Introduction to modular forms

Yao-Rui Yeo

In this notes we describe how modular forms relate to sum of squares and elliptic curves.

1 The sum of squares problem

The sum of squares problem is the following: For fixed positive integers k and n, what can we say about integer solutions $(x_1, \ldots, x_k)$ to the polynomial equation $x_1^2 + \cdots + x_k^2 = n$? Of course, there are the classical well-known results that classify the existence of such solutions for the case $k = 2$ and $k = 3$, and that positive integers can be written as the sum of four squares (commonly credited to Fermat, Legendre, and Lagrange respectively); all of these can be proven via elementary number theory. One can ask further questions:

(a) How many solutions are there to the sum of squares problem?

(b) How are the solutions distributed on the k-sphere of radius $\sqrt{n}$?

It turns out that these two questions can be partially answered via the theory of modular forms. Let us first write out question (a) precisely. Let $r(n, k)$ be the number of ways to represent n as the sum of k squares, i.e.

$$r(n, k) := \#\{x \in \mathbb{Z}^k : n = x_1^2 + \cdots + x_k^2\}.$$

Then a combinatorial technique to determine $r(n, k)$ is to write down a generating function

$$\theta(\tau, k) = \sum_{n=0}^{\infty} r(n, k) q^n, \qquad q = e^{2\pi i \tau} \text{ and } \tau \in \mathbb{H}.$$

This function is holomorphic and satisfies $\theta(\tau + 1, k) = \theta(\tau, k)$. By a combinatorial observation, we have the crude bound $r(n, k) \leq 2^k n^k$, and $\theta(\tau, k_1)\theta(\tau, k_2) = \theta(\tau, k_1 + k_2)$. In particular, $\theta(\tau, k) = \theta(\tau, 1)^k$. Observe that $\theta(\tau, 1)$ is the classical theta function, and one can show [1, section 4.9], via the Poisson summation formula, that

$$\theta\left(-\frac{1}{4\tau}, 1\right) = \sqrt{-2i\tau}\, \theta(\tau, 1).$$

We now restrict ourselves to the case where k is even. Another computation using the above identity will show that

$$\theta\left(\frac{\tau}{4\tau + 1}, k\right) = (4\tau + 1)^{k/2} \theta(\tau, k).$$

Hence θ satisfies

$$\theta(\gamma(\tau), k) = (c\tau + d)^{k/2} \theta(\tau, k), \qquad \text{for } \gamma \in \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\rangle = \Gamma_1(4).$$

(By convention, c and d are the lower left and lower right entries of the matrix γ.)

To summarize the discussion above, one would say that $\theta(\tau, k)$, for k even, is a *modular form of weight k with respect to* $\Gamma_1(4)$. Hence, in order to try to compute $r(n, k)$, one can try to understand more about modular forms, in particular its dimension as a vector space, and how fast the Fourier coefficients grow.

In general, if $k \in \mathbb{Z}_{\geq 0}$ and Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (so $\begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix} \in \Gamma$ for some positive integer N, which we assume to be smallest possible), consider a holomorphic function $f : \mathbb{H} \longrightarrow \mathbb{C}$ satisfying *weight-k invariance*, i.e. $f(\gamma(\tau)) = (c\tau + d)^k f(\tau)$ for $\gamma \in \Gamma$. Then f has a Fourier expansion

$$f(\tau) = \sum_n a_n q_N^n, \qquad q_N = e^{2\pi i \tau / N}$$

about the punctured unit disk. We can also consider, for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the *weight-$k$ operator* $[\gamma]_k$ defined by $f[\gamma]_k(\tau) := (c\tau + d)^{-k} f(\gamma(\tau))$. This admits a Fourier expansion as well as it is modular with respect to the congruence subgroup $\gamma^{-1}\Gamma\gamma$. Such a function f as above is a *modular form of weight k with respect to* Γ if $f[\gamma]_k$ extends holomorphically to zero in the unit disk for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, so the Fourier coefficient $a_{\gamma,n}$ for $f[\gamma]_k$ is zero if $n < 0$. If furthermore $a_{\gamma,0} = 0$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then we say f is a *cusp form.* Also notice that, if k is odd and $-I_2 \in \Gamma$, then we would have $f(\tau) = -f(\tau)$, implying $f \equiv 0$. Hence when discussing question (a) in the sum of squares problem we restrict ourselves to even k (the case for odd k can be recovered from this by a finite sum, assuming a formula exists for even k).

