A short, subjective history of number theory from Fermat to the eTNC

Martin Hofer

From Fermat to Euler. It is said that P. Fermat (1607-1665) got hooked on number theory after picking up a newly published Latin translation of the ancient Greek work of Diophantus - the moment A. Weil ([Wei07, p.1]) calls the birth of modern number theory. Fermat studied questions which can be formulated very easily: Which forms can primes have? What are the integral solutions for x and y of Diophantine equations like $x^2 - Ny^2 = \pm 1$? Are there non-trivial integral solutions to the equation $x^n + y^n = z^n$ for $n \geq 3$? Regarding the latter, he claimed that he can prove that there are none. However, his contemporaries did not share his enthusiasm and it seems that nobody wanted to pick up the baton. So one had to wait until 1729 when C. Goldbach (1690-1764) wrote to his friend L. Euler (1707-1783) about Fermat's assertion that all integers of the form $2^{2^n} + 1$ are primes. This assertion, which Euler later showed to be wrong through proving that $2^{2^5} + 1$ is not a prime, lured Euler to thinking about number theoretical questions.

The Basler Problem. One of these questions Euler considered is called the *Basler Problem*: When $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$, what is the value of $\zeta(2)$?[1] In 1735 he succeeded by proving that $\zeta(2) = \frac{\pi^2}{6}$ and in another proof of this assertion he showed that there is an (Euler) product expansion for $\zeta(s)$. This means $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$, where the product ranges over all rational primes. In 1739, he even showed that

$$\zeta(2k) = (-1)^{k-1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k}, \tag{1}$$

where B_{2k} are the Bernoulli numbers and $k \geq 1$, and from that formula it is easy to obtain

$$\zeta(2k)\pi^{-2k} \in \mathbb{Q}. \tag{2}$$

We remark here that (2) is an archetypical example of a phenomenon we will concern ourselves with further below.

Magnum opus of Gauss. Euler still felt the need to justify his efforts in number theory, which led him to announce that they will be to 'the whole benefit of analysis'. But then things changed quickly for number theory, so that several decades later C.F. Gauss (1777-1855) already proclaimed that 'mathematics is the queen of science and arithmetic is the queen of mathematics'. He himself contributed a lot to this new standing of number theory. In his famous *Disquisitiones Arithmeticae* - abbreviated by D.A. - he summarised the number theory known then and included several of his own results. One of these was a proof of the quadratic reciprocity law, a vital source of motivation for Gauss for studying number theory. Among the many topics contained in this

[1] As one sees here for the first time exemplified, we will use modern notation and definitions throughout this overview which were, most of the time, not known to the mathematicians we are talking about.

monumental work we want to pick up the topic of binary quadratic forms, which is contained in Chapter 5 of D.A. There he developed a notion of when two such forms are equivalent and counted the number of equivalence classes corresponding to a fixed discriminant D, the so-called class number $h(D)$. For example, Gauss gave a list of negative discriminants with class number one and claimed that this list is complete.

A connection between two worlds. In 1837, G.L. Dirichlet (1805-1859) picked up a conjecture which Euler stated in 1783, namely that there are infinitely many primes in an arithmetic progression, i.e. for two coprime numbers a and m there are infinitely many prime numbers contained in the sequence $(a+n\cdot m)_{n\in\mathbb{N}}$. From a modern point of view the result is still interesting, but what really made head-waves were the tools Dirichlet developed because in order to prove the theorem he introduced *Dirichlet characters* and the *Dirichlet L-function.*

A question we have not asked yet is: What are the analytic properties of $\zeta(s)$ and where can it be defined? In his only number-theoretic paper [Rie60] B. Riemann (1826-1866) showed that $\zeta(s)$ has a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$ and that there is a functional equation.[2] In analogy of the ζ-function R. Dedekind (1831-1916) defined a similar function for a general number field K and showed that this function also has an Euler product expansion,

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathcal{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} (1-\mathcal{N}(\mathfrak{p})^{-s})^{-1}, \tag{3}$$

where $\mathcal{N}$ denotes the ideal norm, the sum ranges over all the non-zero integral ideals of the ring of integers $\mathcal{O}_K$ of K and the product over all the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. Dedekind also showed that this function has a simple pole at $s = 1$ and that it converges absolutely for $Re(s) > 1$. The pinnacle of Dedekind's work in this direction was that he succeeded in proving the *analytic class number formula* in the 1870's:

$$\lim_{s\to 1}(s-1)^{-1}\zeta_K(s) = h_K R_K \frac{2^{r_1}(2\pi)^{r_2}}{w_K|d_K|^{1/2}}, \tag{4}$$

where R_K is the regulator, w_K the number of roots of unity, d_K the discriminant and r_1 and r_2 the number of real and complex places of K, respectively.

Prehistory of cyclotomic fields. A classic problem going back to at least the ancient Greeks is the possibility of the construction of a regular n-polygon solely with ruler and compass. In 1796, younger than 20 by then, Gauss showed this to be possible for $n = 17$. In D.A. he even showed a sufficient condition for a general n: the odd prime factors of n are distinct Fermat primes[3]. Although this is certainly an impressive result, the methods he used had even greater impact. Gauss considered in Chapter 7 of D.A. what we nowadays would denote by $\mathbb{Q}(\zeta_n)$, where ζ_n is a root of the equation $x^n - 1 = 0$, and call a cyclotomic field. He also showed that every quadratic number field lies in such a cyclotomic field and also remarked that the cyclotomic theory should have an analogue using the lemniscate and other transcendental functions.

Influx of analysis. Going beyond the results of Gauss, L. Kronecker (1823-1891) claimed in 1853 that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field, an assertion nowadays called *Theorem of Kronecker-Weber.* Over the next years Kronecker obtained some results connecting complex multiplication of elliptic functions with abelian extensions of imaginary

[2] A side note in the paper was that the zeroes of this ζ-function should be at negative even integers and complex numbers that have real part 1/2.

[3] i.e. primes of the form $2^{2^m}+1$

quadratic number fields. This culminated in a letter to Dedekind in 1880 where he admitted that it is his 'liebster Jugendtraum' to prove that all abelian equations with coefficients in imaginary quadratic number fields are exhausted by those which come from the theory of elliptic functions.

And there was hope for such a project because on the analytic side of the problem were also major developments happening. Going back to 1847, G. Eisenstein (1823-1852) proved several properties of the Δ-, ϕ- and j-functions and started what we today would call the theory of Eisenstein series. In 1862, K. Weierstrass (1815-1897) defined his $\wp$-, ζ- and σ-functions and expressed the $\wp$-function in terms of Eisenstein series. In 1877, Dedekind introduced his η-function and proved a transformation formula for it. Also in an article about elliptic functions, Kronecker discovered a limit formula: For $\tau = x + y \cdot i$ with $y > 0$ and $s \in \mathbb{C}$ we have[4]

$$\sum_{(m,n)\neq(0,0)\in\mathbb{Z}^2} \frac{y^s}{|m\tau+n|^{2s}} = \frac{\pi}{s-1} + 2\pi(\gamma - \log(2) - \log(\sqrt{y}|\eta(\tau)|^2)) + O(s-1), \qquad (5)$$

where γ is the Euler constant and $\eta(\tau)$ is the value of the Dedekind eta function. This formula is called *Kronecker's first limit formula.*

Hilbert's summary and predictions. In 1896, D. Hilbert (1862-1943) carefully studied the known instances of algebraic number theory and wrote an exposition of almost all known results of number theory in his own formulation. This exposition is known as 'Zahlbericht'. In this work, led by analogies to Riemann surfaces, he conjectured that for any number field K there is a unique extension L over K such that the Galois group of L/K is isomorphic to the class group of K, L/K is unramified at all places, every abelian extension of K with this property is a subfield of L, for any prime $\mathfrak{p}$ of K, the residue field degree at $\mathfrak{p}$ is the order of $[\mathfrak{p}]$ in the class group of K and every ideal of K is principal in L. A number field satisfying these properties is now called a *Hilbert class field*.

Another consolidating effort of Hilbert was his list of 23 problems presented at the occasion of the International Congress of Mathematicians in 1900. His 12th problem is concerned with the explicit construction of an abelian extension of a number field, citing the model cases of $\mathbb{Q}$ and imaginary quadratic number fields, but only one of these cases was proven at the time he stated this problem.

