Counting supersingular curves via the Langlands-Kottwitz method, following Scholze

Avi Zeff

The various modular curves $X(N)$, $X_0(N)$, etc. are moduli spaces for (generalized) elliptic curves with certain level structures. In section 5 of [1], Scholze shows how we can count points on $X(N)(k)$ isogenous to a given curve E_0/k in terms of orbital integrals, for k a finite field; we'll go over his method and see how we can modify it to count supersingular points of $X_0(N)(k)$.

First: it is well-known that all supersingular curves over k are isogenous, and that if $f : E_0 \to E$ is an isogeny then E is supersingular if and only if E_0 is. Thus to count supersingular curves over k it suffices to fix a single such curve E_0 and count isogenies $f : E_0 \to E$ up to isomorphism. Write $X(N)(k)(E_0)$ for the set of isomorphism classes of curves E over k with level N structure, i.e. points of $X(N)(k)$, equipped with isogenies $f : E_0 \to E$ defined over k, and similarly for $X_0(N)$.

We're now ready to introduce Scholze's method. Let $q = p^r = |k|$, and assume that $p \nmid N$. Write $\mathbb{Q}_q = \mathbb{Q}_{p^r}$ for the unramified extension of $\mathbb{Q}_p$ of degree r, and $\mathbb{Z}_q = \mathbb{Z}_{p^r} = W(\mathbb{F}_q)$ for its ring of integers. Let $\mathbb{A}_f^p$ be the ring of finite adeles with trivial p-component, and similarly let $\widehat{\mathbb{Z}}^p = \prod_{\ell \neq p} \mathbb{Z}_\ell$. Define

$$H^p = H^1_{\text{ét}}(E_0, \mathbb{A}_f^p), \qquad H_p = H^1_{\text{crys}}(E_0/\mathbb{Z}_q) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q.$$

Letting $G_k = \text{Gal}(\overline{k}/k)$, note that H^p carries an action of G_k, generated by the action of the Frobenius Φ_k; and H_p is equipped with a Frobenius F and a Verschiebung V, satisfying $FV = VF = p$. Given an isogeny $f : E_0 \to E$, we can define a G_k-invariant $\widehat{\mathbb{Z}}^p$-lattice $L \subset H^p$ by

$$L = f^* H^1_{\text{ét}}(E, \widehat{\mathbb{Z}}^p)$$

and an F, V-invariant $\mathbb{Z}_q$-lattice $\Lambda \subset H_p$ by

$$\Lambda = f^* H^1_{\text{crys}}(E/\mathbb{Z}_q).$$

Since E_0 and E are equipped with level N structure, which for $X(N)$ means isomorphisms $\phi_0 : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E_0[N]$ and $\phi : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N]$, we have

$$H^1_{\text{ét}}(E, \widehat{\mathbb{Z}}^p) \otimes \mathbb{Z}/N\mathbb{Z} \simeq E[N]$$

and so we get an induced isomorphism $\phi_L : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} L \otimes \mathbb{Z}/N\mathbb{Z}$.

Denote by Y^p the set of all G_k-invariant $\widehat{\mathbb{Z}}^p$-lattices $L \subset H^p$ equipped with isomorphisms $\phi_L : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} L \otimes \mathbb{Z}/N\mathbb{Z}$, and by Y_p the set of all F, V-invariant $\mathbb{Z}_q$-lattices $\Lambda \subset H_p$. Let $B = \text{End}(E_0) \otimes \mathbb{Q}$ be the endomorphism algebra, which since E_0 is supersingular is a quaternion algebra. Then $B^\times$ acts on $Y^p \times Y_p$: if u is an honest endomorphism of E_0 and m is a nonzero integer, then $\frac{u}{m} \cdot L = \frac{1}{m} u^*(L)$, and analogously on ϕ_L and Λ. Fixing an isogeny $f : E_0 \to E$ (with level structure) gives a choice of each of L, ϕ_L, and Λ as above; since we want to allow f to vary over all isogenies $E_0 \to E$, we can replace it by its composition with any element of $B^\times$, which changes the resulting (L, ϕ_L, Λ) by the corresponding action of $B^\times$. Thus we get a map

