Preliminary version
August 30, 1994

Università degli
Studi di Trento

Fermat's Last Theorem.

René Schoof

Dipartimento di Matematica
Università degli Studi di Trento
I-38050 Povo (Trento) ITALY
Email: schoof@volterra.cineca.it

Abstract. In this expository paper we briefly recall the history of Fermat's Last Theorem. Then we explain G. Frey's important idea to prove Fermat's Last Theorem. This involves the arithmetic of elliptic curves and modular forms. We mention Ribet's 1986 result that the Taniyama-Weil conjecture implies Fermat's Last Theorem. We give some explicit examples of his theorem. Finally we discuss Wiles's approach to prove the Taniyama-Weil conjecture.

1. Introduction.

In this expository paper we discuss some of the mathematics involved in the recent attempts to prove Fermat's Last Theorem. These efforts are based on an idea of Gerhard Frey (Essen, at the time in Saarbrücken) who in 1986 proposed a method based on the arithmetic of elliptic curves over the rational number field $\mathbf{Q}$. Soon after Frey announced his idea, Jean-Pierre Serre (Collège de France, Paris) formulated a precise conjecture which would imply Fermat's Last Theorem. His conjecture consisted of two parts: the long-standing and notorious Taniyama-Weil conjecture relating elliptic curves over $\mathbf{Q}$ to modular forms of weight 2 and another hypothesis which was believed to be more accessible and was called "ε" at the time. In short: "Taniyama-Weil plus ε implies Fermat".

Already in the same year Kenneth Ribet (Berkeley) proved "ε", generalizing a result of Barry Mazur (Harvard). Even though the result was called "ε", the proof is not at all easy: it relies on a lot of delicate Grothendieck style algebraic geometry and is based on some very clever new ideas. Ribet's result reduced Fermat's Last Theorem to another unproved hypothesis: the Taniyama-Weil conjecture. It may not seem so, but this was considered to be tremendous progress. A somewhat arbitrary problem like Fermat's Last Theorem had been reduced to a conjecture which, for several reasons, was widely believed to be true. A proof of the Taniyama-Weil conjecture would confirm part of the so-called "Langlands philosophy" which

is directing much of current research in number theory. But ... in 1986 such a proof seemed very far away.

Nevertheless, from 1986 on Andrew Wiles (Princeton) tried to prove enough of the Taniyama-Weil conjecture to prove Fermat's Last Theorem. On June 23, 1993, Wiles announced at the Newton Institute in Cambridge (UK) that he had proved the Taniyama-Weil conjecture for all semi-stable elliptic curves over $\mathbf{Q}$ (see section 3 for semi-stable elliptic curves). His proof was very complicated; it relied upon difficult results by R. Langlands [14], J. Tunnell [23], V. Kolyvagin [12], B. Mazur [16] and M. Flach [7] to name a few. The result claimed by Wiles was strong enough to imply Fermat's Last Theorem.

Wiles's manuscript was not made public. A number of referees began to check the details of Wiles's proof. Not surprisingly, some inaccuracies and minor problems turned up, but all of these could be repaired easily. Unfortunately, somewhere near the end of 1993 it was found that a certain argument was not complete. This time it was not immediate how to fix it. In a widely circulated e-mail message Wiles made this public in december 1993, adding that he was confident he could fill the gap by extending his arguments.

At the moment (august 1994) it seems that the proof has not yet been made to work, but that Wiles still has a proof of the Taniyama-Weil conjecture for a very large class of semi-stable elliptic curves. Even though this result does not quite implies Fermat's Last Theorem, it is of tremendous importance for number theory. Wiles's result is the first step towards a proof of the Taniyama-Weil conjecture, a conjecture which only eight years ago seemed hopelessly intractable.

In this paper we briefly explain the concepts that are involved in Wiles's proof. Unfortunately, for several reasons we cannot present Wiles's work in any detail. We merely sketch the lines of thought and apologize for the many inaccuracies and incomplete statements that the reader will encounter. For a more detailed discussion see the paper by Rubin and Silverberg [19]. After some historical remarks in section 2, we quickly introduce in sections 3 and 4 some of the basic concepts that occur in the proof. In section 5 we explain Frey's idea and mention Ribet's 1986 proof that the Taniyama-Weil conjecture implies Fermat's Last Theorem. In section 6 we say a few words about Wiles's work.

2. History.

Pierre de Fermat was a French magistrate who lived in Toulouse from 1601 to 1665. He was one of the leading mathematicians of his time. In those days most mathematicians were interested in questions concerning analytic geometry, calculus and probability theory. Fermat made substantial contributions to these fields. We know about his work through his correspondence with mathematicians like Pascal, Descartes and Huijgens.

Fermat was one of the few to be interested in questions concerning algebra and arithmetic. These fields were well developed in the Arab world, but not so in Europe. The only texts available were Greek and Latin translations of Arab texts, often in editions containing comments by European scholars. One of the most important available texts was a text on algebra and arithmetic by Diophantus of Alexandria. Diophantus probably lived around 300 AD; by the time Fermat began

to study his arithmetical works, nobody in Europe had an understanding of these problems comparable to Diophantus's insights more than 1000 years earlier.

Fermat studied Bachet's edition of Diophantus text [5] which was published in 1621. After the death of his father, Fermat's son published in 1670 a new edition of Bachet's "Diophantus", this time supplied with the comments his father had written in the margins of his copy. Many of these comments are generalizations of statements in Diopantus's text, usually given without proof. It is here that we find Fermat's famous claim. Near a discussion by Diophantus on the form of the solutions of the Pythagoras equation

$$X^2 + Y^2 = Z^2$$

in integers $X, Y, Z \in \mathbf{Z}$ (for instance $3^2 + 4^2 = 5^2$, $5^2 + 17^2 = 18^2$, $65^2 + 72^2 = 97^2$ ... etc.), Fermat had commented that, on the other hand, it is not possible to write a cube as a sum of two cubes or a fourth power as the sum of two fourth powers and that in general, for any n larger than 2, the sum of two n-th powers of natural numbers cannot itself be an n-th power of a natural number. Unfortunately, Fermat writes, the margin of the book is too small to contain his "truly marvelous proof".

> *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nomines fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*

Sooner or later all Fermat's statements were proved or disproved, except this one, the last. It became known as "Fermat's Last Theorem". In our notation Fermat's statement boils down to the following.

Fermat's Last Theorem. *For every integer $n > 2$, the equation*

$$X^n + Y^n = Z^n$$

has no solutions in integers $X, Y, Z > 0$.

