ON SUPERSINGULAR ELLIPTIC CURVES OVER $\mathbf{F}_p$

TOMMASO GIORGIO CENTELEGHE

Abstract. For a prime number $p > 3$, we give a proof of the known formula relating the number of distinct isomorphisms classes of supersingular elliptic curves defined over $\mathbf{F}_p$ to the class number of $\mathbf{Q}(\sqrt{-p})$. The proof is an application of the gobal Jacquet–Langlands correspondence between GL_2 and the multiplicative group B^* of "the" definite quaternion algebra over $\mathbf{Q}$ ramified also at p.

1. Introduction

Let p be a prime number > 3. The aim of this note is to prove the following theorem.

Theorem 1.1. *Let $h_p^{(1)}$ be the number of isomorphism classes of supersingular elliptic curves over $\mathbf{F}_p$. Then*

$$h_p^{(1)} = \begin{cases} 2^{-1}h_{\sqrt{-p}}, & \text{if } p \equiv 1 \mod 4, \\ 2h_{\sqrt{-p}}, & \text{if } p \equiv 3 \mod 8, \\ h_{\sqrt{-p}}, & \text{if } p \equiv 7 \mod 8. \end{cases}$$

Where $h_{\sqrt{-p}}$ is the class number of the imaginary quadratic field $Q\sqrt{-p}$.

The theorem was known since the classical work of Eichler in the context of the basis problem for the space of modular forms of given weight and level. Eichler shows that traces of Hecke operators are the same as those of certain Brandt matrices. The above theorem consists in the equality between the trace of the p–th Hecke operator T_p acting on $\mathbf{M}_2(\Gamma_0(p))$, and the trace of the p–th Brandt matrix. An excellent exposition of Eichler's work can be found in the first sections of [4].

The proof that we give here is an application of the global Jacquet–Langlands correspondence between certain cusp forms on GL_2 and on the multiplicative group B^* of the quaternion algebra over $\mathbf{Q}$ ramified precisely at p and infinity.

2. Two involutions

By an involution σ on a finite dimensional complex vector space V, we shall mean a $\mathbf{C}$–linear automorphism of V whose square is the identity. The first involution that we want to consider is that given by the Atkin–Lehner operator W_p on the space of classical, weight 2 cusp forms $\mathbf{M}_2^0(\Gamma_0(p))$. Explicitely,

$$W_p(f) = f|_2\gamma, \quad \text{where } \gamma = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix}.$$

Here the symbol $f|_2\alpha$, for $\alpha \in \mathrm{GL}_2^+(\mathbf{Q})$, denotes the usual slash operator in weight 2 on functions on the upper half plane (cf. [6]). It is well known that $W_p = -T_p$, where T_p is the p–th Hecke operator on the space of cusps forms $\mathbf{M}_2^0(\Gamma_0(p))$.

The dimension of the space $\mathbf{M}_2^0(\Gamma_0(p))$, which is equal to the genus g of the modular curve $X_0(p)$, is described by (cf. [6])

$$12g = \begin{cases} p-1, & \text{if } p \equiv 1 \mod 12, \\ p-5, & \text{if } p \equiv 5 \mod 12, \\ p-7, & \text{if } p \equiv 7 \mod 12, \\ p+1, & \text{if } p \equiv 11 \mod 12. \end{cases} \tag{1}$$

Let $h_{\sqrt{-p}}$ be the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$.

