Wydział Matematyki i Informatyki
Uniwersytetu im. Adama Mickiewicza w Poznaniu

Środowiskowe Studia Doktoranckie
z Nauk Matematycznych

Modular Forms and Galois Representations: Arithmetic, Algorithms and Applications

Gerhard Frey

Institute for Experimental Mathematics
University of Duisburg-Essen
frey@iem.uni-due.de

Publikacja współfinansowana ze środków Uni Europejskiej
w ramach Europejskiego Funduszu Społecznego

Very often Diophantine problems can be stated in an elementary way but it is notoriously hard to solve them. The most famous example for this phenomenon was Fermat's Last Theorem. The situation becomes better whenever one finds a mathematical structure behind the problem, and in many cases this structure is delivered by the action of the Galois group on geometric objects like torsion points of elliptic curves or, more generally, abelian varieties. Then the arithmetic of Galois representations plays a dominant role. A key role in this game is occupied by Jacobian varieties of modular curves. These varieties are very well understood, and connections to modular forms allow deep theoretical and practical insights. It is the aim of the lectures to explain both theoretical and algorithmic aspects in this exciting part of arithmetic geometry. An additional bonus is that many of the results can be used to construct public key crypto systems and to discuss their security.

Contents

1. Galois Representations

1.1. Definitions

Let K be a field with separable closure K_s and G_K be an absolute Galois group, i.e., $G_K := \mathrm{Aut}_K(K_s/K)$. G_K is a compact topological group with respect to the profinite topology.

Definition 1.1. *Let R be a topological ring.*

A Galois representation of dimension d is a continuous homomorphism

$$\rho\colon G_K \to Gl_d(R).$$

Equivalently: *There is a free topological R-module V with continuous G_K-action which makes V to a $R[G_K]$-module.*

Equivalent representations have isomorphic $R[G_K]$-modules as representations spaces.

Let K_ρ be the fixed field of $\ker(\rho)$. Since $\ker(\rho)$ is closed we have that K_ρ/K is Galois with $G(K_\rho/K) \cong \mathrm{im}(\rho)$.

Definition 1.2. *The representation ρ is semi simple iff the representation space V_ρ is a semi simple G_K-module.*

This is so iff the representation ρ is determined (up to equivalence) by all the characteristic polynomials of the images of elements in G_K.

1.2. Local-Global Relations

1.2.1. Localization

Let $\mathfrak{p}$ be a non-archimedean (discrete) valuation of K with extension $\tilde{\mathfrak{p}}$ to K_s.

Let $O_\mathfrak{p}$ be the valuation ring of $\mathfrak{p}$, $m_\mathfrak{p}$ its maximal ideal and $\mathbb{F}_\mathfrak{p} := O_\mathfrak{p}/m_\mathfrak{p}$ the residue field of $\mathfrak{p}$. $\tilde{\mathfrak{p}}$ induces a $\mathfrak{p}$-adic metric $d_{\tilde{\mathfrak{p}}}$ on K_s.

Let $K_\mathfrak{p}$ denote the completion of K with respect to this metric.

Definition 1.3. *The decomposition group of $\tilde{\mathfrak{p}}$ is the subgroup $G_{\tilde{\mathfrak{p}}}$ of G_K consisting of all the elements which act continuously with respect to the topology induced by $d_{\tilde{\mathfrak{p}}}$.*

By continuous extension we get a natural isomorphism from $G_{\tilde{\mathfrak{p}}}$ to $G_{K_\mathfrak{p}}$.

It follows that $G_{\tilde{\mathfrak{p}}}$ acts on the valuation ring of $\tilde{\mathfrak{p}}$ and on its maximal ideal and so in a natural way on $\mathbb{F}_{\mathfrak{p},s}$.

By this we have a surjective reduction map

$$r_{\tilde{\mathfrak{p}}}\colon G_{\tilde{\mathfrak{p}}} \to G_{\mathbb{F}_\mathfrak{p}}.$$

Definition 1.4. *The inertia group $I_{\tilde{\mathfrak{p}}}$ is the kernel of $r_{\tilde{\mathfrak{p}}}$.*

The quotient $G_{\tilde{\mathfrak{p}}}/I_{\tilde{\mathfrak{p}}}$ can be identified with $G_{\mathbb{F}_\mathfrak{p}}$.

For a given representation ρ we denote its restriction to $G_{\tilde{\mathfrak{p}}}$ by $\rho_{\tilde{\mathfrak{p}}}$ and call it the *localization* of ρ.

Definition 1.5. *ρ is unramified at $\mathfrak{p}$ iff $I_{\tilde{\mathfrak{p}}} \subset \ker(\rho)$. ρ is tamely ramified at $\mathfrak{p}$ iff $I_{\tilde{\mathfrak{p}}}/(I_{\tilde{\mathfrak{p}}} \cap \ker(\rho_{\mathfrak{p}}))$ has (profinite) order prime to $\mathrm{char}(\mathbb{F}_{\mathfrak{p}})$.*

Exercise 1.6. *Show that the definition is well-defined.*

1.2.2. The Frobenius Automorphisms

Assume that $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q$ is a finite field with q elements. $G_{\mathbb{F}_q}$ is topologically generated by the Frobenius automorphism ϕ_q mapping elements of $\mathbb{F}_{q,s}$ to their q-th power.

Choose an extension $\tilde{\mathfrak{p}}$ and so an embedding of K_s into $K_{\mathfrak{p},s}$ and of $G_{K_{\mathfrak{p}}}$ into G_K with image $G_{\mathfrak{p}}$. Identify $G_{\mathbb{F}_q}$ with the Galois group of the maximal unramified extension of $K_{\mathfrak{p}}$ in its separable closure and hence with a quotient group of $G_{\mathfrak{p}} \subset G_K$. Any element $\sigma_{\mathfrak{p}}$ of the pre-image of ϕ_q in G_K is called a Frobenius element at $\tilde{\mathfrak{p}}$. Choosing another extension of $\mathfrak{p}$ leads to a conjugate decomposition group and hence to conjugate Frobenius elements. By abuse of language we denote the conjugacy class of Frobenius elements again by $\sigma_{\mathfrak{p}}$ and call it the *Frobenius attached to* $\mathfrak{p}$.

Computational Task: *All definitions involving Frobenius elements have to be invariant under conjugation and well-defined modulo inertia groups.*

It is the interplay between the arithmetical properties of K reflected by the set of places $\mathfrak{p}$ and the group theoretical properties of G_K reflected by the set of subgroups $G_{\mathfrak{p}}$ which deeply relates Galois theory with arithmetic.