In this section we discuss the early results concerning Fermat's Last Theorem. First we recall the exponent 2 case:

$$X^2 + Y^2 = Z^2.$$

In this case there are many solutions and they can be parametrized easily. This was known since antiquity.

Theorem 2.1. *Every solution $X, Y, Z \in \mathbf{Z}_{>0}$ with $\gcd(X, Y, Z) = 1$ of the equation*

$$X^2 + Y^2 = Z^2$$

is of the form

$$\begin{aligned} X &= a^2 - b^2, \\ Y &= 2ab, \\ Z &= a^2 + b^2, \end{aligned}$$

(or with the roles of X and Y reversed) where $a, b \in \mathbf{Z}_{>0}$ satisfy $a > b > 0$ and $\gcd(a, b) = 1$.

The proof is well known and rather easy [10]. As an example, we mention the solution

$$65^2 + 72^2 = 97^2.$$

It corresponds to $a = 9$ and $b = 4$ because $X = 65 = 9^2 - 4^2$, $Y = 72 = 2 \cdot 4 \cdot 9$ and $Z = 97 = 9^2 + 4^2$.

The case of exponent 4 was dealt with by Fermat himself. The proof is a beautiful example of Fermat's method of "infinite descent". This method is even today one of the fundamental tools in the study of Diophantine equations. We present the proof of a slightly stronger statement. It is based on the shape of the solutions of the Pythagorean equation.

Theorem 2.2. *The only integral solutions of the equation*

$$X^4 + Y^4 = Z^2$$

are the trivial ones, i.e., the ones with $XYZ = 0$.

Proof. Suppose X, Y, Z is a non-trivial solution of this equation and let's suppose this solution is *minimal* in the sense that $|Z| > 0$ is minimal. This is easily seen to imply that $\gcd(X, Y, Z) = 1$. We may and do assume that $X, Y, Z > 0$. By considering the equation modulo 4, one sees that precisely one of X and Y is odd. Let's say that X is odd. By Theorem 2.1 there are integers $a > b > 0$ with $\gcd(a, b) = 1$ and

$$\begin{aligned} X^2 &= a^2 - b^2, \\ Y^2 &= 2ab, \\ Z &= a^2 + b^2. \end{aligned}$$

consider the first equation $X^2 + b^2 = a^2$. Since $\gcd(a, b, X) = 1$, we can apply Theorem 2.1 once more and we obtain

$$\begin{aligned} X &= c^2 - d^2, \\ b &= 2cd, \\ a &= c^2 + d^2, \end{aligned}$$

for certain integers $c > d > 0$ which satisfy $\gcd(c, d) = 1$. Substituting these expressions for a and b in the equation $Y^2 = 2ab$ above, we find

$$\begin{aligned} Y^2 &= 2ab = 2(2cd)(c^2 + d^2), \\ \left(\frac{Y}{2}\right)^2 &= c \cdot d \cdot (c^2 + d^2). \end{aligned}$$

The numbers c, d and $c^2 + d^2$ have no common divisors and their product is a square. The fundamental fact that every natural number can be factored into a product of prime numbers *in a unique way* implies easily that there exist integers U, V, W with

$$\begin{aligned} c &= U^2, \\ d &= V^2, \\ c^2 + d^2 &= W^2. \end{aligned}$$

It is easy to see that $\gcd(U, V, W) = 1$ and that

$$U^4 + V^4 = W^2.$$

We have obtained a new solution of the equation! It is easily checked that $W \neq 0$ and that $|W| \leq W^2 = c^2 + d^2 = a < a^2 < |Z|$. This contradicts the minimality of $|Z|$. We conclude that there are no non-trivial solutions of the equation, as required.

This clearly implies that the equation $X^4 + Y^4 = Z^4$ also admits only trivial solutions $X, Y, Z \in \mathbf{Z}$. Fermat's result has an important consequence: first we remark that every integer $n \geq 3$ is either divisible by a prime $p \geq 3$ or it is divisible by 4. If there were a solution

$$X^n + Y^n = Z^n$$

with $XYZ \neq 0$ of Fermat's equation, for some n divisible by 4, we would have

$$\left(X^{n/4}\right)^4 + \left(Y^{n/4}\right)^4 = \left(Z^{n/4}\right)^4.$$

By Fermat's result for exponent 4 this is impossible. Therefore the exponent n must be divisible by a prime number $p \geq 3$. Then we have

$$\left(X^{n/p}\right)^p + \left(Y^{n/p}\right)^p = \left(Z^{n/p}\right)^p$$

and we see that for some prime number $p \geq 3$ the equation

$$X^p + Y^p = Z^p$$

also would admit a solution $X, Y, Z \in \mathbf{Z}$ with $XYZ \neq 0$.

Therefore we may restrict our attention to Fermat's equation with *prime* exponent. A proof of the impossibility of the equation with exponent $p = 3$ was found by Euler (1707–1783) in 1753. In 1825 the young German mathematician Lejeune Dirichlet (1805-1859) all but proved the impossibility for exponent 5. His proof was completed by Adrien-Marie Legendre (1752–1833) who was 73 years old at the time. Shortly afterwards the French mathematician Lamé took care of the case with exponent $p = 7$. All these proof are rather involved applications of Fermat's method of infinite descent.

A big step forward was made by Ernst Eduard Kummer (1810–1893) around 1847. Kummer used the ring $\mathbf{Z}[\zeta_p]$ generated by a primitive p-th root of unity ζ_p. Using the elements of this ring Kummer studies Fermat's equation. He writes it as

$$Z^p = X^p + Y^p = \prod_{i=0}^{p-1} \left(X + \zeta_p^i Y\right),$$

where X, Y and Z are positive integers. Kummer showed that the factors in the product either do not have any divisors in common or they admit a common divisor

of a very restricted type. Then he proceeds very much as in the proof of Theorem 2.2: if the ring $\mathbf{Z}[\zeta_p]$ is a unique factorization domain or, more generally, if the ideal class group of $\mathbf{Z}[\zeta_p]$ has cardinality prime to p, this implies that *each* of the factors $X+\zeta_p^i Y$ is, upto a unit of the ring $\mathbf{Z}[\zeta_p]$, *itself* a p-th power in $\mathbf{Z}[\zeta_p]$. By means of an argument that is not important for the moment, Kummer deduced a contradiction from this, proving Fermat's Last Theorem for the exponents p for which the ideal class group of $\mathbf{Z}[\zeta_p]$ has cardinality prime to p.

