Ranks of quadratic twists of Jacobians of generalized Mordell curves

Tomasz Jędrzejak

Uniwersity of Szczecin

JA, 3rd July 2023

Introduction

Definition

An **algebraic curve** is a one-dimensional projective algebraic variety. In other words, an algebraic (plane) curve defined over a field K is a set

$$\left\{[X,Y,Z]\in\mathbb{P}^2\left(\bar{K}\right):F\left(X,Y,Z\right)=0\right\},$$

where $F\in K\left[X,Y,Z\right]$ is a homogenous polynomial.

Definition

A curve is called **non-singular** or **smooth** if every its point is non-singular, i.e., at least one partial derivative of F in it does not vanish.

Definition

An **elliptic curve** defined over a field K is a non-singular algebraic curve E of genus 1 with a distinguished point $P_0\in E\left(K\right)$. Such a curve is isomorphic to a non-singular plane curve given by the Weierstrass equation.

Introduction

In the case $K = \mathbb{Q}$ the (affine) equation of an elliptic curve can take the form:

$$E : y^2 = x^3 + ax + b,\ a, b \in \mathbb{Z}.$$

Non-singularity means that the polynomial $x^3 + ax + b$ has no repeated roots (in $\mathbb{C}$), i.e. its discriminant does not vanish.
The elliptic curve $E_k : y^2 = x^3 + k^2 ax + k^3 b$ is a quadratic twist of E where k is a squarefree integer.

Example

Mordell elliptic curve

$$E_1 : y^2 = x^3 - 1$$

and its quadratic twists

$$E_k : y^2 = x^3 - k^3.$$

Introduction

Definition

A **hyperelliptic curve** C of genus $g \geq 1$ defined over K (char $K \neq 2$) is a non-singular algebraic curve given by an affine equation of the form $y^2 = f(x)$, where $f \in K[x]$ is monic and has the degree $2g+1$.

Definition

An **abelian variety** is a projective algebraic variety which is also an algebraic group, that is the group laws are morphisms.

The important examples of abelian varieties are elliptic curves.
In contrast, hyperelliptic curves of genus > 1 are not abelian varieties!
But with any such curve C of genus g we can associate an abelian variety $Jac(C)$ of dimension g called **Jacobian variety** (or short **Jacobian**) of the curve C such that any elliptic curve is isomorphic to its Jacobian (in general, we have only an embedding $C \hookrightarrow Jac(C)$).

Introduction

As a group Jacobian $Jac\left(C\right)$ is isomorphic to the Picard group $\mathrm{Pic}^0\left(C\right)$ of C, that is to the factor group of degree zero divisors by principal divisors. If an abelian variety A is the Jacobian of the hyperelliptic curve $y^2 = f\left(x\right)$ then its quadratic twist A_k (by squarefree integer k) is the Jacobian of the twisted curve $ky^2 = f\left(x\right)$.

Example

The Jacobian $J_{q,b}$ (of dimension $\left(q-1\right)/2$) of the hyperelliptic curve

$$C_{q,b} : y^2 = x^q - b^q$$

where q is an odd prime and b is a squarefree integer is the quadratic twist (by b) of the Jacobian $J_{q,1}$ of $C_{q,1}$, which is a generalized Mordell curve of degree q.

Introduction

K-number field (i.e., finite extensions of $\mathbb{Q}$)
A-abelian variety
$A(K)$-Mordell-Weil group of K-rational points of A

Theorem (Mordell - Weil)

Group $A(K)$ is finitely generated.

Mordell proved it in 1922-23 for elliptic curves over $\mathbb{Q}$. Weil in 1928 extended it to abelian varieties over number fields.

Corollary

Group $A(K)$ is isomorphic to $T \times \mathbb{Z}^r$, where T is a finite abelian and r is nonnegative integer.

Number r we call *rank* of $A(K)$, and denote by $\operatorname{rank} A(K)$. The group T is the torsion subgroup of $A(K)$, we denote it by $A(K)_{tors}$.

