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

IVAN FESENKO

Let $a, b$ be coprime integers. The affine equation of elliptic curve\footnote{this curve is sometimes called the Frey or Frey–Hellegouarch curve} $E_{a,b}$

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

can be written in the Weierstrass form as

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

We have $\Delta = (c_4^3 - c_6^2)/1728 = 16(ab(a + b))^2$.

In particular,

$$\phi = (a^2 + ab + b^2)^3 = ((b - a)(2a + b)(a + 2b)/2)^2 + 3^3(ab(a + b)/2)^2.$$  \footnote{See e.g. sect. 12.5 of [BG] E. Bombieri, W. Gubler, Heights in Diophantine geometry, CUP 2007. Note that there is a misprint on p.434, top line 2: $\Delta$ should be replaced with $\Delta'$.}

The $j$-invariant of the Weierstrass equation is

$$j_{a,b} = 2^8 \cdot \frac{(a^2 + ab + b^2)^3}{(ab(a + b))^2} = 2^6 \cdot \frac{((b - a)(2a + b)(a + 2b))^2}{(ab(a + b))^2} + 2^6 \cdot 3^3.$$  \footnote{Date: May 2019.}

For a non-zero integer its radical $\text{rad}$ is the product of its prime divisors taken each with multiplicity one and its odd radical $\text{rad}'$ is the product of its odd prime divisors taken each with multiplicity one. If $16 | ab(a + b)$ then $\text{cond}(E_{a,b}) < 2^{12} \text{rad}'(ab(a + b))$. If $16 | ab(a + b)$ and say $2 | (a - 1)$, $16 | b$ then $\text{cond}(E_{a,b}) = \text{rad}(2^{-4}ab(a + b)) \leq \text{rad}(ab(a + b))$. All this is very well known.\footnote{See e.g. sect. 12.5 of [BG] E. Bombieri, W. Gubler, Heights in Diophantine geometry, CUP 2007. Note that there is a misprint on p.434, top line 2: $\Delta$ should be replaced with $\Delta'$.}

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 $0 < A < B$, $(A, B) = 1$,

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

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

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

The map $\phi: (a, b) \mapsto (A, B)$ is an involuition: $\phi^2 = \text{id}$. It is a special map relating the two terms on the RHS of (†).

By (†), we have

$$\phi = (a^2 + ab + b^2)^3 = ((b - a)(2a + b)(a + 2b)/2)^2 + 3^3(ab(a + b)/2)^2.$$  \footnote{Date: May 2019.}

and

$$\phi = (A^2 + AB + B^2)^3 = 3^3(AB(A + B)/2)^2 + ((B - A)(2A + B)(A + 2B)/2)^2.$$  \footnote{Date: May 2019.}

We also have $j_{A,B} = 12^3 j_{a,b}/(j_{a,b} - 12^3) = (12^{-3} - j_{a,b}^{-1})^{-1}$.  \footnote{Date: May 2019.}
Question. Are $\text{rad}(abc)$ and $\text{rad}(ABC)$ (effectively) asymptotically equal? I.e. is it true that for every $\varepsilon > 0$ there are constants $c_\varepsilon, c'_\varepsilon$, effectively depending on $\varepsilon$, such that for all relatively prime positive $a < b$

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

It is sufficient to know that $\text{rad}(ABC) \ll_\varepsilon \text{rad}(abc)^{1+\varepsilon}$, then by symmetry this will imply the asymptotic equality of $\text{rad}(abc)$ and $\text{rad}(ABC)$.

The involution $\phi$ 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 $\text{rad}(abc) = \text{cond}_{[0]+[1]+[\infty]}(a:b) = \text{cond}_{[0]+[1]+[-1/2]}(A:B)$ and $\text{rad}(ABC) = \text{cond}_{[0]+[1]+[\infty]}(A:B)$.

The following problem includes several equivalent statements to the question. The proof of equivalence is straightforward.

Problem. Prove or disprove the following equivalent statements.

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

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

with $\kappa_\varepsilon$ effectively dependent on $\varepsilon$.

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

$$\text{rad}(ABC) < \kappa'_\varepsilon \cdot \text{rad}(abc)^{1+\varepsilon},$$

with $(a,b) \mapsto (A,B)$ defined above and with $\kappa'_\varepsilon$ effectively dependent on $\varepsilon$.

3. $\text{rad}(c_0(E_{a,b}))$ and $\text{rad}(\Delta(E_{a,b}))$ are effectively asymptotically equivalent.

4. $\text{rad}(\Delta(E_{a,b}))$ and $\text{rad}(\Delta(E_{A,B}))$ are effectively asymptotically equivalent.