In his proof Kummer used his theory of "ideal numbers" from which our modern ideal theory was to develop. He also obtained an explicit expression for the cardinality of part of the ideal class group of $\mathbf{Z}[\zeta_p]$. This enabled Kummer to obtain a criterion, which can be formulated entirely in elementary terms. It is the most important contribution to the proof of Fermat's Last Theorem until the developments of 1986:

Theorem 2.3. *Let $p \geq 3$ be a prime. If p does not divide the numerators of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$, then the equation*

$$X^p + Y^p = Z^p$$

admits only solutions $X, Y, Z \in \mathbf{Z}$ with $XYZ = 0$.

Here the Bernoulli numbers are rational numbers defined by the Taylor series expansion

$$\frac{X}{e^X - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} X^k.$$

Since $X/(e^X - 1) + X/2 = \frac{X}{2}\coth(\frac{X}{2})$ is an even function, we see that $B_1 = -1/2$ and that the Bernoulli numbers B_k are zero for odd $k \geq 3$. The first few are:

$$B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30},$$
$$B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730}, \quad B_{14} = \frac{7}{6}, \quad B_{16} = -\frac{3617}{510}, \ldots$$

A computation of the first 100 or so Bernoulli numbers and an application of Theorem 2.3 imply that Fermat's Last Theorem is true for all primes $p < 100$ except possibly $p = 37, 59$ or 67. By refining his arguments slightly Kummer eventually proved that Fermat's Last Theorem is true for every single prime $p < 100$.

By using Theorem 2.3 and variations on it, Fermat's Last Theorem had by 1992 been proved to be true for all primes p less than 4 million [2]. This involved extensive computer calculations involving many smart computational tricks.

For a more thorough discussion of Fermat's work see André Weil's book [26]. For more literature on Fermat's Last Theorem see the texts by Ribenboim [18], Edwards [6] and Washington [24].

3. Elliptic curves.

Elliptic curves are at the heart of Gerhard Frey's approach to Fermat's Last Theorem. They were intensively studied from a complex analytic point of view in the last century. Elliptic curves owe their name to the so-called "elliptic integrals" that one encounters when one computes the circumference of an ordinary ellipse. It appeared that these integrals are best understood in terms of certain Riemann surfaces of genus 1: elliptic curves. The complex analytic theory of the Weierstraß $\wp$-function gives a a very accessible approach to the theory of elliptic curves over $\mathbf{C}$.

In this section we introduce elliptic curves from a rather naive algebraic point of view. See Silverman's book [21] for a more complete discussion. Elliptic curves over $\mathbf{Q}$ are non-singular plane curves given by an equation of the form

$$Y^2 = X^3 + AX^2 + BX + C$$

where $A, B, C \in \mathbf{Q}$. The *discriminant* of E is simply the discriminant of the cubic polynomial. Since the curve is non-singular, the cubic polynomial does not have multiple zeroes and the discriminant is not zero. Even though we have given the curve as a subvariety of the affine plane, one should really work with the *projective* curve E given by the homogeneous equation

$$y^2z = x^3 + Ax^2z + Bxz^2 + Cz^3 \qquad \text{in } \mathbf{P}^2.$$

The points $P = (x : y : z) \in \mathbf{P}^2$ of E with non-zero z-coordinate correspond to the points $(X, Y) = (x/z, y/z)$. There is only one point with $z = 0$; it is *the point at infinity* $(0 : 1 : 0) = \infty$.

The main fact about elliptic curves is, that they are *group varieties:* their (complex) points admit a natural geometric group structure. The neutral element 0 of the group is the point at infinity. Three points on the curve have sum zero if they lie on a straight line. To compute the sum of two points P and Q, one draws the line through P and Q. Since the curve has degree 3, there is a third point of intersection R. Next one draws the line trough R and ∞; in other words, one draws the vertical line through R. The third intersection point is the sum of P and Q. If $P = Q$, one should replace the line through P and Q by the tangent line at P.

Fig.1. The group law on E.

It is clear that the group law is commutative and *algebraic* , i.e. the addition of points can be expressed by means of polynomial functions in their coordinates. It

is a straightforward exercise to verify that the points of order 2 are precisely the points of the form $(e_i, 0)$, where $X^3 + AX^2 + BX + C = (X - e_1)(X - e_2)(X - e_3)$. This means that

$$E[2] = \{P \in E(\mathbf{C}) : P + P = 0\}$$
$$\{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}$$

Here $E(\mathbf{C})$ denotes the group of points of E with complex coordinates and for every integer $n > 0$, we let

$$E[n] = \{P \in E(\mathbf{C}) : \underbrace{P + P + \ldots + P}_{n \text{ times}} = 0\}.$$

The groups $E[n]$ are finite algebraic subgroups of E. For instance

$$E[3] = \{P = (x, y) \in E(\mathbf{C}) : 3x^4 + 4Ax^3 + 6Bx^2 + 12Cx + 4AC - B^2 = 0\} \cup \{\infty\}$$

as one easily finds by an explicit computation.

The polynomials that describe the groups $E[n]$ become more complicated as n grows, but the coefficients are always in $\mathbf{Q}$. This implies that if $P = (x, y)$ is in $E[n]$, so are all the algebraic conjugate points. In other words, the Galois group of $\overline{\mathbf{Q}}$ over $\mathbf{Q}$ acts on $E[n]$. It is an important fact that

$$E[n] \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$$

as abelian groups. The action of the Galois group gives therefore rise to a *Galois representation*

$$\rho_n : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) \quad (= \mathrm{Aut}(E[n])).$$

