ACTA ARITHMETICA
161.3 (2013)

On ranks of Jacobian varieties in prime degree extensions

by

Dave Mendes da Costa (Bristol)

1. Introduction and statement of results. Let $\mathcal{C}$ be a curve (which will be smooth, irreducible and projective unless otherwise stated) defined over a number field K and with genus $g(\mathcal{C}) \geq 1$. We can associate with $\mathcal{C}$ an abelian variety $\mathrm{Jac}(\mathcal{C})$ called the *Jacobian* of $\mathcal{C}$. This variety has dimension equal to $g(\mathcal{C})$ and if $\mathcal{C}(K) \neq \emptyset$ then there is an embedding of $\mathcal{C}$ into $\mathrm{Pic}^0(\mathcal{C})$ defined over K and an isomorphism, also defined over K, between $\mathrm{Jac}(\mathcal{C})$ and $\mathrm{Pic}^0(\mathcal{C})$. Let us assume that $\mathcal{C}(K) \neq \emptyset$ so that we can identify $\mathrm{Jac}(\mathcal{C})$ and $\mathrm{Pic}^0(\mathcal{C})$ throughout.

The celebrated Mordell–Weil Theorem tells us that $\mathrm{Jac}(\mathcal{C})(K)$ has the structure of a finitely generated abelian group. We define the *rank* of $\mathrm{Jac}(\mathcal{C})$ to be the number of copies of $\mathbb{Z}$ appearing in $\mathrm{Jac}(\mathcal{C})(K)$ and denote this by $\mathrm{rk}(\mathcal{C}/K)$. In this paper we shall be interested in how $\mathrm{rk}(\mathcal{C}/L)$ behaves as we vary the field L. When $\mathcal{C}$ is an elliptic curve and $K = \mathbb{Q}$ then a conjecture of Goldfeld [4] asserts that as we let L range across all quadratic extensions of $\mathbb{Q}$ then the rank should remain the same as $\mathrm{rk}(\mathcal{C}/\mathbb{Q})$ 50% of the time and increase by one 50% of the time with the remaining 0% accounting for other behaviour. This is as yet unproved, however it is known that the rank both increases infinitely often and remains the same infinitely often. From this position it is a natural question to ask if this behaviour persists when we make two generalisations:

(1) Replacing $\mathbb{Q}$ by K, and
(2) Considering L/K such that $[L : K] = p$ for some prime p.

In this first case the analogue of Goldfeld's conjecture clashes with other standard conjectures which predict that there are elliptic curves defined over number fields whose rank increases in every quadratic extension (for details, see [2]). With this in mind we ask two questions:

2010 *Mathematics Subject Classification*: Primary 11G05.
Key words and phrases: elliptic curves, ranks, number fields.

DOI: 10.4064/aa161-3-3

QUESTION 1. *Given a curve $\mathcal{C}$, of positive genus, defined over a number field K such that $\mathcal{C}(K) \neq \emptyset$ and a prime p, are there infinitely many extensions L/K with $[L:K] = p$ such that* $\mathrm{rk}(\mathcal{C}/L) > \mathrm{rk}(\mathcal{C}/K)$*?*

We will also be interested in the following related question:

QUESTION 2. *Given a curve $\mathcal{C}$, of positive genus, defined over a number field K such that $\mathcal{C}(K) \neq \emptyset$, is there an $N > 0$ such that if p is a prime and $p \geq N$ then are there infinitely many extensions L/K with $[L:K] = p$ such that* $\mathrm{rk}(\mathcal{C}/L) > \mathrm{rk}(\mathcal{C}/K)$*?*

Our main result is a partial answer to Question 2 for a certain family of curves.

THEOREM 1. *Let $\mathcal{C}$ be a smooth, irreducible curve of positive genus defined over a number field K and with $\mathcal{C}(K) \neq \emptyset$. Suppose further that $\mathcal{C}$ is birational to a plane curve $\mathcal{C}'$ of the form*

$$\mathcal{C}' : g(y) = f(x)$$

where f and g are polynomials whose degrees are coprime. Then there is an integer $N(\mathcal{C}) > 0$, effective and depending on $\mathcal{C}$, such that for all primes $p \geq N(\mathcal{C})$ we have an affirmative answer to Question 1*.*

This theorem has some interesting corollaries. First we note that the family includes all hyperelliptic curves of odd degree.