1.2.3. Artin L-series

Let K be a number field. We give a first and classical example how local information is intertwined to get a global object. Take $\rho\colon G_K \to \mathbb{C}$ with representation space V. Take a non-archimedean place $\mathfrak{p}$ (i.e. an equivalence class of non-archimedean valuations) and choose an extension $\tilde{\mathfrak{p}}$ to K_s. As above let $I_{\tilde{\mathfrak{p}}}$ be the inertia group of $\tilde{p}$. $V^{I_{\tilde{\mathfrak{p}}}}$ is a $G_{\tilde{\mathfrak{p}}}/I_{\tilde{\mathfrak{p}}}$-module and hence we have a well-defined action of Frobenius elements $\sigma_{\tilde{\mathfrak{p}}}$ attached to $\tilde{p}$. Its characteristic polynomial is independent of the choice of $\tilde{\mathfrak{p}}$ and is denoted by $\chi_{\rho(\sigma_{\tilde{p}}|V^{I_{\tilde{p}}})}(T)$. K_ρ is a finite Galois extension of K (why?). Let e_p be the ramification index of $\tilde{\mathfrak{p}}$ in K_ρ/K. It is a basic fact that $e_{\mathfrak{p}}$ is independent of the choice of $\tilde{\mathfrak{p}}$.

Definition 1.7. *The **local L-series** of ρ at p is*

$$L_{\rho,\mathfrak{p}}(s) := \chi_{\rho(\sigma_{\mathfrak{p}}|V^{I_{\tilde{p}}})}(q^{-s})^{-e_{\mathfrak{p}}} \qquad \text{with } s \in \mathbb{C}.$$

The *global* Artin L-series is the product of the local L-series multiplied by a Γ-factor which takes care of the archimedean places. It is a Dirichlet series, and the great *Conjecture of Artin* predicts that it can be continued to an analytic function on $\mathbb{C}$ with functional equation- provided that ρ is not trivial.

1.2.4. Artin Conductor

To refine this statement one has to use another local invariant for representations: the *Artin conductor*. To define it one has to use the filtration of $I_{\mathfrak{p}}$ by higher ramification groups. We assume that the image of ρ is finite, e.g. ρ is a representation over $\mathbb{C}$ or over a finite field. Let G be the Galois group of K_ρ/K. There is a filtration of G by higher

ramification groups $G_{i+1} \subset G_i$ with $G_1 = G$, $G_0 = I_{\mathfrak{p}}$. For $i > 0$ the groups G_i are p-groups with $p = \mathrm{char}(\mathbb{F}_{\mathfrak{p}})$ and give the wild ramification part.

Let $V_i = V^{G_i}$ and $d_i = \mathrm{codim}_V V_i$.

Definition 1.8. *The exponent $f_{\mathfrak{p}}$ of the conductor of ρ at $\mathfrak{p}$ is*

$$f_{\mathfrak{p}} = \sum_{i \geqslant 0} \frac{1}{[G_0 : G_i]} d_i.$$

The Artin conductor of ρ is $N'_\rho := \prod_{\mathfrak{p} \text{ place of } K} \mathfrak{p}^{f_{\mathfrak{p}}}$.

In particular, N'_ρ is a divisor of K whose support consists exactly of the places at which $\mathfrak{p}$ is ramified.

1.2.5. Local-Global Principle: Čebotarev's Density Theorem

In *Number Theory* one tries to solve problems over global fields be looking at them over (all) local fields and then reducing them modulo v to problems over finite fields. One hopes that one looses not to much information. In other words, one wants to establish *local-global principle*. Here is one of the most important principles. It concerns Galois representations which satisfy very natural conditions.

Theorem 1.9 (Čebotarev's Density Theorem)**.** *Let ρ be a Galois representation of G_K which is ramified only at finitely many places of K. If ρ is semi simple then ρ is determined by*

$$\{\chi_{\rho(\sigma_{\mathfrak{p}})}(T); \mathfrak{p} \text{ runs over the places of } K\}.$$

It is even allowed to omit arbitrary finite sets of primes.

1.3. Basic Example

Take n prime to char(K). G_K operates on torsion points $A[n]$ of order n of abelian varieties A that are defined over K. The attached Galois representation of dimension $2\dim(A)$ over $\mathbb{Z}/n$ is denoted by

$$\rho_{A,n} \colon G_K \to Gl_{2d}(\mathbb{Z}/n).$$

A generalization: Take a prime ℓ and define the ℓ-adic Tate module

$$\ell(A) := proj - limA[\ell^k]$$

on which G_K acts continuously (w.r.t. the ℓ-adic topology). The corresponding Galois representation is denoted by

$$\tilde{\rho}_{A,\ell}.$$

It is a $2d$-dimensional ℓ-adic Galois representation.

1.3.1. Arithmetical Properties

Assume that K has a discrete valuation $\mathfrak{p}$.

Theorem 1.10 (Néron, Ogg, Shafarevich)**.** *Assume that ℓ is prime to ¶. Then $\tilde{\rho}_{A,\ell}$ is unramified at $\mathfrak{p}$ iff A has good reduction at $\mathfrak{p}$.*

Hence: Let K be a number field. Then $\tilde{\rho}_{A,\ell}$ is unramified outside of a finite set of places. By geometric local properties one defines the conductor N_A of A. According to the criterion of Néron–Ogg–Shafarevich $\tilde{\rho}_{A,\ell}$ is ramified exactly in the prime divisors of the $\ell \cdot N_A$.

Remark 1.11. *For given ℓ^k the prime-to-ℓ-part of the conductor of ρ_{A,ℓ^k} clearly divides the conductor of A. But it can be much smaller (for special prime numbers ℓ).*

It is a very interesting diophantine question to find such "congruence primes".

A is semi stable iff N_A is square free. A deep theorem of *Grothendieck* states that for every A there is a finite extension L of K such that $A \times L$ is semi-stable.

As consequence we get: $\tilde{\rho}_{A,\ell}$ is potentially semi stable. (For a definition of semi stable at places dividing ℓ we refer to J.M. Fontaine: Représentations p-adiques semi-stables, pp. 113–184, in:Périodes p-adiques, Ast. 223, SMF, 1994.)

1.4. Conjecture of Fontaine–Mazur

Following *Fontaine–Mazur* we define

Definition 1.12. *An ℓ-adic Galois representation ρ_K is geometric iff it is unramified outside a finite set of places and if it is potentially semi-stable at places dividing ℓ.*

Look at the example above. We have used Tate-modules of abelian varieties to construct geometric ℓ-adic representations. We can interpret this by means of étale cohomology: $T_\ell(A)$ is the first étale cohomology group with coefficients in $\mathbb{Z}_\ell$.