For a prime l one can form the projective system

$$\ldots \xrightarrow{l} E[l^n] \xrightarrow{l} \ldots \xrightarrow{l} E[l^2] \xrightarrow{l} E[l]$$

where the transition maps are given by mapping P to the l-fold sum $P + P + \ldots + P$. The projective limit of this system is called the *Tate module* $T_l E$:

$$T_l E = \lim_{\leftarrow} E[l^n].$$

Since $E[l^n] \cong \mathbf{Z}/l^n\mathbf{Z} \times \mathbf{Z}/l^n\mathbf{Z}$, the Tate module $T_l E$ is isomorphic to $\mathbf{Z}_l \times \mathbf{Z}_l$ where $\mathbf{Z}_l$ denotes the ring of l-adic integers. The group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $T_l E$ and this gives rise to an l-adic Galois representation

$$\rho_{l^\infty} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_l).$$

In order to define the L-series of E we need to consider the curve E *modulo prime numbers* q. Without loss of generality we may assume that the coefficients A, B and C of the equation

$$Y^2 = X^3 + AX^2 + BX + C$$

are actually integers. When we view the equation of E modulo a prime number q we obtain a cubic curve over the finite field $\mathbf{F}_q$. This curve need not be non-singular. Apart from the prime $q = 2$, the curve E is singular modulo q precisely when the cubic polynomial $X^3 + AX^2 + BX + C$ acquires a multiple zero modulo q. This happens only for the finitely many prime numbers q that divide the discriminant of E . These are the so-called *bad* primes. The remaining ones are called *good* and when we view the equation of E modulo a good prime q we obtain a *non-singular* curve, i.e. an elliptic curve over the finite field $\mathbf{F}_q$. For good primes $q \neq l$ we can repeat the construction above and we find that $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ acts on the l-adic Tate module of the curve E mod q. This means that we have a representation

$$\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_l).$$

Let φ_q denote the *Frobenius automorphism,* i.e., the canonical topological generator of the Galois group of $\overline{\mathbf{F}}_q$ over $\mathbf{F}_q$ which is defined by

$$\varphi(\alpha) = \alpha^q \qquad \alpha \in \overline{\mathbf{F}}_q.$$

The characteristic polynomial of φ_q, viewed as an l-adic 2×2 matrix is given by

$$T^2 - a_q T + q$$

where a_q is determined by the relation

$$\#E(\mathbf{F}_q) = q + 1 - a_q.$$

Here $E(\mathbf{F}_q)$ denotes the set of points of the curve (E mod q) over $\mathbf{F}_q$. This implies in particular that the characteristic polynomial of φ_q has its coefficients in $\mathbf{Z}$ and does not depend on l.

Definition. The L-series $L(E, s)$ of the elliptic curve E is given by

$$L(E,s) = \prod_{q \text{ good}} \frac{1}{\det(1 - q^{-s}\varphi_q)} \prod_{q \text{ bad}} (\cdots).$$

Here $s \in \mathbf{C}$ has sufficiently large real part to ensure convergence of the product. There is also a "proper" definition for the factors corresponding to the bad primes. We just describe the result:

$$L(E,s) = \prod_{q \text{ good}} \frac{1}{1 - a_q q^{-s} + q^{1-2s}} \prod_{q \text{ bad}} \frac{1}{1 - a_q q^{-s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

For the good primes, the coefficients $a_q \in \mathbf{Z}$ are determined by the formula above. For the bad primes there are two possibilities: If the unique singular point of E mod q is an ordinary double point, then $a_q = +1$ or -1 according as the slopes of the tangent lines are in $\mathbf{F}_q$ or not. In this case the reduction of E is called *semi-stable.* If the singularity is not an ordinary double point, then $a_q = 0$. We have ignored

the fact that one has a lot of choice in choosing an equation for E with coefficients in $\mathbf{Z}$. See [21] for the whole story.

At this point we also introduce the *conductor* N of E. Like the discriminant it measures in some sense the bad reduction properties. The prime divisors of N are precisely the bad primes. If q is a bad prime larger than 3, then the recipee for the exact power of q that divides N is very easy: it is q when the reduction is semi-stable and q^2 otherwise. For the primes $q = 2$ and 3 the recipee is more complicated [3].

Here's an explicit example: consider the elliptic curve E

$$Y^2 = X^3 - X^2 - 77X + 330.$$

The discriminant is equal to $-2^4 3^{10} 11$. See [3] for the correct definitions for the prime 2. The reductions of E modulo 3 and 11 are semi-stable. The conductor turns out to be $N = 132 = 2^2 \cdot 3 \cdot 11$. Modulo 3 the equation of the curve becomes $Y^2 = X^3 + X^2 + X = X(X-1)^2$; the tangent lines at the singular point $(1,0)$ are given by $Y = \pm(X-1)$. Modulo 11 the equation becomes $Y^2 = X^3 - X^2$. The singular point is $(0,0)$ with tangent lines $Y = \pm X$. Therefore the factors corresponding to the bad primes 2, 3 and 11 are 1, $(1-3^{-s})^{-1}$ and $(1-11^{-s})^{-1}$ respectively. To determine the factors $(1 - a_q q^{-s} + q^{1-2s})^{-1}$ of some small good primes, we compute the coefficients a_q using the relation $\#E(\mathbf{F}_q) = q + 1 - a_q$. For instance, the curve has the following six points with coordinates in $\mathbf{F}_7$: $\{\infty, (0, \pm 1), (1, \pm 1), (4, 0)\}$. Therefore $a_7 = 7 + 1 - 6 = 2$. The first few a_q are given in the table.

q	$\#E(\mathbf{F}_q)$	a_q	q	$\#E(\mathbf{F}_q)$	a_q
2	–	–	23	16	-8
3	–	–	29	30	0
5	4	2	31	32	0
7	6	2	37	44	-6
11	–	–	41	42	0
13	8	6	43	54	10
17	22	-4	47	48	0
19	22	-2	53	68	14

The L-series of E begins like this

$$L(E,s) = 1 + \frac{1}{3^s} + \frac{2}{5^s} + \frac{2}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \frac{6}{13^s} + \frac{2}{15^s} - \frac{4}{17^s} - \frac{2}{19^s} + \dots$$

One should view the L-series of an elliptic curve as an analogue of the Riemann ζ-function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{q \text{ prime}} \frac{1}{1-q^{-s}}, \qquad s \in \mathbf{C}, \operatorname{Re} s > 1.$$

Indeed, if we replace the Tate module $T_l E$ by the ring of l-adic integers $\mathbf{Z}_l$ itself provided with the *trivial* Galois action, then the analogue of our definition gives us the Riemann ζ-function. This time the l-adic module has rank 1 rather than 2.

One expects many of the properties of the Riemann ζ-function also to hold for these L-series. For instance, the Riemann ζ-function can be extended meromorphically to all of $\mathbf{C}$ and satisfies a functional equation:

$$Z(s) = Z(1-s)$$

where $Z(s) = \Gamma(s/2)\pi^{-s/2}\zeta(s)$ is a slight modification of the Riemann ζ-function. Here $\Gamma(s)$ denotes the usual Γ-function: $\Gamma(s) = \int_0^\infty e^{-t}t^s\frac{dt}{t}$ (for $s \in \mathbf{C}$, $\mathrm{Re}s > -1$).