$$X(N)(k)(E_0) \to B^\times \backslash Y^p \times Y_p.$$

Theorem 1. *This map is a bijection.*

Proof. First, we show that it is injective: suppose that $f_1 : E_0 \to E_1$, $f_2 : E_0 \to E_2$ yield the same element of $Y^p \times Y_p$ up to the action of $B^\times$, i.e. there exists $\frac{u}{m} \in B^\times$ such that $f_1^* H^1_{\text{ét}}(E_1, \widehat{\mathbb{Z}}^p) = \frac{u}{m} \cdot f_2^* H^1_{\text{ét}}(E_2, \widehat{\mathbb{Z}}^p)$, $m\phi^1_L = u\phi^2_L$ with the obvious notation, and $f_1^* H^1_{\text{crys}}(E_1/\mathbb{Z}_q) = \frac{u}{m} f_2^* \cdot H^1_{\text{crys}}(E_2/\mathbb{Z}_q)$. We can replace f_1 by $f_1 \circ u$ and f_2 by mf_2 and still have isogenies $E_0 \to E_1, E_2$, so we can assume that in fact $f_1 : E_0 \to E_1$ and $f_2 : E_0 \to E_2$ have the same image in $Y^p \times Y_p$.

In $\text{Hom}(E_0, E_1) \otimes \mathbb{Q}$ and $\text{Hom}(E_0, E_2) \otimes \mathbb{Q}$, each of f_1 and f_2 are invertible and so we obtain elements $f_1 f_2^{-1} \in \text{Hom}(E_2, E_1) \otimes \mathbb{Q}$ and $f_2 f_1^{-1} \in \text{Hom}(E_1, E_2) \otimes \mathbb{Q}$. Our goal is to show that in fact these are honest isogenies in $\text{Hom}(E_2, E_1)$ and $\text{Hom}(E_1, E_2)$ respectively, and therefore define inverse morphisms; this implies that E_1 and E_2 are isomorphic as desired.

Set $f = f_1 f_2^{-1} \in \text{Hom}(E_2, E_1) \otimes \mathbb{Q}$, and let M be an integer such that Mf is an honest isogeny $E_2 \to E_1$. We get an induced map $(Mf)^* : H^1_{\text{crys}}(E_1/\mathbb{Z}_q) \to H^1_{\text{crys}}(E_2/\mathbb{Z}_q)$ of Dieudonné modules. By Dieudonné theory there exist corresponding finite p-group schemes G_1 and G_2 to $H^1_{\text{crys}}(E_1/\mathbb{Z}_q)$ and $H^1_{\text{crys}}(E_2/\mathbb{Z}_q)$ respectively, and by (contravariant) functoriality we get an induced map $(Mf)_* : G_2 \to G_1$. For each $i \in \{1, 2\}$, pullback by f_i gives an inclusion $H^1_{\text{crys}}(E_i/\mathbb{Z}_q) \hookrightarrow H^1_{\text{crys}}(E_0, \mathbb{Z}_q)$, up to possibly rescaling by elements of $B^\times$; and by assumption these have the same image in $H^1_{\text{crys}}(E_0, \mathbb{Z}_q)$. Therefore G_2 and G_1 are subgroups of E_0 and therefore abelian, and $(Mf)_*$ is an isomorphism. In particular multiplication by M induces an isomorphism on G_1 and so we can invert it to get a map $f_* : G_2 \to G_1$, which by the antiequivalence between Dieudonné modules and finite p-group schemes gives a morphism $f^* H^1_{\text{crys}}(E_1, \mathbb{Z}_q) \to H^1_{\text{crys}}(E_2, \mathbb{Z}_q)$ such that if we write M^* for the endomorphism of $H^1_{\text{crys}}(E_1, \mathbb{Z}_q)$ induced by multiplication by M then $f^* M^* = (Mf)^*$.