Introduction

Conjecture (Goldfeld 1979)

Average rank of the quadratic twists of any given elliptic curves over $\mathbb{Q}$ is 1/2. *Consequently, for any elliptic curve over rationals, asymptotically there are at least half of quadratic twists with rank* 0.

A weaker conjecture states that the rank zero quadratic twists comprise a positive proportion of all quadratic twists of a given curve.

- **Ono** and **Skinner** (1998): $|\{|k| \leq X : \operatorname{rank} E_k(\mathbb{Q}) = 0\}| >> X/\log X$.
- **Iwaniec** and **Sarnak** (2000, assuming the Riemann Hypothesis): $X/\log X$ can be replaced by X.
- **Smith** (2017 on arxiv): if the Birch and Swinnerton-Dyer conjecture holds for the set of quadratic twists of E, Goldfeld's conjecture holds for E, assuming that $E/\mathbb{Q}$ has full rational 2-torsion but E has no rational cyclic subgroup of order four.

Introduction

Conjecture (Silverman 1997)

For any given elliptic curve $E/\mathbb{Q}$ there are infinitely many primes p such that $\operatorname{rank} E_p(\mathbb{Q}) = 0$, *and there are infinitely many primes p such that* $\operatorname{rank} E_p(\mathbb{Q}) > 0$.

Juyal, Moody and **Roy** (2022) studied ranks of quadratic twists of a Mordell elliptic curve $E_1 : y^2 = x^3 - 1$.
It is natural to ask similar questions about the ranks of quadratic twists of higher dimensional abelian varieties over $\mathbb{Q}$, e.g. Jacobians of algebraic curves of genus > 1.
Now we consider a two-parameter family of hyperelliptic curves over $\mathbb{Q}$, and their Jacobian varieties:

$$\begin{aligned} C_{q,b} &: y^2 = x^q - b^q, \\ J_{q,b} &= Jac\left(C_{q,b}\right), \end{aligned}$$

where q is an odd prime and b is a non-zero squarefree integer.

Results

Theorem (1)

Let $b = \pm 2^{e_1} q^{e_2} p_1 \ldots p_k$ *where* $e_1, e_2 \in \{0, 1\}$, $p_1, \ldots, p_k$ *are distinct odd primes not equal to* q. *Assume that* 2 *and all* p_i *are primitive roots mod* q.
1) If $q \equiv 1 \pmod 4$ *then*

$$\operatorname{rank} J_{q,b}(\mathbb{Q}) \le \frac{q-1}{2}.$$

2) If $q \equiv 3 \pmod 4$ *then*

$$\operatorname{rank} J_{q,b}(\mathbb{Q}) \le \frac{q-1}{2} + k',$$

where $k' = |\{i : p_i \equiv 3 \pmod 4\}| \le k$. *In particular, if* $p_i \equiv 1 \pmod 4$ *for* $i = 1, \ldots, k$ *then also* $\operatorname{rank} J_{q,b}(\mathbb{Q}) \le (q-1)/2$.

Results

2 must be a primitive root modulo q.

Conjecture (Artin 1927)

A given integer a that is neither a square nor -1 (e.g. 2) is a primitive root modulo infinitely many primes p.

Heath-Brown (1986): at least one of 2, 3, or 5 is a primitive root modulo infinitely many primes.

List of all prime numbers less than 1000 for which 2 is a primitive root: 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, 179, 181, 197, 211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461, 467, 491, 509, 523, 541, 547, 557, 563, 587, 613, 619, 653, 659, 661, 677, 701, 709, 757, 773, 787, 797, 821, 827, 829, 853, 859, 877, 883, 907, 941, 947.

The smallest such q is 3, and $J_{3,b}$ form the family of elliptic curves considered by Jual et al. The next one is $q = 5$, and we will focus on this case.

