university of groningen / faculty of science and engineering / mathematics and applied mathematics

Constructing curves with many points over finite fields using coverings of curves with lower genus

Bachelor's Project Mathematics

July 2018

Student: A. Los

First supervisor: Prof.dr. J. Top

Second assessor: Dr. J.S. Müller

CONSTRUCTING CURVES WITH MANY POINTS OVER FINITE FIELDS USING COVERINGS OF CURVES WITH LOWER GENUS

A. LOS

Abstract. Concerning curves over finite fields with many points, for the curves with a specific genus it is not always known what the maximum number of points is. In this project we try to contribute to the knowledge about this by studying certain constructions of curves with a large amount of points. For this we use cubic coverings of suitable curves with lower genus.

Contents

1. Introduction

Concerning curves over finite fields with many points, for the curves with a specific genus it is not always known what the maximum number of points is. In this project we try to contribute to the knowledge about this by studying certain constructions of curves with a large amount of points. For this we use non-Galois coverings of suitable curves with lower genus. We make cubic coverings of curves with low genus and many points over finite fields to obtain curves with a triple amount of points and a not too high genus. We want to keep the genus of the covering curve as low as possible. A problem which arises in our approach is that the number of points on the lower curve contributes to the genus of the covering curve. We want to compare our results to the tables presented at `manypoints.org`. With the use of MAGMA we apply this method to a lot of curves and search for new curves over finite fields with many points and relatively low genus.

First we give some mathematical background. Then we describe the relevance of constructing curves with low genus over small finite fields, such that the curve has many rational points. We briefly mention some known results and how we contribute to these. Additionally we explain our approach and describe our calculations. Finally we give our results and we suggest some improvements.

2. Mathematical background

As background we assume the bachelor courses in algebraic structures. The reader should be familiar with finite fields, field extensions and function fields. We will explain the concepts of curves over finite fields, rational points on these curves, the genus of a curve, divisors and Riemann-Roch spaces.

2.1. **Curves over general fields.**

An algebraic curve (often denoted as C) is a projective algebraic variety of dimension one. The precise definition of this is complicated. We will therefore try to sketch it here and we refer to [Sil09, Chapter II] for more details. Let K be a field and let $\overline{K}$ be an algebraic closure of K. For any integer $n \geq 1$, let $\mathbb{P}^n(\overline{K})$ denote the set of 1-dimensional linear subspaces of $\overline{K}^{n+1}$. The line containing a point $(a_0, a_1, \ldots, a_n) \neq (0, 0, \ldots, 0)$ is denoted by $(a_0 : a_1 : \ldots : a_n)$. By $\mathbb{P}^n(K)$ we denote the subset of all lines containing a point $(a_0, a_1, \ldots, a_n) \neq (0, 0, \ldots, 0)$ with all $a_j \in K$. This is called the set of K-rational points in $\mathbb{P}^n$.

Suppose a prime ideal $I \subset \overline{K}[X_0, \ldots X_n]$ is generated by homogeneous polynomials. Define $V \subset \mathbb{P}^n$ by

$$V := \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all homogeneous } f \in I\}.$$

Such V is called an algebraic variety. We will assume that $X_0 \notin I$: otherwise, all points in V would have first coordinate equal to zero, so deleting this coordinate, we can regard V as a subset of $\mathbb{P}^{n-1}$. With the assumption $X_0 \notin I$, the dimension of a variety V is defined as the transcendence degree over $\overline{K}$ of the field of fractions of $ev_{X_0=1}(\overline{K}[X_0, \ldots, X_n]/I)$. The latter field is called the function field of V over $\overline{K}$ and is denoted $\overline{K}(V)$. A curve is a variety with dimension 1. A curve C over K means that the ideal I is generated by homogeneous polynomials with coefficients in K. In that case the field of fractions of $ev_{X_0=1}(K[X_0, \ldots, X_n]/I)$ is denoted $K(C)$, the function field of C over K. The set of points in $\mathbb{P}^n(K)$ that are on the curve C is denoted $C(K)$.

A smooth curve is a curve without singularities. A singularity of a curve C defined by a homogeneous prime ideal I is a point $P \in C(\overline{K})$ which adheres to the definition described below. Write $P = (a_0 : \ldots : a_n)$ and choose j such that $a_j \neq 0$. Without loss of generality we may assume $a_j = 1$. The points on the curve with j-th coordinate nonzero are precisely all points $(x_0 : \ldots : x_n)$ with $x_j = 1$ satisfying all polynomials in $J := ev_{X_j=1}(I)$. This can be seen as a subset of $\overline{K}^n$. Any line in $\overline{K}^n$ that passes through P can be parametrized as $P + \lambda Q$ where Q is any point different from P. We say that this line is a tangent line to C in P if $f(P + \lambda Q)$ (which is a polynomial in the variable λ) has a zero at $\lambda = 0$ of multiplicity at least 2, for every $f \in J$. Now P is called a singularity of C, if more than one tangent line to C in P exists.

The genus of a curve is a measure for the complexity of a curve. Well-known elliptic curves are the algebraic curves with genus one, but we will mostly work with more complex curves with higher genus. (More information about curves in general and elliptic curves in particular can be

found in 'The arithmetic of elliptic curves', Joseph Silverman [Sil09].) The genus of a curve C over a field K can be defined as the dimension over K of the vector space of regular 1-forms on C. When we look at smooth curves $C \subset \mathbb{P}^2$, the prime ideal I is a (nonzero) principal ideal, so it is generated by one irreducible polynomial. If we denote the degree of this polynomial by d, then the genus g of C equals $g = \frac{1}{2}(d-2)(d-1)$. More generally the genus of a curve is computed using the Riemann-Hurwitz-formula (or Hurwitz's theorem), which we now explain.

A rational map $\pi\colon C_2 \to C_1$ between curves is defined as follows (see [Sil09, Chapter II]). Suppose $C_2 \subset \mathbb{P}^n$ and $C_1 \subset \mathbb{P}^m$. Let $F_0, \ldots, F_m$ be homogeneous polynomials of the same degree d, such that not all $F_j \in I$, with I the ideal defining C_2. Then $(F_0 : \ldots : F_m)\colon C_2 \to \mathbb{P}^m$ is defined for all points $P \in C$ such that at least one of the F_j satisfies $F_j(P) \neq 0$. If the image is contained in the curve C_1, then we call π a rational map from C_2 to C_1. Such a rational map yields an embedding of $\overline{K}(C_1)$ in $\overline{K}(C_2)$, coming from $\overline{K}[\frac{F_1}{F_0}, \ldots, \frac{F_m}{F_0}] \to \overline{K}[\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}]]$. This means that functions $\phi \in \overline{K}(C_1)$ yield functions on C_2 by considering the composition $\phi \circ \pi$. The rational map π is called separable if this extension of function fields is separable.

