Evans Triangles and Edwards Curves

Wensen Wu

Abstract. We reduced the unsolved problem of Evans triangles to the problem of rational points on a class of elliptic curves, that is, the twisted Edwards curves and show there is a group structure on the set of Evans triangles. Using this, we obtain a large class of new Evans triangles, and also give an effective way to test if the rank of an Edwards curve is positive or not.

1. Introduction

An Evans triangle is a triangle with integer side length such that one of its attitudes is n times of the corresponding base, where $n \in \mathbb{Z}$ is called the Evans ratio of the Evans triangle. The problem of finding Evans triangles was raised by Ron J. Evans in 1977 when he proposed this problem in American Mathematics Monthly [4]. Concretely, one can summarize the Evans problem as

(*a*) Given $n \in \mathbb{Z}_{>0}$, if there is an Evans triangle whose Evans ratio is n?
(*b*) If the answer to (*a*) is positive, are there finitely or infinitely many such Evans triangles?

Evans problem has drawn some interests but is still open today. During the last 40 years some progress were made. Among them, one most important result is Xin Bian's paper [5], where Bian concluded that the existence of Evans triangles equals the existence of integral solutions to an indeterminate equation. Based on Bian's work, many sorts of Evans triangles have been found, see [6], [9], and [7]. In [7], when some extra conditions is put on the indeterminate equation, the author discovered that some of their integral solutions are given by the integral solutions to Pell equations. Therefore, for certain n, the existence of solutions to pell equation implies that n is an Evans ratio.

However, all the previous works on Evans problems are basically "elementary mathematics", and the problem has never been understood from the point of view of modern mathematics. One can even hardly estimate the difficulty of

this problem. In this paper, we discover an intrinsic connection between Evans triangles and a class of elliptic curves, that is, the Edwards curves. Concretely, we find there is "almost" a one to one correspondence between Evans triangles and the rational solution class of elliptic curves. In particular, given n, the set of all Evans triangles with Evans raito n is a group (See Theorem 4.2 below). On the one hand, using this group law, we can produce a large class of Evans triangles (See Section 5 below). On the other hand, once we construct an Evans triangle through elementary mathematics, we can test the rank of Edwards curves. For example, as a consequence of all earlier works mentioned in the last paragraph, we know a large class of Edwards curves having a positive rank (See Thm 5.1 below).

Via this paper, we put the Evans problem into the framework of modern mathematics and obtain a much better understaning of this problem. From the point of view of elliptic curves, the meaningfulness and difficulty of Evans triangle problem was underrated. On the one hand, to solve the Evans problem completely, one must have a deep understanding of Edwards curves, which is a central problem of modern mathematics and can never be easy. On the other hand, the fact that Evans triangles can be approached through elementary methods gives us more numerical and intuitive understanding of elliptic curves.

2. Evans Triangles and Algebraic Curves

Apparently, in the Evans problems $(a), (b)$ in §1, we should consider two Evans triangles that are similar as the same. It is an easy observation that if ΔABC is an Evans triangle with the attitude h on the base BC such that $h = n|BC|$, BC must be the strictly shortest side of ΔABC. One can also verify that $|AB| \neq |BC|$ (see also lemma 3.2 below). It is obvious that every Evans triangle of ratio n is similar to a triangle side length a, b and 1 such that $a, b \in \mathbb{Q}_{>0}$, $a > b$ and the attitude on the length 1 side is n. We write such a triangle $\Delta(a, b; n)$. So two Evans triangles are similar if and only if they similar to a same $\Delta(a, b; n)$.

Given $n \in \mathbb{Z}_{>0}$, let $\Delta(n)$ be the set of all triangles $\Delta(a, b; n)$ described as above. For later use, we write $\tilde{\Delta}(n)$ be the set of all triangles $\Delta(a, b; n)$ with the $a > b$ replaced by $a \neq b$. Apparently, every two triangles in $\Delta(n)$ are not similar, $\Delta(n) \subset \tilde{\Delta}(n)$ and every triangle $\Delta(a, b; n) \in \Delta(n)$ is similar to (and therefore congruent to) a unique triangle in $\tilde{\Delta}(n) \backslash \Delta(n)$, which is, $\Delta(b, a; n)$. With these simple argument, we lead to our first observation:

to find all Evans trianles with ratio n, we only have to find all triangles in $\Delta(n)$ or, equivalently, $\tilde{\Delta}(n)$.

From now on, when we mention an Evans triangle, we always means a triganle $\Delta(a,b;n) \in \Delta(n)$ for some n. Now given $\Delta(a,b;n) \in \Delta(n)$, it is obviously that the area of the triangle is $\frac{n}{2}$. On the other hand, by Heron's formula, the area can be computed by

$$\frac{n}{2} = \sqrt{(\frac{a+b+1}{2})(\frac{a+b-1}{2})(\frac{a-b+1}{2})(\frac{-a+b+1}{2})}. \tag{2.1}$$

Set

$$x = a+b, \quad y = a-b. \tag{2.2}$$

we have $x, y \in \mathbb{Q}$ and

$$(x^2-1)(1-y^2) = 4n^2. \tag{2.3}$$

Apparently, equation (2.3) defines an algebraic curve, and we know that every Evans triangle gives a rational point on this curve. So we expect that every rational point on this curve will provide us an Evans triangle. However, an obvious observation on the solution of this curve keeps us away from this expectation: once we have a solution (x,y) on the curve (2.3), we can immediately have another 7 solutions, that are, $(\pm x, \pm y)$, $(\pm y, \pm x)$. To cure this issue, we make the definition of a solution class:

DEFINITION 1. If (x,y) is a solution of curve (2.3), we define its solution class to be the set of 8 solutions $\{(\pm x, \pm y), (\pm y, \pm x)\}$. We write this class as $[x,y]$.