The amazing prediction is that by using such cohomology groups we should get essentially *all* ℓ-adic Galois representations of *number fields.*

Conjecture 1.13 (Fontaine–Mazur)**.** *An irreducible ℓ-adic representation of G_K is geometric iff it is isomorphic to a subquotient of a Tate twist of an étale cohomology group of a smooth projective algebraic variety over K.*

To demonstrate the strength of this conjecture we give one consequence:

Conjecture 1.14. *Let $\Gamma(K,\ell)$ be the Galois group of the maximally unramified pro-ℓ--extension of K. Then any quotient of $\Gamma(K,\ell)$ which is an ℓ-adic analytic group is finite.*

2. Diophantine Applications and Conjectures

We describe how deeply Galois representations influence the arithmetic of abelian varieties.

Recall that for abelian varieties we have defined representations $\tilde{\rho}_{A,\ell}$ attached to the Galois action on Tate modules.

Theorem 2.1 (Faltings). *$\tilde{\rho}_{A,\ell}$ is semi simple.*

Consequences:

Theorem 2.2 (Isogeny Theorem of Faltings). *Two abelian varieties are isogenous (i.e. there is a surjective morphism with finite kernel between them) iff for one (and hence for all) prime(s) ℓ the attached ℓ-adic representations are equivalent over $\mathbb{Q}_\ell$.*

Theorem 2.3 (Conjecture of Shafarevich). *For a given finite set T of places of K and given d there are only finitely many abelian varieties of dimension d with good reduction outside of T.*

Corollary 2.4 (Conjecture of Mordell). *Curves of genus $\geqslant 2$ have only finitely many K-rational points.*

Unsolved computational problem: *For given curve C over $\mathbb{Q}$ determine $C(\mathbb{Q})$!*

Definition 2.5. *Define*

$$L_{A,\mathfrak{l}}(s) := (\chi_{\tilde{\rho}_{A,p}}(\sigma_\mathfrak{l})(N(\mathfrak{l})^{-s}))^{-1}$$

as local factor *at $\mathfrak{l}$ of the* L-series *of A.*

Theorem 2.6 (Effective version of Faltings' Isogeny Theorem). *For given abelian varieties A_1 and A_2 there is a number n such that A_1 is isogenous to A_2 iff the local L-series are equal for a set of primes $\mathfrak{l}_i$ with $N(\prod \mathfrak{l}_i) > n$.*

2.1. Congruent Torsion Structures

We try to make the last statement effective. Assume that for a number N we find Galois invariant subgroups $C_i \subset A_i[N]$ with C_1 Galois isomorphic to A_2. How large (depending on K, *dim* A_i, N_i) has the order of C_1 to be in order to force A_1 and A_2 to have isogenous abelian subvarieties?

Special case: A_1 and A_2 are elliptic curves.

Conjecture 2.7 (Kani). *There is a number n_0 (independent of K) such that for $n \geqslant n_0$ there are, up to twist pairs, only finitely many pairs (E, E') of elliptic curves which are not isogenous* and *with $\rho_{E,n} \cong \mathbb{R}_{E',n}$. For prime numbers n we can choose $n_0 = 23$.*

Geometric background: Description of the moduli space and Lang's conjecture for general surfaces.

There is a variant (and predecessor) of this conjecture stated by the author:

Conjecture 2.8. *We* fix *an elliptic curve E_0/K. There is a number $n_0(E_0, K)$ such that for all elliptic curves E, over K and all $n \geqslant n_0(E_0, K)$ we get:*

$$\textit{If } \rho_{E,n} \cong \rho_{E_0,n} \textit{ then } E \textit{ is isogenous to } E_0.$$

We shall discuss this conjecture later on and relate it with other arithmetic properties of elliptic curves. We remark that its analogue over function fields holds.

2.2. Point Counting

The algorithmic challenge arising from the results above is to compute the local L-series of abelian varieties.

There is another concrete motivation for doing this: since

$$|A^{\mathfrak{l}}(\mathbb{F}_{N(\mathfrak{l})})| = \chi_{\tilde{\rho}_{A,p}}(\sigma_{\mathfrak{l}})(1)$$

we can count points on abelian varieties over finite fields, and this is of importance for public key cryptography based on discrete logarithms.

The key result for all algorithms are results of A. Weil (and H. Hasse for elliptic curves).

Theorem 2.9 (Weil)**.** *Let A be an abelian variety of dimension d defined over a finite field with $q = p^s$ elements. There is a monic polynomial $\chi_A(T) \in \mathbb{Z}[T]$ of degree $2d$ with:*

- *All zeroes of $\chi_A(T)$ have (complex) value $\sqrt{q}$ ("Riemann Hypothesis").*
- *For all n the characteristic polynomial of the Frobenius automorphism ϕ_q under the representation $\rho_{A,n}$ is congruent to $\chi_A(T)$ modulo n.*
- *For all $\ell \neq p$ the characteristic polynomial of the Frobenius automorphism ϕ_q under the representation $\tilde{\rho}_{A,\ell}$ is equal to $\chi_C(T)$.*

The strategy is to compute $\chi_A(T)$ modulo relatively small number n_i and then to use the Chinese remainder theorem to determine the coefficients exactly.

2.3. Global L-series

Finally we come to one of the deepest parts of arithmetic geometry. We put the local information together and form, inspired by the density theorem and by Artin's idea, the *global* L-series of abelian varieties. For finitely many "bad primes" we use an explicit recipe to define a rational function $f^*(s)$ and we form the infinite product

$$L_A(s) := f^*(s) \cdot \prod_{\mathfrak{l} \text{ prime to } N_A} L_{A,\mathfrak{l}}(s)$$

with a complex variable s. This product is a Dirichlet series analytic in a half plane. It has to be seen as an analogue of the Riemann Zeta-function.

Conjecture 2.10 (Taniyama–Shimura–(Hasse) and Birch and Swinnerton–Dyer (BSD))**.** *$L_A(s)$ has an analytic continuation to $\mathbb{C}$, and its analytic behavior at $s = 1$ contains all interesting information about the group of K-rational points of A like its rank (order of the zero), the Tate–Shafarevich group (which describes the failure of the Hasse principle) and the Néron–Tate regulator.*

We shall give a more detailed exposition for the special case that $K = \mathbb{Q}$ and $d = 1$ and study in the following objects related to elliptic curves and/or two-dimensional Galois representations.

