Torsion subgroups of elliptic curves over cubic number fields

BARCELONA, DECEMBER 5-7, 2019

Antonela Trbović
University of Zagreb, Department of Mathematics
antonela.trbovic@math.hr

Abstract

We present some conjectures about splitting of primes in cubic extensions of $\mathbb{Q}$ over which certain torsion subgroups appear. We were able to say something about primes in cubic extensions with the following torsion subgroups: $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z}$, for $n = 13, 14, 16, 18, 20$.

Introduction

For an elliptic curve E defined over a number field K, let $E(K)$ be the set of all $K-$rational points on E. By the Mordell-Weil theorem and the structure theorem for finitely generated abelian groups, we know that

$$E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r,$$

where r is a non-negative integer and $E(K)_{tors}$ is the torsion subgroup.

In the case of $K = \mathbb{Q}$, from Mazur's Theorem [7] we know all the possible torsion subgroups over K. There is a similar result by Kamienny, Kenku and Momose [5, 6], concerning possible torsion subgroups of elliptic curves defined over quadratic fields. As for the cubic fields, we have the following result by M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, D. Zureick-Brown:

Theorem 1. *If $K/\mathbb{Q}$ is a cubic field extension and E/K an elliptic curve, then $E(K)_{tors}$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z}, \text{ for } n = 1, ..., 16, 18, 20, 21,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \text{ for } n = 1, ..., 7.$$

All these groups except $\mathbb{Z}/21\mathbb{Z}$ occur for infinitely many non isomorphic elliptic curves.

Main Objectives

Let p be a prime number in $\mathbb{Q}$ and let K be a cubic extension of $\mathbb{Q}$. Then

$$p\mathcal{O}_K = \prod_{i=1}^{n} P_i^j, n, j \in \{1, 2, 3\}, \tag{1}$$

where P_i are primes in $\mathcal{O}_K$.

Let G be a fixed group from Theorem 1, i.e. a possible torsion subgroup of an elliptic curve defined over a cubic field K. Let's say we have a family of all cubic fields K over which group G can appear as a torsion subgroup.

First, we want to be able to say something about factorization (1) in such K of small prime numbers, i.e. if we have a field K over which G appears, what can we say about splitting of 2, 3, 5,... in such extensions.

Moreover, we want to examine whether we can conclude something about splitting of all prime numbers in the family of extensions K.

Example: $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$

Let K be a cubic number field for which it exists an elliptic curve over K with the torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. In [4] we can find the following theorem:

Theorem 2 (Jeon, Kim, Lee)**.** *Choose $t \in \mathbb{Q}$ such that the polynomial*

$$f(x) = (t^2-1)x^3 + (t^3+2t^2-9t-2)x^2 - 9(t^2-1)x - t^3 - 2t^2 + 9t + 2 \tag{2}$$

is irreducible over $\mathbb{Q}$. Let α_t be a zero of $f(x)$. Let E be an elliptic curve defined by the equation

