ON ASYMPTOTIC EQUIVALENCE OF ELLIPTIC CURVES OVER $\mathbb{Q}$

ABSTRACT. This short paper asks a question about a new asymptotic symmetry of the moduli space of Frey–Hellegouarch elliptic curves over rational numbers. If the answer to the question is positive then this allows to deduce an effective $(1+\varepsilon)$ abc-inequality from effective abc-inequalities established in [3].

1. An elliptic curve over $\mathbb{Q}$ with all its 2-torsions points $\mathbb{Q}$-rational is isomorphic over an algebraic closure of $\mathbb{Q}$ to a (Frey–Hellegouarch) curve $E_{a,b}$ with affine equation

$$y^2 = x(x+a)(x-b)$$

for some coprime non-zero integers a, b. It can be written in the Weierstrass form as

$$Y^2 = X^3 - 27c_4X - 54c_6, \quad c_4 = 16(a^2+ab+b^2), \quad c_6 = 32(b-a)(2a+b)(a+2b).$$

Its discriminant $\Delta = (c_4^3 - c_6^2)/1728 = 16(ab(a+b))^2$. The minimal discriminant of $E_{a,b}$ is the same if 16 does not divide abc or if $a \equiv -1 \mod 4$ and $b \equiv 0 \mod 16$, and $16^{-2}(ab(a+b))^2$ if $a \equiv 1 \mod 4$ and $b \equiv 0 \mod 16$.

Every elliptic curve over $\mathbb{Q}$ all of whose 2-torsion points are in $\mathbb{Q}$ is isomorphic over the algebraic closure of $\mathbb{Q}$ to such a curve.

In particular,

$$(a^2+ab+b^2)^3 = ((b-a)(2a+b)(a+2b)/2)^2 + 3^3(ab(a+b)/2)^2. \qquad (\dagger)$$

The j-invariant of the Weierstrass equation is

$$j_{a,b} = 2^8 \cdot \frac{(a^2+ab+b^2)^3}{(ab(a+b))^2} = 2^6 \cdot \frac{((b-a)(2a+b)(a+2b))^2}{(ab(a+b))^2} + 2^6 \cdot 3^3.$$

For a non-zero integer its radical rad is the product of its prime divisors taken each with multiplicity one and its odd radical rad$'$ is the product of its odd prime divisors taken each with multiplicity one.

If $16 \not| ab(a+b)$ then $\mathrm{cond}(E_{a,b}) < 2^{12}\mathrm{rad}'(ab(a+b))$. If $16|ab(a+b)$ and say $4|(a-1)$, $16|b$ then $\mathrm{cond}(E_{a,b}) = \mathrm{rad}(2^{-4}ab(a+b)) \leqslant \mathrm{rad}(ab(a+b))$. If $16|ab(a+b)$ and say $4|(a+1)$, $16|b$ then $\mathrm{cond}(E_{a,b}) \leqslant 2^{4+2l}\mathrm{rad}'(ab(a+b))$ where l is the maximal power of 2 dividing b. All this is very well known. See e.g. sect. 12.5 of [1]. Note that the statement "Since E has multiplicative reduction all all primes $p|\Delta$" in the top line of its p.434 is incorrect as the example of $E_{1,16}$ shows, but the inequality for the LHS and RHS of the next displayed inequality on that page is correct.

Now let in addition $0 < a < b$, a, b are still coprime. Put $c = a+b$. Define

$$A = (b-a)/d, B = (2a+b)/d, C = A+B = (a+2b)/d,$$

where $d = \gcd(b-a, 2a+b)$ $(= 1$ or $3)$. Then $0 < A < B$, and A, B are coprime.

We have

$$a^2+ab+b^2=d^2(A^2+AB+B^2)/3,$$
$$ab(a+b)=d^3(B-A)(A+2B)(2A+B)/3^3,$$
$$(b-a)(2a+b)(a+2b)=d^3AB(A+B).$$

The map $\phi\colon (a,b)\mapsto (A,B)$ is an involution: $\phi^2=\mathrm{id}$. It is a special map relating the two terms on the RHS of $(\dagger)$. Thus we have an involution map on the moduli space of Frey–Hellegouarch elliptic curves: $E_{a,b}\mapsto E_{A,B}$.

From $(\dagger)$ one gets

$$(a^2+ab+b^2)^3=((b-a)(2a+b)(a+2b)/2)^2+3^3\,(ab(a+b)/2)^2.$$

and

$$(A^2+AB+B^2)^3=3^3\,(AB(A+B)/2)^2+((B-A)(2A+B)(A+2B)/2)^2.$$

We also have $j_{A,B}=12^3 j_{a,b}/(j_{a,b}-12^3)=(12^{-3}-j_{a,b}^{-1})^{-1}$.

