JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Jian WANG

On the cyclic torsion of elliptic curves over cubic number fields (II)

Tome 31, n° 3 (2019), p. 663-670.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2019__31_3_663_0>

© Société Arithmétique de Bordeaux, 2019, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.centre-mersenne.org/), implique l'accord avec les conditions générales d'utilisation (http://jtnb.centre-mersenne.org/legal/). Toute reproduction en tout ou partie de cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.centre-mersenne.org/

Journal de Théorie des Nombres de Bordeaux **31** (2019), 663–670

On the cyclic torsion of elliptic curves over cubic number fields (II)

par Jian WANG

Résumé. Le résultat de Merel sur la forme forte de la conjecture de borne uniforme a mis en valeur la classification des parties de torsion des groupes de Mordell–Weil des courbes elliptiques définies sur les corps de nombres de degré fixé d. Dans cet article, nous étudions les sous-groupes de torsion cycliques des courbes elliptiques sur les corps de nombres cubiques. Pour $N = 49, 40, 25$ ou 22, nous montrons que $\mathbb{Z}/N\mathbb{Z}$ n'est pas un sous-groupe de $E(K)_{\mathrm{tor}}$ pour toute courbe elliptique E sur un corps de nombres cubique K.

Abstract. Merel's result on the strong uniform boundedness conjecture made it meaningful to classify the torsion part of the Mordell–Weil groups of all elliptic curves defined over number fields of fixed degree d. In this paper, we discuss the cyclic torsion subgroup of elliptic curves over cubic number fields. For $N = 49, 40, 25$ or 22, we show that $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{\mathrm{tor}}$ for any elliptic curve E over a cubic number field K.

1. Introduction

In 1996, Merel [16] finally proved the strong uniform boundedness conjecture for elliptic curves over number fields.

Theorem 1.1 (Merel)**.** *For every positive integer d, there exists an integer B_d such that for every number field K of degree d and every elliptic curve E over K, we always have*

$$|E(K)_{\mathrm{tor}}| \leq B_d$$

Merel's result made it meaningful to classify the torsion part of the Mordell–Weil groups of all elliptic curves defined over number fields of fixed degree d. The case $d = 1$ was solved by Mazur [15] and Kubert [13]. The case $d = 2$ was solved by Kamienny [9], Kenku and Momose [12].

In 2016, Derickx and the group of Etropolski, Morrow and Zureick-Brown each announced a solution of the case $d = 3$ [4], but there is still no publicly available preprint until April 2019. In view of the work of Parent [20, 21], Jeon–Kim–Schweizer [8] and Najman [17], we conjectured (see [27]) that

Manuscrit reçu le 16 décembre 2018, révisé le 13 avril 2019, accepté le 11 mai 2019.
2010 *Mathematics Subject Classification.* 11G05, 11G18.
Mots-clefs. torsion subgroup, elliptic curves, modular curves.

$\mathbb{Z}/N\mathbb{Z}$ is not a cyclic torsion subgroup of the Mordell–Weil group of any elliptic curve over a cubic number field for 24 values of N:

$$22, 24, 25, 26, 27, 28, 30, 32, 33, 35, 36, 39, 40,$$
$$42, 45, 49, 55, 63, 65, 77, 91, 121, 143, 169.$$

In [27], six ($N = 55, 65, 77, 91, 143, 169$) of the above values were ruled out using refinements of a criterion originally due to Kamienny. In this paper, we rule out four further values. Namely we obtain the following:

Theorem 1.2. *If $N = 49, 40, 25$ or 22, then $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{\mathrm{tor}}$ for any elliptic curve E over a cubic number field K.*

Acknowledgments. We thank Sheldon Kamienny for valuable ideas and insightful comments. We thank the anonymous referee for helpful comments and suggestions.

2. Preliminaries

In this section, we omit the background materials which were covered in Section 2 of [27]. Readers who are interested may switch there.

Let N be a positive integer. Let $X_1(N)$ (resp. $X_0(N)$) be the modular curve defined over $\mathbb{Q}$ associated to the congruence subgroup $\Gamma_1(N)$ (resp. $\Gamma_0(N)$). We denote by $Y_1(N) = X_1(N)\setminus\{\text{cusps}\}$, $Y_0(N) = X_0(N)\setminus\{\text{cusps}\}$ the corresponding affine curves. Denote by $J_1(N)$ (resp. $J_0(N)$) the Jacobian of $X_1(N)$ (resp. $X_0(N)$).

