

Counting elliptic curves with an isogeny of degree three

John Voight
Dartmouth College

Joint work with
Maggie Pizzo and Carl Pomerance

West Coast Number Theory
Asilomar
17 December 2019

Torsion is rare

Torsion is rare

To quantify the fact that most elliptic curves do not have torsion, we count as follows.

Torsion is rare

To quantify the fact that most elliptic curves do not have torsion, we count as follows.

Every elliptic curve E over \mathbb{Q} is uniquely of the form

$$E: y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$ satisfying $4A^3 + 27B^2 \neq 0$ and such that there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$.

Torsion is rare

To quantify the fact that most elliptic curves do not have torsion, we count as follows.

Every elliptic curve E over \mathbb{Q} is uniquely of the form

$$E: y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$ satisfying $4A^3 + 27B^2 \neq 0$ and such that there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$.

For each such elliptic curve E , define its *height*:

$$\text{ht } E := \max(|4A^3|, |27B^2|).$$

Torsion is rare

To quantify the fact that most elliptic curves do not have torsion, we count as follows.

Every elliptic curve E over \mathbb{Q} is uniquely of the form

$$E: y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$ satisfying $4A^3 + 27B^2 \neq 0$ and such that there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$.

For each such elliptic curve E , define its *height*:

$$\text{ht } E := \max(|4A^3|, |27B^2|).$$

By Mazur's theorem, there are only finitely many possible groups G such that $E(\mathbb{Q})_{\text{tors}} \simeq G$.

Torsion is rare

To quantify the fact that most elliptic curves do not have torsion, we count as follows.

Every elliptic curve E over \mathbb{Q} is uniquely of the form

$$E: y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$ satisfying $4A^3 + 27B^2 \neq 0$ and such that there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$.

For each such elliptic curve E , define its *height*:

$$\text{ht } E := \max(|4A^3|, |27B^2|).$$

By Mazur's theorem, there are only finitely many possible groups G such that $E(\mathbb{Q})_{\text{tors}} \simeq G$. For each such group G , Harron–Snowden prove that

Torsion is rare

To quantify the fact that most elliptic curves do not have torsion, we count as follows.

Every elliptic curve E over \mathbb{Q} is uniquely of the form

$$E: y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$ satisfying $4A^3 + 27B^2 \neq 0$ and such that there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$.

For each such elliptic curve E , define its *height*:

$$\text{ht } E := \max(|4A^3|, |27B^2|).$$

By Mazur's theorem, there are only finitely many possible groups G such that $E(\mathbb{Q})_{\text{tors}} \simeq G$. For each such group G , Harroon–Snowden prove that

$$N_G(H) := \#\{E : \text{ht}(E) \leq H \text{ and } E(\mathbb{Q})_{\text{tors}} \simeq G\}$$

Torsion is rare

To quantify the fact that most elliptic curves do not have torsion, we count as follows.

Every elliptic curve E over \mathbb{Q} is uniquely of the form

$$E: y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$ satisfying $4A^3 + 27B^2 \neq 0$ and such that there is no prime ℓ such that $\ell^4 \mid A$ and $\ell^6 \mid B$.

For each such elliptic curve E , define its *height*:

$$\text{ht } E := \max(|4A^3|, |27B^2|).$$

By Mazur's theorem, there are only finitely many possible groups G such that $E(\mathbb{Q})_{\text{tors}} \simeq G$. For each such group G , Harron–Snowden prove that

$$N_G(H) := \#\{E : \text{ht}(E) \leq H \text{ and } E(\mathbb{Q})_{\text{tors}} \simeq G\} \asymp H^{1/d(G)}$$

(for H large), where $d(G)$ is given explicitly.