Similarly, we have an induced map $(Mf)^* : H^1_{\text{ét}}(E_1, \widehat{\mathbb{Z}}^p) \to H^1_{\text{ét}}(E_2, \widehat{\mathbb{Z}}^p)$. The étale covers of E_1 are given by isogenies $E_1' \to E_1$ and similarly for E_2, so this gives a map $(E_1' \to E_1) \mapsto (E_1' \to E_1 \xrightarrow{(Mf)^\vee} E_2)$. By assumption, pulling back both sides by f_1 and f_2 respectively gives the same lattice in H^p, so $(Mf)^*$ is an isomorphism; therefore similarly we can invert M to see that this factors through M^*. Together with the above we see that the action of Mf on cohomology over every prime factors through multiplication by M, which implies that so does Mf itself; therefore f is a genuine isogeny. The same argument applies to $f_2 f_1^{-1}$, so we conclude that these are inverse isogenies and so E_1 and E_2 are isomorphic. Since by assumption the induced level structures on $H^1_{\text{ét}}(E_i, \widehat{\mathbb{Z}}^p)$ are the same, this isomorphism takes the level structures to each other and so E_1 and E_2 are in the same isomorphism class in $X(N)(k)$.

For surjectivity, fix a triple $(L, \phi_L, \Lambda) \in Y^p \times Y_p$. We can rescale L and Λ by $\mathbb{Q}^\times \subset B^\times$ such that $L \subseteq H^1_{\text{ét}}(E_0, \widehat{\mathbb{Z}}^p)$ and $\Lambda \subseteq H^1_{\text{crys}}(E_0/\mathbb{Z}_q)$. By the theory of Dieudonné modules, since Λ is F, V-invariant it corresponds to some finite group scheme G_p of p-power order, and the inclusion $\Lambda \subset H^1_{\text{crys}}(E_0/\mathbb{Z}_q)$ by functoriality gives an injection $G_p \hookrightarrow E_0$; étale covers of E_0 consist of isogenies $E' \to E_0$, and so any sublattice L cuts out a cofinite set of such isogenies, the intersections of the kernels of the duals of which form a subgroup G^p of E_0 of order prime to p. There is a unique elliptic curve E equipped with an isogeny $f : E_0 \to E$ with kernel G^pG_p; by construction $f^*H^1_{\text{ét}}(E, \widehat{\mathbb{Z}}^p)$ is the sublattice of $H^1_{\text{ét}}(E_0, \widehat{\mathbb{Z}}^p)$ corresponding the the prime-to-p part of $\ker f$, i.e. G_p, which is L by definition, and similarly $f^*H^1_{\text{crys}}(E/\mathbb{Z}_q)$ is the Dieudonné submodule of $H^1_{\text{crys}}(E_0/\mathbb{Z}_q)$ corresponding to the p-part of $\ker f$, i.e. G^p, which is Λ. Since $L \otimes \mathbb{Z}/N\mathbb{Z} \simeq E[N]$ as above, ϕ_L then provides a level N structure on E. This gives a preimage for (L, ϕ_L, Λ) in $X(N)(k)(E_0)$. □

With this theorem in hand, we can decompose the size of $X(N)(k)(E_0)$, or equivalently $B^\times\backslash Y^p \times Y_p$, into a product of terms from each prime. Observe that (non-canonically) $H^p = H^1_{\text{ét}}(E_0, \mathbb{A}^p_f) \cong (\mathbb{A}^p_f)^2$, and so after choosing a basis the induced Frobenius Φ_k can be viewed as an element $\gamma \in \mathrm{GL}_2(\mathbb{A}^p_f)$. On H_p, the Frobenius F is only p-linear, but if we precompose with the lift σ of Frobenius to $\mathbb{Z}_q$ we can find $\delta \in \mathrm{GL}_2(\mathbb{Q}_q)$ such that $F = \delta\sigma$. Let $G_\gamma(\mathbb{A}^p_f)$ be the centralizer of γ, i.e.

