ALGEBRA, LOGIC AND NUMBER THEORY
BANACH CENTER PUBLICATIONS, VOLUME 108
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2016

A NOTE ON THE TORSION OF THE JACOBIANS OF SUPERELLIPTIC CURVES $y^q = x^p + a$

TOMASZ JĘDRZEJAK

Institute of Mathematics, University of Szczecin
Wielkopolska 15, 70-451 Szczecin, Poland
E-mail: tjedrzejak@gmail.com

Abstract. This article is a short version of the paper published in *J. Number Theory* 145 (2014) but we add new results and a brief discussion about the Torsion Conjecture. Consider the family of superelliptic curves (over $\mathbb{Q}$) $C_{q,p,a}\colon\ y^q = x^p + a$, and its Jacobians $J_{q,p,a}$, where $2 < q < p$ are primes. We give the full (resp. partial) characterization of the torsion part of $J_{3,5,a}(\mathbb{Q})$ (resp. $J_{q,p,a}(\mathbb{Q})$). The main tools are computations of the zeta function of $C_{3,5,a}$ (resp. $C_{q,p,a}$) over $\mathbb{F}_l$ for primes $l \equiv 1, 2, 4, 8, 11 \pmod{15}$ (resp. for primes $l \equiv -1 \pmod{qp}$) and applications of the Chebotarev Density Theorem.

1. Introduction. By the famous theorem of Mordell and Weil, the group of F-rational points $A(F)$ of an abelian variety A, where F is a number field, is finitely generated. In particular, the torsion subgroup $A(F)_{\mathrm{tors}}$ is finite. The classical Torsion Conjecture predicts that the order of $A(F)_{\mathrm{tors}}$ is bounded above by a constant depending only on $g := \dim(A)$ and F (weak form) or on g and $d := [F : \mathbb{Q}]$ (strong form) respectively. The strong version is sometimes called Uniform Boundedness Conjecture. Note that, by [5], the Torsion Conjecture for abelian varieties is equivalent to the Torsion Conjecture for Jacobian varieties.

Mazur [20] has proved this conjecture in the case $g = 1$ and $d = 1$. More precisely, he showed that the torsion part of an elliptic curve over $\mathbb{Q}$ is isomorphic to one of the following 15 groups: the cyclic group of order n where $n \in \{1, \dots, 10, 12\}$, the product of two cyclic group of order 2 and $2m$ where $m \in \{1, \dots, 4\}$. Next, Kenku–Momose [18] and Kamienny [17] have proved the Torsion Conjecture for $g = 1$ and $d = 2$ (they also gave

2010 *Mathematics Subject Classification*: Primary 11G10, 11G15, 11G20, 11G25, 11G30; Secondary 11L05, 11R45.

Key words and phrases: complex multiplication, diagonal curve, superelliptic curve, Jacobian, Jacobi sum, torsion part, zeta function.

The paper is in final form and no version of it will be published elsewhere.

DOI: 10.4064/bc108-0-11

the complete list of 26 torsion subgroups of elliptic curves over quadratic number fields). Then, Merel [21] achieved the proof of the (strong) Torsion Conjecture for elliptic curves over arbitrary number fields.

The case of higher dimensional abelian varieties remains widely open. However, for a special class of abelian varieties, namely CM (or CM-type) abelian varieties there are some nice results. For example, Silverberg [22, 23] proved the strong conjecture for abelian varieties of CM-type. Let us recall definitions. We say that an abelian variety A has complex multiplication (or short A is a CM abelian variety) by a number field K if there is an injective homomorphism $\iota : K \to End(A) \otimes \mathbb{Q}$ where $[K : \mathbb{Q}] = 2\dim(A)$ (K is necessarily a CM field, i.e. a totally imaginary quadratic extension of a totally real field). More generally A is said to be of CM-type if A is isogenous to a product of CM abelian varieties.