Results

For simplicity we will write briefly C_b and J_b instead of $C_{5,b}$ and $J_{5,b}$ respectively.
Since ± 2 are primitive roots modulo 5, we immediately obtain from Theorem 1, that if any prime divisor of b not equal to 5 is congruent to $\pm 2 \pmod 5$, then $\operatorname{rank} J_b(\mathbb{Q}) \leq 2$. But careful examination gives a better bounds for the ranks.

Theorem (2)

Assume that $b = \pm 2^{e_1} 5^{e_2} p_1 \dots p_k$ *where* $e_1, e_2 \in \{0, 1\}$, $p_1, \dots, p_k$ *are distinct odd primes which are congruent to* $\pm 2 \pmod 5$. *Then* $\operatorname{rank} J_b(\mathbb{Q}) \leq 1$, *and moreover, if* $b \equiv 3 \pmod 4$ *then* $\operatorname{rank} J_b(\mathbb{Q}) = 0$.

We also allow $k = 0$.

Results

For any non-zero integer m let $\omega(m)$ denote the number of all distinct prime divisors of m, and $\operatorname{sgn} m$ denote the sign of m.

Corollary

For any integer $n \geq 1$ and any $\varepsilon \in \{1, -1\}$ there exist infinitely many squarefree integers b such that $\operatorname{rank} J_b(\mathbb{Q}) = 0$, $\omega(b) = n$, and $\operatorname{sgn} b = \varepsilon$.

Corollary

There are infinitely many primes p such that $\operatorname{rank} J_p(\mathbb{Q}) = 0$, and there are infinitely many primes p such that $\operatorname{rank} J_p(\mathbb{Q}) = 1$ under assumption of the Parity Conjecture. More precisely,

$$\operatorname{rank} J_p(\mathbb{Q}) = \begin{cases} 0 & \textit{if } p \equiv 3, 7 \pmod{20}, \\ 1 & \textit{if } p \equiv 13, 17 \pmod{20} \textit{ and the Parity Conjecture holds.} \end{cases}$$

Parity Conjecture (in our case): $(-1)^{\operatorname{rank} J_b(\mathbb{Q})} = W_b$ where W_b denote the global root number for C_b.

Results

We can deduce the complete lists of rational points on $C_{q,b}$, if rank $J_{q,b}(\mathbb{Q}) = 0$.

Corollary

If rank $J_{q,b}(\mathbb{Q}) = 0$ *and* $b \neq -1, (-1)^{(q+1)/2} q$ *then* $C_{q,b}(\mathbb{Q}) = \{\infty, (b,0)\}$. *In particular, if* $b \neq -1$ *is of the form as in Theorem 2 and* $b \equiv 3 \pmod 4$ *then* $C_b(\mathbb{Q}) = \{\infty, (b,0)\}$. *Moreover,* $C_{-1}(\mathbb{Q}) = \{\infty, (-1,0), (0,1), (0,-1)\}$.

Observe that if $(x,y) \in C_{q,b}(\mathbb{Q})$ and $x \in \mathbb{Z} \setminus \{0\}$ then $(-b,y) \in C_{q,-x}(\mathbb{Q})$.

Results

If rank $J_b(\mathbb{Q}) = 1$, then, since C_q has genus 2, using the Coleman-Chabauty method and Magma, we obtain.

Corollary (4)

If rank $J_b(\mathbb{Q}) = 1$ *then* $|C_b(\mathbb{Q})| \leq 4$ *with possible exceptions for* $b = -30, -15, 10, 30$ *when we have* $|C_b(\mathbb{Q})| \leq 6$. *In particular, this statement is true, if b is of the form as in Theorem 2 and* $b \equiv 1, 2 \pmod 4$. *Furthermore,*

$$\begin{aligned}
C_{-726}(\mathbb{Q}) &= \{\infty, (-726, 0), (-242, 14172488), (-242, -14172488)\},\\
C_{-6}(\mathbb{Q}) &= \{\infty, (-6, 0), (-2, 88), (-2, -88)\},\\
C_{-2}(\mathbb{Q}) &= \{\infty, (-2, 0), (2, 8), (2, -8)\},\\
C_{2}(\mathbb{Q}) &= \{\infty, (2, 0), (6, 88), (6, -88)\},\\
C_{242}(\mathbb{Q}) &= \{\infty, (242, 0), (726, 14172488), (726, -14172488)\},\\
C_{b}(\mathbb{Q}) &= \{\infty, (b, 0)\} \ \textit{for } b = -10, -3, 1, 5, 6.
\end{aligned}$$

Results

Since both Goldfeld's and Silverman's Conjectures are concerned also with positive ranks, we establish a result in this direction. Recall that the squarefree part of non-zero integer b is the largest squarefree divisor of b.