Torsion is rare (Harron–Snowden)

$$N_G(H) := \#\{E : \text{ht}(E) \leq H \text{ and } E(\mathbb{Q})_{\text{tors}} \simeq G\} \asymp H^{1/d(G)}$$

G	$\# \text{ curves} = H^{1/d(G)}$
–	$H^{5/6}$
$\mathbb{Z}/2\mathbb{Z}$	$H^{1/2}$
$\mathbb{Z}/3\mathbb{Z}$	$H^{1/3}$
$\mathbb{Z}/4\mathbb{Z}$	$H^{1/4}$
$\mathbb{Z}/5\mathbb{Z}$	$H^{1/6}$
$\mathbb{Z}/6\mathbb{Z}$	$H^{1/6}$
$\mathbb{Z}/7\mathbb{Z}$	$H^{1/12}$
$\mathbb{Z}/8\mathbb{Z}$	$H^{1/12}$
$\mathbb{Z}/9\mathbb{Z}$	$H^{1/18}$
$\mathbb{Z}/10\mathbb{Z}$	$H^{1/18}$
$\mathbb{Z}/12\mathbb{Z}$	$H^{1/24}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$H^{1/3}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$H^{1/6}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$H^{1/12}$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$H^{1/24}$

Explicit asymptotics

Explicit asymptotics

To study $\#\{E : \text{ht}(E) \leq H\}$, we need to count pairs

$$(A, B) \in \mathbb{Z}^2 \text{ such that } |A| \leq (H/4)^{1/3}, |B| \leq (H/27)^{1/2}$$

and then sieve out those with $\ell^4 \mid A, \ell^6 \mid B$ for some prime ℓ ;

Explicit asymptotics

To study $\#\{E : \text{ht}(E) \leq H\}$, we need to count pairs

$$(A, B) \in \mathbb{Z}^2 \text{ such that } |A| \leq (H/4)^{1/3}, |B| \leq (H/27)^{1/2}$$

and then sieve out those with $\ell^4 \mid A, \ell^6 \mid B$ for some prime ℓ ; the number with $4A^3 + 27B^2 = 0$ are only $O(H^{1/6})$.

Explicit asymptotics

To study $\#\{E : \text{ht}(E) \leq H\}$, we need to count pairs

$$(A, B) \in \mathbb{Z}^2 \text{ such that } |A| \leq (H/4)^{1/3}, |B| \leq (H/27)^{1/2}$$

and then sieve out those with $\ell^4 \mid A, \ell^6 \mid B$ for some prime ℓ ; the number with $4A^3 + 27B^2 = 0$ are only $O(H^{1/6})$. So we need to count lattice points in a rectangle with sides of lengths $2(H/4)^{1/3}$ and $2(H/27)^{1/2}$, as $H \rightarrow \infty$.

Explicit asymptotics

To study $\#\{E : \text{ht}(E) \leq H\}$, we need to count pairs

$$(A, B) \in \mathbb{Z}^2 \text{ such that } |A| \leq (H/4)^{1/3}, |B| \leq (H/27)^{1/2}$$

and then sieve out those with $\ell^4 \mid A, \ell^6 \mid B$ for some prime ℓ ; the number with $4A^3 + 27B^2 = 0$ are only $O(H^{1/6})$. So we need to count lattice points in a rectangle with sides of lengths $2(H/4)^{1/3}$ and $2(H/27)^{1/2}$, as $H \rightarrow \infty$.

By the Principle of Lipschitz, the number of lattice points in a region is given by its area up to an error proportional to length of its (rectifiable) boundary.

Explicit asymptotics

To study $\#\{E : \text{ht}(E) \leq H\}$, we need to count pairs

$$(A, B) \in \mathbb{Z}^2 \text{ such that } |A| \leq (H/4)^{1/3}, |B| \leq (H/27)^{1/2}$$

and then sieve out those with $\ell^4 \mid A, \ell^6 \mid B$ for some prime ℓ ; the number with $4A^3 + 27B^2 = 0$ are only $O(H^{1/6})$. So we need to count lattice points in a rectangle with sides of lengths $2(H/4)^{1/3}$ and $2(H/27)^{1/2}$, as $H \rightarrow \infty$.