LEMMA 2.1. *For every rational solution class to the curve* (2.3)*, it has exactly one representative* $[x,y]$ *such that*

$$x > y > 0. \tag{2.4}$$

PROOF: Let (x,y) be a rational solution to (2.3). We can firstly exclude the situation $x = y$. Indeed, if it is the case, (2.3) turns to be

$$(x^2-1)(1-x^2) = -(x^2-1)^2 = 4n^2. \tag{2.5}$$

This is not possible. If x or y equals 0, (2.3) turns to be

$$x^2 - 1 = 4n^2. \tag{2.6}$$

This means that $x \in \mathbb{Z}$ and $(x+2n)(x-2n) = 1$, which is not possible. So we must have $xy \neq 0$. consider the set $\{(\pm x, \pm y)\}$, there must be exactly one of the four points having both two coordinates positive. Without loss of generality, assume $x > 0$ and $y > 0$, then among the set $\{(\pm y, \pm x)\}$, (y,x) is the only point with two coordinates positive. So we can choose the representative $[x,y]$ if $x > y > 0$, otherwise, choose the representative $[y,x]$. □

From now on, throughout this paper, we always fix a representative $[x,y]$ of a rational solution class of (2.3) such that $x > y > 0$. With this setting, we have the following important observation:

PROPOSITION 2.2. *There is a one to one correspondence between the set* $\Delta(n)$ *and the rational solution classes* $[x, y]$ *on* (2.3). *This correspondence is explicitly given by* $(a, b) \mapsto [a + b, a - b]$, *or equally,*

$$a = \frac{x+y}{2}, \quad b = \frac{x-y}{2}, \tag{2.7}$$

by our convention on x, y *it is easy to see that* $a > b > 0$.

PROOF: By (2.2), the map $(a, b) \mapsto [a+b, a-b]$ defines a map from $\Delta(n)$ to the rational solution classes of (2.3). Obviously $a + b > a - b > 0$, by Lemma 2.1, the uniqueness of representative $[x, y]$ with $x > y > 0$, if $\Delta(a_1, b_1; n)$ and $\Delta(a_2, b_2; n) \in \Delta(n)$ maps to the same solution class, one must have $a_1 + b_1 = a_2 + b_2$ and $a_1 - b_1 = a_2 - b_2$. This implies that $a_1 = a_2$ and $b_1 = b_2$. So the map is injective. To see the map is surjective, once we have a rational solution class, fix its representative $[x, y]$ as in the last lemma. Then it is easily solve $a + b = x$ and $a - b = y$ by (2.7). Since $x > y > 0$, it is directly from (2.3) that $x = a + b > 1$ and $1 > y = a - b > 0$. So $a, b, 1$ could be the three sides of a triangle, say Δ. Substituting a, b into (2.3), dividing both sides by 16 and taking square root, we return to the Heron formula (2.1). This implies that the attitude of Δ on the length 1 side is n, i.e. $\Delta = \Delta(a, b; n) \in \Delta(n)$. □

3. Reduction to twisted Edwards curves

The proposition 2.2 tells us

TO STUDY $\Delta(n)$, ONE ONLY HAS TO STUDY THE RATIONAL SOLUTION CLASSES OF ALGEBRAIC CURVE (2.3).

To do so, by a general strategy of studying algebraic curves [8], we consider the homogeneous equation of (2.3), which is

$$-x^2y^2 + x^2z^2 + y^2z^2 - (1 + 4n^2)z^4 = 0. \tag{3.1}$$

From this we see it is not smooth at infinite, since when the equation is given by

$$x^2y^2 = 0, \tag{3.2}$$

and it has a node. So we expect a rational model of (2.3) which could be clearer to us.

THEOREM 3.1. *The curve (3.1) is bi-rational to a twisted Edwards curve*

$$E_n : Y^2 + Z^2 = 1 + (1 + 4n^2)Y^2Z^2. \tag{3.3}$$

LEMMA 3.2. *There is no finite rational point* (x, y, z) *on curve* (3.1) *such that* x *or* y *equals* 0.

PROOF OF THE LEMMA: Since the equation is symmetric for x and y, we assume $y = 0$. Then the curve (3.1) is

$$x^2z^2 = (1 + 4n^2)z^4. \tag{3.4}$$

Since $z \neq 0$, we only have to solve equation $x^2 = (2n)^2 + 1$ in $\mathbb{Q}$. This is not possible. □

Remark 1. From Proposition 2.2, the lemma also implies there is no Evans triangles of the form $\Delta(a, a; n)$ for any $a \in \mathbb{Q}$ and $n \in \mathbb{Z}_{>0}$. This explains our convention $a > b$ in the setting $\Delta(a, b; n)$.

