ON FAMILIES OF ELLIPTIC CURVES $E_{p,q} : y^2 = x^3 - pqx$ THAT INTERSECT THE SAME LINE $L_{a,b} : y = \frac{a}{b}x$ OF RATIONAL SLOPE

Eldar Sultanow, Malik Amir, Madjid Tehrani, and Bill Buchannan

Abstract. Let p and q be two distinct odd primes, $p < q$ and $E_{p,q} : y^2 = x^3 - pqx$ be an elliptic curve. Fix a line $L_{a.b} : y = \frac{a}{b}x$ where $a \in \mathbb{Z}, b \in \mathbb{N}$ and $(a, b) = 1$. We study sufficient conditions that p and q must satisfy so that there are infinitely many elliptic curves $E_{p,q}$ that intersect $L_{a,b}$.

1. Introduction

Rewrite when the paper is done.

2. Rational points on $E_{p,q}$

Let $L_{a,b} : y = \frac{a}{b}x$ be a linear function where $a \in \mathbb{Z}, b \in \mathbb{N}$ and $(a, b) = 1$. To find rational points on the elliptic curve $E_{p,q} : y^2 = x^3 - pqx$ for fixed (p, q), it is sufficient to solve for (a, b). Conversly, if we fix a pair (a, b), we may want to describe all pairs (p, q) whose corresponding curve $E_{p,q}$ intersects $L_{a,b}$. To proceed in an elementary way, this is equivalent to solve the equation

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

This cubic has 3 solutions, one trivial given by $x = 0$ and the others given by

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

In order for x to be rational, we ask that $a^4 + 4pqb^4$ is a square, say

$$a^4 + 4pqb^4 = c^2$$

for some integer c. This last equation can be factored as $4pqb^4 = c^2 - a^4 = (c - a^2)(c + a^2)$. We are now left with the study of several cases given by the number of ways to assign

2010 *Mathematics Subject Classification.* 14H52.

Key words and phrases. Elliptic Curves, Rational Points.

the divisors of $4pqb^4$ to each of the factors $(c \pm a^2)$. Counting the number of cases boils down to computing half of the number of divisors of 2^2pqb^4. For $\tau(n)$ the divisor function and $n = p_1^{e_1} \cdots p_k^{e_k}$, we have the following identity $\tau(n) = (e_1 + 1) \cdots (e_k + 1)$. In our case we get at least

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

since b is not necessarily prime.

The corresponding 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	$(22bbbb, pq)$

For the rest of this note, we will focus our attention on these cases only. Table 1 and 2 below contain sufficient conditions for $E_{p,q}$ to have a rational point for some fixed line $L_{a,b}$. In Appendix A, we have described briefly the impossible cases.

Case	$c - a^2$	$c + a^2$	**Condition**	**Sample Curve**	a, b	**Rational Points**
1	$4pqb^4$	1	$pq = {}^{1-2a^2}/_{4b^4}$	n/a, reason a		
2	$2pqb^4$	2	$pq = {}^{1-a^2}/_{b^4}$	n/a, reason a		
3	pqb^4	4	$pq = {}^{4-2a^2}/_{b^4}$	n/a, reason a		
4	b^4	$4pq$	$pq = {}^{2a^2+b^4}/_{4}$	n/a, reason b		
5	b^3	$4pqb$	$pq = {}^{2a^2+b^3}/_{4b}$	n/a, reason b		
6	b^2	$4pqb^2$	$pq = {}^{2a^2+b^2}/_{4b^2}$	n/a, reason b		
7	b	$4pqb^3$	$pq = {}^{2a^2+b}/_{4b^3}$	n/a, reason c		
8	1	$4pqb^4$	$pq = {}^{2a^2+1}/_{4b^4}$	n/a, reason d		
9	$4qb^4$	p	$p = 2a^2 + 4qb^4$	n/a, reason e		
10	$2qb^4$	$2p$	$p = a^2 + qb^4$	n/a, reason e		
11	qb^4	$4p$	$p = {}^{2a^2+qb^4}/_{4}$	n/a, reason b		
12	qb^3	$4pb$	$p = {}^{2a^2+qb^3}/_{4b}$	n/a, reason b		
13	qb^2	$4pb^2$	$p = {}^{2a^2+qb^2}/_{4b^2}$	n/a, reason b		
14	qb	$4pb^3$	$p = {}^{2a^2+qb}/_{4b^3}$	Table 2, case 17		
15	q	$4pb^4$	$p = {}^{2a^2+q}/_{4b^4}$	n/a, reason f		
16	$4pb^4$	q	$q = 2a^2 + 4pb^4$	n/a, reason g		
17	$2pb^4$	$2q$	$q = a^2 + pb^4$	$y^2 = x^3 - 921$	$8, 3$	$\left(\frac{307}{9}, \frac{2456}{27}\right), (-27, -72)$
18	pb^4	$4q$	$q = {}^{2a^2+pb^4}/_{4}$	n/a, reason b		
19	pb^3	$4qb$	$q = {}^{2a^2+pb^3}/_{4b}$	n/a, reason b		
20	pb^2	$4qb^2$	$q = {}^{2a^2+pb^2}/_{4b^2}$	n/a, reason b		
21	pb	$4qb^3$	$q = {}^{2a^2+pb}/_{4b^3}$	Table 2, case 9,10		
22	p	$4qb^4$	$q = {}^{2a^2+p}/_{4b^4}$	n/a, reason h		
23	$2b$	$2pqb^3$	$pq = {}^{a^2+b}/_{b^3}$	see case 26		
24	$2b^2$	$2pqb^2$	$pq = {}^{a^2+b^2}/_{b^2}$	see case 26		
25	$2b^3$	$2pqb$	$pq = {}^{a^2+b^3}/_{b}$	see case 26		
26	$2b^4$	$2pq$	$pq = a^2 + b^4$	$y^2 = x^3 - 65x$	$7, 2$	$\left(\frac{65}{4}, \frac{455}{8}\right), (-4, -14)$
27	$4b$	pqb^3	$pq = {}^{2a^2+4b}/_{b^3}$	n/a, reason b		
28	$4b^2$	pqb^2	$pq = {}^{2a^2+4b^2}/_{b^2}$	n/a, reason b		
29	$4b^3$	pqb	$pq = {}^{2a^2+4b^3}/_{b}$	see case 26		
30	$4b^4$	pq	$pq = 2a^2 + 4b^4$	n/a, reason g		

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

Case	$\boldsymbol{c-a^2}$	$\boldsymbol{c+a^2}$	**Condition**	**Sample Curve**	$\boldsymbol{a,b}$	**Rational Points**
1	1	$4pqb^4$	$pq = {}^{2a^2+1}/_{4b^4}$	Table 1, case 8		
2	2	$2pqb^4$	$pq = {}^{a^2+1}/_{b^4}$	$y^2 = x^3 - 3281x$	$1432, 5$	$\left(-\frac{1}{25}, -\frac{1432}{125}\right)$
3	4	pqb^4	$pq = {}^{2a^2+4}/_{b^4}$	n/a, reason b		
4	$4pq$	b^4	$pq = {}^{b^4-2a^2}/_{4}$	n/a, reason b		
5	$4pqb$	b^3	$pq = {}^{b^3-2a^2}/_{4b}$	n/a, reason b		
6	$4pqb^2$	b^2	$pq = {}^{b^2-2a^2}/_{4b^2}$	n/a, reason b		
7	$4pqb^3$	b	$pq = {}^{b-2a^2}/_{4b^3}$	n/a, reason a		
8	$4pqb^4$	1	$pq = {}^{1-2a^2}/_{4b^4}$	Table 1, case 1		
9	p	$4qb^4$	$p = 4qb^4 - 2a^2$	n/a, reason g		
10	$2p$	$2qb^4$	$p = qb^4 - a^2$	$y^2 = x^3 - 21x$	$2, 1$	$(7, 14), (-3, -6)$
11	$4p$	qb^4	$p = {}^{qb^4-2a^2}/_{4}$	n/a, reason b		
12	$4pb$	qb^3	$p = {}^{qb^3-2a^2}/_{4b}$	n/a, reason b		
13	$4pb^2$	qb^2	$p = {}^{qb^2-2a^2}/_{4b^2}$	n/a, reason b		
14	$4pb^3$	qb	$p = {}^{qb-2a^2}/_{4b^3}$	Table 1, case 17		
15	$4pb^4$	q	$p = {}^{q-2a^2}/_{4b^4}$	n/a, reason f		
16	q	$4pb^4$	$q = 4pb^4 - 2a^2$	n/a, reason g		
17	$2q$	$2pb^4$	$q = pb^4 - a^2$	$y^2 = x^3 - 69x$	$5, 2$	$(12, 30), \left(-\frac{23}{4}, -\frac{115}{8}\right)$
18	$4q$	pb^4	$q = {}^{pb^4-2a^2}/_{4}$	n/a, reason b		
19	$4qb$	pb^3	$q = {}^{pb^3-2a^2}/_{4b}$	n/a, reason b		
20	$4qb^2$	pb^2	$q = {}^{pb^2-2a^2}/_{4b^2}$	n/a, reason b		
21	$4qb^3$	pb	$q = {}^{pb-2a^2}/_{4b^3}$	Table 1, case 9,10		
22	$4qb^4$	p	$q = {}^{p-2a^2}/_{4b^4}$	n/a, reason h		
23	$2pqb^3$	$2b$	$pq = {}^{b-a^2}/_{b^3}$	n/a, reason a		
24	$2pqb^2$	$2b^2$	$pq = {}^{b^2-a^2}/_{b^2}$	n/a, reason a		
25	$2pqb$	$2b^3$	$pq = {}^{b^3-a^2}/_{b}$	n/a, reason i		
26	$2pq$	$2b^4$	$pq = b^4 - a^2$	$y^2 = x^3 - 15x$	$1, 2$	$(4, 2), \left(-\frac{15}{4}, -\frac{15}{8}\right)$
27	pqb^3	$4b$	$pq = {}^{4b-2a^2}/_{b^3}$	n/a, reason b		
28	pqb^2	$4b^2$	$pq = {}^{4b^2-2a^2}/_{b^2}$	n/a, reason b		
29	pqb	$4b^3$	$pq = {}^{4b^3-2a^2}/_{b}$	see case 26		
30	pq	$4b^4$	$pq = 4b^4 - 2a^2$	n/a, reason g		