For a modular curve X, let $X^{(d)}$ be the d-th symmetric power of X. Suppose K is a number field of degree d over $\mathbb{Q}$ and $x \in X(K)$. Let $x_1, \ldots, x_d$ be the images of x under the distinct embeddings $\tau_i : K \hookrightarrow \mathbb{C}, 1 \le i \le d$. Define

$$\Phi : X^{(d)} \longrightarrow J_X$$

by $\Phi(P_1 + \cdots + P_d) = [P_1 + \cdots + P_d - d\infty]$ where J_X is the Jacobian of X, and $[\,\cdot\,]$ denotes the divisor class. The following lemma of Frey [5] plays an important role in Lemma 3.5.

Lemma 2.1 (Frey)**.** *Let K be a number field. If $\Phi_{|X^{(d)}(K)}$ is not injective, then there is a K-rational covering $\pi : X \longrightarrow \mathbb{P}^1_K$ of degree $\le d$.*

For a modular curve X over $\mathbb{C}$, X is called d-gonal if there exists a finite $\mathbb{C}$-morphism $\pi : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ of degree d. The smallest possible d is called the $\mathbb{C}$-gonality of X, denoted by $\mathrm{Gon}_{\mathbb{C}}(X)$. Since the cusp at infinity is a rational point, $X_1(N)$ is 1-gonal if and only if N is among the eleven values $N = 1-10, 12$ with genus 0. The complete lists of 2-gonal and 3-gonal ones were determined by Ishii–Momose [7] and Jeon–Kim–Schweizer [8].

Proposition 2.2 (Ishii–Momose)**.** *The modular curve $X_1(N)$ is 2-gonal if and only if N is one of the following:*

$$\begin{aligned} &N = 1-10, 12 \quad (g=0);\\ &N = 11, 14, 15 \quad (g=1);\\ &N = 13, 16, 18 \quad (g=2). \end{aligned}$$

Proposition 2.3 (Jeon–Kim–Schweizer)**.** *The modular curve $X_1(N)$ is 3-gonal if and only if N is one of the following:*

$$\begin{aligned} &N = 1-10, 12 \quad (g=0);\\ &N = 11, 14, 15 \quad (g=1);\\ &N = 13, 16, 18 \quad (g=2);\\ &N = 20 \qquad\quad (g=3). \end{aligned}$$

Any noncuspidal point of $X_1(N)$ is represented by $(E, \pm P)$, where E is an elliptic curve and $P \in E$ is a point of order N. Any noncuspidal point of $X_0(N)$ is represented by (E, C), where E is an elliptic curve and $C \subset E$ is a cyclic subgroup of order N. The map $\pi : X_1(N) \longrightarrow X_0(N)$ sends $(E, \pm P)$ to $(E, \langle P \rangle)$, where $\langle P \rangle$ is the cyclic subgroup generated by P.

Let p be a prime such that $p \nmid N$. Igusa's theorem [6] says that the modular curves $X_1(N)$ and $X_0(N)$ have good reduction at prime p. The following theorem of Serre and Milne says that reducing the modular curve is compatible with reducing the modular interpretation.

Theorem 2.4 (Serre–Milne [19, Theorem 1])**.** *Any point of $Y_1(N)$ or $Y_0(N)$, rational over a field K (of characteristic not dividing N), is represented by a K-rational pair (i.e. E is defined over K, and P is rational over K, or C is a group rational over K), and conversely.*

Let K be a number field with ring of integers $\mathcal{O}_K$, $\wp \subset \mathcal{O}_K$ a prime ideal lying above p, $k = \mathbb{F}_q = \mathcal{O}_K/\wp$ its residue field. Let E be an elliptic curve over K and $P \in E(K)$ a point of order N. Let $\widetilde{E}$ be the fibre over k of the Néron model of E, and let $\widetilde{P} \in \widetilde{E}(k)$ be the reduction of P. The following theorem (see, for instance, [1, §7.3 Proposition 3]) shows that $\widetilde{P}$ has order N when $p \nmid N$.

Theorem 2.5. *Let m be a positive integer relatively prime to $\mathrm{char}(k)$. Then the reduction map*

$$E(K)[m] \longrightarrow \widetilde{E}(k)$$

is injective.