The degree of a nonconstant rational map π is by definition the degree of the resulting extension $\overline{K}(C_1) \subset \overline{K}(C_2)$. Any point $Q \in C_2(\overline{K})$ corresponds to a surjective homomorphism of groups $\mathrm{ord}_Q\colon \overline{K}(C_2)^\times \to \mathbb{Z}$, which measures the 'order of vanishing' of a $\phi \in \overline{K}(C_2)^\times$ at the point Q. The (nonconstant) map $\pi\colon C_2 \to C_1$ then yields a commutative diagram

$$\begin{array}{ccc} \overline{K}(C_1)^\times & \xrightarrow{\mathrm{ord}_{\pi(Q)}} & \mathbb{Z} \\ \cap & & \downarrow \\ \overline{K}(C_2)^\times & \xrightarrow{\mathrm{ord}_\pi} & \mathbb{Z}. \end{array}$$

The resulting homomorphism $\mathbb{Z} \to \mathbb{Z}$ is multiplication by a positive integer e_Q, which is called the ramification index of π at Q. For a separable map $C_2 \to C_1$ of degree d, satisfying the condition that for every point $Q \in C_2$ we have $\mathrm{Char}(K) \nmid e_Q \forall Q \in C_2$ the Riemann-Hurwitz formula states that

$$2g(C_2) - 2 = d(2g(C_1) - 2) + \sum_{Q \in C_2} (e_Q - 1).$$

2.2. **Curves over finite fields.**

The number of $\mathbb{F}_q$-rational points on curves over finite fields is finite, because there is only a finite number of possibilities for $(a_0, a_1, \ldots, a_n)$ with coefficients in $\mathbb{F}_q$.

For many applications it is desired to have curves over finite fields with many rational points. A result of A. Weil slightly improved by J-P. Serre gives good estimates for the number of points: For a finite field $\mathbb{F}_q$ and a curve C over $\mathbb{F}_q$ with genus $g(C)$ we have the following bounds for the number of $\mathbb{F}_q$-rational points:

$$q + 1 - g(C) \cdot \lfloor \sqrt{4q} \rfloor \leq \#C(\mathbb{F}_q) \leq q + 1 + g(C) \cdot \lfloor \sqrt{4q} \rfloor,$$

where $\#C(\mathbb{F}_q)$ denotes the cardinality of the set $C(\mathbb{F}_q)$.

Sometimes the term 'places' is used instead of 'points'. More precisely, a place of degree n on C over $\mathbb{F}_q$ is a $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$-orbit of a point $P \in C(\mathbb{F}_{q^n})$ such that this orbit consists of precisely n distinct points. In other words, $P \in C(\mathbb{F}_{q^n})$ but $P \notin C(\mathbb{F}_{q^m})$ for any $m < n$.

In terms of the function field: A place corresponds to a 'valuation' $\mathbb{F}_q(C)^\times \to \mathbb{Z}$ given by $f \mapsto \mathrm{ord}_P(f)$. If $\mathrm{ord}_P(f) > 0$, then f has a zero of order $\mathrm{ord}_P(f)$ at P and if $\mathrm{ord}_P(f) < 0$, then f has a pole of order $-\mathrm{ord}_P(f)$ at P.

A divisor D is a finite formal sum of points (places) of a curve. In other words, it is an element of the free abelian group $\mathrm{Div}(C)$ on the points of the curve C. Any element of $\mathrm{Div}(C)$ is written as $\sum_{P \in C} n_P P$, with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many points $P \in C$. The sum of the integers n_P is called the degree of the divisor, denoted by $\deg(\sum_{P \in C} n_P P)$. To a place of degree n on C over $\mathbb{F}_q$ one associates the divisor $D_P := \sum \sigma(P)$ where $P \in C$ denotes a point such that the place is the Galois-orbit of P, and σ runs over the elements of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Note that $\deg(D_P) = n$.

Given a divisor $D = \sum n_P P$, which is a combination of divisors of places of C over $\mathbb{F}_q$, one defines the corresponding Riemann-Roch space $L(D)$ by

$$L(D) := \{0\} \cup \{f \in \mathbb{F}_q(C)^\times \ : \ \mathrm{ord}_P(f) + n_P \geq 0 \text{ for all } P \in C\}.$$

This is a finite dimensional vector space over $\mathbb{F}_q$, consisting of functions in $\mathbb{F}_q(C)$ with prescribed poles and zeros. Because $\mathrm{ord}_P(f) + n_P \geq 0$ for all $P \in C$ we have that $\mathrm{ord}_P(f) \geq -n_P$, so f needs to have zeros of multiplicity at least $-n_P$ and can have poles with maximal multiplicity n_P. Functions, which are elements in the Riemann-Roch space $L(E - D)$, with $E = \sum(m_P P)$ and $D = \sum(n_R R)$ divisors, and all $m_P, n_R \geq 0$ and moreover $\{P \mid m_P \neq 0\} \cap \{R \mid n_R \neq 0\} = \emptyset$, have poles of maximal order m_P at the points P and zeros of at least order n_R at the points R.

If $\deg(D) < 0$, then $L(D)$ has dimension 0. So in order to have a space with positive dimension, our divisor should have a non-negative degree, see [Sta, page 12, corollary 3.21]. Therefore, in the case of $L(E - D)$ described above, $\sum m_P \geq \sum n_R$ is a necessary (but not sufficient) condition for $L(E - D)$ to be nonzero. For a divisor $n_P D_P - m_Q D_Q$ of places $P \neq Q$ of degree p, q resp., $n_P \cdot p \geq n_Q \cdot q$ is required for $L(n_P D_P - m_Q D_Q)$ to be nonzero.

For any divisor D which is a combination of divisors of places of C over $\mathbb{F}_q$, it holds that $l(D) \geq \deg(D) - g(C) + 1$. Here $l(D)$ denotes the dimension (over $\mathbb{F}_q$) of the Riemann-Roch space $L(D)$. A stronger result is the Riemann-Roch theorem:

$$l(D) - l(\omega - D) = \deg(D) - g(C) + 1.$$

In this formula ω denotes any canonical divisor on the curve C. This is the divisor one associates to a differential on C, see [Sil09, Chapter II]. It is known that $\deg(\omega) = 2g(C) - 2$. In particular, if $\deg(D) > 2g(C) - 2$, then $\deg(\omega - D) < 0$, hence $l(\omega - D) = 0$. As a consequence $l(D) = \deg(D) - g(C) + 1$ whenever $\deg(D) > 2g(C) - 2$.

3. Relevance and goal

3.1. **Relevance of curves with many points over finite fields.**

Applications of curves with many points over finite fields lie in the fields of coding theory and cryptography. Current methods for encryption and key exchange nearly all use elliptic curve cryptography (ECC). In comparison with non-ECC methods, this method is faster and easier to use. For example, the key length can be smaller and the algorithms work faster for the same level of security (the chance that a code can be cracked in a specific amount of time) [Age16], [Mur10].

Curves of higher genus with many points are especially relevant for constructing good error-correcting codes, see [TVN10]. These codes in turn may be useful for post-quantum cryptography, in particular for creating so-called code-based cryptosystems.

Many applications of curves (with or without many points) use a group which can be described as follows. Start with a curve C over $\mathbb{F}_q$. The abelian group $\mathrm{Div}(C)$ consists of all divisors which are combinations of divisors of places of C over $\mathbb{F}_q$. It has a subgroup $\mathrm{Div}^0(C)$ consisting of divisors of degree zero. For any $\phi \in \mathbb{F}_q(C)^\times$ one has a divisor $\mathrm{div}(\phi) := \sum_{P \in C} \mathrm{ord}_P(\phi) P$. Then $\mathrm{Princ}(C) := \{\mathrm{div}(\phi) \mid \phi \in \mathbb{F}_q(C)^\times\}$ is a subgroup of $\mathrm{Div}^0(C)$. The factor group $\mathrm{Div}^0(C)/\mathrm{Princ}(C)$ plays an important role both in the theory and in various applications. It is isomorphic to the group consisting of the rational points on the Jacobian variety of the curve.

