JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Wojciech WAWRÓW

On torsion of superelliptic Jacobians

Tome 33, n° 1 (2021), p. 223-235.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2021__33_1_223_0>

Journal de Théorie des Nombres
de Bordeaux **33** (2021), 223–235

On torsion of superelliptic Jacobians

par Wojciech WAWRÓW

Résumé. Nous démontrons un résultat décrivant la structure d'un sous-groupe de m-torsion spécifique de la jacobienne d'une courbe superelliptique générale de la forme $y^m = F(x)$, généralisant ainsi le théorème de structure pour la 2-torsion d'une courbe hyperelliptique. Nous étudions l'existence de points de torsion sur les courbes de la forme $y^q = x^p - x + a$ sur les corps finis de caractéristique p. Nous appliquons ces résultats à la minoration du rank de Mordell–Weil des jacobiennes de certaines courbes superelliptiques sur $\mathbb{Q}$.

Abstract. We prove a result describing the structure of a specific subgroup of the m-torsion of the Jacobian of a general superelliptic curve $y^m = F(x)$, generalizing the structure theorem for the 2-torsion of a hyperelliptic curve. We study existence of torsion on curves of the form $y^q = x^p - x + a$ over finite fields of characteristic p. We apply those results to bound from below the Mordell–Weil ranks of Jacobians of certain superelliptic curves over $\mathbb{Q}$.

1. Introduction

Our objects of study are *superelliptic curves*, defined by equations of the form

$$C : y^m = F(x)$$

for separable polynomials F and $m \geq 2$ not divisible by the characteristic of the base field. This family generalizes hyperelliptic curves, which are curves of the above form for $m = 2$, $\deg F > 4$, as well as Picard curves, which are the case $m = 3$, $\deg F = 4$.

We are specifically interested in the points of the form $(\alpha, 0)$, where α is a root of F. The line $x = \alpha$ intersects C at this point with multiplicity m. This lets us find certain divisor classes on the Jacobian $J(C)$, formed by such points and the points at infinity, which are m-torsion.

In particular, suppose that F factors as $(x-\alpha_1)\dots(x-\alpha_r)$ in K. Consider the group Δ consisting of classes of divisors of the form

$$\sum_{i=1}^{r} a_i R_i - \frac{1}{d}\left(\sum_{i=1}^{r} a_i\right)\infty,$$

Manuscrit reçu le 1er juillet 2020, révisé le 19 octobre 2020, accepté le 13 décembre 2020.
2010 *Mathematics Subject Classification.* 14H40, 14G10, 14H45.
Mots-clefs. Jacobian variety, superelliptic curves, Mordell–Weil group.

where $d = \gcd(m, r)$, a_i are integers whose sum is divisible by d, R_i is the point $(\alpha_i, 0)$, and ∞ is the formal sum of points at infinity of C. It is easy to see those classes are m-torsion in $J(C)$.

It appears to be a folklore result that for $m = 2$, Δ is the entire 2-torsion subgroup of $J(C)$. In particular, it is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g}$, where g is the genus of C, equal to either $\frac{r-1}{2}$ or $\frac{r-2}{2}$ according to the parity of r. This statement follows for instance from the results of [14], discussed below, when specialized to the case $m = 2$.

For $m > 2$, those points cannot form all of m-torsion for cardinality reasons. For instance, when $\gcd(m, r) = 1$, Δ has order at most m^{r-1}, while the theory of abelian varieties tells us that over the algebraic closure of the base field the m-torsion consists of m^{2g} points, and $2g > r - 1$ as soon as $m > 2$.

Describing the entire m-torsion of a superelliptic Jacobian is an interesting problem. We provide a result in this direction, showing that Δ always has the maximal possible size, subject to some obvious relations its points satisfy. Specifically, we have

Proposition 1. *Δ is a subgroup of $J(C)$ isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{r-2} \times (\mathbb{Z}/\frac{m}{d}\mathbb{Z})$.*

This result, which does not seem to have appeared in this form in the literature before, can be seen as a generalization of the above mentioned structure theorem for hyperelliptic curves. If m is a prime number the above proposition can be deduced from [14, Proposition 6.2], which furthermore describes the resulting subgroup as the kernel of a certain endomorphism on the Jacobian of the curve.

We can use the proposition above to find families of curves whose Jacobians have high Mordell–Weil ranks over number fields. As a sample application, we show the following.