We write the space of modular forms and cusp forms as $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$ respectively. The explicit dimension formulas for $\mathcal{M}_k(\Gamma)$ [1, chapter 3] implies that the space of modular forms is finite-dimensional. Writing $\mathcal{E}_k(\Gamma) = \mathcal{M}_k(\Gamma)/\mathcal{S}_k(\Gamma)$ to be the space of *Eisenstein series*, we get a natural decomposition

$$\mathcal{M}_k(\Gamma) = \mathcal{S}_k(\Gamma) \bigoplus \mathcal{E}_k(\Gamma).$$

(In fact, the cusp forms and Eisenstein series are "orthogonal": an inner product $<,>_\Gamma$ on $\mathcal{S}_k(\Gamma)$ that does not extend to $\mathcal{M}_k(\Gamma)$, call the *Petersson inner product*, still makes sense if one of its entries is not a cusp form.) This decomposition is useful as an explicit basis for $\mathcal{E}_k(\Gamma)$ can be written out for the important congruence subgroups [1, chapter 4]. Although we cannot write out an explicit basis for $\mathcal{S}_k(\Gamma)$, we are able to exhibit one using the theory of newforms [1, chapter 5], and we can reinterpret it as certain first cohomology via simplicial cohomology or group cohomology [4, chapter 8].

Let us now return to question (a) of the sum of squares problem. It turns out we can use the theory of modular forms to explicitly write out the formulas for $r(n, k)$ for $k = 2, 4, 6, 8$, since a consequence of the dimension formulas imply $\mathcal{S}_{k/2}(\Gamma_1(4)) = \{0\}$ for these values of k, so $\mathcal{M}_{k/2}(\Gamma_1(4))$ admits a basis in terms of Eisenstein series. For example, in case $k = 4$ one has $\dim_{\mathbb{C}} \mathcal{M}_2(\Gamma_1(4)) = 2$ with a basis of Eisenstein series

$$G_{2,2}(\tau) = -\frac{\pi^2}{3}\left(1 + 24\sum_{n=1}^{\infty}\left(\sum_{\substack{0\,<\,d|n\\ d\text{ odd}}} d\right) q^n\right), \qquad G_{2,4}(\tau) = -\pi^2\left(1 + 8\sum_{n=1}^{\infty}\left(\sum_{\substack{0\,<\,d|n\\ 4\nmid d}} d\right) q^n\right).$$

Writing $\theta(k, 4) = 1 + 8q + \cdots$ in terms of $G_{2,2}$ and $G_{2,4}$ would give us $\theta(\tau, 4) = -\pi^{-2} G_{2,4}(\tau)$ by equating Fourier coefficients, so one has

$$r(n, 4) = 8 \sum_{\substack{0\,<\,d|n\\ 4\nmid d}} d, \qquad \text{for } n \geq 1.$$

Similar formulas can be achieved for $r(n, 2)$ and $r(n, 6)$ and $r(n, 8)$ by the same method. For example, in case $r(n, 2)$ we have

$$r(n, 2) = 4 \sum_{\substack{0\,<\,m|n\\ m\text{ odd}}} (-1)^{(m-1)/2},$$

and Fermat's sum of two squares theorem tells us this equals zero if n has a prime factor $p \equiv 3 \pmod 4$.

For the case $k \geq 10$, we will be able to use the same methods to solve the sum of squares problem case by case if we have an explicit basis for the space of cusp forms. We do not have this in general though. Things are not so bad however, since we can get an asymptote in n by ignoring the cusp forms and doing the same computation as above. This is a consequence of Hecke's estimate that as $n \to \infty$ the Fourier coefficients of Eisenstein series dominate those of cusp forms. More precisely, for any congruence subgroup Γ, the Fourier coefficients of cusps forms $f \in \mathcal{S}_k(\Gamma)$ satisfy $|a_n(f)| \leq O(n^{k/2})$ (via analytic estimates), and those of Eisenstein series $f \in \mathcal{E}_k(\Gamma)$ satisfy $|a_n(f)| = O(n^{k-1})$, (via elementary estimates on the coefficients of Eisenstein series, which are generalized divisor functions up to factors of primitive Dirichlet characters).