$$G_\gamma(\mathbb{A}^p_f) = \{g \in \mathrm{GL}_2(\mathbb{A}^p_f) | g^{-1}\gamma g = \gamma\},$$

and let $G_{\delta\sigma}$ be the twisted centralizer of δ

$$G_{\delta\sigma}(\mathbb{Q}_p) = \{h \in \mathrm{GL}_2(\mathbb{Q}_q) | h^{-1}\delta h^\sigma = \delta\}.$$

For any prime $\ell \neq p$ and smooth function f with compact support on $\mathrm{GL}_2(\mathbb{Q}_\ell)$, let γ_ℓ be the ℓth component of γ, $G_\gamma(\mathbb{Q}_\ell)$ be the centralizer of γ_ℓ in $\mathbb{Q}_\ell$, and for any smooth function f with compact support on $\mathrm{GL}_2(\mathbb{Q}_\ell)$ set

$$\mathrm{O}^\ell_\gamma(f) = \int_{G_\gamma(\mathbb{Q}_\ell)\backslash \mathrm{GL}_2(\mathbb{Q}_\ell)} f(g^{-1}\gamma g)\, dg$$

after choosing a Haar measure on $\mathrm{GL}_2(\mathbb{Q}_\ell)$. Similarly for a smooth function ϕ compactly supported on $\mathrm{GL}_2(\mathbb{Q}_q)$ set

$$\mathrm{TO}_{\delta\sigma}(\phi) = \int_{G_{\delta\sigma}(\mathbb{Q}_p)\backslash \mathrm{GL}_2(\mathbb{Q}_q)} \phi(h^{-1}\delta h^\sigma)\, dh.$$

Set $G(\mathbb{A}_f) = G_\gamma(\mathbb{A}^p_f) \times G_{\delta\sigma}(\mathbb{Q}_p)$, so that $B^\times$ embeds into $G(\mathbb{A}_f)$ via its action on $Y^p \times Y_p$ above.

Let

$$K_\ell = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell) | a \equiv d \equiv 1, b \equiv c \equiv 0 \pmod{N} \right\}$$

and

$$K_p = \mathrm{GL}_2(\mathbb{Z}_q) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_q),$$

and let f_ℓ be the indicator function of K_ℓ divided by its volume and ϕ_p be the indicator function of K_p, where we choose Haar measures so that $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathrm{GL}_2(\mathbb{Z}_q)$ have volume 1. Then we have the following.

Corollary 2. *The cardinality of* $X(N)(k)(E_0)$ *is given by*

$$\mathrm{vol}(B^\times\backslash G)\cdot \mathrm{TO}_{\delta\sigma}(\phi_p)\cdot\prod_{\ell\neq p}\mathrm{O}^\ell_\gamma(f_\ell).$$

Proof. Set $K^p=\prod_{\ell\neq p}K_\ell$, with indicator function (divided by volume) $f^p=\prod_{\ell\neq p}f_\ell$. Then by the usual arguments for adelic quotients with level structure $\mathrm{GL}_2(\mathbb{A}_f^p)/K^p$ is in bijection with the set of lattices $L\subset(\mathbb{A}_f^p)^2$, which we can identify with H^p, together with an isomorphism $\phi:(\mathbb{Z}/N\mathbb{Z})^2\xrightarrow{\sim}L\otimes\mathbb{Z}/N\mathbb{Z}$. To restrict to those which are G_k-invariant, we additionally require that a coset $gK^p\in\mathrm{GL}_2(\mathbb{A}_f^p)/K^p$ be Frobenius-invariant, i.e. $\gamma gK^p=gK^p$, or equivalently $g^{-1}\gamma g\in K^p$.