3.2. **Some facts concerning curves of low genus with many points over finite fields.**

We briefly mention some known results on curves of low genus with many points over finite fields.

As is already suggested by the Hasse-Weil-Serre bound, two parameters are important, namely q (the cardinality of the finite field $\mathbb{F}_q$), and g (the genus of the curve C over $\mathbb{F}_q$ one considers). A numerical overview of the current knowledge for pairs (q, g) with $g \leq 50$ and a prime power $q \in \{2, 2^2, \ldots, 2^7\} \cup \{3, \ldots, 3^5\} \cup \{5, \ldots, 5^5\} \cup \cdots \cup \{19, \ldots, 19^5\} \cup \{23, 29, \ldots, 97\}$ can be found on `manypoints.org` [vdGHLR09]. For a lot of these pairs (q, g), people have found an explicit curve attaining the maximal possible the number of points, or one which has a number of points that is close to the Hasse-Weil-Serre bound. These curves, and in many cases the papers in which their construction can be found, are mentioned along with some essential properties of the curve. A lot of examples are, contrary to our approach, found using class field theory. This means that the function field L of the curve is described as a Galois extension L/K of the function field $\mathbb{F}_q(C)$ of some simpler curve C over $\mathbb{F}_q$, and the Galois group of L/K is abelian.

For curves of genus one over finite fields, the elliptic curves, there exists a formula for the maximal number of points, thanks to Deuring and Waterhouse [Wat69]. For a given q it is not difficult to determine an explicit example of a genus one curve over $\mathbb{F}_q$ attaining this maximal number of points. Jean-Pierre Serre defined a formula which calculates the maximum number of points for curves of genus two over finite fields [Ser85]. In his PhD thesis, Soomro [Soo13] gave explicit examples of curves of genus two attaining this maximum for q in the set above.

For genus three or higher it is not known whether a general formula exists, but for genus three there is a conjecture by Jean-Pierre Serre that a constant e exists, such that for all prime powers q the maximum number of points on a genus three curve over $\mathbb{F}_q$ is greater than or equal to $q+1+3\lfloor\sqrt{4q}\rfloor-e$. Jaap Top proved this for q a power of three [Top03] and Jean-François Mestre for q a power of seven. For a fixed genus $g \geq 4$ no similar result is known or conjectured. For example in the case $q = 3^5, g = 9$, it is known that any curve of genus nine over $\mathbb{F}_{243}$ has at most 521 rational points. However no example of any such curve with close to 521 points is known.

3.3. **Goal of our project.**

The aim of our project is to investigate a different method for finding new inputs for the tables on `manypoints.org`. In our research project we apply a new method (for finding explicit curves over finite fields with many rational points) using non-Galois extensions contrary to the class field theory approach that is commonly used.

4. Constructing new curves

4.1. **Idea of our approach.**

The process we propose for making new curves is as follows. More details can be found in Section 4.3.

We examine the tables of `manypoints.org`, looking for cases of specific finite fields $\mathbb{F}_q$ and genus g where no example of a suitable curve with enough points is presented. So no explicit curve of genus g defined over $\mathbb{F}_q$ with a number of points close to the Hasse-Weil-Serre bound is known. For these cases we decide what we find relevant by determining a minimum number of points we want our curve to have. In general we require the number of points to be at least the known upper bound, divided by $\sqrt{2}$, because that is what is required for submitting improvement on `manypoints.org`. As an example, for $q = 243$ and $g = 9$ the known upper bound equals 521, so we require at least $521/\sqrt{2} > 368$ rational points in this case.

For each case we look for curves with lower genus with at least a third of the desired number of points over the same field. From these smaller curves we try to construct the desired curves with three times the number of rational points. Because we did not gain many results, we expanded our method to all kinds of curves and not only those for which an explicit curve is missing in the table.

Starting from a curve C_1 defined over $\mathbb{F}_q$ we construct a new curve C_2 over $\mathbb{F}_q$ as follows. Assume q is odd. Take $r \in \mathbb{F}_q(C_1)$ such that $\mathrm{ord}_Q(r) > 0$ for every $Q \in C_1(\mathbb{F}_q)$. Moreover we want that the polynomial $T^3 - T - r$ is irreducible as a polynomial over $\mathbb{F}_q(C_1)$. Now take the extension of $\mathbb{F}_q(C_1)$ obtained by adjoining a root of $T^3 - T - r$. This clearly is a cubic extension. It is the function field of another curve (which we call C_2) over $\mathbb{F}_q$. In this way we obtain a rational map $\pi\colon C_2 \to C_1$, which yields the associated extension of function fields. Given $Q \in C_2(\mathbb{F}_q)$, its image $\pi(Q)$ is a rational point on C_1. Vice versa given $P \in C_1(\mathbb{F}_q)$, its pre-image $\pi^{-1}(P)$ consists of three rational points on C_2 corresponding to P and the zeros in $\mathbb{F}_q$ of the equation $T^3 - T - r(P)$. As $r(P) = 0$ by construction, there are indeed precisely three such rational pre-images, provided q is odd. This shows $\#C_2(\mathbb{F}_q) = 3 \cdot \#C_1(\mathbb{F}_q)$.

We obtain a suitable r by taking it from an appropriate Riemann-Roch Space of C_1. Namely, we choose suitable divisors D and E where D is the formal sum of all points in $C_1(\mathbb{F}_q)$, so $D = \sum_{P \in C_1(\mathbb{F}_q)} P$. We let E be a sum of places of C_1 of degree at least 2 over $\mathbb{F}_q$. If $l(E - D) \neq 0$, which is certainly the case whenever $\deg(E) - \#C_1(\mathbb{F}_q) = \deg(E - D) > 2g(C_1) - 2$, then such r exists.

Whether indeed the polynomial $T^3 - T - r$ is irreducible in $\mathbb{F}_q(C_1)[T]$ should be tested. For a given r, this is an easy test (using a computer algebra system such as MAGMA). In the paragraphs below, we will study the genus of the curve C_2 obtained in this way. We will investigate how the genus can be computed and how we can restrain the genus by choosing E correctly. Before we do this, we present a small example.

Remark. A degree p extension obtained by adjoining a zero of $T^p - T - r$ to a field of characteristic p is called an Artin-Schreier extension. Artin-Schreier extensions are examples of abelian Galois extensions and are already examined by others. In particular, in the examples and in the theory discussed below we explicitly demand $\mathrm{char}(\mathbb{F}_q) \neq 3$.