Among families of elliptic curves the family (over $\mathbb{Q}$)

$$E_a\colon\ y^2 = x^3 + a$$

is occupying the special place. Its j-invariant is equal to 0. The curve E_a has complex multiplication by a third root of unity. Let $E_a(\mathbb{Q})_{\mathrm{tors}}$ denote the torsion subgroup of the Mordell–Weil group $E_a(\mathbb{Q})$. The full characterization of $E_a(\mathbb{Q})_{\mathrm{tors}}$ is well known (see e.g. [19, Theorem 5.3, p. 134]).

The natural generalizations of such elliptic curves are the hyperelliptic curves

$$C_{2,n,a}\colon\ y^2 = x^n + a$$

and their Jacobian varieties $J_{2,n,a}$. In [14, Theorem 4.1] we give almost full characterization of the torsion parts of $J_{2,p,a}(\mathbb{Q})$ where p is an odd prime and a is a nonzero rational. Note that $J_{2,p,a}(\mathbb{Q})$ is a CM abelian variety (it has complex multiplication by a p-th root of unity).

The next natural generalizations are superelliptic (diagonal) curves

$$C_{m,n,a}\colon\ y^m = x^n + a$$

and their Jacobians $J_{m,n,a}$. In this paper we consider curves $C_{q,p,a}$ where q and p are distinct odd primes. Without loss of generality we assume that $q < p$ and a is a nonzero pq-powerfree integer. The genus g of $C_{q,p,a}$ is equal to $\frac{(q-1)(p-1)}{2}$. Note that the curve $C_{q,p,a}$ has good reduction at primes not dividing qpa. Consequently, over such primes its Jacobian $J_{q,p,a}$ has good reduction too. Moreover, $J_{q,p,a}$ has complex multiplication by a qp-th root of unity.

Our aim is to characterize the torsion part of $J_{q,p,a}(\mathbb{Q})$. We give the partial characterization of $J_{q,p,a}(\mathbb{Q})_{\mathrm{tors}}$ and the full description of $J_{3,5,a}(\mathbb{Q})_{\mathrm{tors}}$ (see Section 2). There is a nice analogy between those results and the formulas for $E_a(\mathbb{Q})_{\mathrm{tors}}$ and $J_{2,p,a}(\mathbb{Q})_{\mathrm{tors}}$.

Note also that the characterization of torsion subgroups of Jacobians may have interesting applications to ranks. For example, in the case of twisted Fermat's curves $C_m^p\colon\ x^p + y^p = m$, a uniform boundedness of $\#\mathrm{Jac}(C_m^p)(\mathbb{Q})_{\mathrm{tors}}$ for fixed odd prime p was used to obtain certain information about the behaviour of ranks in the infinite family $\mathrm{Jac}(C_m^p)(\mathbb{Q})$ (see [6]), and some information about ranks of p-twist of the Jacobians of the quotients of Fermat's curves (namely, $y^p = x^m(x + a)$, see [16]).

2. Main results. In this section we list our main theorems.

THEOREM 2.1. *We have*

$$J_{q,p,a}(\mathbb{Q})_{\mathrm{tors}} \simeq (\mathbb{Z}/2\mathbb{Z})^{e_2} \times (\mathbb{Z}/q\mathbb{Z})^{e_q} \times (\mathbb{Z}/p\mathbb{Z})^{e_p}$$

where $e_2, e_q, e_p \in \{0, 1, \ldots, (p-1)(q-1)/2\}$. *Moreover, if* a *is a* p*-th power then* $e_q > 0$, *and if* a *is a* q*-th power then* $e_p > 0$.

Under additional assumptions we can say more about e_2.

THEOREM 2.2. *Assume that* $2^n \equiv -1 \pmod{qp}$ *for some* n *or the order of* 2 *in* $(\mathbb{Z}/qp\mathbb{Z})^*$ *equals* $\frac{(q-1)(p-1)}{2}$. *Then* $e_2 = 0$ *for any odd* a.

If $q = 3$ we can say more about e_p.

THEOREM 2.3. *Assume that* $q = 3$. *Then* $e_p > 0$ *if and only if* a *is a third power.*

In the case $q = 3$ and $p = 5$ we have the following full characterization of torsion subgroups.