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

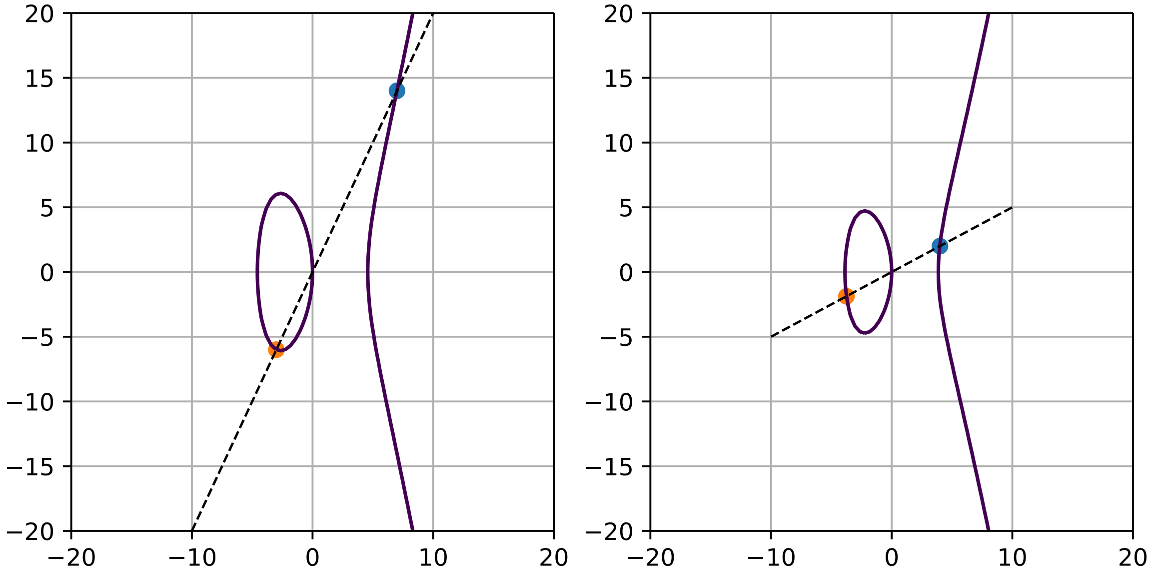

FIGURE 1. Curves for case 10 (left) and case 26 (right) as given in Table 2

Figure 1 shows the curve $y^2 = x^3 - 21x$ (LMFDB [1]) on the left and the curve $y^2 = x^3 - 15x$ (LMFDB [2]) on the right as given by the cases 10 and 26 in Table 2. The rational points including the intersecting line (that has a slope a/b) are depicted too.

3. Six conditions for $E_{p,q}$ to have rational points

3.1. **Table 1, Case 17: $q = a^2 + pb^4$.** For $b = 1$ and $a = 2$ all consecutive primes p, q give a solution whose difference is 4. According to Polignac's conjecture (which isn't proved), there are infinitely many examples per any even difference of both primes [3, p. 295].

3.2. **Table 1, Case 26: $pq = a^2 + b^4$.** By symmetry of the curve with the x axis we can actually consider a and b to be positive, this will probably accelerate getting results. Also, after struggling on the question all night yesterday, I realized its a very hard question and I don't know the tools to solve it. Maybe what we can do instead of spending a year solving this problem is actually to write a paper studying the very basic cases one can get with simple arithmetic and give some numerics about the proportion of primes satisfying each of these cases up to say a very big number. For example, from the list case 26 you sent me yesterday, we could say it boils down to verifying the conjecture that $pq = a^2 + b^4$ has infinitely many solutions (its actually a theorem of iwaniec and frielander that there are infinitely many primes of the form $p = a^2 + b^4$) and up to X (a big integer) we have Y of the primes whose product is a semiprime of the form $a^2 + b^4$, see [4].

One example is the curve $y^2 = x^3 - 65x$, which is also listed in the LMFDB [5]. Th value $c = 81$ and the discriminant is $^{6561}/_{64}$.

In the case that $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$ no solution exist [6, p. 21]. Let us set $p = r^2 + s^2$ and $q = u^2 + v^2$. If $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$ we exactly obtain one solution $r > s > 0$ for p and one solution $u > v > 0$ for q [6, p. 21]. If we now have these unique solutions $p = r^2 + s^2$ and $q = u^2 + v^2$, then the product of both primes is $pq = (r^2 + s^2)(u^2 + v^2) = (ru + sv)^2 + (rv - su)^2 = (ru - sv)^2 + (rv + su)^2$. Consider $b^2 = c$, other integer solutions for $pq = a^2 + c^2 = a^2 + b^4$ do not exist, unless one of the four integers $ru + sv$, $|rv - su|$, $|ru - sv|$ and $rv + su$ is a perfect square.

3.3. **Table 2, Case 2:** $\boldsymbol{pq = {}^{a^2+1}/_{4b^4}}$**.** If $b = 0, 2[4]$ then $a = 1, 3[4]$. If $b = 1, 3[4]$ then $a = 0, 2[4]$ The smallest found example for $b > 1$ is $y^2 = x^3 - 3281x$, which means $p = 17, q = 193$ and $a = 1432, b = 5, c = 2050626$ and the discriminant $\Delta = {}^{1051266747969}/_{625}$. Two rational points on this curve are $(82025, 23491960)$ and $(-^{1}/_{25}, -^{1432}/_{125})$.

3.4. **Table 2, Case 10:** $\boldsymbol{p = qb^4 - a^2}$**.** We note that if b is odd then a must be even. If b is even, then $2^4 | p + a^2$.

This case can be transformed to the problem describing primes of the form $x^2 + ny^2$ which is extensively elaborated by David A. Cox [7].

3.5. **Table 2, Case 17:** $\boldsymbol{q = pb^4 - a^2}$**.** The example given by Table 2 is $y^2 = x^3 - 69x$ where $p = 3, q = 23$, which is also listed in the LMFDB [8]. Another examples are $p = 5, q = 31, a = 7, b = 2$ and $p = 7, q = 31, a = 9, b = 2$ and $p = 5, q = 71, a = 3, b = 2$.

Let us set $b = 2c$ and thus consider $a^2 = 16pc^3 - qc$. It follows $a^2 \equiv 16pc^3 \bmod q$ and $a^2 \equiv -qc \bmod p$. Using these two congruences we can approach a solution using Quadratic residue and the Chinese remainder theorem.

3.6. **Table 2, Case 26:** $\boldsymbol{pq = b^4 - a^2}$**.** One example is $p = 3, q = 15$ where $a = 1, b = 2, c = 31$ and $\Delta = {}^{961}/_{64}$. More generally, we need $p | b^2 - a$ or $p | b^2 + a$ and the same conditions apply to q.

We can write $pq = b^4 - a^2 = (b^2 - a)(b^2 + a)$ which leads us directly to the *prime gap* problem, whose special case $a = 1$ is well known as the *twin prime conjecture*.

4. Considering b being composite

If we consider that b is not necessarily prime, we have to modify these six introduced cases.

4.1. **Table 1, Case 17 modified.** One example is $p = 7, q = 37$ where $a = -5, b = 6, c = 1159$ with a rational point $(-63/4, 105/8)$. In this case we have $(c - a^2)(c + a^2) = 1134 \cdot 1184 = 2b_2^4 p \cdot 2b_1^4 q = 4pqb^4$ with $b = b_1 \cdot b_2 = 2 \cdot 3$. Setting $c - a^2 = 2b_2^4 p$ and $c + a^2 = 2b_1^4 q$ leads to the modified case $b_1^4 q = a^2 + pb_2^4$. The special case $b_1 = 1$ corresponds to the original case. The special case $b_2 = 1$ corresponds to case 10 in Table 2. Therefore this modified case makes the case 10 in Table 2 (Section 3.4) obsolete.

4.2. **Table 1, Case 26 modified.** One example is $p = 5, q = 193$ where $a = -758, b = 65, c = 631686$ with a rational point $(-169/25, 9854/125)$. In this case we have $(c - a^2)(c + a^2) = 57122 \cdot 1206250 = 2b_2^4 \cdot 2b_1^4 pq = 4pqb^4$ with $b = b_1 \cdot b_2 = 5 \cdot 13$. Setting $c - a^2 = 2b_1^4 pq$ and $c + a^2 = 2b_2^4$ leads to the modified case $b_1^4 pq = a^2 + b_2^4$. The special case $b_1 = 1$ corresponds to the original case. The special case $b_2 = 1$ corresponds to case 2 in Table 2. Therefore this modified case makes the case 2 in Table 2 (Section 3.3) obsolete.