Let $k = \mathbb{F}_q$ be the finite field with $q = p^n$ elements. Let E/k be an elliptic curve over k. Let $|E(k)|$ be the number of points of E over k. Then Hasse's theorem states that

$$||E(k)| - q - 1| \leq 2\sqrt{q}$$

i.e.

$$(1 - \sqrt{p^n})^2 \leq |E(k)| \leq (1 + \sqrt{p^n})^2$$

Let $t = q+1-|E(k)|$, E is called ordinary if $(t, q) = 1$, otherwise it is called supersingular. In the range proposed by Hasse's theorem, all the ordinary t appear, while the supersingular t only appears in restricted case. This was determined by Waterhouse [28, Theorem 4.1]:

Proposition 2.6 (Waterhouse)**.** *The isogeny classes of elliptic curves over k are in one-to-one correspondence with the rational integers t having $|t| \leq 2\sqrt{q}$ and satisfying one of the following conditions:*

(1) $(t, p) = 1$*;*
(2) *If n is even: $t = \pm 2\sqrt{q}$;*
(3) *If n is even and $p \not\equiv 1 \mod 3$: $t = \pm\sqrt{q}$;*
(4) *If n is odd and $p = 2$ or 3: $t = \pm p^{\frac{n+1}{2}}$;*
(5) *If either (i) n is odd or (ii) n is even and $p \not\equiv 1 \mod 4$: $t = 0$.*

3. Method

The following Theorem states that the Jacobian $J_1(N)$ decomposes to a direct sum of modular abelian varieties.

Theorem 3.1. [2, Theorem 6.6.6] *The Jacobian $J_1(N)$ is isogenous to a direct sum of abelian varieties (over $\mathbb{Q}$) associated to equavalence classes of newforms*

$$J_1(N) \longrightarrow \bigoplus_f A_f^{m_f}$$

with $f(\tau) = \sum_{n=1}^{\infty} a_n(f) e^{2\pi i n\tau}$ newforms of level dividing N.

The L-series $L(A_f, s)$ of A_f coincides, up to a finite number of Euler factors, with the product

$$\prod_\sigma L(f^\sigma, s) = \prod_\sigma \sum_{n=1}^{\infty} a_n^\sigma n^{-s}$$

where σ runs through embeddings $\sigma : K_f \hookrightarrow \mathbb{C}$ with $K_f = \mathbb{Q}(\{a_n\})$ the number field of f (See [23, §7.5]). The following proposition is a special case of Corollary 14.3 in Kato [10]:

Proposition 3.2. *Let A be an abelian variety over $\mathbb{Q}$ such that there is a surjective homomorphism $J_1(N) \longrightarrow A$ for some $N \geq 1$. If $L(A, 1) \neq 0$, then $A(\mathbb{Q})$ is finite.*

The decomposition of $J_1(N)$ and the non-vanishing of the L-series at $s = 1$ of modular abelian varieties can be calculated in Magma [26]. If $L(A_f, 1) \neq 0$ for all A_f, then we know $A_f(\mathbb{Q})$ is finite for all A_f, therefore $J_1(N)_{/\mathbb{Q}}$ is finite. For the $N \leq 65$ in the list in [27], Table 3.1 is the result of calculations in Magma. The second column t is the number of non-isogenous modular abelian varieties in the decompositon $J_1(N) = \bigoplus_{i=1}^{t} A_i^{m_i}$. The third column list the dimension d_i and multiplicity m_i of each A_i (we omit m_i if $m_i = 1$). The fourth column verifies non-vanishing of L-series at 1 (a mark T means $L(A_i, 1) \neq 0$ is verified, otherwise we place a mark $\boldsymbol{F}$).

The results in Table 3.1 verifies that $J_1(N)(\mathbb{Q})$ is finite for the first 17 values ($N \leq 55$) in the list of Section 1. For $N = 65, 63$, we don't know whether $J_1(N)(\mathbb{Q})$ is finite or not since we fail to verify the non-vanishing at 1 of the L-series of one of its quotients.

