A remark on torsion points of elliptic curves on small extensions of $\mathbf{Q}$

Trâǹ Quôć Dân[a*] and Nguyêñ Quôć Thăńg[b †]

Abstract

In this note we discuss some properties of torsion points on elliptic curves defined over small extensions of $\mathbf{Q}$. As an application, we give a new proof of a theorem of Olson.
AMS Mathematics Subject Classification (2000): Primary 11G05, Secondary 11G07

1. Introduction. Let E be an elliptic curve defined over $\mathbf{Q}$, and let $E(\mathbf{Q})_{tors}$ be the subgroup of $\mathbf{Q}$-torsion points of E. There are many works devoted to the study of $E(\mathbf{Q})_{tors}$. To understand this group, sometimes one needs to extend the base field, and then study the torsion points defined over field extensions. For example, there are several works related to the study of torsion points in the quadratic, cubic or quartic extensions of $\mathbf{Q}$. We just refer the readers to [Fu], [Hu], [JKS], [La], [LL], [P], [ScZ], [Si], [Zi] and reference there for some more results. In this note we are interested in the following question : What can we say about the nature of torsion points over small extensions k of $\mathbf{Q}$?

2. Preliminaries. Let k be a global field, V the set of all non-equivalent

[*]a: Department of Mathematics, Hanoi National University, Hanoi - Vietnam. E-mail: quocdan120782@yahoo.com@math.ac.vn

[†]b: Max Plank Institut für Mathematik, Vivatsgasse str.7, 53111-Bonn, Germany, and Institute of Mathematics, 18 Hoang Quoc Viet, CauGiay, 10307, Hanoi - Vietnam.. Corresponding author. Supported in part by F. R. P. V., I.C.T.P. and M.P.I.M. E-mail : nqthang@math.ac.vn

nontrivial valuations of k, ∞ the set of all archimedean valuations of k, $(\mathcal{O}_v, \pi_v)$ be the valuation ring in k, corresponding to $v \in V$. We denote

$$\mathcal{O}_k = \cap_{v \notin \infty} \mathcal{O}_v$$

the ring of integers of k. Let E be an elliptic curve defined over k with defining affine equation

$$y^2 = x^3 + Ax + B, A, B \in \mathcal{O}_k. \tag{1}$$

We also write the homogeneous equation for E as

$$y^2 z = x^3 + Axz^2 + Bz^3.$$

Denote by $0 = (0 : 1 : 0)$ the identity element for the group structure on E. We need the following well-known results (see e.g. [Hu], p. 111), where we present a short proof in the form convenient for us.

Lemma 1. ([Hu], Chap. 5, Sec. 4) *Let $(x : 1 : z) \in E(k)$, v a nontrivial discrete valuation of k. If $z \neq 0$ and $v(z) > 0$, then $v(x) > 0$, and we have $v(z) = 3v(x)$.*

Proof. Assume that $v(x) \leq 0$. Since $(x : 1 : z) \in E(k)$, we have

$$z = x^3 + Axz^2 + Bz^3,$$

and it is clear that $v(x^3) < v(Axz^2), v(x) < v(Bz^3)$. Therefore

$$v(z) = v(x^3 + Axz^2 + Bz^3)$$

$$= v(x^3) \leq 0,$$

a contradiction. Thus $v(x) > 0$. We have

$$v(x^3+Axz^2+Bz^3) \geq min(v(x^3), v(Axz^2), v(Bz^3)) \geq min(v(x^3), v(xz^2), v(z^3)).$$

If $v(x) \geq v(z)$, then the last inequality shows that $v(z) \geq 3v(z)$, which is impossible, since $v(z) > 0$ Hence $v(x) < v(z)$, so $v(z) = v(x^3) = 3v(x)$. ∎

We consider the following well-known filtration on the group of rational points of E (see, e.g. [Hu]). For $r \geq 1$, we set

$$E^r(k) := \{X = (x : 1 : z) \in E(k) | v(x) \geq r, v(z) > 0\} \cup \{0\}.$$

We have the following

Lemma 2. *Let the notation be as in Lemma 1 and let $(\mathcal{O}, \pi)$ be the valuation ring in k, corresponding to v. Then*
1) *([Hu], Chap. 5, Sec. 4) $E^r(k)$ is a subgroup of $E(k)$ for $r \geq 1$.*
2) *The correspondence $\lambda_r : E^r(k) \to \mathcal{O}/\pi^{4r}\mathcal{O}$,*

$$(x : 1 : z) \mapsto \pi^{-r}x \pmod{\pi^{4r}}, 0 \mapsto 0,$$

is a homomorphism of groups and it defines an exact sequence of commutative groups

$$0 \to E^{5r}(k) \to E^r(k) \to \mathcal{O}/\pi^{4r}\mathcal{O}.$$

3) *If $P = (x : 1 : z) \in E^r(k) \setminus E^{r+1}(k)$, then $\pi^{-r}x \not\equiv 0 \ (mod.\pi)$.*