For the functions $L(E,s)$ one expects the following:

Conjecture. Let E be an elliptic curve over $\mathbf{Q}$, then $L(E,s)$ admits an analytic continuation to $\mathbf{C}$ and

$$\Lambda(E,s) = \pm N^{1-s}\Lambda(E,2-s) \qquad s \in \mathbf{C},$$

where $\Lambda(E,s) = \Gamma(s)(2\pi)^{-s}L(E,s)$ is a slight modification of the L-series on E. Here N denotes the conductor of E. There is also a precise conjecture for the sign, but we will not go into this.

This conjecture is more or less equivalent to the Taniyama-Weil conjecture and is one of the main motivations behind it [1, 25]. In the next section we will discuss the Taniyama-Weil conjecture in terms of modular forms. It is possible to verify the functional equation for every explicitly given curve and this has been done in numerous cases. For completeness sake we remark that there is also an analogue of the Riemann Hypothesis for the functione $L(E,s)$: one expects that the "non-trivial" zeroes of $L(E,s)$ all have real part equal to 1. This has been verified for a few zeroes of a handful of elliptic curves.

4. Modular forms.

The group $\mathrm{SL}_2(\mathbf{Z})$ acts on the upper halfplane $\mathbf{H} = \{z \in \mathbf{C} : \mathrm{Im}z > 0\}$ via fractional linear transformations:

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}(z) = \frac{\alpha z+\beta}{\gamma z+\delta} \qquad z \in \mathbf{H},\ \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

For every positive integer $N \geq 1$ we let

$$\Gamma_0(N) = \{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : \gamma \equiv 0 \pmod N\}.$$

The quotient space $\mathbf{H}/\Gamma_0(N)$ is a Riemann surface. It is naturally compactified by adding finitely many "cusps". These are the $\Gamma_0(N)$-equivalence classes of $\mathbf{Q}\cup\{\infty\}$. The compactified Riemann surface has a model over $\mathbf{Q}$ and is denoted by $X_0(N)$: the *modular curve of level* N.

We will consider modular forms of level N and weight 2 only. These are related to differentials of the curve $X_0(N)$.

Definition. Let $N \geq 1$ be an integer. A *modular form of level* N (and weight 2) is a holomorphic function f on $\mathbf{H}$ for which the differential form $f(z)dz$ is $\Gamma_0(N)$-invariant:

$$f(Mz)d(Mz) = f(z)dz, \qquad \text{for } M \in \Gamma_0(N)$$

and which is holomorphic at the cusps.

Since the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ is contained in $\Gamma_0(N)$, we have that $f(z+1) = f(z)$. Therefore f admits a Fourier expansion which looks like

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z} \qquad a_n \in \mathbf{C}$$

because f is holomorphic at the cusps. A *cusp form* is a modular form which vanishes at the cusps. This implies that the first coefficient a_0 of its Fourier expansion vanishes. The cusp forms of level N form a finite dimensional vector space $S_2(\Gamma_0(N))$. One has that $S_2(\Gamma_0(M)) \subset S_2(\Gamma_0(N))$ whenever M divides N.

On the vector space of cusp forms acts the so-called *Hecke algebra* which is generated by the Hecke operators. We do not give the definitions here.

Definition. Let $N \geq 1$ be an integer. A *newform* of level N (and weight 2) is a modular form of level N and weight 2 which is *not* a modular form of any lower level and which is a normalized eigenform for the action of the Hecke algebra, i.e. $f = \sum_{n\geq 1} a_n e^{2\pi i n z}$ with $a_1 = 1$.

One defines the *L-series* $L(f,s)$ associated to a newform $f = \sum_{n\geq 1} a_n q^n$ by

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad s \in \mathbf{C},\ \mathrm{Re}\, s >> 0.$$

In contrast to the situation for elliptic curves, one knows that the L-function associated to a modular forms satisfies a functional equation.

Theorem 4.1. *Let f be a newform of level N, then*

$$\Lambda(f,s) = \pm N^{1-s}\Lambda(f, 2-s) \qquad s \in \mathbf{C},$$

where $\Lambda(f,s) = \Gamma(s)(2\pi)^{-s}L(f,s)$ is a slight modification of the L-series of f. There is also a precise formula for the sign, but we will not go into this.

In all cases where one can prove that the L-function associated to an elliptic curve E over $\mathbf{Q}$ satisfies the expected functional equation, this is shown by proving that the corresponding Fourier series is a newform of weight two. One expects that this is always so:

Taniyama-Weil Conjecture. *Every elliptic curve E over $\mathbf{Q}$ is modular, i.e., if its L-series is given by*

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

then the associated Fourier series $\sum_n a_n e^{2\pi i n z}$ is a newform of weight 2 and level N, where N is equal to the conductor of E.

The Taniyama-Weil conjecture has been verified in numerous explicit cases [1],[3]. It is equivalent to the statement that there exists a non-constant morphism ϕ :

$X_0(N) \longrightarrow E$. The conjecture clearly implies that the L-series of an elliptic curve over $\mathbf{Q}$ satisfies the expected functional equation. The Taniyama-Weil is actually more or less equivalent to this statement [25].

Finally we mention the important fact that it is possible to associate a 2-dimensional Galois representation to a newform.

Theorem 4.2. *Let $f = \sum_n a_n e^{2\pi i n z}$ be a newform of weight 2 and level N. For every prime l there is a Galois representation*

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(R)$$

such that for almost every prime q the characteristic polynomial of the Frobenius automorphism φ_q is equal to

$$T^2 - a_q T + q.$$

Here R denotes the ring generated by the Fourier coefficients over $\mathbf{Z}_l$.

For the proof for arbitrary weights see [4].

5. The Taniyama-Weil conjecture implies Fermat's Last Theorem.

In 1986 the German mathematician Gerhard Frey proposed a new approach to prove Fermat's Last Theorem [9]. His method was related to methods of Hellegouarch [11] published around 1970. To a solution

$$a^p + b^p = c^p$$

in coprime integers a, b, c of Fermat's equation of prime exponent $p \geq 3$ Frey associated an elliptic curve:

$$Y^2 = X(X - a^p)(X - c^p).$$

Frey's elliptic curve is defined over $\mathbf{Q}$. Frey observed that this curve has rather strange properties. This made him believe that perhaps one could show that a curve with such properties cannot exist and that therefore solutions to Fermat's equations cannot exist either.