4.2. **Explanation using an example.**

For C_1 we take the projective space $\mathbb{P}^1$, which has $q+1$ $\mathbb{F}_q$-rational points. It is a curve of genus 0, and function field $\mathbb{F}_q(t)$ with $t = X/Y$ and $(X : Y)$ the projective coordinates on $\mathbb{P}^1$. The function $t^q - t \in \mathbb{F}_q(t)$ is 0 in $\mathbb{F}_q \subset \mathbb{P}^1(\mathbb{F}_q)$. We also want a zero at infinity, so we divide $t^q - t$ by an element of $\mathbb{F}_q[t]$ of degree $q+1$ which is coprime to $t^q - t$. For example, try $t^{q+1} - c$ with $c \in \mathbb{F}_q$ such that $t^{q+1} - c$ has no zero in $\mathbb{F}_q$. For any possible $a \in \mathbb{F}_q$ we have that $a^{q+1} - c = a^2 - c$, so we choose c to be no square in $\mathbb{F}_q$. Then $r := (t^q - t)/(t^{q+1} - c)$ is a function which is zero on all points of $\mathbb{P}^1(\mathbb{F}_q)$. Now our extension $T^3 - T - r$ gives $3q+3$ points, provided this polynomial is irreducible. In fact it is easy to check that $T^3 - T - r$ is irreducible (even as a polynomial in $\overline{\mathbb{F}}_q(t)[T]$). We can use the Riemann-Hurwitz formula to compute the genus of the resulting curve C_2. As before, we assume $\mathrm{char}(\mathbb{F}_q) > 3$, which guarantees that the extension $\mathbb{F}_q(t) \subset \mathbb{F}_q(C_2)$ is separable and that $\mathrm{char}(\mathbb{F}_q) \nmid e_Q$ for all points $Q \in C_2$.

In our situation the Riemann-Hurwitz formula gives

$$2g(C_2) - 2 = -6 + \sum_{Q \in C_2} (e_Q - 1).$$

By construction $\pi^{-1}(\infty)$ consists of three distinct points, so here π is not ramified. There is ramification with $e_Q = 3$ over every t such that $t^{q+1} - c = 0$. This gives a contribution $2q+2$ in the sum above. There is ramification with $e_Q = 2$ whenever the discriminant of $T^3 - T - r$ is zero. The discriminant is $4 - 27r^2$. This vanishes whenever $4(t^{q+1} - c)^2 - 27(t^q - t)^2 = 0$. In general this happens for $2q+2$ values of t. So in that case one finds $g(C_2) = 1 - 3 + (q+1) + (q+1) = 2q$ (and $\#C_2(\mathbb{F}_q) = 3 \cdot \#C_1(\mathbb{F}_q) = 3(q+1)$).

However, when $4(t^{q+1} - c)^2 - 27(t^q - t)^2$ has less than $2q+2$ zeros, the genus will be smaller. For example this happens when $q = 31$. In that case we have only two different zeros and in fact $g(C_2) = 1 - 3 + (q+1) + 0 = q - 1 = 30$. This curve has $3(q+1) = 96$ points over $\mathbb{F}_{31}$, which is still quite far from the theoretical upper bound.

Another example where this happens is when $q = 5$. In this case $g(C_2) = 4$ and we have $3(q+1) = 18$ rational points, which is actually the maximum for genus 4 over $\mathbb{F}_5$.

4.3. **Specific calculations and choice of divisors.**

In this section we give a more detailed outline of our approach and explain the calculations and choices we make.

In our project, we start with a curve C_1 defined over $\mathbb{F}_q$. Take $r \in \mathbb{F}_q(C_1)$ and $p > 0$ so that $T^p - T - r \in \overline{\mathbb{F}}_q[T]$ is irreducible. Adjoining a zero of this polynomial to $\mathbb{F}_q(C_1)$ yields an extension field of degree p, and this is the function field of a curve C_2 defined over $\mathbb{F}_q$. In our project we mostly look at $p = 3$ and we assume that this is not equal to the field characteristic. (Even though we also tried some other ways to make extensions, for example with $T^4 - T - r$ and $T^2 - T - r$, we will in this report focus only on the cubic extension.)

We want to count the places of degree 1 over $\mathbb{F}_q$ in the field $\mathbb{F}_q(C_2)$. Any such place/point maps to a place of degree 1 over $\mathbb{F}_q$ in $\mathbb{F}_q(C_1)$ under the map $C_2 \to C_1$ corresponding to $\mathbb{F}_q(C_1) \subset \mathbb{F}_q(C_2)$. So one tries to count the points on C_2 by considering how many map to a given point on C_1. For $P \in C_1$, this (generally) depends on the splitting behavior of $T^3 - T - r(P)$ over $\mathbb{F}_q[T]$. Choosing r such that $r(P) = 0$ for all points $P \in C_1$ with coordinates in $\mathbb{F}_q$, thus for $T^3 - T = 0$ with coordinates in $\mathbb{F}_q$, one obtains 3 places of degree 1 in $\mathbb{F}_q(C_2)$ over $\mathbb{F}_q$, for each $P \in C_1(\mathbb{F}_q)$. In this way $\#C_2(\mathbb{F}_q) = 3 \cdot \#C_1(\mathbb{F}_q)$. So we triple the number of $\mathbb{F}_q$-rational points.

To go from our starting curve C_1 to our resulting curve C_2, we make an extension with $T^3 - T - r$, the discriminant of which is $4 - 27r^2$. ($T^3 - T + r$ would give the same discriminant, so with respect to the zeros it does not matter which one we choose.) If the discriminant is zero, this would give ramification.

The Riemann-Hurwitz formula $2g(C_2) - 2 = 3(2g(C_1) - 2) + \sum_{Q \in C_2}(e_Q - 1)$ yields $g(C_2) - 1 = 3(g(C_1) - 1) + \frac{1}{2}\sum_{Q \in C_2}(e_Q - 1)$, so $g(C_2) = 3g(C_1) - 2 + \frac{1}{2}\sum_{Q \in C_2}(e_Q - 1)$. Here e_Q depends on the poles of r and the zeros of $4 - 27r^2$, because only there a ramification can occur. In the following paragraphs we explain how to choose the function r.

We want our resulting genus $g(C_2)$ to be as low as possible, thus we search for functions r with no or few $e > 1$. For each rational point $P \in C_1$, we can distinguish three cases:

Case 1: For P on C_1 with $4-27r^2(P)\neq 0$ we have three points on C_2 (possibly over an extension) and no ramification, so $e_Q=1$ for the three points Q above P.

Case 2: For points P on C_1 with $4-27r^2(P)=0$ we have less zeros. There could not be any threefold zeros, for reasons explained below. Assume we have a threefold zero: $T^3-T-r(P)=(T-\alpha)^3=T^3-3\alpha T^2+3\alpha^2T-\alpha^3$. Since the field characteristic is not 3, $3\alpha T^2=0$ means $\alpha=0$, which is impossible considering the linear term of the polynomial. So in this case we have a double zero and a single zero. This means $e_Q=2$ for exactly one of the points Q above P.