Similarly, $\mathrm{GL}_2(\mathbb{Q}_q)/\mathrm{GL}_2(\mathbb{Z}_q)$ is in bijection with the set of lattices $\Lambda\subset\mathbb{Q}_q^2\simeq H_p$, and to restrict to those cosets hK_p which correspond to F,V-invariant lattices we require $Fh\,\mathrm{GL}_2(\mathbb{Z}_q)\subseteq h\,\mathrm{GL}_2(\mathbb{Z}_q)$ and $Vh\,\mathrm{GL}_2(\mathbb{Z}_q)\subseteq h\,\mathrm{GL}_2(\mathbb{Z}_q)$, or equivalently (since $FV=p$)

$$ph\,\mathrm{GL}_2(\mathbb{Z}_q)\subseteq Fh\,\mathrm{GL}_2(\mathbb{Z}_q)\subseteq h\,\mathrm{GL}_2(\mathbb{Z}_q),$$

or

$$p\,\mathrm{GL}_2(\mathbb{Z}_q)\subseteq h^{-1}\delta h^\sigma\,\mathrm{GL}_2(\mathbb{Z}_q)\subseteq \mathrm{GL}_2(\mathbb{Z}_q).$$

This condition is equivalent to $h^{-1}\delta h^\sigma\in\mathrm{GL}_2(\mathbb{Z}_q)\begin{pmatrix}p&0\\0&1\end{pmatrix}\mathrm{GL}_2(\mathbb{Z}_q)=K_p$.

Thus all in all letting $\mathbb{1}_{K^p}$ and $\mathbb{1}_{K_p}$ be the indicator functions of K^p and K_p respectively we have

$$\begin{aligned}|B^\times\backslash Y^p\times Y_p|&=\int_{B^\times\backslash(\mathrm{GL}_2(\mathbb{A}_f^p)/K^p)\times(\mathrm{GL}_2(\mathbb{Q}_q)/\mathrm{GL}_2(\mathbb{Z}_q))}\mathbb{1}_{K^p}(g^{-1}\gamma g)\mathbb{1}_{K_p}(h^{-1}\delta h^\sigma)\,dg\,dh\\&=\int_{B^\times\backslash\mathrm{GL}_2(\mathbb{A}_f^p)\times\mathrm{GL}_2(\mathbb{Q}_q)}f^p(g^{-1}\gamma g)\phi_p(h^{-1}\delta h^\sigma)\,dg\,dh\\&=\int_{B^\times\backslash G_\gamma(\mathbb{A}_f^p)\times G_{\delta\sigma}(\mathbb{Q}_p)}dv\cdot\int_{G_\gamma(\mathbb{A}_f^p)\backslash\mathrm{GL}_2(\mathbb{A}_f^p)}f^p(g^{-1}\gamma g)\,dg\cdot\int_{G_{\delta\sigma}(\mathbb{Q}_p)}\phi_p(h^{-1}\delta h^\sigma)\,dh\\&=\mathrm{vol}(B^\times\backslash G)\cdot\mathrm{TO}_{\delta\sigma}(\phi_p)\cdot\prod_{\ell\neq p}\mathrm{O}^\ell_\gamma(f^\ell).\end{aligned}$$

Combining this with Theorem 1 concludes the proof. □

To get an analogous formula for $X_0(N)$, we first need to replace Y^p and Y_p by new sets, say Z^p and Z_p, such that there is a bijection $X_0(N)(k)(E_0)\to B^\times\backslash Z^p\times Z_p$. Fix an isogeny $f:E_0\to E$ with both E_0 and E equipped with level structure corresponding to $X_0(N)$, i.e. isogenies $g_0:E_0\to E_0'$, $g:E\to E'$ of degree N. The lattices $L=f^*H^1_{\text{ét}}(E,\widehat{\mathbb{Z}}^p)$ and $\Lambda=f^*H^1_{\text{crys}}(E/\mathbb{Z}_q)$ are independent of the level structure and so are the same as above, and in particular we can set $Z_p=Y_p$; but we no longer have our isomorphism ϕ_L. Instead, the obvious structure induced by the level structure on E is the sublattice $g^*f^*H^1_{\text{ét}}(E,\widehat{\mathbb{Z}}^p)\subset L$. Since g is a degree N isogeny, this is an index N sublattice; and like L it is Galois-invariant. Thus our guess for a replacement for Y^p is the set Z^p of G_k-invariant lattices L of H^p equipped with a G_k-invariant sublattice $L'\subset L$ of index N. As above, quotienting by the choice of f gives a map