THEOREM 2.4. *For any nonzero* $a \in \mathbb{Z}$ *we have*

$$J_{3,5,a}(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \{0\} & \text{if } a \neq \text{third power and } a \neq \text{fifth power}, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } a \neq \text{third power and } a = \text{fifth power}, \\ \mathbb{Z}/5\mathbb{Z} & \text{if } a = \text{third power and } a \neq \text{fifth power}, \\ \mathbb{Z}/15\mathbb{Z} & \text{if } a = \text{third power and } a = \text{fifth power}. \end{cases}$$

Below we state two new results which do not appear in [15] (we keep the notation from Theorem 2.1).

THEOREM 2.5. *We have* $e_2, e_q, e_p \in \{0, 1\}$.

THEOREM 2.6. *If* a *is odd then* $e_2 = 0$.

3. Sketch of the proofs of results from [15]. In this section we give main ingredients and main methods of the proofs of Theorems 2.1, 2.2, 2.3 and 2.4. At first, we list sufficient conditions for existence of points of order p and q in $J_{q,p,a}(\mathbb{Q})$ (the proofs are standard applications of the Riemann–Roch Theorem).

PROPOSITION 3.1. *If* a *is a* p*-th power then* $J_{q,p,a}(\mathbb{Q})$ *contains a subgroup of order* q. *More precisely, let* $a = b^p$. *Then the* $\mathbb{Q}$*-rational divisor* $(-b, 0) - \infty$ *has order* q *in* $J_{q,p,a}(\mathbb{Q})$.

PROPOSITION 3.2. *If* a *is a* q*-th power then* $J_{q,p,a}(\mathbb{Q})$ *contains a subgroup of order* p. *More precisely, let* $a = c^q$. *Then the* $\mathbb{Q}$*-rational divisor* $(0, c) - \infty$ *has order* p *in* $J_{q,p,a}(\mathbb{Q})$.

PROPOSITION 3.3. *If* a *is a* pq*-th power then* $J_{q,p,a}(\mathbb{Q})$ *contains a subgroup of order* pq. *More precisely, let* $a = d^{pq}$. *Then the* $\mathbb{Q}$*-rational divisor* $(-d^q, 0) + (0, d^p) - 2\infty$ *has order* pq *in* $J_{q,p,a}(\mathbb{Q})$.

Next, we show that (at least for $q = 3$ and $p = 5$) these conditions are necessary. In order to compute $J_{q,p,a}(\mathbb{Q})_{\mathrm{tors}}$ it is helpful to consider $J_{q,p,a}(\mathbb{F}_l)$ for primes $l \nmid pqa$. This is because the reduction modulo l homomorphism induces an embedding $J_{q,p,a}(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow J_{q,p,a}(\mathbb{F}_l)$ (cf. [11, Theorem C.1.4, p. 263]) and therefore

$$\#J_{q,p,a}(\mathbb{Q})_{\mathrm{tors}} \,|\, \#J_{q,p,a}(\mathbb{F}_l) \tag{1}$$

We have the general formula for the number of points in $C_{q,p,a}(\mathbb{F}_{l^k})$ in terms of Jacobi (or Gauss) sums, and consequently we get the general formulas for the zeta function of $C_{q,p,a}$ over $\mathbb{F}_l$, and for the order of $J_{q,p,a}(\mathbb{F}_l)$. In some cases these formulas are explicit.

PROPOSITION 3.4. *If prime $l \equiv -1 \pmod{pq}$ and $l \nmid a$ then the zeta function of $C_{q,p,a}$ over $\mathbb{F}_l$ has the form*

$$Z(C_{q,p,a}/\mathbb{F}_l, X) = \frac{(1+lX^2)^g}{(1-X)(1-lX)}$$

where $g = (p-1)(q-1)/2$ is the genus of $C_{q,p,a}$. In particular, $\#J_{q,p,a}(\mathbb{F}_l) = (1+l)^g$.