PROOF OF THE THEOREM: By the lemma above, we know that $x \neq 0$. So set

$$v = \frac{y}{x}, \quad w = \frac{z}{x}, \tag{3.5}$$

we can translate the curve (3.1) into

$$w^2 + v^2w^2 - (1 + 4n^2)w^4 - v^2 = 0. \tag{3.6}$$

By the lemma again we know $v \neq 0$, we set

$$Y = \frac{w}{v}, \quad Z = w, \tag{3.7}$$

We further have

$$Y^2 + Z^2 - (1 + 4n^2)Y^2Z^2 - 1 = 0, \tag{3.8}$$

i.e.

$$Y^2 + Z^2 = 1 + (1 + 4n^2)Y^2Z^2. \tag{3.9}$$

□

We are delight to have this rational model (3.3) of curve (3.1), since it is the so-called twisted Edwards curve which has been well-studied by Edwards and Bernstein, and many other mathematicians (see, for example, [1] and [2]). Concretely, it is a rational model of elliptic curves. It has the advantage that its group structure can be computed faster than the standard ones. Now, by lemma 3.2 and theorem 3.1, to find the rational points on the algebraic curve (2.3), it is equivalent to find the rational solutions (Y, Z) on the new curve E_n such that $YZ \neq 0$. Before we start our calculation on E_n, we need to make a similar observation as Definition 1.

DEFINITION 2. If (Y, Z) is a solution of E_n with $Y, Z \neq 0$, we define its solution class to be the set of 8 solutions $\{(\pm Y, \pm Z), (\pm Z, \pm Y)\}$. We write this class as $[Y, Z]$.

COROLLARY 3.3. *There is a one to one correspondence between rational solutions* (x, y) *of the curve* (2.3)*, and rational solutions* (Y, Z) *of* E_n *with* $YZ \neq 0$*. This correspondence is explicitly given by* $x = \frac{1}{Z}$ *and* $y = \frac{1}{Y}$*. Moreover, this gives us a one to one correspondence between rational classes of solutions of curve* (2.3) *and* E_n*.*

PROOF: This corollary follows from the proof of Theorem 3.1 directly. In equation (2.3), we use the affine coordinate (x, y), which corresponds to the projective coordinate $[x : y : 1]$. By the bi-rational transformation (3.5), we change the coordinate by $v = \frac{y}{x},\ w = \frac{1}{x}$, so the resulting projective coordinate is $[1 : \frac{y}{x} : \frac{1}{x}]$. Then, by transformation (3.7), we get

$$Y = \frac{w}{v} = \frac{\frac{z}{x}}{\frac{y}{x}} = \frac{1}{y}, \quad Z = w = \frac{z}{x} = \frac{1}{x}. \tag{3.10}$$

This gives us the explicit bijection between rational solutions (x, y) of the curve (2.3) and rational solutions (Y, Z) of E_n with $YZ \neq 0$. Apparently, this map $(x, y) \mapsto (\frac{1}{y}, \frac{1}{x})$ induces an bijection between $[x, y]$ and $[\frac{1}{y}, \frac{1}{x}]$. □

From now on, we make the convention that we always fix for every rational solution class of E_n a representative $[Y, Z]$ such that $Y > Z > 0$. This is consistent to our convention for rational solution classes of (2.3).

COROLLARY 3.4. *There is a one to one correspondence between the set* $\Delta(n)$ *and the rational solution classes* $[Y, Z]$ *on* E_n*. This correspondence is explicitly given by* $(a, b) \mapsto (\frac{1}{a-b}, \frac{1}{a+b})$*, or equally,*

$$a = \frac{1}{2}(\frac{1}{Z} + \frac{1}{Y}), \quad b = \frac{1}{2}(\frac{1}{Z} - \frac{1}{Y}). \tag{3.11}$$

by our convention on Y*,* Z*, we can easily find* $a > b > 0$*.*

PROOF: It follows directly from Proposition 2.2 and Corollary 3.3. □

4. Group law on twisted Edwards curve

As mentioned in §3, E_n is an elliptic curve, so its rational points $E_n(\mathbb{Q})$ is an abelian group. By the standard theory of rational points on elliptic curves, (see, for example, [3])

$$E_n(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_n(\mathbb{Q})_{tor}, \tag{4.1}$$

where r is the rank of $E_n(\mathbb{Q})$ and $E_n(\mathbb{Q})_{tor}$ is its torsion part, which is a finite group. Noting that the rational points $(\pm 1, 0)$ on E_n are necessarily torsion, we have the next theorem easily. However, this result seems not easy to prove directly without advanced mathematical technique.