Theorem 2. *Suppose p is an odd prime, q is a prime factor of $p-1$ and k is an integer divisible by some prime larger than p but not by p. Then the Jacobian of the curve*

$$y^q = x(x-1)\dots(x-(p-1)) + k^q$$

has the Mordell–Weil rank at least $p-1$ over $\mathbb{Q}$.

The proof of this result follows the methodology of [8], where we use the proposition as a substitute for results about hyperelliptic curves, along with some calculations using Gauss sums over finite fields, similar to ones presented in [6, §11].

One of the earliest works where Jacobians of high rank depending on the genus of curves are shown to exist is [11] where, among other things, Néron shows that for any g there are infinitely many curves of genus g

with Mordell–Weil rank at least $3g + 7$. This work is, however, ineffective. For $g = 2$ those bounds have been improved and made effective by Shioda in [16] where families with Mordell–Weil rank at least 15 are constructed using a trick introduced by Mestre in [10].

The first completely effective result of this kind for curves of arbitrary genus appears be due to Coleman [1], where the effective Chabauty method is applied to find families of hyperelliptic curves with Jacobians of high ranks. In [8] Coleman's examples are improved, and using a different, more elementary approach the Jacobians are shown to have even higher ranks under additional assumptions. The present work further extends this approach to special families of superelliptic curves, culminating in the explicit examples of Theorem 2 above.

It should be noted that the results mentioned thus far require the genera of the curves, and hence the dimensions of their Jacobians, to grow unboundedly for the ranks to get arbitrarily large. It is a well-known open problem whether the ranks can be arbitrarily large for abelian varieties of a fixed dimension over a fixed number field. For the specific case of elliptic curves over $\mathbb{Q}$, the example with the highest known rank was found by Elkies [3] and has rank at least 28 (exactly 28 assuming some standard conjectures, see [9]). For a recent heuristic argument for boundedness and a brief history of the problem, see [12].

All this is in stark contrast to the situation over function fields, where curves of arbitrarily high rank have been known for a long time, see [18] for the first construction and [19] for the first construction with nonisotrivial curves. Ulmer has further treated related problems for Jacobians of hyperelliptic curves over function fields. For instance in [20] he provides examples of families of hyperelliptic Jacobians with arbitrarily high rank, and further verifies the Birch–Swinnerton–Dyer conjecture for them. See [21] and [22] for general surveys on elliptic curves and general Jacobians over function fields respectively, including constructions of families with high ranks.

1.1. Structure of the paper. Below we recall all the notation, definitions and basic facts used in the following sections. Section 2 is devoted to the proof of Proposition 1. In Section 3 we look at the curves of the form $y^q = x^p - x + a$ over a field of characteristic p. We show under suitable conditions they have no q-torsion over $\mathbb{F}_p$ using methods similar to ones used in [7], involving Gauss sums and Hasse–Weil zeta functions. Lastly, in Section 4, we use those results and methods based on those in [8] to finish the proof of Theorem 2.

1.2. Notation and preliminaries. Let K be an arbitrary perfect field. We define a *superelliptic curve* over K to be a smooth projective model of

an affine curve given by an equation of the form

$$C : y^m = F(x),$$

where $m \geq 2$ is an integer not divisible by the characteristic of K and $F \in K[x]$ is separable, i.e. with no repeated factors over $\overline{K}$. We set $r = \deg F$ and $d = \gcd(m, r)$.

We observe that the affine curve above is smooth, therefore it can be identified with an open subset of its smooth projective model (see [4, I.6]). We refer to the points not included in this open subset as the *points at infinity*. Unless necessary, we shall not distinguish between the projective and the affine model of the curve.

Considering the function field of C, from [17, Proposition 3.7.3] we can show its genus is equal to

$$g = \frac{1}{2}((m-1)(r-1) - (d-1))$$

and it has exactly d points at infinity over $\overline{K}$. We denote their formal sum by ∞, which is a divisor of degree d defined over K.

We refer to [5] for basic facts about Jacobians of curves. We shall identify degree zero divisors with their classes in the Jacobian. We denote the Jacobian of a curve C by $J(C)$, and with $J(C)(K)$ we denote the group of its K-rational points.