Sketch of proof. By assumption, we have to consider characters and Gauss sums over $\mathbb{F}_{l^2}$. The reference to the properties of characters and pure Gauss sums (e.g. [2]) completes the proof. ∎

PROPOSITION 3.5. *For any nonzero integer a the order of $J_{q,p,a}(\mathbb{Q})_{\mathrm{tors}}$ divides $(2pq)^g$.*

Proof. Fix q, p and a. Let r be any prime such that $r \nmid 2qp$. Then, there exists a prime l such that $l \nmid a$, $l \equiv p-1 \pmod{p^2}$, $l \equiv q-1 \pmod{q^2}$, $l \equiv 1 \pmod 4$ and $l \equiv 1 \pmod r$. Therefore by Proposition 3.4, $\#J_{q,p,a}(\mathbb{F}_l) = (1+l)^g \equiv 2^g \not\equiv 0 \pmod r$. Moreover $\mathrm{ord}_i(\#J_{q,p,a}(\mathbb{F}_l)) = g$ for $i = 2, p, q$ (because $\mathrm{ord}_i(1+l) = 1$). Using (1), we are done. ∎

Now Theorem 2.1 follows from Propositions 3.1, 3.2, 3.3 and 3.5.

To prove Theorem 2.2 (and Theorem 2.4) we need to consider more explicit formula for Jacobi sums which uses the Stickelberger relation in the cyclotomic field $\mathbb{Q}(\zeta_{qp})$ where $\zeta_n = \exp(\frac{2\pi i}{n})$. Then Theorem 2.2 easily follows from the formula (1) and the following

PROPOSITION 3.6. *Assume that $2^n \equiv -1 \pmod{qp}$ for some n or the order of 2 in $(\mathbb{Z}/qp\mathbb{Z})^*$ equals $\frac{(q-1)(p-1)}{2}$. Then $2 \nmid \#J_{q,p,1}(\mathbb{F}_2)$.*

From now we assume that $q = 3$. Theorem 2.3 is an improvement of Theorem 2.1 in this case. In order to prove it, we start with the following proposition (its proof is based on the congruence modulo p of the coefficients of the numerator of the zeta function $Z(C_{3,p,a}/\mathbb{F}_l, X)$).

PROPOSITION 3.7. *If prime $l \equiv 1 \pmod{3p}$ and a is not a cube modulo l, then $p \nmid \#J_{3,p,a}(\mathbb{F}_l)$.*

The proof of the next proposition is an example of an application of the Chebotarev Density Theorem (in the formulation of [24, pp. 35–36]).

PROPOSITION 3.8. *If a is not a cube in $\mathbb{Z}$ then $p \nmid \#J_{3,p,a}(\mathbb{Q})_{\mathrm{tors}}$.*

Proof. We will show that by the Chebotarev Density Theorem, there exist infinitely many primes l such that $l \equiv 1 \pmod{3p}$ and a is not a cube modulo l. Indeed, consider the polynomial

$$h(x) := (x^2+3)(x^3-a)(x^{p-1}+x^{p-2}+\ldots+1) \in \mathbb{Z}[x]$$

and its splitting field K (over $\mathbb{Q}$). Then $K = \mathbb{Q}(\zeta_3, \sqrt[3]{a}, \zeta_p)$ and $K/\mathbb{Q}$ is a Galois extension of degree $\le 6(p-1)$. There exists an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\sqrt{-3}) = \sqrt{-3}$, $\sigma(\sqrt[3]{a}) = \zeta_3 \sqrt[3]{a}$ and $\sigma(\zeta_p) = \zeta_p$. If we arrange the zeroes of h in the following order: $\sqrt{-3}, -\sqrt{-3}, \sqrt[3]{a}, \zeta_3\sqrt[3]{a}, \zeta_3^2\sqrt[3]{a}, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$ then σ, as an element of the symmetric

group on $p+4$ letters, is the product $(1)(2)(3,4,5)(6)(7)\dots(p+4)$ of disjoint cycles, i.e. has the cycle pattern $1,1,3,1,\dots,1$. By the Chebotarev Density Theorem, there exist infinitely many primes l such that h has the decomposition type $1,1,3,1,\dots,1$ over $\mathbb{F}_l$. So the polynomial x^3-a is irreducible over $\mathbb{F}_l$ but x^2+3 and $x^{p-1}+x^{p-2}+\ldots+1$ split completely over $\mathbb{F}_l$. Therefore such primes l satisfy desired properties. Hence by Proposition 3.7 and (1), we are done. ∎

Now Theorem 2.3 follows immediately from Proposition 3.8 and Theorem 2.1.