TABLE 3.1. Decompostion of $J_1(N)$

N	t	$d_i(m_i)$	$L(A_i, 1) \neq 0$
49	5	$1, 48, 6, 12, 2$	T, T, T, T, T
25	2	$8, 4$	T, T
27	2	$1, 12$	T, T
32	4	$1, 4, 8, 2(2)$	T, T, T, T
65	19	$1, 2, 2, 6, 20, 20, 8, 2(2), 8,$	$\boldsymbol{F}, T, T, T, T, T, T, T, T,$
		$2, 8, 2, 8, 4, 4, 12, 6, 2, 2$	$T, T, T, T, T, T, T, T, T, T$
39	10	$1, 2, 4, 8, 2, 2(2), 4, 2, 4, 2$	$T, T, T, T, T, T, T, T, T, T$
26	5	$1, 1, 2(2), 2, 2$	T, T, T, T, T
55	10	$1, 2, 1(2), 4, 32, 8, 8, 16, 4, 4$	$T, T, T, T, T, T, T, T, T, T$
33	6	$1, 1(2), 8, 4, 4, 2$	T, T, T, T, T, T
22	2	$1(2), 4$	T, T
35	8	$1, 2, 2, 4, 4, 4, 4, 4$	T, T, T, T, T, T, T, T
63	20	$1, 2, 1(2), 6, 6, 2, 10, 4, 2(2), 2,$	$T, T, T, T, T, T, T, T, T, \boldsymbol{F}$
		$10, 2, 2, 2(2), 2, 10, 2, 10, 12, 4$	$T, T, T, T, T, T, T, T, T, T$
28	4	$1(2), 4, 2, 2$	T, T, T, T
45	8	$1, 1(2), 2, 6, 16, 4, 2, 8$	T, T, T, T, T, T, T, T
30	4	$1, 1(2), 4, 2$	T, T, T, T
40	7	$1, 1(2), 4, 2(2), 8, 2, 4$	T, T, T, T, T, T, T
36	5	$1, 8, 2, 2(2), 2$	T, T, T, T, T
24	3	$1, 2, 2$	T, T, T

The famous specialization lemma is an immediate consequence of the classification of Oort–Tate [25] on finite flat group schemes of rank p (this result was generalized to finite flat group schemes of type $(p, \ldots, p)$ by Raynaud [22]). If the group scheme is contained in an abelian variety, as

we stated in the following, the specialization lemma follows from elementary properties of formal Lie groups (see, for example, the Appendix of Katz [11]).

Lemma 3.3 (Specialization Lemma)**.** *Let K be a number field. Let $\wp \subset \mathcal{O}_K$ be a prime above p. Let A/K be an abelian variety. Suppose the ramification index $e_\wp(K/\mathbb{Q}) < p-1$. Then the reduction map*

$$\Psi : A(K)_{\mathrm{tor}} \longrightarrow A(\overline{\mathbb{F}}_p)$$

is injective.

In the proof of Lemma 3.5, we also use a theorem of Manin [14] and Drinfeld [3].

Theorem 3.4 (Manin–Drinfeld)**.** *Let $\Gamma \subset SL_2(\mathbb{Z})/(\pm 1)$ be a congruence subgroup. $x, y \in \mathbb{P}^1(\mathbb{Q})$ and $\overline{x}, \overline{y}$ the images of x and y respectively, on $\overline{\mathbb{H}}/\Gamma$. Then the class of divisors $(\overline{x}) - (\overline{y})$ on curve $\overline{\mathbb{H}}/\Gamma$ has finite order.*

Lemma 3.5. *Suppose$N > 4$ such that $\mathrm{Gon}_{\mathbb{C}}(X_1(N)) > d$, $J_1(N)(\mathbb{Q})$ is finite, $p > 2$ is a prime not dividing N. Let K be a number field of degree d over $\mathbb{Q}$ and $\wp$ a prime of K over p. Let $E_{/K}$ be an elliptic curve with a K-rational point P of order N, i.e. $x = (E, \pm P) \in Y_1(N)(K)$. Then E has good reduction at $\wp$.*

Proof. Suppose E has additive reduction at $\wp$, then $\widetilde{E}(k)^0 \cong \mathbb{G}_{a/k}$ with $|\mathbb{G}_{a/k}| = p^i, i \leq d$ and $\widetilde{E}(k)/\widetilde{E}(k)^0 \cong G$ with $|G| \leq 4$ (this comes from the Kodaira–Néron classification of special fibers on Néron models of elliptic curves. see for example [24, §IV.8]). Since $\widetilde{P}$ is a k-rational point of order N in $\widetilde{E}$, then N divides $|\widetilde{E}(k)| = |\mathbb{G}_{a/k}||G|$, which is impossible under our assumption.