By the Principle of Lipschitz, the number of lattice points in a region is given by its area up to an error proportional to length of its (rectifiable) boundary. So the above count is

$$4(1/4)^{1/3}(1/27)^{1/2}H^{5/6} + O(H^{1/2}).$$

Explicit asymptotics

To study $\#\{E : \text{ht}(E) \leq H\}$, we need to count pairs

$$(A, B) \in \mathbb{Z}^2 \text{ such that } |A| \leq (H/4)^{1/3}, |B| \leq (H/27)^{1/2}$$

and then sieve out those with $\ell^4 \mid A, \ell^6 \mid B$ for some prime ℓ ; the number with $4A^3 + 27B^2 = 0$ are only $O(H^{1/6})$. So we need to count lattice points in a rectangle with sides of lengths $2(H/4)^{1/3}$ and $2(H/27)^{1/2}$, as $H \rightarrow \infty$.

By the Principle of Lipschitz, the number of lattice points in a region is given by its area up to an error proportional to length of its (rectifiable) boundary. So the above count is

$$4(1/4)^{1/3}(1/27)^{1/2}H^{5/6} + O(H^{1/2}).$$

The condition at ℓ says we have *overcounted* and need to multiply the result by $1 - \ell^{-10}$;

Explicit asymptotics

To study $\#\{E : \text{ht}(E) \leq H\}$, we need to count pairs

$$(A, B) \in \mathbb{Z}^2 \text{ such that } |A| \leq (H/4)^{1/3}, |B| \leq (H/27)^{1/2}$$

and then sieve out those with $\ell^4 \mid A, \ell^6 \mid B$ for some prime ℓ ; the number with $4A^3 + 27B^2 = 0$ are only $O(H^{1/6})$. So we need to count lattice points in a rectangle with sides of lengths $2(H/4)^{1/3}$ and $2(H/27)^{1/2}$, as $H \rightarrow \infty$.

By the Principle of Lipschitz, the number of lattice points in a region is given by its area up to an error proportional to length of its (rectifiable) boundary. So the above count is

$$4(1/4)^{1/3}(1/27)^{1/2}H^{5/6} + O(H^{1/2}).$$

The condition at ℓ says we have *overcounted* and need to multiply the result by $1 - \ell^{-10}$; a standard sieve argument then gives

$$\#\{E : \text{ht}(E) \leq H\} = 2^{4/3}3^{-3/2}\zeta(10)^{-1}H^{5/6} + O(H^{1/2}).$$

Explicit asymptotics: $\#G = 2, 3$

Explicit asymptotics: $\#G = 2, 3$

Harron–Snowden carried out this strategy for the cases $\#G = 2, 3$:

$$\begin{aligned} \#\{E : \text{ht}(E) \leq H \text{ and } E(\mathbb{Q})_{\text{tors}} \simeq G\} \\ = \frac{\text{area}(R_G)}{\zeta(12/d(G))} H^{1/d(G)} + O(H^{1/e(G)}) \end{aligned}$$

for

G	$H^{1/d(G)}$	$O(H^{1/e(G)})$
–	$H^{5/6}$	$O(H^{1/2})$
$\mathbb{Z}/2\mathbb{Z}$	$H^{1/2}$	$O(H^{1/3})$
$\mathbb{Z}/3\mathbb{Z}$	$H^{1/3}$	$O(H^{1/4})$

Explicit asymptotics: $\#G = 2, 3$

Harron–Snowden carried out this strategy for the cases $\#G = 2, 3$:

$$\begin{aligned} \#\{E : \text{ht}(E) \leq H \text{ and } E(\mathbb{Q})_{\text{tors}} \simeq G\} \\ = \frac{\text{area}(R_G)}{\zeta(12/d(G))} H^{1/d(G)} + O(H^{1/e(G)}) \end{aligned}$$

for

G	$H^{1/d(G)}$	$O(H^{1/e(G)})$
–	$H^{5/6}$	$O(H^{1/2})$
$\mathbb{Z}/2\mathbb{Z}$	$H^{1/2}$	$O(H^{1/3})$
$\mathbb{Z}/3\mathbb{Z}$	$H^{1/3}$	$O(H^{1/4})$

Question

Without computing the constant, can one use this method to prove there exists an effectively computable constant for all G ?

Question

In the cases above, is there a (meaningful?) secondary term?

Counting isogenies

Counting isogenies

Today, we count elliptic curves *with an isogeny* (over \mathbb{Q}).

Counting isogenies

Today, we count elliptic curves *with an isogeny (over \mathbb{Q})*.