Then the last two developments got entangled because after studying Hilbert's 'Zahlbericht' T. Takagi (1875-1960) decided that he wanted to do algebraic number theory. He started working on 'Kronecker's Jugendtraum' and accomplished some partial results in 1903 essentially solving the case $\mathbb{Q}(i)$. In this direction R. Fueter (1880-1950) in [Fue14] proved 'Kronecker's Jugendtraum' for abelian extensions of imaginary quadratic number fields of odd degree. Closely connected to these results is a result of Fueter from 1910 in [Fue10], where he uses methods of Dedekind and limit formulas like Kronecker's in (5) to obtain class number formulas for abelian extensions of imaginary quadratic number fields.

Takagi revolutionizes class field theory. Takagi also started thinking about generalizing the properties of Hilbert class fields and even dared to contemplate that maybe every abelian extension is a class field, which was originally only considered for imaginary quadratic base fields. In giving a new definition of a class field using norms of ideals instead of splitting laws and also incorporating infinite places into the modulus he was able to show this vast generalization of the known ideas by then. Indeed, the main results of his work published in [Tak20] were his *Existence Theorem* (which asserts that for an ideal group H there is a class field over K), the *Isomorphism*

[4] at first for $Re(s) > 1$ and then analytically continued to $\mathbb{C}$

Theorem (which says that if H is an ideal group with modulus $\mathfrak{m}$ and class field L, and $I_K(\mathfrak{m})$ the group of all ideals coprime to $\mathfrak{m}$ then there is an isomorphism $\mathrm{Gal}(L/K) \cong I_K(\mathfrak{m})/H$) and the *Completeness Theorem* (which says that any finite abelian extension of K is a class field). As if this had not been enough, Takagi fulfilled 'Kronecker's Jugendtraum' in this momentous work as well. This was obviously a big breakthrough but not yet utterly satisfying. Takagi had proved the Isomorphism Theorem by reducing the problem to the cyclic case and using the fact that two cyclic groups of equal order are isomorphic, so there was no explicit isomorphism given.

Artin L-function. At about the same time E. Hecke (1887-1947) in [Hec17] showed that the Dedekind ζ-function for a number field K has a meromorphic continuation to $\mathbb{C}$, satisfies a functional equation and has a simple pole at $s = 1$. So for an extension L/K the quotient ζ_L/ζ_K is meromorphic on $\mathbb{C}$. If the extension is abelian, one already knew that this quotient is even an entire function, because it was possible to express it in terms of Weber[5] L-functions of non-trivial characters. But E. Artin (1898-1962) wanted to know if the same thing was true for non-abelian extensions. On his path to discover L-functions of not necessarily abelian representations of Galois groups he made a definition which was also helpful in the abelian case. In [Art24] he defined an L-function for a finite abelian extension L/K with Galois group G: For $\chi \in \widehat{G}$ and $Re(s) > 1$, define $L(s, \chi) = \prod_{\mathfrak{p}}(1 - \chi(Fr_{\mathfrak{p}})\mathcal{N}(\mathfrak{p})^{-s})^{-1}$, where $Fr_{\mathfrak{p}}$ is the Frobenius element and the product ranges over all prime ideals $\mathfrak{p}$ of K which are unramified in L. But now one has two L-functions, from Weber and Artin, which are defined on characters of isomorphic groups, so it is natural to ask for an explicit isomorphism which identifies possibly these L-functions. The first thing that comes to one's mind is the map $\mathfrak{p} \mapsto Fr_{\mathfrak{p}}$. For this map, extended multiplicatively, Artin in [Art27] was able to show that it gives an explicit isomorphism in the Isomorphism Theorem. This theorem is called *Artin reciprocity law* because it also subsumes all the classical reciprocity laws.

In [Art30], Artin gave a definition of a more general L-function: Let L/K be a Galois extension of number fields with Galois group G and let (ρ, V) be a representation of G. Then we set

$$L_{L/K}(\rho, s) = \prod_{\mathfrak{p}}(\det(1 - Fr_{\mathfrak{P}}\mathcal{N}(\mathfrak{p})^{-s}; V^{I_{\mathfrak{P}}}))^{-1}, \tag{6}$$

where the product ranges over all prime ideals of K, $\mathfrak{P}$ is a prime ideal of L above $\mathfrak{p}$, $Fr_{\mathfrak{P}}$ the corresponding Frobenius element and $I_{\mathfrak{P}}$ the inertia group.[6] Nowadays we call this an *Artin L-function*.

On the shoulders of Hensel and Kummer. In the mathematical world of Dedekind and Hilbert number theory had been the study of algebraic number fields and Hilbert's 'Zahlbericht' was a manifestation thereof. The ideas of E. Kummer (1810-1893) and Kronecker were somehow eclipsed by the glory and success of the Dedekind-Hilbert approach to number theory. Though there remained results and methods of Kummer that were not well-embedded in the existing theories, as for example his famous *Kummer's Congruence*: For p prime and $l, k \in 2\mathbb{Z}_+$ with $(p-1) \nmid l$ or $(p-1) \nmid k$ we have

$$B_l/l \equiv B_k/k \bmod p \quad \text{if } l \equiv k \bmod (p-1), \tag{7}$$

where B_i are again Bernoulli numbers. Or also the fact that a prime p is irregular, i.e. p does not divide $h(\mathbb{Q}(\zeta_p))$, if and only if p divides one of the numerators of $\zeta(-1), \ldots, \zeta(4-p)$. Even

[5] H. Weber (1842-1913)

[6] One can show that this is well-defined and it only depends on the character.

more generally, one can define generalized Bernoulli numbers B_χ^m and show that they occur as values of Dirichlet L-functions $L(s,\chi)$ at odd negative integers:

$$L(1-m,\chi) = -\frac{B_\chi^m}{m}. \tag{8}$$

For any prime p the generalized Bernoulli numbers satisfy certain p-adic congruences which are called *generalized Kummer congruences.* T. Kubota and H.-W. Leopoldt (1927-2011) in [KL64] observed that those congruences can be interpreted in such a way that the $\frac{B_\chi^m}{m}$ are in a sense p-adically continuous functions on m. More precisely: There is one and only one p-adically continuous function $L_p(s,\chi)$ defined on $\mathbb{Z}_p$ such that (for χ even and $p>2$):

$$L_p(1-m,\chi) = -\frac{B_\chi^m}{m}(1-\chi(p)p^{m-1}), \tag{9}$$

for negative integers $1-m$ with $(p-1)\mid m$. These numbers $1-m$ are dense in $\mathbb{Z}_p$. But it turns out that $L_p(s,\chi)$ is holomorphic in a region larger than $\mathbb{Z}_p$, at least if $\chi\neq 1$, whereas for $\chi=1$ there is one pole for $s=1$. Based on these p-adic L-functions Leopoldt considered for any abelian number field K the corresponding p-adic zeta function $\zeta_{K,p}(s)$ as a product of $L_p(s,\chi)$ over all characters. He arrived at the p-adic class number formula which is an analogue of the analytic class number formula given in (4).

One related problem is also to prove the non-vanishing of the *p-adic regulator* of a number field K which appears in the p-adic class number formula. This regulator $R_{K,p}$ is obtained if one replaces the ordinary logarithms in the classical regulator with p-adic logarithms. The non-vanishing of $R_{K,p}$ means that the p-adic rank of the topological closure of the image under a suitable diagonal embedding of the group of units of K equals the ordinary rank - this is now known as *Leopoldt's conjecture.* In [Bru67], A. Brumer with the help of a reduction of J. Ax (1937-2006) in [Ax65] proved Leopoldt's conjecture for arbitrary abelian extensions of $\mathbb{Q}$ or an imaginary quadratic base field.

