RATIONAL POINTS IN ELLIPTIC CURVES $y^2 = x^3 + pqx$

Eldar Sultanow, Jorma Jormakka, and Sourangshu Ghosh

Abstract. Let p and q be two distinct primes and $p \leq q$. This paper distills the conditions that both primes must satisfy in order for the elliptic curve $y^2 = x^3 - pqx$ to have rational solutions. Based on these conditions we demonstrate that any elliptic curve of this form has a rational solution.

2010 *Mathematics Subject Classification.* 14H52.
Key words and phrases. Elliptic Curves, Rational Points.

1. Introduction

TBD

2. Conditions for the curve $y^2 = x^3 - pqx$ to have a rational solution

We intersect a linear function $y = {}^a\!/_b \cdot x$ that has a rational slope $(a, b \in \mathbb{N})$ with the elliptic curve $y^2 = x^3 - pqx$. In order to retrieve the intersection points we must solve the following equation 1:

$$0 = x^3 - \left(\frac{a}{b}\right)^2 x^2 - pqx \tag{1}$$

One intersection point trivially is $(x, y) = (0, 0)$. The two remaining intersection points we retrieve by the quadratic formula 2:

$$x = \frac{1}{2}\left(\frac{a}{b}\right)^2 \pm \sqrt{\frac{\left(\frac{a}{b}\right)^4 + 4pq}{4}} \tag{2}$$

We can slightly convert the discriminant (the term under the square root) such that one can recognize at a glimpse the condition to be met for obtaining a rational solution:

$$\Delta = \frac{a^4 + 4pqb^4}{4b^4} \tag{3}$$

In order to obtain a rational solution, the sum $a^4 + 4pqb^4 = c^2$ must be a square number. We get $4pqb^4 = c^2 - a^4 = (c - a^2)(c + a^2)$. Now there exist several cases to be considered, how the factors $2 \cdot 2 \cdot p \cdot q \cdot b \cdot b \cdot b \cdot b$ are assigned to the two factors $(c - a^2)$ and $(c + a^2)$.

One case is $c - a^2 = 2pq$ and $c + a^2 = 2b^4$ which after substracting both equations from each other leads to $2pq = 2b^4 - 2a^2$ providing the condition that $pq = b^4 - a^2$ must be a difference of a fourth power and square number. This case is shown by the first row in Table 2. Let us retrace this principle by an example $p = 3$ and $q = 5$. In this case $3 \cdot 5 = 2^4 - 1^2 = b^4 - a^2$ and thus $c = 31$ and the discriminant $\Delta = {}^{961}\!/_{64}$ which finally leads to the rational solutions $(x, y) = (4, 2)$ and $(x, y) = ({}^{-15}\!/_4, {}^{-15}\!/_8)$.

$c - a^2$	$c + a^2$	**Condition**	**Example Curve**	**Rational Points**
$2pq$	$2b^4$	$pq = b^4 - a^2$	$y^2 = x^3 - 15x$	$(4, 2), (-15/4, -15/8)$
$2b^2$	$2pqb^2$	$pq - 1 = \left(\frac{a}{b}\right)^2$	tbd	tbd
$2pqb$	$2b^3$	$pq = \frac{b^3 - a^2}{b}$	$y^2 = x^3 - 21x$	$(7, 14), (-3, -6)$

References

[1] C. Koch, E. Sultanow, and S. Cox. Divisions by two in collatz sequences: A data science approach. *International Journal of Pure Mathematical Sciences*, 21, 2020.

[2] Collag3n. Comment on answer to "a possible way to prove non-cyclicity of eventual counterexamples of the collatz conjecture?", December 2020.

[3] E. Sultanow, C. Koch, and S. Cox. Collatz sequences in the light of graph theory. Technical report, University of Potsdam, 2020.

[4] L. Halbeisen and N. Hungerbühler. Optimal bounds for the length of rational collatz cycles. *Acta Arithmetica*, 78(3):227–239, 1997.

Eldar Sultanow, Capgemini, Bahnhofstrasse 30, 90402 Nuremberg, Germany
Email address: eldar.sultanow@capgemini.com

Sourangshu Ghosh, Indian institute of Technology Kharagpur, Kharagpur, West Bengal 721302, India
Email address: sourangshu@iitkgp.ac.in

Sourangshu Ghosh, Indian institute of Technology Kharagpur, Kharagpur, West Bengal 721302, India
Email address: sourangshu@iitkgp.ac.in