Case 3: Our r has a pole in a rational point P. We can write $(\frac{T}{r})^3-\frac{1}{r^2}\frac{T}{r}+\frac{1}{r^2}=0$. We choose a uniformizer function h with a zero of order 1 in P and a function u with $u(P)\neq 0$ such that $r=uh^{-n}$ with $n=3k-m\geq 1$, $k\in\mathbb{Z}_{>0}$ and $m\in\{0,1,2\}$. If we now multiply T^3-T-r by h^{3k}, we have $(h^kT)^3-h^{2k}(h^kT)+uh^m=0$. If $m=0$ we have $(h^kT)^3-h^{2k}(h^kT)+u=0$. Filling in P gives $(h^kT)^3+u(P)=0$, because the second coefficient is zero in P. This equation has three distinct solutions, so there is no ramification over P. If $m=1$, $(h^kT)^3-h^{2k}(h^kT)+uh=0$, which is, as a polynomial in h^kT, Eisenstein at h. So this gives one point over P and a ramification $e=3$ at this point. If $m=2$, we obtain an equation $(h^kT)^3-h^{2k}(h^kT)+uh^2=0$. Choose a (uniformizer) function $h_Q\in\overline{\mathbb{F}}_q(C_2)$ with $\mathrm{ord}_Q(h_Q)=1$ for a point Q above P. Then write $h=h_Q^a u_Q$ with $\mathrm{ord}_Q(u_Q)=0$ and write $(h^kT)=h_Q^b v_Q$ with $b\geq 0, \mathrm{ord}_Q(v_Q)=0$. Now we can rewrite our equation into $h_Q^{3b}v_Q^3-h_Q^{2ka+b}u_Q^{2k}v_Q+uh_Q^{2a}u_Q^2=0$. The poles should cancel out, so $3b=2a$. Then $a=3$, so we have one solution, $e=3$. Thus $m=1,2$ give ramification with index $e=3$, only $m=0$ gives us no ramification. So we want an $r=uh^{-n}$ with $n=3k$, that is, an r which has only poles of order a multiple of 3.

In order to avoid ramification, we want for each $P\in C_1$ either no poles, or case 3 with poles of order 0 mod 3. So in any case we want the function r to have poles of order exactly 0 mod 3. This means that r for some $n\in\mathbb{Z}_{\geq 0}$ has maximal order $3n$ and at least order $3n$. That means r is in the Riemann-Roch space of $3nE_{is}-D$, for some divisors E_{is} and D, but not in the Riemann-Roch space of $(3n-1)E_{is}-D$. In this way we require that r has poles of maximal order $3n$, but it does not have poles of maximal order $3n-1$. The $-D$, which we choose to be $\sum_{P\in C_1}-P$ is necessary to assure that r has zeros (of at least order one) in all the $\mathbb{F}_q$-rational points of both C_1 and C_2. As said in the background section, if a divisor D satisfies $\deg(D)<0$, then $L(D)$ has dimension 0. We want nonzero vectors in the Riemann-Roch space, thus the dimension of $L(D)$ should be greater than zero. So our divisor $kE_{is}-D$ should have a non-negative degree. (This is a necessary but not sufficient condition for the Riemann-Roch space to have positive dimension. So in our code we check that the degree is positive.) We want the degree of our divisor as low as possible, because a higher degree means a higher genus, as we can see from the right-hand side of the Riemann-Roch theorem: $l(D)-l(\omega-D)=\deg(D)-g(C)+1$. To satisfy these conditions we take the coefficient $k=3n$ of E_{is} to be the lowest possible threefold for which $\deg(kE_{is}-D)\geq 0$. Thus we take k to be $3\lceil\lceil\deg(D)/3\rceil/\deg(E_{is})\rceil$. Here $\deg(D)=\deg(\sum_{P\in C_1}P)=\#C_1(\mathbb{F}_q)$ and $\deg(E_{is})\geq 2$ is the degree of the place E_{is}. We could have taken different places instead of E_{is}, even of different degree, and to each assign a (possibly different) coefficient, but we didn't in order to keep it simple and more easy to go over all possibilities.

Following the method above, we obtain a suitable Riemann-Roch space from where we can take a function r. In our code we go over all r in the space. For each r we check the irreducibility of T^3-T-r and make the extension of the function field $\mathbb{F}_q(C_1)$ by adjoining a zero of this polynomial. The resulting field is $\mathbb{F}_q(C_2)$. We know that the number of $\mathbb{F}_q$-rational points on C_2 is equal to $3\cdot\#C_1(\mathbb{F}_q)$. The genus of C_2 is not immediately clear and should be computed.

As in the example in 4.2, we can use the Riemann-Hurwitz formula. As we showed in the beginning of this paragraph, $g(C_2)=3g(C_1)-2+\frac{1}{2}\sum_{Q\in C_2}(e_Q-1)$.

Because we have only poles of order 0 modulo 3, the only contribution to the last term is $e_Q=2$ for every $P\in C_1$ with $4-27r^2(P)=0$, see case 2 above. The precise amount of zeros of the discriminant depends on the choice of r. We can only give an upper bound. In words: The amount of zeros without multiplicity is lower than or equal to the number of zeros with multiplicity. The amount of zeros counting multiplicities is equal to the amount of poles of the discriminant. This is equal to two times the number of poles of r, counting multiplicity. So it it less than or equal to two times the degree of the pole divisor that we take. In formulas: $\#\{P\colon 4-27r^2(P)=0\}$(without multiplicities) $\leq\#\{P\colon 4-27r^2(P)=0\}$(with multiplicities) $=\#\{P\colon 4-27r^2(P)=\infty\}$(with multiplicities) $=\#\{P\colon r^2(P)=\infty\}$(with multiplicities) $=$

$2\#\{P\colon r(P) = \infty\} \leq 2\deg(kE_{is})$. Thus $\frac{1}{2}\sum_{Q\in C_2}(e_Q - 1)$ is bounded above by $i \cdot k$, where $i = \deg(E_{is})$ and $k = 3\left\lceil \lceil \deg(D)/3 \rceil / \deg(E_{is}) \right\rceil$. For each choice of $\deg(D)$ and $\deg(E_{is})$ we have $i \cdot k \leq \deg(D) + 2 + 3(\deg(E_{is}) - 1)$. This gives $\frac{1}{2}\sum_{Q\in C_2}(e_Q - 1) \leq \deg(D) + 3\deg(E_{is}) - 1$. So we have as an upper bound for the genus of resulting curves of our method

$$g(C_2) \leq 3g(C_1) + \deg(D) + 3\deg(E_{is}) - 3.$$

In case there are less different zeros of the discriminant $4 - 27r^2(P)$ for some $P \in C_1$, these zeros cause a decrease of $\frac{1}{2}\sum_{Q\in C_2}(e_Q - 1)$. In this case there are less rational points P on C_1 where ramification can take place. So there are less (different) $P \in C_1$ with $e_Q = 2$ for one of the points Q above P. Therefore the bound for the ramification term is not attained. Thus $g(C_2) < 3g(C_1) - 2 + i \cdot k$ and $g(C_2) < 3g(C_1) + \deg(D) + 3\deg(E_{is}) - 3$.

When we take only E_{is} with relatively small degree (at most 3 or 4), then the last term in the Riemann-Hurwitz formula is approximately the number of rational points of the starting curve C_1. Sometimes it is a bit higher, due to rounding (when dividing by 3) and $\deg(E_{is})$, and sometimes a bit lower, due to multiple zeros of $4 - 27r^2$.

4.4. **MAGMA-code.**

In the process of trying to find new curves, we used different codes in the mathematical software package MAGMA. To give further insight in the calculations, the final code for cubic extensions over curves is explained here. In some cases we made the field extension belonging to the curve in two (instead of one) steps. For that code, see the first appendix.

