

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux


Floris VERMEULEN

Curves of fixed gonality with many rational points

Tome 35, n° 1 (2023), p. 135-149.

<https://doi.org/10.5802/jtnb.1240>

© Les auteurs, 2023.

 Cet article est mis à disposition selon les termes de la licence
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE.
<http://creativecommons.org/licenses/by-nd/4.0/fr/>



*Le Journal de Théorie des Nombres de Bordeaux est membre du
Centre Mersenne pour l'édition scientifique ouverte*

<http://www.centre-mersenne.org/>

e-ISSN : 2118-8572

Curves of fixed gonality with many rational points

par FLORIS VERMEULEN

RÉSUMÉ. Étant donné un entier $\gamma \geq 2$ et une puissance q d'un nombre premier impair, nous montrons que pour chaque genre g suffisamment grand, il existe une courbe C définie sur \mathbb{F}_q , non singulière, de genre g et de gonality γ , telle que son nombre de points rationnels est exactement $\gamma(q+1)$, c'est-à-dire le maximal possible, démontrant ainsi une conjecture récente de Faber–Grantham. Les méthodes que nous employons sont en lien avec l'étude des courbes sur les surfaces toriques et avec les travaux de Poonen sur les valeurs sans facteur carré de polynômes.

ABSTRACT. Given an integer $\gamma \geq 2$ and an odd prime power q we show that for every large genus g there exists a non-singular curve C defined over \mathbb{F}_q of genus g and gonality γ and with exactly $\gamma(q+1)$ \mathbb{F}_q -rational points. This is the maximal number of rational points possible. This answers a recent conjecture by Faber–Grantham. Our methods are based on curves on toric surfaces and Poonen's work on squarefree values of polynomials.

1. Introduction

In this article we study the maximal number of rational points on curves over finite fields. Curves will always be geometrically integral, but may be singular. Let q be a prime power and fix a positive integer g . Define $N_q(g)$ to be the maximal number of \mathbb{F}_q -rational points of a non-singular genus g curve defined over \mathbb{F}_q . The famous Weil bound yields that

$$N_q(g) \leq 2\sqrt{q}g + q + 1.$$

By work of Ihara [11] and later Vladut and Drinfeld [16], when g is large compared to q , this bound can be improved to $N_q(g) \leq (\sqrt{q} - 1 + o(1))g$ as $g \rightarrow \infty$. To find lower bounds on the quantity $N_q(g)$ one has to construct non-singular curves with many rational points. Many approaches have been developed to deal with this problem, and we refer to the introduction of [13] for an overview. By work of Elkies, Howe, Kresch, Poonen, Wetherell and

Manuscrit reçu le 4 novembre 2021, révisé le 5 décembre 2022, accepté le 14 décembre 2022.

Mathematics Subject Classification. 11G20, 14G05, 14G15, 14M25.

Mots-clés. Curves over finite fields, rational points, gonality, toric surfaces.

The author was partially supported by KU Leuven IF C14/17/083, and partially by F.W.O. Flanders (Belgium) with grant number 11F1921N.

Zieve [4], it is currently known that for every q there exists some constant c such that for every genus g

$$cg < N_q(g).$$

Now suppose that C is a curve over \mathbb{F}_q equipped with a degree γ map $C \rightarrow \mathbb{P}^1$, also defined over \mathbb{F}_q . Then since every \mathbb{F}_q -rational point of C must map to an \mathbb{F}_q -rational point of \mathbb{P}^1 we have

$$(1.1) \quad \#C(\mathbb{F}_q) \leq \gamma(q+1).$$

In particular, this is true when γ is equal to the gonality of C over \mathbb{F}_q . Recall that the *gonality* of a curve C is the minimal degree of a morphism defined over \mathbb{F}_q to \mathbb{P}^1 . For a positive integer γ , denote by $N_q(g, \gamma)$ the maximal number of \mathbb{F}_q -rational points on a non-singular genus g curve of gonality γ , defined over \mathbb{F}_q . By convention, if no such curve exists we put $N_q(g, \gamma) = -\infty$. In [8], van der Geer asks about the behaviour of this function $N_q(g, \gamma)$. Recently, this quantity has been studied for small q and g by Faber and Grantham in [5] and [6]. They conjecture that for fixed q, γ and g sufficiently large, we have $N_q(g, \gamma) = \gamma(q+1)$. We prove this conjecture in odd characteristic.

Theorem 1.1. *Let q be an odd prime power and fix a positive integer $\gamma \geq 2$. Then for all sufficiently large g , there exists a non-singular curve C defined over \mathbb{F}_q , of genus g and gonality γ , and with $\gamma(q+1)$ \mathbb{F}_q -rational points. In other words*

$$\lim_{g \rightarrow \infty} N_q(g, \gamma) = \gamma(q+1).$$

For the proof, we will use the theory of curves on toric surfaces. The idea is to construct the desired curve C inside a certain toric surface S . Such a method was introduced by Kresch, Wetherell and Zieve in [13] to construct non-singular curves over \mathbb{F}_q of every sufficiently large genus g with at least $c_q g^{1/3}$ \mathbb{F}_q -rational points, for some constant c_q depending on q . In our setting, we also want to control the gonality of C . It would be desirable if C would be smooth in the surface S . However, S has only roughly $(q+1)^2$ \mathbb{F}_q -rational points, so we cannot hope for this if γ is large compared to q . Instead, we construct C as a singular curve inside S . By carefully controlling the singularities of C , we are able to control both the rational points on C and the (geometric) genus of C . To do this we rely on work by Poonen [15] to make sure that a certain discriminant polynomial is squarefree. This is also where the condition that the characteristic is not 2 is needed.