COROLLARY 1. *Let $\mathcal{C}$ be birational to the plane curve cut out by the equation*

$$\mathcal{C}' : y^2 = g(x)$$

where g is a polynomial and $k = \deg(g)$ is odd. Then there is an $N(\mathcal{C})$ such that for all primes $p \geq N(\mathcal{C})$ Question 1 *has an affirmative answer. What is more, we can take $N(\mathcal{C}) = k + 1$.*

This has the following pleasing corollary.

COROLLARY 2. *Question* 1 *has an affirmative answer for every prime p when $\mathcal{C}$ is an elliptic curve.*

2. Strategy of proof. The strategy we shall employ for proving these theorems is wholly inspired by the paper [1] of Tim Dokchitser where he proves that Question 1 has an affirmative answer for elliptic curves over number fields when the prime p is 3. Moreover, he shows that this is true even if one restricts the number fields L to be of the form $K(\sqrt[3]{m})$ for some $m \in K$.

The idea is as follows. Let us call an element of $L \setminus K$ a *strictly-L* element of L. We note that for a prime p, the 'yes' answer to Question 1 is equivalent to there being infinitely many extensions L/K of degree p such

that $\mathrm{Jac}(\mathcal{C})(L)$ contains a strictly-L point, i.e., $\mathrm{Jac}(\mathcal{C})(L) \setminus \mathrm{Jac}(\mathcal{C})(K) \neq \emptyset$. This is essentially shown in [1] but we shall prove it now for the sake of completeness.

LEMMA 1. *Let $\mathcal{C}$ be a smooth, projective curve defined over K with $g(\mathcal{C}) \geq 1$ and p a prime number. Let $\mathcal{J} = \mathrm{Jac}(\mathcal{C})$. Then there are infinitely many degree p extensions L/K such that $\mathrm{rk}(\mathcal{C}/L) > \mathrm{rk}(\mathcal{C}/K)$ if and only if there are infinitely many such L/K such that $\mathcal{J}(L)$ has a strictly-L point.*

Proof. Clearly if the rank increases then a new point has been obtained, so one direction is clear. For the other direction we note that the only way in which a new point does not lead to an increase in rank is if the point divides a point in $\mathcal{J}(K)$. We claim this can only happen in finitely many degree p extensions. First of all, let F be the compositum of all the degree p fields. Then the torsion of $\mathcal{J}(F)$ is finite since the residue field for each prime of F is finite. Hence there are only finitely many degree p extensions in which we obtain new torsion.

Having dealt with new points which divide the identity we need to consider points which divide other points in $E(K)$. Such points in an extension L/K would lead to the map

$$f : \frac{\mathcal{J}(K)}{\ell\mathcal{J}(K)} \to \frac{\mathcal{J}(M)}{\ell\mathcal{J}(M)}$$

failing to be injective for some prime ℓ where M is the Galois closure of L. The kernel of f is contained in the cohomology group $H^1(\mathrm{Gal}(M/K), \mathcal{J}[\ell])$. Since $\mathrm{Gal}(M/L)$ has order dividing $p!$ we see that if $\ell > p$ then this cohomology group vanishes, implying that f is injective. For $\ell \leq p$ it suffices to observe that there are only finitely many degree p extensions L in which we can gain a point $Q \in \mathcal{J}(L)$ such that $\ell Q = R$ for some $R \in E(K)$. To see this note that $\ell Q = R = a_1 P_1 + \cdots + a_r P_r$ where the P_i generate $\mathcal{J}(K)$ and by repeatedly subtracting multiples of ℓP_i for each i we can assume that $a_i < \ell$. There are only finitely many such R and hence only finitely many degree p extensions in which they become divisible by ℓ.

Thus we see that an infinitude of new points all in different degree p extensions implies that the rank must increase in infinitely many of those extensions. ∎

The next step is to find infinitely many L/K of degree p such that $\mathcal{J}(L)$ has a strictly-L point. This is achieved by constructing such points on $\mathcal{C}$ itself and then carrying them over to $\mathcal{J}$ via the embedding

$$j : \mathcal{C}(\overline{K}) \to \mathrm{Pic}^0(\mathcal{C})(\overline{K}) = \mathcal{J}(\overline{K}), \qquad R \mapsto (R) - (Q),$$

where $Q \in \mathcal{C}(K)$ and (R) denotes the divisor class of R. We note that since

$Q \in \mathcal{C}(K)$ it follows that if R is a strictly-L point on $\mathcal{C}$ then $j(R)$ is a strictly-L point on $\mathcal{J}$. So all that remains is to construct the points on $\mathcal{C}$.

