ℓ-adic Representations and the Čebotarev Density Theorem

Jennifer Balakrishnan

May 24, 2004

Abstract

The Čebotarev Density Theorem, generalizing Dirichlet's theorem on primes in arithmetic progression, gives us a notion of the density of prime ideals in a number field. We motivate our exposition of the theorem by giving a brief introduction to ℓ-adic representations, as can be found in [Hus04]. We give a brief introduction to class field theory, drawing from [Cox89], and present Deuring's [Deu35] simple proof of the Čebotarev Density Theorem. We conclude by following the impact of the Čebotarev Density Theorem on ℓ-adic representations, by looking at ℓ-adic representations attached to elliptic curves, one of the more famous instances being in the proof of Fermat's Last Theorem.

1 Introduction

In this paper, we provide a brief survey of ℓ-adic representations of number fields, which we use to motivate an exposition of the Čebotarev Density Theorem. We assume the reader has a level of familiarity with algebraic number theory, class field theory, and elliptic curves.[1]

In Section 2, we introduce the topic of ℓ-adic representations of number fields, drawing mostly from the exposition in [Hus04]. The Frobenius is introduced, and a natural question concerning this object lends nicely to an application of the Čebotarev Density Theorem.

This celebrated theorem is the main subject of Section 3, but for the sake of the reader, rather than going straight to the proof, we summarize some of the main results in class field theory, as can be found in [Cox89]. After this brief exposition, we provide Deuring's [Deu35] elegant proof of the Čebotarev Density Theorem and answer the question posed in Section 2.

With this in hand, we continue our study of ℓ-adic representations, and in Section 4, concern ourselves with a slightly different slant, that of ℓ-adic representations attached to elliptic curves. After quickly reviewing some basic facts about elliptic curves and Tate modules, our exposition comes full circle by following an application

[1] For the motivated reader who might be lacking such background, we cite the standard references on each of the relevant subjects.

of the Čebotarev Density Theorem to ℓ-adic representations, as can be found in Wiles' proof of Fermat's Last Theorem.

2 ℓ-adic Representations of Number Fields

Let K be a number field, and let $\bar{K}$ denote its algebraic closure. Recall that a *complex n-dimensional representation* (also called an *Artin representation*) of $\mathrm{Gal}(\overline{K}/K)$ is a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_n(\mathbb{C}).$$

That ρ is continuous means that there is a finite Galois extension $L/K, L \subset \bar{K}$, such that ρ factors through $\mathrm{Gal}(L/K)$:

$$\begin{tikzcd}
\mathrm{Gal}(\overline{K}/K) \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{GL}_n(\mathbb{C}) \\
& \mathrm{Gal}(L/K) \arrow[ur, "\rho'"'] &
\end{tikzcd}$$

Taylor [Tay02] concedes that Artin representations are perhaps the most obvious representations to study, but argues that replacing the complex numbers $\mathbb{C}$ with the ℓ-adic numbers $\mathbb{Q}_l$ proves more useful in understanding the Galois group $\mathrm{Gal}(\overline{K}/K)$ than complex representations. Thus, we define an *n-dimensional ℓ-adic representation* of the Galois group $\mathrm{Gal}(\overline{K}/K)$, or of the field K, to be the continuous[2] homomorphism

$$\rho : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{Q}_l),$$

where V is an n-dimensional $\mathbb{Q}_l$-vector space.

Remark 2.1. As we shall see when considering Tate modules in Section 4, ℓ-adic representations typically have infinite image. Thus Artin representations can be thought of as a special case of ℓ-adic representations: those with finite image.

The representation ρ is said to be unramified at a place v of K provided for each place w of $\bar{K}$ over K, we have that the inertia group I_w acts trivially on V, i.e., that $\rho(I_w) = 1$.

Example 2.2 *(Tate twist).* For the one-dimensional Galois representation $\mathbb{Q}_l(1)(\bar{K})$, the representation is unramified at v if and only if v does not divide ℓ.

Example 2.3. Let $H = \ker(\rho)$, where $\rho : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(V)$ is an ℓ-adic representation. Let L be the fixed subfield of $\bar{K}$ corresponding to H. Then ρ is unramified if and only if the extension L/K is unramified at the place v.