Question (abc-ABC question). *Are the following equivalent statements true?*
1. $\mathrm{rad}(abc)$ *and* $\mathrm{rad}(ABC)$ *are effectively asymptotically equal, i.e. for every* $\varepsilon>0$ *there are constants* $\mathfrak{c}_\varepsilon,\mathfrak{c}'_\varepsilon$*, effectively depending on* ε*, such that for all relatively prime positive* $a<b$

$$\mathrm{rad}(abc)<\mathfrak{c}_\varepsilon\cdot\mathrm{rad}(ABC)^{1+\varepsilon},\quad \mathrm{rad}(ABC)<\mathfrak{c}'_\varepsilon\cdot\mathrm{rad}(abc)^{1+\varepsilon}.$$

2. For every $\varepsilon>0$ *there is a positive constant* κ_ε *such that for all positive coprime integers* $a<b$

$$\mathrm{rad}((b-a)(2a+b)(a+2b))<\kappa_\varepsilon\cdot\mathrm{rad}(ab(a+b))^{1+\varepsilon}$$

with κ_ε *effectively dependent on* ε*.*
3. $\mathrm{rad}(\Delta(E_{a,b}))$ *and* $\mathrm{rad}(\Delta(E_{A,B}))$ *are effectively asymptotically equivalent.*
4. $\mathrm{rad}(c_6(E_{a,b}))$ *and* $\mathrm{rad}(\Delta(E_{a,b}))$ *are effectively asymptotically equivalent.*

The proof of the equivalences is immediate.

The involution ϕ corresponds to $x\mapsto(1-x)/(2x+1)$ on $\mathbb{P}^1$ sending the divisor $[0]+[1]+[\infty]$ to $[0]+[1]+[-1/2]$. We have $\mathrm{rad}(abc)=\mathrm{cond}_{[0]+[1]+[\infty]}(a:b)=\mathrm{cond}_{[0]+[1]+[-1/2]}(A:B)$ and $\mathrm{rad}(ABC)=\mathrm{cond}_{[0]+[1]+[\infty]}(A:B)$.

The positive answer to the Question signifies a new asymptotic symmetry of the moduli space of elliptic curves over $\mathbb{Q}$ all of whose 2-torsion points are $\mathbb{Q}$-rational.

2. A recent paper [3] slightly extends the IUT theory of S. Mochizuki [2] and establishes two effective abc inequalities.

One of the established effective abc inequalities is:

for every $\varepsilon>0$ *there is an effectively described constant* C'_ε *such that for all relatively prime positive integer numbers* a,b*, the inequality*

$$\log(a+b)<1.5(1+\varepsilon)\cdot\log\mathrm{rad}(ab(a+b))+C'_\varepsilon$$

holds. The constant C'_1 is slightly larger than $8.5\cdot 10^{29}$. A version of this inequality is also established over quadratic imaginary fields.

Another established effective abc inequality is:

for every $\varepsilon > 0$ *there is an effectively described constant* C_ε *such that for all relatively prime positive integer numbers* a, b*, the inequality*

$$\log(ab(a+b)) < 3(1+\varepsilon)\cdot \log \operatorname{rad}(ab(a+b)) + C_\varepsilon$$

holds. The constant C_1 is slightly larger than $1.7\cdot 10^{30}$.

The second abc inequality implies the first one. The second inequality was stated as a conjecture by Szpiro in [4] in 1990.

Among several motivations for the Question in the previous section, one motivation comes from the study of an issue of how to deduce an effective $(1+\varepsilon)$-abc inequality from the effective abc inequalities in [3] and mentioned above. Let's see how a potential positive answer to the abc-ABC Question helps in this direction.

Fix a positive integer m. The second abc inequality above implies that *for every positive* ε *for all non-zero integers* a,b,c *such that* $a+b+c=0$ *and* $\gcd(a,b,c)$ *divides* m *we have*

$$\log|abc| < 3(1+\varepsilon)\cdot \log \operatorname{rad}(abc) + C_\varepsilon + 3\log m. \qquad (\sharp)$$

In view of (†), consider the equation

$$x^3 = y^2 + 3^3 z^2, \qquad x,y,z>0, \quad \gcd(x,y,z)|3.$$

The following is a variation of arguments presented in sect. 12.5 of [1].

