Tôhoku Math. J.
50 (1998), 291–302

0-CYCLES ON THE ELLIPTIC MODULAR SURFACE OF LEVEL 4

ANDREAS LANGER

(Received October 30, 1996, revised April 21, 1997)

Abstract. We prove a finiteness result on the torsion subgroup in the Chow group of zero cycles on the elliptic modular surface of level four. The main ingredient is Shioda's interpretation of this surface as the Kummer surface associated to the self-product of a certain elliptic curve. On the way we extend the main finiteness theorem on torsion zero cycles on the self-product of a modular elliptic curve to the case where the elliptic curve has complex multiplication and its conductor is a power of a prime.

Introduction. In this paper we will provide a new example for the finiteness of torsion zero cycles on an algebraic surface defined over a number field. Let B' be the subvariety in $\boldsymbol{P}^2 \times (\boldsymbol{P}^1 \setminus \Sigma)$, $\Sigma = (0, \infty, \pm 1, \pm i)$, defined by the equation

$$y^2 = x(x-1)\left(x - \frac{1}{2}\left(\sigma + \frac{1}{\sigma}\right)^2\right)$$

where (x, y) and σ are the inhomogeneous coordinates of $\boldsymbol{P}^2$ and of $\boldsymbol{P}^1$. Then B' is a smooth algebraic surface defined over $\boldsymbol{Q}$. Let B be its minimal model. Then B is an elliptic surface over $\boldsymbol{P}^1$. It is evident from the work of Shioda [Shi, Theorem 1] that after base change to the field $K = \boldsymbol{Q}(i)$, B becomes isomorphic to the elliptic modular surface C, which is defined as a suitable compactification of the universal elliptic curve over the modular curve $X(4)$ defined over K, i.e. we have $B \otimes_{\boldsymbol{Q}} K \cong C$. The main results in the paper are the following:

For a variety X let $\mathrm{CH}_0(X)$ be the Chow group of zero cycles modulo rational equivalence and $\mathrm{CH}_0(X)\{p\}$ its p-primary torsion subgroup for a prime p.

THEOREM A. *Let B be as above and p a prime such that $p > 3$. Then $\mathrm{CH}_0(B)\{p\}$ is a finite group.*

For the elliptic modular surface C we have a weaker result which shows that we have at least enough elements in the K-Theory of C to kill cycles in the closed fibers at good reduction primes. Let $\mathscr{C}$ be a proper smooth model of C over $O_K[1/2]$ and $C_\wp$ the closed fiber of $\mathscr{C}$ at the prime $\wp$, $\wp \nmid 2$. Let $\mathrm{CH}^2(\mathscr{C})$ be the Chow group of codimension 2 of $\mathscr{C}$. Then we have:

1991 *Mathematics Subject Classification.* Primary 14J27; Secondary 19E15, 14F30.

Key words and phrases: torsion zero cycles, elliptic modular surface, K-cohomology, Selmer groups, self-product of an elliptic curve with complex multiplication.

THEOREM B. *The cokernel of the boundary map*

$$H^1(C, \mathcal{K}_2) \xrightarrow{\partial} \bigoplus_{\wp \nmid 2} \mathrm{Pic}(C_\wp)$$

is a finite group. Equivalently the kernel of the map

$$\mathrm{CH}^2(\mathscr{C}) \longrightarrow \mathrm{CH}^2(C) = \mathrm{CH}_0(C)$$

is a finite group.

Here $H^1(C, \mathcal{K}_2)$ denotes the Zariski cohomology of C and $\mathrm{Pic}(C_\wp)$ the Picard group of the fiber $C_\wp$. The main ingredients in the proof of Theorems A and B are:

— Shioda's interpretation of B (resp. C) as Kummer surfaces associated to a certain abelian surface $A/\boldsymbol{Q}$ (resp. $E \times_K E$, where E is an elliptic curve defined over $\boldsymbol{Q}$ with complex multiplication by $\boldsymbol{Z}[i]$ (compare [Shi]).

— The finiteness of the p-primary Selmer group of the symmetric square of the elliptic curve considered over $\boldsymbol{Q}$. This follows from Wiles' paper on Fermat's last theorem [W, Theorems (3.1), (3.3)].

In the course of the proofs we will also reprove—under some slightly different assumptions—a result obtained in joint work with Raskind [L-R]. Our proof there used the Iwasawa-Theory of elliptic curves with complex multiplication performed by Rubin. Here we rely instead on Wiles' result on Selmer groups associated to deformation theories.

THEOREM C. *Let E be an elliptic curve over $\boldsymbol{Q}$ with conductor $N = q^s$ a power of a prime q. Assume that E has complex multiplication by the ring of integers in an imaginary quadratic field L. Then $\mathrm{CH}_0(E \times_{\boldsymbol{Q}} E)\{p\}$ is finite for all primes $p \nmid 6N$.*

In [L-S] we proved an analogous result for elliptic curves without complex multiplication. The proof of Theorem C will be very similar to the methods used in the non-CM-case.

The author would like to thank Klaus Künnemann, Shuji Saito and Andrew Wiles for helpful comments.