3. Modular Curves and Forms

We want to study 2-dimensional Galois representations of $G_{\mathbb{Q}}$ in more detail, and it turns out that the major tool for this are modular varieties.

3.1. Modular Curves

Let $\mathbb{H}$ be the complex half plane consisting of complex numbers with positive imaginary part. The classical theory of elliptic curves over $\mathbb{C}$ shows that there is a 1-1 correspondence between isomorphy classes of elliptic curves /$\mathbb{C}$ and $Y(1) := \mathbb{H}/Sl(2,\mathbb{Z})$ made explicit by the *modular function* j. Hence we can regard $Y(1)$ as affine line with j as coordinate function. The algebraic theory of elliptic curves shows that we can interpret $Y(1)$ as coarse moduli space for isomorphy classes of elliptic curves over $\mathbb{Z}$. The existence of twists prevent this moduli space to be fine.

Take $n \in \mathbb{N}$ and define

$$\Gamma(n) := \ker(Sl(2,\mathbb{Z}) \stackrel{\text{mod } n}{\longrightarrow} Sl(2,\mathbb{Z}/n)).$$

Then $Y(n) := \mathbb{H}/\Gamma(n)$ is a Galois cover of $Y(1)$ and hence again an affine algebraic curve. It has an obvious modular interpretation: It parameterizes isomorphy classes of elliptic curves together with (canonical) level-n-structures, i.e. isomorphisms of the group of points of order n with fixed determinant.

Every group Γ between $\Gamma(n)$ and $Sl(2,\mathbb{Z})$ is called a *congruence subgroup of level* n. It gives rise to an intermediate cover Y_Γ between $Y(1)$ and $Y(n)$ with Galois group $\Gamma = G(Y(n)/Y_\Gamma)$. Hence points on Y_Γ have a modular interpretation: they correspond to orbits under Γ of level-n-structures.

Example 3.1. *1.*

$$\Gamma_0(n) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in Sl(2,\mathbb{Z}); c \equiv 0 \mod n \right\}$$

gives rise to the modular curve $Y_0(n)$ which parameterizes pairs (E, C_n) where E is an elliptic curve and C_n a cyclic group of order n in $E[n]$.

2.

$$\Gamma_1(n) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in Sl(2,\mathbb{Z}); a \equiv 1 \mod n, c \equiv 0 \mod n \right\}$$

gives rise to the modular curve $Y_1(n)$ which parameterizes pairs (E, P) where E is an elliptic curve and P is a point of order n.

It is an important but not trivial remark (Igusa, Katz, Mazur, Deligne-Rapoport) that both $Y_0(n)$ and $Y_1(n)$ are defined over $\mathbb{Z}$.

$Y_0(n)$ is a coarse moduli scheme, $Y_1(n)$ is a fine moduli scheme. But in both cases rational points on the curves correspond to elliptic curves with cyclic isogeny respectively a rational point of order n.

$Y_1(n)$ is a cyclic cover of degree $\phi(n)$ of Y_0. Hence we have a splitting of meromorphic functions on $Y_1(n)$ into eigenspaces of characters of $\mathbb{Z}/n^*$. These characters are called "*nebentype*". (In fact, we have to take into account that $-id \in \Gamma_0 \setminus \Gamma_1$ if $n \neq 2$.)

3.1.1. Compactification

The modular curves Y_Γ are affine, so some points are "missing". We come to projective curves X_Γ in a natural way: We add "*cusps*" to $\mathbb{H}$ and define

$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}.$$

One sees easily that $Sl(2,\mathbb{Z})$ is acting on the cusps and so on $\mathbb{H}^*$. But now

$$X(n) = \mathbb{H}^*/Sl(2,\mathbb{Z})$$

is compact and hence a *projective curve* containing $Y(n)$. The same is true for $X_\Gamma := \mathbb{H}^*/\Gamma$ for congruence subgroups. In particular we get the projective modular curves $X_0(n)$ and $X_1(n)$. The new points are called cusps, and though they do not have a modular interpretation by elliptic curves they have a meaning: they describe degenerations!

3.2. Modular Forms

We want to study spaces of functions and differentials on $X_1(n)$. We use that $X_1(n)$ is a Galois cover of $X_0(n)$ with Galois group $(\mathbb{Z}/n)^*$ and look for eigenspaces under this action. This leads to the notion of "nebentype".

Definition 3.2. *Let χ be a Dirichlet character with conductor dividing n. Let k be a non negative integer. Let f be a function on $\mathbb{H}^*$ that is*

- *holomorphic on $\mathbb{H}$*
- *holomorphic in the cusps (and that satisfies*

for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(n)$ and $z \in \mathbb{H}$ we have

$$f\Big(\frac{az+b}{cz+d}\Big) = \chi(d)(cz+d)^k f(z).$$

Then f is a modular form *of level n, weight k with nebentype χ. If in addition f vanishes in the cusps, then f is a* cusp form.

The set of modular forms of level n, weight k and nebentype χ forms a finite dimensional $\mathbb{C}$-vector space which is denoted by $M_k(n,\chi)$. The subspace of cusp forms is denoted by $S_k(n,\chi)$.

For trivial $\chi = \chi_0$ we define $M_k(n) := M_k(n,\chi_0)$ and $S_k(n) = S_k(n,\chi)$.

3.2.1. Geometric Case

For $k \geqslant 2$ one can interpret $M_k(n,\chi)$ ($S_k(n,\chi)$) as subspace of (symmetric products) of meromorphic (holomorphic) differential forms.

Exercise 3.3. *1. Show that $S_2(n)$ is in a natural way (how concretely?) isomorphic to the space of holomorphic differentials of $X_0(n)$.*

2. Give an interpretation for $k > 2$!

It follows that the dimensions of these spaces can be easily computed by using the Hurwitz genus formula. We remark that the genus is of size $O(n)$ for $X_0(n)$ and $O(n^2)$ for $X_1(n)$. Hence the dimensions of $M_k(n,\chi)$ resp. $S_k(n,\chi)$ are of size $O(k \cdot N)$ for $k \geqslant 2$.

Example 3.4. – *$n = 2$: $X(2)$ and hence $X_1(2)$ and $X_0(2)$ have genus 0 and therefore are isomorphic to $\mathbb{P}^1$.*
– *$n = 11$: $X_0(11)$ is a elliptic curve with Weierstraß equation*

$$E: \ y^2 + y = x^3 - x^2 - 10x - 20.$$

Remark 3.5. *The situation is much more difficult, if one wants to determine the dimension of $S_1(n,\chi)$. There is no "geometrical" formula existing but one needs arithmetic of $\mathbb{Q}$ to determine it.*

3.3. Structures on $S_k(n,\chi)$

Assume that $k \geqslant 2$.