THEOREM 4.1.

$$rank(E_1(\mathbb{Q})) = rank(E_2(\mathbb{Q})) = 0. \tag{4.2}$$

PROOF: Since there is no Evans triangles with ratio $n = 1$ or $n = 2$, it follows from Corollary 3.4 immediately. □

To explore more information on $E_n(\mathbb{Q})$ for general n, and to find more Evans triangles, we need to study the structure of $E_n(\mathbb{Q})$ in detail. Indeed, the group law of $E_n(\mathbb{Q})$ is explicitly given in [2, §3], as for two points (Y_1, Z_1), (Y_2, Z_2) in $E_n(\mathbb{Q})$,

$$(Y_1, Z_1)+(Y_2, Z_2) = (\frac{Y_1Z_2 + Z_1Y_2}{1 + (1 + 4n^2)Y_1Y_2Z_1Z_2}, \frac{Z_1Z_2 - Y_1Y_2}{1 - (1 + 4n^2)Y_1Y_2Z_1Z_2}). \tag{4.3}$$

The point $(0, 1)$ is the identity element of the group law, $(0, -1)$ has order 2, and $(\pm 1, 0)$ both have order 4. The inverse of a point (x, y) on E_n is $(-x, y)$. Actually, $C := \{(1, 0), (0, -1), (-1, 0), (0, 1)\}$ is a torsion subgroup of $E_n(\mathbb{Q})$ of order 4 generated by $(1, 0)$. Moreover, since $1 + 4n^2$ cannot be a square, it follows from [2, §3] that the addition law is complete, that is, it can be used to compute $2(x, y)$, $3(x, y)$ and so on.

Since we have defined the solution class in last section we would like to see the relations between the points in a same solution class under group law. It is easy to check that if P is an element in $E_n(\mathbb{Q})$, then its solution class $[P]$ is a union of $P + C$ and $-P + C$. Indeed, if $P = (Y, Z)$, $P + (1, 0) = (Z, -Y), P + (0, -1) = (-Y, -Z), P + (-1, 0) = (-Z, Y)$; and $-P = (-Y, Z)$ $-P + (1, 0) = (Z, Y), P + (0, -1) = (Y, -Z), P + (-1, 0) = (-Z, -Y)$.

THEOREM 4.2. *Given $n \in \mathbb{Z}_{>0}$. There is a one to one correspondence between the set $\overline{\Delta}(n) := \tilde{\Delta}(n) \cup \{0\}$ and the quotient group $E_n(\mathbb{Q})/C$. Therefore we can define an abelian group structure on $\overline{\Delta}(n)$ by:*

$$\Delta(a_1, b_1; n) + \Delta(a_2, b_2; n) = \Delta(a, b; n), \tag{4.4}$$

such that in $E_n(\mathbb{Q})$, $(\frac{1}{a-b}, \frac{1}{a+b})$ is in the coset of

$$(\frac{2a_1a_2 - 2b_1b_2}{(a_1^2 - b_1^2)(a_2^2 - b_2^2) + (1 + 4n^2)}, \frac{2a_1b_2 + 2a_2b_1}{(1 + 4n^2) - (a_1^2 - b_1^2)(a_2^2 - b_2^2)}). \tag{4.5}$$

Under this group structure, the opposite of $\Delta(a, b; n)$ is $\Delta(b, a; n)$.

PROOF: We first show there is a one to one correspondence between $\overline{\Delta}(n)$ and $E_n(\mathbb{Q})/C$. Indeed, we define $\gamma : \overline{\Delta}(n) \to E_n(\mathbb{Q})$ by setting $\gamma(0) = 0$ and

$$\gamma : \tilde{\Delta}(n) \to E_n(\mathbb{Q}) \quad \Delta(a, b; n) \mapsto (\frac{1}{a - b}, \frac{1}{a + b}) + C. \tag{4.6}$$

According to Corollary 3.4, γ is well-defined. Since $a, b \in \mathbb{Q}_{>0}$ and $a \neq b$, that $\gamma(\Delta(a, b; n)) \notin C$. So $0 \in \overline{\Delta}(n)$ is the only element which maps to $0 \in$

$E_n(\mathbb{Q})/C$. Now if $\gamma(\Delta(a_1,b_1;n)) = \gamma(\Delta(a,b;n))$, by the computation before the Theorem, we must have $(\frac{1}{a_1-b_1}, \frac{1}{a_1+b_1})$ lying in the set

$$\{(\frac{1}{a-b},\frac{1}{a+b}),(\frac{1}{a+b},-\frac{1}{a-b}),(-\frac{1}{a-b},-\frac{1}{a+b}),(-\frac{1}{a+b},\frac{1}{a-b})\}. \tag{4.7}$$