Proof. 1) First we claim that

if $P = (x : 1 : z), P' = (x' : 1 : z') \in E^r(k)$, and if L is the line passing through P, P' and meeting $E(k)$ at $P'' = (x'' : 1 : z'')$, then $v(x+x'+x'') \geq 5r$, $v(z'') = 3v(x'') \geq 3r$.

Indeed, let the equation of L be of the form $Z = cX + b$. If $P \neq P'$, and if $x \neq x'$, then we have $c = (z - z')/(x - x') \in k$. Hence $b \in k$. Since $P \neq P'$ are points of $E(k)$, we have

$$c = (z-z')/(x-x') = (x^2+xx'+x'^2+Az^2)/(1-Ax'(z+z')-B(z^2+zz'+z^2)).$$

By assumption $min(v(x), v(x')) \geq r \geq 1$, and $v(z) > 0$, so by Lemma 1, we have $v(z') \geq 3v(x')$. Since $v(A) \geq 0, v(B) \geq 0$, so

$$v(c) = v(x^2 + xx' + x'^2 + Az^2) \geq min(v(x), v(x') \geq 2r.$$

If $P = P'$, then the line is tangent to the curve

$$(*) \qquad Z = X^3 + AXZ^2 + BZ^3,$$

with the slope $c = dZ/dX$. From the equation it follows that

$$c = (3x^2 + Az^2)/(1 - 2Axz - 3Bz^2),$$

hence in this case we also have

$$v(c) = v(3x^2 + Az^2) \geq 2v(x) \geq 2r.$$

Since $P \in L$, so $z = cx + b$, $v(b) = v(z - cx) \geq min(v(z), v(cx)) \geq 3r$. Substituting $z = cx + b$ into the equation of the curve $(*)$, we have

$$cx + b = x^3 + Ax(cx + b)^2 + B(cx + b)^3.$$

the latter defines a cubic polynomial in x, which has roots x and x' in k, hence it has also another root $x'' \in k$. Let $P'' = (x'' : 1 : z'') \in L \cap E(\bar{k})$. Then $z'' \in k$, since $c, b \in k$, and it follows that $P'' \in E(k)$. Since

$$x + x' + x'' = (-2Abc - 3Bbc^2)/(1 + Ac^2 + Bc^3),$$

from above it follows that $v(x + x' + x'') \geq 5r$, and by Lemma 1, we have $v(z'') \geq 3v(x'') \geq 3r$. Since P, P', P'' are on the same line, $P'' = -(P + P')$ (the addition is in E), we see that $P'' \in E^r(k)$. Moreover, if $P = (x : 1 : z) \in E^r(k)$, then $-P = (-x : 1 : -z) \in E^r(k)$. Thus $E^r(k)$ is a subgroup of $E(k)$.

2) Let $P = (x : 1 : z), P' = (x' : 1 : z') \in E^r(k)$, $P'' = -(P + P')$. As above we have

$$v(x + x' + x'') \geq 5r,$$

thus

$$v(\pi^{-r}x + \pi^{-r}x' + \pi^{-r}x'') \geq 4r,$$

hence

$$\lambda_r(P) + \lambda_r(P') + \lambda_r(P'') \equiv 0 \pmod{\pi^{4r}},$$

i.e., $\lambda_r(P) + \lambda_r(P') \equiv -\lambda_r(P'') (mod.\ \pi^{4r})$. On the other hand, one checks that $\lambda_r(-P) = \pi^{-r}(-x) \equiv \pi^{-r}(x) = \lambda_r(P)\ (mod.\ \pi^{4r})$. Therefore λ_r is a group homomorphism. It is clear that

$$\lambda_r(P) = 0 \Leftrightarrow \pi^{-r}(x) \equiv 0 \ (mod.\ \pi^{4r})$$
$$\Leftrightarrow x \equiv 0 \ (mod.\ \pi^{5r})$$
$$\Leftrightarrow P \in E^{5r}(k).$$

From this we derive the exact sequence above.
3) If $0 \neq P \in E^r(k) \setminus E^{r+1}(k)$, then $v(x) = r$, so $\pi^{-r}x \not\equiv 0 \ (mod.\ \pi)$. ∎

We have the following property of torsion points on elliptic curves over cubic field extension of $\mathbf{Q}$, analogous to Nagell - Lutz Theorem.