In upcoming work together with Faber [7], we use another approach using class field theory to try to prove Theorem 1.1. In particular, we are able to

prove that for fixed q, γ , we have that

$$\limsup_{g \rightarrow \infty} N_q(g, \gamma) = \gamma(q + 1)$$

where one can assume that the resulting covers $C \rightarrow \mathbb{P}^1$ are all abelian. In particular this holds when q is even. Nevertheless, we also argue that abelian covers do not suffice to prove Theorem 1.1 in general.

2. Curves on toric surfaces

We will construct the desired curve having many rational points as a singular curve in a toric surface. This section contains the relevant background material. We refer the reader to [3] and [13, Sec. 3] for more information.

Let k be a perfect field and let $f \in k[t^{\pm 1}, y^{\pm 1}]$ be a Laurent polynomial. Write $f = \sum_{i,j} c_{i,j} t^i y^j$. Then the *Newton polygon* of f is defined to be

$$\Delta(f) = \text{conv}\{(i, j) \mid c_{i,j} \neq 0\} \subseteq \mathbb{R}^2,$$

where conv denotes the convex hull. If $\Delta \subseteq \mathbb{R}^2$ is any lattice polygon we denote by $\Delta^{(1)}$ the convex hull of its interior lattice points. Assume now that f is absolutely irreducible and let \tilde{C} be the non-singular projective model of the curve defined by $f = 0$ in the torus $(k^\times)^2$. There is a strong relation between the combinatorics of $\Delta(f)$ and the geometry of \tilde{C} . The first result in this direction, proven by Baker, is that the genus of \tilde{C} is bounded above by the number of interior lattice points of $\Delta(f)$, i.e.

$$g(\tilde{C}) \leq \#(\Delta(f)^{(1)} \cap \mathbb{Z}).$$

We will call this *Baker's bound*, see [1]. The quantity $\#(\Delta(f)^{(1)} \cap \mathbb{Z})$ has an interesting geometric interpretation. To explain, we introduce some toric geometry. Let Δ be a (2-dimensional) lattice polygon and consider the map

$$\phi : (k^\times)^2 \rightarrow \mathbb{P}^{\#(\Delta \cap \mathbb{Z}^2) - 1} : (t, y) \mapsto (t^i y^j)_{(i,j) \in \Delta \cap \mathbb{Z}^2}.$$

Define $S(\Delta)$ to be the closure of the image of ϕ , this is a toric surface. Its fan is obtained by taking all primitive inward facing normals of Δ . Denote the coordinates on $\mathbb{P}^{\#(\Delta \cap \mathbb{Z}^2) - 1}$ by $X_{i,j}$ for $(i, j) \in \Delta \cap \mathbb{Z}^2$. If $f = \sum_{i,j} c_{i,j} t^i y^j$ is an absolutely irreducible Laurent polynomial supported on Δ and each edge of Δ contains a lattice point from $\Delta(f)$ then the hyperplane section

$$\sum_{(i,j) \in \Delta} c_{i,j} X_{i,j} = 0$$

cuts out a curve C in $S(\Delta)$. This curve is automatically birationally equivalent to \tilde{C} by our assumptions. Then the quantity $\#(\Delta(f)^{(1)} \cap \mathbb{Z}^2)$ is the arithmetic genus $g_a(C)$ of the curve C , see [10] and [13, Lem. 3.4]. In particular, there is equality in Baker's bound if and only if C is non-singular in $S(\Delta)$.

Definition 2.1. Let $f \in k[t^{\pm 1}, y^{\pm 1}]$ be an absolutely irreducible Laurent polynomial and let $\Delta \subseteq \mathbb{R}^2$ be a lattice polygon. We say that f is a Δ -polynomial if

- (1) $\Delta(f) \subseteq \Delta$,
- (2) every edge of Δ contains a lattice point from $\Delta(f)$.

If moreover the genus of the curve defined by $f = 0$ is equal to the number of interior lattice points of Δ , then we call f Δ -toric.

By the remarks above, a Δ -polynomial f is Δ -toric if and only if C is non-singular in $S(\Delta)$.

Suppose that f is a Δ -polynomial for some lattice polygon Δ which is contained in the strip $\mathbb{R} \times [0, \gamma]$ for some positive integer γ . Then there is naturally a morphism $C \rightarrow \mathbb{P}^1$ of degree at most γ , obtained from the map

$$V(f) \subseteq (k^\times)^2 \rightarrow k^\times : (y, t) \mapsto t.$$

If Δ is not contained in any smaller horizontal strip of the form $\mathbb{R} \times [a, b]$ then this map has degree equal to γ .

Lemma 2.2. Let γ be a positive integer and let $0 = k_0 \leq k_1 < k_2 < \dots < k_\gamma$ be integers. Define $\ell_j = \sum_{i=0}^j k_i$ and let f be an absolutely irreducible Laurent polynomial over a field k with

$$\Delta(f) = \text{conv}\{(0, 0), (\ell_1, 1), (\ell_2, 2), \dots, (\ell_\gamma, \gamma), (m_0, 0), (m_1, 1), \dots, (m_\gamma, \gamma)\},$$

for certain integers $m_j > \ell_j$. Let $C \subseteq S(\Delta(f))$ be the curve defined by $f = 0$ in $S(\Delta(f))$ and let $\pi : C \rightarrow \mathbb{P}^1$ be the degree γ map as above. Then $\pi^{-1}(0)$ consists of γ distinct non-singular k -rational points.

Note that we are not saying anything about C being non-singular above other points of \mathbb{P}^1 . See also [13] for a similar argument to construct curves of a prescribed genus having many rational points. The shape of $\Delta(f)$ might look like figure 2.1. Note that the left side of this polygon consists of γ distinct line segments, each containing two lattice points.

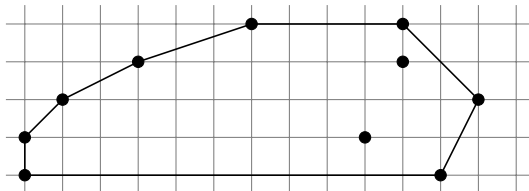


FIGURE 2.1. A typical Newton polygon arising from Lemma 2.2 with $\gamma = 4$. The indicated lattice points are the points (ℓ_i, i) and (m_i, i) .