Acknowledgments. I thank Prof. Wojciech Gajda for suggesting the topic, Bartosz Naskręcki for help with computational aspects of my research, and Jędrzej Garnek for providing many useful references. I also thank all three of them for many invaluable discussions. Further I would like to thank Sebastian Petersen for his comments on an older version of this paper, as well as Royce Peng for proof-reading the final version. Additional thanks to the anonymous referee for their valuable comments and for pointing me towards additional references.

2. Proof of Proposition 1

We may assume that the base field K is algebraically closed. We have the following equalities of divisors on C:

$$\operatorname{div}(x - \alpha_i) = mR_i - \frac{m}{d}\infty,$$

$$\operatorname{div}(y) = \sum_{i=1}^{r} R_i - \frac{r}{d}\infty,$$

From there it is not hard to see that Δ is generated as a subgroup of $J(C)$ by the following points:

$$D_i = R_i - R_{r-1} \quad \text{for } i = 1, \dots, r-2,$$
$$D_{r-1} = dR_{r-1} - \infty.$$

and that those points satisfy equalities $mD_i = 0$ for $i = 1, \dots, r-2$ and $\frac{m}{d} D_{r-1} = 0$ in $J(C)$. This gives a surjection from $(\mathbb{Z}/m\mathbb{Z})^{r-2} \times (\mathbb{Z}/\frac{m}{d}\mathbb{Z})$ to Δ given by

$$(a_1, \dots, a_{r-1}) \mapsto -\sum_{i=1}^{r-1} a_i D_i.$$

We wish to show it is also injective.

If the kernel of this map is nontrivial, then, by adding suitable multiples of divisors $\operatorname{div}(x - \alpha_i)$, we can find a principal divisor of the form

$$D = -\sum_{i=1}^{r-1} a_i R_i + \frac{1}{d}\left(\sum_{i=1}^{r-1} a_i\right)\infty$$

with $0 \le a_i < m$ not all zero. We shall prove this is impossible.

Consider the auxiliary divisor

$$E = -\infty + \sum_{i=1}^{r-1} (m-1) R_i.$$

Observe that $\deg E = (r-1)(m-1) - d = 2g - 1$, therefore Riemann–Roch theorem gives us $\ell(E) = \deg(E) - g + 1 = g$, where, as usual, $\ell(E)$ is the dimension of the K-vector space $L(E)$ of functions $f \in K(C)$ satisfying $E + \operatorname{div}(f) \ge 0$. With this in mind, we can find an explicit basis of $L(E)$.

For any $0 < i < r, 0 < j < m$ let $f_{ij} \in K(C)$ be given by

$$f_{ij} = \frac{y^j}{\prod_{k \le i}(x - \alpha_k)}.$$

We have

$$\operatorname{div}(f_{ij}) = \sum_{k=1}^{i} (j-m) R_k + \sum_{k=i+1}^{r} j R_k + \frac{1}{d}(im - jr)\infty.$$

It is clear that $f_{ij} \in L(E)$ iff $im - jr > 0$. Let

$$A = \{(i,j) : 0 < i < r, 0 < j < m, im - jr > 0\},$$
$$B = \{(i,j) : 0 < i < r, 0 < j < m, im - jr < 0\}.$$

The equation $im - jr = 0$ has exactly $d - 1$ solutions in the range $0 < i < r, 0 < j < m$, which implies that the set $A \cup B$ has $(m-1)(r-1) - (d-1) = 2g$ elements. Further, since $(r-i)m - (m-j)r = -(im - jr)$, the map

$(i,j) \mapsto (r-i, m-j)$ gives a bijection from A to B, showing A has exactly $\frac{1}{2}|A \cup B| = g$ elements.

It follows that $\{f_{ij} : (i,j) \in A\}$ is a set of $g = \ell(E)$ elements of $L(E)$, so to show it is a basis it is enough to show their linear independence. Assume there exist $b_{ij} \in K$, not all zero, such that

$$\sum_{(i,j)\in A} b_{ij} f_{ij} = 0.$$

Take the largest index k such that $b_{kj} \neq 0$ for some j. Observe f_{ij} for $i < k$ are all regular at R_k, while f_{kj} has a pole of order $m-j$ at this point. Thus, letting l be the least index such that $b_{kl} \neq 0$, the left-hand side above has a pole of order $m-l$ at R_k, so clearly is not zero. This contradiction establishes linear independence, and hence that the set above is a basis.