In the code presented here we make the function field of the curve in one step.

```
//Input: p, f, max i.
//Output: p, Genus(C2), #Places(C2), f, Genus(C1), i, s, k, r

p:=5;
K<x>:=FunctionField(GF(p));
PK<Y>:=PolynomialRing(K);
f:= (x^4 + 4)*Y^4 + x^3*Y^3 + 3*x*Y + 4*x^4;
C1<z>:=ext<K|f>;
Q:=Places(C1,1);
D:=&+Q;
Sd:=#Q;
for i:=2 to 5 do
ming:=100;
k:=3*Ceiling(Ceiling(Sd/3)/i);
for s:=1 to #Places(C1,i) do
Eis:=Places(C1,i)[s];
V, phi:=RiemannRochSpace(k*Eis-D);
dimv:=Dimension(V);
if dimv ne 0 then
W, ksi:=RiemannRochSpace((k-1)*Eis-D);
if dimv ne Dimension(W) then
PC1<T>:=PolynomialRing(C1);
for v in V do
r:=phi(v);
if IsIrreducible(T^3-T-r) then
C2<u>:=ext<C1|T^3-T-r>;
if Genus(C2) lt ming then
ming:=Genus(C2);
print p, Genus(C2), #Places(C2,1), f, Genus(C1), i, s, k, r;
end if;
end if;
end for;
end if;
end if;
end for;
end for;
```

In short:
In line 4 to 5 we make the base field.
In line 5 to 8 we make the curve, here called C_1. The genus of this curve is printed in line 29.
In line 9 to 17 we make the Riemann-Roch space of the right divisor(s).
In line 26 we make our new curve over the field.
In line 27 to 28 we check if the curve is better than previous curves, cause we need only one example of a good curve.
In line 29 all the output is printed. We print the size of the base field and the genus and number of rational points of our resulting curve C_2. After that also how we came to this curve by printing the rest of the input and finally the explicit formula for the curve.

More detailed:
Line 4: We choose the cardinality p of the field we want to work in.
Line 5: We make the function field K of the field with p elements.
Line 6: We make the polynomial ring over this field, so we could the polynomial equation for the curve.
Line 7: We give the function f, which zeros describe a curve.
Line 8: We make the curve C_1 over K as an extension of K with the zeros of f.
Line 9: The places on C_1 of degree 1 are the rational points on C_1 over K. The function Places(C, i) gives for a curve C over K a sequence containing the places of degree i of the function field (/curve) C/K.
Line 10: To make a divisor D containing all zeros, we take the formal sum of all rational points.
Line 11: We want to know the number of rational points on the curve C_1 over K.
Line 12: We want to make another divisor E_{is} containing places of degree $i > 1$ where poles can occur. When the degree is too high, the computer cannot handle this in memory and time, so we go along all i that work. For some curves we were able to choose i equal to 6 or 7.
Line 13: For each degree i we want to find curves with minimal genus. Here we introduce a far too high starting bound, therefore any curve we consider would fall inside this bound.
Line 14:Because we want only poles of order 0 mod 3, and the order should be as low as possible (but positive), we take k to be the threefold that is equal to or just above the number of rational points divided by i. In this way $kE_{is} \geq D$.
Line 15: We want to test all possible divisors that use one place of degree $i > 0$.
Line 16: We make the divisor E_{is} as the sth place of degree i.
Line 17: We make the Riemann-Roch space of the combination $(kE_{is} - D)$ of divisors. V is a vector space and *phi* is an isomorphism from V to the Riemann-Roch space in the function field of the curve on which the divisor $kE_{is} - D$ lies.
Line 18: *dimv* is the dimension of the vector space V, which is dimension of the Riemann-Roch space.
Line 19: We want the dimension to be positive, not equal to zero.
Line 20: We want our functions to have precisely the order of poles that are allowed by our chosen divisors. So not in the Riemann-Roch space where poles of that order -1 are allowed. Functions should be in $phi(V)$, but not in $ksi(W)$. We here only test if such functions exist, but (unfortunately) in this code we do not test if the functions we use indeed do have poles of the right order.
Line 21: The dimension of W should be less than the dimension of V.
Line 22: We want to make an extension of our curve C_1, so we define a polynomial ring over it to make it possible to define a curve C_2 over it.
Line 23: We go over all vectors v in our space V to obtain all functions in the isomorphic Riemann-Roch space.
Line 24: The functions r in the Riemann-Roch space are the images of $v \in V$ under the isomorphism *phi*.
Line 25: The polynomial $T^3 - T - r$ should be irreducible.
Line 26: We make C_2 as an extension of our lower curve C_1 by adding the zeros of $T^3 - T - r$ to it.
Line 27: We want only one example (per i) of a curve that has the lowest possible genus, not a lot of examples that have the same genus and same number of rational points.
Line 28: So after each result we make the restriction on the genus more tight.
Line 29: We give as output all relevant information.

5. Results and discussion

In this section we will present the results that we found with the above approach, take a look to the originality of the results and discuss some improvements that can be made.

5.1. **Results.**

In the second appendix, a table can be found with our results. For all (or sometimes the best) curves we found, the output is given, sorted to genus and size/cardinality of the base field. Our best result (and second best) is marked orange. This is where we found a curve over $\mathbb{F}_5$ with genus 18 and 36 $\mathbb{F}_q$-rational points. The known upper bound for genus 18 over $\mathbb{F}_5$ is 51. So unfortunately our result is just below $51/\sqrt{2}$, and falls outside the criterion of `manypoints.org` for relevance of new lower bounds. For characteristics 3 and 5 and some genera we found results with an amount of rational points within the upper bound divided by $\sqrt{2}$. But this is only in cases where already input on `manypoints.org` is with an explicit curve with an higher amount of rational points. For all our other results the number of rational points is farther away from the known upper bound divided by $\sqrt{2}$.

In general our curves have three times the amount of rational point of the starting curve. For the genus we have $g(C_2) = 3g(C_1) - 2 + \frac{1}{2}\sum_{Q \in C_2}(e_Q - 1)$. The last term is approximately the number of rational points on the starting curve, but sometimes 2 or 4 less or till 8 more. We calculated the bound $g(C_2) \leq 3g(C_1) + \deg(D) + 3\deg(E_{is}) - 3$. In general for curves of higher genus or over fields with higher cardinality, our results are relatively further away from the Hasse-Weil-Serre upper bound. This is because for higher characteristic, the number of rational points is bigger relative to the genus and in our construction, the number of points on the starting curve adds to the genus of the resulting curve via the ramification term.

So the part of our goal to add some new results to the table, is not achieved, but this does not mean that our project is useless. It shows how such a method, using coverings, could be used and shows that it is really difficult to get very good results with this method, but really easy to get near to good results. It is interesting that, contrary to the approach of most mathematicians working on such curves, without the use of class-field theory we can so easily get close to relevant results.

5.2. **Improvements.**

There are several ways in which our project could be improved or extended.

Firstly, we were not able to run the program for all possible curves, partly due to restricted time and partly due to the limited usage of memory for the student version of magma. It is possible that for other input values the program will give relevant results. For example, for $i \geq 6$, MAGMA gave a memory error in nearly all cases. We tried mostly only starting curves with a maximal number of rational points (known) for that genus, but it could be useful to use curves with less, but a threefold of, rational points.

Secondly, the code could be extended. We only tried divisors that were built up from one of the degree-i places times the threefold k (minus the rational points). But it is well possible to use combinations of more places, even of different degree. Besides that, we (hardly) only used the extension $T^3 - T - r$, but maybe extensions of degree two, four or even higher would work. For example, $T^4 - T - r$ might work. In these cases we have to look again how to make a divisor, because the calculations for the ramification index resulting in the threefold k depend on the degree of the extension. It is also possible to vary the polynomial keeping the degree constant, for example $a \cdot T^3 - b \cdot T - r$, with $a, b \in \mathbb{Z}$.