1. We first recall Shioda's interpretation of the surfaces B and C as certain singular $K3$-surfaces (with Néron-Severi-rank 20) ([Shi]). Let E_0 be the elliptic curve over $\boldsymbol{Q}$ obtained as the normalization of the curve $y^2 = x^4 - 1$. It has complex multiplication by the ring of integers in $\boldsymbol{Q}(i)$, a Weierstraß-form given by $y^2 = x^3 + 4x$, and its conductor is 2^{12}. Consider the translation T_v on E_0 defined by the point $v = (-1, 0)$ of order 2 and let A be the quotient $A := (E_0 \times E_0)/T_{(v,v)}$ by the translation of order 2. Then A is an abelian surface over $\boldsymbol{Q}$. It follows from [Shi, Theorem 1] and its proof that $B/\boldsymbol{Q}$ is isomorphic to $\mathrm{Km}(A)$, the Kummer surface associated to A. (Let $\iota \colon A \to A$, $\iota(u) = -u$ be the inversion. Then A/ι has 16 singular points corresponding to the points of order

2 on A. Km(A) is the blowing-up of A/ι with respect to these 16 singular points.) Furthermore we have:

LEMMA 1.1 (Shioda). (a) *$A\times_{\boldsymbol{Q}}K$ is isomorphic to $E_0\times E_0\times_{\boldsymbol{Q}}K$.*
(b) *C/K is isomorphic to* $\mathrm{Km}(E_0\times_K E_0)$.

The proof follows from [Shi, Theorem 1].

Note that by definition we have an isogeny of abelian surfaces over $\boldsymbol{Q}$ of degree 2.

$$\sigma : E_0\times_{\boldsymbol{Q}} E_0 \longrightarrow A\,.$$

PROPOSITION 1.2. *Let $\mathscr{B}$ be a proper smooth model of B over $\boldsymbol{Z}[1/2]$ and B_p its closed fiber at p. Then the cokernel of the map*

$$H^1(B,\mathscr{K}_2)\longrightarrow \bigoplus_{\wp\nmid 2}\mathrm{Pic}(B_p)$$

is a torsion group.

In the course of the proof of Proposition 1.2 we will also derive Theorem B.

PROOF. Consider the Galois extension $\pi_B: B_K\to B_{\boldsymbol{Q}}$. Then we have a commutative diagram

$$\begin{array}{ccc}
H^1(B,\mathscr{K}_2) & \xrightarrow{\partial_{\boldsymbol{Q}}} & \bigoplus_{p\nmid 2}\mathrm{Pic}(B_p)\\
\Big\downarrow{\scriptstyle \pi_B^*} & & \Big\downarrow{\scriptstyle \pi_B^*}\\
H^1(B_K,\mathscr{K}_2) & \xrightarrow{\partial_K} & \bigoplus_{\wp\in\mathrm{Spec}\,O_K[1/2]}\mathrm{Pic}(B_\wp)\\
{\scriptstyle \pi_{B_*}=N_{K/\boldsymbol{Q}}}\Big\downarrow & & \Big\downarrow{\scriptstyle N_{K/\boldsymbol{Q}}}\\
H^1(B,\mathscr{K}_2) & \xrightarrow{\partial_{\boldsymbol{Q}}} & \bigoplus_{\wp\nmid 2}\mathrm{Pic}(B_\wp)\,.
\end{array}$$

The composite $\pi_{B_*}\pi_B^*$ is the multiplication by $[K:\boldsymbol{Q}]=2$. Therefore it suffices to show that the map ∂_K has finite cokernel. Since B_K is isomorphic to C this will also imply Theorem B.

CLAIM. *The map*

$$H^1(B_K,\mathscr{K}_2)\xrightarrow{\partial_K}\bigoplus_{\wp\in\mathrm{Spec}\,O_K[1/2]}\mathrm{Pic}(B_\wp)$$

has finite cokernel.

Consider the following commutative diagram of surfaces over $K=\boldsymbol{Q}(i)$:

$$(\dagger) \qquad \begin{array}{ccc} E_0 \times E_0 & \xleftarrow{f} & \tilde{C} \\ \big\downarrow & & \big\downarrow \pi \\ E_0 \times E_0/\iota & \longleftarrow & \mathrm{Km}(E_0 \times E_0) = C . \end{array}$$

Here E_0 is considered as an elliptic curve over K and $\tilde{C}$ is the blowing-up of $E_0 \times E_0$ at the 16 points of order 2. π is outside the exceptional fibers a Galois covering of degree 2. Now look at the following commutative diagram:

$$(*) \qquad \begin{array}{ccccc} H^1(E_0 \times E_0, \mathcal{K}_2) & \xrightarrow{f^*} & H^1(\tilde{C}, \mathcal{K}_2) & \xrightarrow{\pi_*} & H^1(C, \mathcal{K}_2) \\ \big\downarrow \partial & & \big\downarrow \partial & & \big\downarrow \partial \\ \bigoplus_{\wp \nmid 2} \mathrm{Pic}(E_\wp \times E_\wp) & \xrightarrow{f^*} & \bigoplus_{\wp \nmid 2} \mathrm{Pic}(\tilde{C}_\wp) & \xrightarrow{\pi_*} & \bigoplus_{\wp \nmid 2} \mathrm{Pic}(C_\wp) \end{array}$$

π_* is well-defined for K-cohomology, because π is proper; f^* is well-defined because K-theory is contravariant for arbitrary morphisms. The diagram commutes on the right-hand side because the Brown-Gersten spectral sequence is covariant for proper morphisms. To see the commutativity on the left-hand side we interpret f^* on the level of Brown-Gersten resolutions. An element z in $H^1(E_0 \times E_0, \mathcal{K}_2)$ is given by a formal sum $\sum_Y g_Y$ where Y is an irreducible curve on $E_0 \times E_0$ and g_Y is a rational function on Y, i.e. $g_Y \in k(Y)^*$. By the moving lemma we may assume that the curves Y do not pass through the points of order 2 on $E_0 \times E_0$. Then $f^{-1}(Y)$ is isomorphic to Y and we define $f^*(z) = \sum_{f^{-1}(Y)} g_{f^{-1}(Y)}$ which evidently defines an element in $H^1(\tilde{C}, \mathcal{K}_2)$ (the moving lemma is not really necessary here but it makes the argument easier). We also define a map