Iwasawa's growth formula. One of the first number-theoretic results of K. Iwasawa (1917-1998) is concerned with the growth of certain class numbers in [Iwa59a]. Indeed, let F be a finite extension of $\mathbb{Q}$ and fix, from now on, for simplicity an odd prime p. Then a $\mathbb{Z}_p$-extension is a Galois extension F_∞ of F such that $\Gamma := \mathrm{Gal}(F_\infty/F)\cong\mathbb{Z}_p$. Furthermore, we set $\Gamma_n := \Gamma^{p^n}$ as well as $F_n := F_\infty^{\Gamma_n}$ and we easily see that F_n/F is a cyclic extension. Let now e_n be the largest natural number such that $p^{e_n}\mid h_{F_n}$, where h_{F_n} is the class number of F_n. Then Iwasawa proved the existence of λ,μ,ν for sufficiently large n such that $e_n=\lambda n+\mu p^n+\nu$. The main tool in the proof is the usage of the compact $\mathbb{Z}_p$-module $X=\mathrm{Gal}(L_\infty/F_\infty)$, where L_n is the p-Hilbert class field of F_n, i.e. the maximal abelian p-extension unramified at all primes, and $L_\infty := \bigcup_n L_n$. In 1959, J. P. Serre realised that one can view X as a module over the ring $\Lambda=\mathbb{Z}_p[[T]]$ and then derived the Iwasawa growth formula from the structure theorem for Λ-modules. The latter asserts that for a finitely-generated torsion Λ-module M there is a homomorphism $M\to\bigoplus_{i=1}^t\Lambda/(f_i(T)^{a_i})$, where $f_i(T)$ are irreducible elements of Λ, with finite kernel and cokernel[7]. Then we can define the following invariants of M:

$$f_M(T)=\prod_{i=1}^t f_i(T)^{a_i},\qquad \lambda(M)=\deg(f_M(T)),\qquad \mu(M)=\max\{m\in\mathbb{N}_0 : p^m\mid f_M(T)\}, \tag{10}$$

where $f_M(T)$ is called *characteristic polynomial.* Now we have $\lambda(X)=\lambda$ and $\mu(X)=\mu$, where λ and μ are the same as in the growth formula above.

[7]The value of t, $f_i(T)$ and a_i are uniquely determined by M, up to the order. Moreover, $f_i(T)$ can be chosen as a polynomial.

Herbrand's Theorem. Until now we have only encountered the cardinality of the class group, but also the structure is interesting. J. Herbrand (1908-1931) proved in [Her32] that for $\mathbb{Q}(\zeta_p)$, $2 \le i, j \le p-2$, $i+j \equiv 1 \bmod (p-1)$ and i odd, we have that if $A^{\omega^i} \ne 0$, then $p \mid B_j$, where A is the p-primary subgroup of $Cl(\mathbb{Q}(\zeta_p))$, B_j are the Bernoulli numbers and ω is defined below.

The Iwasawa Main Conjecture for cyclotomic fields. [8] In [Iwa59b], Iwasawa continued by studying the extension $F_\infty := \mathbb{Q}(\zeta_{p^\infty})$. He defined M_∞ as the maximal abelian extension of F_∞ which is pro-p and such that only the primes lying over p are ramified, and set $Y := \mathrm{Gal}(M_\infty/F_\infty)$. Now Galois theory gives a natural decomposition $\mathrm{Gal}(F_\infty/\mathbb{Q}) = \Delta \times \Gamma$ and we can define the Teichmüller character as $\omega : \Delta \to \mu_{p-1} \subset \mathbb{Z}_p^\times$ given by the action of Δ on μ_{p^∞}. Moreover, for any $\mathbb{Z}_p$-module N on which Δ acts we get a decomposition

$$N = \bigoplus_{k=0}^{p-2} N^{\omega^k} \quad \text{with } N^{\omega^k} := \{a \in N : \delta(a) = \omega^k(\delta)a \ \forall \delta \in \Delta\}. \tag{11}$$

Iwasawa showed that X^{ω^i} for odd i has no non-zero finite Λ-submodules and that for all k, Y^{ω^k} has no non-zero, finite Λ-submodules.

Let now $\mathbb{Q}_\infty$ be the unique subfield of $\mathbb{Q}(\zeta_{p^\infty})$ such that $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. Then for any number field F the extension $F_\infty := F \cdot \mathbb{Q}_\infty$ over F is called *cyclotomic $\mathbb{Z}_p$-extension*. Iwasawa conjectured that for such extensions the μ-invariant is always zero[9]. This general conjecture is still open, but B. Ferrero and L. Washington in [FW79] proved it for $F/\mathbb{Q}$ being an abelian extension and later W. Sinnott in [Sin84] found another proof of this result by different methods.

In [Iwa64], Iwasawa went on to study the structure of class groups of $F_n := \mathbb{Q}(\zeta_{p^n})$. He defined

$$\theta_n^{(i)} = \frac{-1}{p^{n+1}} \sum_{a=1}^{p^{n+1}} a\omega^{-i}(a) \langle \sigma_a \rangle^{-1} \quad \text{and} \quad \theta^{(i)} := \varprojlim_n \theta_n^{(i)} \in \Lambda = \mathbb{Z}_p[[\Gamma]], \tag{12}$$

where $\sigma_a \in \mathrm{Gal}(F_n/\mathbb{Q})$ is determined by $\sigma_a(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^a$, $\langle \sigma_a \rangle$ is the projection to $\mathrm{Gal}(F_n/F)$ in the decomposition $\mathrm{Gal}(F_n/\mathbb{Q}) = \Delta \times \mathrm{Gal}(F_n/F)$ and $\omega^{-i}(a)$ is determined by the projection of σ_a to Δ, regarding ω^{-i} as character of that group. It follows from Stickelberger's theorem that $\theta_n^{(i)}$ annihilates $A_n^{\omega^i}$. Iwasawa proved, under a *cyclicity hypothesis*, that for i odd and $3 \le i \le p-2$, we have

$$X^{\omega^i} \cong \Lambda/(\theta^{(i)}) \text{ as } \Lambda\text{-modules.} \tag{13}$$

For the proof we identify Λ with $\mathbb{Z}_p[[T]]$ and therefore $\theta^{(i)}$ with a power series $g_i(T)$. Moreover, we set $f_i(T) := f_{X^{\omega^i}}(T)$. As $\theta^{(i)}$ annihilates X^{ω^i}, we have $g_i(T) \in (f_i(T))$. Now it remains to show that $f_i(T)/g_i(T) \in \Lambda^\times$, which Iwasawa did under the above-mentioned cyclicity hypothesis. With the help of some computations with Iwasawa invariants one can reduce proving $(f_i(T)) = (g_i(T))$ to show that $g_i(T) \mid f_i(T)$ even without the cyclicity hypothesis, which Iwasawa did in Chapter 7 in [Iwa72].

Let κ be the restriction of the cyclotomic character to Γ and define for $s \in \mathbb{Z}_p$ a continuous homomorphism κ^s by $\kappa(\gamma)^s$ for $\gamma \in \Gamma$ and then extend it to a continuous $\mathbb{Z}_p$-algebra homomorphism $\varphi_s : \Lambda \to \mathbb{Z}_p$. Then Iwasawa proved in [Iwa69] that for j even with $2 \le j \le p-3$ we have $L_p(s, \omega^j) = \varphi_s(\theta^{(i)})$ for all $s \in \mathbb{Z}_p$. Or, equivalently, $g_i(T)$ satisfies the following interpolation property:

$$g_i(\kappa(\gamma_0)^{1-m} - 1) = -(1 - p^{m-1})\frac{1}{m} B_m \tag{14}$$

[8] This section is based on [Gre01] and we again assume that p is an odd prime.
[9] Meaning X corresponding to F_∞/F has μ-invariant zero.

for all $m \geq 1$ such that $m \equiv j \bmod (p-1)$, where γ_0 is a generator of Γ. We see that the interpolation property determines $g_i(T)$ uniquely. Now we can state a version of the *Iwasawa Main Conjecture*, abbreviated by IMC, for cyclotomic fields: For each i odd, $3 \leq i \leq p-3$ we have

$$(f_i(T)) = (g_i(T)) \text{ as ideals of } \Lambda. \tag{15}$$

Let $\dot{g}_i(T) := g_i(\kappa(\gamma_0)(1+T)^{-1} - 1)$, U_n denote the group of units in the completion $(F_n)_{\mathfrak{p}_n}$, where $\mathfrak{p}_n$ is the unique prime of F_n above p, and $\overline{E}_n$ resp. $\overline{C}_n$ the closure of the units E_n resp. cyclotomic units[10] C_n of F_n in U_n. Then we can set $\mathcal{X} := \varprojlim \overline{E}_n/\overline{C}_n$, $\mathcal{Y} := \varprojlim U_n/\overline{C}_n$ and $\mathcal{Z} := \varprojlim U_n/\overline{E}_n$ and Iwasawa showed that there is an exact sequence

$$0 \to \mathcal{X}^{\omega^j} \to \mathcal{Y}^{\omega^j} \to \mathcal{Z}^{\omega^j} \to 0 \tag{16}$$

of finitely generated torsion Λ-modules and that for even j, $2 \leq j \leq p-3$, there is an Λ-isomorphism

$$\mathcal{Y}^{\omega^j} \cong \Lambda/(\dot{g}_i(T)), \text{ where } i+j \equiv 1 \bmod (p-1). \tag{17}$$

One can give another formulation of the IMC, namely that for even j, $2 \leq j \leq p-3$, the characteristic ideals of X^{ω^j} and $\mathcal{X}^{\omega^j}$ are equal.