For $m \in \mathbb{Z}_{\geq 1}$, let

$$N_{m,\text{cyc}}(H) := \left\{ E : \begin{array}{l} \text{ht}(E) \leq H \text{ and} \\ \text{there exists } \phi: E \rightarrow E' \text{ cyclic of degree } m \end{array} \right\}.$$

Counting isogenies

Today, we count elliptic curves *with an isogeny (over \mathbb{Q})*.

For $m \in \mathbb{Z}_{\geq 1}$, let

$$N_{m,\text{cyc}}(H) := \left\{ E : \begin{array}{l} \text{ht}(E) \leq H \text{ and} \\ \text{there exists } \phi: E \rightarrow E' \text{ cyclic of degree } m \end{array} \right\}.$$

For $m = 1, 2$, a generator of the kernel of a cyclic m -isogeny is a rational m -torsion point, so we are in the previous case:

$$N_{m,\text{cyc}}(H) = N_{\mathbb{Z}/m\mathbb{Z}}(H) \text{ for } m = 1, 2.$$

Counting isogenies

Today, we count elliptic curves *with an isogeny* (over \mathbb{Q}).

For $m \in \mathbb{Z}_{\geq 1}$, let

$$N_{m,\text{cyc}}(H) := \left\{ E : \begin{array}{l} \text{ht}(E) \leq H \text{ and} \\ \text{there exists } \phi: E \rightarrow E' \text{ cyclic of degree } m \end{array} \right\}.$$

For $m = 1, 2$, a generator of the kernel of a cyclic m -isogeny is a rational m -torsion point, so we are in the previous case:

$N_{m,\text{cyc}}(H) = N_{\mathbb{Z}/m\mathbb{Z}}(H)$ for $m = 1, 2$. (In terms of modular curves, $X_1(m) = X_0(m)$ for $m = 1, 2$.)

Counting isogenies

Today, we count elliptic curves *with an isogeny (over \mathbb{Q})*.

For $m \in \mathbb{Z}_{\geq 1}$, let

$$N_{m,\text{cyc}}(H) := \left\{ E : \begin{array}{l} \text{ht}(E) \leq H \text{ and} \\ \text{there exists } \phi: E \rightarrow E' \text{ cyclic of degree } m \end{array} \right\}.$$

For $m = 1, 2$, a generator of the kernel of a cyclic m -isogeny is a rational m -torsion point, so we are in the previous case:

$N_{m,\text{cyc}}(H) = N_{\mathbb{Z}/m\mathbb{Z}}(H)$ for $m = 1, 2$. (In terms of modular curves, $X_1(m) = X_0(m)$ for $m = 1, 2$.)

Example

On $E: y^2 = x^3 - 1$, the subgroup $C := \langle \infty, (0, \pm\sqrt{-1}) \rangle$ defines a 3-isogeny $\phi: E \rightarrow E/C$, where $E/C: y^2 = x^3 + 27$ and $\phi(x, y) = (x - 4/x^2, (1 + 8/x^3)y)$.

Main result: counting cyclic 3-isogenies

Main result: counting cyclic 3-isogenies

Theorem (Pizzo–Pomerance–V)

There exist $c_1, c_2 \in \mathbb{R}$ such that for $H \geq 1$,

$$N_{3,\text{cyc}}(H) = \frac{2}{3\sqrt{3}\zeta(6)} H^{1/2} + c_1 H^{1/3} \log H + c_2 H^{1/3} + O(H^{7/24}).$$

Main result: counting cyclic 3-isogenies

Theorem (Pizzo–Pomerance–V)

There exist $c_1, c_2 \in \mathbb{R}$ such that for $H \geq 1$,

$$N_{3,\text{cyc}}(H) = \frac{2}{3\sqrt{3}\zeta(6)} H^{1/2} + c_1 H^{1/3} \log H + c_2 H^{1/3} + O(H^{7/24}).$$

Moreover,

$$\frac{2}{3\sqrt{3}\zeta(6)} = 0.378338\dots \quad c_1 = \frac{c_0}{8\pi^2\zeta(4)} = 0.107437\dots$$

where c_0 is explicitly given (as an integral) and c_2 is effectively computable.