$$\bigoplus_{\substack{x \text{ codim } 2 \\ \text{in } E_0 \times E_0}} \boldsymbol{Z}_x \longrightarrow \bigoplus_{\substack{x \text{ codim } 2 \\ \text{in } \tilde{C}}} \boldsymbol{Z}_x$$

as follows: If x is not of order 2, we take the identity map $\boldsymbol{Z}_x = \boldsymbol{Z}_{f^{-1}(x)}$. If x is of order 2, let x' be the base point in $f^{-1}(x) \cong \boldsymbol{P}^1$ and take the identity map $\boldsymbol{Z}_x = \boldsymbol{Z}_{x'}$. Using the inclusion $k(E_0 \times E_0) \subset k(\tilde{C})$ of function fields we also get a map $\mathcal{K}_2(k(E_0 \times E_0)) \to \mathcal{K}_2(k(\tilde{C}))$. These maps altogether define a map f^* from the Gersten-Quillen resolution of $\mathcal{K}_2/E_0 \times E_0$ to the Gersten-Quillen resolution of $\mathcal{K}_2/\tilde{C}$. Compatibility with the tame symbol maps and the divisor maps is clear. In particular the map f^* constructed for $H^1(\ , \mathcal{K}_2)$ as above coincides with the one defined by the contravariance property of K-theory. Now a similar interpretation of the map f^* on the level of the Picard groups of the closed fibers yields—by looking at the Gersten-Quillen resolutions of $\mathcal{K}_2$ for $E_0 \times E_0$, $\tilde{C}$ and their models over $O_K[1/2]$, the resolutions of $\mathcal{K}_1$ for $E_\wp \times E_\wp$ and $\tilde{C}_\wp$ and the explicit definition of the map ∂ by using these resolutions—the compatibility of f^* with ∂. We do not work out the full details here because the large diagram one has in mind is evident. Thus the diagram $*$ is commutative as claimed.

Now π_* is surjective on the level of Pic's as is easily seen. So it remains to show that

$$\partial: H^1(\tilde{C}, \mathcal{K}_2) \longrightarrow \bigoplus_{\wp \nmid 2} \mathrm{Pic}(\tilde{C}_\wp)$$

has finite cokernel.

Now $\mathrm{Pic}(\tilde{C}_p) = \mathbf{Z}^{16} \oplus \mathrm{Pic}(E_\wp \times E_\wp)$ by standard properties of the blowing-up, the inclusion of $\mathrm{Pic}(E_\wp \times E_\wp)$ in $\mathrm{Pic}(\tilde{C}_\wp)$ being given by f^*. The image of $\mathrm{Pic}(\tilde{C}) \otimes K^* \to H^1(\tilde{C}, \mathcal{K}_2) \to \bigoplus_{\wp \nmid 2} \mathrm{Pic}(\tilde{C}_\wp)$ certainly covers all cycles arising from exceptional fibers. On the other hand the map ∂ on the level $E_0 \times E_0$ has finite cokernel by a result of Mildenhall [Mi, Theorem 0.1]. So the boundary map ∂ considered over $\tilde{C}$ also has this property. This finishes the proof of the claim and implies Proposition 1.2 and Theorem B.

Remark. Another way of explaining the "surjectivity property of ∂" on the elliptic modular surface C is as follows: For $p \equiv 3$ (4), i.e. for primes where E_0 has supersingular reduction the Néron-Severi rank of C_p is 22 [Shi, Corollary 1]. Note that such primes p remain prime in K and therefore the notation C_p makes sense here. There are two elements u_1, u_2 in $\mathrm{NS}(C_p)$ arising from sections of $C_p \to X(4)_p$ ($X(4)_p$ denotes the reduction of the modular curve at p) of infinite order, i.e. of $K(X(4)_p)$-rational points of infinite order of the elliptic curve $C_p \times K(X(4)_p)$ over the function field $K(X(4)_p)$ of the modular curve at p. Let $y_1, y_2 \in H^1(E_0 \times_K E_0, \mathcal{K}_2)$ be the elements Mildenhall constructed to kill multiples of Fr_p and $(\mathrm{Fr}_p \circ \mathrm{CM}_p)$ where Fr_p is the graph of the Frobenius on the reduction E_p and $\mathrm{Fr}_p \circ \mathrm{CM}_p$ is the composition of the Frobenius with complex multiplication on E_p. The above functorial proof shows that $\pi_* f^*(y_1)$ and $\pi_* f^*(y_2)$ are the "non-trivial" elements in $H^1(C, \mathcal{K}_2)$ that we need: $\partial_p(\pi_* f^*(y_1))$ and $\partial_p(\pi_* f^*(y_2))$ kill multiples of u_1 and u_2.

2. Let X denote either the selfproduct $E \times_{\mathbf{Q}} E$ for a CM-elliptic curve E satisfying the assumptions of Theorem C or the Kummer-surface $B = \mathrm{Km}(A)$ as constructed in §1. By Bloch [B] and Merkurjev-Suslin [M-S] we have the exact sequence

$$\begin{aligned} 0 \longrightarrow H^1(X, \mathcal{K}_2) \otimes (\mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow K_N H^3(X, (\mathbf{Q}_p/\mathbf{Z}_p)(2)) \\ \longrightarrow \ker(\mathrm{CH}_0(X)\{p\} \longrightarrow \mathrm{CH}_0(\bar{X})\{p\}) \longrightarrow 0 \end{aligned}$$

where

$$K_N H^3(X, (\mathbf{Q}_p/\mathbf{Z}_p)(2)) := \ker(NH^3(X, \mathbf{Q}_p/\mathbf{Z}_p(2)) \longrightarrow H^3(\bar{X}, (\mathbf{Q}_p/\mathbf{Z}_p)(2)))$$

and

$$NH^3(X, (\mathbf{Q}_p/\mathbf{Z}_p)(2)) := \ker(H^3(X, \mathbf{Q}_p/\mathbf{Z}_p(2)) \longrightarrow H^3(\mathbf{Q}(X), (\mathbf{Q}_p/\mathbf{Z}_p)(2)))$$

is the first step in the coniveau filtration on $H^3(X, (\mathbf{Q}_p/\mathbf{Z}_p)(2))$.