4.3. **Table 2, Case 17 modified.** One example is $p = 11, q = 43$ where $a = -536, b = 65, c = 341046$ with a rational point $(-1859/25, 76648/125)$. In this case we have $(c-a^2)(c+a^2) = 53750 \cdot 628342 = 2b_1^4 q \cdot 2b_2^4 p = 4pqb^4$ with $b = b_1 \cdot b_2 = 5 \cdot 13$. Setting $c - a^2 = 2b_1^4 q$ and $c + a^2 = 2b_2^4 p$ leads to the modified case $b_1^4 q = pb_2^4 - a^2$. The special case $b_1 = 1$ corresponds to the original case. The special case $b_2 = 1$ corresponds to case 10 in Table 1 which cannot occur. Moreover b_2 must be larger than b_1.

4.4. **Table 2, Case 26 modified.** One example is $p = 5, q = 11$ where $a = 39, b = 14, c = 3281$ with a rational point $(49/4, 273/8)$. In this case we have $(c - a^2)(c + a^2) = 1760 \cdot 4802 = 2b_1^4 pq \cdot 2b_2^4 = 4pqb^4$ with $b = b_1 \cdot b_2 = 2 \cdot 7$. Setting $c - a^2 = 2b_1^4 pq$ and $c + a^2 = 2b_2^4$ leads to the modified case $b_1^4 pq = b_2^4 - a^2$. The special case $b_1 = 1$ corresponds to the original case. The special case $b_2 = 1$ corresponds to case 2 in Table 1 which cannot occur. Moreover b_2 must be larger than b_1.

5. Unveiled Patterns

Using the four cases presented by Section 4 we cover any curve $E_{p,q}$ given by $y^2 = x^3 - pqx$. In a matrix where the x-axis is labeled by prime values p and the y-axis is labeled by primes values q we colorize each cell by red for case 4.1, green for case 4.2, blue for case 4.3 and yellow for case 4.4. The more curves covered by case 4.1 exist, the more intense is the color red. Analogously, the more curves covered by case 4.2 exist, the more intense is the color green. The more curves covered by case 4.3 exist, the more intense is the color blue. The more curves covered by case 4.4 exist, the more intense is the color yellow.

We unveiled the following patterns:

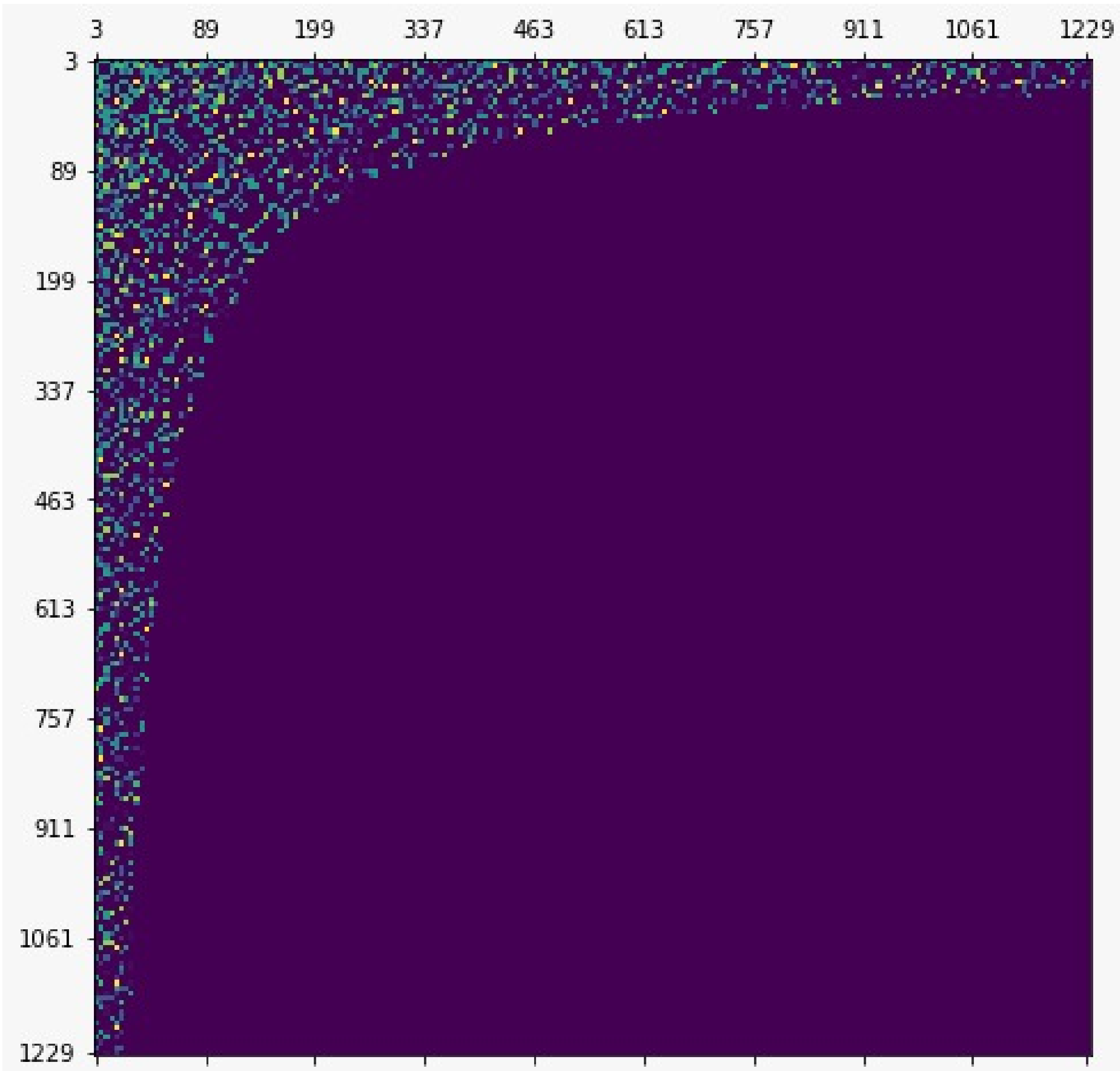

FIGURE 2. Cases 1,2,3,4 up to $p, q \leq 1229$

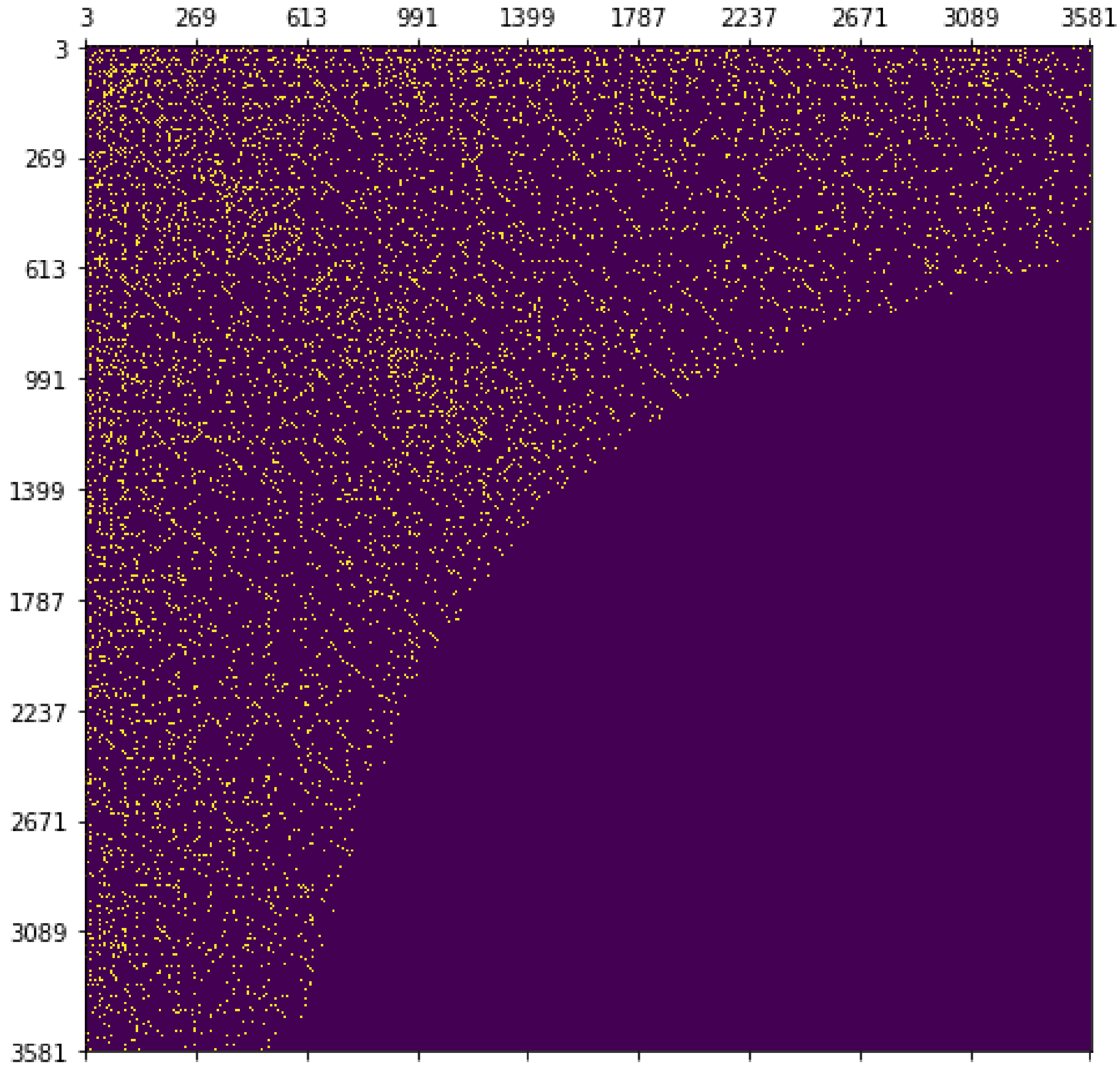

Figure 3. Only Case 1 curves up to $p, q \leq 3581$

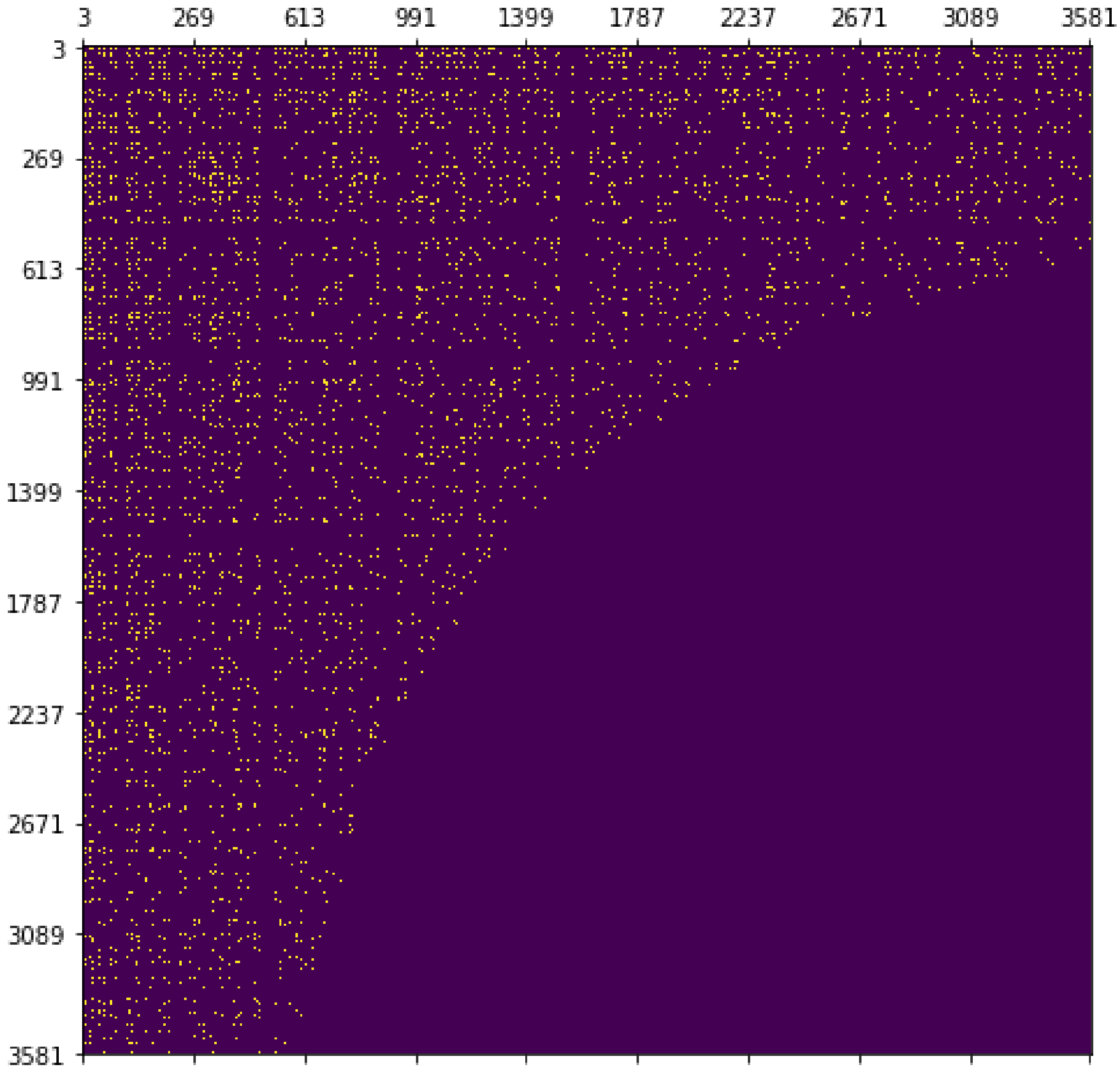

FIGURE 4. Only Case 2 curves up to $p, q \leq 3581$ – it shows square patterns

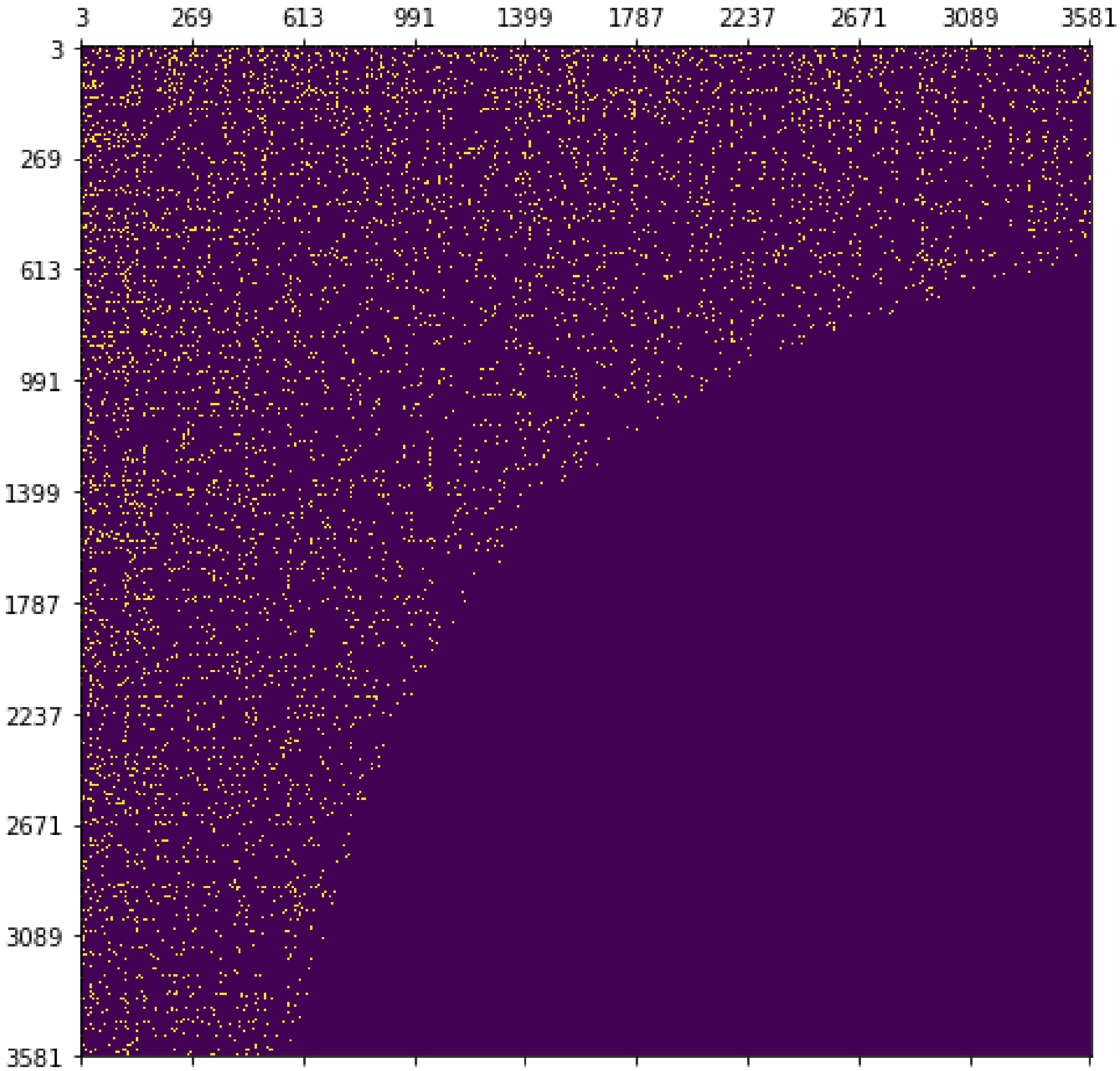