Theorem (3)

For any odd prime q there exist infinitely many integers b with distinct squarefree parts (hence there exist infinitely many non-isomorphic over $\mathbb{Q}$ curves $C_{q,b}$) such that $C_{q,b}$ has a $\mathbb{Q}$-rational point with non-zero coordinates, and consequently $\operatorname{rank} J_{q,b}(\mathbb{Q}) \geq 1$.

Ingredients of the proofs: 2-descent on hypereliptic curves

Given a hyperelliptic curve C over K and its Jacobian J_C it is possible, to bound rank $J_C(K)$ from above by computing the order of a suitable Selmer group. For any positive integer m, the factor group $J_C(K)/mJ_C(K)$ embeds into m-Selmer group $S^m(J_C, K)$. Hence knowing the torsion and the size of this Selmer group, we deduce the upper bound for the rank.

One usually looks at $m = 2$, since the multiplication by 2 isogeny is always available, has low degree, and its kernel is easily determined. This method is called 2-descent.

Ingredients of the proofs: 2-descent on hypereliptic curves

A general way to find a Selmer group is to study principal homogenous spaces. This is feasible for elliptic curves but becomes unwieldy in genus greater than 1. Fortunately, there is a method that avoids homogenous spaces, if one is willing consider K of moderate degree, in particular $K = \mathbb{Q}$.

Cassels (1983) first described the basic algorithm in the genus two case. **Schaefer** (1995) puts it into a more general framework (e.g. for higher genus and superelliptic curves).
Stoll (2006) detailed and exhaustively presented the algorithms used later in Magma Computational Algebra System. Also Stoll investigated the family of hyperellitic curves $y^2 = x^p + a$ (p is an odd prime) and their Jacobians, and obtained many arithmetic facts.

Ingredients of the proofs: 2-descent on hypereliptic curves

Let C be a hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 2$. Assume that C has a plane model $y^2 = f\left(x\right)$, where $f \in \mathbb{Z}\left[x\right]$.
A degree 0 divisor of C over $\mathbb{Q}$ is said to be a *good*, if its support does not include the point at infinity ∞ and points with zero y- coordinate.
Let $D = \sum n_P P$ be a good divisor of C over K. We set

$$\delta_K\left(D\right) := \prod_P \left(x_P - T\right)^{n_P} \in L_K^*,$$

where $P = \left(x_P, y_P\right)$ and $L_K = K\left[T\right]/\left(f\left(T\right)\right)$. We will write $\delta := \delta_{\mathbb{Q}}$ and $\delta_p := \delta_{\mathbb{Q}_p}$ for any (rational) prime p or $p = \infty$.

Ingredients of the proofs: 2-descent on hypereliptic curves

Let $N_{L_K/K} : L_K \longrightarrow K$ denote the norm map (a generalization of fields extension norm). Note that

- $N_{L_K/K}(L_K^*) \subset K^*$,
- $N_{L_K/K}$ is a well-defined group homomorphism $L_K^*/L_K^{*2} \longrightarrow K^*/K^{*2}$,
- the map δ_K is a well-defined map from $J(K)$ to the $\ker(N_{L_K/K} : L_K^*/L_K^{*2} \rightarrow K^*/K^{*2})$, and
- it is injection from $J(K)/2J(K)$ to L_K^*/L_K^{*2}.

