil conjectures. Once these would be proved the (pRH) would simply follow. A fascinating idea. However most of this material seems completely inaccessible for the time being.

Inspiration from other fields. Deligne tried to prove the (pRH) directly (as many others had tried). Finally he was convinced he could prove the (pRH), Deligne wrote to Serre and remembers: "I wrote him a letter ... I think he got it just before he had to go to the hospital for an operation of a torn tendon. He told me later that he went in a euphoric state because he knew now that the proof was roughly done." See [32, p. 19].

A wonderful description of the proof to appear later in [4] we find in [40]. We will not — alas! — describe the beautiful proof of Deligne here. It seems much better either to read the original paper by Deligne, or to go through the description of Serre [40], or the description by Katz in [20].

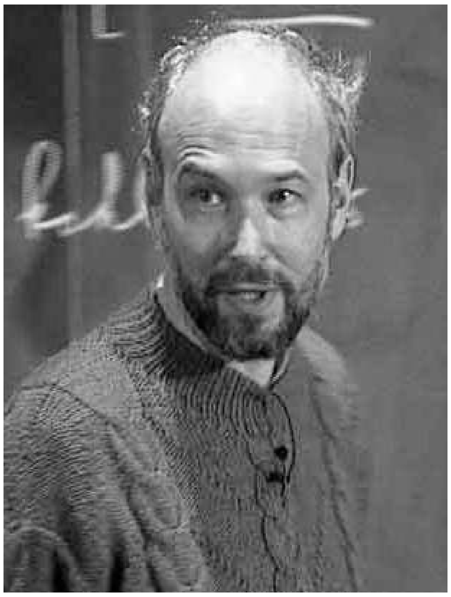
Deligne knew aspects and difficulties of this problem inside out ("I had all these tools at my disposal"). Instead of finishing of the general program of Grothendieck on cycles (still a complete mystery), Deligne followed a suggestion by Serre: "I think it was Serre who told me about an estimate due to Rankin"; see [29] (or came the suggestion from Langlands?, see [20, p. 287]). This idea did put Deligne on the right track to finish the proof. However, as Deligne says: "It would have been much nicer if the program had been realized", see [32, p. 18] (i.e. the program by Grothendieck: the proof of the Weil conjectures via the standard conjectures).

For a description of the prehistory see [33] (4 papers), [8, 26, 46], and references to E. Artin, F.K. Schmidt and Hasse cited above. For a description of the Weil conjectures, see: [10, 26–27, 44] and [17, Appendix C]. Work by Tate, see [41] can be seen as pre-history of Grothendieck's standard conjectures. For a complete and beautiful survey of the prehistory, and of Deligne's proof see [20]. For a survey of Deligne's proof, see [40].

Pierre Deligne

Maybe the essence of mathematics of Pierre Deligne is described in his words: "Proofs in geometry make sense at that age because surprising statements have not too difficult proofs." These words are telling us about his interests in mathematics already at a very early stage [32, p. 16]. I would like to see this as a qualification for all of his mathematical work. Throughout the years Deligne has amazed us by his clear insight and his beautiful and clear description of structures and proofs in mathematics.

We hope this note will give enough credit to all mathematicians on whose shoulders the theory was built (Euler, Riemann, Emil Artin, Hasse, Weil, Serre, Grothendieck and many others) on the one hand, and on the other hand it will show the quantum leap, the deep insight of Deligne that was vital in this proof of the Weil conjectures (well, a 'surprising statement', however not an easy proof).