Proposition 2.1. *The dimension g^+ of the eigenspace $\mathbf{M}_2^0(\Gamma_0(p))^+$ of W_p with respect to the eigenvalue 1 is described by*

$$4g^+ = \begin{cases} 2g+2-h_{\sqrt{-p}}, & \text{if } p \equiv 1 \mod 4, \\ 2g+2-4h_{\sqrt{-p}}, & \text{if } p \equiv 3 \mod 8, \\ 2g+2-2h_{\sqrt{-p}}, & \text{if } p \equiv 7 \mod 8, \end{cases}$$

Proof. Let $\overline{\Gamma}_0(p) = \Gamma_0(p)/\{\pm 1_2\}$ be the projective image of $\Gamma_0(p)$ in $\mathrm{PGL}_2(\mathbf{Q})$, and let $\overline{\Gamma}_0^+(p)$ be the subgroup of $\mathrm{PGL}_2(\mathbf{Q})$ generated by the image of γ and by $\overline{\Gamma}_0(p)$. Since conjugation by γ on $\mathrm{GL}_2(\mathbf{Q})$ stabilizes $\Gamma_0(p)$, and $\gamma^2 = -p{\cdot}1_2$ is scalar, we see that

$$\overline{\Gamma}_0^+(p) \simeq \overline{\Gamma}_0(p) \rtimes \mathbf{Z}/2,$$

where the semi–direct product structure is described by the automorphism of $\overline{\Gamma}_0(p)$ induced by conjugation by γ.

The groups $\overline{\Gamma}_0(p)$ and $\overline{\Gamma}_0^+(p)$ are discrete subgroups of $\mathrm{PGL}_2(\mathbf{R})$, they act naturally on the upper half plan $\mathcal{H}$. Let $X_0(p)$ (resp. $X_0^+(p)$) be the canonical compactification of the open Riemann surface $\overline{\Gamma}_0(p)\backslash\mathcal{H}$ (resp. $\overline{\Gamma}_0^+(p)\backslash\mathcal{H}$) (cf. [6]). There is a natural two fold ramified covering

$$\phi : X_0(p) \to X_0^+(p),$$

induced by the inclusion $\overline{\Gamma}_0(p) \subset \overline{\Gamma}_0^+(p)$.

The space $\mathbf{M}_2^0(\Gamma_0(p))$ can be identified with the space of holomorphic differential forms on $X_0(p)$, the subspace

$$\mathbf{M}_2^0(\Gamma_0(p))^+ \subset \mathbf{M}_2^0(\Gamma_0(p)),$$

consists of those holomorphic one–forms that descend to $X_0^+(p)$. Therefore g^+ is equal to the genus of $X_0^+(p)$.

The genera g and g^+ are related to each other by the Riemann–Hurwtiz formula. In this case, the formula takes the form

$$4g^+ = 2g + 2 - \Sigma, \tag{2}$$

where Σ denotes the number of points of $X_0(p)$ at which ϕ is ramified. The map ϕ identifies the two cusps of $X_0(p)$ with that of $X_0^+(p)$, and it is therefore unramified at infinity. Its ramification points are in correspondence with the orbits $\overline{\Gamma}_0(p)z_0$ in $\overline{\Gamma}_0(p)\backslash\mathcal{H}$ so that the equality

$$\overline{\Gamma}_0(p)z_0 = \overline{\Gamma}_0(p)\gamma.z_0 \tag{3}$$

holds in $\overline{\Gamma}_0(p)\backslash\mathcal{H}$.

Using now the interpretation of the open Riemann Surface $\overline{\Gamma}_0(p)\backslash\mathcal{H}$ as moduli of complex elliptic curves equipped with an order p subgroup, one sees that an orbit $\overline{\Gamma}_0(p)z_0$ satisfies equation 3 if and only if the corresponding point (E, C) in the moduli space is so that

i) E admits an isogeny $\pi_E : E \to E$ so that $\pi_E^2 = -p$;

ii) the order p subgroup C is the kernel of π_E.