[2] with respect to the ℓ-adic topology on $\mathrm{GL}_n(\mathbb{Q}_l)$

Now let L be a Galois extension of K with Galois group $\mathrm{Gal}(L/K)$, and let w be a place of L extending a place v of K. The decomposition subgroup D_w of $\mathrm{Gal}(L/K)$ is the set of all $s \in \mathrm{Gal}(L/K)$ such that $ws = w$. Reducing modulo the maximal ideal, we have a surjective map

$$D_w \twoheadrightarrow \mathrm{Gal}(k(w)/k(v)), \tag{2.1}$$

where $k(w)$ and $k(v)$ denote the residue class field of R_w and R_v, respectively. The group $\mathrm{Gal}(k(w)/k(v))$ is generated by Frob_w, where $\mathrm{Frob}_w(a) = a^{|k(w)|}$. The kernel of the map (2.1) is the inertia subgroup I_w of the place w, and hence we have the natural isomorphism

$$D_w/I_w \longrightarrow \mathrm{Gal}(k(w)/k(v)). \tag{2.2}$$

If $\rho : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(V)$ is unramified at v, then $\rho|_{D_w} : D_w \longrightarrow \mathrm{GL}(V)$ induces a map $D_w/I_w \longrightarrow \mathrm{GL}(V)$, which can be composed with the inverse of the natural map (2.2), which yields a canonical l-adic representation of the field

$$\rho_w : \mathrm{Gal}(k(w)/k(v)) \longrightarrow \mathrm{GL}(V).$$

We denote the image of the canonical generator Frob_w in $\mathrm{GL}(V)$ by $\mathrm{Frob}_{w,\rho}$. Two places w and w' extending v are conjugate under the Galois group, which implies that $\mathrm{Frob}_{w,\rho}$ and $\mathrm{Frob}_{w',\rho}$ are conjugate in $\mathrm{GL}(V)$. Thus they have the same characteristic polynomial, which are dependent solely on the v that they are extending and the representation ρ.

At this point, a natural question to ask is if there are sufficiently many Frobenius elements in the Galois group. As it turns out, this question is answered for us by the Čebotarev Density Theorem.

3 The Čebotarev Density Theorem

The goal of this section is to prove the following:

Theorem 3.1 (Čebotarev Density Theorem). *Let L/K be a finite Galois extension of number fields, and denote $\mathrm{Gal}(L/K)$ by G. For each subset $C \subset G$ that is stable under conjugation, let S denote the set of places v of K that are unramified in L such that the Frobenius element $Frob_w$ is in C for any w extending v. Then S has Dirichlet density*[3] *equal to*

$$\frac{|C|}{|G|}.$$

3.1 Some Class Field Theory

Before we can present Deuring's proof [Deu35] of the Čebotarev Density Theorem, some preliminaries from Class Field Theory[4] are in order.

[3] We shall define Dirichlet density in the next section.

[4] Mostly drawn from the exposition in [Cox89] and [Lan94]

Given a number field K, we define a *modulus*[5] in K to be a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}},$$

over all primes $\mathfrak{p}$ of K, where the exponents $n_{\mathfrak{p}}$ are such that

- $n_{\mathfrak{p}} \geq 0$, and at most finitely many are nonzero,
- $n_{\mathfrak{p}} = 0$ whenever $\mathfrak{p}$ is a complex infinite prime, and
- $n_{\mathfrak{p}} \leq 1$ whenever $\mathfrak{p}$ is a real infinite prime.

A modulus $\mathfrak{m}$ can thus be written in the form $\mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an $\mathcal{O}_K$-ideal and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes of K. In the case that all of the $n_{\mathfrak{p}} = 0$, we let $\mathfrak{m} = 1$.

Denote by $I_K(\mathfrak{m})$ the group of all fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{m}$, and let $P_{K,1}(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ is such that $a \equiv 1 \bmod \mathfrak{m}_0$ for every real infinite prime σ dividing $\mathfrak{m}_\infty$. It is a well-known fact that $P_{K,1}(\mathfrak{m})$ has finite index in $I_K(\mathfrak{m})$.

A *congruence subgroup* for $\mathfrak{m}$ is a subgroup $H \subset I_K(\mathfrak{m})$ such that

$$I_{K,1}(\mathfrak{m}) \subset H \subset I_K(\mathfrak{m}).$$

Furthermore, the quotient $I_K(\mathfrak{m})/H$ is known as a *generalized ideal class group* for $\mathfrak{m}$.