1. $S_k(n,\chi)(\mathbb{C})$ has a Hermitian structure induced by the *Petersson scalar product*.
2. $S_k(n,\chi)(\mathbb{C})$ has a rational structure since $X_0(n)$ and $X_1(n)$ are in a canonical way defined over $\mathbb{Z}$ and, because of the geometric interpretation, the spaces $S_k(n,\chi)$ and $M_k(n,\chi)$ have $\mathbb{Z}$-bases. Denote by
$$S_k(n,\chi)$$
respectively by $M_k(n,\chi)(\mathbb{Z})$ the span over $\mathbb{Z}$. Then we get for all commutative rings R with unit:
$$S_k(n,\chi)(R) = S_k(n,\chi)(\mathbb{Z}) \otimes_{\mathbb{Z}} (R).$$
3. *q-expansion principle*
   – over $\mathbb{C}$: Since the transformation
   $$z \mapsto z + 1$$
   is in $\Gamma_1(n)$ cusp forms $f(z)$ are periodic on $\mathbb{H}$ with period 1. Therefore $f(z) \in S_k(n,\chi)(\mathbb{C})$ has a Fourier expansion near infinity
   $$f(z) = \sum_{j=1}^{\infty} a_j q^j \text{ with } a_j \in \mathbb{C}$$
   with $q = e^{2\pi i z}$.
   This expansion determines f.
   – It follows rather immediately that for all fields $\mathbb{Q} \subset K$ we get
   $$S_k(n,\chi)(K) = \{f(z) = \sum_{n=1}^{\infty} a_j q^j \text{ with } a_j \in K\}.$$
   – Going a bit deeper and use (universal) Tate curves one gets for all commutative rings r with unit that elements in $S_k(n,\chi)(R)$ have a q-expansion with coefficients in R and are uniquely determined by this extension.

3.3.1. Degeneracy Morphisms

Let d be a proper divisor of n. Then $X_1(n)$ (resp. $X_0(n)$) covers $X_1(d)$ (resp.$X_0(d)$) in a natural way by a morphism φ_d. This map has a modular interpretation: One passes from pairs (elliptic curves, point of order n) to pairs (elliptic curves, point of order d), it is a forget-functor in the language of moduli spaces. Obviously φ_d induces maps on differentials and derived objects and so on modular forms. One (corresponding to the conorm) is: Take the q-expansion of a form of level d and interpret this as the q-expansion of a form of level n. We denote this map by α_d. The other possibility is: Replace the complex variable z by dz, or: in terms of q- expansions: replace q by $q^{n/d}$. Then it is easily seen that the result is the q-expansion of a modular form of level n. We denote this map by β_d.

3.3.2. Old-and New-Spaces

For fixed n, k and a Dirichlet character χ define

$$S_k(n)(\chi)(\mathbb{C})^{\text{old}} := \mathbb{C}\text{-span of } \bigcup_{\substack{d|n, d<n, \\ \chi \text{ defined modulo } d}} \{\alpha_d(S_k(d,\chi)(\mathbb{C}), \beta_d(S_k(d,\chi)(\mathbb{C})\}.$$

Definition 3.6. *The orthogonal complement of $S_k(n)(\chi)(\mathbb{C})^{old}$ with respect to the Petersson scalar product is the new-space $S_k(n)(\chi)(\mathbb{C})^{new}$.*

3.3.3. Algorithmic Property

The reason why one is able to use computers in the theory of modular forms is the following fact.

Proposition 3.7. *Assume that $f(z) = \sum a_j q^j \in M_k(n,\chi)$. With $\mu := n \cdot \prod_{p|n}(1+\frac{1}{p}) = [Sl(2,\mathbb{Z}) : \Gamma_0(n)]$ we have: If $a_j = 0$ for $0 \leqslant n \leqslant \frac{\mu \cdot k}{12}$, then $f = 0$. In other words: $f \in M_k(n,\chi)$ is determined by the Fourier coefficients $a_0, \ldots, a_{[\frac{\mu k}{12}]}$.*

Exercise 3.8. *Prove the proposition for $k = 2$.*

3.4. Endomorphisms of Modular Jacobians

3.4.1. Automorphisms of $X_0(n)$

Take n prime to $\text{char}(K)$ and (for simplicity) $d \mid n$ with $gcd(d, n/d) = 1$. For $x = (E, C_n) \in X_0(n)(K)$ let C_d be the cyclic subgroup of order d of C_n.

Definition 3.9. $w_d(x) := (E/C_d, E[d]/C_d \times C_n/C_d)$. *Applying this map to a generic point we get an* automorphism w_d *of $X_0(n)$ which is obviously an involution. Taking $d = n$ gives the* Fricke involution w_n.

Exercise 3.10. *Interpret the degeneracy map β_d in the context of involutions.*

3.4.2. Hecke Operators

One of the important features of modular curves is that a big part (in interesting cases even all) endomorphisms of their Jacobians can be constructed via natural correspondences between modular curves. For simplicity assume that $m \in \mathbb{N}$ is prime to n and $\text{char}(K)$ does not divide mn. We recall that we have the forget-morphism $\phi_m \colon X_0(mn) \to X_0(n)$.

Definition 3.11. *The m-th* Hecke operator *of level n is the correspondence*

$$\varphi_{m,*} \circ w_m \circ \varphi_m^*$$

of $X_0(m)$ and, denoted with the same letter, the endomorphisms induced on the Jacobian $J_0(n)$ of $X_0(n)$ and spaces of modular forms $M_k(n)(\chi)$ resp. cusp forms $S_k(n)(\chi)$. The Hecke algebra $\mathbb{T}_n$ (of level n) is the algebra generated by $\{T_m, w_d;\ d \mid n\}$.

Basic Properties: $\mathbb{T}_n$ is a commutative finitely generated $\mathbb{Z}$-algebra embedded into $\mathrm{End}_{\mathbb{Z}}(J_0(n)$ in a natural way. For m prime to m' we have: $T_m \circ T_{m'} = T_{mm'}$. T_m is a self-adjoint hermitian operators with respect to the Petersson scalar product.