Thus the total number of orbits of $\overline{\Gamma}_0(p)\backslash\mathcal{H}$ satisfying 3 is equal to the number of isomorphism classes of complex elliptic curves E so that the order $\mathbf{Z}[\sqrt{-p}]$ embeds in $\mathrm{End}_{\mathbf{C}}(E)$. We have

$$\Sigma = \begin{cases} h(-4p) & \text{if } p \equiv 1 \mod 4, \\ h(-p) + h(-4p) & \text{if } p \equiv 3 \mod 4, \end{cases}$$

where, for a negative integer $d \equiv 0, 1 \bmod 4$, $h(d)$ denotes the class number of the imaginary quadratic order of discriminant d. If $p \equiv 3 \bmod 4$, then the discriminant $h(-4p)$ of the (non–maximal) order $\mathbf{Z}[\sqrt{-p}]$ is related to $h(-p)$ (cf. [2], thm 7.24), and we obtain

$$\Sigma = \begin{cases} h(-4p) & \text{if } p \equiv 1 \mod 4, \\ 4h(-p) & \text{if } p \equiv 3 \mod 8, \\ 2h(-p) & \text{if } p \equiv 7 \mod 8, \end{cases}$$

completing the proof of the proposition. □

We have obtained a description of the spectrum of W_p (and hence of T_p) in terms of the class number of a quadratic field: the characteristic polynomial of T_p acting on $\mathbf{M}_2^0(\Gamma_0(p))$ is

$$P_{T_p}(x) = (x+1)^{g^+}(x-1)^{g-g^+}. \tag{4}$$

Thank to equations 1 and proposition 2.1, g^+ and $g - g^+$ are explicit arithmetic functions of p involving $h_{\sqrt{-p}}$.

Consider now the set Ω_p of isomorphism classes of supersingular elliptic curves over $\overline{\mathbf{F}}_p$, and let V_p the space of complex valued functions on Ω_p. It is well–known that Ω_p is a finite set and that, moreover, every supersingular elliptic curve E admits a model over the quadratic extension $\mathbf{F}_{p^2} \subset \overline{\mathbf{F}}_p$ of the prime field. Let $h_p^{(1)}$ be the number of isomorphism classes of supersingular elliptic curves that admit a model over $\mathbf{F}_p$, and let $h_p^{(2)}$ be the number of supersingular invariants j_E so that $j_E \in \mathbf{F}_{p^2} \smallsetminus \mathbf{F}_p$.

For a supersingular elliptic curve E defined over $\mathbf{F}_{p^2}$, denote by $E^{(p^n)}$ be its twist by the the n–th power of the absolute frobenius, we have that $E^{(p^2)} \simeq E$. Let $F : V_p \to V_p$ be the involution of V_p so that

$$F(\varphi)(E) = \varphi(E^{(p)}).$$

Let V_p^0 be the subspace of V_p consisting of those functions φ so that

$$\sum_{E \in \Omega_p} \varphi(E) = 0.$$

We have that V_p^0 has codimension one in V_p and it is preserved by F. Denote by $F^{(0)}$ the restriction of F to V_p^0. It is now easy to see that

Proposition 2.2. *The characteristic polynomial of $F^{(0)}$ is*

$$P_{F^{(0)}}(x) = (x-1)^{h_p^{(1)}+2^{-1}h_p^{(2)}}(x+1)^{2^{-1}h_p^{(2)}}.$$

In the next section, theorem 1.1 will be proved by showing that the involutions T_p and $F^{(0)}$ have the same characteristic polynomials. Besides a classical theorem of Deuring relating supersingular elliptic curves to a certain quaternion algebra over $\mathbf{Q}$, the fundamental ingredient used is, as already said, the Jacquet–Langlands global correspondence.

3. $T_p \simeq F^{(0)}$

Let B be the quaternion algebra over $\mathbf{Q}$ ramified precisely at p and infinity, and let B^* be its multiplicative group. For any prime number ℓ, we let B^*_ℓ denote the group of $\mathbf{Q}_\ell$–valued points of B^*; by definition of B, we have that B^*_ℓ is isomorphic to $\mathrm{GL}_2(\mathbf{Q}_\ell)$ for $\ell \neq p$, and to the multiplicative group of the unique quaternion division algebra over $\mathbf{Q}_p$ for $\ell = p$.