Suppose E has multiplicative reduction at $\wp$, i.e. x specializes to a cusp of $\widetilde{X}_1(N)$. Recall the notation of τ_i and x_i, $1 \leq i \leq d$, in Section 2. Then $\tau_i(K)$ is also a cubic field with prime ideal $\tau_i(\wp)$ over p and residue field $k_i = k$. And $\tau_i(E)$ also has multiplicative reduction at $\tau_i(\wp)$. This means all the images $x_1, \ldots, x_d$ of x specialize to cusps of $\widetilde{X}_1(N)$. Let $c_1, \ldots, c_d$ be the cusps such that

$$x_i \otimes \overline{\mathbb{F}}_p = c_i \otimes \overline{\mathbb{F}}_p, \quad 1 \leq i \leq d$$

We know all the cusps of $X_1(N)$ are defined over $\mathbb{Q}(\zeta_N)$ [18]. Let $\wp'$ be a prime in $\mathbb{Q}(\zeta_N)$ over p. We also know p ramifies in $\mathbb{Q}(\zeta_N)$ if and only if $p|N$. So $e_{\wp'}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = 1$ under our assumption $p \nmid N$. Therefore by Lemma 3.3, the specialization map

$$\Psi : J_1(N)(\mathbb{Q}(\zeta_N))_{\mathrm{tor}} \longrightarrow J_1(N)(\overline{\mathbb{F}}_p)$$

is injective.

Since $\mathrm{Gon}_{\mathbb{C}}(X_1(N)) > d$, then by Lemma 2.1, the map

$$\Phi : X_1(N)^{(d)}(\mathbb{Q}(\zeta_N)) \longrightarrow J_1(N)(\mathbb{Q}(\zeta_N))$$

is injective.

We know $x_1 + \cdots + x_d$ is $\mathbb{Q}$-rational and $J_1(N)(\mathbb{Q})$ is finite, so $[x_1 + \cdots + x_d - d\infty]$ is in $J_1(N)(\mathbb{Q}(\zeta_N))_{\mathrm{tor}}$. By Theorem 3.4, the difference of two cusps of $X_1(N)$ has finite order in $J_1(N)$. So $[c_1 + \cdots + c_d - d\infty]$ is also in $J_1(N)(\mathbb{Q}(\zeta_N))_{\mathrm{tor}}$. Therefore $\Psi \circ \Phi(x_1 + \cdots + x_d) = \Psi \circ \Phi(c_1 + \cdots + c_d)$ implies $x_1 + \cdots + x_d = c_1 + \cdots + c_d$ since $\Psi \circ \Phi$ is injective. This is a contradiction because we assume x is a noncuspidal point.

Therefore E has good reduction at $\wp$. □

4. Proof of Theorem 1.2

If $N = 49, 40, 25$ or 22, as is seen in Table 3.1, $J_1(N)(\mathbb{Q})$ is finite. By Proposition 2.2 and 2.3, we know $\mathrm{Gon}_{\mathbb{C}}(X_1(N)) > 3$. Let K be a cubic field and $\wp$ a prime of K over 3. Suppose $x = (E, \pm P) \in Y_1(N)(K)$. Therefore by Lemma 3.5, E has good reduction at $\wp$. By Theorem 2.5, the reduction $\widetilde{P}$ of P is a k-rational point of order N in the elliptic curve $\widetilde{E}$ over $k = \mathcal{O}_K/\wp$.

In the case $N = 49$ or 40, $\widetilde{E}(k)$ cannot have a point of order N since $N > (1 + \sqrt{3^3})^2 \approx 38.4$. Now consider the case $N = 25$ or 22. If $k = \mathbb{F}_3$ or $\mathbb{F}_{3^2}$, then $\widetilde{E}(k)$ cannot have a point of order N since $N > (1 + \sqrt{3^2})^2$. If $k = \mathbb{F}_{3^3}$, suppose $\widetilde{E}(k)$ has a point of order N, then $\widetilde{E}(k) \cong \mathbb{Z}/N\mathbb{Z}$ since $Nm > (1 + \sqrt{3^3})^2$ for any $m > 1$. But by Theorem 2.6, $|\widetilde{E}(k)| \neq N$ ($t = 3$ for $N = 25$, $t = 6$ for $N = 22$). Thus, in any of the four cases, we have a contradiction. So $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{\mathrm{tor}}$.

References

[1] S. Bosch, W. Lütkebohmert & M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge., vol. 21, Springer, 1990.