Proof. The edges of $\Delta = \Delta(f)$ correspond precisely to the one-dimensional torus invariant divisors of $S(\Delta)$. The points above 0 of π are precisely the intersections of C with the torus invariant divisors corresponding to the edges on the left side of Δ . We consider $S(\Delta)$ as sitting in $\mathbb{P}^{\#(\Delta \cap \mathbb{Z}^2)-1}$ via the map ϕ as described above. Denote by $X_{i,j}$ the coordinates on $\mathbb{P}^{\#(\Delta \cap \mathbb{Z}^2)-1}$, where $(i, j) \in \Delta \cap \mathbb{Z}^2$.

Fix such an edge τ on the left side of Δ and note that it contains exactly two lattice points, say (ℓ_j, j) and $(\ell_{j+1}, j + 1)$. Let D be the corresponding torus invariant divisor on $S(\Delta)$. Then D is defined by taking $X_{i,j} = 0$ for $(i, j) \notin \tau$. Thus, on D , C is defined by the hyperplane section

$$aX_{\ell_j, j} + bX_{\ell_{j+1}, j+1} = 0$$

for certain $a, b \in k^\times$. Hence C contains exactly one k -rational point on D . Moreover, this point is not invariant under the torus action, since both $a, b \neq 0$. Since there are γ such edges on the left hand side of Δ , we conclude that $\pi^{-1}(0)$ consists of γ distinct k -rational points. The fact that these are all non-singular follows from the fact that π has degree γ . \square

3. Poonen's theorem

We recall here a theorem by Poonen on squarefree values of multivariate polynomials over $\mathbb{F}_q[t]$. Fix a prime power q . For a in $\mathbb{F}_q[t]$ define $|a| = \#(\mathbb{F}_q[t]/(a)) = q^{\deg a}$. For A a subset of $\mathbb{F}_q[t]^n$ and positive integers d_1, \dots, d_n define

$$\begin{aligned} A(d_1, \dots, d_n) &= \{(f_1, \dots, f_n) \in A \mid \deg f_i \leq d_i\}, \\ A(d_1, \dots, d_n)' &= \{(f_1, \dots, f_n) \in A \mid \deg f_i = d_i\}. \end{aligned}$$

In particular, $\mathbb{F}_q[t]^n(d_1, \dots, d_n)$ consists of all elements $(f_1, \dots, f_n) \in \mathbb{F}_q[t]^n$ with $\deg f_i \leq d_i$. We define the *density* of A to be

$$\mu(A) = \lim_{d_1, \dots, d_n \rightarrow \infty} \frac{\#A(d_1, \dots, d_n)}{\#\mathbb{F}_q[t]^n(d_1, \dots, d_n)} = \lim_{d_1, \dots, d_n \rightarrow \infty} \frac{\#A(d_1, \dots, d_n)}{q^{\sum_i (d_i+1)}},$$

if the limit exists. Here the limit means that for every $\varepsilon > 0$ there exists an M such that if $d_1, \dots, d_n \geq M$, then

$$\left| \frac{\#A(d_1, \dots, d_n)}{\#\mathbb{F}_q[t]^n(d_1, \dots, d_n)} - \mu(A) \right| \leq \varepsilon.$$

Then Poonen's theorem states the following.

Theorem 3.1 ([15]). *Let $F \in \mathbb{F}_q[t][x_1, \dots, x_n]$ be a polynomial which is squarefree when considered in $\mathbb{F}_q(t)[x_1, \dots, x_n]$. Let*

$$A = \{a \in \mathbb{F}_q[t]^n \mid F(a) \text{ is squarefree}\}.$$

Then $\mu(A)$ exists and is equal to $\prod_p (1 - c_p/|p|^{2n})$ where the product is over all non-zero primes p of $\mathbb{F}_q[t]$ and c_p is the number of solutions of $F(x) = 0$ in $\mathbb{F}_q[t]/(p^2)$. Moreover, $\mu(A) > 0$ if and only if $c_p < |p|^{2n}$ for all primes p .

This result implies the following for $A(d_1, \dots, d_n)'$.

Corollary 3.2. *Let $F \in \mathbb{F}_q[t][x_1, \dots, x_n]$ be a polynomial which is square-free when considered in $\mathbb{F}_q(t)[x_1, \dots, x_n]$. Let*

$$A = \{a \in \mathbb{F}_q[t]^n \mid F(a) \text{ is squarefree}\}.$$

Then

$$\lim_{d_i \rightarrow \infty} \frac{\#A(d_1, \dots, d_n)'}{q^{\sum_i d_i} (q-1)^n} = \mu(A).$$

Proof. The inclusion-exclusion principle gives that

$$\begin{aligned} & \#A(d_1, \dots, d_n)' \\ &= \#A(d_1, \dots, d_n) - \#A(d_1 - 1, d_2, \dots, d_n) - \#A(d_1, d_2 - 1, d_3, \dots, d_n) \\ & \quad - \dots + \#A(d_1 - 1, d_2 - 1, d_3, \dots, d_n) + \dots \pm \#A(d_1 - 1, \dots, d_n - 1). \end{aligned}$$

Dividing by $q^{\sum_i d_i} (q-1)^n$ and taking the limit $d_i \rightarrow \infty$ gives the desired statement. \square

4. Constructing curves with many points

In this section we prove Theorem 1.1. Let $\gamma \geq 2$ be the given gonality and let q be an odd prime power. Let g be a sufficiently large integer. We will construct a non-singular curve C over \mathbb{F}_q of gonality γ and of genus g with $\gamma(q+1)$ rational points. The proof proceeds along several steps, which we first outline.