Ingredients of the proofs: 2-descent on hypereliptic curves

$L := L_{\mathbb{Q}} = \mathbb{Q}[T]/(f(T)) \cong \prod L_i$, where L_i are fields corresponding to the irreducible factors of f.
Let S be a finite set containing $2, \infty$ and all primes of bad reduction for J.
Suppose $l \in L^*$maps to $l_i \in L_i^*$. Then l is *unramified outside* S if for each i, the field extension $L_i\left(\sqrt{l_i}\right)/L_i$ is unramified outside of primes in L_i lying over primes of S.
This property depends only on l modulo L^{*2} and the set G of elements of L^*/L^{*2} which are unramified outside S is a group.
Let H be the kernel of the norm map $G \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$, i.e.,

$$H = G \cap \ker N_{L/\mathbb{Q}} \subset L^*/L^{*2}.$$

We have

$$\delta(J(\mathbb{Q})) \subset H.$$

Ingredients of the proofs: 2-descent on hypereliptic curves

Let $L_p := L_{\mathbb{Q}_p} = \mathbb{Q}_p [T] / (f(T))$. The following diagram is commutative.

$$\begin{tikzcd}
0 \arrow[r] & J(\mathbb{Q})/2J(\mathbb{Q}) \arrow[r, "\delta"] \arrow[d] & L^*/L^{*2} \arrow[d] \\
0 \arrow[r] & \prod_{p\in S} J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \arrow[r, "\prod \delta_p"] & \prod_{p\in S} L_p^*/L_p^{*2}.
\end{tikzcd}$$

From this diagram and the above consideration one can deduce that the 2-Selmer group $S^2(J, \mathbb{Q})$ of the Jacobian of C over $\mathbb{Q}$ can be identified with the set of elements in the kernel of the norm from L^*/L^{*2} to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ that map to the image of δ_p in L_p^*/L_p^{*2} for all primes $p \in S$. Moreover, it consists of the elements which are unramified outside S.

Ingredients of the proofs: 2-descent on hypereliptic curves

Hence

$$S^2(J,\mathbb{Q}) = \{h \in H : h_p \in \operatorname{im}\delta_p \text{ for all } p \in S\}$$

where h_p denote the image of h in L_p^*/L_p^{*2}. The Selmer group is effectively computable and this will give bounds for the size of $J(\mathbb{Q})/2J(\mathbb{Q})$, since the latter embeds into $S^2(J,\mathbb{Q})$. By the Mordell-Weil's theorem, $J(\mathbb{Q})/2J(\mathbb{Q}) \cong J(\mathbb{Q})_{tors}/2J(\mathbb{Q})_{tors} \times (\mathbb{Z}/2\mathbb{Z})^r$, so in order to estimate the rank is helpful to estimate the size of $J(\mathbb{Q})/2J(\mathbb{Q})$. In conclusion,

$$\operatorname{rank} J(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} S^2(J,\mathbb{Q}) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]$$

where the latter is the kernel of multiplication by 2 in $J(\mathbb{Q})$.

Ingredients of the proofs: squares in p-adic fields

By the Hensel lemma, we deduce several criterions of 'being squares' in $\mathbb{Q}_p$ and its finite extensions that we will use in the proofs of Theorems 1 and 2. For example, let $K_{2,q} = \mathbb{Q}_2\left(\zeta_q\right)$ where 2 is a primitive root modulo q. Then $K_{2,q}$ is an unramified degree $q-1$ extension of $\mathbb{Q}_2$, and so 2 is a uniformizer. If $\mathcal{O}_{2,q}$ is the valuation ring of $K_{2,q}$ then $\mathcal{O}_{2,q}/2\mathcal{O}_{2,q} \cong \mathbb{F}_{2^{q-1}}$. Note that any element of $K_{2,q}^*$ has the form $2^n u$ where $n \in \mathbb{Z}$ and $v_2\left(u\right) = 0$. For $q = 5$ we get

Criterion

An element $z = 2^n u$ is a square in $K_{2,5}^*$ if and only if $2 \mid n$ and the congruence $x^2 \equiv u \left(\mathrm{mod}\ 2^3\mathcal{O}_{2,5}\right)$ has a solution. The second condition is equivalent to $v_2\left(N_{K_{2,5}/\mathbb{Q}_2}\left(u - x^2\right)\right) \geq 12$ for some $x \in \mathcal{O}_{2,5}$ with $v_2\left(x\right) = 0$.

