Universiteit Leiden
The Netherlands

Diophantine equations in positive characteristic

Koymans, P.H.

Citation
Koymans, P. H. (2019, June 19). *Diophantine equations in positive characteristic*. Retrieved from https://hdl.handle.net/1887/74294

Version: Not Applicable (or Unknown)
License: Leiden University Non-exclusive license
Downloaded from: https://hdl.handle.net/1887/74294

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

Cover Page

Universiteit Leiden

Leiden University Repository

The handle http://hdl.handle.net/1887/74294 holds various files of this Leiden University dissertation.

Author: Koymans, P.H.
Title: Diophantine equations in positive characteristic
Issue Date: 2019-06-19

Diophantine equations in positive characteristic

Proefschrift

ter verkrijging van
de graad 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 19 juni 2019
klokke 16.15 uur

door

Peter Hubrecht Koymans

geboren te Eindhoven

in 1992

Promotor	prof. dr. P. Stevenhagen	Leiden University
Copromotor	dr. J.-H. Evertse	Leiden University

Doctorate Committee

Chair	prof. dr. A. W. van der Vaart	Leiden University
Secretary	prof. dr. B. de Smit	Leiden University
Member	dr. A. Bartel	University of Glasgow
Member	prof. dr. E. Fouvry	University of Paris-Sud
Member	prof. dr. J. F. Voloch	University of Canterbury

Contents

Preface **v**

1 The generalized Catalan equation in positive characteristic **1**

1.1 Introduction 1

1.2 Heights 2

1.3 A generalization of Mason's ABC-theorem 3

1.4 Proof of Theorem 1.1.1 4

1.5 Discussion of Theorem 1.1.1 7

2 Two variable unit equations in positive characteristic **9**

2.1 Introduction 9

2.2 Valuations and heights 10

2.3 Proof of Theorem 2.1.2 11

2.4 Proof of Theorem 2.1.1 20

2.5 Acknowledgements 20

Addendum **21**

3 Unit equations and Fermat surfaces in positive characteristic **23**

3.1 Introduction 23

3.2 Preliminaries 27

3.3 Proof of Theorem 3.1.1 31

3.4 Proof of Theorem 3.1.2 34

3.5 Application to Fermat surfaces 40

3.6 Curves inside Fermat surfaces 45
3.7 Acknowledgements 47

4 On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1 \bmod 4$ 49

4.1 Introduction 49
4.2 Encoding the 16-rank of $\mathrm{Cl}(-8p)$ 51
4.3 Prerequisites 54
4.4 Proof of Proposition 4.3.7 61
4.5 Proof of Proposition 4.3.8 65

5 The 16-rank of $\mathbb{Q}(\sqrt{-p})$ 67

5.1 Introduction 67
5.2 Preliminaries 69
5.3 The sieve 72
5.4 Definition of the sequence 73
5.5 Sums of type I 77
5.6 Sums of type II 86

6 Joint distribution of spins 95

6.1 Introduction 95
6.2 Prerequisites 98
6.3 Linear sums 102
6.4 Bilinear sums 113
6.5 Governing fields 117

7 Vinogradov's three primes theorem with primes having given primitive roots 119

7.1 Introduction 119
7.2 Uniform ternary Goldbach with certain splitting conditions 128
7.3 The circle method and Hooley's approach 137
7.4 Artin's factor for ternary Goldbach 143

Bibliography 159

Samenvatting **165**

Acknowledgements **167**

Curriculum vitae **169**

Preface

In this preface we shall give a mathematical introduction to the various topics in the thesis. The thesis consists of three parts. The first part is devoted to exponential Diophantine equations in positive characteristic, while the second part revolves around class number statistics. These two parts form the main body of the thesis, whence the title of this thesis. The final and third part is a paper that solves the ternary Goldbach problem for Artin primes.

An exponential Diophantine equation is an equation where some of the variables occur as exponents. Famous examples of such equations are the Fermat equation

$$x^N + y^N = z^N \text{ in integers } N > 2,\ xyz \neq 0,$$

where N occurs as an exponent, and the Catalan equation

$$x^m - y^n = 1 \text{ in integers } x, y, m, n > 1,$$

where m and n occur as exponents. There is a well-known analogy between number fields and global function fields. Therefore, it is natural to solve these equations over global (or even more general) function fields instead of number fields. The advantage of global function fields is that one can use derivations, and this allows us to use elementary methods to establish our results.

Let K be a finitely generated field over $\mathbb{F}_p$ and fix $a, b \in K^*$. In the first chapter we shall study the generalized Catalan equation

$$ax^m + by^n = 1 \text{ in } x, y \in K \text{ and integers } m, n \text{ coprime with } p.$$

This equation was already studied by Silverman [66], but his main theorem is false as we shall demonstrate in the first chapter. We will prove that there are only finitely many solutions up to a natural equivalence relation provided that the pair (m, n) does not belong to an explicit finite list.

In the next chapter we shall study the so-called unit equation. Let K be a field of characteristic 0 and let G be a multiplicative subgroup of $K^* \times K^*$. Then the equation

$$x + y = 1 \text{ in } (x, y) \in G$$

is an exponential Diophantine equation. Siegel and Mahler showed finiteness of the solution set in important special cases, while Lang proved finiteness in general. Mahler and later Evertse [17] gave upper bounds for the solution sets in important special cases, while Beukers and Schlickewei [3] gave an upper bound in full generality. Namely, they showed that there are at most 2^{8r+8} solutions, where r is the rank of G. In characteristic $p > 0$ the situation turns out to be rather different. Indeed, if we have

$$x + y = 1 \text{ for some } (x, y) \in G,$$

we can apply Frobenius to find another solution

$$x^p + y^p = 1.$$

Voloch [78] gave an upper bound for the number of solutions up to a natural equivalence relation. His upper bound depends on both r and p, and he asked if the dependence on p could be removed. Together with Pagano I gave the upper bound $31 \cdot 19^r$, which answers Voloch's question. To do so, we adapt the method of Beukers and Schlickewei to positive characteristic.