It is a fact that every such $\mathcal{C}$ is birational over K to a plane curve $\mathcal{C}'$ which has the same genus but is not necessarily smooth. We can resolve these singularities by blowing up to obtain a smooth curve $\mathcal{C}'_s$. Blowing up carries strictly-L points on $\mathcal{C}'$ to strictly-L points on $\mathcal{C}'_s$ and since $\mathcal{C}$ is birational to $\mathcal{C}'_s$ over K we have $\mathrm{rk}(\mathcal{C}/L) = \mathrm{rk}(\mathcal{C}'_s/L)$ for all L/K. Thus it is sufficient to construct strictly-L points on $\mathcal{C}'$.

We do this by constructing covering maps $\phi : \mathcal{C}_1 \to \mathcal{C}'$ where $\mathcal{C}_1$ has degree p and where the map ϕ and the curves $\mathcal{C}_1$ are explicit. Indeed $\mathcal{C}_1$ and ϕ will be constructed so that the strictly-L points we find on $\mathcal{C}_1(L)$ are in fact S-integers (for a fixed set of places S) and such that ϕ carries strictly-L points on $\mathcal{C}_1$ to strictly-L points on $\mathcal{C}'$. This will allow us to apply Siegel's Theorem (e.g., [5, Part D]) to assert that $\mathcal{C}_1(L)$ can have only finitely many S-integer points and so we can deduce that the infinitely many points on $\mathcal{C}_1$ we generate must lie inside infinitely many different degree p extensions, as desired.

3. Proof of Theorem 1. Let us suppose that we have an irreducible curve $\mathcal{C}$ defined over K and with genus $g(\mathcal{C}) \geq 1$. We shall suppose that $\mathcal{C}$ is birational to a plane curve $\mathcal{C}'$ of the form

$$\mathcal{C}' : g(y) = f(x)$$

where f and g are polynomials having degree k and d respectively. We suppose further that $(d,k) = 1$, which allows us to assume that f and g are both monic, and also, given some $q \in \mathcal{O}_K$, that their non-leading coefficients are divisible by q^n for any $n \geq 0$. Since $(d,k) = 1$ there are $a, b \in \mathbb{Z}$ such that $bk - ad = 1$. Interchanging x and y if necessary, we can assume that $a, b > 0$.

Consider the following rational map:

$$\phi : \mathbb{A}^2_K \to \mathbb{A}^2_K, \qquad (u,t) \mapsto \left(u + \frac{q^b}{t^n}, q^a t^m\right),$$

where $n, m > 0$ are integers to be specified later and $q \in \mathcal{O}_K$ is a generator of any prime ideal. We shall construct a cover of $\mathcal{C}'$ by taking the Zariski closure of the preimage of $\mathcal{C}'$ under ϕ. Call this curve $\mathcal{C}_1$. It is cut out by the following equation:

$$\begin{aligned}\mathcal{C}_1 : h(u,t) := g(q^a t^m)t^{kn} - f(u)t^{nk} - f^{(1)}(u)q^b t^{n(k-1)} \\ - \frac{f^{(2)}(u)}{2!}t^{n(k-2)}q^{2b} - \cdots - q^{kb} = 0.\end{aligned}$$

Note that h is of degree $dm + kn$ in t, has leading coefficient q^{ad} and has all its coefficients in $\mathcal{O}_K$. The most important fact for us is the following.

LEMMA 2. *The polynomial h is irreducible over K.*

Proof. Let us first of all assume (after perhaps performing a change of variables on our base curve $\mathcal{C}'$) that the non-leading coefficients of $g(y)$ and $f(x)$ are all divisible by q^{da+1}. Suppose that h is reducible. Then for any specialisation of the variable u to an element $m \in K$ the resulting polynomial $h(m,t)$ must be reducible into two polynomials in t of degree at least one. Consider then the polynomial $h(0,t)$. Since $(1/i!)f^{(i)}(0)$ is just the ith coefficient of f we see that every coefficient of $h(0,t)$ is divisible by q^{da}. Hence $h(0,t) = q^{da}h_1(t)$. Since $kb - ad = 1$ we note that the constant term in $h_1(t)$ is q, the leading term is 1 and every other coefficient is divisible by q. Hence $h_1(t)$ is Eisenstein and thus irreducible. Therefore, $h(0,t)$ and thus $h(u,t)$ are irreducible also. ∎

We are now in a position to complete the proof of Theorem 1.