Thirdly, we did not optimize our program. Maybe it can be made a bit shorter. Additionally, the amount of required computer memory or the number of calculations could be reduced. It is also possible to make it a function which asks for input instead of a code in which we should change the input in different lines.

References

[Age16] U.S. National Security Agency. Commercial national security algorithm suite and quantum computing faq, 1 2016. https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf.

[Mur10] V. Kumar Murty. Algebraic curves and cryptography. *Fields Institute Communications*, 58, 2010. American Mathematical Society, Providence, RI.

[Ser85] Jean-Pierre Serre. Rational points on curves over finite fields. Unpublished notes by F.Q. Gouvêa of lectures at Harvard., 1985.

[Sil09] Joseph H. Silverman. *The artithmetic of elliptic curves. Graduate Texts in Mathematics 106.* Springer-Verlag, New York, 2 edition, 2009.

[Soo13] Muhammad Afzal Soomro. *Algebraic curves over finite fields.* PhD thesis, University of Groningen, 7 2013. ISBN 9789036762694 (printed version), ISBN 9789036762687 (electronic version).

[Sta] James Stankewicz. The riemann-roch theorem. pages 1–11. www.stankewicz.net/Riemann-Roch.pdf.

[Top03] Jaap Top. Curves of genus 3 over small finite fields. *Indag. Math. (N.S.)*, 2(14):275–283, 2003.

[TVN10] Michael Tsfasman, Serge Vladut, and Dmitry Nogin. Algebraic geometric codes: basic notions. *Mathematical Surveys and Monographs*, 139, 2010. American Mathematical Society, Providence, RI.

[vdGHLR09] Gerard van der Geer, Everett W. Howe, Kristin E. Lauter, and Christophe Ritzenthaler. Tables of curves with many points. 2009. http://www.manypoints.org, Retrieved [14-05-2018].

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 2(4):521–560, 1969.

6. Appendices

6.1. **MAGMA-code.** Final code for cases where the function field of the curve is made in two steps, so with $f1$ and $f2$ instead of f on line 2, 7 to 11 and 32:

```
1  //Input: p, f1, f2, max i.
2  //Output: p, Genus(C2), #Places(C2), f1, f2, genus(C1) i, s, k, r
3
4  p:=7;
5  K<x>:=FunctionField(GF(p));
6  PK<Y>:=PolynomialRing(K);
7  f1:= Y^2-( (x^2 + 4) * (x^3 + 2*x^2 + 2) );
8  K1<y>:=ext<K|f1>;
9  PK1<Z>:=PolynomialRing(K1);
10 f2:=Z^2-(( x^2 + 4) * (x^3 + 4*x^2 + 6*x + 1));
11 C1<z>:=ext<K1|f2>;
12 Q:=Places(C1,1);
13 D:=&+Q;
14 Sd:=#Q;
15 for i:=2 to 4 do
16 ming:=100;
17 k:=3*Ceiling(Ceiling(Sd/3)/i);
18 for s:=1 to #Places(C1,i) do
19 Eis:=Places(C1,i)[s];
20 V, phi:=RiemannRochSpace(k*Eis-D);
21 dimv:=Dimension(V);
22 if dimv ne 0 then
23 W, ksi:=RiemannRochSpace((k-1)*Eis-D);
24 if dimv ne Dimension(W) then
25 PC1<T>:=PolynomialRing(C1);
26 for v in V do
27 r:=phi(v);
28 if IsIrreducible(T^3-T-r) then
29 C2<u>:=ext<C1|T^3-T-r>;
30 if Genus(C2) lt ming then
31 ming:=Genus(C2);
32 print p, Genus(C2), #Places(C2,1), f1, f2, Genus(C1), i, s, k, r;
33 end if;
34 end if;
35 end for;
36 end if;
37 end if;
38 end for;
39 end for;
```

6.2. **Tables with results.** For all (or sometimes the best) curves we found, the output of the code is given, sorted to genus $g(C_2)$ of the resulting curve and cardinality q of the base field $\mathbb{F}_q$. For the sake of readability, we do not put the functions r in the table. Our best results are marked orange. (Though most of the theory and calculations do not hold for $\mathbb{F}_3$, we also applied the code to some curves over $\mathbb{F}_3$ to see what happens.)