We wrote a code in Magma that checks if a given element belongs to $\mathbb{Q}_2\left(\zeta_5\right)^{*2}$.

Ingredients of the proofs: Coleman-Chabauty method

Proposition (Coleman-Chabauty bounds 1985)

Let C be a smooth curve of genus $g \geq 2$ defined over $\mathbb{Q}$, and $l > 2g$ be a prime of good reduction. If the Jacobian of C has rank less than g, then $|C(\mathbb{Q})| \leq |C(\mathbb{F}_l)| + 2g - 2$.

Proof of Corollary 4.

By Stoll's result, we obtain $|C_b(\mathbb{Q})| \leq 6$, and if moreover, b has a prime factor > 5, then $|C_b(\mathbb{Q})| \leq 4$. Now we use Magma. First, for certain b (including $b \mid 30$) we looked for $\mathbb{Q}$-rational points on C_b by using the command Points and found non-trivial points (x, y) (i.e., $y \neq 0$) for $b \in \{-726, -6, -2, 2, 242\}$. For $b = -10, -3, 1, 5, 6$ we found no such points, but we did find an element of infinite order in the Jacobian. We have that rank $J_b(\mathbb{Q}) = 1$ for such b This bound is less than the genus of C_b which is equal to 2, so by using the Coleman-Chabauty method implemented in Magma for genus 2 curves over $\mathbb{Q}$, we are done. □

Ingredients of the proofs: positive rank

Proof of Theorem 3.

Let prime $p \neq q$, and let $a = p + 1$, and $b = a^q - 1$. Observe that $\left(ab, b^{(q+1)/2}\right) \in C_{q,b}(\mathbb{Q})$, and since $ab \neq 0$, we obtain, that the divisor $\left(ab, b^{(q+1)/2}\right) - \infty$ gives the element of infinite order in $J_{q,b}(\mathbb{Q})$. Next we have $b = p\left(a^{q-1} + \ldots + a + 1\right)$ and $a^{q-1} + \ldots + a + 1 \equiv q \pmod{p}$. Therefore $\gcd\left(p, a^{q-1} + \ldots + 1\right) = 1$, and so p divides the squarefree part of b. Consequently, there are infinitely many b with distinct squarefree parts such that $\operatorname{rank} J_{q,b}(\mathbb{Q}) > 0$. Since C_{q,b_1} is isomorphic (over $\mathbb{Q}$) to C_{q,b_2} if and only if $b_1/b_2 \in \mathbb{Q}^{*2}$, there exist infinitely many curves $C_{q,b}$ (non-isomorphic over $\mathbb{Q}$) where $\operatorname{rank} J_{q,b}(\mathbb{Q}) > 0$, which is our claim. □

References

- W. S. Cassels, *The Mordell-Weil group of curves of genus 2.*, in: M. Artin, J. Tate (eds.) *Arithmetic and Geometry I*, Birkhäuser, Boston, (1983), 27-60.
- R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), 765-780.
- T. Jędrzejak, *Ranks of quadratic twists of Jacobians of generalized Mordell curves,* submitted
- A. Juyal, D. Moody, B. Roy, *On ranks of quadratic twists of a Mordell curve*, Ramanujan J. **59** (2022), 31-50.
- M. Stoll, *On the Arithmetic of the Curves $y^2 = x^l + A$ and their Jacobians*, J.reine angew. Math. **501** (1998), 171-189.
- M. Stoll,*On the number of rational squares at fixed distance from a fifth power*, Acta Arith. **98** (2001), no. 3, 245-277.

Acknowledgements

Merci pour votre attention!
Dziękuję za uwagę!
Thank you for the attention!