Exercise 3.12. *If $f(z) = \sum_{j=0}^{\infty} a_j q^j \in M_k(n, \chi)$ and if p is a prime not dividing n, then*

$$T_p(f)(z) = \sum_{j=0}^{\infty} b_j q^j, \quad b_j = (a_{pj} + \chi(p)p^{k-1}a_{\frac{j}{p}})$$

with $a_{\frac{j}{p}} := 0$ if $p \nmid j$.

Definition 3.13. *$f \in M_k(n, \chi)$ is an* eigenform*, if for all primes $p \nmid n$ we have: $T_p f = \lambda_p \cdot f$ with $\lambda_p \in \mathbb{C}$ (i.e. λ_p is the eigenvalue of f with respect to T_p).*

3.5. New Forms

Definition 3.14. *$f \in S_k(n, \chi)$ is a (normed) New form, if $f = q + \sum_{j=2}^{\infty} a_j q^j$, $f \in S_k(m, \chi)^{\mathrm{new}}$ and f is an eigenform.*

3.5.1. Example: New Forms Attached to Elliptic Curves.

Let E be an elliptic curves defined over $\mathbb{Q}$ with conductor N_E.

Theorem 3.15 (Taylor, Wiles, Conrad, Breuil, Diamond)**.** *There is a non-constant morphism*

$$\varphi\colon X_0(N_E) \to E$$

be a defined over $\mathbb{Q}$.

We can assume that φ is primitive. Take a a holomorphic differential $\omega_E \neq 0$ of E. Describe E by a minimal ("best possible") Weierstraß equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

for E and define $\omega_E = \frac{dX}{2Y + a_1X + a_3}$.

Then $\varphi^*(\omega_E)$ is a holomorphic differential on $X_0(N_E)(\mathbb{Z})$ and hence

$$\varphi^*(\omega) = f(z)dz \text{ with } f_E(z) \in S_2(N_E) \text{ is a cusp form of level } N_E, \text{ weight } 2$$

and trivial nebentype character.

$$f_E(z) = \sum_{j=1}^{\infty} a_j q^j \text{ with } a_j \in \mathbb{Z},$$

the modular form attached to E, is a *new form* in $S_2(N_E)(\mathbb{Z})$. It is the key to the arithmetic of E (provided that BSD is true).

3.5.2. L-series

Theorem 3.16 (Atkin-Li)**.** – *Normalized New forms are determined by their eigenvalues (multiplicity one property).*

– *The Mellin transform of the Fourier expansion of a New form f is an* Euler product: *To $f \in S_k(n,\chi)$ define*

$$L_f(s) := \sum_{j\geqslant 1}^{\infty} a_j j^{-s}, \text{ the associated L-series.}$$

Then

$$L_f(s) = \prod_{p\in\mathbb{P}} (1 - a_p p^{-s} + \chi(p)p^{k-1-2s})^{-1}.$$

– *The L-series satisfies the* Functional equation:

$$n^{k/2}(nz)^{-k} f(-\frac{1}{nz}) = \gamma \cdot \overline{f(-\overline{z})}$$

with $\gamma \in \mathbb{C}$. If $\chi = \chi_0$, then

$$n^{k/2}(nz)^{-k} f(-\frac{1}{nz}) = w_f f$$

with $w_f \in \{1, -1\}$.

3.6. Basis

Since the Hecke operators $T_p(p\dagger n)$ commute and since they are hermitian with respect to $\langle\,,\,\rangle$ *it follows that $S_k(n,\chi)$ has a base of eigenfunctions* and that $S_k(n,\chi)^{\text{new}}$ has a base consisting of *New forms*.

Moreover the eigenvalues are totally real numbers, and for given New form f the field $K_f := \mathbb{Q}(\lambda_p)$ is a finite totally real field.

4. Modular Abelian Varieties and Galois Representations

4.1. Subvarieties of $J_0(n)$

Take a New form $f = q + \sum_{j\geqslant 2} a_j q^j$ of weight 2 and level n. $K_f = \mathbb{Q}(a_1, \ldots, a_j, \ldots)$ is a totally real field of degree d with embeddings $I_f := \{\sigma_1, \ldots, \sigma_d\}$. f induces an algebra homomorphism

$$\lambda_f \colon \mathbb{T}_n \otimes \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$$

by sending T to $a_1(T(f))$. Let $I_f := \ker(\lambda_f) \cap \mathbb{T}_n$.

Define:

$$A_f := \bigcap_{\eta\in I_f} \ker(\eta) \subset J_0(n).$$

Theorem 4.1. – *A_f is an $\mathbb{Q}$-irreducible abelian variety of dimension $[K_f : \mathbb{Q}]$.*
– *If n is square free then A_f is absolutely irreducible.*
– *A_f has good reduction outside of n.*
–

$$\Theta\colon K_f \to \mathrm{End}(A_f) \otimes \mathbb{Q}$$

given by $\Theta(a_j) = T_j \mid A_f$ gives A_f real multiplication.
– *The above construction gives a decomposition of the "New part" of $J_0(n)$ in simple varieties over $\mathbb{Q}$, and hence, by using the degeneration maps, of $J_0(n)$.*

4.2. Modular Representations

The *Eichler-Shimura Relation:* Let $p \neq \ell$ be a prime, $\mathfrak{p}$ lying over p and $\sigma_\mathfrak{p}$ the Frobenius automorphism. Then as endomorphisms of $T_\ell(A_f)$ we get the identity

$$T_p = \sigma_\mathfrak{p} + \sigma_\mathfrak{p}^t$$

where $\sigma_\mathfrak{p}^t$ is the dual of the Frobenius morphism, called "Verschiebung".

This is the fundamental relation between $\mathbb{T}_n$ and arithmetic.

Theorem 4.2 (Shimura, Deligne–Serre)**.** *Let $f = q + \sum_{j\geqslant 2} a_j q^j$ be a New form of weight k and level n , ℓ a prime number not dividing n. Then there exists a unique semi-simple ℓ-adic representation*

$$\rho_\ell\colon G_\mathbb{Q} \to GL(2, K_f \otimes \mathbb{Q}_\ell)$$

such that ρ_ℓ is unramified outside $\ell \cdot n$ and

$$tr(\rho_\ell(\sigma_\mathfrak{p})) = a_p,\ \det(\rho_\ell(\sigma_\mathfrak{p})) = p^{k-1}$$

for all p prime to ℓn.

Let $\mathbb{F}_q$ be a field with $q = \ell^r$.

Definition 4.3. *A representation*

$$\rho\colon G_\mathbb{Q} \to Gl(2, \mathbb{F}_q)$$

is modular of level n and weight k iff there is a New form f in $S_k(n)$ and a divisor $\mathfrak{l}$ of ℓ in K_f such that ρ is the reduction modulo $\mathfrak{l}$ of ρ_ℓ attached to f.

