The Weil Conjecture

Deligne's best known achievement is his spectacular solution of the last and deepest of the Weil conjectures, namely the analogue of the Riemann hypothesis for algebraic varieties over a finite field.

André Weil wrote in 1949, in the paper *Numbers of solutions of equations in finite fields: .. and other examples which we cannot discuss here, seem to lend some support to the following conjectural statements, which are known to be true for curves, but which I have not so far been able to prove for varieties of higher dimension.*


André Weil

The statements Weil was not able to prove have been named the Weil conjectures. The issue of the Weil conjectures is so-called zeta functions. Zeta functions are mathematical constructions that keep track of the number of solutions of an equation, in different number systems. When Weil says that the conjectural statements are known to be true for curves, he means that they are true for equations in two unknown. Varieties in higher dimensions, as referred to, correspond to equations in three or more unknowns.

The equation $x^2-y^2=3$ describes a plane curve, and as we have showed in the frame above the equation has 4 solutions in the number system {0,1,2,3,4} when counting modulo 5.

We notice that none of the numbers 0,1,2,3,4 have square equal to 2. We therefore introduce a new number α, the square root of 2. This number is not an element of the original set 0,1,2,3,4 and is determined by the equation $\alpha^2=2$. Extending the number system to include α, gives us many new solutions to the equation $x^2-y^2=3$, e.g. $x=0$ and $y=\alpha$ since $0^2-\alpha^2=-2=3$ when counting modulo 5. Another solution is given by $x=\alpha$ and $y=2$. All together we find 24 different solutions in the extended number system. The two numbers 4 and 24 decides the two first terms of the zeta function in this example.

The Weil conjectures are formulated in four statements. Weil proved himself the conjectures in the curve case. For more general equations, three of the four statements were proved by other mathematicians in the following 10-15 years after the publishing of Weil's paper in 1949. The last statement, the most difficult, analogous to the Riemann hypothesis, was proved by Pierre Deligne in 1974.

It soon became clear that the conjectures would be proved if one could find a certain type of cohomology, called Weil cohomology. Cohomology are mathematical tools that were developed in 1920- and 30`s to understand and systematize knowledge about geometric shapes and structures. The more complicated the structure, the more cohomology. Weil had no suggestions on how to define Weil cohomology, but he knew what qualities cohomology should have to provide a proof of the Weil conjectures.

At the end of the 1940s nobody knew any cohomology which could solve the conjectural problem and thus unify the geometric aspect, related to the solution of equations and the arithmetic aspect, represented by the finite fields (number systems). The solution came in 1960. At that time Alexander Grothendieck introduced the concept of étale cohomology and proposed that it should play the role of the mysterious, unknown, but essential Weil cohomology. The problem however, was to prove that the étale cohomology satisfies the requirements to be a Weil cohomology. Grothendieck was not able to do so, but fortunately he had a young student, Pierre Deligne who succeeded in this task. By a complicated reasoning, where he based his arguments on several previous achievements made by other mathematicians, Deligne was able to prove the Weil conjectures in full generality. The result provoked attention and brought Deligne into the mathematical elite.

NUMBERS OF SOLUTIONS OF EQUATIONS IN FINITE FIELDS

ANDRÉ WEIL

The equations to be considered here are those of the type

$$a_0x_0^{n_0} + a_1x_1^{n_1} + \cdots + a_rx_r^{n_r} = b. \tag{1}$$

Such equations have an interesting history. In art. 358 of the *Disquisitiones* [1 a],[1] Gauss determines the Gaussian sums (the so-called cyclotomic "periods") of order 3, for a prime of the form $p=3n+1$, and at the same time obtains the numbers of solutions for all congruences $ax^3-by^3\equiv 1 \pmod p$. He draws attention himself to the elegance of his method, as well as to its wide scope; it is only much later, however, viz. in his first memoir on biquadratic residues [1b], that he gave in print another application of the same method; there he treats the next higher case, finds the number of solutions of any congruence $ax^4-by^4\equiv 1 \pmod p$, for a prime of the form $p=4n+1$, and derives from this the biquadratic character of 2 mod p, this being the ostensible purpose of the whole highly ingenious and intricate investigation. As an incidental consequence ("*coronidis loco*," p. 89), he also gives in substance the number of solutions of any congruence $y^2=ax^4-b \pmod p$; this result includes as a special case the theorem stated as a conjecture ("*observatio per inductionem facta gravissima*") in the last entry of his *Tagebuch* [1c];[2] and it implies the truth of what has lately become known as the Riemann hypothesis, for the function-field defined by that equation over the prime field of p elements.

Gauss' procedure is wholly elementary, and makes no use of the Gaussian sums, since it is rather his purpose to apply it to the determination of such sums. If one tries to apply it to more general cases, however, calculations soon become unwieldy, and one realizes the necessity of inverting it by taking Gaussian sums as a starting point. The means for doing so were supplied, as early as 1827, by Jacobi, in a letter to Gauss [2a] (cf. [2b]). But Lebesgue, who in 1837 devoted two papers [3a, b] to the case $n_0=\cdots=n_r$ of equation (1), did not

Received by the editors October 2, 1948; published with the invited addresses for reasons of space and editorial convenience.

[1] Numbers in brackets refer to the bibliography at the end of the paper.

[2] It is surprising that this should have been overlooked by Dedekind and other authors who have discussed that conjecture (cf. M. Deuring, Abh. Math. Sem. Hamburgischen Univ. vol. 14 (1941) pp. 197–198).

Counting modulo 5

Counting modulo 5 means that in stead of counting 0,1,2,3,4,5,6,7,8,..., we count 0,1,2,3,4,0,1,2,3,..., i.e. we start again at 0 every time we reach 5. The computation 4+2 means counting 2 steps further from 4. Counting modulo 5, doesn't bring us to 6, but rather to 1, i.e. 4+2=1.

Another example of modulo-counting is time, where we count modulo 12. If we leave home at 10 o'clock and stays out for four hours, then we return at 2 o'clock.

Back to modulo 5 counting. The computation $3 \cdot 4$ modulo 5, means counting to 4 three times, i.e. 1,2,3,4,0,1,2,3,4,0,1,2, which gives $3 \cdot 4 = 2$. The number system $\{0,1,2,3,4\}$ with these computation rules is called **a finite field** of 5 elements.

Our aim is to find the solutions of the equation $x^2 - y^2 = 3$ within this number system. Computing all the squares, $0^2=0$, $1^2=1$, $2^2=4$, $3^2=4$ and $4^2=1$, we see that the only possibility to achieve a difference 3 between two squares is when $x^2=4$ og $y^2=1$. There are two numbers of square 4 (2^2 and 3^2), and two of square 1 (1^2 and 4^2), thus we get all together four solutions, $x=2$ and $y=1$, $x=2$ and $y=4$, $x=3$ and $y=1$, and $x=3$ and $y=4$.