FIGURE 5. Only Case 3 curves up to $p, q \leq 3581$

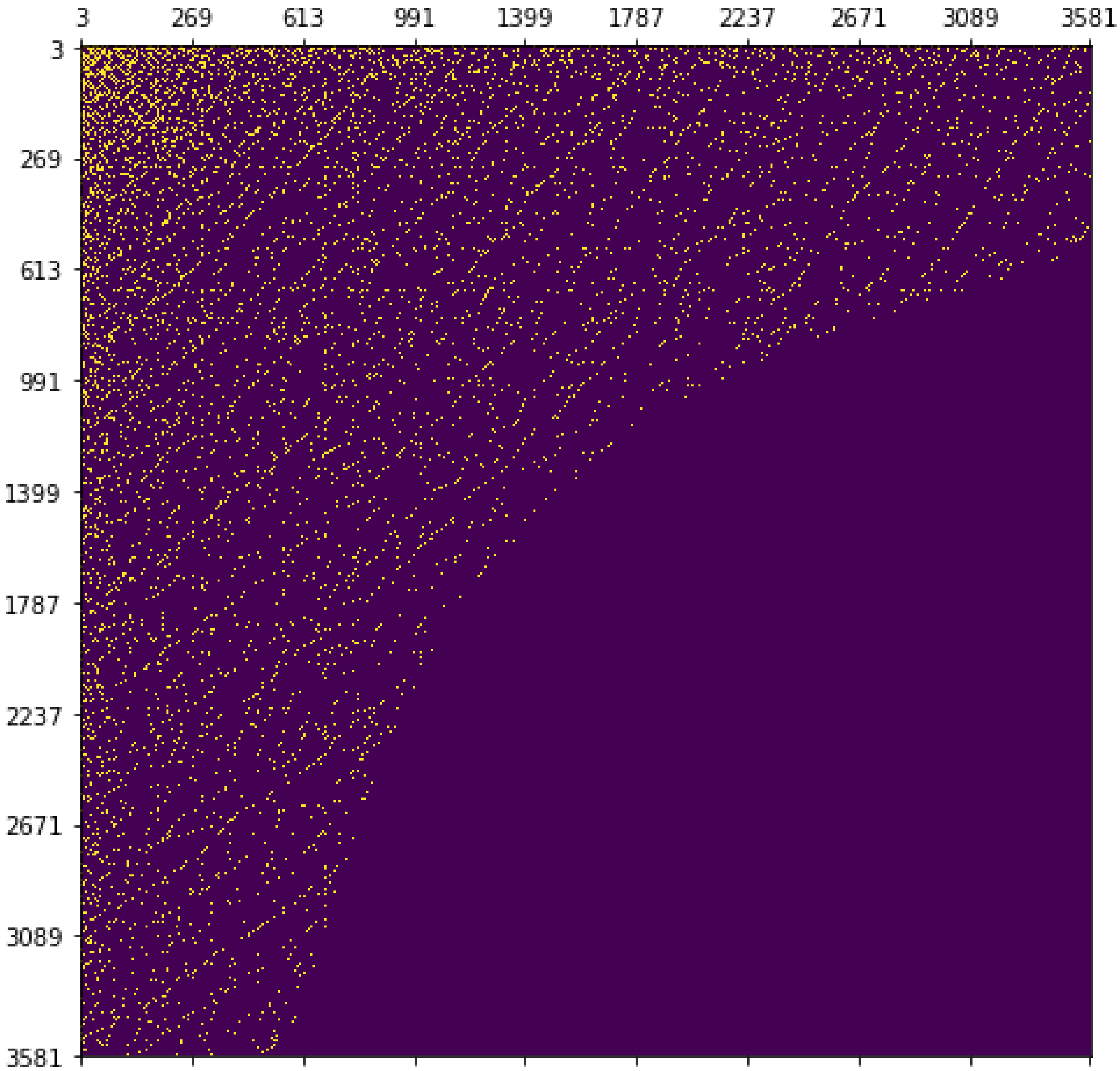

FIGURE 6. Only Case 4 curves up to $p, q \leq 3581$

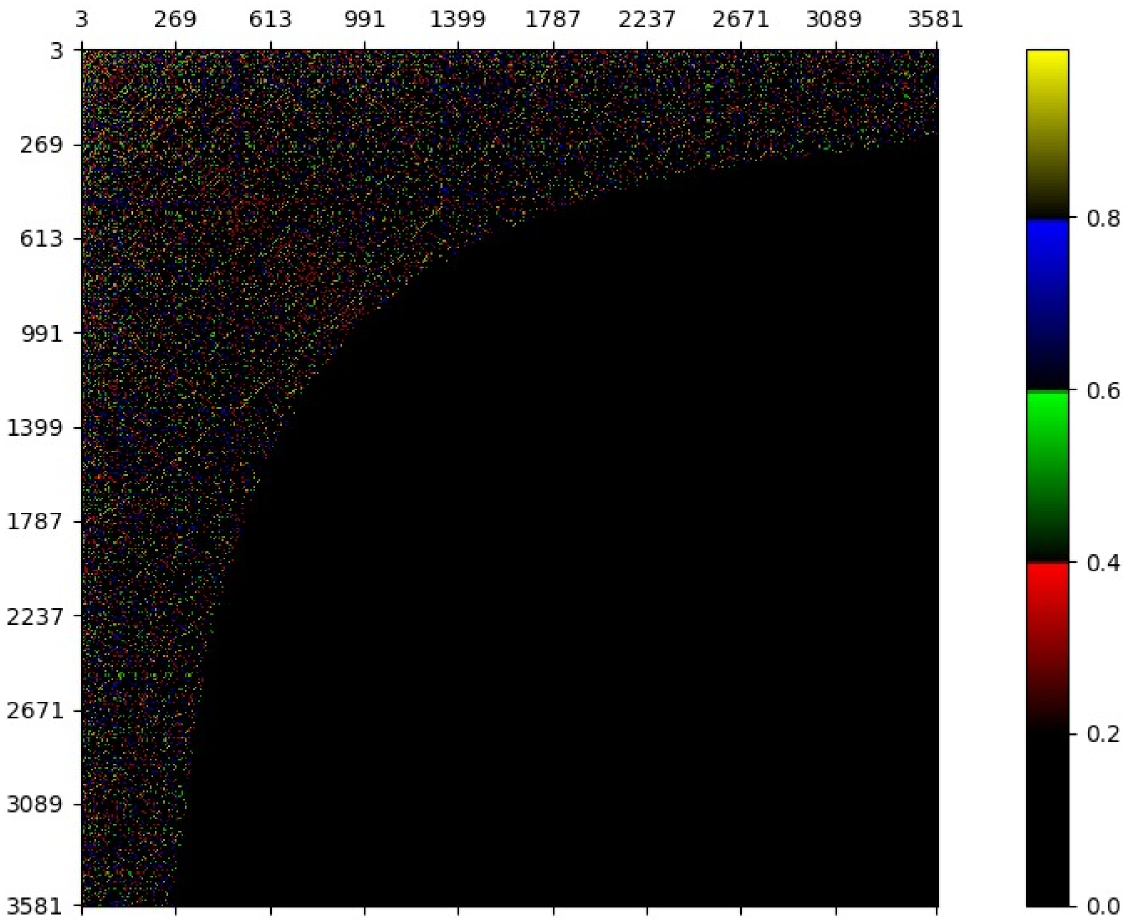

Figure 7. Case 1,2,3,4 curves up to $p, q \leq 3581$

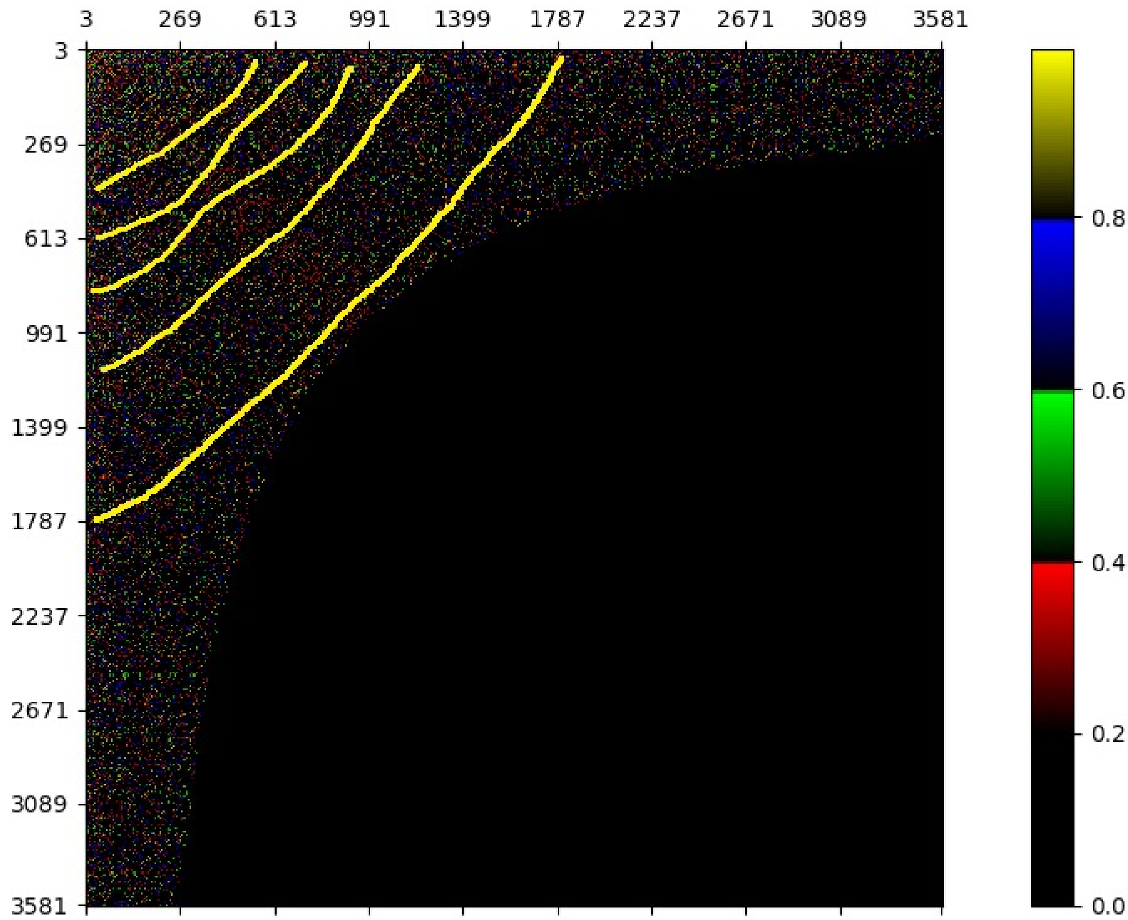

FIGURE 8. Case 1,2,3,4 curves up to $p, q \leq 3581$ – highlighting the circle pattern

