



Universiteit  
Leiden  
The Netherlands

## Geometric quadratic chabauty and other topics in number theory

Lido, G.M.

### Citation

Lido, G. M. (2021, October 12). *Geometric quadratic chabauty and other topics in number theory*. Retrieved from <https://hdl.handle.net/1887/3216956>

Version: Publisher's Version

[Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

License: <https://hdl.handle.net/1887/3216956>

**Note:** To cite this publication please use the final published version (if applicable).

# **GEOMETRIC QUADRATIC CHABAUTY AND OTHER TOPICS IN NUMBER THEORY**

Proefschrift

ter verkrijging van  
de graad van doctor aan de Universiteit Leiden  
op gezag van rector magnificus prof. dr. ir. H. Bijl,  
volgens besluit van het college voor promoties  
te verdedigen op dinsdag 12 oktober 2021  
klokke 11.15 uur

door

**Guido Maria Lido**  
geboren te Roma, Italia, in 1992

**Promotor:** Prof. dr. Bas Edixhoven (Universiteit Leiden)

**Promotor:** Prof. dr. René Schoof (Università di Roma “Tor Vergata”)

**Samenstelling van de promotiecommissie:**

**Voorzitter:** Prof. dr. F.A. van der Duijn Schouten

**Secretaris:** Prof. dr. Peter Stevenhagen (Universiteit Leiden)

Prof. dr. Davide Lombardo (Università di Pisa)

Prof. dr. Marusia Rebolledo (Université B. Pascal Clermont-Ferrand 2)

Prof. dr. Michael Stoll (Universität Bayreuth)

This work was carried out at Università di Roma “Tor Vergata” and Universiteit Leiden. It was funded jointly by Università di Roma “Tor Vergata” and Universiteit Leiden.

The images in the front cover of this thesis, from the bottom to the top, are: an illustration of the geometric quadratic Chabauty method drawn by Sachi Hashimoto, available in [51], and representations of the modular curves  $X_{\text{ns}}(13)$  and  $X_{\text{ns}}^+(13)$ , drawn using the equations in [36].

The illustration in the back cover has been drawn by Giulia Caudullo and represents the descent algorithm in Chapter 4.



# Contents

---

<b>Introduction</b>	<b>v</b>
<b>1 Geometric quadratic Chabauty</b>	<b>1</b>
1.1 Introduction . . . . .	1
1.2 Algebraic geometry . . . . .	3
1.3 From algebraic geometry to formal geometry . . . . .	6
1.4 Integral points, closure and finiteness . . . . .	7
1.5 Parametrisation of integral points, and power series . . . . .	12
1.5.1 Logarithm and exponential . . . . .	12
1.5.2 Parametrisation by power series . . . . .	14
1.5.3 The $p$ -adic closure . . . . .	16
1.6 Explicit description of the Poincaré torsor . . . . .	16
1.6.1 Norms . . . . .	17
1.6.2 Norms along finite relative Cartier divisors . . . . .	18
1.6.3 Explicit description of the Poincaré torsor of a smooth curve . . . . .	19
1.6.4 Explicit isomorphism for norms along equivalent divisors . . . . .	22
1.6.5 Symmetry of the Norm for divisors on smooth curves . . . . .	24
1.6.6 Explicit residue disks and partial group laws . . . . .	26
1.6.7 Extension of the Poincaré biextension over Néron models . . . . .	30
1.6.8 Explicit description of the extended Poincaré bundle . . . . .	31
1.6.9 Integral points of the extended Poincaré torsor . . . . .	34
1.7 Description of the map from the curve to the torsor . . . . .	36
1.8 An example with genus 2, rank 2, and 14 points . . . . .	39
1.8.1 The torsor on the jacobian . . . . .	40
1.8.2 Some integral points on the biextension . . . . .	42
1.8.3 Some residue disks of the biextension . . . . .	43

## CONTENTS

---

1.8.4	Geometry mod $p^2$ of integral points . . . . .	44
1.8.5	The rational points with a specific image mod 5. . . . .	48
1.8.6	Determination of all rational points . . . . .	48
1.9	Some further remarks . . . . .	49
1.9.1	Complex uniformisations of some of the objects involved . . . . .	49
1.9.2	Finiteness of rational points . . . . .	52
1.9.3	The relation with $p$ -adic heights . . . . .	56
	Author contributions . . . . .	58
	Acknowledgements . . . . .	58
<b>2</b>	<b>Formal biextensions and quadratic Chabauty</b>	<b>59</b>
2.1	Recap on formal group laws . . . . .	59
2.2	Commutative formal biextension laws . . . . .	61
2.3	Biextensions over the $p$ -adics and convergence . . . . .	69
2.4	Another proof of Theorem 1.4.10 . . . . .	72
<b>3</b>	<b>Automorphisms of Cartan curves</b>	<b>77</b>
3.1	Introduction . . . . .	77
3.2	Modular curves . . . . .	81
3.3	Hecke operators . . . . .	83
3.4	Cartan modular curves and their jacobians . . . . .	92
3.5	Field of definition of automorphisms . . . . .	98
3.6	Automorphisms . . . . .	105
3.7	Appendix . . . . .	113
<b>4</b>	<b>Discrete logarithms in small characteristic</b>	<b>117</b>
	Acknowledgements . . . . .	118
4.1	Elliptic presentations . . . . .	119
4.2	Traps . . . . .	121
4.3	Divisors and discrete logarithm . . . . .	122
4.4	The main algorithm . . . . .	124
4.5	Strategy of proof of Theorem 4.4.1: the descent procedure . . . . .	128
4.6	A technical lemma . . . . .	132
4.7	Descent 3-to-2 . . . . .	138
4.7.1	The definition of $\mathcal{C}$ . . . . .	138
4.7.2	The irreducible components of $\mathcal{C}$ . . . . .	139
4.7.3	$k$ -rational points on $\mathcal{C}$ . . . . .	140
4.8	Descent 4-to-3 . . . . .	141

4.8.1	The definition of $\mathcal{C}$	141
4.8.2	Irreducibility of a projection of $\mathcal{C}$	142
4.8.3	The irreducible components of $\mathcal{C}$	151
4.8.4	$k$ -rational points on $\mathcal{C}$	153
<b>References</b>		<b>155</b>
<b>Summary</b>		<b>165</b>
<b>Samenvatting</b>		<b>167</b>
<b>Riassunto</b>		<b>169</b>
<b>Acknowledgements</b>		<b>171</b>
<b>Curriculum Vitae</b>		<b>173</b>

## CONTENTS