Going beyond Iwasawa. The Iwasawa Main Conjecture can also be stated in a more general setting where F is a finite abelian extension of $\mathbb{Q}$ or a totally real field and $F_\infty = F\mathbb{Q}_\infty$. The necessary p-adic L-functions were constructed by P. Deligne and K. Ribet in [DR80] using Hilbert modular forms and by D. Barsky in [Bar78] and P. Cassou-Noguès in [CN79] using explicit formulas of T. Shintani (1943-1980).

In 1976 [Rib76], Ribet proved the converse of Herbrand's theorem mentioned above, namely that for $2 \leq i, j \leq p-2$, i odd and $i+j \equiv 1 \bmod (p-1)$ it holds: If $p \mid B_j$ then $\mathrm{Gal}(L_0/F_0)^{\omega^i} \neq 0$. Building on ideas of the proof of Ribet the IMC for cyclotomic fields was proven by B. Mazur and A. Wiles in [MW84] and the IMC for totally real base fields was proved by Wiles in [Wil90] using the theory of modular forms.[11]

Elliptic curves and the conjecture of Birch and Swinnerton-Dyer. There is a point of view of number-theoretic problems we have not mentioned yet: the geometric perspective. We will mainly focus on elliptic curves here, which are implicitly already contained in the work of Diophantus.

A modern definition of an elliptic curve over a number field K would read: E is a projective curve of genus 1 with a specific base point on the curve. We denote by $E(K)$ the set of points over K. It turns out that this is an abelian group and H. Poincaré (1854-1912) in [Poi01] defined the rank of $E(K)$ as the minimal number of generators of $E(\mathbb{Q})$, which was not known to be finite at that time. This was only shown 20 years later in [Mor22] by L. Mordell (1888-1972) and then extended and simplified by Weil: For an elliptic curve E over K, $E(K)$ is a finitely generated abelian group, i.e. $E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}$, where $E(K)_{tors}$ is a finite abelian group.[12] So we have a well-defined rank r of E.

Let Δ be the discriminant of the elliptic curve and define the integer a_p by the equation $|E(\mathbb{F}_p)| = p + 1 - a_p$, where $E(\mathbb{F}_p)$ is the number of solutions of the defining equation of E in $\mathbb{F}_p$

[10]For $n \not\equiv 2 \bmod 4$ let $V_{\mathbb{Q}(\zeta_n)}$ be the multiplicative group generated by $\{\pm\zeta_n, 1-\zeta_n^a : 1 \leq a \leq n-1\}$, then the cyclotomic units of $\mathbb{Q}(\zeta_n)$ are $C_{\mathbb{Q}(\zeta_n)} := V_{\mathbb{Q}(\zeta_n)} \cap \mathcal{O}^\times_{\mathbb{Q}(\zeta_n)}$.

[11]The approach uses 2-dimensional p-adic representations associated to Hilbert modular forms.

[12]Weil extended this result also to abelian varieties.

plus the origin. Then we can define an incomplete Hasse-Weil L-function for an elliptic curve $E/\mathbb{Q}$ by setting

$$L(E,s) := \prod_{p \nmid 2\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}, \tag{18}$$

where the product converges for the real part at least 3/2. H. Hasse (1898-1979) conjectured that as a complex function in s it has a holomorphic continuation to $\mathbb{C}$. This was only shown as a consequence of the modularity theorem proved by C. Breuil, B. Conrad, F. Diamond and R. Taylor in [BCDT01].[13] Now the conjecture of B. Birch and P. Swinnerton-Dyer (BSD conjecture)[14] based on [BSD63] and [BSD65] predicts that the Taylor expansion of $L(E,s)$ at $s=1$ has the form

$$L(E,s) = c(s-1)^r + \text{ higher order terms, with } c \neq 0 \text{ and } r = \operatorname{rank}(E(\mathbb{Q})), \tag{19}$$

which can be shortly stated as $\operatorname{ord}_{s=1}(L(E,s)) = \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. Now we can compare this to the Dedekind ζ-function, where we have $\operatorname{ord}_{s=0}(\zeta_K(s)) = \operatorname{rank}_{\mathbb{Z}}(\mathcal{O}_K^\times)$. In [Tat68], J. Tate stated the rank-BSD conjecture in the more general setting of abelian varieties over a number field K, where it says that the rank of the group of K-rational points of an abelian variety A is the order of the zero of an incomplete L-function at $s=1$. This statement uses a generalization of the Hasse-Weil L-function given by Serre [Ser65] or A. Grothendieck (1928-2014), where each of them defines an L-function for arithmetic schemes[15]. We want to focus on the special case of an elliptic curve over $\mathbb{Q}$ on a more refined conjecture given also in [Tat68].

In order to do that, one has to define Euler product factors for so-called *bad primes*, which are those dividing 2Δ. Although we skip a description of them here, we assume that from now on $L(E,s)$ is a *complete* Hasse-Weil L-function over $E/\mathbb{Q}$. As we have seen above, Dedekind was not only able to compute the order of the zero at $s=0$, but also gave a description of the leading term of the Taylor expansion at $s=1$ in terms of arithmetic invariants (cf. Equation (4)). Now in our special case, Tate's conjecture mentioned above, which can be seen as a refinement of the BSD conjecture, predicts that the leading term $L^*(E,1)$ of the complete Hasse-Weil L-function $E/\mathbb{Q}$ is:

$$L^*(E,1) = \frac{\Omega_E \cdot R_E \cdot \#(\text{Ш}(E/\mathbb{Q})) \cdot \prod_{p|\Delta} c_{E,p}}{\#(E(\mathbb{Q})_{tors})^2} \tag{20}$$

where Ω_E is the period $\Omega = \int_{E(\mathbb{R})} \frac{dx}{|2y+a_1+a_3|} \in \mathbb{R}$ for the normal form[16] of E, $c_{E,p}$ are small positive integers that measure the reduction of E at p, the regulator R_E measures the complexity of a minimal set of generators of $E(\mathbb{Q})$, and $\text{Ш}(E/\mathbb{Q})$ measures the failure of the Hasse principle. In order to have a well-defined conjecture one has to assume that $\text{Ш}(E/\mathbb{Q})$ is a finite group.

We also want to define an important class of elliptic curves: For an elliptic curve over $\mathbb{C}$ the endomorphism ring $\operatorname{End}(E)$ can now either be isomorphic to $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic number field k. If $\operatorname{End}(E) \cong \mathcal{O}$, we say that E has *complex multiplication*.

Why imaginary quadratic number fields? It is not hard to understand why 19th century mathematicians like Gauss, Kummer and Kronecker were drawn especially to the theory of cyclotomic fields. The beauty and simplicity of the results those mathematicians could obtain for cyclotomic fields is today as mesmerizing as it was then. But the theory served also as a

[13] For an important class of elliptic curves, the elliptic curves with complex multiplication, which we will discuss below, this was already known beforehand.

[14] This is sometimes also called rank part of the BSD conjecture or weak BSD conjecture.

[15] a scheme of finite type over $\mathbb{Z}$

[16] i.e. $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

blueprint of what could be true in other situations. We have already mentioned that Gauss foresaw the theory of complex multiplication by extrapolating from what he knew about the cyclotomic theory and 'Kronecker's Jugendtraum' also falls in this category. These two instances are evidence for the notion that looking at abelian extensions of imaginary quadratic number fields is the obvious next thing to do after proving a result for cyclotomic fields. But one might ask why. The most compelling reason is simply that it often works as we will see again below.