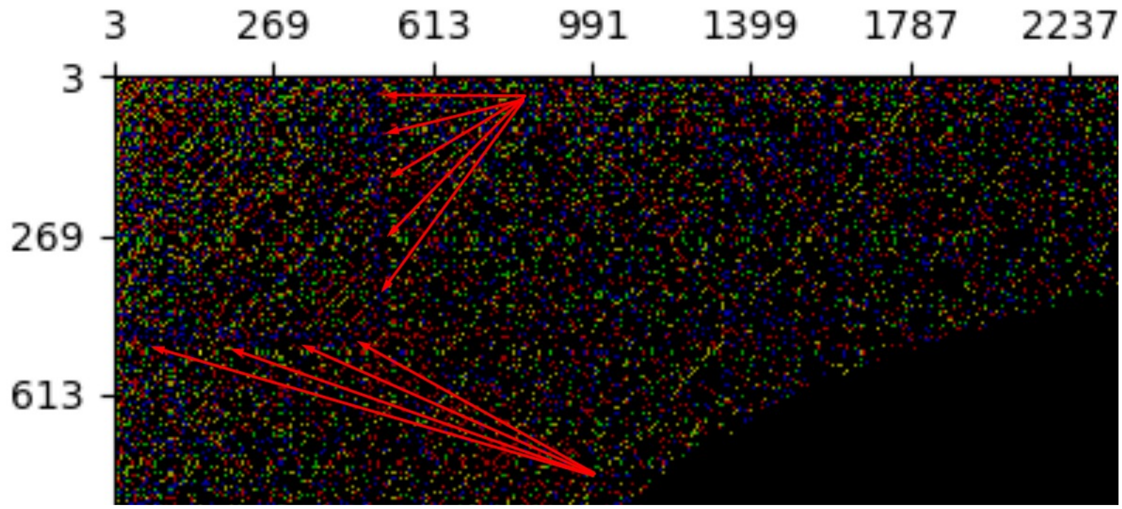

FIGURE 9. Case 1,2,3,4 curves up to $p, q \leq 3581$ – highlighting the squares pattern

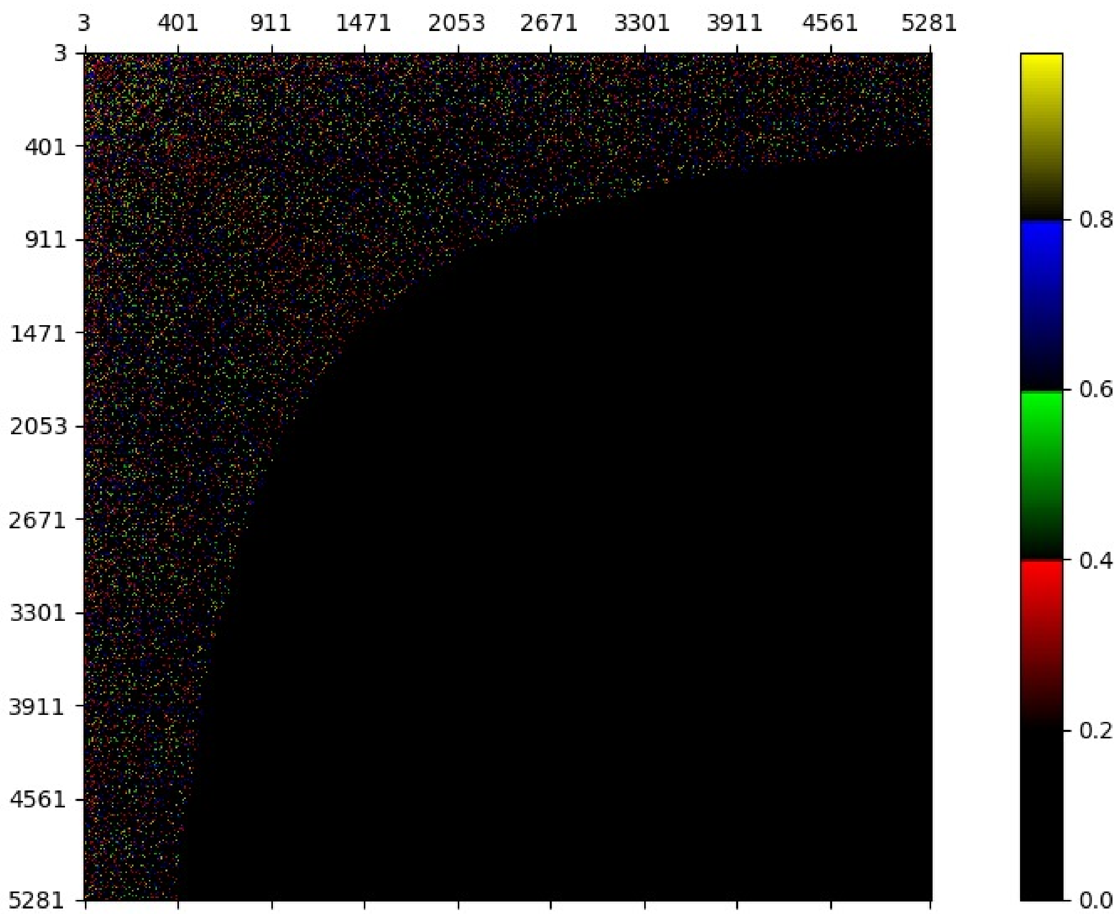

FIGURE 10. Case 1,2,3,4 curves up to $p, q \leq 5281$

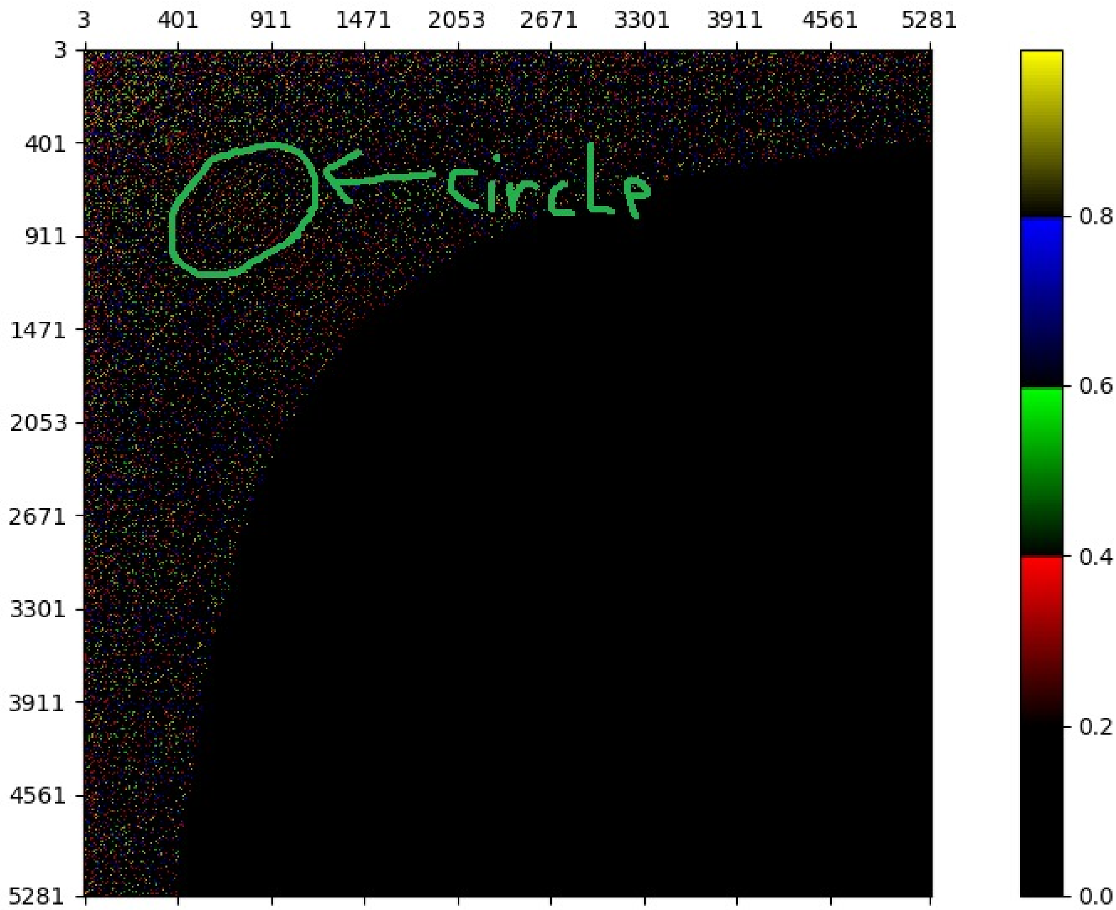

FIGURE 11. Case 1,2,3,4 curves up to $p, q \leq 5281$ – highlighting the circle pattern