$$y^2 + (1-c)xy - by = x^3 - bx^2, \tag{3}$$

where b is given by

$b = (5 + 13\alpha_t - \alpha_t^3 + 16t - 12\alpha_t^2 t + 5\alpha_t^2 t^2 + \alpha_t^3 t^2 - 4\alpha_t t - 13\alpha_t t^2 - \alpha_t^2 - 9t^2 - 4t^3 + 4\alpha_t t^3)(-3 - t - \alpha_t + \alpha_t t)^2(-5 - 12\alpha_t + 4\alpha_t^3 - 25t + \alpha_t^4 + 26\alpha_t^2 t + 26\alpha_t^2 t^2 + 8\alpha_t^3 t - 12\alpha_t^3 t^2 - 24\alpha_t t + 28\alpha_t t^2 - \alpha_t^4 t^2 - \alpha_t^4 t - 4\alpha_t^2 - 25t^2 + 17t^3 + 6t^4 + 16\alpha_t t^3 - 8t^4\alpha_t - 18t^3\alpha_t^2 + 2\alpha_t^2 t^4 + \alpha_t^4 t^3)(-5t^4 + 7t^4\alpha_t - 3\alpha_t^2 t^4 + \alpha_t^3 t^4 + 6t^3\alpha_t^2 - 4\alpha_t t^3 - 4\alpha_t^3 t^3 - 15t^3 + \alpha_t^4 t^3 + 3t^2 + 8\alpha_t^2 t^2 + 10\alpha_t t^2 - 3\alpha_t^4 t^2 - 2\alpha_t^3 t^2 + 10\alpha_t^2 t - 36\alpha_t t + 3\alpha_t^4 t + 12\alpha_t^3 t - 37t - 10 - 7\alpha_t^3 - \alpha_t^4 - 21\alpha_t^2 - 41\alpha_t)/(1 + 8\alpha_t + 4\alpha_t^3 - 5t + \alpha_t^4 + 6\alpha_t^2 t + 30\alpha_t^2 t^2 + 4\alpha_t^3 t - 4\alpha_t^3 t^2 - 20\alpha_t t - 4\alpha_t t^2 - \alpha_t^4 t^2 - \alpha_t^4 t + 2\alpha_t^2 - 37t^2 + 5t^3 + 4t^4 + 20\alpha_t t^3 - 4t^4\alpha_t - 6t^3\alpha_t^2 - 4\alpha_t^3 t^3 + \alpha_t^4 t^3)^2(-1 - 4t - t^2 - 3\alpha_t - 2\alpha_t t + \alpha_t t^2 + 2\alpha_t^2 t)(t - 5 - \alpha_t + \alpha_t t)^3$

and c is given by

$c = (5 + 12\alpha_t - 4\alpha_t^3 + 25t - \alpha_t^4 - 26\alpha_t^2 t - 26\alpha_t^2 t^2 - 8\alpha_t^3 t + 12\alpha_t^3 t^2 + 24\alpha_t t - 28\alpha_t t^2 + \alpha_t^4 t^2 + \alpha_t^4 t + 4\alpha_t^2 + 25\alpha_t^2 - 17t^3 - 6t^4 - 16\alpha_t t^3 + 8t^4\alpha_t + 18t^3\alpha_t^2 - 2\alpha_t^2 t^4 - \alpha_t^4 t^3)(-3 - t - \alpha_t + \alpha_t t)^2(5 + 13\alpha_t - \alpha_t^3 + 16t - 12\alpha_t^2 t + 5\alpha_t^2 t^2 + \alpha_t^3 t^2 - 4\alpha_t t - 13\alpha_t t^2 - \alpha_t^2 - 9t^2 - 4t^3 + 4\alpha_t t^3)/(1 + 8\alpha_t + 4\alpha_t^3 - 5t + \alpha_t^4 + 6\alpha_t^2 t + 30\alpha_t^2 t^2 + 4\alpha_t^3 t - 4\alpha_t^3 t^2 - 20\alpha_t t - 4\alpha_t t^2 - \alpha_t^4 t^2 - \alpha_t^4 t + 2\alpha_t^2 - 37t^2 + 5t^3 + 4t^4 + 20\alpha_t t^3 - 4t^4\alpha_t - 6t^3\alpha_t^2 - 4\alpha_t^3 t^3 + \alpha_t^4 t^3)(3t - 3t^2 - t^3 - \alpha_t t - 3\alpha_t t^2 + \alpha_t t^3 + 2\alpha_t^2 t^2 + 1 + 3\alpha_t - 2\alpha_t^2 t)(t - 5 - \alpha_t + \alpha_t t)^2$.

Then the torsion subgroup of E over a cubic number field $\mathbb{Q}(\alpha_t)$ is equal to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ for almost all t.