Consider the group $\mathrm{B}^*_{\hat{\mathbf{Z}}}$ of points of B^* valued in the ring of finite adèles $\hat{\mathbf{Z}}$. Let $K = \prod K_\ell$ be a maximal compact subgroup of $\mathrm{B}^*_{\hat{\mathbf{Z}}}$, where, for a prime number ℓ, $K_\ell \subset \mathrm{B}^*_\ell$ is a maximal compact subgroup of B^*_ℓ. The double coset $B^*_{\mathbf{Q}}\backslash \mathrm{B}^*_{\hat{\mathbf{Z}}}/K$ is a finite set, let S_p denote the space of functions

$$\varphi : B^*_{\mathbf{Q}}\backslash \mathrm{B}^*_{\hat{\mathbf{Z}}}/K \longrightarrow \mathbf{C}.$$

The automorphic representation Π' of B^* generated by the right translation action of the adelic points of B^* on S_p decomposes as

$$\Pi' \simeq \oplus_{1\leq i\leq n} m_i \pi'_i,$$

where π'_i ranges in the finite list of irreducible cusp forms π'_i appearing in Π'. By the maximality of K, the central character of each of the π'_i's is trivial. A consequence of the global Jacquet–Langlands correspondence (cf. [3], [5]) is that the multiplicity one statement for which $m_i = 1$, for all $1 \leq i \leq n$.

Let now $\pi'_i \simeq \otimes' \pi'_{i,\nu}$ be restricted tensor product decomposition of π'_i into representations of the local groups B^*_ℓ and $\mathrm{B}^*_{\mathbf{R}}$, as ν varies among all the places of $\mathbf{Q}$. We have that $\mathrm{B}^*_{\mathbf{R}}$ is the one–dimensional trivial representation.

Since K_p is normal in B^*_p, for each i in $(1,\ldots,n)$, the representation $\pi'_{i,p}$ is trivial on K_p, and it is therefore described by a character

$$\Psi_i : \mathrm{B}^*_p \longrightarrow \mathbf{Q}^*_p \longrightarrow \mathbf{C}^*$$

that factors through the reduced norm map $N : B_p^* \to \mathbf{Q}_p^*$. If $\omega \in \mathrm{B}_p^*$ is a uniformizer, Ψ is uniquely determined by the value $\Psi_i(\omega)$, where $\omega \in \mathrm{B}_p^*$ is a uniformizer. Moreover, $\Psi_i(\omega^2) = \Psi_i(p)$ is equal to 1 since π_i' has trivial character, hence $\Psi_i(\omega) \in \{\pm 1\}$.

Consider the uniformized ω as an element of $\mathrm{B}_{\hat{\mathbf{Z}}}^*$, thank to the embedding $\mathrm{B}_p^* \subset \mathrm{B}_{\hat{\mathbf{Z}}}^*$. The upshot of what we said is that the involution ϵ of S_p defined by

$$\epsilon(\varphi)(B_{\mathbf{Q}}^* \cdot x \cdot K) = \varphi(B_{\mathbf{Q}}^* \cdot x\omega \cdot K)$$

encoded information about the types at p of the cusp forms π_i''s. More precisely,

$$\mathrm{trace}(\epsilon) = \mathrm{s}^+ - \mathrm{s}^-,$$

where s^+ (resp. s^-) denotes the number of cusp forms π_i' so that its component at p satisfies $\Psi_i(\omega) = 1$ (resp. $\Psi_i(\omega) = -1$).