Lemma 2.1. $H^2(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), H^1(\bar{X}, (\mathbf{Q}_p/\mathbf{Z}_p)(2))) = 0$.

By Jannsen's cohomological Hasse principle [J] we have

$$H^2(\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}), H^1(\bar{X}, (\mathbf{Q}_p/\mathbf{Z}_p)(2))) \cong \bigoplus_l H^2(\mathrm{Gal}(\bar{\mathbf{Q}}_l/\mathbf{Q}_l), H^1(\bar{X}, (\mathbf{Q}_p/\mathbf{Z}_p)(2))).$$

Since the elliptic curve E_0 (§1) has potentially good reduction everywhere, A and also B (except possibly at $l=2$) have potentially good reduction everywhere. By local Tate-duality we have

$$\begin{aligned}&\operatorname{Hom}(H^2(\operatorname{Gal}(\bar{\boldsymbol{Q}}_l/\boldsymbol{Q}_l), H^1(\bar{X}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2)), (\boldsymbol{Q}_p/\boldsymbol{Z}_p)))\\ &\cong H^0(\operatorname{Gal}(\bar{\boldsymbol{Q}}_l/\boldsymbol{Q}_l), H^3(\bar{X}, \boldsymbol{Z}_p(1)))\end{aligned}$$

and in both cases of X, i.e. $X=E\times_{\boldsymbol{Q}}E$ and all l or $X=B$ and $l\neq 2$, $H^3(\bar{X}, \boldsymbol{Z}_p(1))$ is torsion-free and its local Galois invariants are zero by Deligne's proof of the Weil Conjectures. In the case $X=B$ and $l=2$ we argue as follows: Recall that $C\cong B\times_{\boldsymbol{Q}}K$ and consider again the commutative diagram (†) in §1. Let U be the complement in C of all exceptional fibers and $\tilde{U}$ the complement in $\tilde{C}$ of all exceptional fibers. Then $\iota\colon \tilde{U}\to U$ is a Galois extension with Galois group isomorphic to $\boldsymbol{Z}/2$ and we have (for $p\neq 2$) an isomorphism $H^3(\bar{U}, \boldsymbol{Z}_p(2))\cong H^0(\boldsymbol{Z}/2, H^3(\bar{\tilde{U}}, \boldsymbol{Z}_p(2)))$. By standard properties of the cohomology of blow-ups and the fact that $H^i(\boldsymbol{P}^1, \boldsymbol{Z}_p)=0$ for odd i we have an injection: $H^3(\bar{B}, \boldsymbol{Z}_p(2)) \hookrightarrow H^3(\bar{U}, \boldsymbol{Z}_p(2))$. On the other hand we have an isomorphism $H^3(\bar{\tilde{U}}, \boldsymbol{Z}_p(2))\cong H^3(\bar{E}_0\times\bar{E}_0, \boldsymbol{Z}_p(2))$ and therefore a Galois equivariant injection $H^3(\bar{B}, \boldsymbol{Z}_p(2)) \hookrightarrow H^3(\bar{E}_0\times\bar{E}_0, \boldsymbol{Z}_p(2))$. Since $E_0\times E_0$ has potentially good reduction at $l=2$, we finally have

$$H^3(\bar{B}, \boldsymbol{Z}_p(2))^{\operatorname{Gal}(\bar{\boldsymbol{Q}}_2/\boldsymbol{Q}_2)}=H^3(\bar{E}_0\times\bar{E}_0, \boldsymbol{Z}_p(2))^{\operatorname{Gal}(\bar{\boldsymbol{Q}}_2/\boldsymbol{Q}_2)}=0$$

by Deligne's proof of the Weil Conjectures.

COROLLARY 2.2. *There is an injection*

$$K_N H^3(X, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2)) \hookrightarrow H^1(\operatorname{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}), H^2(\bar{X}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2)))\,.$$

PROOF. This follows from Lemma 2.1 using the Hochschild-Serre spectral sequence.

PROPOSITION 2.3. *Let p be a prime such that*

$$\begin{aligned}&p>3 && \text{if } X=B\\ &p\nmid 6N && \text{if } X=E\times E\,.\end{aligned}$$

Then we have

$$H^1(X, \mathscr{K}_2)\otimes(\boldsymbol{Q}_p/\boldsymbol{Z}_p)=K_N H^3(X, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))_{\mathrm{div}}$$

where for an abelian group M, M_{div} denotes its maximal divisible subgroup.

Proposition (2.3) implies Theorems A and C. Indeed, let $\mathscr{X}$ be a smooth proper model of X over

$$\begin{aligned}&\boldsymbol{Z}[1/2p]\,, && \text{if } X=B\\ &\boldsymbol{Z}[1/6Np]\,, && \text{if } X=E\times_{\boldsymbol{Q}}E\,.\end{aligned}$$

The kernel of the map

$$\mathrm{CH}_0(\mathscr{X}) \longrightarrow \mathrm{CH}_0(X)$$

is a torsion group by Proposition 1.2, if $X=B$ and by [Mi], if $X=E\times_{\boldsymbol{Q}}E$. Therefore we have a surjection

$$\mathrm{CH}_0(\mathscr{X})\{p\} \longrightarrow \mathrm{CH}_0(X)\{p\}$$

on the p-primary torsion subgroups. But $\mathrm{CH}_0(\mathscr{X})\{p\}$ is a subquotient of $H^3_{\mathrm{et}}(\mathscr{X}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))$ and therefore co-finitely generated as a $\boldsymbol{Z}_p$-module. So $\mathrm{CH}_0(X)\{p\}$ is cofinitely generated. Proposition 2.3 implies that $\ker(\mathrm{CH}_0(X)\{p\}\to\mathrm{CH}_0(\bar{X})\{p\})$ is finite. But $(\mathrm{CH}_0(\bar{X})\{p\})^{\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})}$ is known to be finite, too. Hence $\mathrm{CH}_0(X)\{p\}$ is finite in both cases for primes p satisfying the assumption in Proposition 2.3. This finishes the proof of Theorems A and C and it remains to show Proposition 2.3.