Elliptic units. So we want to look at another success story of this principle. There is the classical result (e.g. Theorem 4.9 in [Was97]) that for an even non-trivial Dirichlet character χ with conductor f we have

$$L(1,\chi) = \frac{-\tau(\chi)}{f} \sum_{a=1}^{f} \overline{\chi}(a) \log |1 - \zeta_f^a|, \tag{21}$$

where $\tau(\chi)$ is a Gauss sum. What is the corresponding result in the case of abelian extensions of imaginary quadratic number fields? After preliminary results of Fueter in [Fue10], a complete answer was given by C. Meyer (1919-2011) in [Mey57], as he succeeded in expressing $L(1,\chi)$ for primitive ray/ring class characters.[17] The main ingredient in the computations are the Kronecker limit formulas, of which one instance is already mentioned in (5).

Probably a better known reference for these results are the lecture notes of C.L. Siegel (1869-1981) ([Sie65]), where he wanted to introduce the students to 'some of the important and beautiful ideas which were developed by L. Kronecker and E. Hecke'. They contain an explicit description of the value of $L(1,\chi)$ in the imaginary quadratic case as well as many other results, e.g. for abelian extensions of real quadratic fields, where Hecke did some pioneering work. Based on the content of these lectures K. Ramachandra (1933-2011) in [Ram64] constructed what is now called *Ramachandra invariants*, which he used to express also the value of $L(1,\chi)$ using again Kronecker's limit formulas as main input in the proof. He did even more: he showed that his invariants are algebraic, described when they are units and determined their Galois action. He also used them to construct a subgroup of the global unit group of a class field with finite index which he could give explicitly in terms of the class numbers of the class field and the base field and some other arithmetic invariants.

In [Rob73], G. Robert picked up the topic again and constructed, with the same classical modular functions, the invariants for each element of the ray class group $Cl(\mathfrak{f})$, which he called *elliptic units*. He showed their relation to the Ramachandra invariants and that they satisfy similar properties. With these units he also constructed a subgroup of finite index of $\mathcal{O}_{k(\mathfrak{f})}^{\times}$ and computed this index.

BSD conjecture and elliptic units. Although these are certainly interesting results on their own, they seem to help solving only a very particular problem. This changed when J. Coates and Wiles in [CW77] established a link between the BSD conjecture and elliptic units as defined by Robert. They showed that if an elliptic curve E/F has complex multiplication by $\mathcal{O}_k$, where k is imaginary quadratic with class number one, we have: $E(F)$ is infinite implies that $L(E/F,1) = 0$ if $F = \mathbb{Q}$ or $F = k$. The problem can be reduced to showing that a certain number $L^*(1)$ (treated as an 'elliptic Bernoulli number') is divisible by infinitely many prime ideals $\mathfrak{p}$ of k. In order to do that they showed that $L^*(1)$ is divisible by a prime of degree 1 if and only if $\mathfrak{p}$ is irregular in an appropriate sense. This notion of irregularity arises from local properties of the elliptic units of Robert.

[17] Meyer also obtained similar results for abelian extensions of real quadratic number fields in [Mey57].

In giving analogues of theorems of Iwasawa theory in cyclotomic fields elliptic units are also recognized as being useful. In [CW78], Coates and Wiles gave an elliptic analogue of a result of Iwasawa which described the quotient of local units modulo cyclotomic units in terms of p-adic L-functions (cf. (17)): Let k be an imaginary quadratic number field with class number one, and E an elliptic curve over k with CM by $\mathcal{O}_k$, ψ a Größencharacter of E over k, $p\mathcal{O}_k = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p} \neq \overline{\mathfrak{p}}$ and p is not anomalous for E and not in a certain set S. Then for $(p-1) \nmid i$ we have

$$\varprojlim_n (U_n/\overline{C}_n)^{(i)} \cong \mathbb{Z}_p[[T]]/(G_i(T)), \tag{22}$$

where we first have to introduce some notation in order to understand this theorem: $G_i(T)$ is a power series related to the Hecke L-series for ψ. For the definition of U_n we fix one of the prime factors $\mathfrak{p}$, a uniformizer π coming from $\mathfrak{p}$ via the Größencharacter, let $E_{\pi^{n+1}}$ be the kernel of the endomorphism of π^{n+1} and set $F_n := k(E_{\pi^{n+1}})$. Then $\mathfrak{p}$ is totally ramified in F_n and we denote the unique prime ideal above $\mathfrak{p}$ by $\mathfrak{p}_n$, so we can define U_n as the local units of the completion of F_n at $\mathfrak{p}_n$ which are congruent to 1 mod $\mathfrak{p}_n$. $\overline{C}_n$ is the closure of Robert's group of elliptic units C_n in U_n with respect to the $\mathfrak{p}_n$-adic topology and $(U_n/\overline{C}_n)^{(i)}$ denotes the eigenspace of $U_n/\overline{C}_n$ on which $\mathrm{Gal}(F_0/k)$ acts via χ^i, where χ is the canonical character of $\mathrm{Gal}(F_0/k)$ on E_π.

Prelude to Euler Systems. Usually the main desire of a mathematician is to prove new results. But often finding a different proof of a known theorem can also induce striking developments. One instance of this is certainly the proof of F. Thaine [Tha88] of a result which could also be deduced from the IMC for cyclotomic fields proved by Mazur-Wiles in [MW84]. The result we are talking about is the following: Let F be a real abelian extension of $\mathbb{Q}$ of degree prime to p and $G := \mathrm{Gal}(F/\mathbb{Q})$. Let E be the group of global units of F, C be the subgroup of cyclotomic units, and A be the p-Sylow subgroup of the ideal class group of F. If $\theta \in \mathbb{Z}[G]$ annihilates the p-Sylow subgroup of E/C, then 2θ annihilates A. The method of Thaine used to prove this theorem was also independently found by V. Kolyvagin [Kol88], who applied it at first when studying Selmer groups of modular elliptic curves using Heegner points.

Already in 1987 a paper of K. Rubin ([Rub87a]) was published which contained an extension of the method of Thaine to the case of abelian extensions of imaginary quadratic number fields. Now cyclotomic units were replaced with elliptic units and there was the additional condition that the abelian extension F of the imaginary quadratic number field k had to contain the Hilbert class field of k. In fact, Rubin defined special units of F and used them to construct elements of $\mathbb{Z}[\mathrm{Gal}(F/K)]$ which annihilate certain subquotients of the ideal class group of F. Cyclotomic units and elliptic units are examples of such special units.

Why do we care about the method of proof for these annihilation results? Because now an almost magical thing happens: Most of the things discussed so far suddenly fit together. Rubin in [Rub87b] used the techniques developed in [CW77] and [CW78] to obtain results for the BSD conjecture and the ideal class annihilators arising from elliptic units to prove the following: For an elliptic curve E over an imaginary quadratic number field k he proved that the Tate-Shafarevich group under certain conditions is finite or the $\mathfrak{p}$-part is trivial and that for an elliptic curve over $\mathbb{Q}$ with CM it holds: If $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \geq 2$, then $\mathrm{ord}_{s=1} L(E,s) \geq 2$.

One-variable main conjecture. At this point nobody will be surprised to find out that there is also a generalization of the IMC for cyclotomic fields to abelian extensions over an imaginary quadratic number field k.[18] Let M_∞ be the maximal abelian p-extension of $F_\infty := \bigcup_n F_n$ which is unramified outside the primes above $\mathfrak{p}$ and $Y := \mathrm{Gal}(M_\infty/F_\infty)$, with $Y^{(i)}$ the eigenspace of Y

[18] We resume here the notation of **BSD conjecture and elliptic units**.

on which $\mathrm{Gal}(F_0/k)$ acts via χ^i. For split primes in k it was already mentioned in [CW78] that for $(p-1) \nmid i$ the assertion

$$Y^{(i)} \text{ and } \varprojlim_n (U_n/\overline{C}_n)^{(i)} \text{ have the same characteristic ideal,} \tag{23}$$

could be true, later called *one-variable main conjecture*, and that the case $i \equiv 1 \bmod (p-1)$ would 'have deep consequences for the study of the arithmetic of elliptic curves'. It is also worth recalling (13) and (17) for cyclotomic fields at this point. This conjecture, (23), was proved by Rubin, under some hypotheses, in [Rub91] by controlling the size of certain class groups and using the techniques described above. Also for non-split primes, a formulation of the conjecture was given and proved under more restrictive hypotheses. These results again had applications to the arithmetic of elliptic curves with CM, i.e. results surrounding the BSD conjecture.