Pierre Deligne

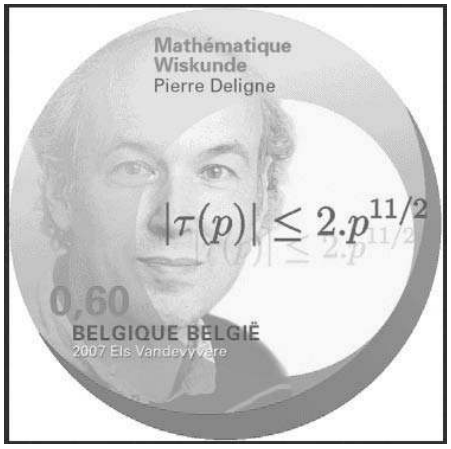
Pierre Deligne was born in 1944 in Belgium. Already at a young age it was clear his insight and taste for deep mathematics could enable him to do extraordinary things. In the interview with Pierre Deligne in the Newsletter of the European Mathematical Society of September 2013 we obtain a clear picture of this modest and friendly person, see [32]. In the period Deligne was still in elementary school the father of a friend gave him Bourbaki mathematics to read. His ('excellent elementary school') teacher did put him in contact with Jacques Tits. In high school Deligne enjoys problems in geometry (see the citation above).

Deligne at age 16 joins a course by Jacques Tits, who comments: "A remarkable feature of Pierre Deligne's thinking is that, when confronted with a new problem or a new theory, he understands and, so to speak, makes his own its basic principles at a tremendous speed, and is immediately able to discuss the problem or use the theory as a completely familiar object." See http://www-history.mcs.st-and.ac.uk/Biographies/Deligne.html I fully agree with this remarkable description. Indeed, you have the feeling: Pierre Deligne is "able to discuss the problem or use the theory as a completely familiar object".

With this ability he came under the influence of Serre (1926) and of Grothendieck (1928) (his official PhD-advisor) in his Paris years. Not only did he learn much from these two towering figures in algebraic geometry, but the respect and admiration was certainly reciprocal. In their correspondence Grothendieck complains to Serre that his 'anciens élèves' did not continue his work. Serre answers that this is not surprising: "You have the vision on a programme, and they do not have that (with the exception of Deligne, of course)", see [2, p. 244].

In his Paris period Deligne has an impressive production, not only in diversity of problems studied, but especially in depth of understanding. Grothendieck tries to prove the Weil conjectures, and Deligne witnessed, and collaborated at close range. In 1973 Deligne proves the last missing part, the Riemann hypothesis (pRH), in the program of the Weil conjectures. This is seen as his most prestigious achievement. For this he receives in 1978 the Fields medal. In 1984 Deligne moved to the Institute for Advanced Study in Princeton.

Let me mention here one of his theorems: The *Ramanujan-Petersson conjecture*. This is a statement about Fourier coefficients of an interesting modular form (no explanation given here). Ramanujan conjectured their absolute values should satisfy inequalities as printed on a Belgium stamp. In 1971 Deligne proved this would follow from pRH. Hence the proof (1974) of the aspect pRH of the Weil conjectures implies the Ramanujan-Petersson conjecture holds true. E.g. see [25, 6.4.1].



Pierre Deligne on a Belgian postage stamp

Pierre Deligne

Some of his many awards:
Abel Prize (2013)
Wolf Prize (2008)
Balzan Prize (2004)
Crafoord Prize (1988)
Fields Medal (1978)

Timeline:
1944 Born
1962 Finishes High School
1966 Finishes University (Free University Brussels)
1968 PhD University of Paris-Sud (France)
1972 Doctorat d'État des Sciences Mathé matiques
1968–1970, 1970–1984 IHES Bures sur Yvette (France)
≥ 1984 IAS Princeton (USA)

References

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

2 P. Colmez and J-P. Serre, eds., *Correspondance Grothendieck–Serre*, Documents Mathématiques (Paris), No. 2, Soc. Math. France, Paris, 2001. Translated and edited as a bilingual version by the American Mathematical Society in 2003.

3 P. Deligne, Formes modulaires et représentations ℓ-adiques, Exp. 355 in *Sém. Bourbaki, 1968/69*, Lecture Notes in Mathematics, No. 179, Springer, Berlin, New York, 1971.