Consider again our divisor D. Suppose it is principal, that is, there is a nonzero $f \in K(C)$ such that $\operatorname{div}(f) = D$. We have

$$E + \operatorname{div}(f) = E + D = \sum_{i=1}^{r-1}(m-1-a_i)R_i + \left(-1 + \sum_{i=1}^{r-1} a_i\right)\infty \geq 0$$

since the a_i are all at most $m-1$ and their sum is positive. This means $f \in L(E)$, so that it can be written in terms of the basis we have found:

$$f = \sum_{(i,j)\in A} c_{ij} f_{ij}$$

with $c_{ij} \in K$. But each f_{ij} has a zero at R_r, hence so does f, which is clearly not the case since the coefficient of R_r in $D = \operatorname{div}(f)$ is zero. We conclude D is not a principal divisor, as we wanted. □

Remark 3. When $d = 1$ we have that ∞ is just a single point, and Δ is generated by the points $D_i' = R_i - \infty$ for $i = 1, \ldots, r-1$. The proposition then shows that an integer linear combination of those D_i' is zero in $J(C)$ if and only if all of its coefficients are divisible by m.

3. Curves of the form $y^q = x^p - x + a$

We move on to study superelliptic curves C with equations of the form

$$C : y^q = x^p - x + a$$

over finite fields of characteristic p, where p, q are distinct primes and $a \in \mathbb{F}_p^\times$. Observe that the polynomial on the right-hand side is always separable, since its derivative -1 doesn't vanish. We denote the Jacobian of C by J.

Assume first $q \mid p-1$. We shall compute the zeta function of this curve using Gauss sums of additive and multiplicative characters.

For any additive character $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ we define a character $\psi_n : \mathbb{F}_{p^n} \to \mathbb{C}^\times$ by

$$\psi_n(\alpha) = \psi(\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha)),$$

where $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}$ denotes the field-theoretic trace map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Similarly, for a multiplicative character $\chi : \mathbb{F}_p \to \mathbb{C}$, we define $\chi_n : \mathbb{F}_{p^n} \to \mathbb{C}$ by

$$\chi_n(\alpha) = \chi(\mathrm{N}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha)),$$

where $\mathrm{N}_{\mathbb{F}_{p^n}/\mathbb{F}_p}$ is the field-theoretic norm.

Remark 4. We adopt the convention for multiplicative characters χ that $\chi(0) = 0$ for nontrivial characters χ, but $\chi(0) = 1$ for χ the trivial character.

Since $\gcd(p, q) = 1$, C has exactly one point at infinity, so we just need to count the points on its affine part.

Lemma 5. *C has exactly*

$$\sum_{w-z=a} \sum_{\psi} \sum_{\chi} \psi_n(z)\chi_n(w)$$

affine points over $\mathbb{F}_{p^n}$, where the first sum ranges over all pairs $w, z \in \mathbb{F}_{p^n}$ satisfying $w - z = a$, the second over all additive characters of $\mathbb{F}_p$ and the third one over multiplicative characters of $\mathbb{F}_p$ of order dividing q.

Proof. For each $z, w \in \mathbb{F}_{p^n}$ we count the number of points on C satisfying $x^p - x = z$ and $y^q = w$. For such a solution to exist we need to have $w - z = a$, so we only need to consider pairs z, w satisfying this. For each such pair it is sufficient to count the number of solutions x, y to $x^p - x = z, y^q = w$.

It is standard that for any z, w the number of solutions to $y^q = w$ in $\mathbb{F}_{p^n}$ is equal to

$$\sum_{\chi} \chi_n(w),$$

while the number of solutions to $x^p - x = z$ is equal to

$$\sum_{\psi} \psi_n(z),$$

where the ranges of the sums are as in the statement of the lemma. Combining all of those observations we get the formula for the number of points in $C(\mathbb{F}_{p^n})$. □

We consider modified Gauss sums defined by

$$G_a(\psi_n, \chi_n) = \sum_{w-z=a} \psi_n(z)\chi_n(w)$$

with the sum over $z, w \in \mathbb{F}_{p^n}$ satisfying $z - w = a$. The previous lemma gives

$$|C(\mathbb{F}_{p^n})| = 1 + \sum_{\psi} \sum_{\chi} G_a(\psi_n, \chi_n).$$

The sums G_a have the following properties:

Lemma 6. *Let ψ be an additive character of $\mathbb{F}_p$ and χ a multiplicative character of $\mathbb{F}_p$.*