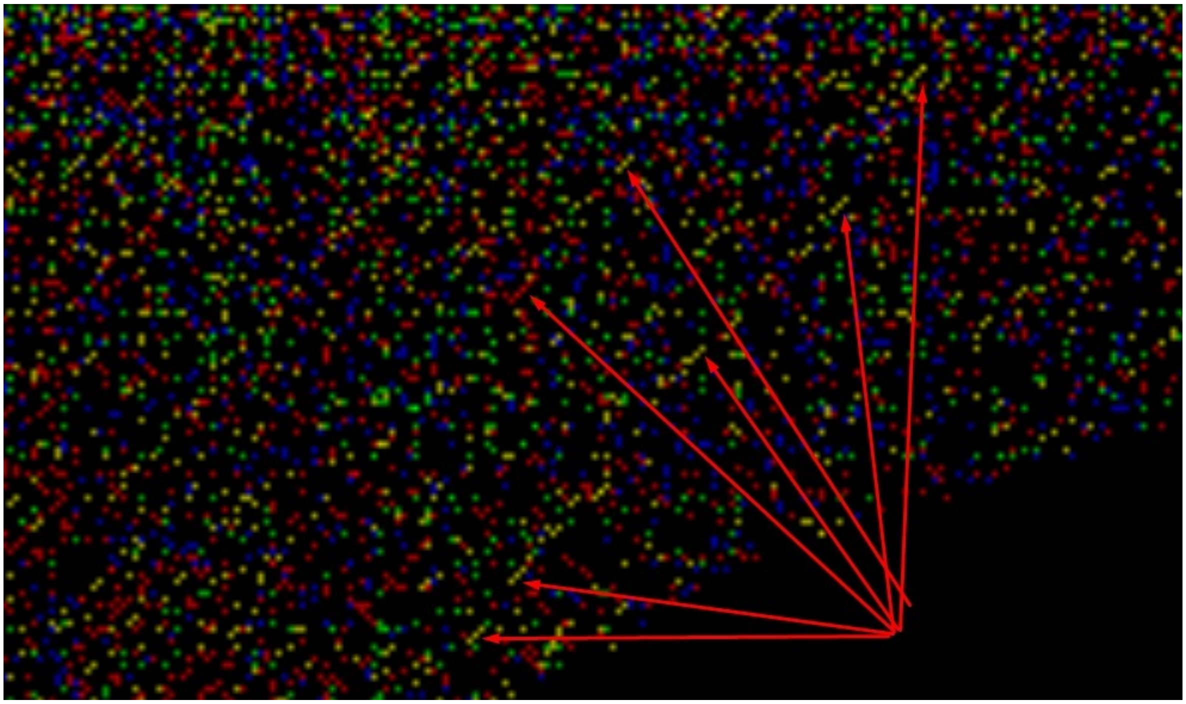

Figure 12. Case 1,2,3,4 curves – highlighting triple pattern

6. What is the torsion subgroup of these elliptic curves?

Recall, if for an element of a group $a \in G$ exists an integer $m > 0$ with $a^m = e$ (e denoting the identity element of G), then the smallest such m is the *order* of a, written $m = \mathrm{ord}(a)$ [9, p. 35], [10, p. 50], [11, p. 240]. If no such m exists, we formally write $\mathrm{ord}(a) = \infty$. In an abelian group, the set of elements of finite order form a subgroup, called the *torsion subgroup* [12, p. 36]. Let $m \geq 1$ be an integer. The set of points of E having an order m is the *m-torsion subgroup* of E, denoted by $E[m]$, see [13, p. 69].

Looks like all these elliptic curves have torsion subgroup being $\mathbb{Z}/2\mathbb{Z}$. To be verify with the Nagekk-Lutz theorem. Also, SAGE computes automatically the torsion subgroup of any curve and the order of the group. This means that all point have infinite order except 1 point with y-coordinate equal to 0. Suspect that this point is the point at infinity. This means that all other points have infinite order. Also, this means that for any of the curves, once there is a non-trivial rational point on them, there must be infinitely many necessarily. The Neron-Tate pairing and canonical heights gives us a way to construct elliptic curves with rank of at least r where r is the number of linearly independent rational points. What is the rank of the curves we found in each example ? There is a known upper bound that can be computed using the discriminant. How big can we go in rank in each of these cases ? What are the obstructions we encounter ?

Remark. *Note that all cases can be reduced to studying a system of equation given by the Chinese remainder theorem.*

Remark. *Take a look at this paper : https://arxiv.org/pdf/2103.08947.pdf*

7. 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.

Interesting directions are:

- fixing a line and search for a family of curves where pq is a congruent number. Plot the (p, q) pairs and explore a structure
- fixing a curve and search for a family of lines that intersect this curve in rational points

8. Acknowledgements

We are grateful for the kind assistance and useful input from mathematics communities like the Stack Exchange Network or the MatheBoard Community. As an example let us mention Servaes and HAL 9000, for whose instant help in matters of number theory we are very grateful as for the help by many other pleasant people from the math communities.

Appendix A. Reasons for the condition's unsatisfiability

In the following we provide (numbered) reasons for the unsatisfiability of conditions in Table 1 and Table 2:

a) Cases 1, 2, 3 in Table 1 and cases 7, 23, 24 in Table 2 can never occur. The conditions given by these cases are unsatisfiable, because the fact that pq is an integer requires the fraction's nominator to be larger than the denominator.

b) These cases require b to be even and as a consequence a to be odd (since $a \in \mathbb{Z}$, $b \in \mathbb{N}$ and the fraction a/b is reduced). Let us take for example case 4 in Table 1 with the equation $4pq = 2a^2 + b^4$ that leads to $2pq = a^2 + b^4/2$ when dividing it by 2 and thus to the contradictory requirement a is even. Another example is case 27 in Table 1 with $pqb^3 = 2a^2 + 4b$. Also here b must be even and therefore a odd. But $pqb^3/2 = a^2 + 2b$ requires a must be even.

c) Case 7 in Table 1 is unsolvable. We know that b must be even and by substituting b with $2t$ we have to solve $16t^3pq = a^2 + t$ which is $(16t^2pq - 1)t = a^2$. Since t is coprime with $16t^2pq - 1$, we conclude that $16t^2pq - 1$ is a perfect square, which is impossible by an argument mod4. Recall that if x is a perfect square then $x \equiv 0 \bmod 4$ or $x \equiv 1 \bmod 4$ [6, p. 21].

d) Case 8 in Table 1 (which is identical to case 1 in Table 2) cannot occur because the equation $4pqb^4 = 2a^2 + 1$ has no solution. The reason for this is that on the left side of the equation is an even number and on the right side is an odd number.

e) Cases 9, 10 in Table 1 are unsatisfiable due to the assumed inequality $q > p$

f) Case 15 in Tables 1 and 2 is unsatisfiable, since it would require q to be even.

g) Case 9, 16, 30 in both Tables 1 and 2 are unsatisfiable, since p and q are odd primes and the difference or sum of two even integers cannot be odd.

h) Case 22 in Tables 1 and 2 is unsatisfiable, since it would require p to be even.

i) Case 25 in Table 2 is unsatisfiable, because it requires $b = 1$ leading to the equation $pq = 1 - a^2$ which has no solution.

Appendix B. Reasons for the condition's redundancy

B.1. **Table 1, Case 14: $p = 2a^2+qb/4b^3$.** We can rewrite this condition as $q = 4b^2p - a^2 \cdot 2/b$. There are only two possible solutions $b = 1$ and $b = 2$. Setting $b = 1$ leads to $q = 4p - 2a^2$ which is a special case of case 16 in Table 2 and impossible to occur by reason g (Appendix A). Setting $b = 2$ leads to $q = 2^4p - a^2$ which is a special case of case 17 in Table 2.

B.2. **Tables 1 & 2, Case 21: $q = pb\pm 2a^2/4b^3$.** We can rewrite condition of case 21 in Table 1 as $p = 4b^2q - a^2 \cdot 2/b$. There are only two possible solutions $b = 1$ and $b = 2$.

Setting $b = 1$ leads to $p = 4q - 2a^2$ which is a special sub case of case 9 in Table 2. Setting $b = 2$ leads to $p = 2^4 q - a^2$ which is a special sub case of case 10 in Table 2.

Analoguously, we can rewrite condition of case 21 in Table 2 as $p = 4b^2 q + a^2 \cdot {}^2/_b$. There are only two possible solutions $b = 1$ and $b = 2$. Setting $b = 1$ leads to $p = 4q + 2a^2$ which is a special sub case of case 9 in Table 1. Setting $b = 2$ leads to $p = 2^4 q + a^2$ which is a special sub case of case 10 in Table 1. Both cases are impossible to occur by reason e (Appendix A).

B.3. **Table 1, Case 23: $pq = {}^{a^2+b}/_{b^3}$.** It must b be odd and a must be even. Only solutions for $b = 1$ exist, since the right-hand side of ${}^{a^2}/_b = pqb^2 - 1$ is an integer and the left-hand side is a fraction unless b is 1. Setting $b = 1$ boils the condition down to $pq = a^2 + 1$ which is a special sub case of case 26.

B.4. **Table 1, Case 24: $pq = {}^{a^2+b^2}/_{b^2}$.** Also here no solution exist for $b > 1$. The product $pq = ({}^a/_b)^2 + 1$ can only be an integer when $b = 1$ because the fraction ${}^a/_b$ is reduced (by assumption a and b are coprime). For this reason, case 24 is the same special case of case 26, just as case 23 does.

B.5. **Table 1, Case 25: $pq = {}^{a^2+b^3}/_b$.** This case is identical with cases 23 and 24, since it provides only solutions for $b = 1$ as well. The reason for this is analogous to both previous cases. Here ${}^{a^2}/_b$ is a fraction unless $b = 1$. For this reason, case 25 is the same special case of case 26, just as case 23 does.