$$X_0(N)(k)(E_0)\to B^\times\backslash Z^p\times Z_p.$$

Theorem 3. *This map is again a bijection.*

Proof. The proof of Theorem 1 showed that there is a bijection between the set of isomorphism classes of elliptic curves E isogenous to E_0 and the set of G_k-invariant $\widehat{\mathbb{Z}}^p$-lattices $L \subset H^p$ and F, V-invariant $\mathbb{Z}_q$-lattices $\Lambda \subset H_p$, which takes an $X(N)$-structure E to a unique level structure on L; thus the same proof is enough to show that replacing the $X(N)$-structure on E by an $X_0(N)$ structure yields a unique G_k-invariant sublattice L' of L of index N, compatibly with this bijection. □

We can now replace K_ℓ, which corresponded to $X(N)$, with

$$J_\ell = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_\ell) | c \equiv 0 \pmod{N} \right\}$$

corresponding to $X_0(N)$, and again let f'_ℓ be its indicator function divided by its volume. Otherwise we use the same notation as from Corollary 2.

Corollary 4. *The cardinality of $X_0(N)(k)(E_0)$ is given by*

$$\mathrm{vol}(B^\times \backslash G) \cdot \mathrm{TO}_{\delta\sigma}(\phi_p) \cdot \prod_{\ell \neq p} \mathrm{O}^\ell_\gamma(f'_\ell).$$

The proof is essentially identical to that of Corollary 2.

In the case where E_0 is supersingular, this gives a formula for the number of supersingular points on $X_0(N)(k)$, since these are the points isogenous to E_0. It remains only to determine when there exists a supersingular E_0 over k with level N structure at all; but this turns out to be relatively easy. First, it's easy to see from the Hasse invariant that there exists at least one supersingular curve E_0 defined over each finite field; in fact for every k we can choose a supersingular E_0 with $E_0(k)$ cyclic (see e.g. Theorem 2.1 of [2]). Since every supersingular curve over $\overline{\mathbb{F}}_p$ is defined over $\mathbb{F}_{p^2}$, we can restrict to the cases $k = \mathbb{F}_p, \mathbb{F}_{p^2}$.

Consider first the former case. Since E_0 is supersingular, it satisfies $|E_0(\mathbb{F}_p)| = p + 1$ for $p > 3$; for $p \leq 3$ it satisfies $|E_0(\mathbb{F}_p)| \in \{1, p+1, 2p+1\}$. A necessary condition for the existence level N structure, i.e. a chosen cyclic subgroup of E_0 of order N, is that N divide the order of $E_0(\mathbb{F}_p)$; and in fact since $E_0(\mathbb{F}_p)$ is abelian there exists a subgroup of order m for every divisor m of $|E_0(\mathbb{F}_p)|$, which since we are assuming that $E_0(\mathbb{F}_p)$ is cyclic must also be cyclic. Therefore for $p > 3$ the number of supersingular k-points on $X_0(N)(\mathbb{F}_p)$ is given Corollary 4 whenever $p \equiv -1 \pmod{N}$ and by 0 otherwise. For $p \leq 3$, we conclude that there are no supersingular curves with level N structure defined over $\mathbb{F}_p$ for $N > 7$; we leave it as an exercise for the reader to work out exactly which $X_0(N)$ do have supersingular points over $\mathbb{F}_2$ and $\mathbb{F}_3$.