- (1) Construct a family of polynomials in $\mathbb{F}_q[t, y]$ among which we look for a suitable defining equation.
- (2) Use Poonen's theorem to a certain discriminant polynomial. This allows us to ensure that the curve is non-singular above $\mathbb{A}^1(\overline{\mathbb{F}_q}) \setminus \mathbb{A}^1(\mathbb{F}_q)$.
- (3) Construct a good candidate Newton polygon for the polynomial having a prescribed number of interior lattice points. This will give us control over the genus as well as the points above $\infty \in \mathbb{P}^1$.
- (4) Construct the desired curve using the previous steps.
- (5) Check that the curve satisfies all required conditions: it is geometrically integral, non-singular, and has genus g , gonality γ and $\gamma(q+1)$ \mathbb{F}_q -rational points.

On $\mathbb{A}^1 \times \mathbb{P}^1$ write t for the coordinate on \mathbb{A}^1 and y, z for the coordinates on \mathbb{P}^1 . We will look for a curve which is defined in $\mathbb{A}^1 \times \mathbb{P}^1$ by an equation

$$(4.1) \quad f(t, y, z) = \sum_{i=0}^{\gamma} f_i(t) y^i z^{\gamma-i} = 0,$$

where $f_i \in \mathbb{F}_q[t]$. We will also write $f \in \mathbb{F}_q[t, y]$ for the dehomogenized polynomial $f(t, y, 1)$. Let Δ be the convex hull of $\Delta(f)$ together with $(0, 0)$ and $(0, \gamma)$. We let C be the curve defined by $f = 0$ inside the surface $S(\Delta) = S$. Let us assume that $f_0, f_\gamma \neq 0$. Then projection onto t gives a degree γ morphism $\pi : C \rightarrow \mathbb{P}^1$, which extends to a morphism $S \rightarrow \mathbb{P}^1$. Inside S , there is naturally a copy of $\mathbb{A}^1 \times \mathbb{P}^1$ obtained as the union of the torus and all torus invariant divisors except those corresponding to edges on the right hand side of Δ . Depending on the f_i , C might not be geometrically integral. If C is geometrically integral however, we denote by \tilde{C} the non-singular model of C . The map π naturally induces a degree γ map $\tilde{C} \rightarrow \mathbb{P}^1$, which we also denote by π .

Step 1. We first ensure that \tilde{C} has γ distinct non-singular \mathbb{F}_q -rational points above every point of $\mathbb{A}^1(\mathbb{F}_q)$. To do this, we will require the f_i to be of a specific form so that we can apply Lemma 2.2.

We take integers $0 = k_0 \leq k_1 < k_2 < \dots < k_\gamma$, e.g. $k_i = i - 1$ for $i > 0$ will do, and put $\ell_j = \sum_{i=0}^j k_i$ and $L(\ell) = \sum_{j=1}^{\gamma-1} \ell_j$. Define $\alpha = t^\ell - t = \prod_{a \in \mathbb{F}_q} (t - a) \in \mathbb{F}_q[t]$. We would like to take every f_i of the form

$$\alpha(t)^{\ell_i} (1 + \alpha(t) g_i(t)),$$

for some polynomials $g_i \in \mathbb{F}_q[t]$. Indeed, in that case we could apply Lemma 2.2 above every point of $\mathbb{A}^1(\mathbb{F}_q)$. However, to make sure that f is absolutely irreducible we require something more. We fix an irreducible polynomial $\beta \in \mathbb{F}_q[t]$ of degree 2 (any degree > 1 will do). Then define

$$f_i = \alpha(t)^{\ell_i} \beta(t)^{\delta_i} (1 + \alpha(t) \beta(t)^{\delta'_i} g_i(t)),$$

where $\delta_i = 1$ if $i < \gamma$ and 0 if $i = \gamma$, and $\delta'_i = 1$ if $i = 0, \gamma$ and 0 if $i \neq 0, \gamma$. Note that then f is automatically a Δ -polynomial, and also an Eisenstein polynomial with respect to β . We will want to pick the g_i in such a way that the resulting curve \tilde{C} has all of the desired properties.

Step 2. To ensure that the curve is non-singular at all points except above $\mathbb{A}^1(\mathbb{F}_q)$, we make sure that a certain discriminant polynomial is squarefree. The following lemma tells us that the generic discriminant polynomial is squarefree. A proof can be found at [2], but let us include it for completeness sake. (See also [9, p. 15] for a more general result in characteristic zero.)

Lemma 4.1. *Let k be a field of characteristic not 2 and γ a positive integer and let*

$$D = \operatorname{disc}_Y \left(\sum_{i=0}^{\gamma} x_i Y^i \right) \in k[x_0, \dots, x_\gamma]$$

be the generic discriminant polynomial over k . Then D is irreducible in $k[x_0, \dots, x_\gamma]$, so in particular it is squarefree.

Proof. Consider the generic polynomial $p = Y^\gamma - s_1 Y^{\gamma-1} + \dots + (-1)^\gamma s_\gamma \in k[s_1, \dots, s_\gamma][Y]$, whose coefficients are the elementary symmetric polynomials s_i in the roots r_1, \dots, r_γ of p . Recall that the extension

$$k(r_1, \dots, r_\gamma)/k(s_1, \dots, s_\gamma)$$

is Galois with Galois group the symmetric group S_γ .

It is enough to prove that the discriminant polynomial

$$D(s_1, \dots, s_\gamma) = \prod_{i < j} (r_i - r_j)^2$$

is irreducible in $k[s_1, \dots, s_\gamma]$. So assume towards a contradiction that D factors as $D_1 D_2$, for some non-constant polynomials $D_1, D_2 \in k[s_1, \dots, s_\gamma]$. By unique factorization there exist for every pair $i < j$ a power $\varepsilon_{i,j} \in \{0, 1, 2\}$ such that $D_1 = c \prod_{i < j} (r_i - r_j)^{\varepsilon_{i,j}}$, for some $c \in k^\times$. By Galois theory, one sees that $\varepsilon_{i,j} \leq \varepsilon_{i',j'}$ for every two pairs $i < j, i' < j'$. Hence we conclude that

$$D_1 = c \prod_{i < j} (r_i - r_j).$$

But now, since k has characteristic not 2, switching r_1 and r_2 and keeping the other r_i fixed changes the sign of D_1 , implying that D_1 does not have coefficients in $k[s_1, \dots, s_\gamma]$. This is a contradiction, and we conclude that D is irreducible. \square

As a side remark, note that the above proof also shows that in characteristic 2, the generic discriminant polynomial is the square of an irreducible polynomial.