Remark 4.4. *There is an alternative description: modular representations in characteristic ℓ are related to maximal ideals $\mathfrak{m} \subset \mathbb{T}_n$ containing ℓ. Then the representation is induced by the action of $G_\mathbb{Q}$ on $\cap_{T\in\mathfrak{m}} \ker(T)$ which is a finite group scheme $\subset J_0(n)[\ell]$.*

4.3. L-series

A consequence of the Eichler–Shimura relation is

Theorem 4.5. *The L-series of A_f is equal to*

$$L_{A_f}(s) = \prod_{\sigma \in I_f} L(f^{\sigma_i}, s).$$

In particular, L-series of abelian varieties that are isogenous to products of subvarieties of $J_0(n)$ are holomorphic on $\mathbb{C}$ and satisfy a functional equation of the predicted type.

Remark 4.6. *For simplicity, we have assumed in the above discussion that the nebentype of the New forms was trivial. But all the results and definitions about representations can be generalized to the nebentype case, too. Hence we have the notion of modular representations with nebentype, too. This nebentype χ occurs in the determinant by the condition:*

$$\det(\rho(\sigma_p)) = p^{k-1}\chi(p).$$

5. Serre's Conjecture

5.1. Statement of the conjecture

Let $\mathbb{F}$ be a finite field. Let

$$\rho\colon G_{\mathbb{Q}} \to GL(2, \mathbb{F})$$

be a continuous, absolutely irreducible, twodimensional, odd representation with Artin conductor $N\rho'$. N_ρ, its prime-to-p part, is called the Serre conductor.

Following Serre (Duke J. 1987) one defines a weight k_ρ with $2 \leqslant k_\rho \leqslant p^2 - 1$ if $p \neq 2$ ($k_\rho = 2$ or 4 if $p = 2$). $k(\rho)$ is determined by an explicit recipe depending on $\rho|Ip$. For a careful definition see G. Wiese (on the web page).

Theorem 5.1 (Serre's conjecture: Khare, Wintenberger, Kisin, Taylor, et al.)**.** *Let ρ be as above. Then ρ is modular (with nebentype possibly to satisfy the determinant condition) of level N_ρ and weight k_ρ.*

Example 5.2.
- *If ρ is finite at p the weight is equal to 2. Here finiteness means that the representation space V_ρ defines a finite group scheme at p. This is so if $\mathbb{Q}(V_\rho(\overline{\mathbb{Q}}))$ is "little ramified" at p, i.e. it is obtained be a tame extension followed by radical extensions extracting roots of p-adic units.*
- *Let E be a semi stable elliptic curve over $\mathbb{Q}$ with j-invariant j_E with $Min(0, v_p(j_E))$ divisible by p. Then $\rho_{E,p}$ is modular of weight 2 with trivial nebentype and level $2^\delta \cdot \prod_{p \neq l \dagger \mathrm{Min}(0, v_l(j_E))} l$.*

5.2. Applications

5.2.1. Artin's Conjecture

Theorem 5.3. *The L-series of irreducible two-dimensional odd complex representations ρ are holomorphic.*

Computational Task: *Compute representations*!

5.2.2. Taniyama's Conjecture

From Serre's conjecture we get an immediate proof of the above-mentioned result of Taylor-Wiles and Breuil-Conrad-Diamond (that was Taniyama's conjecture): Elliptic curves E over $\mathbb{Q}$ are quotients of $J_0(N_E)$.

Computational Task: *List all elliptic curves with attached modular forms*!

5.2.3. Fermat's Last Theorem

FLT is true

6. Heights and Congruences

Part of Theorem 5.1 is that the conductor and hence the level of modular representations attached to abelian varieties can be much smaller that the conductor of ℓ-adic representation. This means that different eigenforms are congruent modulo certain primes. Hence the corresponding non-isogenous factors of $J_1(n)$ have finite subschemes which are Galois isomorphic. So we are led to questions asked in the first lecture.

Computational Task: *Find and interpret congruences explicitly (also modulo higher powers).*

6.1. The Height Conjecture for Elliptic Curves

Let E be an elliptic curve over a global field. I stated a conjecture which generalizes the conjecture of Szpiro. A coarse variant is:

Conjecture 6.1. *The size of the Faltings height $h(E)$ of E is $O(\log N_E)$.*

Now specialize and take $\varphi\colon X_0(N_E) \to E/\mathbb{Q}$ minimal.

Theorem 6.2 (Frey-Mai-Murty)**.** *The height conjecture over $\mathbb{Q}$ is true iff $\log deg(\varphi) = O(logN_E)$.*

Interpretation of $\deg\varphi$. $\varphi^*(E) = E^*$ is an elliptic subvariety of $J_0(N_E)$ which occurs with multiplicity 1. Let B_E be the kernel of φ_*. The height conjecture is true iff for all elliptic curves E

$$\log \mid E^* \cap B_E \mid = O(\log N_E).$$

Computational Task: *Compute the modular degree (which is a congruence problem for cusp forms).*

6.2. The ABC-Conjecture

The ABC-conjecture in its most general form for number fields is

Conjecture 6.3. *Let K be a number field.*

There are numbers c, d such that for all $x \in K* \setminus \{1\}$ we have

$$h(x) < c \cdot deg(|\ (x(x-1))\ |) + d.$$

The analogue of this conjecture for function fields is true.

For $K = \mathbb{Q}$ we give a more explicit conjecture:

Conjecture 6.4 (Masser-Oesterlé)**.** *For every $\epsilon > 0$ there is a $c(\epsilon)$ such that we get: for all $A \in \mathbb{N}$, B/Z prime to A and $C = A - B$ we have*

$$A \leqslant c \cdot \Big(\prod_{p \in \mathbb{P};\ p|ABC} p\Big)^{1+\epsilon}.$$

Theorem 6.5 (Frey–Mai–Murty)**.** *The ABC-conjecture over $\mathbb{Q}$ is equivalent with the degree conjecture.*

Hence many ternary diophantine problems are related to congruences of modular forms. For example the generalized Fermat Conjecture would follow as well as Conjecture 2.8 about elliptic curves with isomorphic torsion structure.

6.3. BSD

Let E be an elliptic curve over $\mathbb{Q}$. We know that its L-series $L_E(s)$ is holomorphic.