Let $M=H^2(\bar{X}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))$ and consider the composite maps

$$\psi: H^1(X, \mathscr{K}_2)\otimes(\boldsymbol{Q}_p/\boldsymbol{Z}_p) \longrightarrow K_N H^3(X, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2)) \xrightarrow{\alpha'} \bigoplus_{\text{all } l} H^1(\boldsymbol{Q}_l, M)/H^1_f(\boldsymbol{Q}_l, M)$$

where α' is the restriction (using Corollary 2.2) of the map

$$\alpha: H^1(\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}), M) \longrightarrow \bigoplus_{\text{all } l} H^1(\boldsymbol{Q}_l, M)/H^1_f(\boldsymbol{Q}_l, M)$$

the kernel of which defines the Selmer group.

PROPOSITION 2.4. *Under the above assumptions we have*

$$\mathrm{Im}\,\psi = \bigoplus_{l\neq p} H^1(\boldsymbol{Q}_l, M)_{\mathrm{div}}/H^1_f(\boldsymbol{Q}_l, M)\oplus H^1_g(\boldsymbol{Q}_p, M)/H^1_f(\boldsymbol{Q}_p, M)$$

and this image coincides with the image of

$$K_N H^3(X, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))_{\mathrm{div}}$$

under the restriction map α'.

LEMMA 2.5. *Let α'_p be the p-component of α'. Then*

$$\mathrm{Im}\,\alpha'_p \subset H^1_g(\boldsymbol{Q}_p, M)\,.$$

PROOF. By [L-S, Lemma 5.4] we have

$$K_N H^3(X_{\boldsymbol{Q}_p}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2)) \subset H^3(\mathscr{X}, \tau_{\leq 2}Rj_*(\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))$$

where $\mathscr{X}$ is a smooth proper model of $\mathscr{X}$ over $\boldsymbol{Z}_p$. Therefore it remains to show that $H^3(\mathscr{X}, \tau_{\leq 2}Rj_*\boldsymbol{Q}_p(2))$ is contained in $H^1_g(\boldsymbol{Q}_p, V)$ where $V=H^2(\bar{X}, \boldsymbol{Q}_p(2))$. This follows from the proof of Theorems 0.1 in [L]. Note that $\mathscr{X}/Z_p$ is smooth and therefore in particular semistable, because the conditions on the singularities in the closed fiber is trivial (the log-structure on $\mathscr{X}$ is $j_*O_X^* \cap O_{\mathscr{X}}$, where $j\colon X_{\boldsymbol{Q}_p} \to \mathscr{X}$ is the canonical inclusion).

In the rest of this paragraph we restrict ourselves to the case where $X = E \times_{\boldsymbol{Q}} E$ is the selfproduct of a CM-elliptic curve E with conductor $N = q^s$.

The main finiteness result on Selmer groups associated to deformation theories by Wiles [W, Theorem (3.1)] implies the following:

THEOREM 2.6. *Let E be as above, p a prime, $p \nmid 6q$. Then* $\ker \alpha$ *is finite, i.e. the p-primary Selmer group associated to the symmetric square of E over $\boldsymbol{Q}$ is finite.*

Indeed, consider the Galois representation on the p-torsion points of E

$$\varrho_p\colon \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}) \longrightarrow GL_2(E_p(\bar{\boldsymbol{Q}})) = GL_2(\boldsymbol{F}_p)\,.$$

Since complex multiplication is not defined over the field $\boldsymbol{Q}\,(\sqrt{(-1)^{(p-1)/2}p})$ the restriction of ϱ_p to $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\sqrt{(-1)^{(p-1)/2}p}))$ is absolutely irreducible and we may apply Theorem (3.1) in [W] to the minimal deformation theory associated to ϱ_p in order to get Theorem 2.6. Consider now the commutative diagram (for $p \nmid 6N$)

$$\begin{array}{ccccccc}
 & & & & H^1(X, \mathscr{K}_2) \otimes \boldsymbol{Q}_p & \xrightarrow{\partial_p} & \mathrm{Pic}(X_p) \otimes \boldsymbol{Q}_p \\
 & & & & \downarrow & & \downarrow \cong \\
0 & \longrightarrow & H^3_{\mathrm{syn}}(\mathscr{X}, \boldsymbol{Q}_p(2)) & \longrightarrow & H^3(\mathscr{X}, \tau_{\le 2} Rj_* \boldsymbol{Q}_p(2)) & \longrightarrow & H^1_g(\boldsymbol{Q}_p, V)/H^1_f(\boldsymbol{Q}_p, V)
\end{array}$$

(compare [L-S, Lemma 4.5 and its proof]). The surjectivity of ∂_p implies the surjectivity of

$$\psi_p\colon H^1(X, \mathscr{K}_2) \otimes (\boldsymbol{Q}_p/\boldsymbol{Z}_p) \longrightarrow H^1_g(\boldsymbol{Q}_p, M)/H^1_f(\boldsymbol{Q}_p, M)\,.$$