The zeroes of the polynomial $X(X - a^p)(X - c^p)$ are evidently equal to 0, a^p and c^p. They coincide modulo a prime number l if and only if l divides both a and c. But by Fermat's equation, l then also divides b, which contradicts the fact that a, b and c were supposed to be coprime integers. Therefore this cannot happen and we conclude that the curve is *semi-stable:* ignoring a small complication when $l = 2$, the only bad primes are the divisors of a, b or c. Modulo these Frey's curve acquires an ordinary double point.

Upto a power of 2, the discriminant of Frey's curve is equal to

$$\left(a^p c^p (a^p - c^p)\right)^2 = (abc)^{2p}.$$

This is a p-th power and that is a crucial observation. It implies that the structure of the subgroup of p-torsion points on Frey's curve is very restricted. This is easily

seen using Tate's rigid analytic p-adic model of the semi-stable elliptic curve. One way to express this fact is to say that the subgroup scheme $E[p]$ of points of order p is finite and flat over $\mathbf{Z}$ of type (p,p). One can, at present, not prove very much about such finite flat group schemes. One expects [20] that they are isomorphic to products of the group schemes $\mathbf{Z}/p\mathbf{Z}$ and μ_p.

In this particular case one should have that

$$E[p] \cong \mathbf{Z}/p\mathbf{Z} \times \mu_p$$

for every prime p. In other words, $E[p]$ is a direct sum of two summands, one with trivial action by the Galois group of $\overline{\mathbf{Q}}$ over $\mathbf{Q}$ and the other isomorphic to the group scheme of the p-th roots of unity. This is known to be true only when $p \leq 17$. This is a consequence of J.-M. Fontaine's 1983 results [8] on finite flat group schemes over $\mathbf{Z}$.

However, if the conjecture about these finite flat group schemes is correct in general, then it follows at once that Frey's elliptic curve must have a point of order p with coordinates in $\mathbf{Q}$: the points in the summand of $E[p]$ with trivial Galois action are such points. It is a consequence of the results in Barry Mazur's famous "Eisenstein ideal" paper [15] that this is impossible for $p > 3$. This contradiction shows that Frey's curve cannot exist and hence that there are no non-trivial solutions to Fermat's equation $a^p + b^p = c^p$ for $p > 3$.

Mazur's 1976 paper [15] has been very important for the development of arithmetic during the past years. In it Mazur applies delicate arithmetic algebraic geometry to the study of modular curves. The main result of the paper is the solution of an infinite family of Diophantine equations. Mazur's method is still Fermat's method of infinite descent, expressed in the language of flat cohomology.

Frey hoped that one could still prove that his elliptic curves could not exist without using the unproved conjectures concerning finite flat group schemes. Later in 1986, J.-P. Serre formulated a precise conjecture on elliptic curves over $\mathbf{Q}$ which would imply Fermat's Last Theorem. This conjecture was proved by Ribet, but only under the assumption of yet another conjecture: the Weil-Taniyama conjecture, which was mentioned in the previous section. Ribet proved the following [18].

Theorem 5.1. *Let N be a positive integer and let l be a prime dividing N. Suppose $f = \sum_n a_n e^{2\pi i n z}$ is a newform of weight 2 for $\Gamma_0(N)$ and suppose that the associated action of the Galois group on the p-torsion points of the representation of Theorem 4.2 is "finite" and irreducible. Then there is a newform $g = \sum_n b_n e^{2\pi i n z}$ of weight 2 for the group $\Gamma_0(N/l)$ such that*

$$a_q \equiv b_q \pmod{\mathfrak{p}}, \qquad \text{for almost all primes } q$$

for some prime ideal over $\mathfrak{p}$ of some number field.

The condition that the action on the p-torsion points is finite means that the Galois representation "comes from" a finite flat group scheme over $\mathbf{Z}$. In particularly, the primes $q \neq p$ are unramified. The proof of Theorem 4.1 involves a lot of subtle algebraic geometry of modular curves and Shimura curves. We won't say

a word about it. We give instead an explicit example, taken from the tables of modular elliptic curves [3].

Let E be the elliptic curve

$$Y^2 = X^3 - X^2 + 25158X - 775719.$$

The bad primes are 2, 3, 7 and 11. The discriminant is equal to $-2^4 3^5 7^5 11^7$. The curve E is semi-stable modulo the primes 3, 7 and 11. The conductor of E is $924 = 4 \cdot 3 \cdot 7 \cdot 11$. It is the curve 924A1 in J. Cremona's table of modular elliptic curves [3]. In the table the first few values of the coefficients a_q of the newform associated to E are given. It can be shown that the Galois action on $E[3]$ and $E[7]$ are irreducible. Since the exponents of the primes 3 and 7 in the factorization of the discriminant are both equal to 5, we conclude that $E[5]$ is "finite" at both 3 and 7.

Consider the prime 7. By Ribet's theorem there should exist a newform of level $132 = 4 \cdot 3 \cdot 11$ whose Fourier coefficients b_q are, up to a finite number of exceptions, congruent to a_q modulo 5. Indeed there is such a form: the newform associated to the elliptic curve 132B1:

$$Y^2 = X^3 - X^2 - 77X + 330.$$

The first few values of the b_q are listed in the table.

The discriminant of "132B1" is equal to $-2^4 3^{10} 11$. This confirms that the 5-torsion points are "finite". Applying Ribet's theorem one more time, we find that there exists a newform of level 44 whose Fourier coefficients c_q are congruent to a_q modulo 5. Indeed, the newform associated to the elliptic curve 44A1

$$Y^2 = X^3 + X^2 + 3X - 1$$

has this property.

	q	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
924A1	a_q	$-$	$+$	-3	$+$	$+$	1	-4	3	2	5	0	9	0	10	5	-6	13
132B1	b_q	$-$	$+$	2	2	$+$	6	-4	-2	-8	0	0	-6	0	10	0	14	-12
44B1	c_q	$-$	1	-3	2	$+$	-4	6	8	-3	0	5	-1	0	-10	0	-6	3

One could say that Ribet's result allows us to "lower" the level of the representation on the points of order 5: the representation was associated to a curve of conductor $44 \cdot 3 \cdot 11$, but its "proper level" turned out to be 44. Here's how this theorem together with the Taniyama-Weil conjecture implies Fermat's Last Theorem:

Let E be the Frey curve $Y^2 = X(X - a^p)(X - c^p)$ associated to a hypothetical non-trivial solution of Fermat's equation $a^p + b^p = c^p$. We may and do assume that $p \geq 5$. By the Taniyama-Weil conjecture, the curve E is modular. Let $f = \sum_n a_n e^{2\pi i n z}$ denote the associated newform of weight 2. Since E is semi-stable, f has level

$$N = \prod_{l | abc} l.$$

Since the discriminant of the Frey curve is a p-th power, the subgroup scheme $E[p]$ is finite and flat and the action of the Galois group on the points of order p is finite. Since $p \geq 5$ the results of Mazur's "Eisenstein ideal" paper [15] imply that the Galois action is also irreducible. Therefore the conditons of Ribet's theorem are satisfied. So there exists a newform $g = \sum_n b_n q^n$ of weight 2 and level N/l for which the b_n are congruent to a_n modulo some prime $\mathfrak{p}$ over p. This implies that the action of the Galois group associated to g is again finite, flat and irreducible. Now we proceed by induction: we"eliminate" all odd primes from the level and we end up with a newform of weight 2 for the group $\Gamma_0(2)$. But such a form does not exist, since the curve $X_0(2)$ is rational and the vector space of cusp forms of weight 2 has dimension 0. This contradiction shows that the solution a, b, c with $a^p + b^p = c^p$ does not exist.

6. Wiles's approach.

Since Frey's elliptic curves are semi-stable, it is actually not necessary to prove the full Taniyama-Weil conjecture in order to prove Fermat's Last Theorem. It suffices to prove the conjecture for semi-stable curves.

Wiles's's idea is to "lift" Galois representations. More precisely

Conjecture 6.1. *Suppose E is a semi-stable elliptic curve over $\mathbf{Q}$ with L-series $\sum_n a_n n^{-s}$. Let l be an odd prime satisfying the following conditions.*

(i) The group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts irreducibly on $E[l]$.

(ii) There is an eigenform $f = \sum_n b_n e^{2\pi i n z}$ and a prime iedeal $\mathfrak{l}$ over l such that for all but finitely many primes q

$$a_q \equiv b_q \pmod{\mathfrak{l}}.$$

Then E is modular, i.e. the Fourier series $\sum_n a_n e^{2\pi i n z}$ is a modular form of weight 2 for some $\Gamma_0(N)$.

In other words, if the Fourier series $\sum a_n e^{2\pi i n z}$ associated to E is congruent to a modular form modulo l, then it actually is a modular form. It suffices to assume the truth of this conjecture for the primes $l = 3$ and 5 to prove the Taniyama-Weil conjecture for semi-stable elliptic curves over $\mathbf{Q}$. Very roughly one proceeds as follows.

Let E be a semi-stable elliptic curve over $\mathbf{Q}$. Consider the prime $l = 3$ and the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $E[3]$. By considering the action of $\mathrm{PGL}_2(\mathbf{F}_3)$ on the four points of $\mathbf{P}^1(\mathbf{F}_3)$, we see that $\mathrm{PGL}_2(\mathbf{F}_3) \cong S_4$. The group S_4 is a subgroup of $\mathrm{PGL}_2(\mathbf{C})$. The extension of S_4 by $\{\pm 1\}$ contained in $\mathrm{GL}_2(\mathbf{C})$ is isomorphic to $\mathrm{GL}_2(\mathbf{F}_3)$. So, the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $E[3]$ gives rise to a representation

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{C})$$

whose image is contained in a subgroup isomorphic to $GL_2(\mathbf{F}_3)$ and whose image in $\mathrm{PGL}_2(\mathbf{C})$ is contained in a subgroup isomorphic to S_4. It follows from the work of R. Langlands [14] and J. Tunnell [23] that such a representation is modular. In

their work it is essential that S_4 is a *solvable* group. One cannot hope to obtain a similar result using any prime $l > 3$.

With some extra work [19] one can find an eigenform $f = \sum_n a_n e^{2\pi inz}$ of weight 2 for some $\Gamma_0(N)$ such that the corresponding representation is isomorphic to ρ_3 *modulo 3.*

If the action of the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $E[3]$ is irreducioble, then the conditions of Conjecture 6.1 are satisfied and we conclude that E is modular. If the action is *not* irreducible, Wiles considers $E[5]$. If $E[5]$ would also admit a reducible Galois action, then E would have a subgroup of order 15 which is respected by $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. This would give rise to a rational point on the modular curve $X_0(15)$, which parametrizes elliptic curves together with a subgroup of order 15. The genus of this curve is 1 and its rational points consist of four cusps and of four points that correspond to certain non-semi-stable curves (the curves of conductor 50 to be precise; they are modular).

Therefore the Galois action on $E[5]$ is irreducible. Using the Hilbert irreducibility theorem and the fact that the genus of the modular curve $X(5)$ is zero, Wiles constructs another semi-stable elliptic curve E' over $\mathbf{Q}$ which satisfies

$$E'[3] \text{ is irreducible;}$$
$$E'[5] \cong E[5] \quad \text{as Galois modules.}$$

Since $E'[3]$ is irreducible, E' is modular by Conjecture 6.1. Let $\sum_n b_n e^{2\pi inz}$ be the associated newform of weight 2. Then

$$a_q \equiv b_q \pmod 5 \qquad \text{for almost all primes } q.$$

But now the conditions of Conjecture 6.1 are satisfied for E with $l = 5$ rather than $l = 3$! We conclude that the representation on the Tate module T_5E is modular and hence that E is modular.

It is amusing to see how the various torsion points of the Frey curve have entered into the proof: the curve itself has been constructed by specifying its 2-torsion points, Ribet's proof exploits the structure of the subgroup scheme of p-torsion points and Wiles exploits the 3-torsion and 5-torsion points.

To prove the conjecture Wiles studies all the "liftings" of the (irreducible) representation

$$\rho_l : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{F}_l) \quad (= \mathrm{Aut}(E[l])).$$

Here a lifting of ρ_l is a representation $\rho_R : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(R)$, where R is a complete local Noetherian $\mathbf{Z}_l$-algebra with maximal ideal $\mathfrak{m}$ and residue class field $\mathbf{F}_l$, such that ρ_R "modulo" $\mathfrak{m}$ is ρ_l.

By assumption two such lifting exist: one is simply the representation on the Tate module T_lE of E:

$$\rho_{l,\infty} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_l) \quad (= \mathrm{Aut}(T_lE)).$$

and the other one is the Galois representation associated to the eigenform $f = \sum_n b_n e^{2\pi i n z}$. Both representation are rather special: there are all kinds of restrictions on the decomposition and ramification groups etc.