Without loss of generality, assume $a > b > 0$. If $a_1 > b_1 > 0$, both $\frac{1}{a_1-b_1}$ and $\frac{1}{a_1+b_1}$ are positive. Then $(\frac{1}{a_1-b_1}, \frac{1}{a_1+b_1}) = (\frac{1}{a-b}, \frac{1}{a+b})$. This implies $a = a_1$ and $b = b_1$. If $b_1 > a_1 > 0$, $\frac{1}{a_1-b_1} < 0$ and $\frac{1}{a_1+b_1} > 0$. So the only possibility is $(\frac{1}{a_1-b_1}, \frac{1}{a_1+b_1}) = (-\frac{1}{a+b}, \frac{1}{a-b})$. However, this implies that $b = -a_1 < 0$. So it is not possible. So we proved the injectivity of γ. Now we show that γ is surjective. Let $P \notin C$ be any rational solution of E_n, then we can find $Y, Z \in \mathbb{Q}_{>0}$ such that $P \in (Y,Z) + C$. If $Y > Z > 0$, set $a = \frac{1}{2}(\frac{1}{Z} + \frac{1}{Y})$ and $b = \frac{1}{2}(\frac{1}{Z} - \frac{1}{Y})$, then $a > b > 0$ and $\gamma(\Delta(a,b;n)) = (Y,Z) + C$. If $Z > Y > 0$, then $(Y,Z) \in (-Z,Y) + C$, set $a = \frac{1}{2}(\frac{1}{Y} - \frac{1}{Z})$ and $b = \frac{1}{2}(\frac{1}{Y} + \frac{1}{Z})$. Then $b > a > 0$ and $\gamma(\Delta(a,b;n)) = (Y,Z) + C$.

Now since γ is bijective, we can define group structure on $\overline{\Delta}(n)$ by translating the group structure of $E_n(\mathbb{Q})/C$ via γ as

$$\Delta(a_1,b_1;n) + \Delta(a_2,b_2;n) := \gamma^{-1}(\gamma(\Delta(a_1,b_1;n)) + \gamma(\Delta(a_2,b_2;n))), \tag{4.8}$$

so that the image of $(\Delta(a_1,b_1;n) + \Delta(a_2,b_2;n))$ under γ is the sum of the image of $\Delta(a_1,b_1;n)$ and $\Delta(a_2,b_2;n)$. Concretely, if $\Delta(a_1,b_1;n) + \Delta(a_2,b_2;n) = \Delta(a,b;n)$, then $(\frac{1}{a-b}, \frac{1}{a+b})$ is belong to the coset of $(\frac{1}{a_1-b_1}, \frac{1}{a_1+b_1}) + (\frac{1}{a_2-b_2}, \frac{1}{a_2+b_2})$, which is

$$(\frac{2a_1a_2 - 2b_1b_2}{(a_1^2-b_1^2)(a_2^2-b_2^2) + (1+4n^2)}, \frac{2a_1b_2 + 2a_2b_1}{(1+4n^2) - (a_1^2-b_1^2)(a_2^2-b_2^2)}). \tag{4.9}$$

Finally,

$$\gamma(\Delta(b,a;n)) = (\frac{1}{b-a}, \frac{1}{a+b}) + C, \tag{4.10}$$

so $\gamma(\Delta(b,a;n)) + \gamma(\Delta(a,b;n)) = 0$ in $E_n(\mathbb{Q})/C$. Then

$$\Delta(a,b;n) + \Delta(b,a;n) = 0 \in \overline{\Delta}(n). \tag{4.11}$$

This completes the proof. □

Remark 2. There are actually two more observations from the proof above:

(1) If we write $Y = \frac{2a_1a_2-2b_1b_2}{(a_1^2-b_1^2)(a_2^2-b_2^2)+(1+4n^2)}$, $Z = \frac{2a_1b_2+2a_2b_1}{(1+4n^2)-(a_1^2-b_1^2)(a_2^2-b_2^2)}$, it is not possible to verify $Y > Z > 0$ since we can easily find a counterexample by computer (see the computation in the next section). So we have to leave the last theorem in this cumbersome form. However, once we know this point, it is easy to compute all the elements in its coset as the paragraph before Theorem 4.2. Actually, we only have to pick up one pair among the four pairs $\{(Y,Z),(Z,-Y),(-Y,-Z),(-Z,Y)\}$.

(2) By the proof of Theorem 4.2, to compute the inverse of γ, one should always choose the representative $[Y, Z]$ for a coset such that $|Y| > Z > 0$. If $Y > 0$, its preimage under γ is in $\Delta(n)$; if $Y < 0$, its preimage under γ is in $-\Delta(n)$. This observation can simply our program for computation in the next section.

5. Applications

With the help of Theorem 4.2, once we have an Evans triangle $\Delta(a, b; n)$, we can obtain some new Evans triangles, simply by computing the doubling, tripling...of $\Delta(a, b; n)$. This also gives us a way to test the Evans problem (b) in §1, as long as we have a positive answer to the problem (a).

Let's compute the simplest example of Bian to illustrate the situation. Recall in [5], for Evans ratio $n = k^2 - 1$, Bian constructed an Evans triangle whose three sides are $a = k^2 - \frac{1}{2} + \frac{1}{2k}$, $b = k^2 - \frac{1}{2} - \frac{1}{2k}$ and $c = 1$. By Theorem 4.2, this Evans triangle corresponds to the coset of point $(k, \frac{1}{2k^2-1})$ in $E_3(\mathbb{Q})/C$.