5. $\text{cond}(E_{a,b})$ and $\text{cond}(E_{A,B})$ are effectively asymptotically equivalent.

Thus, the positive answer to the problem signifies a new asymptotic symmetry of the moduli space of elliptic curves over rational numbers with a non-trivial rational point of order 2.

Among several motivations for the stated problem, one comes from the study of an issue to deduce the $1+\varepsilon$-version of abc inequality from another of its versions, and we now describe this aspect.

Szpiro\textsuperscript{3} stated the following version: let $a, b$ be coprime positive integers, then for every $\varepsilon > 0$ there is effectively given $c_\varepsilon > 0$ such that

$$\log(ab(a+b)) \leq 3(1+\varepsilon) \cdot \log \text{rad}(ab(a+b)) + C_\varepsilon \quad (\dagger)$$

In view of (\dagger), consider the equation $x^3 = y^2 + 3z^2$ with $(x, y, z) = 1; x, y, z > 0$. The following is a kind of variation of some arguments in sect. 12.5 of [BG].

Applying (\dagger), we obtain $x^3y^2z^2 \ll_\varepsilon \text{rad}(xyz)^3(1+\varepsilon)$. Since $y^2 \cdot 3z^2 \leq x^6/4$, we deduce $yz \ll_\varepsilon \text{rad}(xyz)^{1+\varepsilon}$. Assume that $y^2 \leq 3z^2$, then we deduce $y \ll_\varepsilon \text{rad}(xyz)^{(1+\varepsilon)/2}$, and since $x^3 \geq 2 \cdot 3z^2$, we get $x^3 \cdot y^2 \ll_\varepsilon \text{rad}(xyz)^3(1+\varepsilon)$ and $x^3 \cdot y^6 \ll_\varepsilon \text{rad}(xyz)^{5(1+\varepsilon)}$. Substituting the latter in the RHS of $y \ll_\varepsilon \text{rad}(xyz)^{(1+\varepsilon)/2}$, we obtain $y \ll_\varepsilon \text{rad}(z)^{(1+\varepsilon)}$. From $x^3 \cdot y^2 \ll_\varepsilon \text{rad}(xyz)^{3(1+\varepsilon)}$ we deduce $x^3 \ll_\varepsilon \cdot \text{rad}(z)^{(1+\varepsilon)} < \text{rad}(z)^{6(1+\varepsilon)}$, hence $x \ll_\varepsilon \text{rad}(z)^{2(1+\varepsilon)}$. Thus, (\dagger) implies: if $y^2 \leq 3z^2$ then $x^3, y^2 \ll_\varepsilon \text{rad}(z)^{6(1+\varepsilon)}$ and, similarly, if $y^2 \geq 3z^2$ then $x^3, z^2 \ll_\varepsilon \text{rad}(y)^{6(1+\varepsilon)}$, with effective implied constants.

Now, using $x = a^2 + ab + b^2$, $y = (b-a)(2a+b)(a+2b)/2$, $z = ab(a+b)/2$ in (\dagger), we deduce from (\dagger):

\textsuperscript{3} Szpiro, L. Discriminant et conducteur des courbes elliptiques, Astérisque 183(1990) 7–18.
if \(((b - a)(2a + b)(a + 2b)) \leq 3^3(ab(a + b))\) then \(a^2 + ab + b^2 \ll \varepsilon \text{rad}(abc)^{2+\varepsilon}\) and hence \(\max\{a, b, c\} \ll \varepsilon \text{rad}(abc)^{1+\varepsilon}\); if \(((b - a)(2a + b)(a + 2b)) \geq 3^3(ab(a + b))\) then \(A^2 + AB + B^2 \ll \varepsilon \text{rad}(ABC)^{2+\varepsilon}\) and hence \(\max\{a, b, c\} \ll \varepsilon \text{rad}(ABC)^{1+\varepsilon}\), with effective implied constants.

Therefore, \((\sharp)\) implies: for coprime positive integers \(a, b\) (with \(c = a + b\) and \(A, B, C\) as above)

\[c \ll \varepsilon \max\{\text{rad}(abc), \text{rad}(ABC)\}^{1+\varepsilon},\]

with an effective implied constant.

Thus we obtain that \((\sharp)\) via \((\circ)\) and the positive answer to the stated problem imply the stronger inequality \(\max\{a, b, c\} \ll \varepsilon \text{rad}(abc)^{1+\varepsilon}\) with an effective implied constant depending on \(\varepsilon\).

It is not currently known whether the conjectural inequality \(\max\{a, b, c\} \ll \varepsilon \text{rad}(abc)^{1+\varepsilon}\) implies the positive answer to the stated problem.