[2] F. Diamond & J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer, 2005.

[3] V. G. Drinfeld, "Two theorems on modular curves", *Funkts. Anal. Prilozh.* **7** (1973), no. 2, p. 83-84.

[4] A. Etropolski, J. Morrow & D. Zureick-Brown, "Sporadic torsion", 2016, `http://www.mathcs.emory.edu/~dzb/slides/DZB-SERMON-cubic-torsion.pdf`.

[5] G. Frey, "Curves with infinitely many points of fixed degree", *Isr. J. Math.* **85** (1994), no. 1, p. 1-3.

[6] J.-I. Igusa, "Kroneckerian model of fields of elliptic modular functions", *Am. J. Math.* **81** (1959), p. 561-577.

[7] N. Ishii & F. Momose, "Hyperelliptic modular curves", *Tsukuba J. Math.* **15** (1991), no. 2, p. 413-423.

[8] D. Jeon, C. H. Kim & A. Schweizer, "On the torsion of elliptic curves over cubic number fields", *Acta Arith.* **113** (2004), no. 3, p. 291-301.

[9] S. Kamienny, "Torsion points on elliptic curves and q-coefficients of modular forms", *Invent. Math.* **109** (1992), no. 2, p. 221-229.

[10] K. KATO, "p-adic Hodge theory and values of zeta functions of modular forms", in *Cohomologies p-adiques et applications arithmétiques*, Astérisque, vol. 295, Société Mathématique de France, 2004, p. 117-290.
[11] N. M. KATZ, "Galois properties of torsion points on abelian varieties", *Invent. Math.* **62** (1981), no. 3, p. 481-502.
[12] M. A. KENKU & F. MOMOSE, "Torsion points on elliptic curves defined over quadratic fields", *Nagoya Math. J.* **109** (1988), p. 125-149.
[13] D. S. KUBERT, "Universal bounds on the torsion of elliptic curves", *Proc. Lond. Math. Soc.* **33** (1976), no. 2, p. 193-237.
[14] Y. I. MANIN, "Parabolic points and zeta functions of modular curves", *Izv. Akad. Nauk SSSR, Ser. Mat.* **36** (1972), p. 19-66.
[15] B. MAZUR, "Modular curves and the Eisenstein ideal", *Publ. Math., Inst. Hautes Étud. Sci.* **47** (1977), p. 33-186.
[16] L. MEREL, "Bornes pour la torsion des courbes elliptiques sur les corps de nombres", *Invent. Math.* **124** (1996), no. 1-3, p. 437-449.
[17] F. NAJMAN, "Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$", *Math. Res. Lett.* **23** (2016), no. 1, p. 245-272.
[18] A. P. OGG, "Rational points on certain elliptic modular curves", in *Analytic Number Theory*, Proceedings of Symposia in Pure Mathematics, vol. 1972, American Mathematical Society, 1972, p. 221-231.
[19] ———, "Diophantine equations and modular forms", *Bull. Am. Math. Soc.* **81** (1975), p. 14-27.
[20] P. PARENT, "Torsion des courbes elliptiques sur les corps cubiques", *Ann. Inst. Fourier* **50** (2000), no. 3, p. 723-749.
[21] ———, "No 17-torsion on elliptic curves over cubic number fields", *J. Théor. Nombres Bordeaux* **15** (2003), no. 3, p. 831-838.
[22] M. RAYNAUD, "Schémas en groupes de type $(p, \ldots, p)$", *Bull. Soc. Math. Fr.* **102** (1974), p. 241-280.
[23] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 1, Mathematical Society of Japan, 1971.
[24] J. H. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994.
[25] J. TATE & F. OORT, "Group schemes of prime order", *Ann. Sci. Éc. Norm. Supér.* **3** (1970), p. 1-21.
[26] THE MAGMA DEVELOPMENT TEAM, "Magma", `http://magma.maths.usyd.edu.au/magma/`.
[27] J. WANG, "On the cyclic torsion of elliptic curves over cubic number fields", *J. Number Theory* **183** (2018), p. 291-308.
[28] W. C. WATERHOUSE, "Abelian varieties over finite fields", *Ann. Sci. Éc. Norm. Supér.* **2** (1969), p. 521-560.

Jian WANG
College of Mathematics
Jilin Normal University
Siping, Jilin 136000, China
E-mail: `blandye@gmail.com`