In the remainder of this section we assume that $q=3$ and $p=5$. To prove Theorem 2.4 (the full characterizations of $J_{3,5,a}(\mathbb{Q})_{\mathrm{tors}}$) it is enough to show that $\#J_{3,5,a}(\mathbb{Q})_{\mathrm{tors}} \mid 15$ and

PROPOSITION 3.9. *If a is not a 5-th power in $\mathbb{Z}$ then $3 \nmid \#J_{3,5,a}(\mathbb{Q})_{\mathrm{tors}}$.*

To this end we have to calculate (explicitly, in terms of quadratic partitions of prime l) the order of $J_{3,5,a}(\mathbb{F}_l)$ for $l \equiv 2,4,8,11 \pmod{15}$. For $l \equiv 4,11 \pmod{15}$ we use the result due to Friesen *et al.* [8] about the cyclotomic number of order 15. For $l \equiv 2,8 \pmod{15}$ our calculation is a new result (we use the Stickelberger relation and the arithmetic of $\mathbb{Q}(\zeta_{15})$). Then we apply a few times the Chebotarev Density Theorem. Once (in the proof of Proposition 3.11) we also apply the result due to Iwaniec [13].

Here are an sample formula for zeta function of $C_{3,5,a}$.

PROPOSITION 3.10. *Assume that $l \equiv 2,8 \pmod{15}$. Then $l = 3u^2+5v^2$ for some uniquely determined positive integers u, v, and*

$$Z(C_{3,5,a}/\mathbb{F}_l, X) = \frac{1+2l(3u^2-5v^2)X^4+l^4X^8}{(1-X)(1-lX)}.$$

In particular,

$$\#J_{3,5,a}(\mathbb{F}_l) = 1+2l(3u^2-5v^2)+l^4.$$

PROPOSITION 3.11. *For $a \in \mathbb{Z}\setminus\{0\}$ we have $9 \nmid \#J_{3,5,a}(\mathbb{Q})_{\mathrm{tors}}$ and $25 \nmid \#J_{3,5,a}(\mathbb{Q})_{\mathrm{tors}}$.*

4. Proofs of new results. In this section we give the proofs of Theorems 2.5 and 2.6. In both proofs we strongly use properties of CM abelian varieties.

Proof of Theorem 2.5. The proof is based on [1, Corollary 8.8] (see also [1, Example 8.9]. The map $(x,y) \mapsto (\zeta_p x, \zeta_q y)$ defines an automorphism of $C_{q,p,a}$, and it induces an endomorphism $\iota(\zeta_{qp}) \in End(J_{q,p,a})$. Therefore we obtain an isomorphism $\iota : K \to End(J_{q,p,a}) \otimes \mathbb{Q}$, where $K := \mathbb{Q}(\zeta_{qp})$ is the qp-th cyclotomic field. Since $[K:\mathbb{Q}] = (q-1)(p-1) = 2\dim(J_{q,p,a})$, the Jacobian $J_{q,p,a}$ is a CM abelian variety. Moreover, this abelian variety is absolutely simple (cf. [10]), and $End(J_{q,p,a}) \cong \mathbb{Z}[\zeta_{qp}]$ (the ring of integers of K). Note that K has exactly $2qp$ roots of unity, namely the only roots of unity in K are $\pm\zeta_{qp}^s$ with $0 \le s \le qp-1$ (see [2, Theorem 2.1.13]). Thus by [1, Corollary 8.8], we get $J_{q,p,a}(\mathbb{Q})_{\mathrm{tors}} \subset \mathbb{Z}/2qp\mathbb{Z}$, and the assertion follows. ∎

To prove Theorem 2.6 we need following two lemmas.