Introduction of Euler Systems. So the main input to all these new results is the ability to give an upper bound to the size of ideal classes of cyclotomic fields and Selmer groups of certain elliptic curves. An Euler system was then defined in [Kol90] as a collection of certain Galois cohomology classes satisfying conditions like a norm compatibility. The cyclotomic units, elliptic units and Heegner points mentioned above are all examples of such an Euler system. After preliminary work of Kolyvagin in [Kol90], Rubin in [Rub00], as well as K. Kato and B. Perrin-Riou independently developed then an abstract cohomological machinery which uses an axiomatically defined Euler system as an input and produces upper bounds for the sizes of appropriate Selmer groups as an output.

Coleman power series and applications. Picking up on a technique introduced in Theorem 5 in [CW78] and [Wil78], Coleman showed in [Col79] the following: Let K be a local field with local parameter π, H be a complete unramified extension, $\mathcal{F}$ a Lubin-Tate formal group, W_n the n-division values and $H_n := H(W_n)$. Then for each $\alpha \in H_n$ there exists an $f_\alpha \in \mathcal{O}_H((T))^\times$ such that $\varphi^i f_\alpha(\omega_n) = N_{n,i}(\alpha)$, where ω_n is a generator of W_n as an $\mathcal{O}_K$-module, $N_{n,i} : H_n \to H_i$ the norm, and φ the Frobenius for H over K. Such a series for a norm-coherent sequence $(\alpha_n)_n$ satisfies a uniqueness property and is called a *Coleman power series*.

In [dS87], E. deShalit generalized Lubin-Tate theory and the theory of Coleman power series to relative extensions in the context of abelian extensions of an imaginary quadratic field. He used these theories to construct p-adic L-functions and proved a functional equation and an analogue of 'Kronecker's second limit formula' for these p-adic L-functions. Then he applied his results to the one-variable main conjecture and the BSD conjecture.

Inspired by [Tha88], D. Solomon in [Sol92] constructed cyclotomic p-units and computed their valuation using the theory of Coleman power series. He applied this result to a 'weak analogue' of Stickelberger's theorem for real abelian fields.

In the meantime there had also been some new developments in the basic theory of elliptic units. Robert succeeded in constructing a function ψ that is a twelfth root of the function φ, which is used to define elliptic units. Now using elliptic units defined via this function ψ and the theory of Coleman series for relative Lubin-Tate extensions W. Bley constructed in [Ble04] elliptic $\mathfrak{p}$-units and computed their valuation in the situation for split primes, under certain hypotheses, in analogy to the result of Solomon.

Stark's conjecture. As we have seen so far, Gauss's D.A. had a major influence on the algebraic number theory of the 19th century. It was possible to embed large parts of his results into a more general framework. One of the more elusive questions coming from D.A. was certainly the class number one problem, namely the question of how many quadratic number fields have class number one. For imaginary quadratic number fields Gauss already suspected he had a complete list of them.

In the 1960s H. Stark gave the first accepted proof ([Sta67]) of this fact and based on the methods used he had the idea that it maybe was possible to evaluate a general Artin L-function at $s = 1$. He later realized that looking at $s = 0$ is simpler and tried to find a theoretical description of $L'(0, \chi)$ for an L-function with a first order zero at $s = 0$ with the help of numerical computations. In 1970, he published his first 'very vague conjectures' which were later tersely presented by Tate (in [Tat84]) giving a Galois-equivariant conjectural link between the values at $s = 0$ of the first non-vanishing derivative of the S-imprimitive Artin L-function $L_{K/k,S}(s, \chi)$ associated to a Galois extension of number fields K/k and certain $\mathbb{Q}[\mathrm{Gal}(K/k)]$-module invariants of the group U_S of S-units in K, where S is a set of places of K satisfying certain conditions. Siegel and Ramachandra proved the instances of the conjecture for imaginary quadratic number fields via complex multiplication and the applications of the Kronecker limit formulas.

Now building on the work of Siegel and Ramachandra, Stark developed an integral refinement of his conjecture for abelian extensions K/k and abelian S-imprimitive L-functions with order at most 1 at $s = 0$ and under additional hypothesis on S: There exists a special v-unit ϵ, called *Stark unit*, such that

$$L'_{K/k,S}(0, \chi) = \frac{-1}{w_K} \sum_{\sigma \in G} \chi(\sigma) \log |\epsilon^\sigma|_w \text{ for each character } \chi \text{ of } G, \tag{24}$$

where v is a prime which splits completely in K and w a place above v. Stark proved the cases of $k = \mathbb{Q}$ or k imaginary quadratic in [Sta80]. It has to be noted that a proof of the integral refinement would have far reaching applications to Hilbert's 12th problem and already in the 1980's B. Gross ([Gro81], [Gro88]) developed a refinement of Stark's integral conjecture.

Rubin-Stark conjecture and beyond. Finding Euler systems is generally a difficult task, so it is quite remarkable that Stark's integral conjecture is a source for them. Motivated by this observation Rubin generalized Stark's integral conjecture to the case of abelian extensions of number fields K/k and their S-imprimitive L-functions of order $r \geq 0$ under certain conditions on S. This conjecture is now called the *Rubin-Stark conjecture*. A conjectural Gross-type refinement of Rubin-Stark conjecture was also found by work of Tate, Gross, D. Burns, C. Greither and C. Popescu. This has led to a *Gross-Rubin-Stark conjecture*, which implies the Rubin-Stark conjecture and Gross conjectures and predicts a subtle link between special values of derivatives of global and p-adic L-functions.

Inspired by work of Gross in [Gro88], H. Darmon in [Dar95] formulated a refined class number formula which relates cyclotomic units to certain algebraic regulators in a very particular situation. After proving the non-2-part of this conjecture using Kolyvagin systems, which were developed from Euler systems, in [MR16] Mazur and Rubin generalized Darmon's conjecture and proved certain cases of it. The same conjecture was independently found by T. Sano and so is known as *Mazur-Rubin-Sano conjecture*.

Deligne's and Beilinson's conjecture(s). One of the main themes so far is the interpretation of values of L-series at integers by arithmetical objects. A conjecture of Deligne in [Del79] brings some order to several results presented so far. He conjecturally describes the irrational part of the L-values as determinants of a matrix whose coefficients are up to factor of $2\pi i$ periods at a 'critical integer' for different L-functions.

In a more abstract setting Beilinson's conjectures ([Bei84]) link the leading coefficients at integral arguments of L-functions of algebraic varieties over number fields to the global arithmetical geometry of these varieties. In particular, the leading term should be equal to a value related to a certain regulator up to a rational factor. This should be compared to the leading term of the Dedekind zeta function at $s = 0$ and the covolume of the image of the Dirichlet regulator map. Beilinson's conjectures also deal with the orders of vanishing of quite general L-functions and regulators using the rank and the covolume of motivic cohomology in a very abstract setting.

Tamagawa Number Conjecture and its equivariant refinements. If one would have to summarize most of the number theory presented so far, one way of doing it would be to say that L-functions are related to arithmetic invariants. Prominent instances of the phenomenon we have seen so far are the analytic class number formula (4), the refinement of the BSD conjecture (20) or the Iwasawa Main Conjecture (15).

Although we are far away from fully understanding all these results and conjectures there is an incessant quest for a conjectural framework in a more general setting probably driven by a popular view in mathematics that everything is as we expect it to be. We already encountered the conjectures of Beilinson and Deligne which express the values at integer points of L-functions of smooth projective varieties over number fields in terms of periods and regulator integrals. But these conjectures only determine the special values of the L-functions up to a non-zero rational number. The logical next step was done by S. Bloch and Kato in [BK90], in which they generalized the refinement of the BSD conjecture to L-functions for arbitrary smooth projective varieties over number fields. They were therefore removing the $\mathbb{Q}^{\times}$ ambiguity, which culminated in a conjecture now known as *Tamagawa Number Conjecture (TNC)* or *Bloch-Kato conjecture for special values of L-functions*. It is rather unsurprising that the first partial results Bloch and Kato showed concern the Riemann zeta function, e.g. they show the TNC up to a power of 2 for the Tate motive $\mathbb{Q}(r)$ and r even as well as the elliptic curves with complex multiplication since these are the classic test cases for conjectures in arithmetic geometry.