Conjecture 6.6. *Assume that $L_E(1) \neq 0$. Then the Selmer group $S_{\mathbb{Q}}(E)$ is a finite group, and hence $E(\mathbb{Q})$ and $Ш_{\mathbb{Q}}(E)$ are finite groups. Moreover*

$$L_E(1) = \int_{E^0(\mathbb{R})} \omega_E \prod_{p|N_E \cdot \infty} c_p \cdot \frac{\#S_{\mathbb{Q}}(E)}{\#(E(\mathbb{Q}))^3}$$

where $E^0(\mathbb{R})$ is the connected component of $E(\mathbb{R})$, $c_\infty = [E(\mathbb{R}) : E^0(\mathbb{R})]$, and for primes p $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$.

Computational Task: *Compute a_p fast and "verify" BSD*!

Remark 6.7. *Using modular forms of weight $3/2$ (e.g. by using modular forms of weight $1/2$ (binary quadratic forms) and cusp forms of weight 1) one can use a theorem of Waldspurger to do this fast in Twist families of certain elliptic curves.*

6.4. Boundedness of Torsion

L. Merel proved his famous theorem on the uniform boundedness of orders of torsion points on elliptic curves over number fields of degree d by using modular forms and Hecke operators. Following ideas of Kamienny and Mazur he proved that for n large enough one has a formal immersion of $X_0(n)^{(d)}$ into the Eisenstein quotient of $J_0(n)$ at $(\infty, \cdots, \infty)$.

6.5. Realize Galois Groups, Study Congruences

Modular representations can be used to realize as images certain linear groups. Hence they occur in a very controlled way as Galois groups. (Work of Dieulefait, Vila, de Reyna, Wiese,...) Take tables of New forms and study higher congruences (Taixes, Ph.D Thesis Essen 2009). etc...

7. The Basic Algorithm

It is obvious that modular forms play an important role in the arithmetic theory of Galois representations. But in addition they are accessible to computations. The background are modular symbols (Birch, Manin) and work of Merel.

In the lectures we shall present in detail an algorithm and an implemented by Basmaji (Thesis Essen).

As output we shall be able to compute Fourier expansions of a $\mathbb{Z}$-base, or alternatively, of a basis consisting of eigenforms, of $S_2(n)$. With this algorithm one is able to solve some of the computational tasks mentioned above:

— find congruences
— compute two-dimensional Galois representations with given conductor
— compute elliptic curves with given conductor
— compute curves of small genus ($\leqslant 5$) with real multiplication
— test BSD for examples
etc...

8. Literature and Background

In the lectures we shall explain all necessary notions. But it will be helpful to have a good knowledge of the basic structures in algebra and in (algebraic) number theory as well as in the basic theory of algebraic geometry, e.g. curves and their Jacobians. A good test for this is browsing through the first and the last of the references below. But we emphasize that the lectures are NOT intended for specialists in arithmetic geometry (though such people are welcome, too), and that we want to give an impression of the treated area rather than a classical mathematical course in the Landau style.

There is an extensive literature about abelian varieties, representations of profinite groups, and modular forms on nearly all levels of difficulty. We give a very short list. For elliptic curves and their arithmetic properties we recommend the two books of J. Silverman on *The Arithmetic of Elliptic Curves*.

A classical monography on modular forms is G. Shimura: *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton 1971.

Many aspects about the relations between modular representations and diophantine equations can be found by browsing through *Modular Forms and Fermat's Last Theorem*, G. Cornell, J. H. Silverman, G. Stevens edts., Springer 1997.

Computational aspects are treated in W. Stein: *Modular Forms*: *A computational Approach* (available via the web page of William Stein).

A nice treatment of all mentioned topics is given in three lecture notes by Gabor Wiese and available on his home page. In particular, one finds there many more references.

Gerhard Frey

Gerhard Frey jest matematykiem niemieckim, który jest sławny ze swoich wyników uzyskanych w teorii liczb. Krzywe Freya (to znaczy krzywe eliptyczne przyporządkowane rozwiązaniom równań Fermata) stanowią centralne narzędzie w dowodzie Wielkiego Twierdzenia Femata uzyskanego przez Andrew Wilesa w 1994 roku.

Frey studiował matematykę i fizykę na uniwersytecie w Tübingen. Doktorat z matematyki uzyskał na uniwersytecie w Heidelbergu w 1970, a habilitację trzy lata później na tym samym uniwersytecie. W latach 1969–1973 pracował jako profesor asystent w Heidelbergu, następnie (już jako profesor) w Erlangen (1973–1975), Saarbrüecken (1975–1990), oraz do 2009 na uniwersytecie w Duisburgu-Essen, gdzie kierował zorganizowanym przez siebie Instytutem Matematyki Eksperymentalnej.

Badania naukowe Gerharda Freya koncentrują się wokół zagadnień teorii liczb, geometrii arytmetycznej oraz ich zastosowań w teorii kodowania i kryptologii algebraicznej. Jest autorem ponad siedemdziesięciu prac opublikowanych, między innymi w *Canadian Bulletin of Mathematics*, *Journal für die reine Mathematik*, *Compositio Mathematicae* i *Journal of Number Theory*. Był profesorem wizytującym w *Ohio State University* w Columbus, *Harvard University*, *University of California at Berkeley*, *Mathematical Sciences Research Institute* (MSRI) w Berkeley, w *Institute for Advanced Studies* w *Hebrew University* w Jerozolimie oraz w IMPA w Rio de Janeiro.

W 1985 roku Frey odkrył związek pomiędzy Wielkim Twierdzeniem Fermata (wtedy hipotezą Fermata) i hipotezą Shimury–Taniyamy–Weila z teorii krzywych eliptycznych, co wkrótce doprowadziło do dowodu przez Kennetha Ribeta twierdzenia, które mówi, że hipoteza STW pociąga WTF. Ten związek stanowił podstawę dla Andrew Wilesa w jego dowodzie Wielkiego Twierdzenia Fermata. Za swoją pracę na temat WTF Frey uzyskał w 1996 roku medal imienia Gaussa towarzystwa *Braunschweigische Westfählische Gesellschaft*. Od 1998 roku Frey jest członkiem Akademii Nauk w Getyndze.

W 1998 roku Frey zaproponował atak na problem dyskretnego logarytmu oparty na własnościach formy dwuliniowej Weila w przypadku krzywych eliptycznych nad ciałem skończonym złożonego stopnia. Atak podany przez Freya spowodował, że wspomniane krzywe nie są już stosowane w kryptografii. Za swoje osiągnięcia w kryptografii i kryptologii krzywych eliptycznych w 2006 roku Gerhard Frey został uhonorowany nagrodą Certicom ECC Vision Award.