Let us now move on to question (b) in the sum of squares problem, which asks how elements of the set $X_n = \{x \in \mathbb{Z}^k : n = x_1^2 + \cdots + x_k^2\}$ are distributed on the sphere of radius $\sqrt{n}$ (note that $\#X_n = r(n, k)$ by definition). We are most interested in knowing if the solutions are *equidistributed.* Roughly speaking, this means that one sees about the same amount of solutions anywhere on the sphere. More precisely, writing

S^k to be the unit k-sphere, equidistribution means that, for every $F \in C^\infty(S^k)$,

$$\lim_{n\to\infty} \frac{1}{r(n,k)} \sum_{x\in X_n} F\left(\frac{x}{|x|}\right) = \int_{S^k} F.$$

We can easily show that this holds if $k = 8\kappa$ is a positive multiple of eight by an application of Hecke's estimate (this assumption is used to avoid analytic difficulties). A way to attack it is using *Weyl's equidistribution criterion*, which states that it suffices to show

$$\lim_{n\to\infty} \frac{1}{r(n,k)} \sum_{x\in X_n} P\left(\frac{x}{|x|}\right) = 0$$

with P a homogeneous harmonic polynomial on $\mathbb{R}^k$ of degree $d > 0$. The explicit Eisenstein basis in our case implies that $r(n,k) \geq C_k n^{4\kappa-1}$ for large enough n and some constant $C_k > 0$ depending on k. Also, it can be shown analogously for the function $\theta(\tau,k)$ that the following more general function

$$\sum_{n=0}^{\infty} r_P(n,k)q^n, \qquad r_P(n,k) := \sum_{x\in X_n} P(x)$$

is a cusp form in $\mathcal{S}_{4\kappa+d}(\Gamma_1(4))$ (if $d = 0$, this function is *not* a cusp form). Hecke's estimate applies to give $r_P(n,k) \leq Cn^{(4\kappa+d)/2}$ for some other constant $C > 0$. By homogeneity of P and the various inequalities above,

$$\frac{1}{r(n,k)} \sum_{x\in X_n} P\left(\frac{x}{|x|}\right) \leq \frac{Cn^{(4\kappa+d)/2}}{C_k n^{4\kappa-1} n^{d/2}}, \qquad \text{which tends to zero as } n\to\infty.$$

Remark 1. Lagrange's four-square theorem asserts $Q(x) = x_1^2 + \cdots + x_k^2$ admits all positive integers if $k \geq 4$, and we have a complete list of integers not represented by two or three squares. A generalization of these facts is the 15-theorem, which states that a positive definite quadratic form $Q(x)$ with integer matrix admits all positive integers if it admits $1, 2, 3, 5, 6, 7, 10, 14, 15$. This theorem, among other observations, is immediately deduced by Bhargava from his idea of escalations, after quite a bit of computation. Briefly speaking, the idea of escalations reinterprets such $Q(x)$ with a lattice L having integer inner products, and constructs finitely many possible sequences of lattices $L_0 \subsetneq \cdots \subsetneq L_l \subset L$, with $\dim L_d = d$ and $l \in \{4,5\}$, such that L_l has its points with norms of all positive integers. A generalization of the 15-theorem is the 290-theorem, which states that a positive definite quadratic form $Q(x)$ with integer coefficients admits all positive integers if it admits (a subset of twenty-nine) positive integers up to 290. The proof of this uses a difficult extension of escalations, together with a tighter variation of Hecke's estimate on the Fourier coefficients of modular forms, and computational power (lasting two weeks according to his talk last year).