Kato in [Kat93a] refined the theory by defining for a variety X over a number field K and a finite abelian extension L/K the $\mathrm{Gal}(L/K) \ni \sigma$-part of the corresponding L-function and relating special values of such partial L-functions to the $\mathrm{Gal}(L/K)$-module structure on the étale cohomology of $\mathrm{Spec}(\mathcal{O}_L)$ with coefficients in an étale sheaf coming from X. For the situation $K = \mathbb{Q}$, $X = \mathbb{Q}(r)$ and L being a cyclotomic extension of $\mathbb{Q}$ it can be shown that this conjecture is equivalent to the IMC for cyclotomic fields. So Bloch and Kato described the value at zero of L-functions attached to motives with negative weight. By using perfect complexes and their determinants Kato and, independently, J.M. Fontaine (1944-2019) and Perrin-Riou ([FPR94], [Fon92]) also took into account the action of the variety under consideration. This approach via perfect complexes was then used by Burns and M. Flach in [BF96] to define invariants which measure the Galois module structure of the various cohomology groups arising from a motive M over a number field, which admits the action of a finite abelian Galois group. At the end of the 1996 paper they gave a formulation of the *equivariant Tamagawa Number Conjecture* (eTNC) with abelian coefficients, which is Conjecture 4 in [BF96]. In [BF01] Burns and Flach also gave a formulation of the eTNC with non-commutative coefficients and the work of Kato from [Kat93b] on p-adic zeta functions was also generalized, e.g. by T. Fukaya and Kato [FK06], who dealt with the non-abelian situation, too.

The abelian number fields case. So we now have surveyed a massive conjectural framework but learned few about results so far except the testing cases around which the general conjectures are built. But there are some proven instances of the eTNC, the most prominent one being the case of Tate motives of weight ≤ 0 for abelian extensions over $\mathbb{Q}$, i.e. the cyclotomic case proved by Burns and Greither in [BG03] (and independently by A. Huber/G. Kings in [HK03] plus work of M. Witte in [Wit06]). This result can, in a way, be seen as a (probably tentative) peak of the study of cyclotomic fields initiated by Gauss in D.A. approximately 200 years ago. The beauty of this result lies in the fact that it uses a lot of knowledge about cyclotomic fields we have collected over the years. First of all, one can use the Theorem of Kronecker-Weber to reduce to cyclotomic fields and Stark's conjecture for the rationality part of the conjecture. It used the computation of the evaluation of the Dirichlet L-function at $s = 1$, and the functional equation to get the leading term at $s = 0$. The conjecture for a cyclotomic Iwasawa tower is then proved by using the IMC for cyclotomic fields, the vanishing of the μ-invariant for abelian extensions over $\mathbb{Q}$ and a reduction to the localization at height one prime ideals of an Iwasawa algebra. From this result one descents to the finite level of interest with techniques described by J. Nekovář. This descent procedure is quite delicate and uses the result of Solomon on cyclotomic p-units mentioned above as well as a result of Ferrero and R. Greenberg ([FG79]) on the first derivative of a p-adic L-function. Maybe the best way of describing the proof of this result is due to Nekovář who wrote at the end of his review of the paper: 'This is what Iwasawa theory should look like in the new millennium!'.

eTNC implies ... What makes the eTNC such a grand conjecture is that it subsumes a lot of independently developed conjectures in algebraic number theory. For the motive $M = \mathbb{Q}(r)$ it implies or generalizes Stark's conjecture [Tat84], the Rubin-Stark conjecture [Rub96] and its refinements, Popescu's conjecture in [Pop02], the Mazur-Rubin-Sano conjecture of [MR16] and [BKS16], the strong Stark conjecture of Chinburg from [Chi83], the '$\Omega(3)$' conjecture of T. Chinburg from [Chi83] and [Chi85], the Lifted Root Number Conjecture of K. Gruenberg (1928-2007), J. Ritter and A. Weiss [GRW99], and many more. Proofs for this implications can be found in for example in [Bur10], [Bur07], [BKS16]. It certainly also generalizes the analytic class number formula as alluded above and for $M = h^1(E)(1)$, the twisted motive associated to an elliptic curve E, the eTNC (in fact already the TNC) implies the refinement of the BSD conjecture. A proof of this is given in [Kin11]. The list given is only focussing on results discussed above or very near to them by plugging in two classical motives with abelian coefficients. So one may assume this is only the tip of the iceberg.

References

[Art24] Emil Artin. Über eine neue Art von L-Reihen. *Abh. Math. Sem. Univ. Hamburg*, 3(1):89–108, 1924.

[Art27] Emil Artin. Beweis des allgemeinen Reziprozitätsgesetzes. *Abh. Math. Sem. Univ. Hamburg*, 5(1):353–363, 1927.

[Art30] Emil Artin. Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren. *Abh. Math. Sem. Univ. Hamburg*, 8(1):292–306, 1930.

[Ax65] James Ax. On the units of an algebraic number field. *Illinois J. Math.*, 9:584–589, 1965.

[Bar78] Daniel Barsky. Fonctions zeta p-adiques d'une classe de rayon des corps de nombres totalement réels. In *Groupe d'Etude d'Analyse Ultramétrique (5e année: 1977/78)*, pages Exp. No. 16, 23. Secrétariat Math., Paris, 1978.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[Bei84] Alexander Beilinson. Higher regulators and values of L-functions. In *Current problems in mathematics, Vol. 24*, Itogi Nauki i Tekhniki, pages 181–238. Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984.

[BF96] David Burns and Matthias Flach. Motivic L-functions and Galois module structures. *Math. Ann.*, 305(1):65–102, 1996.

[BF01] David Burns and Matthias Flach. Tamagawa numbers for motives with (non-commutative) coefficients. *Doc. Math.*, 6:501–570 (electronic), 2001.

[BG03] David Burns and Cornelius Greither. On the equivariant Tamagawa number conjecture for Tate motives. *Invent. Math.*, 153(2):303–359, 2003.

[BK90] Spencer Bloch and Kazuya Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[BKS16] David Burns, Masato Kurihara, and Takamichi Sano. On zeta elements for $\mathbb{G}_m$. *Doc. Math.*, 21:555–626, 2016.

[Ble04] Werner Bley. Wild Euler systems of elliptic units and the equivariant Tamagawa number conjecture. *J. Reine Angew. Math.*, 577:117–146, 2004.

[Bru67] Armand Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[BSD63] Bryan Birch and Peter Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[BSD65] Bryan Birch and Peter Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[Bur07] David Burns. Congruences between derivatives of abelian L-functions at $s = 0$. *Invent. Math.*, 169(3):451–499, 2007.

[Bur10] David Burns. On leading terms and values of equivariant motivic L-functions. *Pure Appl. Math. Q.*, 6(1, Special Issue: In honor of John Tate. Part 2):83–172, 2010.

[Chi83] Ted Chinburg. On the Galois structure of algebraic integers and S-units. *Invent. Math.*, 74(3):321–349, 1983.

[Chi85] Ted Chinburg. Exact sequences and Galois module structure. *Ann. of Math. (2)*, 121(2):351–376, 1985.

[CN79] Pierrette Cassou-Noguès. Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. *Invent. Math.*, 51(1):29–59, 1979.

[Col79] Robert F. Coleman. Division values in local fields. *Invent. Math.*, 53(2):91–116, 1979.

[CW77] John Coates and Andrew Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[CW78] John Coates and Andrew Wiles. On p-adic L-functions and elliptic units. *J. Austral. Math. Soc. Ser. A*, 26(1):1–25, 1978.

[Dar95] Henri Darmon. Thaine's method for circular units and a conjecture of Gross. *Canad. J. Math.*, 47(2):302–317, 1995.

[Del79] Pierre Deligne. Valeurs de fonctions L et périodes d'intégrales. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2*, Proc. Sympos. Pure Math., XXXIII, pages 313–346. Amer. Math. Soc., Providence, R.I., 1979. With an appendix by N. Koblitz and A. Ogus.

[DR80] Pierre Deligne and Kenneth A. Ribet. Values of abelian L-functions at negative integers over totally real fields. *Invent. Math.*, 59(3):227–286, 1980.

[dS87] Ehud de Shalit. *Iwasawa theory of elliptic curves with complex multiplication*, volume 3 of *Perspectives in Mathematics*. Academic Press, Inc., Boston, MA, 1987.