For $\mathbb{F}_{p^2}$, we can work similarly; since E_0 is supersingular over $\mathbb{F}_p$ it has $p+1$ $\mathbb{F}_p$-points, and since it is still supersingular over $\mathbb{F}_{p^2}$ it has $p^2 + ap + 1$ points over $\mathbb{F}_{p^2}$ for $-2 \leq a \leq 2$; since the $\mathbb{F}_p$-points form a subgroup of the $\mathbb{F}_{p^2}$-points we can only have $a = 2$. Since E_0 is supersingular we have $E_0(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$, so any subgroup of $E_0(\mathbb{F}_{p^2})$ is a product of subgroups of the factors; therefore there is a cyclic subgroup of $E_0(\mathbb{F}_{p^2})$ of order N if and only if there is a cyclic subgroup of $\mathbb{Z}/(p+1)\mathbb{Z} \simeq E_0(\mathbb{F}_p)$ of order N, and so the above criterion applies in general.

Let's try to compute this number in the simplest case, where $k = \overline{\mathbb{F}}_p$. (The discerning reader may object that this is not a finite field; nevertheless all the above goes through with this choice of k, replacing $\mathbb{Z}_q$ by the Witt vectors $W(\overline{\mathbb{F}}_p)$ and $\mathbb{Q}_q$ by $\widehat{\mathbb{Q}}_p^{\mathrm{unr}} := \operatorname{Frac} W(\overline{\mathbb{F}}_p)$.) In this case there is no Galois action, and so the Frobenius is trivial on both H^p and H_p. Therefore each centralizer $G_\gamma(\mathbb{Q}_\ell)$ is equal to the whole group $\mathrm{GL}_2(\mathbb{Q}_\ell)$ and similarly $G_{\delta\sigma}(\mathbb{Q}_p) = \mathrm{GL}_2(\widehat{\mathbb{Q}}_p^{\mathrm{unr}})$, and so the quotients $G_\gamma(\mathbb{Q}_\ell)\backslash \mathrm{GL}_2(\mathbb{Q}_\ell)$ and $G_{\delta\sigma}(\mathbb{Q}_p)\backslash \mathrm{GL}_2(\widehat{\mathbb{Q}}_p^{\mathrm{unr}})$ are trivial. Therefore $\mathrm{O}_\gamma^\ell(f'_\ell) = f'_\ell(1)$ for each $\ell \neq p$, and $\mathrm{TO}_{\delta\sigma}(\phi_p) = \phi_p(1)$. Since $1 \in \mathrm{GL}_2(\mathbb{Q}_\ell)$ is certainly in J_ℓ, we have $f'_\ell(1) = \frac{1}{\operatorname{vol} J_\ell}$; since ϕ_p is just the indicator function we have more simply $\phi_p(1) = 1$, so we can ignore this factor.

If $\ell \nmid N$, then N is invertible in $\mathbb{Z}_\ell$, and so the condition that c be divisible by N is trivial: for any c we have $c = NN^{-1}c$. Therefore $\operatorname{vol} J_\ell = \operatorname{vol} \mathrm{GL}_2(\mathbb{Z}_\ell) = 1$. If $\ell | N$, then write $N = u \cdot \ell^a$ for some integer $a \geq 1$ and unit $u \in \mathbb{Z}_\ell^\times$. Reducing modulo ℓ^a, we have $\operatorname{vol}(\mathrm{GL}_2(\mathbb{Z}_\ell)/J_\ell) = \operatorname{vol}(\mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z})/B)$, where B is the Borel subgroup consisting of upper triangular matrices over $\mathbb{Z}/\ell^a\mathbb{Z}$ (apologies for the conflict with the quaternion algebra, which is distinct). This quotient classifies full flags in $(\mathbb{Z}/\ell^a\mathbb{Z})^2$, which in this case is just the set of one-dimensional subspaces of $(\mathbb{Z}/\ell^a\mathbb{Z})^2$, of which there are $\ell^{a-1}(\ell+1)$; therefore $\operatorname{vol} J_\ell = \frac{1}{\ell^{a-1}(\ell+1)}$. Therefore in all we've shown, using Corollary 4, that the number of supersingular points on $X_0(N)(\overline{\mathbb{F}}_p)$ is given by