Example 3.2. As a simple example, or perhaps to see how this generalizes the notion of ideal class group, consider the modulus $\mathfrak{m} = 1$. $P_K = P_{K,1}(1)$ is a congruence subgroup, and our common notion of ideal class group $\mathcal{CL}(\mathcal{O}_K) = I_K/P_K$ is a "generalized" ideal class group.

At the center of class field theory is the notion that the generalized ideal class groups for $\mathfrak{p} \in K$ are the Galois groups of all Abelian extensions of K. These two ideas are connected by the Artin map, which we shall now briefly discuss.

Given $\mathfrak{p}$ a modulus divisible by all ramified primes of an Abelian extension $K \subset L$ and a prime $\mathfrak{p}$ not dividing $\mathfrak{m}$, we have the Artin symbol

$$\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$$

which extends by multiplicativity to give us a map

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K),$$

called the *Artin map* for $K \subset L$ and $\mathfrak{m}$.

The following famous result, known as the *Artin Reciprocity Theorem*, states that $\mathrm{Gal}(L/K)$ is a generalized ideal class group for some modulus:

[5] In the terminology of Lang, a "cycle"

Theorem 3.3. *Let $K \subset L$ be an Abelian extension, and let $\mathfrak{m}$ be a modulus divisible by all primes of K, finite or infinite, that ramify in L. Then the Artin map $\Phi_{\mathfrak{m}}$ is surjective. Furthermore, if the exponents of the finite primes dividing $\mathfrak{m}$ are sufficiently large, then $\ker(\Phi_m)$ is a congruence subgroup for $\mathfrak{m}$ and thus the isomorphism $I_K(\mathfrak{m})/\ker(\Phi_{\mathfrak{m}}) \longrightarrow \mathrm{Gal}(L/K)$ tells us that $\mathrm{Gal}(L/K)$ is a generalized ideal class group for the modulus $\mathfrak{m}$.*

Remark 3.4. A proof of the Artin Reciprocity Theorem can be found in [Jan73]. The important observation to make is that $\ker(\Phi_m)$ being a congruence subgroup, i.e., $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_m)$, means that the Artin symbol $((L/K)/\mathfrak{p})$ depends only on $\mathfrak{p}$ up to multiplication by α such that $\alpha \equiv 1 \bmod \mathfrak{m}$.

Remark 3.5. Note that the $\mathfrak{m}$ for which $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup is not unique. Indeed, if $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}})$ and $\mathfrak{n}$ is any modulus divisible by $\mathfrak{m}$, then $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}})$ implies that $P_{K,1}(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}})$, and thus $\mathrm{Gal}(L/K)$ is a generalized ideal class group for infinitely many moduli.

Finally, we introduce the notion of *Dirichlet density.* Let $\mathcal{P}_K$ the set of all finite primes of K. Given a subset $\mathcal{S} \subset \mathcal{P}_K$, the Dirichlet density of $\mathcal{S}$ is the limit

$$\delta(\mathcal{S}) = \lim_{s \to 1+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} \frac{1}{N(\mathfrak{p})}}{\log \frac{1}{s-1}}.$$

Some basic properties of Dirichlet density are as follows:

- $\delta(\mathcal{P}_K) = 1$
- If $\delta(\mathcal{S})$ exists, $0 \leq \delta(\mathcal{S}) \leq 1$
- $\delta(I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})) = \frac{1}{[I_K(\mathfrak{m}):P_{K,1}(\mathfrak{m})]}$

3.2 The Theorem

We are now ready to present Deuring's proof [Deu35] of the Čebotarev Density Theorem.

Recall the statement of the theorem:

Theorem 3.6 (Čebotarev Density Theorem). *Let L/K be a finite Galois extension of number fields, and denote $\mathrm{Gal}(L/K)$ by G. For each subset $C \subset G$ that is stable under conjugation, let S denote the set of places v of K that are unramified in L such that the Frobenius element $Frob_w$ is in C for any w extending v. Then S has Dirichlet density equal to*

$$\frac{|C|}{|G|}.$$

Proof. Fix $\sigma \in G$ of order f, let C denote its conjugacy class, and let Z denote its fixed field. Then L/Z is cyclic of degree f and is a class field. If $\mathfrak{m}$ is a modulus for L/Z, then by the Artin Reciprocity Theorem, we have the isomorphism