4 P. Deligne, La conjecture de Weil: I, *Publications Mathématiques de l'IHÉS* 43 (1974), 273–307.

5 P. Deligne, La conjecture de Weil: II, *Publications Mathématiques de l'IHÉS* 52 (1980), 137–252.

6 P. Deligne and D. Mumford, The irreducibility of the space of curves of given genus, *Publications Mathématiques de l'IHÉS* 36 (1969), 75–109.

7 P. Deligne and J-P. Serre, Formes modulaires de poids 1, *Annales scientifiques de l'École Normale Supérieure, Sér. 4* 7 (1974), 507–530.

8 J. Dieudonné, On the history of the Weil conjectures, *The Mathematical Intelligencer* 10 (1975), 7–21. Reprinted in [10], pp. IX–XVIII.

9 B. Dwork, On the rationality of the zeta function of an algebraic variety, *American Journal of Mathematics* 82 (1960), 631–648

10 E. Freitag and R. Kiehl, *Etale Cohomology and the Weil Conjecture*, with an historical introduction by J.A. Dieudonné, Ergebnisse der Mathematik und ihrer Grenzgebiete 3 Folge, No. 13, Springer, 1988.

11 C. Gauss, *Disquisitiones Arithmeticae*, Fleischer, Leipzig, 1801. Translation by A. Clarke: *Disquisitiones Aritmeticae*, Yale University Press, 1965.

12 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, No. 256 (5th ed.), Verlag Harri Deutsch, Frankfurt am Main, 2005.

13 A. Grothendieck, The cohomology theory of abstract algebraic varieties, *Proc. Internat. Congress Math. (Edinburgh, 1958)*, Cambridge Univ. Press, New York, 1960, pp. 103–118.

14 A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L, Exp. 279 in *Sém. N. Bourbaki, 1964–1966*, pp. 41–55.

15 A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L, in *Dix exposés sur la cohomologie des schémas*, Advanced Studies in Pure Mathematics, No. 3, North-Holland, Amsterdam; Masson et Cie, Editeur, Paris, 1968; Exp. III, pp. 31–45.

16 A. Grothendieck, Standard conjectures on algebraic cycles, *Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968)*, Oxford University Press, 1969, pp. 193–199.

17 R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, No. 52, Springer, 1977.

18 H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, *Anh. Math. Sem. Hamburg* 10 (1934), 325–348.

19 H. Hasse, Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit volkommenem Konstantenkörper bei beliebiger Charakteristik, I, II and III, *Journ. reine angew. Math. (Crelle)* 175 (1936), 55–62, 69–88 and 193–208.

20 N. Katz, An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields, in *Mathematical Developments Arising from Hilbert Problems* (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), Amer. Math. Soc., Providence, RI, 1976, pp. 275–305.

21 S. Kleiman, Algebraic cycles and the Weil conjectures, *Dix exposés sur la cohomologie des schémas*, Advanced Studies in Pure Mathematics, No. 3, North-Holland, Amsterdam, and Masson et Cie, Editeur, Paris, 1968, pp. 359–386.

22 S. Kleiman, Motives, in *Algebraic Geometry*, F. Oort, ed., Proc. Fifth Nordic Summer School in Math., Oslo, 1970, pp. 53–82; Appendix I, Finiteness theorems for algebraic cycles, pp. 83–88.

23 S. Kleiman, Finiteness theorems for algebraic cycles, *Actes du Congrès International des Mathématiciens (Nice, 1970)*, No. 1, Gauthier-Villars, Paris, 1971, pp. 445–449.

24 S. Kleiman, The standard conjectures, *Motives* (Seattle, WA, 1991), Proceedings of Symposia in Pure Mathematics, No. 55, American Mathematical Society, 1994 pp. 3–20.

25 Yu. Manin and A. Panchishkin, *Introduction to Modern Number Theory: Fundamental Problems, Ideas and Theories*, Springer, 2007, 2nd ed.