Define

$$H = \sum_{i=0}^{\gamma} \alpha(t)^{\ell_i} \beta(t)^{\delta_i} (1 + \alpha(t)\beta(t)^{\delta'_i} x_i) Y^i \in \mathbb{F}_q[t][x_0, \dots, x_\gamma, Y],$$

and

$$F_1 = \operatorname{disc}_Y (H(x, Y)) \in \mathbb{F}_q[t][x_0, \dots, x_\gamma].$$

Note that this is simply the discriminant of f with respect to y , where we consider the g_i as variables.

Lemma 4.2. *We have that $\alpha^{2L(\ell)} \cdot \beta^{\gamma-1}$ divides F_1 in $\mathbb{F}_q[t][x_0, \dots, x_\gamma]$.*

Proof. Let us first prove that $\alpha^{2L(\ell)}$ divides F_1 . Fix a degree one prime p of $\mathbb{F}_q[t]$, i.e. a divisor of α , and denote by v_p the valuation corresponding to p on $\mathbb{F}_q(t)$. We work in some fixed algebraic closure $\overline{\mathbb{F}_q(t, x_0, \dots, x_\gamma)}$ of $\mathbb{F}_q(t, x_0, \dots, x_\gamma)$ and denote by v_p also any extension of v_p to this field, where we require that $v_p(x_i) \geq 0$ for any i . Now let r_1, \dots, r_γ be the roots of the polynomial H in $\overline{\mathbb{F}_q(t, x_0, \dots, x_\gamma)}$. By looking at the slopes of the Newton polygon of this polynomial with respect to the valuation v_p , see e.g. [12, p. 97], we may assume, after reordering, that $v_p(r_i) = -k_i$. Hence we have that

$$v_p(F_1) = v_p \left(f_\gamma^{2\gamma-2} \prod_{i < j} (r_i - r_j)^2 \right) = v_p(f_\gamma^{2\gamma-2}) - \sum_{i < j} k_j = 2L(\ell),$$

and we conclude that $\alpha^{2L(\ell)}$ divides F_1 . In fact, our argument shows that this is the exact power of α dividing F_1 .

We use a similar argument with respect to β to show that $\beta^{\gamma-1}$ divides F_1 . Let p be a linear factor of β in $\overline{\mathbb{F}_q[t]}$ and let v_p be an extension of the valuation corresponding to p on $\overline{F\mathbb{F}_q(t)}$ to the field $\overline{\mathbb{F}_q(t, x_0, \dots, x_\gamma)}$, with $v_p(x_i) \geq 0$ for any i . Let r be any root of H in this field. Since H is an Eisenstein polynomial with respect to β , we have by [12, p. 66] that $v_p(r) = 1/\gamma$. Then $F_1 = \pm f_\gamma^{\gamma-2} N((\partial_Y H)(r))$, where N denotes the norm map from $\overline{\mathbb{F}_q(t, x_0, \dots, x_\gamma)}$ to $\mathbb{F}_q(t, x_0, \dots, x_\gamma)$. Now we have that

$$\partial_Y H(r) = \gamma f_\gamma r^{\gamma-1} + (\gamma-1) f_{\gamma-1} r^{\gamma-2} + \dots + f_1,$$

and the terms here satisfy $v_p(i f_i r^{i-1}) \geq (\gamma + i - 1)/\gamma$ for $i = 1, \dots, \gamma - 1$. Therefore, we certainly have that $\beta^{\gamma-1}$ will divide F_1 . \square

Now define

$$F(x_0, \dots, x_\gamma) = \frac{F_1(x_0, \dots, x_\gamma)}{\alpha(t)^{2L(\ell)} \beta(t)^{\gamma-1}} \in \mathbb{F}_q[t][x_0, \dots, x_\gamma].$$

We will apply Poonen's theorem to this polynomial. The highest degree part of F_1 is equal to

$$\text{disc}_Y \left(\sum_{i=0}^{\gamma} \alpha(t)^{\ell_i+1} \beta(t)^{\delta_i+\delta'_i} x_i Y^i \right).$$

By Lemma 4.1 the generic discriminant polynomial $\text{disc}_Y(\sum_{i=0}^{\gamma} x_i Y^i)$ is squarefree when considered in $\mathbb{F}_q(t)[x_0, \dots, x_\gamma]$, and so we conclude the same about F_1 . Hence, also F is squarefree in $\mathbb{F}_q(t)[x_0, \dots, x_\gamma]$. Define

$$A = \{(g_i)_i \in \mathbb{F}_q[t]^{\gamma+1} \mid F((g_i)_i) \text{ squarefree}\}.$$

Then Poonen's theorem 3.1 states that the density $\mu(A)$ exists, and is equal to the product of $(1 - c_p/|p|^{2\gamma+2})$ over all non-zero primes p of $\mathbb{F}_q[t]$, where

c_p is the number of zeroes of F over $\mathbb{F}_q[t]/(p^2)$. We need to show that $\mu(A) > 0$.

Lemma 4.3. *We have that $\mu(A) > 0$.*

Proof. We have to prove that $c_p < |p|^{2\gamma+2}$ for all primes p of $\mathbb{F}_q[t]$.