$$I_{L/Z}(\mathfrak{m})/H \longrightarrow \mathrm{Gal}(L/Z),$$

where H is a subgroup of $I_{L/Z}(\mathfrak{m})$ containing $P_{L/Z,1}$. Let S be as above, and let $S_{L,\sigma}$ be the set of w in L such that w extends v for any $v \in S$ and $\sigma = \mathrm{Frob}_w$. Let w extend $\mathfrak{q}$ for $\mathfrak{q} \in Z$. Then $S_{L,\sigma}$ is in bijection with the set S_Z of $\mathfrak{q} \in Z$ that lie in a given class mod H and that divide v splitting completely in Z. However, the density is dependent solely on those primes of degree 1 over $\mathbb{Q}$, and thus S_Z has density $1/f$. But for a fixed v, the number of $w \in L$ lying above v such that $\mathrm{Frob}_w = \sigma$ is equal to the quotient

$$\frac{[G_\sigma : 1]}{[G_w : 1]},$$

where G_σ is the subgroup of elements of G commuting with σ and G_w is the decomposition group of w. Since $[G : G_\sigma] = |C|$, we see that

$$\frac{[G_\sigma : 1]}{[G_w : 1]} = \frac{|G|}{|C|f}.$$

Hence the density of S is

$$\frac{\frac{1}{f}}{\frac{|G|}{|C|f}} = \frac{|C|}{|G|},$$

as desired. □

As a corollary, we have an answer to our original question posed in Section 1:

Corollary 3.7. *Let L be an algebraic Galois extension of a number field K which is unramified outside a finite number of places of K. Then the Frobenius elements of the unramified places of L are dense in* $\mathrm{Gal}(L/K)$*.*

Proof. By Theorem 3.6, we know that the set of Frobenius elements maps surjectively onto every finite quotient of $\mathrm{Gal}(L/K)$, which implies that every element of $\mathrm{Gal}(L/K)$ is arbitrarily close to a Frobenius element. □

4 ℓ-adic Representations and Elliptic Curves

In Section 2, we examined ℓ-adic representations of number fields K, and in so doing, were drawn to ask if there were sufficiently many Frobenius elements of a Galois group. We answered this question in Section 3 with the Čebotarev Density Theorem. Now we return to the subject of ℓ-adic representations, this time considering ℓ-adic representations of elliptic curves over $\mathbb{Q}$.

We begin with some basic facts about elliptic curves, proofs of which can be found in [Sil92].

Let E be an elliptic curve over $\mathbb{Q}$ in Weierstrass normal form $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$. It is well-known that

Fact 4.1. *The points on an elliptic curve form an abelian group.*

With an addition law on the points on an elliptic curve, we can talk about the m-torsion points on an elliptic curve, which we denote $E[m]$. One can show that

Fact 4.2. *The set of m-torsion points on an elliptic curve, $E[m]$, is such that*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

Yet this is just the tip of the iceberg, because $E[m]$ has even more structure! Each element of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ can act on $E[m]$, since if $[m]P = \mathcal{O}$ for $P \in E[m]$, then

$$[m](P^\sigma) = ([m]P)^\sigma = \mathcal{O}.$$

Hence, we have a representation

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

where the last isomorphism necessitates choosing a basis for $E[m]$.

However, we must make a slight adjustment: these representations are not exactly what we want, since it is usually to one's best interest to work with representations whose matrices have coefficients in a ring with characteristic 0. So the natural thing to do is to piece together the information for various m, à la the inverse limit construction of the ℓ-adic integers $\mathbb{Z}_l$ from the finite groups $\mathbb{Z}/l^n\mathbb{Z}$.

Thus, given E an elliptic curve and $l \in \mathbb{Z}$ a prime, the *ℓ-adic Tate module* of E is the group

$$T_l(E) = \varprojlim E[l^n],$$

the inverse limit being taken with respect to the natural maps

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n].$$

As each $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, we see that the Tate module has a natural structure as a $\mathbb{Z}^l$-module, namely,

$$T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l.$$

We therefore have that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on each $E[l^n]$ commutes with the multiplication-by-ℓ maps used to form the inverse limit, so $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ also acts on $T_l(E)$. Furthermore, as the profinite group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts continuously on each finite (and thus, discrete) group $E[l^n]$, the action on $T_l[E]$ is continuous as well.

Hence we can define the *ℓ-adic representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on* E, denoted by ρ_l, to be the map

$$\rho_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(T_l(E)),$$

with the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_l(E)$ as detailed above.