2 Modular forms and elliptic curves

A complex elliptic curve E is the quotient $\mathbb{C}/\Lambda$ of the complex plane by a lattice $\Lambda \cong \mathbb{Z}^2$. We denote its N-torsion points as $E[N]$, which is isomorphic to $(\mathbb{Z}/NZ)^2$. On this torsion subgroup, we can also define a bilinear form $e_N : E[N] \times E[N] \longrightarrow \mu_N$, also known as *Weil pairing*. Via the Weierstrass $\wp$-function of Λ, this $\mathbb{C}/\Lambda$ is in bijection with the solution set of $(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$ of $\mathbb{C}^2$, where the coefficients of g_2 and g_3 are constant multiples of Eisenstein series. More generally, an elliptic curve E over an arbitrary field k is the solution set in an algebraic closure $\overline{k}$ of a cubic equation of Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in k$$

such that its discriminant is nonzero. If $\mathrm{char}(k) \neq 2, 3$, then we can do admissible change of variables (that fixes the infinity point and preserves Weierstrass form) to convert it into the form $y^2 = x^3 + c_2x + c_3$. Contrary to the complex case, the N-torsion points $E[N]$ is not usually isomorphic to $(\mathbb{Z}/NZ)^2$, though this is still true if $\mathrm{char}(k)$ does not divide N.

We now discuss a relationship between modular forms and elliptic curves. For an elliptic curve E over $\mathbb{Q}$, one is naturally interested in the solution count as we reduce it over a prime p (where we need to reduce it carefully). If $\widetilde{E}$ is the reduction of E modulo p, then we can define $a_p(E) = p+1-\#\widetilde{E}(\mathbb{F}_p)$, where $\widetilde{E}(\mathbb{F}_p)$ denote the points of $\widetilde{E}$ defined in $\mathbb{F}_p$, and in the counting of points we also include the infinity point. The reduction modulo p of E does not necessarily yield an elliptic curve $\widetilde{E}$ as its discriminant might be zero modulo p, and the conductor $N_E = \prod_{\text{primes}} p^{f_p}$ of E is able to tell us this information since p divides N_E if and only if $\widetilde{E}$ is not an elliptic curve. The numbers $a_p(E)$ are related to modular forms as follows. Define

$$\Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

(This is a generalization of the group $\Gamma_1(4)$ in the previous section.) In modular forms there is the theory of Hecke operators $T_n : \mathcal{S}_k(\Gamma_1(N)) \longrightarrow \mathcal{S}_k(\Gamma_1(N))$ for any positive integer n that interacts nicely with Fourier coefficients, in the sense that we can write explicit formulas of how T_n acts on them. In particular, the newforms mentioned in the previous section are cusp forms that satisfy $a_1(f) = 1$, have Fourier coefficients completely determined by those $a_p(f)$ with p prime, and are eigenforms for all T_n with eigenvalue $a_n(f)$ (i.e. $T_n(f) = a_n(f)f$). Denote $\Gamma_0(N)$ in the same way, except allowing the two 1's in the definition of $\Gamma_1(N)$ to be arbitrary integers (so $\Gamma_1(N) \subset \Gamma_0(N)$ and $\mathcal{M}_k(\Gamma_0(N)) \subset \mathcal{M}_k(\Gamma_1(N))$). The *modularity theorem* tells us that for an elliptic curve E over $\mathbb{Q}$, there exists a newform $f \in \mathcal{S}_2(\Gamma_0(N_E))$ such that $a_p(f) = a_p(E)$ for all primes p. Hence newforms are useful here as they parametrizes arithmetic information of elliptic curves.

We can reinterpret the modularity theorem of the previous paragraph in terms of L-functions. For a modular form $f = \sum_{n=0}^{\infty} a_n(f)q^n \in \mathcal{M}_k(\Gamma_1(N))$, we can define its L-function as $L(s,f) := \sum_{n=1}^{\infty} a_n(f)n^{-s}$. The Hecke estimate implies that $L(s,f)$ converges absolutely for $\Re(s) > k$. If f is a newform in $\mathcal{M}_k(\Gamma_0(N))$, then because of the nice formulas its Fourier coefficients obey one has an Euler product expansion