If p is a prime of degree 1, fix any values of g_i and let r_1, \dots, r_γ be the roots of $f = 0$ in $\overline{\mathbb{F}_q}(t, y)$. Let v_p be an extension of the valuation corresponding to p to this field with $v_p(y) \geq 0$ (note that this is not the same valuation v_p as above). Then by a similar argument as above, we have

$$v_p(F(g_0, \dots, g_\gamma)) = v_p(F_1(g_0, \dots, g_\gamma)) - 2L(\ell) = 0,$$

so that F cannot even have any zeroes modulo p . Hence $c_p = 0$. For $p = \beta$, take g_0, \dots, g_γ such that $v_\beta(f_1) = 1$. Then reasoning as above, one obtains that

$$v_\beta(F(g_0, \dots, g_\gamma)) = v_\beta(F_1(g_0, \dots, g_\gamma)) - (\gamma - 1) = \begin{cases} 0 & \text{if } \text{char}(\mathbb{F}_q) \nmid \gamma \\ 1 & \text{if } \text{char}(\mathbb{F}_q) \mid \gamma. \end{cases}$$

Hence, we see that $F_1(g_0, \dots, g_\gamma)$ is non-zero modulo β^2 and so $c_\beta < |\beta|^{2\gamma+2}$. If p is another prime, not of degree 1 or equal to β , then α and β are both invertible modulo p . Then $F \bmod p$ is obtained from the generic discriminant polynomial $\text{disc}_Y(\sum_{i=0}^\gamma x_i Y^i) \bmod p$ by linear substitution in the x_i . Since there exist squarefree polynomials of every degree over every finite field, we see that $c_p < |p|^{2\gamma+2}$. We conclude that $\mu(A) > 0$, as desired. \square

Step 3. We will want to take $(g_i)_i \in A(d_0, \dots, d_\gamma)'$ for suitable integers d_i (depending on the genus g). Note that these d_i also determine the Newton polygon of f . In particular, they also determine Δ , which we recall is the convex hull of $\Delta(f)$ together with $(0, 0)$ and $(0, \gamma)$. So we now look for a good candidate for Δ , which will give us control over the arithmetic genus of the curve and moreover ensures that the curve is non-singular above ∞ .

The choice of Δ will depend on $g \bmod \gamma - 1$. So fix some residue class $g \equiv n \bmod \gamma - 1$ of genera with $n = 0, \dots, \gamma - 2$ and put $m = n + qL(\ell)$. Take $k'_2 > \gamma - 3$ such that

$$k'_2 \equiv \sum_{j=1}^{\gamma-3} j^2 - m \pmod{\gamma - 1}.$$

Define $k'_i = \gamma - i$ for $i = 3, \dots, \gamma$ and put $k'_1 = k'_2 + 1$. Note that

$$k'_1 > k'_2 > \dots > k'_\gamma, \quad \sum_j k'_j \geq 0, \quad \text{and} \quad \sum_{j=1}^{\gamma-1} (\gamma - j)k'_j \equiv m \pmod{\gamma - 1}.$$

Define $\ell'_j = \sum_{i=1}^j k'_i$, $\ell'_0 = 0$ and for $r \geq 0$ a positive integer consider the lattice polygon

$$\Delta_r = \text{conv}\{(0, 0), (0, \gamma), (r, \gamma), (r + \ell'_1, \gamma - 1), (r + \ell'_2, \gamma - 2), \dots, (r + \ell'_\gamma, 0)\},$$

see Figure 4.1. Our choice of integers k'_j guarantees that the number of interior lattice points of Δ_r is congruent to m modulo $\gamma - 1$. Moreover, Δ_{r+1} has exactly $\gamma - 1$ interior lattice points more than Δ_r . Thus, for every sufficiently large integer s there is some r such that this polygon Δ_r has exactly $n + qL(\ell) + s(\gamma - 1)$ interior lattice points. Note also that by our choice of k'_i , the right hand side of Δ consists of γ line segments, each containing exactly two lattice points.

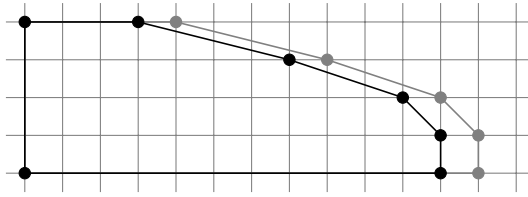


FIGURE 4.1. The typical shape for the lattice polygons Δ_r constructed above (here $\gamma = 4$). The polygon Δ_{r+1} is pictured in grey.

Step 4. We now construct the desired polynomial f . By Corollary 3.2 there exists some M such that if $d_0, \dots, d_\gamma \geq M$ then

$$A(d_0, \dots, d_\gamma)' \neq \emptyset.$$

Let g be the desired genus for our curve and assume that $g \equiv n \pmod{\gamma - 1}$. If g is sufficiently large, then there exists some positive integer r such that the polygon $\Delta = \Delta_r$ constructed in the previous step has exactly $g + qL(\ell)$ interior lattice points. We will construct f in such a way that it will be a Δ -polynomial, see Figure 4.2 for the relation between Δ and $\Delta(f)$. Recall that $\deg \beta = 2$ and define for every $i \in \{0, \dots, \gamma\}$

$$d_i = r + \ell'_{\gamma-i} - q(\ell_i + 1) - 2(\delta_i + \delta'_i).$$

This will be the desired degree of g_i . If g is sufficiently large, then so is r and hence $d_i \geq M$ for all i . Therefore, there exists some element

$$(g_0, \dots, g_\gamma) \in A(d_0, \dots, d_\gamma)'.$$

Let f be the polynomial as constructed above from the $(g_i)_i$, namely we put

$$f_i = \alpha(t)^{\ell_i} \beta(t)^{\delta_i} (1 + \alpha(t)\beta(t)^{\delta'_i} g_i(t)) \in \mathbb{F}_q[t],$$

and define $f = \sum_{i=0}^{\gamma} f_i(t)y^i \in \mathbb{F}_q[t, y]$. Let $C = V(f)$ inside $S = S(\Delta)$. We claim that this curve is as desired. Namely, f is a Δ -polynomial which is

absolutely irreducible and the non-singular model of C is of genus g with $\gamma(q + 1)$ \mathbb{F}_q -rational points and gonality γ .