B.6. **Tables 1 & 2, Case 29: $pq = {}^{4b^3 \pm 2a^2}/_b$.** In this case we get solutions if b divides $2a^2$. Therefore only solutions exist if $b = 2$, as per assumption a and b are coprime. In Table 1, setting $b = 2$ boils the condition down to $pq = a^2 + 2^4$ which is a special sub case of case 26. In Table 2, setting $b = 2$ boils the condition down to $pq = 2^4 - a^2$ which is a special sub case of case 26 too.

B.7. **Table 2, Case 14: $p = {}^{qb-2a^2}/_{4b^3}$.** We can rewrite this condition as $q = 4b^2 p + a^2 \cdot {}^2/_b$. There are only two possible solutions $b = 1$ and $b = 2$. Setting $b = 1$ leads to $q = 4p + 2a^2$ which is a special case of case 16 in Table 1 and impossible to occur by reason g (Appendix A). Setting $b = 2$ leads to $q = 2^4 p + a^2$ which is a special case of case 17 in Table 1.

References

[1] LMFDB The L-functions and Modular Forms Database. Elliptic curve with lmfdb label 14112.r1 (cremona label 14112bk1). https://www.lmfdb.org/EllipticCurve/Q/14112/r/1, 2021.

[2] 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.

[3] O. Bordellès. *Arithmetic Tales. Advanced Edition*. Springer, 2020.

[4] J. Friedlander and H. Iwaniec. Using a parity-sensitive sieve to count prime values of a polynomial. *Proc. Natl. Acad. Sci. USA*, 94(4):1054–1058, 1997.

[5] LMFDB The L-functions and Modular Forms Database. Elliptic curve with lmfdb label 135200.bq1 (cremona label 135200o1). https://www.lmfdb.org/EllipticCurve/Q/135200/bq/1, 2021.

[6] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK*. Springer, 5 edition, 2014.

[7] D. A. Cox. *Primes of the Form* $x^2 + ny^2$. Wiley, 2 edition, 2013.

[8] LMFDB The L-functions and Modular Forms Database. Elliptic curve with lmfdb label 152352.ba1 (cremona label 152352y1). https://www.lmfdb.org/EllipticCurve/Q/152352/ba/1, 2021.

[9] J. Wolfart. *Einführung in die Zahlentheorie und Algebra*. Vieweg+Teubner, Wiesbaden, Germany, 2 edition, 2011.

[10] O. Forster. *Algorithmische Zahlentheorie*. Springer Spektrum, Wiesbaden, Germany, 2 edition, 2015.

[11] F. Modler and M. Kreh. *Tutorium Analysis 2 und Lineare Algebra 2*. Spektrum Akademischer Verlag, Heidelberg, Germany, 2 edition, 2012.

[12] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*, volume 97 of *Graduate Texts in Mathematics*. Springer, 2 edition, 1993.

[13] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2 edition, 2009.

[14] D. G. Northcott. *Ideal Theory*, volume 42 of *Cambridge Tracts in Mathematics and Mathematical Physics*. Cambridge University Press, Cambridge, United Kingdom, 1953.

[15] S. Shahriari. *Algebra in Action: A Course in Groups, Rings, and Fields*, volume 27 of *Pure and applied undergraduate texts*. American Mathematical Society, 2017.

[16] J. B. Fraleigh. *A First Course in Abstract Algebra*. Pearson, Harlow, United Kingdom, 7 edition, 2014.

[17] A. R. Tarrida. *Affine Maps, Euclidean Motions and Quadrics*. Springer Undergraduate Mathematics Series. Springer, 2011.

[18] J. Hilgert. *Arbeitsbuch Mathematik für das erste Studienjahr: Beweise und Lösungen zum Lesebuch*. Springer Spektrum, 2013.

[19] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and its Applications. CRC Press, 2 edition, 2008.

Fundamentals short and sweet

unit	An element a of a ring R is called a "unit" (an invertible element) if there exist an element b such that $ab = 1$ [14, p. 24]. Units are elements with inverses with respect to multiplication in the ring. Let F be a field, then an element a of F is a non-unit iff $a = 0$. The sum of any two non-units in F is again a non-unit in F.
unitary ring	A unitary ring is a ring with a multiplicative identity 1 (which differs from the additive identity $1 \neq 0$) such that $1a = a = a1$ for all elements a of the ring.
Ideal	Let $(R, +, \cdot)$ be a commutative unitary ring. Then the subset $I \subseteq R$ is called an ideal of R if $(I, +)$ is a commutative group and if $xI \subseteq I$ for all $x \in R$, see [9, p. 66-67]. As the property that makes up an ideal, one can imagine a kind of magnetism with which an element from the ideal pulls elements to itself by multiplying it with elements lying outside the ideal. The terms left ideal and right ideal [15, p. 330–331] generalize the ideal concept to noncommutative rings.
Proper Ideal	An ideal of a ring R is called "proper" when it is not entirely R, but a proper subset of R.
max. ideal	A proper Ideal M of a ring R is called "maximal ideal" of R if there is no other proper ideal N of R properly containing M [16, p. 247], [14, p. 37]. A Note on "proper containment": If R is any set, then R is the improper subset of R. Any other subset $N \neq R$ is a proper subset of R and denoted by $N \subset R$ or $N \subsetneq R$ [16, p. 2].
prime ideal	Let a and b are two elements of R and P a proper ideal such that their product ab is an element of P. P is called a prime ideal if at least one of a and b belongs to P, in other words from $ab \in P$ and $a \notin P$ always follows $b \in P$ [14, p. 9].
max. prime ideal	A proper prime ideal P is said to be a "maximal prime ideal" of the ring R, if there is no other proper prime ideal containing P [14, p. 23].
Algebraic closure $\bar{K}$ of a field K	Starting with a field K, we can find a field $\bar{K}$, called the algebraic closure of K, which contains the roots of all polynomials over K. In other words, in $\bar{K}$ every polynomial in the polynomial ring $K[x]$ over K splits, see [15, p. 503].

Group of units $K^\times$ of a field K	Let K be a field. The group of units of K, denoted by $K^\times$ or sometimes by K^* contains only the elements from K that are invertible with respect to multiplication – the units of K. It is the set $K \setminus \{0\}$.
Affine space $\mathbb{A}$ over a field K	Let K be a field. An affine space over K is a triple $(\mathbb{A}, V, +)$ of a non-empty point set $\mathbb{A}$, a K-vector space V (which is said to be associated to $\mathbb{A}$) and an action $+ : \mathbb{A} \times V \to \mathbb{A}$ of the additive group $(V, +, 0)$ with $(a, v) \mapsto a + v$ such that [17, p. 2]: (1) $a+0 = a$ for all $a \in \mathbb{A}$, where 0 is the identity element (zero vector) of V (2) $a + (v + w) = (a + v) + w$ for all $a \in \mathbb{A}$ and $v, w \in V$ (3) given $a, b \in \mathbb{A}$, there exists a unique $v \in V$ such that $a + v = b$ The dimension of $\mathbb{A}$ equals to the dimension of its associated vector space. Often one speaks of an affine space $\mathbb{A}$ referring to the whole construct and not only to the set $\mathbb{A}$ [17, p. 4]. In contrast to the vector space, no scalar multiplication and no addition of points is included in the definition of an affine space. We "borrow" the vectors from V to translate our points in $\mathbb{A}$. An affine space has no distinguished point serving as an origin.
Projective n-space $\mathbb{P}^n$ over a field K	Let $\mathbb{A}^{n+1}$ be an affine $(n+1)$-space over K and $\sim$ an equivalence relation on $\mathbb{A}^{n+1}$ with $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ if there exists a $\lambda \in \bar{K}^\times$ such that $x_i = \lambda y_i$ for all i. The projective n-space over K is the quotient set $\mathbb{P}^n = \mathbb{A}^{n+1}/\sim$, that is the partition (the set of all equivalence classes) of $\mathbb{A}^{n+1}$ created by $\sim$, see [13, p. 6]. The equivalence class of a tuple $(x_0, \ldots, x_n)$ only depends on the ratios of x_0 to x_1 to x_2 to $\ldots$ and so forth. Therefore, the equivalence is denoted by $[x_0 : \ldots : x_n]$. We can see a projective n-space as a set of lines in $\mathbb{A}^{n+1}$. In a more general fashion we can use a topological space $M = K^{n+1} \setminus \{0\}$ instead of $\mathbb{A}^{n+1}$, see [18, p. 157].
Elliptic curve E over a field K	An elliptic curve E is the graph of an equation of the form (the so called generalized Weierstrass equation) $y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, see [19, p. 9-10]. Its coefficients lie in the field K: $a_i \in K$ $(i = 1, 2, 3, 4, 6)$, see [19, p. 9], [13, p. 42]. E is a projective variety defined over K.
L-rational points	Let E be an elliptic curve over a field K. It's L-rational points for any $L \supseteq K$ is a set of points in $\mathbb{P}^2(L)$ and defined as $E(L) = \{O\} \cup \{(x, y) \in L^2 : y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\}$, [19, p. 9]. This point set forms an abelian group [19, p. 16], [13, p. 41,52], [12]. The point O at infinity acts as the identity element.

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

Madjid G. Tehrani, George Washington University, Science & Engineering Hall, 800 22nd St NW, Washington, DC 20052, USA
Email address: Madjid_tehrani@gwu.edu

Bill Buchannan, Edinburgh Napier University, EH11 4BN, Edinburgh, UK
Email address: w.buchanan@napier.ac.uk