In the tables below we give the simple cases, $k = 2$ and therefore $n = 3$. For general n, a code for computation is given in the Appendix. If $k = 2$ then $n = 3, a = \frac{15}{4}, b = \frac{13}{4}$. This gives a coset of $P = (2, \frac{1}{7})$ in $E_3(\mathbb{Q})$,. Let's write the coset by $\overline{P}$. Via Mathematica, we have:

	Coset (Y, Z), $\lvert Y\rvert > Z > 0$, the coordinate Y
$\overline{P}$	2
$2\overline{P}$	$-(65/33)$
$3\overline{P}$	$25742/25741$
$4\overline{P}$	$\frac{163114249}{80295799}$
$5\overline{P}$	$-\frac{4199554676462}{2164213391339}$
$6\overline{P}$	$\frac{17564230801725723 05}{17561501576716811 67}$
$7\overline{P}$	$\frac{88153404243832133322916 82}{42709848106198449555178 81}$
$8\overline{P}$	$-\frac{71918128090672361012875817 5428001}{37609808620040414511893751 6463199}$
$9\overline{P}$	$\frac{23824391195538061515927976024613428973 7122}{23816062019541038924496942869167824002027 9}$
$10\overline{P}$	$\frac{12627912270646996403366431655021284640533233845878 25}{60195076399887747958657718359261855515101326127643 3}$
$11\overline{P}$	$-\frac{81612891084824610496929341969266534162205906393724187911755822}{43297303780850008446187016204949465275022964402741765496531579}$
$12\overline{P}$	$\frac{85656248924466060638719780383134373778586841016678927046760453322703218249}{85603013679751445799289823565450360205297210385759149519598432627081657801}$
$\cdots$	$\cdots$

TABLE 1. $k = 2, Y$

	Coset (Y, Z), $\lvert Y\rvert > Z > 0$ the coordinate Z
$\overline{P}$	$1/7$
$2\overline{P}$	$28/197$
$3\overline{P}$	$131/89173$
$4\overline{P}$	$\frac{23663640}{164821801}$
$5\overline{P}$	$\frac{2077854653029}{14695325574013}$
$6\overline{P}$	$\frac{154811197320779 72}{526929198224337 4997}$
$7\overline{P}$	$\frac{44522996135038418614016 39}{30860098726698594287374447}$
$8\overline{P}$	$\frac{10216706693274352929384165166728 0}{72640197161920987603078349280720 1}$
$9\overline{P}$	$\frac{36368746628862286921560035704774083999 59}{82530913351480083371789462348380860549276 7}$
$10\overline{P}$	$\frac{55504435878421859550715789675787472059066139467397 2}{38288182757323848507272364074243815181672780938045 97}$
$11\overline{P}$	$\frac{39941655267536738848424543773873972462969447633886463800755691}{28552286024098329275656541115371156920927696184216864298327313 3}$
$12\overline{P}$	$\frac{50324029919391184621477336618760162296372139357993422630314152785444908 0}{85657727208984630797997571871376449620207917270464140514721551327188516201}$
$\cdots$	$\cdots$

TABLE 2. $k = 2$, Z

	Evans triangles $\Delta(a, b; 3) \in \overline{\Delta}(3)$, the side length a
$\overline{P}$	$15/4$
$2\overline{P}$	$11881/3640$
$3\overline{P}$	$2298863437/6744404$
$4\overline{P}$	$\frac{2878487516999080 9}{771975373441272 0}$
$5\overline{P}$	$\frac{57216902371136505411266175}{17452128450272526726606796}$
$6\overline{P}$	$\frac{92822932246389707899516395177796114 09}{54382792008673557793078876135530920}$
$7\overline{P}$	$\frac{29105797982752656247594898956227954303536314465681 3}{78497073528772348022738097333859535746537001733596}$
$8\overline{P}$	$\frac{48398986205615941353941339491836267248921599417302049243603740648 1}{14695328412634691414957244075186385815146778713951640153849501456 0}$
$9\overline{P}$	$\frac{19749103686635763299324988668668697839553261613242905334386057712429823564280516513 5}{17329264939548424486902093601058185137190914479280411441455790016079686574911559 96}$
$10\overline{P}$	$\frac{51691075044432732007257604462335703051201345388218678713271273710384607270296082084404416371435373334 01}{14018102938089255976818445569509062901430419560750140765381663833050113109295311862647785961709511818 00}$
$11\overline{P}$	$\frac{21572980113446442513910402115574893786107340777955365840820310 09}{65353648178654551873263625772703633474505331303564189834642 37}/$ $\frac{65195079221941741136067356309833726030155447439712533371446561658493 91}{16202226042809031124230773848377723656385893253776600 4}$
$12\overline{P}$	$\frac{73801984903328956462317268729116607565863769023740336516585107910575 85}{03932459473640300963600060248356569483877859974527787781141130891189771462512 9}/$ $\frac{86211352673152980279913765113071350839348561123831273849923379148445 04}{13042000679931367952216153284847296912402089161077819078875656683377945218 40}$
$\cdots$	$\cdots$