LEMMA 4.1. *If $\mathbb{Z}/2\mathbb{Z} \subset J_{q,p,a}(\mathbb{Q})$ then $(\mathbb{Z}/2\mathbb{Z})^{(q-1)(p-1)} \subset J_{q,p,a}(K)$, where $K = \mathbb{Q}(\zeta_{qp})$.*

Proof. Repeat *mutatis mutandis* the proof of Lemma 1.3 from [9]. ∎

LEMMA 4.2. *If a is odd, then $J_{q,p,a}$ is not ordinary over $\mathbb{F}_2$.*

Proof. First of all, note that since a is odd, $J_{q,p,a}$ has a good reduction at 2. It is well known (see [7]) that an abelian variety is ordinary over $\mathbb{F}_l$ if and only if all slopes in the Newton polygon of the characteristic polynomial for its Frobenius endomorphism are either 0 or 1. We will show (using Blake's generalisations of Deuring's reduction criterion [3]) that at least one slope of $J_{q,p,a}$ over $\mathbb{F}_2$ is neither 0 nor 1.

To this end we introduce some notation. Let G denote the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, let $\mathfrak{l}$ be any prime in K lying above 2, and let $D = D_{\mathfrak{l}}$ be its decomposition group. Finally, let Φ denote the CM-type of $J_{q,p,a}$. Observe that G is isomorphic to $(\mathbb{Z}/qp\mathbb{Z})^*$ via the map $\sigma_k \mapsto k$, where $\sigma_k(\zeta_{qp}) = \zeta_{qp}^k$. Under this identification, D is the subgroup of $(\mathbb{Z}/qp\mathbb{Z})^*$ generated by 2 (e.g. [12, Corollary, p. 197]). In turn Φ may be identified with $S := \{k \in (\mathbb{Z}/qp\mathbb{Z})^* : \left[\frac{k}{q} + \frac{k}{p}\right] - \left[\frac{k}{q}\right] - \left[\frac{k}{p}\right] = 1\}$. This is because $k \in S \Leftrightarrow -k \notin S$, hence S is a set of coset representatives for the subgroup $\{1, -1\}$. Now, by [3, Theorem 1.2], the Newton polygon of $J_{q,p,a}$ over $\mathbb{F}_2$ has slopes $\lambda_\gamma = \#(D\gamma \cap \Phi)/\#(D\gamma)$, where γ ranges through a set of representatives for G/D. Taking $\gamma = 1$, we get immediately $1 \in D$ but $1 \notin \Phi$, hence $\lambda_1 < 1$. On the other hand, observe that $2^{f-1} \in D \cap \Phi$ where $f = \#D$. Indeed, $2^{f-1} \equiv 2^{-1} \equiv \frac{p+1}{2} \pmod p$ and $2^{f-1} \equiv 2^{-1} \equiv \frac{q+1}{2} \pmod q$. Therefore $\left[\frac{2^{f-1}}{q} + \frac{2^{f-1}}{p}\right] - \left[\frac{2^{f-1}}{q}\right] - \left[\frac{2^{f-1}}{p}\right] = \left[\frac{q+1}{2q} + \frac{p+1}{2p}\right] = 1$. Consequently, $\lambda_1 > 0$, which completes the proof. ∎

Proof of Theorem 2.6. Suppose, on the contrary, that $J_{q,p,a}(\mathbb{Q})$ has a point of order 2. Let $\mathfrak{l}$ be a prime of K lying above 2. By Lemma 4.1, we get $(\mathbb{Z}/2\mathbb{Z})^{(q-1)(p-1)} \subset J_{q,p,a}(K_{\mathfrak{l}})$, where $K_{\mathfrak{l}}$ is the completion of K at the place $\mathfrak{l}$. But $K_{\mathfrak{l}}$ is an unramified extension of $\mathbb{Q}_2$, hence by [9, Lemma 1.4], $J_{q,p,a}$ must be ordinary over $\mathbb{F}_2$, contrary to Lemma 4.2, and we are done. ∎

5. Problems

REMARK 5.1. Among the pairs of primes (q, p) where $2 < q < p < 1000$ circa 37% satisfy assumptions of Theorem 2.2.