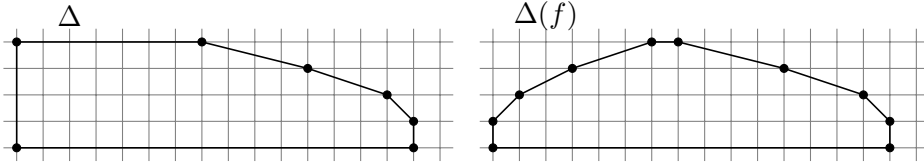


FIGURE 4.2. Typical lattice polygons $\Delta = \Delta_r$ and $\Delta(f)$ in the construction. Note that the right hand sides of both polygons are the same.

Step 5. We first prove that f is absolutely irreducible and that C is smooth above $\mathbb{A}^1(\overline{\mathbb{F}}_q) \setminus \mathbb{A}^1(\mathbb{F}_q)$. We need a general lemma.

Lemma 4.4. *Let k be a field and let $f = \sum_{i=0}^{\gamma} f_i(t)y^i z^{\gamma-i} \in k[t, y, z]$ be a polynomial over k . Let $C = V(f)$ be the curve determined by $f = 0$ inside $\mathbb{A}^1 \times \mathbb{P}^1$, where the coordinate on \mathbb{A}^1 is t and the coordinates on \mathbb{P}^1 are y, z . If C has a singularity above a non-zero prime p of $k[t]$ then p^2 divides $\text{disc}_y f(t, y, 1)$.*

Proof. By invariance of the discriminant under translations and taking reciprocals we can assume that C has a singularity at $t = a, y = 0, z = 1$, where $p(a) = 0$. Here we have to move to some algebraic closure of k but this is not a problem. Now, being a singularity means that

$$f(a, 0) = f_0(a) = 0, (\partial_t f)(a, 0) = f'_0(a) = 0, (\partial_y f)(a, 0) = f_1(a) = 0.$$

By computing the discriminant from the Sylvester matrix of $f, \partial_y f$, one sees that $(t - a)^2$ will divide $\text{disc}_y f(t, y)$. Since the original f is defined over k , this situation occurs for any root a of p and so p^2 will divide $\text{disc}_y f(t, y)$. \square

The condition of having squarefree discriminant at a prime p is stronger than being non-singular. Geometrically, having squarefree discriminant means that all ramification types of the map $C \rightarrow \mathbb{A}^1$ are of the form $(2, 1, \dots, 1)$ or $(1, \dots, 1)$, by [14, Thm. III.2.6].

Lemma 4.5. *The polynomial f is absolutely irreducible and C has no singularities above $\mathbb{P}^1(\overline{\mathbb{F}}_q) \setminus \mathbb{A}^1(\mathbb{F}_q)$.*

Proof. Suppose that $f = a \cdot b$ for certain $a, b \in \overline{\mathbb{F}}_q[t, y]$. Write $a = \sum_{i=0}^{\lambda} a_i(t)y^i$, $b = \sum_{i=0}^{\gamma-\lambda} b_i(t)y^i$ where λ is the y -degree of a , and $a_i, b_i \in \overline{\mathbb{F}}_q[t]$. Let p be a linear factor of β in $\overline{\mathbb{F}}_q[t]$ and denote by v_p the induced valuation on $\overline{\mathbb{F}}_q[t]$. Then we have that

$$1 = v_p(f_0) = v_p(a_0) + v_p(b_0), \quad 0 = v_p(f_\gamma) = v_p(a_\lambda) + v_p(b_{\gamma-\lambda}).$$

So without loss of generality, $v_p(a_\lambda) = v_p(b_{\gamma-\lambda}) = v_p(b_0) = 0$ and $v_p(a_0) = 1$. Now take $\lambda' \geq 0$ such that $v_p(a_{\lambda'}) = 0$ but $v_p(a_i) \geq 1$ for $i = 0, \dots, \lambda' - 1$. Then

$$v_p(f_{\lambda'}) = v_p(b_0 a_{\lambda'} + b_1 a_{\lambda'-1} + \dots) = 0$$

and by construction of f , $\lambda' = \gamma$ and hence also $\lambda = \gamma$. This implies that $b = b_0 \in \overline{\mathbb{F}_q}[t]$. It is clear that b_0 is coprime to both α and β , because α and β do not divide f . But then $b_0^{2\gamma-2}$ would divide $\text{disc}_y f(t, y)$, which contradicts the fact that $(g_i)_i \in A$. So we conclude that f is absolutely irreducible.

That C has no singularities above primes p not dividing α or β follows directly from Lemma 4.4 and the fact that $(g_i)_i \in A$. That the same holds above β follows from the fact that f is an Eisenstein polynomial with respect to β . Finally, by an argument similar to Lemma 2.2 but using the right hand side of Δ , we see that the fibre of C above ∞ consists of γ non-singular \mathbb{F}_q -rational points. \square

We have just proven that f is absolutely irreducible, so denote by \tilde{C} the non-singular model of C . As for the genus of \tilde{C} , and the points above $\mathbb{P}^1(\mathbb{F}_q)$ we have the following.