For all $l \neq q$, $l \neq p$, we have by [L-S, Lemma 4.5] an isomorphism $\gamma\colon \mathrm{Pic}(X_l) \otimes \boldsymbol{Q}_p \cong H^1(\boldsymbol{Q}_l, V)/H^1_f(\boldsymbol{Q}_l, V)$ fitting into a commutative diagram

$$\begin{array}{ccc}
H^1(X, \mathscr{K}_2) \otimes \boldsymbol{Q}_p & \xrightarrow{\partial_l} & \mathrm{Pic}(X_l) \otimes \boldsymbol{Q}_p \\
 & \searrow^{\psi_l} & \downarrow \gamma \\
 & & H^1(\boldsymbol{Q}_l, V)/H^1_f(\boldsymbol{Q}_l, V)\,.
\end{array}$$

We have the surjectivity of the map (Mildenhall)

$$H^1(X, \mathscr{K}_2) \otimes \boldsymbol{Q}_p \xrightarrow{\partial} \bigoplus_{\substack{l \nmid N \\ l \neq p}} \mathrm{Pic}(X_l) \otimes \boldsymbol{Q}_p$$

which implies by [L-S, Lemma 4.5] the surjectivity of

$$(2.7)\quad H^1(X, \mathscr{K}_2) \otimes (\boldsymbol{Q}_p/\boldsymbol{Z}_p) \twoheadrightarrow \bigoplus_{\substack{l \neq q \\ l \neq p}} H^1(\boldsymbol{Q}_l, M)_{\mathrm{div}}/H^1_f(\boldsymbol{Q}_l, M) \oplus H^1_g(\boldsymbol{Q}_p, M)/H^1_f(\boldsymbol{Q}_p, M)\,.$$

Now consider $l = q$ (recall that the conductor of E is a power of the prime q by our assumption). There is a totally ramified extension of local fields $N_{\mathfrak{q}}/\boldsymbol{Q}_q$ such that E has good reduction over $N_{\mathfrak{q}}$. Since $\mathfrak{q}$ is ramified in the CM-field L we may assume that

$N_{\mathfrak{q}}$ contains L. Take an algebraic number field N containing L such that its completion at $\mathfrak{q}$ is $N_{\mathfrak{q}}$ (note that N from now on denotes this number field and not the conductor of E). Since the residue field of $N_{\mathfrak{q}}$ is $\boldsymbol{F}_q$ we have rank NS $(E_{\mathfrak{q}} \times E_{\mathfrak{q}})=4$. On the other hand we know that $\mathrm{Pic}(X_N)$ also has Néron-Severi rank 4. Therefore the composite map

$$\mathrm{Pic}(X_N) \otimes N^* \longrightarrow H^1(X_N, \mathscr{K}_2) \longrightarrow \mathrm{Pic}(X_{\mathfrak{q}})$$

has finite cokernel, which implies the surjectivity of

$$H^1(X_N, \mathscr{K}_2) \otimes \boldsymbol{Q}_p \xrightarrow{\partial_{\mathfrak{q}}} \mathrm{Pic}(X_{\mathfrak{q}}) \otimes \boldsymbol{Q}_p .$$

By [L-S, Lemma 4.5] the map

$$\psi_{\mathfrak{q}}: H^1(X_N, \mathscr{K}_2) \otimes (\boldsymbol{Q}_p/\boldsymbol{Z}_p) \longrightarrow H^1(N_{\mathfrak{q}}, M)_{\mathrm{div}}/H^1_f(N_{\mathfrak{q}}, M)$$

is surjective. Now we have a commutative diagram

$$\begin{array}{ccc} H^1(X_N, \mathscr{K}_2) \otimes \boldsymbol{Q}_p & \xrightarrow{\psi_{\mathfrak{q}}} & H^1(N_{\mathfrak{q}}, V)/H^1_f(N_{\mathfrak{q}}, V) \\ \Big\downarrow N_{N/\boldsymbol{Q}} & & \Big\downarrow \mathrm{cor}' \\ H^1(X, \mathscr{K}_2) \otimes \boldsymbol{Q}_p & \xrightarrow{\psi_{\mathfrak{q}}} & H^1(\boldsymbol{Q}_q, V)/H^1_f(\boldsymbol{Q}_q, V) . \end{array}$$

Here $V=H^2(\bar{X}, \boldsymbol{Q}_p(2))$. To get the map cor$'$ on the right-hand side we start with the corestriction map

$$H^1(N_{\mathfrak{q}}, V) \longrightarrow H^1(\boldsymbol{Q}_{\mathfrak{q}}, V) .$$

This induces a commutative diagram

$$\begin{array}{ccc} H^1(N_{\mathfrak{q}}, V) & \xrightarrow{\mu_{N_{\mathfrak{q}}}} & H^1(I_{N_{\mathfrak{q}}}, V) \\ \mathrm{cor} \Big\downarrow & & \Big\downarrow \mathrm{cor} \\ H^1(\boldsymbol{Q}_q, V) & \xrightarrow{\mu_{\boldsymbol{Q}_q}} & H^1(I_{\boldsymbol{Q}_q}, V) . \end{array}$$