TABLE 3. $k = 2$, a

	Evans triangles $\Delta(a,b;3) \in \overline{\Delta}(3)$, the side length b
$\overline{P}$	$13/4$
$2\overline{P}$	$13729/3640$
$3\overline{P}$	$2292119295/6744404$
$4\overline{P}$	$\frac{24984693407894089}{7719753734412720}$
$5\overline{P}$	$\frac{662107441018193318888697837}{174521284502725267266066796}$
$6\overline{P}$	$\frac{92279188829221249798873385906437047 61}{54382792008673557793078876135530920}$
$7\overline{P}$	$\frac{25302657178431953263080280335197516645555157024289 5}{78497073528772348022738097333859535746537001733596}$
$8\overline{P}$	$\frac{56083953874838628514794242187209756142783940026826389421026226392 1}{14695328412634691414957244075186385815146778713951640153849501456 0}$
$9\overline{P}$	$\frac{19575871621578571637665903095281746134610469783148845257701835142089309852859962801 3}{17329264939548424486902093601058185137190914479280411441455579001607968657491155996}$
$10\overline{P}$	$\frac{45008887527964183085548600455843575946348585656955025897754391732346559885352498309523959474303331296 49}{14018102938089255976818445569509062901430419560750140765381663833050113109295311862647785961709511818 00}$
$11\overline{P}$	$\frac{25031712076703494711036124516793535244506277697824087257596286912168 09}{55624777704041723996878805587110996113400567782743964 15}/$ $\frac{65195079221941741136067356309833726030155447439712533371446561658493 91}{16202226042809031124230773848377723656385893253776600 4}$
$12\overline{P}$	$\frac{72940407179006983537239148571543662588452782984725307515505162387477 56}{56648633002533718099085055957497522478469980070457667126130503189645783607896 9}/$ $\frac{86211352673152980279913765113071350839348561123831273849923379148445 0}{41304200067993136795221615328484729691240208916107781907887565668337794521840}$
...	...

TABLE 4. $k = 2$, b

Surely we can keep computing the higher multiples of $\overline{P}$, however, we choose to stop at the step 12. There are two reasons. Firstly, the number is even more terrible if we keep computing. Secondly, and most importantly, it is easy to see from our computation above that $\overline{P}$ is not of order less than or equal to 12. According to Mazur's famous Theorem [3, §2.5], that any torsion point of an elliptic curve has an order less than or equal to 12. So our computation is enough to verify that P is not torsion. So we have verified the next theorem for the case $n = 3$.

THEOREM 5.1. *There are infinitely many Evans triangles with the ratios* $3, 8, 15$*, and rank of* $E_3, E_8, E_{15} > 0$

PROOF: The theorem is verify via a computation via Mathematica, the program is given in the Appendix. The precise results of the computation is too large to be fit in a table. So in the tables below, we only compute the results upto 15-digital decimal. However, it is enough to see they are not torsion. In case $k = 3$, then $n = 8$, $a = 26/3$ and $b = 25/3$. So the rational point in $E_8(\mathbb{Q})$ is $(3, 1/17)$. In case $k = 4$, then $n = 15$, $a = 125/8$ and $b = 123/8$. So the rational point in $E_{15}(\mathbb{Q})$ is $(4, 1/31)$.

	Coset (Y, Z), $\lvert Y\rvert > Z > 0$	Evans triangle $\Delta(a, b; 8)$, (a, b)
$\overline{P}$	$(3.000000000000000, 0.058823529411764)$	$(8.66666666666667, 8.33333333333333)$
$2\overline{P}$	$(-1.28458498023715, 0.0392006149116065)$	$(12.3656711915535, 13.1441327300151)$
$3\overline{P}$	$(1.17426203512330, 0.0327445764898540)$	$(15.6955036272942, 14.8439049465151)$
$4\overline{P}$	$(-4.73327432073915, 0.0609755593073093)$	$(8.09437166454124, 8.30564190417608)$
$5\overline{P}$	$(-1.00808501383545, 0.00789952065648606)$	$(62.7989898369691, 63.7909696663243)$
$6\overline{P}$	$(2.22215820573825, 0.0557271436079622)$	$(9.19729480722687, 8.74728184351541)$
$7\overline{P}$	$(-1.44341877680018, 0.0450249254945549)$	$(10.7585602581648, 11.4513598919737)$
$8\overline{P}$	$(1.09763831072356, 0.0257603670124760)$	$(19.8651848103736, 18.9541378924314)$
$9\overline{P}$	$(-11.6559204202252, 0.0621491847030033)$	$(8.00226117568193, 8.08805448620117)$
$10\overline{P}$	$(-1.03300876033239, 0.0156713679976759)$	$(31.4212963098427, 32.3893423113870)$
$11\overline{P}$	$(1.78753437475464, 0.0517354824950684)$	$(9.94426185923725, 9.38483205798531)$
$12\overline{P}$	$(-1.67790757997724, 0.0501243507574858)$	$(9.67720135664176, 10.2731817383583)$
$\cdots$	$\cdots$	$\cdots$

