Joint work with Ari Shnidman.

Question$_p$. Are there absolutely simple Abelian varieties / $\mathbb{Q}$ with arbitrarily large p-part of the Tate-Shafarevich group?

So far in the literature:

p	2 ✓	3 ✓ (Cassels)	5 ✓	7 ✓	11 ✓	13 ✓
	$d=1$ (Bölling)	$d=1$	$d=1$	$d=1$	$d=1$	$d=1$
	$d=2$ (Flynn)	$d=2$	Fisher [Two 5-isogenies]		Matsuno	
	Any d	B-F-5				

Question$_p$: Yes for $p = 2, 3, 5, 7, 11, 13$.

[Over number fields k, there are results of Creutz, Clark-Sherif, Kloosterman]

Anything in square brackets is verbal

[We shall show: Yes $\forall p$]

Toy Example

$E_k : y^2 = x(x+k)(x-k)$.

$\hat{E}_k : y^2 = x(x^2 + 4k^2)$.

$k = p_1 \cdots p_t$, each $p_i \equiv 5 \pmod 8$, each $\left(\frac{p_i}{p_j}\right) = 1$ for $i \neq j$
(t odd).

$$E_k(\mathbb{Q})/2E_k(\mathbb{Q}) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} : (x,y) \longmapsto [x, x+k]$$

$$\downarrow i_q \qquad\qquad \downarrow j_q$$

$$E_k(\mathbb{Q}_q)/2E_k(\mathbb{Q}_q) \hookrightarrow \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \times \mathbb{Q}_q^*/\mathbb{Q}_q^{*2}.$$

Using: $\boxed{\#E_k(\mathbb{Q}_q)/2E_k(\mathbb{Q}_q) = \#E_k(\mathbb{Q}_q)[2]}$ for $q \neq 2, \infty$

and local arguments : 2-Selmer bound on rank $\leq t+1$

Local arguments using descent via 2-isogeny : $2t-2$.

Yields arbitrarily large 2-part of Sha.

[Mention: Fisher, Flynn : runs out of steam, as hard to find C_p^g in $A(\mathbb{Q})$ to give $A \to \hat{A}' \to A$.]

Let $p > 3$ be prime.

Let J be Jacobian of $C : y^p = x(x-e_1)(x-e_2)$,

$0 \neq e_1, e_2 \in \mathbb{Z}$, distinct. Genus $g = p-1$.

Let $D_0 = [(0,0) - \infty]$, $D_1 = [(e_1,0) - \infty]$, $D_2 = [(e_2,0) - \infty] \in J(\mathbb{Q})$,

each order p [function $x - e_i$]. $D_0 + D_1 + D_2 = 0$ [function y].

Let $\underline{D = D_0 + D_1}$,

and $\hat{A} := J/H$, where $H = \langle D_0, D_1 \rangle \cong C_p \times C_p$

$\hat{B} := J/D$.

$\hat{\phi} : J \to \hat{A}$, $\hat{\psi} : J \to \hat{B}$.

Dual $\phi : A \to J$, $\psi : B \to J$

[identifying J with its dual via principal polarisation]

Define $\partial^H : J(\mathbb{Q})/\phi(A(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^p \times \mathbb{Q}^*/(\mathbb{Q}^*)^p$

$$: \left[\sum_{j=1}^{g} (x_j, y_j) - g\cdot\infty\right] \mapsto \left(\prod_{j=1}^{g} x_j, \prod_{j=1}^{g} (x_j - e_1)\right)$$

$\partial^D : J(\mathbb{Q})/\psi(B(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^p$

$$: \left[\sum_{j=1}^{g} (x_j, y_j) - g\cdot\infty\right] \mapsto \prod_{j=1}^{g} x_j (x_j - e_1).$$

Note: image elements can be written as

$r =$ p^{th}-power-free members of $\mathbb{Z}$,

and $\{\text{primes dividing } r\} \subseteq U = \{\text{primes dividing } pe_1e_2(e_1-e_2)\}$