Here $I_{N_{\mathfrak{q}}}$, $I_{\boldsymbol{Q}_{\mathfrak{q}}}$ are the inertia groups and note that $I_{N_{\mathfrak{q}}}=I_{\boldsymbol{Q}_{\mathfrak{q}}} \cap \mathrm{Gal}(\bar{N}_{\mathfrak{q}}/N_{\mathfrak{q}})$. Since $H^1_f(N_{\mathfrak{q}}, V)$ (resp. $H^1_f(\boldsymbol{Q}_q, V)$) is $\ker \mu_{N_{\mathfrak{q}}}$ (resp. $\ker \mu_{\boldsymbol{Q}_q}$)—note that $q \neq p$. We obviously get the map cor$'$ by taking quotients. Since cor is surjective, cor$'$ is also surjective. Therefore the map

$$H^1(X, \mathscr{K}_2) \otimes \boldsymbol{Q}_p \longrightarrow H^1(\boldsymbol{Q}_q, V)/H^1_f(\boldsymbol{Q}_q, V) \tag{2.8}$$

is surjective. Now the restriction of the map $\psi_q \circ N_{N/\boldsymbol{Q}}$ to the image of $(\mathrm{Pic}(X_N) \otimes \langle q^{\boldsymbol{Z}} \rangle) \otimes \boldsymbol{Q}_p$ in $H^1(X_N, \mathscr{K}_2) \otimes \boldsymbol{Q}_p$ is still surjective, whereas its image in $\bigoplus_{\mathrm{all}\, l \neq q} H^1(\boldsymbol{Q}_l, V)/H^1_f(\boldsymbol{Q}_l, V)$ under the map $\bigoplus_{\mathrm{all}\, l \neq q} \psi_l \circ N_{N/\boldsymbol{Q}}$ is zero. This fact together with (2.7), (2.8) and Lemma 2.5 imply all the statements of Proposition 2.4 in the case $X=E \times E$. Finally Proposition 2.4 and Theorem 2.6 imply Proposition 2.3 in the case $X=E \times_{\boldsymbol{Q}} E$ for a CM-elliptic curve E. This finishes the proof of Theorem C.

3. In this paragraph we will finish the proof of our main Theorem A; i.e. we prove Proposition 2.3 in case $X=B$. Recall B is isomorphic to the Kummer surface Kim(A), where A is an abelian surface with an isogeny $E_0 \times E_0 \to A$ of degree 2 and E_0 is the elliptic curve explicitly constructed in §1. E_0 has complex multiplication by $\mathbf{Z}[i]$, and conductor 2^{12}. We will of course use the tools in the proof of Theorem C to derive Theorem A.

PROPOSITION 3.1. *There is for all primes $l \nmid 2p$ an isomorphism*

$$\mathrm{Pic}(B_l) \otimes \mathbf{Q}_p \cong H^1(\mathbf{Q}_l, V)/H^1_f(\mathbf{Q}_l, V)$$

fitting into a commutative diagram

$$\begin{array}{ccc} H^1(B, \mathscr{K}_2) & \xrightarrow{\partial_l} & \mathrm{Pic}(B_l) \otimes \mathbf{Q}_p \\ & {\scriptstyle\psi_l} \searrow & \downarrow \cong \\ & & H^1(\mathbf{Q}_l, V) H^1_f(\mathbf{Q}_l, V) . \end{array}$$

This is proven in the same way as [L-S, Lemma 4.5]. One needs the Tate conjecture for the closed fiber B_l of B which is known (compare [Shi]). Similarly the crystalline Tate conjecture (which is easily derived for B_p since it is known for A_p) yields—by the same methods as in the proof of [L-S, Lemma 4.5] an isomorphism

$$\mathrm{Pic}(B_p) \otimes \mathbf{Q}_p \cong H^1_g(\mathbf{Q}_p, V)/H^1_f(\mathbf{Q}_p, V)$$

fitting into a commutative diagram

$$\begin{array}{ccc} H^1(B, \mathscr{K}_2) & \longrightarrow & \mathrm{Pic}(B_p) \otimes \mathbf{Q}_p \\ & {\scriptstyle\psi_p} \searrow & \downarrow \cong \\ & & H^1_g(\mathbf{Q}_p, V) H^1_f(\mathbf{Q}_p, V) . \end{array} \tag{3.2}$$

Now consider the case $l=2$. To show the surjectivity of the map

$$H^1(B, \mathscr{K}_2) \otimes (\mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow H^1(\mathbf{Q}_2, M)_{\mathrm{div}}/H^1_f(\mathbf{Q}_2, M)$$

it suffices to show—by a norm argument—the surjectivity of this map when working over the field K. Again we use the fact that $B \otimes_{\mathbf{Q}} K$ is isomorphic to C. Let $\mathfrak{q}=(1+i)$ be the unique prime of $\mathbf{Z}[i]$ lying above 2. Usint the commutative diagram † and standard cohomological arguments of blow-ups that are similar to the ones applied in the proof of Lemma 2.1 we have an isomorphism of Gal($\bar{\mathbf{Q}}/K$)-modules

$$M = H^2(\bar{C}, \mathbf{Q}_p/\mathbf{Z}_p(2)) \cong H^2(\bar{E}_0 \times \bar{E}_0, \mathbf{Q}_p/\mathbf{Z}_p(2)) \oplus (\mathbf{Q}_p/\mathbf{Z}_p(1))^{16}$$

where the right summand on the right-hand side corresponds to the exceptional fibers in the blown-up points. Let Z be the subgroup of Pic(C) generated by the 16 exceptional fibers. It is then easy to see that the image of the map

$$(Z\otimes K^*)\otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p \longrightarrow H^1(C, \mathscr{K}_2)\otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p \xrightarrow{\psi_{\mathrm{q}}} H^1(K_{\mathrm{q}}, M)_{\mathrm{div}}/H^1_f(K_{\mathrm{q}}, M)$$

is $H^1(K_{\mathrm{q}}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p(1))^{16})/H^1_f(K_{\mathrm{q}}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p(1))^{16})$ (use the above decomposition of M and compare the proof of [L-S, Lemma 4.1]). Now the crucial commutative diagram $(*)$ in §1 implies that the image of $H^1(E_0\times E_0, \mathscr{K}_2)\otimes \boldsymbol{Q}_p/\boldsymbol{Z}_p$ under the map $\psi_{\mathrm{q}}\circ\pi_*\circ f^*$ is