This theorem gives us a family of cubic fields over which the torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ appears, together with an elliptic curve with that torsion subgroup. This family does not contain every cubic field with such property, but we use it to form conjectures which we later prove for all cubic fields. Although, in [3] we can find families of all cubic fields with similar property for the groups $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/20\mathbb{Z}$.

Using the polynomial (2) for different values of t, we can generate in MAGMA [1] entire families of cubic number fields K and elliptic curves E/K with the torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. We can also check how small primes split in those extensions.

Conjectures

From [2, Theorem 1.2] we know that if there exists an elliptic curve over a cubic field K with a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, then K is normal over $\mathbb{Q}$, which means that K is Galois over $\mathbb{Q}$. Then in 1 we have only 3 possibilities for the splitting of primes, as shown in Table 1.

$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$	2	3	5	7	11	13
P_1	×	✓	✓	✓	✓	✓
P_1^3	×	×	×	×	×	×
$P_1 \cdot P_2 \cdot P_3$	✓	✓	✓	✓	✓	✓

Table 1: Splitting of small primes in fields with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$

In MAGMA, for a large family of $t \in \mathbb{Q}$ we generate polynomials as in (2) and for such polynomials that are irreducible we generate cubic fields associated to them. Now, for a prime number p, we can check what are the possibilities for splitting in all those extensions. We did such a thing for small primes up to 13, and the outcome is presented in Table 1.

In a similar manner, by examining large families of prime numbers (up to a certain bound, which was here 1000000) in MAGMA, we can conjecture the following:

$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$
· if p ramifies, then $p \equiv 1 \pmod 3$
· there are no primes $p \neq 2$ that split everywhere
· there are no primes that remain prime everywhere

Table 2: Conjectures

How to prove this?

We will now describe a method for proving conjectures from Table 1.

Suppose that 3 ramifies (which we conjectured does not). The idea is to go through each type of possible reduction (good, additive, multiplicative) and prove that it cannot happen.

First, if we assume that 3 has good reduction, then $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ (as prime to 3 torsion) into $E(\mathcal{O}_K/P)$, where P is a prime lying over 3.

Since we said that 3 ramifies, we have

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \hookrightarrow E(\mathbb{F}_3).$$

By the Hasse-Weil bound we have $|\#E(\mathbb{F}_3) - (3+1)| \leq 2\sqrt{3}$, so

$$\#E(\mathbb{F}_3) \leq 7.5 < 28,$$

so good reduction cannot happen.

For the other two types of reduction things get more complicated. For example, with additive reduction we have that $E_0(K)[n]$ injects mod p to $E_{ns}(K) \cong \mathbb{F}_3$. With this we can determine the upper bound for the number of elements in $E_0(K)[n]$ and with that the upper bound on the number of elements in $E(K)$, since we know that $|E(K)/E_0(K)|$, the Tamagawa number, is less than 4.

Forthcoming Research

It is possible to consider the splitting of primes over quartic number fields, or number fields of higher degrees, as long as it is not too difficult to get equations as in [4]. We could also look at some other properties of number fields over which certain torsion subgroups appear, or properties of elliptic curves with those torsion subgroups, using (3) for example.

References

[1] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system. i. the user language. *J. Symbolic Comput.*, 24:235–265, 1997.

[2] P. Bruin and F. Najman. Fields of definition of elliptic curves with prescribed torsion. *Acta Arith.*, 181:85–96, 2017.

[3] M. Derickx and F. Najman. Torsion of elliptic curves over cyclic cubic fields. *Math. Comp.*, 88:2443–2459, 2019.

[4] D. Jeon, H. Kim, and Y. Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Mathematics of Computation*, 80(273):579–591, January 2011.

[5] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109:221–229, 1992.

[6] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–148, 1988.

[7] B. Mazur. Modular curves and the eisenstein ideal. *Inst. Hautes Etudes Sci. Publ. Math.*, 47:33–186, 1978.

Acknowledgements

The author was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004).