Theorems 2.5, 2.6, 2.3, 2.4, other partial results (see [15]), and numerical computations in Magma [4] allow us to believe (at least for $q = 3$, $p = 7$) the following

CONJECTURE. For any primes $p > q > 2$ and any nonzero $a \in \mathbb{Z}$ we have

$$J_{q,p,a}(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \{0\} & \text{if } a \neq q\text{-th power and } a \neq p\text{-th power,} \\ \mathbb{Z}/q\mathbb{Z} & \text{if } a \neq q\text{-th power and } a = p\text{-th power,} \\ \mathbb{Z}/p\mathbb{Z} & \text{if } a = q\text{-th power and } a \neq p\text{-th power,} \\ \mathbb{Z}/qp\mathbb{Z} & \text{if } a = q\text{-th power and } a = p\text{-th power.} \end{cases}$$

References

[1] N. Aoki, *Torsion points on CM abelian varieties*, Comment. Math. Univ. St. Pauli 55 (2006), 207–229.

[2] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Canad. Math. Soc. Ser. Monogr. Adv. Texts 21, A Wiley-Interscience Publ., John Wiley & Sons, New York 1998.

[3] C. Blake, *A Deuring criterion for abelian varieties*, Bull. Lond. Math. Soc. 46 (2014), 1256–1263.

[4] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[5] A. Cadoret, A. Tamagawa, *Note on torsion conjecture*, in: Geometric and Differential Galois Theories, Sémin. Congr. 27, Soc. Math. France, Paris 2013, 57–68.

[6] A. Dąbrowski, T. Jędrzejak, *Ranks in families of Jacobian varieties of twisted Fermat curves*, Canad. Math. Bull. 53 (2010), 58–63.

[7] P. Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. 8 (1969), 238–243.

[8] C. Friesen, J. B. Muskat, B. K. Spearman, K. S. Williams, *Cyclotomy of order* 15 *over* $GF(p^2)$, $p \equiv 4, 11 \pmod{15}$, Internat. J. Math. Math. Sci. 9 (1986), 665–704.

[9] B. H. Gross, D. E. Rohrlich, *Some results on the Mordell–Weil group of the Jacobian of the Fermat curve*, Invent. Math. 44 (1978), 201–224.

[10] F. Hazama, *Hodge cycles on the Jacobian variety of the Catalan curve*, Compositio Math. 107 (1997), 339–353.

[11] M. Hindry, J. H. Silverman, *Diophantine Geometry. An Introduction*, Grad. Texts in Math. 201, Springer, New York 2000.

[12] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Grad. Texts in Math. 84, Springer, New York 2000.

[13] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Acta Arith. 24 (1973/74), 435–459.

[14] T. Jędrzejak, *Characterization of the torsion of the Jacobians of two families of hyperelliptic curves*, Acta Arith. 161 (2013), 201–218.

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

[16] T. Jędrzejak, M. Ulas, *Variations on twists of tuples of hyperelliptic curves and related results*, J. Number Theory 137 (2014), 222–240.

[17] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. 109 (1992), 221–229.

[18] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 109 (1988), 125–149.

[19] A. Knapp, *Elliptic Curves*, Math. Notes 40, Princeton Univ. Press, Princeton, NJ 1992.

[20] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1978), 33–186.

[21] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), 437–449.

[22] A. Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Math. 68 (1988), 241–249.

[23] A. Silverberg, *Points of finite order on abelian varieties*, in: p-adic Methods in Number Theory and Algebraic Geometry, Contemp. Math. 133, Amer. Math. Soc., Providence, RI 1992, 175–193.

[24] P. Stevenhagen, H. W. Lenstra, *Chebotarev and his Density Theorem*, Math. Intelligencer 18 (1996), no. 2, 26–37.