Commutative diagram:

$$\begin{array}{ccc} J(\mathbb{Q})/\phi(A(\mathbb{Q})) & \xrightarrow{\partial^H} & \mathbb{Q}^*/(\mathbb{Q}^*)^p \times \mathbb{Q}^*/(\mathbb{Q}^*)^p \\ \downarrow & & \\ J(\mathbb{Q})/\hat{\phi}(B(\mathbb{Q})) & \xrightarrow{\partial^D} & \mathbb{Q}^*/(\mathbb{Q}^*)^p \end{array}$$

$[r_1, r_2] \in \mathbb{Z}$, $[r_1, r_2] \to r_1 r_2$

$$Sel(B) := \{r \in \mathbb{Z} : r \in \operatorname{im} \partial_q^H, \forall q\}$$

[where: ∂_q^H, ∂_q^D are the local maps] ← everywhere replacing $\mathbb{Q}$ by $\mathbb{Q}_q$ in above

---

Lemma Spse prime $q \equiv 1 \pmod p$. Then: $\#J(\mathbb{Q}_q)/\phi(A(\mathbb{Q}_q)) = p^2$.

Sketch Proof Let $\zeta_p \in \mathbb{Q}_q^*$ denote primitive p^{th} root of unity.
$[p \mid \#\mathbb{F}_q^*] \longrightarrow [\text{exists}]$.

$\zeta_p : J(\mathbb{Q}_q) \to J(\mathbb{Q}_q)$ induced by $(x,y) \mapsto (x, \zeta_p y)$ on C.

Can check that $1-\zeta_p$, $\hat{\phi}$ same kernel, and same map up to composition with automorphism.

J, A, $\hat{A}$ all isomorphic over $\mathbb{Q}_q$

Standard: $\#J(\mathbb{Q}_q)/(\widehat{1-\zeta_p})(J(\mathbb{Q}_q)) = \#J(\mathbb{Q}_q)[1-\zeta_p] = p^2$,

giving result [$\because J, A$ isom and $\widehat{1-\zeta_p} = \phi$ up to isom].

Note also:

$$0 \to J(\mathbb{Q})/\phi(B(\mathbb{Q})) \xrightarrow{\partial^D} Sel(B) \to Ш(B)[\phi] \to 0.$$

$\deg(\phi) = p$. $\quad Ш(B)[\phi] \subseteq Ш(B)[p]$.

[Difference: we don't have isogenous models, don't attempt an overall Selmer bound on rank. Instead, we find explicit r which we show to be in $Sel(B)$ but not in $\operatorname{im}\partial^D$.

For the latter, use the above lemma which gives $\#J(\mathbb{Q}_v)/\phi(A(\mathbb{Q}_v))$ for some v, and use commutative diagram to disquality r]

Let $\mathcal{C} = \mathcal{C}_{u,v} : y^p = x(x-3u)(x-9v)$

where prime $p > 3$ and $3 \nmid u$, $3 \nmid v$, $u, v \in \mathbb{Z}$, Jacobian J.

Twist : $\mathcal{C}_k = \mathcal{C}_{u,v,k} : y^p = x(x-3uk)(x-9vk)$, Jacobian J_k. Let $U = \{$primes dividing $3puv(u-3v)\}$

Let $k = p_1 \cdots p_t$, each $p_i \notin U$ satisfying:

(1) $p_i \in \left(\mathbb{Q}_{p_j}^*\right)^p$ $\forall i \neq j$ in $\{1, \cdots, t\}$.

(2) $p_i \in \left(\mathbb{Q}_q^*\right)^p$ $\forall i \in \{1, \cdots, t\}$, $q \in U$.

(3) $q \in \left(\mathbb{Q}_{p_i}^*\right)^p$ $\forall i \in \{1, \cdots, t\}$, $q \in U \setminus \{3\}$.

(4) $3 \notin \left(\mathbb{Q}_{p_i}^*\right)^p$ $\forall i \in \{1, \cdots, t\}$.

and corresponding $A_k, \hat{A}_k, B_k, \hat{B}_k$.

Thm. Each $p_i \notin \operatorname{im} \delta^0$,

$$p_i \in Sel(B).$$