Main result: counting cyclic 3-isogenies

Theorem (Pizzo–Pomerance–V)

There exist $c_1, c_2 \in \mathbb{R}$ such that for $H \geq 1$,

$$N_{3,\text{cyc}}(H) = \frac{2}{3\sqrt{3}\zeta(6)} H^{1/2} + c_1 H^{1/3} \log H + c_2 H^{1/3} + O(H^{7/24}).$$

Moreover,

$$\frac{2}{3\sqrt{3}\zeta(6)} = 0.378338\dots \quad c_1 = \frac{c_0}{8\pi^2\zeta(4)} = 0.107437\dots$$

where c_0 is explicitly given (as an integral) and c_2 is effectively computable.

- ▶ Same asymptotic if we count those *equipped* with a 3-isogeny.

Main result: counting cyclic 3-isogenies

Theorem (Pizzo–Pomerance–V)

There exist $c_1, c_2 \in \mathbb{R}$ such that for $H \geq 1$,

$$N_{3,\text{cyc}}(H) = \frac{2}{3\sqrt{3}\zeta(6)} H^{1/2} + c_1 H^{1/3} \log H + c_2 H^{1/3} + O(H^{7/24}).$$

Moreover,

$$\frac{2}{3\sqrt{3}\zeta(6)} = 0.378338\dots \quad c_1 = \frac{c_0}{8\pi^2\zeta(4)} = 0.107437\dots$$

where c_0 is explicitly given (as an integral) and c_2 is effectively computable.

- ▶ Same asymptotic if we count those *equipped* with a 3-isogeny.
- ▶ The main term of order $H^{1/2}$ counts *just* those elliptic curves with $A = 0$ (having j -invariant 0).

Main result: counting cyclic 3-isogenies

Theorem (Pizzo–Pomerance–V)

There exist $c_1, c_2 \in \mathbb{R}$ such that for $H \geq 1$,

$$N_{3,\text{cyc}}(H) = \frac{2}{3\sqrt{3}\zeta(6)} H^{1/2} + c_1 H^{1/3} \log H + c_2 H^{1/3} + O(H^{7/24}).$$

Moreover,

$$\frac{2}{3\sqrt{3}\zeta(6)} = 0.378338\dots \quad c_1 = \frac{c_0}{8\pi^2\zeta(4)} = 0.107437\dots$$

where c_0 is explicitly given (as an integral) and c_2 is effectively computable.

- ▶ Same asymptotic if we count those *equipped* with a 3-isogeny.
- ▶ The main term of order $H^{1/2}$ counts *just* those elliptic curves with $A = 0$ (having j -invariant 0).
- ▶ Matches computations to $H = 10^{25}$, suggesting $c_2 \approx 0.163$.

A hint of the proof

A hint of the proof

An elliptic curve E has a 3-isogeny (defined over \mathbb{Q}) if and only if its 3-division polynomial

$$\psi(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

has a root in \mathbb{Q} ;

A hint of the proof

An elliptic curve E has a 3-isogeny (defined over \mathbb{Q}) if and only if its 3-division polynomial

$$\psi(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

has a root in \mathbb{Q} ; if $a \in \mathbb{Q}$ is such a root, then in fact $a \in \mathbb{Z}$.

A hint of the proof

An elliptic curve E has a 3-isogeny (defined over \mathbb{Q}) if and only if its 3-division polynomial

$$\psi(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

has a root in \mathbb{Q} ; if $a \in \mathbb{Q}$ is such a root, then in fact $a \in \mathbb{Z}$.

So we need to count triples $(A, B, a) \in \mathbb{Z}^3$ satisfying:

- (N1) $A \neq 0$ and $\psi_{A,B}(a) = 0$;
- (N2) $|4A^3|, |27B^2| \leq H$;
- (N3) $4A^3 + 27B^2 \neq 0$; and
- (N4) there is no prime ℓ with $\ell^4 \mid A$ and $\ell^6 \mid B$.

A hint of the proof

An elliptic curve E has a 3-isogeny (defined over \mathbb{Q}) if and only if its 3-division polynomial

$$\psi(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

has a root in \mathbb{Q} ; if $a \in \mathbb{Q}$ is such a root, then in fact $a \in \mathbb{Z}$.