$$H^1(K_{\mathrm{q}}, H^2(\bar{E}_0\times\bar{E}_0, \boldsymbol{Q}_p/\boldsymbol{Z}_p(2)))_{\mathrm{div}}/H^1_f(K_{\mathrm{q}}, H^2(\bar{E}_0\times\bar{E}_0, \boldsymbol{Q}_p/\boldsymbol{Z}_p(2)))$$

in view of the $\mathrm{Gal}(\bar{\boldsymbol{Q}}/K)$-equivariant splitting of M and the surjectivity of the map ψ_{q} in the case $X=E_0\times E_0$ that was shown in §2. This shows the surjectivity of ψ_{q} $(X=C)$ and therefore also of ψ_2 $(X=B)$. By applying an argument that is almost identical to the one used at the end of §2 we see that Proposition 1.2, Proposition 3.1, Lemma 2.5, 3.2 and the surjectivity of ψ_2 imply Proposition 2.4 in the case $X=B$. Now we show:

THEOREM 3.3. *In the notation* $M=H^2(\bar{B}, \boldsymbol{Q}_p/\boldsymbol{Z}_p(2))$, *the kernel of the map*

$$\alpha\colon H^1(\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}), M)\longrightarrow \bigoplus_{\text{all } l} H^1(\boldsymbol{Q}_l, M)/H^1_f(\boldsymbol{Q}_l, M)$$

is finite, i.e. the p-primary Selmer group $S_{p^\infty}(\boldsymbol{Q}, H^2(B)(2))$ *is finite.*

End of the proof of Theorem A: Theorem 3.3 and Proposition 2.4 (case $X=B$) finish the proof of Proposition 2.3 that implies Theorem A.

PROOF OF THEOREM 3.3. Consider the commutative diagram

$$\begin{array}{ccc} A & \longleftarrow & \tilde{A} \\ \downarrow & & \downarrow \\ A/\iota & \longleftarrow & B\cong \mathrm{Km}(A)\,, \end{array}$$

where $\tilde{A}$ is the blow-up of the abelian surface A at all 16 points of order 2. From the Hochschild-Serre spectral sequence it is easy to see that

$$H^2(\bar{\tilde{A}}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))\cong H^2(\bar{B}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2)) \tag{3.4}$$

as $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-modules (note that the inversion ι acts trivially on $H^2(\bar{\tilde{A}}, \boldsymbol{Q}_p/\boldsymbol{Z}_p(2))$).

Furthermore we have a direct sum decomposition of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-modules

$$H^2(\bar{\tilde{A}}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))=H^2(\bar{A}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))\oplus(\boldsymbol{Q}_p/\boldsymbol{Z}_p)(1)^{16} \tag{3.5}$$

It is well-known that the Selmer group of $(\boldsymbol{Q}_p/\boldsymbol{Z}_p)(1)$ vanishes. The isogeny $\sigma\colon E_0\times E_0\to A$ of degree 2 implies an isomorphism (multiplication by $\deg\sigma=2$, note that $p\nmid 2$) of the composite map

$$H^2(\bar{A}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))\xrightarrow{\sigma^*} H^2(\bar{E}_0\times\bar{E}_0, \boldsymbol{Q}_p/\boldsymbol{Z}_p(2))\xrightarrow{\sigma_*} H^2(\bar{A}, (\boldsymbol{Q}_p/\boldsymbol{Z}_p)(2))\,.$$

Hence we get a surjection of Selmer groups

$$S_{p^\infty}(\boldsymbol{Q}, H^2(E_0 \times E_0)(2)) \twoheadrightarrow S_{p^\infty}(\boldsymbol{Q}, H^2(A)(2)) .$$

By Wiles' theorem 2.6, that we may apply to E_0, $S_{p^\infty}(\boldsymbol{Q}, H^2(E_0 \times E_0)(2))$ is finite. Using (3.4) and (3.5) we see that $S_{p^\infty}(\boldsymbol{Q}, H^2(B)(2))$ is also finite and Theorem 3.3 holds.

References

[B] S. Bloch, Lectures on algebraic cycles, Duke Univ. Math. Series, Durham 1980.

[J] U. Jannsen, On the l-adic cohomology of varieties over number fields and its Galois cohomology, in: Galois groups over $\boldsymbol{Q}$, Math. Sci. Res. Inst. Publ. 16, Springer-Verlag, New York 1989, 315–360.

[L] A. Langer, Local points of motives in semistable reduction, to appear in Compositio Mathematica.

[L-R] A. Langer and W. Raskind, 0-cycles on the selfproduct of a CM-elliptic curve over $\boldsymbol{Q}$, preprint 1996.

[L-S] A. Langer and S. Saito, Torsion zero-cycles on the selfproduct of a modular elliptic curve, in: Duke Math. J. 85 no. 2 (1996), 415–447.

[Mi] S. Mildenhall, Cycles in a product of elliptic curves, and a group analogous to the class group, Duke Math. J. 67 (1992), 387–406.

[M-S] A. S. Merkurjev and A. Suslin, K-cohomology of Severi-Brauer varieties and the norm residue homomorphism, Math. USSR Izv. 21 (1983), 307–340.

[Shi] T. Shioda, Algebraic cycles on certain $K3$-surfaces in char. p, in: Manifolds, Tokyo 1973, 357–364, ed. by A. Hattori, Univ. of Tokyo Press, Tokyo, 1975.

[W] A. Wiles, Modular elliptic curves and Fermat's last theorem, Annals of Math. 142 (1995), 443–551.

Mathematisches Institut
Universität Münster
Einsteinstr. 62
48149 Münster
Germany