- *If ψ, χ are both trivial, then $G_a(\psi_n, \chi_n) = p^n$.*
- *If exactly one of ψ, χ is trivial, then $G_a(\psi_n, \chi_n) = 0$.*
- *If both ψ, χ are nontrivial, then $-G_a(\psi_n, \chi_n) = (-G_a(\psi, \chi))^n$.*

Proof. The first two claims are immediate. Observe

$$\begin{aligned} G_a(\psi_n, \chi_n) &= \sum_{w-z=a} \psi_n(z)\chi_n(w) = \sum_{w} \psi_n(w-a)\chi_n(w) \\ &= \psi_n(-a) \sum_{w} \psi_n(w)\chi_n(w) = \psi(-a)^n G(\psi_n, \chi_n), \end{aligned}$$

where $G(\psi_n, \chi_n)$ is the usual Gauss sum. The last statement now follows from the usual Hasse–Davenport relations for Gauss sums, see [6, §11.4]. □

We therefore have

$$|C(\mathbb{F}_{p^n})| = 1 + p^n - \sum_{\psi \neq 1} \sum_{\chi \neq 1} (-G_a(\psi, \chi))^n,$$

where with 1 we denote the trivial character (both additive and multiplicative). This gives us an explicit formula for the zeta function of C:

$$Z(C, T) = \frac{\prod_{\psi \neq 1} \prod_{\chi \neq 1} (1 + G_a(\psi, \chi)T)}{(1 - T)(1 - pT)}.$$

By [13, §5.4], evaluating the numerator at $T = 1$ gives us the number of points on the Jacobian of C over $\mathbb{F}_p$, i.e.

$$|J(\mathbb{F}_p)| = \prod_{\psi \neq 1} \prod_{\chi \neq 1} (1 + G_a(\psi, \chi)),$$

With this formula we can now establish

Proposition 7. *If $q \mid p - 1$, the Jacobian of C has no q-torsion over $\mathbb{F}_p$.*

Proof. Let ζ_{pq} be a primitive pq-th root of unity. Note that $G_a(\psi, \chi) \in \mathbb{Z}[\zeta_{pq}]$ for all a, ψ, χ, and that $\mathbb{Z}[\zeta_{pq}]$ is a Dedekind domain. Take any prime ideal factor $\mathfrak{q}$ of q in this ring.

We have a classical equality of ideals $(q) = (1-\zeta_q)^{q-1}$ in any ring containing ζ_q, so that necessarily $1-\zeta_q \in \mathfrak{q}$. It follows we have $\chi_n(w) \equiv 1 \pmod{\mathfrak{q}}$ for all $w \in \mathbb{F}_{p^n}^\times$, hence for $\psi, \chi \neq 1$ we get

$$G_a(\psi,\chi) \equiv \sum_{z \neq -a} \psi(z) = -\psi(-a) + \sum_z \psi(z) = -\psi(-a) \pmod{\mathfrak{q}},$$

thus

$$|J(\mathbb{F}_p)| \equiv \prod_{\psi\neq 1}\prod_{\chi\neq 1}(1-\psi(-a)) \pmod{\mathfrak{q}}.$$

Observe that since $-a \in \mathbb{F}_p^\times$, $\psi(-a)$ is a primitive p-th root of unity for every $\psi \neq 1$, so $1-\psi(-a)$ is a factor of p in $\mathbb{Z}[\zeta_{pq}]$. It follows that $1-\psi(-a) \notin \mathfrak{q}$, as otherwise we would find $p \in \mathfrak{q}$, which cannot hold as p, q are distinct rational primes. It follows $1-\psi(-a)$ is not in $\mathfrak{q}$, hence neither is $|J(\mathbb{F}_p)|$. Consequently $q \nmid |J(\mathbb{F}_p)|$, so $J(\mathbb{F}_p)$ has no q-torsion. □

If we now drop the condition that q divides $p-1$ and merely assert that it is different from p, we can instead reason using a field extension $\mathbb{F}_{p^k}$ for k such that $q \mid p^k - 1$. This way we can give an exact condition for when q-torsion exists in $\mathbb{F}_p$:

Theorem 8. *Let p, q be distinct primes and let $k = \operatorname{ord}_q p$ be the least k such that $q \mid p^k - 1$. Then the Jacobian of C has no q-torsion over $\mathbb{F}_p$ iff $p \nmid k$.*