So we need to count triples $(A, B, a) \in \mathbb{Z}^3$ satisfying:

- (N1) $A \neq 0$ and $\psi_{A,B}(a) = 0$;
- (N2) $|4A^3|, |27B^2| \leq H$;
- (N3) $4A^3 + 27B^2 \neq 0$; and
- (N4) there is no prime ℓ with $\ell^4 \mid A$ and $\ell^6 \mid B$.

We show that this count is of size $H^{1/3} \log H$;

A hint of the proof

An elliptic curve E has a 3-isogeny (defined over \mathbb{Q}) if and only if its 3-division polynomial

$$\psi(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

has a root in \mathbb{Q} ; if $a \in \mathbb{Q}$ is such a root, then in fact $a \in \mathbb{Z}$.

So we need to count triples $(A, B, a) \in \mathbb{Z}^3$ satisfying:

(N1) $A \neq 0$ and $\psi_{A,B}(a) = 0$;

(N2) $|4A^3|, |27B^2| \leq H$;

(N3) $4A^3 + 27B^2 \neq 0$; and

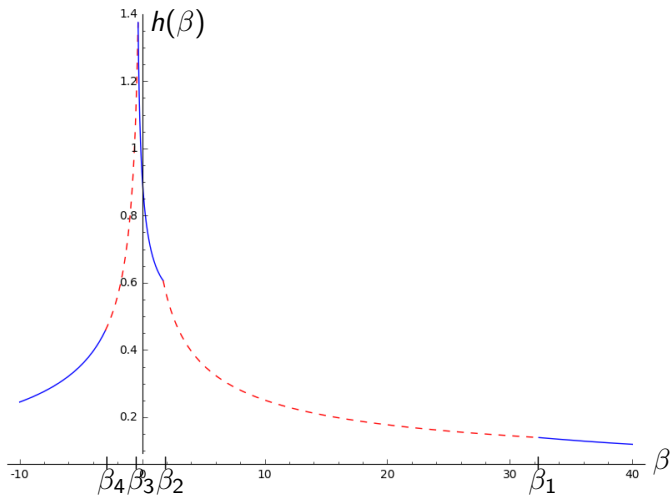
(N4) there is no prime ℓ with $\ell^4 \mid A$ and $\ell^6 \mid B$.

We show that this count is of size $H^{1/3} \log H$; we use that

$$12B = \frac{A^2}{a} - 6Aa - 3a^3$$

so it is enough to work with A, a such that $a \mid A^2$, together with conditions at 2, 3.

Our region



Conclusion (Main result again)

Theorem (Pizzo–Pomerance–V)

There exist $c_1, c_2 \in \mathbb{R}$ such that for $H \geq 1$,

$$N_{3,\text{cyc}}(H) = \frac{2}{3\sqrt{3}\zeta(6)} H^{1/2} + c_1 H^{1/3} \log H + c_2 H^{1/3} + O(H^{7/24}).$$

Moreover,

$$\frac{2}{3\sqrt{3}\zeta(6)} = 0.378338\dots \quad c_1 = \frac{c_0}{8\pi^2\zeta(4)} = 0.107437\dots$$

where c_0 is explicitly given (as an integral) and c_2 is effectively computable.

Conclusion (Main result again)

Theorem (Pizzo–Pomerance–V)

There exist $c_1, c_2 \in \mathbb{R}$ such that for $H \geq 1$,

$$N_{3,\text{cyc}}(H) = \frac{2}{3\sqrt{3}\zeta(6)} H^{1/2} + c_1 H^{1/3} \log H + c_2 H^{1/3} + O(H^{7/24}).$$

Moreover,

$$\frac{2}{3\sqrt{3}\zeta(6)} = 0.378338\dots \quad c_1 = \frac{c_0}{8\pi^2\zeta(4)} = 0.107437\dots$$

where c_0 is explicitly given (as an integral) and c_2 is effectively computable.

We hope that our method and the lower-order terms in our result will be useful in understanding counts of rational points on stacky curves (as in recent work of Ellenberg–Satriano–Zureick-Brown).