26 B. Mazur, Eigenvalues of Frobenius acting on algebraic varieties over finite fields, *Algebraic Geometry* (Humboldt State Univ., Arcata, Calif., 1974), Proc. Sympos. Pure Math., No. 29, Amer. Math. Soc., Providence, RI, 1975, pp. 231–261.

27 J. Milne, *Etale cohomology*, Princeton Mathematical Series, No. 33, Princeton University Press, Princeton, NJ, 1980.

28 J. Milne, Lectures on etale cohomology, Notes for a course taught at the University of Michigan in 1989 and 1998. http://www.jmilne.org/math/CourseNotes/lec.html

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

30 G. Rieger, Die Zahlentheorie bei C.F. Gauss, in *C.F. Gauss Gedenkband anlässlich des 100 Todestages am 23. Februar 1955*, Teubner, 1957, pp. 37–77.

31 B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Grösse, *Monatsberichte der Berliner Akademie*, November 1859, 6 pp; in *Monath. der Köl. Preuss. Akad. der Wissen. zu Berlin aus der Jahre 1859* (1860), 671–680; also in *Gesammelte math. Werke und wissensch. Nachlass* 2 (1892), 145–155. http://www.claymath.org/millennium/Riemann_Hypothesis/1859_manuscript, http://en.wikipedia.org/wikiOn_the_Number_of_Primes_Less_Than_a_Given_Magnitude

32 M. Raussen and C. Skau, Interview with Abel laureate Pierre Deligne, *Newsletter European Math. Soc.* 89 (2013), 15–23.

33 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, in *Hamburger Beiträge zur Geschichte der Mathematik*, Mitt. Math. Ges. Hamburg, No. 21 (2002), 79-157; Part 2: The first steps by Davenport and Hasse, No. 22 (2004) 5–74; Part 3: The elliptic case, No. 25 (2006), 103–176; Part 4: Davenport–Hasse fields, No. 32 (2012) 145–210.

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

35 J-P. Serre, Sur la topologie des variétés algébriques en caractéristique p, *Symposium internacional de topología algebraica*, Mexico (1958), pp. 24–53.

36 J-P. Serre, Espaces fibrés algébriques, in *Anneaux de Chow et applications*, Sém. C. Chevally E.N.S., No. 2 (1958), pp. 1-01–1-37; also in J-P. Serre, *Exposés de séminaires (1950–1999)*, 2nd ed., Docum. Math., No. 1, Soc. Math. France, 2008, pp. 107–140.

37 J-P. Serre, Rationalité des fonctions ζ des variétés algébriques, Exp. 198 in *Sém. Bourbaki, 1959/60*, No. 12.

38 J-P. Serre, Zeta and L functions, in *Arithmetical Algebraic Geometry* (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 82–92.

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

40 J-P. Serre, Valeurs propres des endomorphisms de Frobenius, Exp. 446 in *Sém. Bourbaki, 1973/1974*.

41 J. Tate, Algebraic cycles and poles of zeta functions, in *Arithmetical Algebraic Geometry* (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 93–110.

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

43 A. Weil, On the Riemann hypothesis in function fields, *Proc. Nat. Acad. Sci. U.S A.* 27 (1941), 345–347.

44 A. Weil, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* 55 (1949), 497–508.

45 A. Weil, Abstract versus classical algebraic geometry, in *Proceedings of the International Congress of Mathematicians, 1954, Amsterdam*, Vol. III, Noordhoff, Groningen, and North-Holland, Amsterdam, 1956, pp. 550–558.

46 A. Weil, Prehistory of the zeta-function, in *Sympos. Atle Selberg (1987): Number Theory, Trace Formulas and Discrete Groups*, A. Aubert, E. Bombieri and D. Goldfeld, eds., Acad. Press, 1989.

47 http://www.claymath.org/millennium/Riemann_Hypothesis/riemann.pdf

48 http://www.claymath.org/millennium/Riemann_Hypothesis/riemann.pdf