Proof. We can repeat the reasoning preceding Theorem 7 and in the proof of the theorem to find

$$|J(\mathbb{F}_{p^k})| = \prod_{\psi\neq 1}\prod_{\chi\neq 1}(1-(-G_a(\psi_k,\chi))) \equiv \prod_{\psi\neq 1}\prod_{\chi\neq 1}(1-\psi_k(-a)) \pmod{\mathfrak{q}},$$

where this time ψ ranges over all additive characters of $\mathbb{F}_p$, while χ ranges over all multiplicative characters of $\mathbb{F}_{p^k}$ of order dividing q. It is clear that $\psi_k(-a) = \psi(-a)^k$, so as long as $p \nmid k$ it is again a primitive root of unity. Hence $J(\mathbb{F}_{p^k})$ has no q-torsion, thus neither does its subgroup $J(\mathbb{F}_p)$.

When $p \mid k$ we have $\psi_k(-a) = \psi(-a)^k = 1$, so that $|J(\mathbb{F}_{p^k})| \equiv 0 \pmod{\mathfrak{q}}$, hence $q \mid |J(\mathbb{F}_{p^k})|$. From the following lemma we also have $q \mid |J(\mathbb{F}_p)|$, so $J(\mathbb{F}_p)$ contains a q-torsion point. □

Lemma 9. *For p, q, k as above we have*

$$|J(\mathbb{F}_{p^k})| = |J(\mathbb{F}_p)|^k.$$

Proof. From the Weil conjectures it follows there is a unique (up to ordering) collection of $2g$ numbers $\alpha_1, \ldots, \alpha_{2g}$ such that, for all n,

$$p^n + 1 - C(\mathbb{F}_{p^n}) = \sum_{i=1}^{2g} \alpha_i^n.$$

But for $k \nmid n$ we have q and $p^n - 1$ relatively prime, so that $y \mapsto y^q$ is a bijection on $\mathbb{F}_{p^n}$. It follows that $C(\mathbb{F}_{p^n}) = p^n + 1$, hence

$$\sum_{i=1}^{2g} \alpha_i^n = 0. \tag{3.1}$$

Note that if we multiply each of $\alpha_1, \ldots, \alpha_{2g}$ by ζ_k^j, where ζ_k is a primitive k-th root of unity and j is arbitrary, we get

$$\sum_{i=1}^{2g} (\zeta_k^j \alpha_i)^n = \zeta_k^{nj} \sum_{i=1}^{2g} \alpha_i^n = \sum_{i=1}^{2g} \alpha_i^n$$

for all n—if $k \nmid n$ this follows from (3.1), while if $k \mid n$ it is immediate. The uniqueness statement above leads us to a conclusion that $\alpha_i \mapsto \zeta_k^j \alpha_i$ is a permutation for any j. Using again [13, §5.4],

$$|J(\mathbb{F}_p)|^k = \left(\prod_{i=1}^{2g} (1 - \alpha_i) \right)^k = \prod_{i=1}^{2g} \prod_{j=0}^{k-1} (1 - \zeta_k^j \alpha_i) = \prod_{i=1}^{2g} (1 - \alpha_i^k) = |J(\mathbb{F}_{p^k})|. \quad \square$$

Remark 10. As pointed out by a referee, essentially the same argument shows that $|J(\mathbb{F}_{p^{k'}})| = |J(\mathbb{F}_p)|^{k'}$ for any $k' \mid k$. The lemma holds more generally for any superelliptic curve $y^q = F(x)$ with $F \in \mathbb{F}_p[x]$ of degree not divisible by q. Further, numerical evidence suggests that the following holds:

Conjecture. *Consider a superelliptic curve C given by $y^q = F(x)$ with q prime, $F \in \mathbb{F}_p[x]$ of degree not divisible by q and set $k = \operatorname{ord}_q p$. There exists an isomorphism*

$$J(\mathbb{F}_{p^k}) \cong J(\mathbb{F}_p)^k$$

of abstract groups.

Remark 11. The previous two theorems still hold when we take C to be defined by an equation $y^{q^l} = x^p - x + a$. The proofs are analogous using the fact $1 - \zeta_{q^l} \in \mathfrak{q}$ for any prime $\mathfrak{q}$ of $\mathbb{Z}[\zeta_{pq^l}]$ containing q. We get that $q \mid |J(\mathbb{F}_p)|$ iff $p \mid \operatorname{ord}_q p$.

