Torsion points on elliptic curves over number fields of small degree

Derickx, M.

Torsion points on elliptic curves over number fields of small degree

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 21 september 2016
klokke 11:15 uur

door

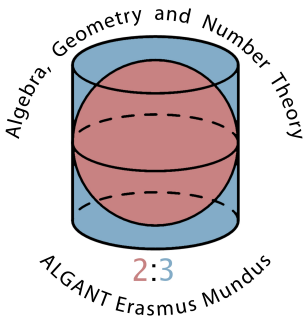
Maarten Derickx
geboren te Voorst, Nederland,
in 1986

Promotor: Prof. dr. Sebastian J. Edixhoven
Copromotor: Prof. dr. Lambertus van Geemen (Università d.s. di Milano)
Copromotor: dr. Pierre Parent (Université de Bordeaux)

Samenstelling van de promotiecommissie:

Prof. dr. Adrianus W. van der Vaart
Prof. dr. Samir Siksek (Warwick University)
Prof. dr. Loic Merel (Universite Paris Diderot)
dr. Marusia Rebolledo (Universite Blaise Pascal Clermont-Ferrand)
Prof. dr. Bart de Smit
dr. Peter Bruin

This work was funded by Algant-Doc Erasmus-Mundus and was carried out at Universiteit Leiden, Université de Bordeaux and Università degli studi di Milano



université de BORDEAUX

Contents

Preface

The main subject of this thesis is the study of torsion points on elliptic curves over number fields. This is a subject of study that goes as far back as 1906, where it starts with the work of Beppo Levi who studied torsion points on elliptic curves over $\mathbb{Q}$. He showed that for each of the groups

$$\mathbb{Z}/N\mathbb{Z} \quad \text{for } N = 1, 2, \ldots, 10, \text{ or } 12 \tag{1}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad \text{for } N = 1, 2, 3, \text{ or } 4 \tag{2}$$

over $\mathbb{Q}$ there are infinitely many non isomorphic elliptic curves whose torsion subgroup is isomorphic to that group. In addition he also showed that the group structures $\mathbb{Z}/N\mathbb{Z}$ for $N = 14, 16, 20$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $N = 10, 12$ do not occur as the torsion group of an elliptic curve over $\mathbb{Q}$. Bepo Levi shared his ideas on what would happen for larger values of N on the 1908 International Mathematical conference in Rome. He believed that the groups in (1) and (2), with the possible addition of $\mathbb{Z}/24\mathbb{Z}$, are the only groups that can occur as the torsion subgroup of an elliptic curve over $\mathbb{Q}$. However this conjecture seems to have been forgotten and it has been restated by Trygve Nagell in 1952 and by Andrew Ogg in 1970. As a result the conjecture that the groups in the lists (1) and (2) are the only groups that can occur as a torsion group of an elliptic curve over $\mathbb{Q}$ came to be known as Ogg's conjecture. This conjecture was later proven by Barry Mazur in his breaktrough paper[1]. A very nice exposition of the above history of the study of torsion points on elliptic curves over $\mathbb{Q}$, can be found in article [7] on Beppo Levi's life and mathematical work.

After Mazur's proof of Beppo Levi's conjecture which was later restated by Nagell and Ogg, the study moved to torsion points on elliptic curves over number fields other than $\mathbb{Q}$. Sheldon Kamienny generalized the techniques of Mazur to number fields of higher degree[2] and together with Mazur he determined all group structures that can occur as the torsion subgroup of an elliptic curve over a quadratic field[3], and

[1] B. Mazur. "Modular curves and the Eisenstein ideal". In: *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186 (1978).

[2] S. Kamienny. "Torsion points on elliptic curves over fields of higher degree". In: *Internat. Math. Res. Notices* 6 (1992), pp. 129–133.

[3] S. Kamienny and B. Mazur. "Rational torsion of prime order in elliptic curves over number fields". In: *Astérisque* 228 (1995). With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992), pp. 3, 81–100.

the list of all such groups turned out to be finite again. This phenomenon continues to hold in higher degrees. In fact, building on the ideas of Mazur an Kamienny, Loïc Merel proved that if $d > 0$ is an integer then the list of groups that occur as the torsion group of an elliptic curve over a number field of degree d is finite[4]. Degrees 1 and 2 are the only degrees for which this finite list is known, although the list of primes that can divide the order of the torsion group is also known for degree 3 by work of Parent[5][6].

This thesis contains several new results considering which group structures can occur as the torsion subgroup of an elliptic curve over a number field of small degree. This thesis consist of four chapters, the first of which is introductory and contains no new results. The three other chapters are research articles that have been written together with several co-authors to whom I am very grateful for their successful collaboration. The three articles all contain original ideas both from my co-authors as well ones from myself and ones that came up during the many fruitful discussions we had on the subject. What follows is a short summary of the main results of each of the three research article chapters.

Chapter 2 is an article that has been published in the Journal of Algebra and is joint work with Mark van Hoeij. In this chapter the torsion groups of the form $\mathbb{Z}/N\mathbb{Z}$ are studied over number fields of degree 5,6,7, and 8. For of these degrees the explicit list of all integers N such that the torsion structure $\mathbb{Z}/N\mathbb{Z}$ occurs for infinitely many non isomorphic elliptic curves is determined, where the study of degrees ≤ 4 was omitted because here the answer was already known.

Chapter 3 is an article that is joint work with Sheldon Kamienny, William Stein and Michael Stoll, this article is not yet published but will soon be submitted for publication. In this article the primes that can divide the order of a torsion group of an elliptic curve over a number field of degree d are determined for degrees $4, 5$, and 6. Aside from the main result it also contains a section in which theory is developed that allows one to determine the set of all rational points on symmetric powers of a curve in certain situations. The Appendix of this chapter contains a proof of Joseph Oesterlé's Theorem that states that if an elliptic curve over a number field of degree d contains a torsion point of order p, then $p < (3^{d/2} + 1)^2$. It is included because a proof of this statement has not yet been published. The appendix closely follows Oesterlé's unpublished notes which he made available to me, although it contains some minor simplifications using literature that did not exists yet at the time that Oesterlé proved his Theorem.

---

[4]L. Merel. "Bornes pour la torsion des courbes elliptiques sur les corps de nombres". In: *Invent. Math.* 124.1-3 (1996), pp. 437–449.

[5]P. Parent. "Torsion des courbes elliptiques sur les corps cubiques". In: *Ann. Inst. Fourier (Grenoble)* 50.3 (2000), pp. 723–749.

[6]P. Parent. "No 17-torsion on elliptic curves over cubic number fields". In: *J. Théor. Nombres Bordeaux* 15.3 (2003), pp. 831–838.

The final chapter is an article that will appear in a memorial volume for Fumiyuki Momose. It is co-authored by Barry Mazur and Sheldon Kamienny. In this article the question is asked what one can still do if d, N are integers such that there are infinitely many non isomorphic elliptic curves over number fields of degree d with a torsion point of order N. Can one somehow still find all of them? As a first start in answering this question is done by an explicit case study, namely the question is answered for $N = 17$ and $d = 4$. This value of d is the smallest integer for which there exist infinitely many elliptic curves over a number field of degree d with a point of order 17.