By a classical theorem of Deuring (cf. [4] for more details) there exists a bijection between the set Ω_p introduced in section 2 and the double coset $B_{\mathbf{Q}}^* \backslash \mathrm{B}_{\hat{\mathbf{Z}}}^* / K$. Moreover, if we let $D : V_p \to S_p$ denote the induced identification of V_p and S_p we have

Proposition 3.1. *The linear isomorphism $D : V_p \to S_p$ intertwines the involutions F and ϵ.*

We are now only left with applying the Jacquet–Langlands correspondence to the infinite dimensional cusp forms that appear in the decomposition of Π'. This enables us to link the involution ϵ on S_p to the p–th Hecke operator on $\mathbf{M}_2^0(\Gamma_0(p))$.

Let $\chi : \mathbf{Q}_p^* \to \mathbf{C}^*$ be a character. The local Jacquet–Langlands correspondant of the one dimensional representation of B_p^* given by

$$\chi \cdot N : B_p^* \longrightarrow \mathbf{Q}_p^* \longrightarrow \mathbf{C}^*$$

is the special representation $\mathrm{St}(\chi)$. Here $\mathrm{St}(\chi)$ is the unique infinite dimensional irreducible submodule of the representation $\mathrm{Ind}(\chi||^{1/2}, \chi||^{-1/2})$ of $\mathrm{GL}_2(\mathbf{Q}_p)$ induced by the character $(\chi||^{1/2}, \chi||^{-1/2})$ of the Borel subgroup of upper triangular matrices.

If π_i' is an infinite dimensional cusp form appearing in Π', then its Jacquet–Langlands correspondant is a certain unitary cusp form π_{f_i} on GL_2 that is

i) discrete series of weight 2 at infinity;

ii) special at p of conductor p;

iii) of trivial central character.

Fact ii) follows from an explicit analysis of the conductor of special representations. Therefore π_{f_i} is associated with a normalized cuspidal eigenform $f_i \in \mathbf{M}_2^0(\Gamma_0(p))$. Conversely, it is easy to see that every normalized eigenform $f \in \mathbf{M}_2^0(\Gamma_0(p))$ gives rise to an automorphic representation π_f of GL_2 satisfying i), ii) and iii) above.

In particular, the type at p of π_f is always of type $\mathrm{St}(\chi)$, where χ is either the trivial character of $\mathbf{Q}_p^*$, or is its unramified quadratic character. Accordingly, we will write $\chi = 1$ or $\chi = -1$.

Using this convention, a calculation shows that if $\mathrm{St}(\chi)$ is the type at p of π_f, then $\chi = a_p(f)$, the p–th eigenvalue of the Hecke operator associated with f (cf. [1] p. 119).

Finally, since the only finite dimensional cusp form π_i' of B^* appearing in the decomoposition of Π' is the one–dimensional trivial character, the global Jacquet–Langlands correspondence gives us

Proposition 3.2. *The involutions ϵ on S_p and $T_p \oplus \mathrm{Id}_{\mathbf{C}}$ on $\mathbf{M}_2^0(\Gamma_0(p)) \oplus \mathbf{C}$ have the same characteristic polynomial. Therefore the characteristic polynomial of T_p equal that of $F^{(0)}$.*

The equality between $P_{T_p}(x)$ in equation 4 and $P_{F^{(0)}}(x)$ in proposition 2.2 establishes the seeked relation between the class number $h_{\sqrt{-p}}$ and $h_p^{(1)}$, the number of supersingular invariants of the prime field. Thus completing the proof of theorem 1.1.

References

1. W. Casselman, *On representations of* GL_2 *and the arithmetic of modular curves*, Modular Functions of One Variable II, Lecture Notes in Math. **349**, Springer–Verlag, 107–141 (1973).
2. D. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, (1989).
3. S. Gelbart, *Automorphic Forms on Adele Groups*, Princeton University Press, 1975.
4. B. Gross, *Heights and the Special Values of L–series*, Number Theory, CMS Conference Proceedings **7**, 115–187 (1987).
5. J. Rogawski, *Modular forms, the Ramanujan conjecture and the Jacquet-Langlands correspondence*, Available at http://www.math.ucla.edu/ jonr/eprints.html
6. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Pressm, 1971.