4. Applications to bounding ranks

We now apply the established results to reductions of certain curves over the rationals to bound their Mordell–Weil ranks from below. Specifically, consider curves defined by

$$C : y^m = (x - a_1) \ldots (x - a_r) + k^m,$$

where $a_1, \ldots, a_r$ and k are integers and m, r are relatively prime. We take the points $P_i = (a_i, k) \in C$, their images $D_i = P_i - \infty \in J(C)$ under the

Albanese map and the subgroup Γ those images generate. It is clearly a subgroup of $J(C)(\mathbb{Q})$. The following result is implicit in [8] for $m = 2$.

Proposition 12. *Assume there is a prime p such that:*

(1) *m is not divisible by p,*
(2) *k is divisible by p,*
(3) *the a_i are pairwise incongruent modulo p.*

Suppose further Γ contains no nontrivial m-torsion. Then Γ is free of rank $r-1$.

Proof. The sum of all D_i is equal to $\operatorname{div}(y-k)$, so Γ is generated by $D_1, \ldots, D_{r-1}$. It is enough to show there is no relation between those points.

Since $p \mid k$, the reduction of the equation of C modulo p is

$$\widetilde{C} : y^m = (x - a_1) \ldots (x - a_r).$$

We have $p \nmid m$ by the first assumption, and the right-hand side is separable by the third, from which we deduce C has good reduction modulo p. It follows $J(C)$ also has good reduction (see [2, Corollary VII.12.3]), which induces a reduction homomorphism $J(C)(\mathbb{Q}) \to J(\widetilde{C})(\mathbb{F}_p)$.

Suppose there is a nontrivial relation between the points $D_1, \ldots, D_{r-1}$, say

$$\sum_{i=1}^{r-1} a_i D_i = 0$$

with not all a_i zero. Reordering the points and changing the sign if necessary, we may assume $a_1 > 0$ and a_1 is the smallest possible among all such relations. The relation is preserved by the reduction homomorphism, so

$$\sum_{i=1}^{r-1} a_i \widetilde{D}_i = 0,$$

where $\widetilde{D}_i$ is the image of D_i under reduction. But the reduction of the point $P_i = (a_i, k)$ is $(\widetilde{a_i}, 0)$ (as we assumed $p \mid k$), so the points $\widetilde{D}_i$ coincide with the points D_i' considered in Remark 3. This gives rise to a vanishing linear combination of the D_i', which by the remark implies the coefficients are all divisible by m. Writing $a_i = mb_i$ we have $b_1 < a_1$, so, by minimality of a_1, the point $D = \sum_{i=1}^{r-1} b_i D_i \in J(C)(\mathbb{Q})$ is nonzero. However, the original relation gives us $mD = 0$, which contradicts the assumption that Γ has no m-torsion. □

Remark 13. Suitable versions of this proposition also hold for curves satisfying $\gcd(m, r) > 1$, as well as for curves over arbitrary number fields in place of $\mathbb{Q}$, and lead to more general variants of Theorem 2

Proof of Theorem 2. Let C be a curve as in the statement of the theorem. First we show C has no q-torsion over $\mathbb{Q}$. The reduction of the equation of this curve modulo p is

$$\widetilde{C} : y^q = x^p - x + k^q$$

and, as we have noted before, the right-hand side is separable, so as before the curve and its Jacobian have good reduction and we get a reduction homomorphism $J(C)(\mathbb{Q}_p) \to J(\widetilde{C})(\mathbb{F}_p)$.

The kernel of this reduction homomorphism is isomorphic to a group associated to a g-parameter formal group over $\mathbb{Z}_p$ (see [5, §C.2]). By [15, Theorems II.9.3 and II.9.4] this group has no torsion, so all torsion of $J(C)(\mathbb{Q}_p)$ survives into $J(\widetilde{C})(\mathbb{F}_p)$. But Theorem 7 tells us this last group has no q-torsion, therefore neither does $J(C)(\mathbb{Q}_p)$ nor $J(C)(\mathbb{Q})$. We are now done by the previous proposition. □

Using Dirichlet's theorem on primes in arithmetic progressions, this gives us, for any fixed q, families of superelliptic curves whose Jacobians have Mordell–Weil ranks that grow at least linearly with the genus of the curve.