Lemma 4.6. *Every fibre of $\pi : \tilde{C} \rightarrow \mathbb{P}^1$ above $\mathbb{P}^1(\mathbb{F}_q)$ consists of γ distinct non-singular \mathbb{F}_q -rational points. Moreover, the genus of \tilde{C} is equal to*

$$g(\tilde{C}) = \#(\Delta^{(1)} \cap \mathbb{Z}^2) - qL(\ell) = g.$$

Proof. The first statement for fibres above $\mathbb{A}^1(\mathbb{F}_q)$ follows directly from Lemma 2.2 and our construction of f . Note that the right hand side of $\Delta(f)$ consists of γ line segments, each containing two lattice points. Above ∞ , a similar argument as Lemma 2.2 using the right hand side of $\Delta(f)$ then gives that also $\pi^{-1}(\infty)$ consists of γ non-singular \mathbb{F}_q -rational points.

By the previous lemma, C has no singularities in S , except above points of $\mathbb{A}^1(\mathbb{F}_q)$. The curve C has arithmetic genus $\#(\Delta^{(1)} \cap \mathbb{Z}^2)$. Recall that the torus-invariant points of S correspond to the lattice points on the boundary of Δ , so let $p \in S$ be the torus-invariant point corresponding to $(0, \gamma) \in \Delta$. By looking at the fans of S and $S' = S(\Delta(f))$, see Figure 4.2, one sees that there is a toric morphism $\psi : S' \rightarrow S$ which is an isomorphism away from p . The strict transform of C under this morphism is the curve C' defined by f , but in the surface S' , and ψ restricts to a morphism $C' \rightarrow C$ which is an isomorphism away from p . Since $\pi(p) = 0$, the curve C is isomorphic to C' above $\mathbb{P}^1 \setminus \{0\}$. By Lemma 2.2, the curve C' is non-singular above 0, and by comparing Newton polygons, the arithmetic genus of C' is equal to

$$\#(\Delta(f)^{(1)} \cap \mathbb{Z}^2) = g_a(C) - L(\ell).$$

The same reasoning holds above every other point of $\mathbb{A}^1(\mathbb{F}_q)$, by our construction of the polynomial f . After resolving the singularities above every $a \in \mathbb{A}^1(\mathbb{F}_q)$, we end up with the curve \tilde{C} , since these were the only singularities of C . Hence we conclude that this curve has genus

$$\#(\Delta(f)^{(1)} \cap \mathbb{Z}^2) - qL(\ell) = g. \quad \square$$

This lemma implies immediately that \tilde{C} has $\gamma(q+1)$ \mathbb{F}_q -rational points. Finally, the fact that \tilde{C} has gonality γ follows directly from the gonality bound 1.1 since \tilde{C} has $\gamma(q+1)$ \mathbb{F}_q -rational points and we have an \mathbb{F}_q -rational map $\tilde{C} \rightarrow \mathbb{P}^1$ of degree γ .

Acknowledgments. The author would like to thank Wouter Castryck and Xander Faber for helpful discussions and for comments on an earlier version of this article. The author thanks Art Waeterschoot for discussions around singular curves. The author thanks the referee for helpful comments.

References

- [1] P. BEELEN, “A generalization of Baker’s theorem”, *Finite Fields Appl.* **15** (2009), no. 5, p. 558-568.
- [2] R. BRYANT, “Irreducibility of discriminant”, MathOverflow, <https://mathoverflow.net/q/221771>.
- [3] W. CASTRYCK & F. COOLS, “Linear pencils encoded in the Newton polygon”, *Int. Math. Res. Not.* **2017** (2017), no. 10, p. 2998-3049.
- [4] N. D. ELKIES, E. W. HOWE, A. KRESCH, B. POONEN, J. L. WETHERELL & M. E. ZIEVE, “Curves of every genus with many points, II: Asymptotically good families”, *Duke Math. J.* **122** (2004), no. 2, p. 399-422.
- [5] X. FABER & J. GRANTHAM, “Ternary and Quaternary Curves of Small Fixed Genus and Gonality With Many Rational Points”, *Exp. Math.* (2021), <https://doi.org/10.1080/10586458.2021.1926015>.
- [6] ———, “Binary curves of small fixed genus and gonality with many rational points”, *J. Algebra* **597** (2022), p. 24-46.
- [7] X. FABER & F. VERMEULEN, “On abelian covers of the projective line with fixed gonality and many rational points”, *Int. J. Number Theory* **18** (2022), no. 10, p. 2211-2216.
- [8] G. VAN DER GEER, “Curves over finite fields and codes”, in *3rd European congress of mathematics (ECM)*, Progress in Mathematics, vol. 202, Birkhäuser, 2001.
- [9] I. GELFAND, M. KAPRANOV & A. ZELEVINSKY, *Discriminants, Resultants, and Multidimensional Determinants*, Mathematics: Theory & Applications, Birkhäuser, 1994.
- [10] A. G. HOVANSKIĬ, “Newton polyhedra, and the genus of complete intersections”, *Funkts. Anal. Prilozh.* **12** (1978), no. 1, p. 51-61.
- [11] Y. IHARA, “Some remarks on the number of rational points of algebraic curves over finite fields”, *J. Fac. Sci., Univ. Tokyo, Sect. I A* **28** (1981), p. 721-724.
- [12] N. KOBLITZ, *p-adic Analysis and Zeta functions*, Graduate Texts in Mathematics, vol. 58, Springer, 1977.
- [13] A. KRESCH, J. L. WETHERELL & M. E. ZIEVE, “Curves of every genus with many points, I: Abelian and toric families”, *J. Algebra* **250** (2002), no. 1, p. 353-370.
- [14] J. NEUKIRCH, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer, 1999.
- [15] B. POONEN, “Squarefree values of multivariable polynomials”, *Duke Math. J.* **118** (2003), no. 2, p. 353-373.

- [16] S. VLADUT & V. G. DRINFELD, “Number of points of an algebraic curve”, *Funct. Anal. Appl.* **17** (1983), no. 1, p. 53-54.

Floris VERMEULEN

KU Leuven, Department of Mathematics,

Celestijnenlaan 200B,

3001 Leuven, Belgium

E-mail: floris.vermeulen@kuleuven.be

URL: <https://sites.google.com/view/floris-vermeulen/homepage>