[FG79] Bruce Ferrero and Ralph Greenberg. On the behavior of p-adic L-functions at $s = 0$. *Invent. Math.*, 50(1):91–102, 1978/79.

[FK06] Takako Fukaya and Kazuya Kato. A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory. In *Proceedings of the St. Petersburg Mathematical Society. Vol. XII*, volume 219 of *Amer. Math. Soc. Transl. Ser. 2*, pages 1–85. Amer. Math. Soc., Providence, RI, 2006.

[Fon92] Jean-Marc Fontaine. Valeurs spéciales des fonctions L des motifs. *Astérisque*, 206:Exp. No. 751, 4, 205–249, 1992. Séminaire Bourbaki, Vol. 1991/92.

[FPR94] Jean-Marc Fontaine and Bernadette Perrin-Riou. Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 599–706. Amer. Math. Soc., Providence, RI, 1994.

[Fue10] Rudolf Fueter. Die verallgemeinerte Kroneckersche Grenzformel und ihre Anwendung auf die Berechnung der Klassenzahlen. *Rend. Circ. Mat. Palermo*, 29:380–395, 1910.

[Fue14] Rudolf Fueter. Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern. *Math. Ann.*, 75:177–255, 1914.

[FW79] Bruce Ferrero and Lawrence C. Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math. (2)*, 109(2):377–395, 1979.

[Gre01] Ralph Greenberg. Iwasawa theory—past and present. In *Class field theory—its centenary and prospect (Tokyo, 1998)*, volume 30 of *Adv. Stud. Pure Math.*, pages 335–385. Math. Soc. Japan, Tokyo, 2001.

[Gro81] Benedict H. Gross. p-adic L-series at $s = 0$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):979–994 (1982), 1981.

[Gro88] Benedict H. Gross. On the values of abelian L-functions at $s = 0$. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 35(1):177–197, 1988.

[GRW99] Karl W. Gruenberg, Jürgen Ritter, and Alfred Weiss. A local approach to Chinburg's root number conjecture. *Proc. London Math. Soc. (3)*, 79(1):47–80, 1999.

[Har40] Godfrey H. Hardy. *A Mathematician's Apology*. Cambridge University Press, Cambridge, England; Macmillan Company, New York, 1940.

[Hec17] Erich Hecke. Über die Zetafunktion beliebiger algebraischer Zahlkörper. *Nachr. Ges. Wiss. Göttingen*, pages 77–89, 1917.

[Her32] Jacques Herbrand. Sur les classes des corps circulaires. *J. Math. Pures Appl., IX. Ser.*, 11:417–441, 1932.

[HK03] Annette Huber and Guido Kings. Bloch-Kato conjecture and Main Conjecture of Iwasawa theory for Dirichlet characters. *Duke Math. J.*, 119(3):393–464, 2003.

[Iwa59a] Kenkichi Iwasawa. On Γ-extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, 65:183–226, 1959.

[Iwa59b] Kenkichi Iwasawa. On the theory of cyclotomic fields. *Ann. of Math. (2)*, 70:530–561, 1959.

[Iwa64] Kenkichi Iwasawa. On some modules in the theory of cyclotomic fields. *J. Math. Soc. Japan*, 16:42–82, 1964.

[Iwa69] Kenkichi Iwasawa. On p-adic L-functions. *Ann. of Math. (2)*, 89:198–205, 1969.

[Iwa72] Kenkichi Iwasawa. *Lectures on p-adic L-functions*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972. Annals of Mathematics Studies, No. 74.

[Kat93a] Kazuya Kato. Iwasawa theory and p-adic Hodge theory. *Kodai Math. J.*, 16(1):1–31, 1993.

[Kat93b] Kazuya Kato. Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{mdR}. I. In *Arithmetic algebraic geometry (Trento, 1991)*, volume 1553 of *Lecture Notes in Math.*, pages 50–163. Springer, Berlin, 1993.

[Kin11] Guido Kings. The equivariant Tamagawa number conjecture and the Birch-Swinnerton-Dyer conjecture. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 315–349. Amer. Math. Soc., Providence, RI, 2011.

[KL64] Tomio Kubota and Heinrich-Wolfgang Leopoldt. Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen. *J. Reine Angew. Math.*, 214/215:328–339, 1964.

[Kol88] Victor A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[Kol90] Victor A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, Boston, MA, 1990.

[Mey57] Curt Meyer. *Die Berechnung der Klassenzahl Abelscher Körper über quadratischen Zahlkörpern*. Akademie-Verlag, Berlin, 1957.

[Mor22] Louis Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, 21:179–192, 1922.

[MR16] Barry Mazur and Karl Rubin. Refined class number formulas for $\mathbb{G}_m$. *J. Théor. Nombres Bordeaux*, 28(1):185–211, 2016.

[MW84] Barry Mazur and Andrew Wiles. Class fields of abelian extensions of $\mathbb{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[Poi01] Henri Poincaré. Sur les propriétés arithmétiques des courbes algébriques. *Jour. Math. Pures Appl.*, 7(Ser. 5), 1901.

[Pop02] Cristian D. Popescu. Base change for Stark-type conjectures 'over $\mathbb{Z}$'. *J. Reine Angew. Math.*, 542:85–111, 2002.

[Ram64] Kanakanahalli Ramachandra. Some applications of Kronecker's limit formulas. *Ann. of Math. (2)*, 80:104–148, 1964.

[Rib76] Kenneth A. Ribet. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[Rie60] Bernhard Riemann. Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsber. Kgl. Preuß. Akad. Wiss. Berlin aus dem Jahre 1859*, pages 671–680, 1860.

[Rob73] Gilles Robert. *Unités elliptiques.* Société Mathématique de France, Paris, 1973. Bull. Soc. Math. France, Mém. No. 36, France, Tome 101.

[Rub87a] Karl Rubin. Global units and ideal class groups. *Invent. Math.*, 89(3):511–526, 1987.

[Rub87b] Karl Rubin. Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. *Invent. Math.*, 89(3):527–559, 1987.

[Rub91] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[Rub96] Karl Rubin. A Stark conjecture "over $\mathbb{Z}$" for abelian L-functions with multiple zeros. *Ann. Inst. Fourier (Grenoble)*, 46(1):33–62, 1996.

[Rub00] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

[Ser65] Jean-Pierre Serre. Zeta and L functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 82–92. Harper & Row, New York, 1965.

[Sie65] Carl L. Siegel. *Lectures on advanced analytic number theory.* Notes by S. Raghavan. Tata Institute of Fundamental Research Lectures on Mathematics, No. 23. Tata Institute of Fundamental Research, Bombay, 1965.

[Sin84] Warren Sinnott. On the μ-invariant of the Γ-transform of a rational function. *Invent. Math.*, 75(2):273–282, 1984.

[Sol92] David Solomon. On a construction of p-units in abelian fields. *Invent. Math.*, 109(2):329–350, 1992.

[Sta67] Harold M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[Sta80] Harold M. Stark. L-functions at $s = 1$. IV. First derivatives at $s = 0$. *Adv. in Math.*, 35(3):197–235, 1980.

[Tak20] Teiji Takagi. Über eine Theorie des relativ-Abelschen Zahlkörpers. *J. Fac. Sci. Univ. Tokyo*, 41(9):1–133, 1920.

[Tat68] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Dix exposés sur la cohomologie des schémas*, volume 3 of *Adv. Stud. Pure Math.*, pages 189–214. North-Holland, Amsterdam, 1968.

[Tat84] John Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, volume 47 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1984. Lecture notes edited by Dominique Bernardi and Norbert Schappacher.

[Tha88] Francisco Thaine. On the ideal class groups of real abelian number fields. *Ann. of Math. (2)*, 128(1):1–18, 1988.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wei07] André Weil. *Number theory*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. An approach through history from Hammurapi to Legendre, Reprint of the 1984 edition.

[Wil78] Andrew Wiles. Higher explicit reciprocity laws. *Ann. Math. (2)*, 107(2):235–254, 1978.

[Wil90] Andrew Wiles. The Iwasawa conjecture for totally real fields. *Ann. of Math. (2)*, 131(3):493–540, 1990.

[Wit06] Malte Witte. On the equivariant main conjecture of Iwasawa theory. *Acta Arith.*, 122(3):275–296, 2006.