Remark 14. The methods described above can be applied to curves which have the form $y^q = x^p + a$ after reduction modulo some prime $\ell \equiv 1 \pmod{pq}$. Torsion on Jacobians of such curves is studied at length in [7], see for instance Lemma 4 of that paper, where one can find a different proof of the analogue of Theorem 7 for the case $q = 3$.

References

[1] R. F. Coleman, "Effective Chabauty", *Duke Math. J.* **52** (1985), no. 3, p. 765-770.

[2] G. Cornell & J. H. Silverman (eds.), *Arithmetic geometry*, Springer, 1986, Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984, xvi+353 pages.

[3] N. D. Elkies, "$\mathbb{Z}^{28}$ in $E(\mathbb{Q})$, etc.", 2006, NMBRTHRY mailing list.

[4] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer, 1977, xvi+496 pages.

[5] M. Hindry & J. H. Silverman, *Diophantine geometry, An introduction*, Graduate Texts in Mathematics, vol. 201, Springer, 2000, xiv+558 pages.

[6] K. Ireland & M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer, 1990, xiv+389 pages.

[7] T. Jędrzejak, "On the torsion of the Jacobians of superelliptic curves $y^q = x^p + a$", *J. Number Theory* **145** (2014), p. 402-425.

[8] K. Joshi & P. Tzermias, "On the Coleman-Chabauty bound", *C. R. Math. Acad. Sci. Paris* **329** (1999), no. 6, p. 459-463.

[9] Z. Klagsbrun, T. Sherman & J. Weigandt, "The Elkies curve has rank 28 subject only to GRH", *Math. Comp.* **88** (2019), no. 316, p. 837-846.

[10] J.-F. Mestre, "Courbes elliptiques de rang ≥ 11 sur $\mathbf{Q}(t)$", *C. R. Math. Acad. Sci. Paris* **313** (1991), no. 3, p. 139-142.

[11] A. Néron, "Propriétés arithmétiques de certaines familles de courbes algébriques", in *Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, vol. III*, Erven P. Noordhoff N.V.; North-Holland, 1956, p. 481-488.

[12] J. Park, B. Poonen, J. Voight & M. M. Wood, "A heuristic for boundedness of ranks of elliptic curves", *J. Eur. Math. Soc.* **21** (2019), no. 9, p. 2859-2903.
[13] B. Poonen, "Lectures on rational points on curves", 2006, available at `https://math.mit.edu/~poonen/papers/curves.pdf`.
[14] B. Poonen & E. F. Schaefer, "Explicit descent for Jacobians of cyclic covers of the projective line", *J. Reine Angew. Math.* **488** (1997), p. 141-188.
[15] J.-P. Serre, *Lie algebras and Lie groups*, Lecture Notes in Mathematics, vol. 1500, Springer, 2006, 1964 lectures given at Harvard University, Corrected fifth printing of the second (1992) edition, viii+168 pages.
[16] T. Shioda, "Genus two curves over $\mathbf{Q}(t)$ with high rank", *Comment. Math. Univ. St. Pauli* **46** (1997), no. 1, p. 15-21.
[17] H. Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer, 2009, xiv+355 pages.
[18] D. T. Tèĭt & I. R. Šafarevič, "The rank of elliptic curves", *Dokl. Akad. Nauk SSSR* **175** (1967), p. 770-773.
[19] D. Ulmer, "Elliptic curves with large rank over function fields", *Ann. Math.* **155** (2002), no. 1, p. 295-315.
[20] ———, "L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields", *Invent. Math.* **167** (2007), no. 2, p. 379-408.
[21] ———, "Elliptic curves over function fields", in *Arithmetic of L-functions*, IAS/Park City Mathematics Series, vol. 18, American Mathematical Society, 2011, p. 211-280.
[22] ———, "Curves and Jacobians over function fields", in *Arithmetic geometry over global function fields*, Advanced Courses in Mathematics - CRM Barcelona, Springer, 2014, p. 283-337.

Wojciech Wawrów
Adam Mickiewicz University
Faculty of Mathematics and Computer Science
Uniwersytetu Poznańskiego 4
61-614 Poznań, Poland
Current address: London School of Geometry and Number Theory
Department of Mathematics
University College London
Gower Street
London, WC1E 6BT, United Kingdom
E-mail: `wojtek.wawrow@gmail.com`
URL: `https://sites.google.com/view/wojtekwawrow`