$$\operatorname{vol}(B^\times\backslash \mathrm{GL}_2(\mathbb{A}_f^p) \times \mathrm{GL}_2(\widehat{\mathbb{Q}}_p^{\mathrm{unr}})) \cdot \prod_{\ell^a | N} \ell^{a-1}(\ell+1),$$

where the product is over maximal prime powers ℓ^a dividing N. The last factor can also be written, perhaps more familiarly, as

$$N \prod_{\ell | N} \left(1 + \frac{1}{\ell}\right)$$

where the product is over primes dividing N.

It remains only to compute this volume factor. Write $B^\times(\mathbb{A}_f^p)$ for the $\mathbb{A}_f^p$-points of $B^\times$, given by the restricted product at $\ell \neq p$ of the completions $(B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times$, and analogously $B^\times(\mathbb{A}_f)$ for the restricted product over all ℓ; and write $B_p^\times$ for the local factor $(B \otimes_{\mathbb{Q}} \widehat{\mathbb{Q}}_p^{\mathrm{unr}})^\times$. Then we can factor the volume $\operatorname{vol}(B^\times\backslash \mathrm{GL}_2(\mathbb{A}_f^p) \times \mathrm{GL}_2(\widehat{\mathbb{Q}}_p^{\mathrm{unr}}))$ as

$$\operatorname{vol}(B^\times \backslash B^\times(\mathbb{A}_f)) \cdot \operatorname{vol}(B^\times(\mathbb{A}_f^p)\backslash \mathrm{GL}_2(\mathbb{A}_f^p)) \cdot \operatorname{vol}(B_p^\times\backslash \mathrm{GL}_2(\widehat{\mathbb{Q}}_p^{\mathrm{unr}})).$$

Since B splits away from p and ∞, the middle factor is just 1 since $B^\times(\mathbb{A}_f^p) = \mathrm{GL}_2(\mathbb{A}_f^p)$. Similarly, although B is ramified at p it splits over $\widehat{\mathbb{Q}}_p^{\mathrm{unr}}$, so the third factor is also 1; and the first factor is given by

$$|B^\times \backslash B^\times(\mathbb{A}_f)/\, \mathrm{O}(\mathbb{A}_f)|$$

where O is a maximal order of B (and so isomorphic to $\operatorname{End}(E_0)$), so that $\mathrm{O}(\mathbb{A}_f) = \prod_\ell \mathrm{O} \otimes \mathbb{Q}_\ell$. By p-adic uniformization this is simply the number of supersingular curves over $\overline{\mathbb{F}}_p$, and so we have shown that the number of supersingular points on $X_0(N)(\overline{\mathbb{F}}_p)$ is equal to the number of supersingular curves over $\overline{\mathbb{F}}_p$ (with no level structure) times

$$\prod_{\ell^a | N} \ell^{a-1}(\ell+1) = N \prod_{\ell | N} \left(1 + \frac{1}{\ell}\right).$$

In fact, this is exactly the expected formula: over $\overline{\mathbb{F}}_p$, any cyclic subgroup of order N of a given supersingular curve E is a subgroup of the N-torsion $E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$, or equivalently a one-dimensional subspace of the free module $(\mathbb{Z}/N\mathbb{Z})^2$, i.e. a point of the projective line over $\mathbb{Z}/N\mathbb{Z}$. The number of such points is exactly $\prod_{\ell^a | N} \ell^{a-1}(\ell+1)$, so we obtain the same formula.

References

[1] Peter Scholze. The Langlands–Kottwitz approach for the modular curve. *International Mathematics Research Notices*, 2011(15):3368–3425, 2011.

[2] S. G. Vlăduţ. On the cyclicity of elliptic curves over finite field extensions. *Finite Fields and Their Applications*, 5:354–363, 1999.