Mazur [16] showed that there exists a universal lifting (subject to the restrictions on the ramification ...) $\rho_{\text{univ}} : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \text{GL}_2(R_{\text{univ}})$. Here R_{univ} is a local Noetherian $\mathbf{Z}_l$-algebra. In other words, for every lifting ρ_R there is a unique homomorphsim $f : R_{\text{univ}} \longrightarrow R$ such that $f \cdot \rho_{\text{univ}} = \rho_R$.

On the other hand, there exists such a representation which is universal for the *modular* liftings of ρ_l. This ring $\mathbf{T}$ is related to the Hecke algebra. By the universal property there is a homomorphism

$$R_{\text{univ}} \longrightarrow \mathbf{T}$$

which is surjective. We must show that this map is an isomorphism. This implies that every lifting of ρ_l is modular, in particular, $\rho_{l,\infty}$ is modular as required.

The ring $\mathbf{T}$ is a Gorenstein ring and this property enables Wiles to reduce this problem to the "tangent spaces" of $\text{Spec}(R_{\text{univ}})$ and $\text{Spec}(\mathbf{T})$ at the "point" whose existence is guaranteed by the results of Langlands and Tunnell. It suffices to show that the tangent spaces are equal and this boils down to proving a formula for the cardinality of a certain "Selmer" group. This cardinality should essentially be equal to a special value of the L-series associated to the symmetric square representation of the elliptic curve E. One step in the direction of such a formula had been taken by Matthias Flach [7] in 1992. He had proved that the conjectural value at least *annihilated* the Selmer group.

Formulas expressing cardinalities of arithmetically interesting groups in terms of special values of L-series are quite common in number theory. Recently the Russian mathematician V. Kolyvagin [12] developed his powerful "Euler systems" to prove such equalities. Kolyvagin was partially inspired by the work of F. Thaine [22], who proved in 1988, a certain annihilation result for class groups of cyclotomic fields, a result somewhat similar to Flach's. A few years later Kolyvagin extended Thaine's result and obtained formulas for the cardinalities of the class groups ussing his Euler systems. In a similar way Wiles has applied Kolyvagin's method of Euler systems to extend Flach's result to obtain a formula for the cardinality of the Selmer group.

The Euler system is based on Flach's construction. The precise details have not been published.

Bibliography

[1] Birch, B. and Kuyk, W. eds.: *Modular functions in one variable IV*, Lecture Notes in Math. **476**, Springer-Verlag, New York Heidelberg Berlin 1975.

[2] Buhler, J., Crandall, R., Ernvall, R. and Metsänkylä, T.: Irregular primes and cyclotomic invariants to four million, *Math. Comp.* **61**, (1993), 151–154.

[3] Cremona, J.: *Algorithms for modular elliptic curves*, Cambridge Univ. Press, Cambridge 1992.

[4] Deligne, P.: Formes modulaires et représentations l-adiques, *Sém. Bourbaki*, Exp. 355, (1968/1969), Lect. Notes in Math. **179**, Springer-Verlag, Berlin Heidelberg New York 1969.

[5] Diophanti Alexandrini Arithmeticorum libri sex, et de numeris multangulis liber unus. Nunc primum Græcè et Latinè editi, atque absolutissimus Comentariis illustrati. Auctore Claudio Gaspare Bacheto Meziriaco Sebusiano V.C., Lutetiae Parisiorum, Sumptibus Hioronymi Drouart, via Jacobæa, Sub Scuto Solari M.DC.XXI Cum Privilegio Regis.

[6] Edwards, H.: *Fermat's last theorem, a genetic introduction to algebraic number theory*, Grad. Texts in Math. **50**, Springer-Verlag, New York 1977.

[7] Flach, M.: A finiteness theorem for the symmetric square of an elliptic curve, *Invent. Math.* **109** (1992), 307–327.

[8] Fontaine, J.-M.: Il n'y a pas de variété abélienne sur $\mathbf{Z}$, *Invent. Math.*, **81**, (1985) 515–538.

[9] Frey, G.: Links between solutions of $A-B=C$ and elliptic curves, in *Number Theory*, Ulm 1987, Proceedings, Lecture Notes in Mathematics **1380**, Springer-Verlag, Berlin Heidelberg New York 1989, 31–62.

[10] Hardy, G.H. and Wright, E.M.: *An introduction to the theory of numbers*, (4th ed.), Oxford Univ. Press, Oxford 1960.

[11] Hellegouarch, Y.: Étude des points d'ordre fini des variétés de dimension un définies sur un anneau principal, *Journal für die reine und angew. Math.* **244** (1970), 20–36.

[12] Kolyvagin, V.B.: Euler systems, in *The Grothendieck Festschrift* II, 435–483. Eds. P. Cartier et al., Birkhäuser, Boston 1990.

[13] Kummer, E.E.: *Collected Papers* (ed. by A. Weil), Springer-Verlag, New York 1975.

[14] Langlands, R.: *Base change for* GL(2), Ann. of Math. Studies **96**, Princeton University Press, Princeton NJ, 1980.

[15] Mazur, B.: Modular curves and the Eisenstein ideal, *Publ. Math. IHES*, **47** (1977), 33–186.

[16] Mazur, B.: Deforming Galois representations, in *Galois groups over* $\mathbf{Q}$ (Y. Ihara, K. Ribet and J.-P. Serre Eds.), MSRI Publ. **16**, Springer-Verlag, Berlin Heidelberg New York 1989, 385–437.

[17] Oesterlé, J.: Nouvelles approches du "théorème de Fermat, *Sém. Bourbaki* **694** (1987–1988), *Astérisque* **161/162** (1988), 165–186.

[18] Ribet, K.: On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431–476.

[19] Rubin, K. and Silverberg, A.: A report on Wiles' Cambridge lectures, *Bull. AMS (new series)* **31** (1994), 15–38.

[20] Serre, J.-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, *Duke Math. J.* **54** (1987), 179–230.

[21] Silverman, J.: *The arithmetic of elliptic curves*, Grad. Texts in Math. **106**, Springer-Verlag, Berlin Heidelberg New York 1986.

[22] Thaine, F.: On the ideal class groups of real abelian number fields, *Ann. of Math.* **128** (1988), 1–18.
[23] Tunnell, J.: Artin's conjecture for representations of octahedral type, *Bull. AMS (new series)* **5** (1981), 173–175.
[24] Washington, L.C.: *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, Berlin Heidelberg New York 1982.
[25] Weil, A.: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.* **168** (1967), 149–156.
[26] Weil, A.: *Number Theory, An approach through history*, Birkhäuser, Boston 1984.