TABLE 5. $k = 3$

	Coset (Y, Z), $\lvert Y\rvert > Z > 0$	Evans triangle $\Delta(a, b; 8)$, (a, b)
$\overline{P}$	$(4.00000000000000, 0.0322580645161290)$	$(15.6250000000000, 15.3750000000000)$
$2\overline{P}$	$(-1.14269788182832, 0.0161279833517591)$	$(30.5644551534225, 31.4395771046420)$
$3\overline{P}$	$(1.45464220675284, 0.0242004990779207)$	$(21.0044580736648, 20.3170038011586)$
$4\overline{P}$	$(-1.88117183528003, 0.0282222825384067)$	$(17.4507057952180, 17.9822893439645)$
$5\overline{P}$	$(1.04926557255756, 0.0100935069689079)$	$(50.0133202146205, 49.0602726486334)$
$6\overline{P}$	$(-18.1470815261894, 0.0332642660589389)$	$(15.0035921663228, 15.0586974458443)$
$7\overline{P}$	$(-1.01981331872933, 0.00653857350956616)$	$(75.9789928885131, 76.9595645104311)$
$8\overline{P}$	$(2.29800068268954, 0.0299982503536006)$	$(16.8852191892855, 16.4500583089895)$
$9\overline{P}$	$(-1.31031588050509, 0.0215347432758587)$	$(22.8367065953550, 23.5998813495330)$
$10\overline{P}$	$(1.22461622645142, 0.0192374043348572)$	$(26.3993236099268, 25.5827412566962)$
$11\overline{P}$	$(-2.81670117200166, 0.0311467714920034)$	$(15.8755155463843, 16.2305407829767)$
$12\overline{P}$	$(1.00610351084978, 0.00366606104045919)$	$(136.883130131149, 135.889196615148)$
$\cdots$	$\cdots$	$\cdots$

TABLE 6. $k = 4$

□

Apparantly, once we have an Evans triangle in $\Delta(n)$, the stradegy above gives a way to produce more Evans triangles with the same ratio, and to test the positivity of rank of E_n. Since we already have lots of examples of Evans triangles from elementary methods, it gives us an opportunity to verify the rank of a large class of Edwards curves. For example, given any integer m, consider the Pell equation

$$x^2 - (m^2-2)y^2 = 1, \tag{5.1}$$

which has the primal solution (m^2-1, m). So the relation

$$x_k + y_k\sqrt{m^2-2} = ((m^2-1) + m\sqrt{m^2-2})^k \tag{5.2}$$

gives us an algorithm to compute the k-th solution (x_k, y_k) of (5.1). The Author's early work [7] then gives a way to attach the kth solution an Evans triangle with distinct Evans ratio.

6. APPENDEX

In this Appendex, we give the Mathematica codes used in computing Theorem 5.1. Given k,

$$f[k\_,\{x\_,y\_\}] := \{(k*y+1/(2*k^2-1)*x)/(1+(1+4*(k^2-1)^2)*k/(2*k^2-1)*x*y),$$

$$(-k*x+1/(2*k^2-1)*y)/(1-(1+4*(k^2-1)^2)*k/(2*k^2-1)*x*y)\}$$

$$g[\{x\_,y\_\}] := f[k,\{x,y\}]$$

$$h[\{a\_,b\_\}] := If[Abs[a] > b > 0, \{a,b\}, \{b,-a\}]$$

$$l[\{x\_,y\_\}] := Nest[h[\#]\&, \{x,y\}, 4]$$

$$d[\{x\_,y\_\}] := l[g[\{x,y\}]]$$

$$coset[\{x\_,y\_\},m\_] := Nest[d[\#]\&, \{x,y\}, m-1]$$

$$cor[\{y\_,z\_\}] := \{1/2*(1/z+1/y), 1/2*(1/z-1/y)\}$$

$$tri[\{x\_,y\_\},m\_] := cor[coset[\{x,y\},m]$$

Now if $P=(Y,Z) \in \mathbb{E}_{k^2-1}(\mathbb{Q})$, $YZ \neq 0$, to compute the $m\overline{P}$ in $\mathbb{E}_{k^2-1}(\mathbb{Q})/C$, one only has to input

$$coset[\{Y,Z\},m]$$

To compute $\Delta(a,b;k^2-1)$ corresponding to $m\overline{P}$, one has to input

$$tri[\{Y,Z\},m]$$

To draw a table for m from 1 to 12.

$$Table[coset[\{Y,Z\},i],i,12]$$

$$Table[tri[\{Y,Z\},i],i,12]$$

To obtain an approximation of 15-digital decimal, one only has to input

$$N[Table[coset[\{Y,Z\},i],i,12],15]$$

$$N[Table[tri[\{Y,Z\},i],i,12],15]$$

References

[1] H. Edwards *A normal form for elliptic curves*, Bulletin of the American Mathematical Society, Volume 44, No. 3, 393-422 (2007)

[2] D. Bernstein and T. Lange *Faster addition and doubling on elliptic curves*,

[3] J. Silverman and J. Tate *Rational points on elliptic curves*, UTM Springer (2015)

[4] R. Evans *Problem E2685, Amer. Math. Monthly*, American Mathematics Monthly, Volume 84, 820 (1977)

[5] X. Bian *Evans traingle and its applications*, mathematical pedagogy, Volume 17, 16-18 (2010)

[6] X. Bian *A new solution to the Evans triangle problem*, mathematical pedagogy, Volume 2, 68-69 (2011)

[7] Wensen Wu *Evans triangle and pell equations* (2016)

[8] M. Stoll *Rationalpoints on curves*, Journal de Theorie des Nombres de Bordeaux,

[9] Y. Li, *Study of one class of primitive Evans triangle*, Adanced Mathematical Studies, Volume 13, 31-32 (2010)