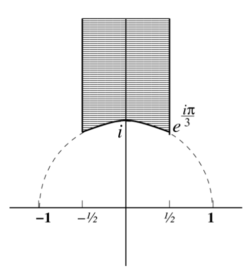
$$L(s,f) = \prod_p (1 - a_p(f)p^{-s} + \mathbb{1}_N(p)p^{1-2s})^{-1},$$

where $\mathbb{1}_N(p)$ is the trivial Dirichlet character modulo N that assigns 1 if p does not divide N, and assigns 0 otherwise. Furthermore, we have a functional equation for $L(s,f)$ that implies it has an analytic continuation to the complex plane. An analogous L-function can be defined for an elliptic curve E over $\mathbb{Q}$ with conductor N_E by

$$L(s,E) := \prod_p (1 - a_p(E)p^{-s} + \mathbb{1}_{N_E}(p)p^{1-2s})^{-1}.$$

The modularity theorem rephrases as follows: For every elliptic curve E over $\mathbb{Q}$ with conductor N_E, there exists a newform $f \in \mathcal{S}_2(\Gamma_0(N_E))$ such that $L(s,f) = L(s,E)$. In particular, the analytic continuation of $L(s,f)$ applies to $L(s,E)$ (so the modularity theorem immediately implies the Hasse-Weil conjecture for elliptic curves). Various other questions can be asked about this L-function. Of particular importance and significance is the Birch-Swinnerton-Dyer conjecture, which asks if the order of vanishing of $L(s,E)$ at $s=1$ equals the rank of $E(\mathbb{Q})$.

There is an important object that has not yet been mentioned: the modular curve. We will concentrate on this object in the remainder of this report summary. For a congruence subgroup Γ, one can let it act on the upper-half plane $\mathbb{H}$ and look at the quotient space $Y(\Gamma) := \Gamma \backslash \mathbb{H}$. The example $Y(\mathrm{SL}_2(\mathbb{Z}))$ is represented by the shaded area in the following well-known picture, where the sides are identified appropriately.



By adjoining the "cusps" to $Y(\Gamma)$ (i.e. the set $\mathbb{Q} \cup \{\infty\}$ up to Γ-equivalence, necessarily finitely many) and constructing appropriate charts, one compactifies $Y(\Gamma)$ into a compact Riemann surface $X(\Gamma) = \Gamma \setminus \mathbb{H}^*$, where we let $\mathbb{H}^* = \mathbb{C} \cup \mathbb{Q} \cup \{\infty\}$. This $X(\Gamma)$ is the *modular curve for* Γ. For example, the case $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ has only one cusp, and $X(\Gamma)$ is the sphere. Notice how this gives a geometric interpretation of the last condition in the definition of modular forms: we want modular form to be holomorphic at the cusps, and cusps forms are those vanishing at the cusps.

Define the space of automorphic forms $\mathcal{A}_k(\Gamma)$ in the same way as for $\mathcal{M}_k(\Gamma)$, by replacing the word "holomorphic" with "meromorphic". Thus, for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the Fourier coefficients of an automorphic form satisfy $a_{\gamma,n} = 0$ for $a_{\gamma,n} < m_\gamma$ and some $m_\gamma \in \mathbb{Z}$. Clearly $\mathcal{M}_k(\Gamma) \subset \mathcal{A}_k(\Gamma)$. In fact $\mathcal{A}_k(\Gamma) = \mathbb{C}(X(\Gamma))f$, where f is a nonzero element of $\mathcal{A}_k(\Gamma)$ (exists except the degenerate case where k is odd and $-I_2 \in \Gamma$) and $\mathbb{C}(X(\Gamma))$ is the field of meromorphic functions on $X(\Gamma)$. Hence, with a suitable definition of div, one has

$$\begin{aligned}\mathcal{M}_k(\Gamma) &= \{f_0 f \in \mathcal{A}_k(\Gamma) : f_0 f = 0 \text{ or } \mathrm{div}(f_0 f) \geq 0\} \\ &\cong \{f_0 \in \mathbb{C}(X(\Gamma)) : f_0 = 0 \text{ or } \mathrm{div}(f_0) + \mathrm{div}(f) \geq 0\}.\end{aligned}$$

This is the key reinterpretation of $\mathcal{M}_k(\Gamma)$ which allows us to compute its dimension via Riemann-Roch theorem. To compute the dimension of $\mathcal{S}_k(\Gamma)$ one replaces $\mathrm{div}(f)$ in the inequality above by $\mathrm{div}(f) - \sum_i \epsilon_i x_i$, where x_i are the cusp points and ϵ_i equals 1 or 1/2 accordingly if x_i is regular or irregular.

Another important example of how modular curves arise in the study of elliptic curves is another version of the modularity theorem (which we will call version $X_\mathbb{C}$): if E is a complex elliptic curve with rational j-invariant, then there exists a surjective holomorphic function $X(\Gamma_0(N)) \longrightarrow E$ for some positive integer N.

