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

Eldar Sultanow, Malik Amir, Sourangshu Ghosh, and Jorma Jormakka

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. These conditions establish the basis for proving that any elliptic curve of this form has a rational solution.

1. Introduction

The fact whether an elliptic curve has rational points or not has been occupying mathematicians for a fairly while. There are stringent conditions under which elliptic curves have definitely rational points. We lay the foundation for a weaker condition under which elliptic curves are guaranteed to feature rational points.

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 $(a, b \in \mathbb{Z})$ 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:

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

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

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 must be a difference of a fourth power and square number $pq = b^4 - a^2$. This case has number 26 and it is listed in the 26th row of 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 $(x, y) = ({}^{-15}/_{4}, {}^{-15}/_{8})$. This curve is listed in the LMFDB [1] too.

Finding all possibilities to split the set $P = \{2, 2, p, q, b, b, b, b\}$ of elements (factors) into two subsets is equivalent to finding half the number of divisors of 2^2pqb^4. For this we can use the divisor function $\tau(n)$, also denoted as $d(n)$ or $\sigma_0(n)$, which returns the number of positive divisors of n, see [2, p. 123], [3]. Suppose that $n = p_1^{e_1} \cdots p_k^{e_k}$, then we obtain the number of divisors via $\tau(n) = (e_1 + 1) \cdots (e_k + 1)$, see [2, p. 125].

In our case the number of possibilities for splitting the set P into two subsets is:

$$\frac{1}{2}\tau(2^2pqb^4) = \frac{1}{2}(2 + 1)(1 + 1)(1 + 1)(4 + 1) = 30$$

The corresponding combinations (numbered cases) are:

1	$(22pqbbbb, \emptyset)$	9	$(22qbbbb, p)$	16	$(22pbbbb, q)$	23	$(2b, 2pqbbb)$
2	$(2pqbbbb, 2)$	10	$(2qbbbb, p2)$	17	$(2pbbbb, q2)$	24	$(2bb, 2pqbb)$
3	$(pqbbbb, 22)$	11	$(qbbbb, p22)$	18	$(pbbbb, q22)$	25	$(2bbb, 2pqb)$
4	$(bbbb, 22pq)$	12	$(qbbb, p22b)$	19	$(pbbb, q22b)$	26	$(2bbbb, 2pq)$
5	$(bbb, 22pqb)$	13	$(qbb, p22bb)$	20	$(pbb, q22bb)$	27	$(22b, pqbbb)$
6	$(bb, 22pqbb)$	14	$(qb, p22bbb)$	21	$(pb, q22bbb)$	28	$(22bb, pqbb)$
7	$(b, 22pqbbb)$	15	$(q, p22bbbb)$	22	$(p, q22bbbb)$	29	$(22bbb, pqb)$
8	$(\emptyset, 22pqbbbb)$					30	$(22bbbb, pq)$

At this point we accept that (because b is not necessarily prime) not all cases are covered. Table 1 and 2 deduce from these cases the conditions that both primes p, q must satify for the curve $y^2 = x^3 - pqx$ to have a rational solution.

In some cases the conditions overlap, for example condition 19 in Table 2 leads directly to condition 25 when substituting a with ${}^{2a}/_{p}$ and b with ${}^{2b}/_{p}$:

$$q = \frac{p\left(\frac{2b}{p}\right)^3 - 2\left(\frac{2a}{p}\right)^2}{4\frac{2b}{p}} = \frac{p(8pb^3 - 8pa^2)}{8p^3b} = \frac{b^3 - a^2}{pb}$$

Similarly, condition 12 in Table 2 leads to condition 25 when a is replaced with ${}^{2a}/_{q}$ and b with ${}^{2b}/_{q}$.

In Table 2, substituting a with $2a$ and b with $2b$ leads condition in case 3 to the condition given by case 1, and similarly case 4 leads to case 30, case 11 leads to case 9, and case 18 to case 16. The same occurs with the equal-numbered cases in Table 1.

In Table 1, case 1 is identical to case 8 in Table 2 and, conversely, case 8 in Table 1 is identical to case 1 in Table 2.

In Table 1, replacing b with $-b$ brings the conditions of cases 5,7,12,14,19,21,23,25,27,29 to the same-numbered cases in Table 2.

Moreover condition 1 in Table 1 (which is equal to condition 8 in Table 2) is impossible, since $4b^4pq + 2a^2 = 1$ has no integer solutions a, b. For the same reason, the condition given by case 2 in Table 1 can never be satisfied too.