Finally, we mention a key invariant and an interesting property of elliptic curves.

The *conductor* N of an elliptic curve is an integer attached to the elliptic curve which measures the extent to which E fails to define an elliptic curve over $\mathbb{F}_p$ for each prime p. A semistable elliptic curve is one with squarefree conductor.

With this in mind, an elliptic curve over $\mathbb{Q}$ with conductor N is said to be modular if one of the two equivalent formulations of modularity hold:

1. (Analytic modularity) There exists a modular form $f \in \Gamma_0(N)$ of weight two such that $L(E, \chi, s) = L(f, \chi, s)$ for all Dirichlet characters χ.

2. (Geometric modularity) E can be parametrized by a modular curve $X_0(N)$ by means of a non-constant morphism, i.e., $X_0(N) \longrightarrow E$.

All of these ideas play a crucial role in the proof of Fermat's Last Theorem. Ken Ribet [Rib93] notes that at the crux of the issue is proving Taniyama's conjecture, i.e., showing that a semistable elliptic curve $E/\mathbb{Q}$ is modular. Wiles [Wil95] begins by fixing an odd prime ℓ, which, as it turns out, is 3 or 5. The elliptic curve E is associated with an ℓ-adic representation $\rho_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_l)$. E satisfies Taniyama's conjecture if and only if ρ_l is modular, i.e., associated to a weight-two cuspidal eigenform. Indeed, the representation ρ_l appears to have the necessary modularity properties, as it has the right determinant and satisfies certain local conditions at ℓ and certain other ramified primes.

Drawing from the work of Mazur, Hida, Tilouine, Flach, Kolyvagin, and others, Wiles proves that a representation ρ_l is modular if it reduces mod ℓ to a representation $\bar{\rho}_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_l)$ that is (1) surjective and (2) is itself modular. That $\bar{\rho}_l$ is modular means that $\bar{\rho}_l$ lifts to a modular representation, which implies that we want ρ_l to be congruence to some modular representation. Wiles approaches this problem using the deformation theory of Mazur [Maz89].

The next important step is to show that E is modular. By first looking at the case $\ell = 3$, Wiles observes that $\bar{\rho}_3$ satisfies (2) whenever it satisfies (1). Hence E is modular whenever $\bar{\rho}_3$ is surjective. However, what happens when $\bar{\rho}_3$ is not surjective? Wiles considers the function field $\mathbb{Q}(t)$ of a component of a twist of $X(5)/\mathbb{Q}$ and uses the Hilbert irreducibility theorem to show that there exists a t_1 such that $f(x, t_1) \in \mathbb{Q}(t)[x]$ corresponding to $\bar{\rho}_3$ is irreducible. Then using the Čebotarev density theorem, he picks a prime $p_1 \neq 5$ such that $f(x, t_1)$ does not have a root mod p_1. Finally, a $t_0 \in \mathbb{Q}$ is chosen that is p_1-adically close to t_1 and 5-adically close to the original value of t giving E. This construction thus gives us a semistable elliptic curve E' having a mod 3 representation satisfying (1) and having a mod 5 representation isomorphic to $\bar{\rho}_5$. Wiles uses his key theorem to show that E' is modular, which implies that $\bar{\rho}_5$ is modular, as it can be thought of as coming from E'. Applying his key theorem to ρ_5, he concludes that E is modular.

References

[Cox89] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1989, Pure and Applied Mathematics.

[Deu35] M. Deuring, *Über den Tschebotareffschen Dichtigkeitssatz*, Math. Ann. **110** (1935), 414–415.

[Hus04] D. Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2004.

[Jan73] G. Janusz, *Algebraic number fields*, Academic Press, New York, 1973.

[Lan94] S. Lang, *Algebraic number theory*, second ed., Springer-Verlag, New York, 1994.

[Maz89] B. Mazur, *Deforming Galois representations*, Galois groups over **Q** (Berkeley, CA, 1987), Springer, New York, 1989, pp. 385–437.

[Rib93] K. Ribet, *Wiles proves Taniyama's conjecture; Fermat's last theorem follows*, Notices Amer. Math. Soc. **40** (1993), no. 6, 575–576.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Tay02] R. Taylor, *Galois representations*, Proc. Internat. Congr. Mathematicians (Beijing, 2002), Higher Education Press, Beijing, 2002, pp. 449–474.

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.