Proof of Theorem 1. We want to find an $N(\mathcal{C}) > 0$ such that for all primes $p \geq N(\mathcal{C})$ we have an affirmative answer to Question 1. We formed a cover $\mathcal{C}_1$ of $\mathcal{C}'$ which is given by $\mathcal{C}_1 : h(u,t) = 0$ where h has degree $md+nk$. Now $(k,d) = 1$, therefore if we let n range in $0 \leq n \leq d-1$ then nk occupies all the congruence classes modulo d. This is easily seen: if $ak \equiv bk \pmod{d}$ then $a \equiv b \pmod{d}$. Therefore we can express every number greater than $k(d-1)$ in the form $md+nk$ and in particular we can represent every prime $p > k(d-1)$ by $p = md + kn$ with $0 < m$ and $0 < n \leq d-1$.

Now we are in a good position. We can form a curve $\mathcal{C}_1 : h(u,t) = 0$ of degree p with $h(u,t) \in \mathcal{O}_K$ and irreducible for all primes $p \geq k(d-1)+1 = N(\mathcal{C})$. By Hilbert's Irreducibility Theorem we can find infinitely many $m \in K$ such that $h(m,t)$ is an irreducible polynomial of degree p in t. Take such an m and let α_m be a root of $h(m,t)$. Then $Q_m = (m, \alpha_m) \in \mathcal{C}_1(L_m)$ where $L_m = K(\alpha_m)$. Note that $[L_m : K] = p$. We can form infinitely many such points and since $\phi|_{\mathcal{C}_1} : \mathcal{C}_1 \to \mathcal{C}'$ has degree strictly less than p we see that strictly-L_m points on $\mathcal{C}_1$ are taken to strictly-L_m points on $\mathcal{C}'$. (This is in virtue of the fact that if p is prime and $l < p$ then l and p are coprime—this is the only place we use the primality of p in our argument.)

By Lemma 1, all we need to show now is that the extensions L_m do not coincide too often. To see this we note that if $S = \{\mathfrak{P} \in \operatorname{Spec} \mathcal{O}_{L_m} : q \in \mathfrak{P}\}$ then the roots of the polynomial $g(m,t)$ are all S-integers and by Siegel's Theorem there are only finitely many S-integers lying on $\mathcal{C}'$. Therefore, there must be infinitely many different extensions L_m and so by Lemma 1 we are done. ∎

We can now use this result to prove some interesting corollaries as stated in the introduction.

COROLLARY 1. *Let $\mathcal{C}$ be birational over K to the plane curve cut out by the equation $\mathcal{C}' : y^2 = g(x)$ where $k = \deg(g)$ is odd. Then there is an $N(\mathcal{C})$ such that for all primes $p \geq N(\mathcal{C})$ Question 1 has an affirmative answer. What is more, we can take $N(\mathcal{C}) = k + 1$.*

Proof. This is a straightforward application of Theorem 1. The proof of the theorem gives $N(\mathcal{C}) = k(d-1) + 1 = k + 1$. ∎

This has the following pleasing corollary.

COROLLARY 2. *Question 1 has an affirmative answer for every prime p when $\mathcal{C}$ is an elliptic curve.*

Proof. Since elliptic curves can be written in the form $\mathcal{C} : y^2 = x^3 + Ax + B = g(x)$, Corollary 1 gives us the result for all primes $p \geq 5$. The cases of the primes 2 and 3 are not hard to prove. For $p = 2$, if we take $m \in \mathcal{O}_K$ then $P_m = (m, \sqrt{f(m)})$ lies on $\mathcal{C}$. The value $f(m)$ cannot be a square infinitely often or else $E(\mathcal{O}_K)$ would be infinite, contradicting Siegel's Theorem. The same theorem also tells us that the points P_m must lie in infinitely many different quadratic extensions. For $p = 3$, we apply the same argument by putting $y = m \in \mathcal{O}_K$. This gives a monic cubic polynomial in x. If this is reducible then there must be a linear factor and since the cubic is monic this yields an $\mathcal{O}_K$ point on $\mathcal{C}$. Thus the cubics obtained this way must be irreducible almost all of the time and so give us our desired degree 3 points. ∎

REMARK. It is worth remarking that the degree p extensions for $p > 3$ which are constructed in the proof of Theorem 1 take on, for elliptic curves, a particularly simple form. For a curve of the shape $y^2 = x^3 + Ax + B$ the constructed degree p extensions are of the form $K[t]/g(k,t)$ where

$$g(k,t) = q^2t^p - (k^3 + Ak + B)t^3 - (3k^2 + A)qt^2 - 3q^2kt - q^3,$$

q is any prime in $\mathcal{O}_K$ and k is to be considered as an element of $\mathcal{O}_K$ so that $g(k,t) \in K[t]$. If we specify k so that $g(k,t)$ is irreducible then the extension is generated by a root of a polynomial of the form $q^2t^p - f(t)$ where $f \in \mathcal{O}_K[t]$ is a cubic.