Case	$\boldsymbol{c - a^2}$	$\boldsymbol{c + a^2}$	**Condition**	**Sample Curve**	$\boldsymbol{a, b, c}$	$\boldsymbol{\Delta}$	**Rational Points**
1	$4pqb^4$	1	$pq = {}^{1-2a^2}/_{4b^4}$	Tab. 2, case 8			
2	$2pqb^4$	2	$pq = {}^{1-a^2}/_{b^4}$	impossible			
3	pqb^4	4	$pq = {}^{4-2a^2}/_{b^4}$	see case 1			
4	b^4	$4pq$	$pq = {}^{2a^2+b^4}/_{4}$	see case 30			
5	b^3	$4pqb$	$pq = {}^{2a^2+b^3}/_{4b}$	Tab. 2, case 5			
6	b^2	$4pqb^2$	$pq = {}^{2a^2+b^2}/_{4b^2}$				
7	b	$4pqb^3$	$pq = {}^{2a^2+b}/_{4b^3}$	Tab. 2, case 7			
8	1	$4pqb^4$	$pq = {}^{2a^2+1}/_{4b^4}$	Tab. 2, case 1			
9	$4qb^4$	p	$p = 2a^2 + 4qb^4$				
10	$2qb^4$	$2p$	$p = a^2 + qb^4$				
11	qb^4	$4p$	$p = {}^{2a^2+qb^4}/_{4}$	see case 9			
12	qb^3	$4pb$	$p = {}^{2a^2+qb^3}/_{4b}$	Tab. 2, case 12			
13	qb^2	$4pb^2$	$p = {}^{2a^2+qb^2}/_{4b^2}$				
14	qb	$4pb^3$	$p = {}^{2a^2+qb}/_{4b^3}$	Tab. 2, case 14			
15	q	$4pb^4$	$p = {}^{2a^2+q}/_{4b^4}$				
16	$4pb^4$	q	$q = 2a^2 + 4pb^4$				
17	$2pb^4$	$2q$	$q = a^2 + pb^4$				
18	pb^4	$4q$	$q = {}^{2a^2+pb^4}/_{4}$	see case 16			
19	pb^3	$4qb$	$q = {}^{2a^2+pb^3}/_{4b}$	Tab. 2, case 19			
20	pb^2	$4qb^2$	$q = {}^{2a^2+pb^2}/_{4b^2}$				
21	pb	$4qb^3$	$q = {}^{2a^2+pb}/_{4b^3}$	Tab. 2, case 21			
22	p	$4qb^4$	$q = {}^{2a^2+p}/_{4b^4}$				
23	$2b$	$2pqb^3$	$pq = {}^{a^2+b}/_{b^3}$	Tab. 2, case 23			
24	$2b^2$	$2pqb^2$	$pq = {}^{a^2+b^2}/_{b^2}$				
25	$2b^3$	$2pqb$	$pq = {}^{a^2+b^3}/_{b}$	Tab. 2, case 25			
26	$2b^4$	$2pq$	$pq = a^2 + b^4$				
27	$4b$	pqb^3	$pq = {}^{2a^2+4b}/_{b^3}$	Tab. 2, case 27			
28	$4b^2$	pqb^2	$pq = {}^{2a^2+4b^2}/_{b^2}$				
29	$4b^3$	pqb	$pq = {}^{2a^2+4b^3}/_{b}$	Tab. 2, case 29			
30	$4b^4$	pq	$pq = 2a^2 + 4b^4$				

TABLE 1. Conditions for elliptic curves $y^2 = x^3 - pqx$ to have rational solutions

Case	$c-a^2$	$c+a^2$	**Condition**	**Sample Curve**	a,b,c	Δ	**Rational Points**
1	1	$4pqb^4$	$pq = {}^{2a^2+1}/_{4b^4}$				
2	2	$2pqb^4$	$pq = {}^{a^2+1}/_{b^4}$				
3	4	pqb^4	$pq = {}^{2a^2+4}/_{b^4}$	see case 1			
4	$4pq$	b^4	$pq = {}^{b^4-2a^2}/_{4}$	see case 30			
5	$4pqb$	b^3	$pq = {}^{b^3-2a^2}/_{4b}$				
6	$4pqb^2$	b^2	$pq = {}^{b^2-2a^2}/_{4b^2}$				
7	$4pqb^3$	b	$pq = {}^{b-2a^2}/_{4b^3}$				
8	$4pqb^4$	1	$pq = {}^{1-2a^2}/_{4b^4}$	impossible			
9	p	$4qb^4$	$p = 4qb^4 - 2a^2$				
10	$2p$	$2qb^4$	$p = qb^4 - a^2$				
11	$4p$	qb^4	$p = {}^{qb^4-2a^2}/_{4}$	see case 9			
12	$4pb$	qb^3	$p = {}^{qb^3-2a^2}/_{4b}$	see case 25			
13	$4pb^2$	qb^2	$p = {}^{qb^2-2a^2}/_{4b^2}$				
14	$4pb^3$	qb	$p = {}^{qb-2a^2}/_{4b^3}$				
15	$4pb^4$	q	$p = {}^{q-2a^2}/_{4b^4}$				
16	q	$4pb^4$	$q = 4pb^4 - 2a^2$				
17	$2q$	$2pb^4$	$q = pb^4 - a^2$				
18	$4q$	pb^4	$q = {}^{pb^4-2a^2}/_{4}$	see case 16			
19	$4qb$	pb^3	$q = {}^{pb^3-2a^2}/_{4b}$	see case 25			
20	$4qb^2$	pb^2	$q = {}^{pb^2-2a^2}/_{4b^2}$				
21	$4qb^3$	pb	$q = {}^{pb-2a^2}/_{4b^3}$				
22	$4qb^4$	p	$q = {}^{p-2a^2}/_{4b^4}$				
23	$2pqb^3$	$2b$	$pq = {}^{b-a^2}/_{b^3}$				
24	$2pqb^2$	$2b^2$	$pq = {}^{b^2-a^2}/_{b^2}$				
25	$2pqb$	$2b^3$	$pq = {}^{b^3-a^2}/_{b}$	$y^2 = x^3 - 77x$	$6, 9, 1422$	$\frac{6241}{81}$	$(9,6), (-\frac{77}{9}, -\frac{154}{27})$
26	$2pq$	$2b^4$	$pq = b^4 - a^2$	$y^2 = x^3 - 15x$	$1, 2, 31$	$\frac{961}{64}$	$(4,2), (-\frac{15}{4}, -\frac{15}{8})$
27	pqb^3	$4b$	$pq = {}^{4b-2a^2}/_{b^3}$				
28	pqb^2	$4b^2$	$pq = {}^{4b^2-2a^2}/_{b^2}$				
29	pqb	$4b^3$	$pq = {}^{4b^3-2a^2}/_{b}$				
30	pq	$4b^4$	$pq = 4b^4 - 2a^2$				