The final chapter of the first part studies the Fermat surface

$$x^N + y^N + z^N = 1, \tag{1}$$

where $x, y, z \in \mathbb{F}_p(t)$ and N is a positive integer. The main result is that there are infinitely many primes N for which equation (1) has no solutions satisfying $x, y, z \notin \mathbb{F}_p(t^p)$ and $x/y, x/z, y/z \notin \mathbb{F}_p(t^p)$. We also show that the conditions on x, y and z can not be removed. This chapter is also joint work with Pagano.

The second part of the thesis revolves around the 2-part of the class groups of imaginary quadratic number fields. Cohen and Lenstra [10] put forward conjectures about the average behavior of such class groups. Let p be an odd prime. Their conjecture predicts that for all finite abelian p-groups A

$$\lim_{X\to\infty} \frac{|\{K \text{ imaginary quadratic} : |D_K| < X \text{ and } \mathrm{Cl}(K)[p^\infty] \cong A\}|}{|\{K \text{ imaginary quadratic} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1 - \frac{1}{p^i}\right)}{|\mathrm{Aut}(A)|},$$

where D_K and $\mathrm{Cl}(K)$ are respectively the discriminant and narrow class group of K. Although Cohen and Lenstra stated their conjecture already in 1984, there are very few proven instances despite significant effort. Davenport and Heilbronn [14] obtained partial results in the case $p = 3$, and the case $p > 3$ is still wide open. Although the conjecture was originally stated only for odd p, Gerth proposed the following modification; instead of $\mathrm{Cl}(K)[2^\infty]$, it is $(2\mathrm{Cl}(K))[2^\infty]$ that behaves randomly. This was recently proven by Smith [69] and can be considered a major breakthrough in the area.

One way to study $\mathrm{Cl}(K)[2^\infty]$ is by the use of governing fields. Let $k \geq 1$ and $d \not\equiv 2 \bmod 4$ be integers. Then Cohn and Lagarias [11] conjectured that there exists a finite normal field extension $M_{d,k}$ over $\mathbb{Q}$ such that

$$\dim_{\mathbb{F}_2} \frac{2^{k-1}\mathrm{Cl}(\mathbb{Q}(\sqrt{dp}))}{2^k\mathrm{Cl}(\mathbb{Q}(\sqrt{dp}))}$$

is determined by the splitting of p in $M_{d,k}$. Such a hypothetical field $M_{d,k}$ is called a governing field. Stevenhagen [70] showed in his thesis that governing field exists for $k \leq 3$ and all values of d. If one is able to give an explicit description of $M_{d,3}$, then one can get density results for $\mathrm{Cl}(\mathbb{Q}(\sqrt{dp}))[8]$ using the Chebotarev density theorem, where p varies over the primes.

It is a natural question to ask what happens for $\mathrm{Cl}(\mathbb{Q}(\sqrt{dp}))[16]$, and we analyze this problem for $d = -4$ and $d = -8$. This leads to the following density theorems, and we devote a chapter to each theorem.

Theorem (joint work with Milovic)**.** Let $h(-2p)$ be the class number of $\mathbb{Q}(\sqrt{-2p})$. Then we have

$$\lim_{X\to\infty} \frac{|\{p \leq X : p \text{ prime},\ p \equiv 1 \bmod 4 \text{ and } 16 \mid h(-2p)\}|}{|\{p \leq X : p \text{ prime}\}|} = \frac{1}{16}.$$

Theorem. Let $h(-p)$ be the class number of $\mathbb{Q}(\sqrt{-p})$. Then we have

$$\lim_{X\to\infty} \frac{|\{p \leq X : p \text{ prime and } 16 \mid h(-p)\}|}{|\{p \leq X : p \text{ prime}\}|} = \frac{1}{16}.$$

The proof of both theorems do not make any appeal to the theory of L-functions. Instead they rely on a method due to Vinogradov. This suggests that there is no governing field. The following theorem, which is proven in the final chapter of the second part, provides even more evidence towards the non-existence of governing fields.

Theorem (joint work with Milovic)**.** Assume a short character sum conjecture. Then the field $M_{-4,4}$ does not exist.

In the final part of this thesis we combine two classical problems in analytic number theory. The first problem is the well-known ternary Goldbach conjecture which states that every odd integer $n > 5$ can be written as the sum of three primes, i.e.

$$n = p_1 + p_2 + p_3$$

for primes p_1, p_2 and p_3. Vinogradov [74] showed that every sufficiently large odd integer admits such a representation, and Helfgott [34] settled the full ternary Goldbach conjecture. Another famous problem in analytic number theory is Artin's conjecture on primitive roots. Let g be an integer that is neither a square nor -1. Then Artin's conjecture states that there are infinitely many primes p such that g is a primitive root modulo p, or in other words g generates the group $(\mathbb{Z}/p\mathbb{Z})^*$. Hooley [35] showed the veracity of Artin's conjecture conditional on GRH.

We are interested in writing n as a sum of three primes, all of which have g as primitive root. The following is a simple corollary of our work that is particularly pleasing to state.

Corollary (joint with Frei and Sofos)**.** Assume GRH. Then there is a constant $C > 0$ such that for all odd integers $n > C$ we have the following equivalence: there are odd primes p_1, p_2, p_3 with 27 as primitive root and $n = p_1+p_2+p_3$ if and only if $n \equiv 3 \bmod 12$.