4. A result when the degrees are not coprime. A major hypothesis in the statement of Theorem 1 is that the degrees of the two polynomials involved be coprime. In this final section we shall consider an example of a class of curves not fitting this restriction but where something can still be said.

THEOREM 2. *Let $\mathcal{C}$ be a smooth, irreducible curve of positive genus, defined over K and birational to a plane curve of the shape*

$$\mathcal{C}' : y^d = x^k + D$$

where $D \in \mathcal{O}_K^\times$ (and with no restrictions on d or k). Then there is an $N(\mathcal{C}) > 0$ such that for all primes $p > N(\mathcal{C})$ there are infinitely many extensions L/K of degree p where $\mathrm{rk}(\mathcal{C}/L) > \mathrm{rk}(\mathcal{C}/K)$.

Proof. We follow our usual strategy of constructing points on $\mathcal{C}'$. We begin by covering $\mathcal{C}'$ by the curve

$$\mathcal{C}_1 : y^n = x^n + D$$

where $n = \mathrm{lcm}(d, k)$. Note that we can assume that q^n divides D exactly for any q outside of a finite set. Let us assume then that q^{2n} exactly divides D for some prime q. Let $w = y - x$; then by factorising $y^n - x^n$ we have

$$\mathcal{C}_1 : w^n + w^{n-1}x + \cdots + wx^{n-1} = D.$$

Now, we are going to form a cover of $\mathcal{C}_1$ by looking at its preimage under the map $\phi : \mathbb{A}^2_{(u,t)} \to \mathbb{A}^2_{(x,w)}$ given by

$$\phi(u, t) = (qt^s + u, q^n t^r).$$

As we have seen, the key point is showing that the curve $\mathcal{C}_2 : h(u, t) = 0$ given as the Zariski closure of $\phi^{-1}(\mathcal{C}_1)$ is irreducible. Consider the specialisation $h(0, t)$. This is given by

$$h(0,t) = (q^n t^r)^n + (q^n t^r)^{n-1}(qt^s) + \cdots + (q^n t^r)(qt^s)^{n-1} - D$$

and one can observe that every coefficient is divisible by q^{2n} except for the coefficient of $t^{(n-1)s+r}$ (the last non-constant monomial in the equation above). This has a coefficient of q^{2n-1} and so we can divide out by this to get an Eisenstein polynomial, showing that $h(0, t)$ is irreducible and thus so is $h(u, t)$.

If we have $s > r$ in ϕ then $h(u, t)$ is of degree $(n - 1)s + r$ in t. We can express every prime $p \geq (n - 1)(n - 2)$ as $p = (n - 1)s + r$ for some r, s with $r > s$ and so we see, by Hilbert's Irreducibility Theorem, that for such a p we can specialise $h(u, t)$ to $h(m, t)$ for infinitely many $m \in K$ to get an irreducible polynomial of degree p. The roots of this polynomial will then correspond to points strictly in a degree p extension L/K. These points are then mapped to our original plane curve $\mathcal{C}'$. Since p is larger than the degrees of any of the covering maps involved we see that the end point is still strictly-L. Thus we are done by Lemma 1. ∎

Acknowledgments. I would like to thank Tim Dokchister for his encouragement and his reading of earlier drafts. I would also like to express my gratitude to Vladimir Dokchitser and Dan Loughran for answering several questions and finally to Ariyan Javanpeykar for reminding me that there is more in mathematics than elliptic curves! This work was supported by an EPSRC Doctoral Training Award.

References

[1] T. Dokchitser, *Ranks of elliptic curves in cubic extensions*, Acta Arith. 126 (2007), 357–360.

[2] T. Dokchitser and V. Dokchitser, *Elliptic curves with all quadratic twists of positive rank*, Acta Arith. 139 (2009), 193–197.

[3] J. Fearnley, H. Kisilevsky and M. Kuwata, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*, J. London Math. Soc. 86 (2012), 539–557.

[4] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in: Lecture Notes in Math. 751, Springer, 1979, 108–118.

[5] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, Springer, 2000.

Dave Mendes da Costa
School of Mathematics
University Walk
Bristol, BS8 1TW, United Kingdom
E-mail: djmdac@gmail.com

Received on 14.9.2012
and in revised form on 9.7.2013 (7193)