The Enigmatic Tate-Shafarevich group.

$E/\mathbb{Q}$ – an elliptic curve over $\mathbb{Q}$.

$E(\mathbb{Q})$ – group of $\mathbb{Q}$-rational points.

g_E – in numerical examples, easy to determine g_E by classical arguments.

However, we are unable to prove most deep theoretical assertions about g_E because of our lack of knowledge about the Tate-Shafarevich group of E

Defn. $$Ш(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), E(\bar{\mathbb{Q}})) \to \bigoplus_v H^1(\mathrm{Gal}(\bar{\mathbb{Q}}_v/\mathbb{Q}_v), E(\bar{\mathbb{Q}}_v))\right).$$

This group is unquestionably the most enigmatic group in number theory, and probably in the whole of mathematics. It is a torsion abelian group

$$Ш(E/\mathbb{Q}) = \bigoplus_p Ш(E/\mathbb{Q})(p).$$

Classical Galois cohomology $\Rightarrow$

$$Ш(E/\mathbb{Q})(p) = \left(\mathbb{Q}_p/\mathbb{Z}_p\right)^{t_{E,p}} \oplus \text{finite group},$$

where $t_{E,p}$ is some integer ≥ 0.

Enigmatic for following reasons: —

(i). It is impossible by classical methods to compute $Ш(E/\mathbb{Q})(p)$ numerically once $p > 7$.

(ii). $Ш(E/\mathbb{Q})$ is conjectured to always be finite ($\Rightarrow t_{E,p} = 0$ for every p).

(iii). $Ш(E/\mathbb{Q})$ has never been proven finite for a single E with $g_E \geq 2$.

(iv). The BSD conjecture gives a nice analytic formula for $\#(Ш(E/\mathbb{Q}))$. Computations with this analytic formula suggest that $Ш(E/\mathbb{Q}) = 0$ for virtually all $E/\mathbb{Q}$ with $g_{E/\mathbb{Q}} \geq 2$.

Example 1. We recall that an integer $D \geq 1$ is said to be congruent if D is the area of a right-angled triangle, all of whose sides have rational length.

Lemma. D is congruent $\Leftrightarrow g_{E_D} \geq 1$ where

$$E_D : y^2 = x^3 - D^2 x.$$

Celebrated special case of BSD conjecture.

CONJECTURE. Every positive integer D with $D \equiv 5, 6, 7 \bmod 8$ is congruent.

Suffices. To prove $Ш(E_D)(\mathbb{Q})$ finite for a single D, but this is unknown.

Ye Tian of Chinese Academy of Sciences has very recently made deep progress on this problem.

Take $N = p_0 \cdots p_k$ where $p_0, \ldots, p_k$ are distinct odd primes with $p_1, \ldots, p_k \equiv 1 \bmod 8$ and $p_0 \equiv 3, 5, 7 \bmod 8$.

Defn. A = 2-primary subgroup of ideal class group of $\mathbb{Q}(\sqrt{-2N})$.

Theorem. Assume that $2A = 0$ when $N \equiv 3, 5 \bmod 8$, and $2A = \mathbb{Z}/2\mathbb{Z}$ when $N \equiv 7 \bmod 8$. Then N is congruent when $N \equiv 5, 7 \bmod 8$, and $2N$ is congruent if $N \equiv 3 \bmod 8$. In both cases, $Ш(E_D)$ is finite.

$k = 0$ (Heegner, followed by Birch, Stephens)
$k = 1$ (Monsky & Gross).

Tian uses induction on k, and uses some beautiful work by Zhao Chunlai of Peking University, as well as Shouwu Zhang's generalized Gross-Zagier formula.

Corollary. For every integer $s \geq 1$, there are infinitely many square free integers $D \geq 1$, which are congruent, have precisely s odd prime factors, and satisfy $D \equiv 5, 6, 7 \bmod 8$.

The proof uses Zhang's generalization of the Gross-Zagier formula, and some beautiful earlier work of Zhao Chunlai on the non-vanishing of certain L-values.

Earlier: $k = 0$ (Heegner and later Stephens), $k = 1$ Monsky.

The proof is a remarkable marriage of abstract methods and hard classical arguments.