We can reinterpret the uncompactified modular curve $Y(\Gamma)$ by relating it with complex elliptic curves as follow. It can be shown that $Y(\Gamma_0(N))$ is in bijection with $S(\Gamma_0(N))$, the isomorphism classes of $[E, C]$, where $E = \mathbb{C}/\Lambda$ is a complex elliptic curve and C is a cyclic subgroup of order N. The bijection can be written down simply as $\Gamma\tau \longleftrightarrow [\mathbb{C}/\Lambda_\tau, 1/N]$, where $\Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$. In particular, isomorphism classes of elliptic curves are parametrized by $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$. Similarly, it can be shown that there is a bijection of $Y(\Gamma_1(N))$ with $S(\Gamma_1(N))$, the isomorphism classes of $[E, P]$, where P is a point of order N, by $\Gamma\tau \longleftrightarrow [\mathbb{C}/\Lambda_\tau, 1/N]$. Note that the isomorphism classes here are different from the previous case: here $[E, P]$ is isomorphic to $[E', P']$ if there is an isomorphism $E \cong E'$ that takes P to P', not just taking the cyclic group generated by P to that generated by P'. If we analogously define $\Gamma(N)$ by letting $* = 0$ in the definition of $\Gamma_1(N)$, then there is a bijection of $Y(\Gamma(N))$ with $S(\Gamma(N))$, the isomorphism classes of $[E, (P, Q)]$, where P, Q generates $E[N]$ with Weil pairing $e_N(P, Q) = e^{2\pi i/N}$, by $\Gamma\tau \longleftrightarrow [\mathbb{C}/\Lambda_\tau, (1/N, \tau/N)]$.

With the descriptions of $Y(\Gamma)$ in case $\Gamma \in \{\Gamma_0(N), \Gamma_1(N)\}$ as above, it allows us to define Hecke operators on $X(\Gamma)$ and $S(\Gamma)$ respectively, compatible with the Hecke operators on modular forms. After some work (background, with more equivalences of the modularity theorem in [1, chapters 6 to 8]) one can describe Hecke operators T_p on the Picard group $\mathrm{Pic}^0(X(\Gamma)_{\mathrm{alg}})$ of algebraic analogs $X(\Gamma)_{\mathrm{alg}}$ of the modular curve $X(\Gamma)$ and arrive at the Eichler-Shimura relation, allowing us to interpret T_p on $\mathrm{Pic}^0(X(\Gamma)_{\mathrm{alg}})$ using mod-p Frobenius maps for primes p not dividing N.

Remark 2. The Eichler-Shimura relation is implicitly used to construct two important Galois representations $\rho_E, \rho_f : G_\mathbb{Q} \longrightarrow \mathrm{GL}_2(K)$, for elliptic curves E over $\mathbb{Q}$ and for weight-two newforms f with respect to $\Gamma_0(N)$. Another version of the modularity theorem tells us that ρ_E is isomorphic to some ρ_f with more precise conditions. Wiles proved this version of modularity on semistable elliptic curves, after Ribet and Serre had proven it implies version $X_\mathbb{C}$ for $N = 2$. Assuming these hard results (or/and the more general modularity theorem), this is enough to imply Fermat's Last Theorem by constructing the Frey elliptic curve C_F for a solution to Fermat's equation, which one can easily show not to exist via applying the Riemann-Hurwitz formula to $X(\Gamma_0(2)) \longrightarrow C_F$ after noticing that $X(\Gamma_0(2))$ has genus zero by the dimension formulas.

References

[1] Fred Diamond and Jerry Shurman, *A First Course in Modular Forms*, Springer, 2005.

[2] Daniel Bump, "Chapter 1: Modular Forms', *Automorphic Forms and Representations*, Cambridge University Press, 1998.

[3] Paul Garrett, *Harmonic theta series and equidistribution*, notes available at `http://www.math.umn.edu/~garrett/m/mfms/notes_2013-14/10_thetas_equi.pdf`, last retrieved December 21, 2016.

[4] Goro Shimura, *Introduction to Arithmetic Theory of Automorphic Forms*, Princeton University Press, 1971.