TABLE 2. Conditions for elliptic curves $y^2 = x^3 - pqx$ to have rational solutions (reversed cases)

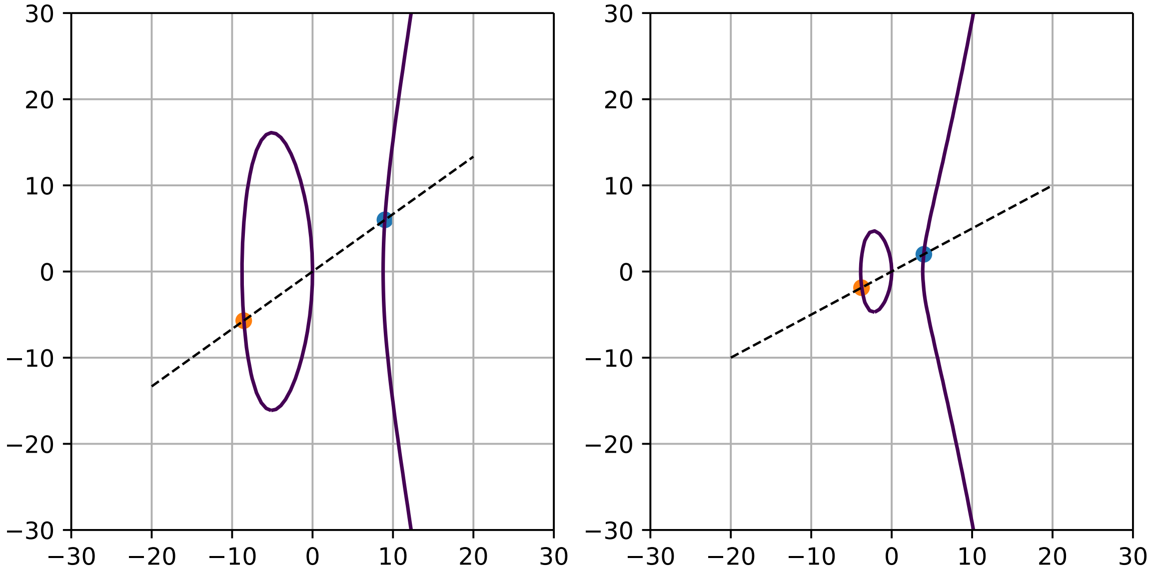

Figure 1. Curves for case 25 (left) and case 26 (right) as given in Table 2

Figure 1 shows the curve $y^2 = x^3 - 77x$ on the left and the curve $y^2 = x^3 - 15x$ on the right as given by the cases 25 and 26 in Table 2. The rational points including the intersecting line (that has a slope $^a/_b$) are depicted too.

3. Conclusion and Outlook

So far, we have inferred the conditions that two distinct odd primes p, q must satisfy for the elliptic curve $y^2 = x^3 - pqx$ to have rational points. The next step consists in demonstrating that there exist no product of two odd primes p, q for which all these contitions do not match. Inversly stated, at least one of the conditions is true for both primes. That means any product of two odd primes p, q shall be a congruent number.

References

[1] LMFDB The L-functions and Modular Forms Database. Elliptic curve with lmfdb label 14400.cq1 (cremona label 14400de1). https://www.lmfdb.org/EllipticCurve/Q/14400/cq/1, 2021.
[2] Benjamin Fine and Gerhard Rosenberger. *Number Theory: An Introduction via the Distribution of Primes*. Birkhäuser, 2007.
[3] The OEIS Foundation. d(n), the number of divisors of n. https://oeis.org/A000005, 2021.

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

Malik Amir, École Polytechnique Fédérale de Lausanne, CH-1015 Lausanne, Switzerland
Email address: malik.amir@epfl.ch

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

Jorma Jormakka, Aalto University, Department of Communications and Networking, Helsinki, Finland
Email address: jorma.o.jormakka@gmail.com