Example 2. $y^2 = x^3 - 82x$

$g_E = 3$ $(-9, 3)$, $(-8, 12)$, $(-1, 9)$ generators mod torsion

BSD $\Rightarrow$ $Ш(E/\mathbb{Q}) = 0$.

Unknown. Is $Ш(E/\mathbb{Q})$ finite.

One of the great mysteries is the link between these problems of a purely arithmetic nature and L-functions arising from the conjecture of Birch and Swinnerton-Dyer.

$L(E, s)$ - complex L-function of $E/\mathbb{Q}$.

$L(E, s)$ is entire because of the deep theorem that E is modular (Wiles, ...).

Defn. $r_{E,\infty} = \operatorname{ord}_{s=1} L(E, s)$.

Conjecture (BSD): $r_{E,\infty} = g_E$.

Theorem (Kolyvagin, Gross-Zagier). If $r_{E,\infty} \leq 1$, then $r_{E,\infty} = g_E$ & $Ш(E/\mathbb{Q})$ is finite.

Theoretically, no link has ever been proven between $r_{E,\infty}$ & g_E when $r_{E,\infty} \geq 2$ (in particular, when $g_E \geq 2$). For example, it has never been shown that $r_{E,\infty} \geq g_E$ - indeed it has never been shown that $r_{E,\infty}$ is ≥ 4 for a single $E/\mathbb{Q}$.

However, when we pass to the p-adic world, the situation is completely different.

p - any prime where E has good ordinary reduction and $p > 2$.

$s \in \mathbb{Z}_p$.

Defn. $L_p(E, s)$ = p-adic L-function of $E/\mathbb{Q}$.

It is entire as a function of s (an Iwasawa function).

Key Fact. The so called "Main Conjectures" of Iwasawa theory imply (unconditionally) the following theorem.

Defn. $r_{E,p} = \operatorname{ord}_{s=1} L_p(E, s)$.

Theorem. $r_{E,p} \geq g_E + t_{E,p}$.

Opens the door to proving two types of results which are at present inaccessible with the complex L-function

(i). An upper bound for $r_{E,p}$ will at least give an upper bound for $t_{E,p}$.

(ii). Numerical determination of $r_{E,p}$ will give numerical upper bound for $t_{E,p}$ $(r_{E,p} = g_E \Rightarrow t_{E,p} = 0)$.

One can carry through this programme for all $E/\mathbb{Q}$ but at present we get much stronger results if we work with E admitting complex multiplication.

Defn. We say E admits complex multiplication if $K = \operatorname{End}_{\bar{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic field.

Assume E admits CM $\longleftrightarrow$ ψ_E = grossencharacter of E/K.

p ordinary $\Rightarrow p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$.

K_∞ = unique Galois extension of K, unramified outside of $\mathfrak{p}$, with $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$.

There is a unique p-adic L-function $L_{\mathfrak{p}}(E,s)$ related to E/K_∞ via a main conjecture.

$\mathcal{L}$ = period lattice of E = $\Omega_\infty \mathcal{O}_K$, $\Omega_\infty \in \mathbb{C}^\times$.

Fact. There exists a unique $L_{\mathfrak{p}}(E,s)$ such that

$$L_{\mathfrak{p}}(E,n) = \Omega_{\mathfrak{p}}^{n}\,\Omega_\infty^{-n}\,(n-1)!\,L(\overline{\psi}_E^{\,n}, n)\left(1 - \frac{\psi_E^{n}(\mathfrak{p})}{N\mathfrak{p}}\right)$$

for all integers $n \geq 1$ with $n \equiv 1 \bmod (p-1)$.

Key remark for bounding $r_{E,\mathfrak{p}} = \mathrm{ord}_{s=1} L_{\mathfrak{p}}(E,s)$.

$\Omega_{\mathfrak{p}}^{-p} L_{\mathfrak{p}}(E,p) \neq 0$ and belongs to $\mathbb{Q}_p K^\times$.

Main Conjecture $\Rightarrow$ $r_{E,\mathfrak{p}} \geq g_E + t_{E,p}$.

In this way we can prove:—

Theorem. Assume E has CM. Then, for each $\varepsilon > 0$, we have $t_{E,p} \leq \left(\frac{1}{2} + \varepsilon\right)p - g_E$ for all sufficiently large good ordinary primes p.

Weak but the first theoretical result of its kind.