Applying ($\sharp$), we obtain $x^3y^2z^2 \ll_\varepsilon \operatorname{rad}(xyz)^{3(1+\varepsilon)}$. Since $y^2\cdot 3^3z^2 \leqslant x^6/4$, we deduce $yz \ll_\varepsilon \operatorname{rad}(xyz)^{1+\varepsilon}$. Assume that $y^2 \leqslant 3^3z^2$, then we deduce $y \ll_\varepsilon \operatorname{rad}(xyz)^{(1+\varepsilon)/2}$, and since $x^3 \leqslant 2\cdot 3^3z^2$, we get $x^6y^2 \leqslant x^3\cdot 2\cdot 3^3z^2\cdot y^2 \ll_\varepsilon \operatorname{rad}(xyz)^{3(1+\varepsilon)}$ and $x^6y^6 \ll_\varepsilon \operatorname{rad}(xyz)^{5(1+\varepsilon)}$, so $xy \ll_\varepsilon \operatorname{rad}(z)^{5(1+\varepsilon)}$. Substituting the latter in the RHS of $y \ll_\varepsilon \operatorname{rad}(xyz)^{(1+\varepsilon)/2}$, we obtain $y \ll_\varepsilon \operatorname{rad}(z)^{3(1+\varepsilon)}$. From $x^6y^2 \ll_\varepsilon \operatorname{rad}(xyz)^{3(1+\varepsilon)}$ we deduce $x^3 \ll_\varepsilon y^{1+\varepsilon}\cdot \operatorname{rad}(z)^{3(1+\varepsilon)}$ so $x^3 \ll_\varepsilon \operatorname{rad}(z)^{6(1+\varepsilon)}$, hence $x \ll_\varepsilon \operatorname{rad}(z)^{2(1+\varepsilon)}$. Thus, ($\sharp$) implies: if $y^2 \leqslant 3^3z^2$ then $x \ll_\varepsilon \operatorname{rad}(z)^{2(1+\varepsilon)}$. We obtain similarly that if $y^2 \geqslant 3^3z^2$ then $x \ll_\varepsilon \operatorname{rad}(y)^{2(1+\varepsilon)}$. All the implied constants are explicit functions of C_ε.

Now, for positive coprime $a<b$ denote $x = a^2+ab+b^2$, $y=(b-a)(2a+b)(a+2b)/2$, $z=ab(a+b)/2$. Then $x^3 = y^2+3^3z^2$. Note that since a and b are coprime, $\gcd(x,y,z)$ divides 3, so we can apply the previous paragraph to x,y,z. We deduce from the previous paragraph: if $((b-a)(2a+b)(a+2b))^2 \leqslant 3^3(ab(a+b))^2$ then $3c^2/4 \leqslant a^2+ab+b^2 \ll_\varepsilon \operatorname{rad}(abc)^{2+\varepsilon}$ and hence $c \ll_\varepsilon \operatorname{rad}(abc)^{1+\varepsilon}$; if $((b-a)(2a+b)(a+2b))^2 \geqslant 3^3(ab(a+b))^2$, i.e. $((B-A)(2A+B)(A+2B))^2 \leqslant 3^3(AB(A+B))^2$, then $A^2+AB+B^2 \ll_\varepsilon \operatorname{rad}(ABC)^{2+\varepsilon}$ and hence $c \ll_\varepsilon \operatorname{rad}(ABC)^{1+\varepsilon}$. All the implied constants are explicit functions of C_ε.

Therefore, the inequality ($\sharp$) implies:

Theorem 1. *For every positive* ε *there is an effectively described constant* K_ε *such that for all coprime positive integers* a,b *and their sum* $c=a+b$ *and* A,B,C *defined for* a,b *as above*

$$\log c < (1+\varepsilon)\cdot \log\max\{\operatorname{rad}(abc), \operatorname{rad}(ABC)\} + K_\varepsilon. \qquad (\diamond)$$

Using Theorem 1 we obtain

Theorem 2. *Assume that the* abc-ABC Question *has positive answer. Then for every positive ε there is an effectively described constant L_ε such that for all coprime positive integers a,b and their sum $c = a+b$ the inequality*

$$\log c < (1+\varepsilon)\cdot \log \operatorname{rad}(abc) + L_\varepsilon$$

holds.

References

[1] E. Bombieri, W. Gubler, Heights in Diophantine geometry, CUP 2007.

[2] Sh. Mochizuki, Inter-universal Teichmüller theory I: Constructions of Hodge theaters, *Publ. Res. Inst. Math. Sci.* 57(2021) 3–207; II: Hodge-Arakelov-theoretic evaluation, *Publ. Res. Inst. Math. Sci.* 57(2021) 209–401; III: Canonical splittings of the log-theta-lattice, *Publ. Res. Inst. Math. Sci.* 57(2021) 403–626; IV: Log-volume computations and set-theoretic foundations, *Publ. Res. Inst. Math. Sci.* 57(2021) 627–723.

[3] S. Mochizuki, I. Fesenko, Y. Hoshi, A. Minamide and W. Porowski, Explicit estimates in inter-universal Teichmüller theory, RIMS Preprint 1933, November 2020, available from https://www.kurims.kyoto-u.ac.jp/~motizuki/Explicit%20estimates%20in%20IUTeich.pdf

[4] L. Szpiro, Discriminant et conducteur des courbes elliptiques, *Astérisque* 183(1990) 7–18.