Characteristic

Genus	3	5	7	11	13	17	19	25
12		5 12 30 Y^2 + 4*x^3 + 2*x, 1 5 1 3						
13		5 13 30 Y^2 + 4*x^3 + 2*x, 1 2 1 6						
13		5 13 30 Y^2 + 4*x^3 + 2*x, 1 4 1 3						
14	3 14 24 Y^2 + 2*x^6 + 2*x^4 + 2*x^2 + 2, 2 2 1 6	5 14 30 Y^2 + 4*x^3 + 2*x, 1 5 1 3						
14		5 14 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 2 5 6						
15		5 15 30 Y^2 + 4*x^3 + 2*x, 1 6 1 3	7 15 39 Y^2 + 6*x^3 + 4, 1 2 1 9					
15			7 15 39 Y^2 + 6*x^3 + 4, 1 6 1 3					
16	3 16 24 Y^2 + 2*x^6 + 2*x^4 + 2*x^2 + 2, 2 4 1 3	5 16 30 Y^2 + 4*x^3 + 2*x, 1 5 1 3	7 16 39 Y^2 + 6*x^3 + 4, 1 5 1 3					
16	3 16 24 Y^2 + 2*x^6 + 2*x^4 + 2*x^2 + 2, 2 6 9 3	5 16 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 2 5 6						
16		5 16 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 4 1 3						
17		5 17 30 Y^2 + 4*x^3 + 2*x, 1 3 1 6	7 17 39 Y^2 + 6*x^3 + 4, 1 2 1 9					
17		5 17 30 Y^2 + 4*x^3 + 2*x, 1 6 1 3	7 17 39 Y^2 + 6*x^3 + 4, 1 6 1 3					
17		5 17 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 5 17 3						
18		5 18 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 3 1 6						
18		5 18 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 6 1 3						
19	3 19 24 Y^2 + 2*x^6 + 2*x^4 + 2*x^2 + 2, 2 5 1 3	5 19 30 Y^2 + 4*x^3 + 2*x, 1 3 1 6	7 19 39 Y^2 + 6*x^3 + 4, 1 2 1 9					
19		5 19 30 Y^2 + 4*x^3 + 2*x, 1 6 1 3	7 19 39 Y^2 + 6*x^3 + 4, 1 6 1 3					
19		5 19 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 5 1 3						
20		5 20 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 3 1 6	7 20 48 Y^2 + 6*x^6 + 6, 2 3 5 6					
20		5 20 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 6 2 3	7 20 48 Y^2 + 6*x^6 + 6, 2 6 1 3					
21		5 21 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 7 3 3	7 21 39 Y^2 + 6*x^3 + 4, 1 4 1 6					
22	3 22 24 Y^2 + 2*x^6 + 2*x^4 + 2*x^2 + 2, 2 6 1 3	5 22 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 3 1 6	7 22 48 Y^2 + 6*x^6 + 6, 2 2 1 9					
22		5 22 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 6 1 3	7 22 48 Y^2 + 6*x^6 + 6, 2 6 1 3					
23		5 23 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 7 1 3						
24		5 24 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 8 1000 3	7 24 48 Y^2 + 6*x^6 + 6, 2 4 1 6					
25	3 25 30 Y^3 + 2*Y + 2*x^4 + x^2, 3 3 1 6	5 25 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 7 1 3	7 25 39 Y^2 + 6*x^3 + 4, 1 4 1 6					
26		5 26 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 8 1000 3	7 26 48 Y^2 + 6*x^6 + 6, 2 4 1 6					
27		5 27 48 Y^4 + x^4 + 3, 3 4 1 6					19 27 84 Y^2 + 18*x^3 + 11, 1 2 5 15	
28	3 28 36 (x^4 + 2*x^2 + 1)*Y^3 + (2*x^4 + x^2 + 2)*Y + 2*x^3 + x, 4 6 1 3	5 28 36 Y^2 + 4*x^6 + x^4 + 2*x^2 + 4, 2 8 1000 3	7 28 48 Y^2 + 6*x^6 + 6, 2 4 1 6	5*x^4 + 5*x^2 + 10, 2 2 3 12 11 28 72 Y^2 + 10*x^6 + 5*x^4 + 5*x^2 + 10, 2 3 3 9				
29				11 29 72 Y^2 + 10*x^6 + 5*x^4 + 5*x^2 + 10, 2 3 3 9		17 29 78 Y^2 + 16*x^3 + 14*x, 1 2 1 15	19 29 84 Y^2 + 18*x^3 + 11, 1 2 1 15	
30			7 30 48 Y^2 + 6*x^6 + 6, 2 5 1 6					
31	3 31 36 (x^4 + 2*x^2 + 1)*Y^3 + (2*x^4 + x^2 + 2)*Y + 2*x^3 + x, 4 7 264 3	5 31 48 Y^4 + x^4 + 3, 3 4 1 6		11 31 72 Y^2 + 10*x^6 + 5*x^4 + 5*x^2 + 10, 2 3 1 9		17 31 78 Y^2 + 16*x^3 + 14*x, 1 2 1 15	19 31 84 Y^2 + 18*x^3 + 11, 1 2 1 15 19 31 84 Y^2 + 18*x^3 + 11, 1 5 1 6	
32			7 32 48 Y^2 + 6*x^6 + 6, 2 5 1 6					
33							19 33 84 Y^2 + 18*x^3 + 11, 1 4 1 9	
34	3 34 36 (x^4 + 2*x^2 + 1)*Y^3 + (2*x^4 + x^2 + 2)*Y + 2*x^3 + x, 4 8 1 3		7 34 48 Y^2 + 6*x^6 + 6, 2 5 1 6					
36						17 36 96 Y^2 + 16*x^6 + 16*x^4 + 6*x^2 + 9, 2 4 1 9	19 36 108 Y^2 + 18*x^6 + 4*x^4 + 4*x^2 + 18, 2 4 7 9	
37	3 37 36 (x^4 + 2*x^2 + 1)*Y^3 + (2*x^4 + x^2 + 2)*Y + 2*x^3 + x, 4 9 1 3	5 37 60 Y^2 + 2*x^4 + 4, Z^2 + 3*x^4 + 2*x^3 + 3*x^2 + 2*x + 4, 5 2 1 12		11 37 84 Y^4 + (6*x^2 + 8)*Y^2 + x^4 + 8*x^2 + 1, 3 2 3 15			19 37 84 Y^2 + 18*x^3 + 11, 1 3 1 12	25 37 108 Y^2 + 4*x^3 + 4, 1 2 1 18
37		5 37 60 Y^2 + 2*x^4 + 4, Z^2 + 3*x^4 + 2*x^3 + 3*x^2 + 2*x + 4, 5 4 5 6		11 37 84 Y^4 + (6*x^2 + 8)*Y^2 + x^4 + 8*x^2 + 1, 3 5 18 6				
38						17 38 96 Y^2 + 16*x^6 + 16*x^4 + 6*x^2 + 9, 2 2 1 18 17 38 96 Y^2 + 16*x^6 + 16*x^4 + 6*x^2 + 9, 2 4 1 9		
40	3 40 36 (x^4 + 2*x^2 + 1)*Y^3 + (2*x^4 + x^2 + 2)*Y + 2*x^3 + x, 4 10 1 3	5 40 60 Y^2 + 2*x^4 + 4, Z^2 + 3*x^4 + 2*x^3 + 3*x^2 + 2*x + 4, 5 3 2 9				17 40 96 Y^2 + 16*x^6 + 16*x^4 + 6*x^2 + 9, 2 2 1 18	19 40 108 Y^2 + 18*x^6 + 4*x^4 + 4*x^2 + 18, 2 2 1 18	

17 40 96 Y^2 + 16*x^6 + 16*x^4 + 6*x^2 + 9, 2 4 1 9

19 40 108 Y^2 + 18*x^6 + 4*x^4 + 4*x^2 + 18, 2 4 1 9

40

5 41 60 Y^2 + 2*x^4 + 4, Z^2 + 3*x^4 + 2*x^3 + 3*x^2 + 2*x + 4, 5 5 1 6

41

7 43 78 Y^3 + 3*x^2 + 3*x + 2, Z^2 + 5*x^4 + 6*x^3 + x + 1, 5 5 7 6

11 43 84 Y^4 + (6*x^2 + 8)*Y^2 + x^4 + 8*x^2 + 1, 3 3 1 12

3 43 36 (x^4 + 2*x^2 + 1)*Y^3 + (2*x^4 + x^2 + 2)*Y + 2*x^3 + x, 4 11 1 3

43

11 43 84 Y^4 + (6*x^2 + 8)*Y^2 + x^4 + 8*x^2 + 1, 3 4 1 9

43

7 49 78 Y^3 + 3*x^2 + 3*x + 2, Z^2 + 5*x^4 + 6*x^3 + x + 1, 5 4 1 9

49

7 52 84 Y^2 + 6*x^5 + 5*x^4 + 3*x^3 + 4*x^2 + 6, Z^2 + 6*x^5 + 3*x^4 + 4*x^3 + 4*x^2 + 4*x + 3, 6 3 1 12

13 52 114 Y^2 + 12*x^3 + 9, Z^2 + 12*x^3 + 12*x^2 + 4*x + , 4 2 1 21

52

13 52 114 (x^4 + 7)*Y^4 + x^3*Y^3 + 5*x*Y + 7*x^4, 4 2 7 21

52

11 55 111 Y^5 + x^3*Y^3 + 4*x^2*Y^2 + 7*x*Y + x^5 + 6, 5 2 1 21,

13 55 114 (x^4 + 7)*Y^4 + x^3*Y^3 + 5*x*Y + 7*x^4, 4 3 1 15

55

11 58 111 Y^5 + x^3*Y^3 + 4*x^2*Y^2 + 7*x*Y + x^5 + 6, 5 3 1 15

13 58 114 (x^4 + 7)*Y^4 + x^3*Y^3 + 5*x*Y + 7*x^4, 4 4 1 12

58

11 58 111 Y^5 + x^3*Y^3 + 4*x^2*Y^2 + 7*x*Y + x^5 + 6, 5 5 1 9

58

11 59 111 Y^5 + x^3*Y^3 + 4*x^2*Y^2 + 7*x*Y + x^5 + 6, 5 4 1 12

59

11 61 111 Y^5 + x^3*Y^3 + 4*x^2*Y^2 + 7*x*Y + x^5 + 6, 5 4 1 12

61