Theorem 3. *Let k be a number field (resp. global function field) such that $[k : \mathbf{Q}] \leq 3$ (resp. characteristic $p > 3$) with the ring of integers $\mathcal{O}_k$. Let E be an elliptic curve over k, defined by the equation*

$$y^2 = x^3 + Ax + B,\ A, B \in \mathcal{O}_k. \tag{1}$$

If $P = (x, y) \in E(k)$ is a torsion point, then x, y are belonging to $\mathcal{O}_k$.

Proof. Let n be the order of P.

First we assume that n is odd. Then P is not of order 2, so $y \neq 0$. We write $y = 1/z, z \neq 0, x = x_1/z$. Then we have

$$z = x_1^3 + Ax_1z^2 + Bz^3.$$

We may then consider P as a point on the curve defined by the last equation, which is also a torsion point. Let v be any discrete valuation of k, $(\mathcal{O}_v, \pi)$ the valuation ring in k, corresponding to v. We claim that $v(z) \leq 0$. We consider the following cases.

1) k is a number field. Let p be the prime number corresponding to the restriction $v_p = v|_{\mathbf{Q}}$ of v to $\mathbf{Q}$. If $(n, p) = 1$, then $v(n) = 0$. If $v(z) > 0$ then by Lemma 1, we have $v(x_1) > 0$ and there is a maximal number $r > 0$ such that the point $(x_1 : 1 : z) \in E^r(k)$. Then with notation as in Lemma 2 we have

$$0 = \lambda_r(0) = \lambda_r(n.P)$$

$$= n\lambda_r(P),$$

hence $v(n\pi^{-r}x_1) \geq 4r$, so $v(x_1) \geq 5r$, thus $P \in E^{5r}(k)$, which contradicts with the maximality of r. Therefore $v(z) \leq 0$.

Now we assume $p|n$, $n = pm$. Let $Q = mP$. Then we have $pQ = 0$ in E. Assume that $v(z) > 0$. Then there exists $r \geq 1$ such that $P = (x_1 : 1 : z) \in E^r(k)$. Then $Q = (x_Q : 1 : z_Q) \in E^r(k)$, too. There exists largest number s ($\geq r \geq 1$) such that $Q \in E^s(k)$. Then by considering the homomorphism

$$\lambda_s : E^s(k) \to \mathcal{O}_v/\pi^{4s}\mathcal{O}_v,$$

we have

$$0 = \lambda_s(pQ)$$

$$= p\lambda_s(Q)$$

$$= p\pi^{-s}x_Q\ (mod.\pi^{4s}),$$

hence $v(p\pi^{-s}x_Q) \geq 4s$, thus $v(p) \geq 4s$, since $v(x_Q) = s$. Since $v(p) \leq [k : \mathbf{Q}] \leq 3$, it follows that $s < 1$, impossible. Therefore we have $v(z) \leq 0$ for all v.

2) k is a global function field. We consider any non-trivial discrete valuation of k as above, and in this case, the proof is simpler. In fact, we derive immediately as above (without considering other cases, since we have $v(n) = 0$) that $v(z) \leq 0$, and then we can proceed as above.

Thus in any case $v(z) \leq 0$, which means that $y \in \mathcal{O}_k$. From the equation $y^2 = x^3 + Ax + B$, it follows readily that $x \in \mathcal{O}_k$, too. Thus we have proved that if $P = (x, y) \in E(k)$ is a torsion point of odd order, then its coordinate are algebraic integers.

Next we assume that $P = (x_P, y_P)$ satisfying (1) is a torsion point of $E(k)$ of order 2^n. We proceed by induction on n. If $n = 1$, then $2P = 0$, thus $y_P = 0$ and $x_P^3 + Ax_P + B = 0$. It follows that x_P is also an algebraic integer. Assuming the assertion for order 2^l, with $l \leq n$. Assume that $P \in E$ is a torsion point of order 2^{n+1}. Therefore $2^nP \neq 0$. Set $Q = 2P = (x_1, y_1)$. We have (since $char.k \neq 2$)

$$x_1 = (x^4 - 2Ax^2 - 8Bx + A^2)/(4y^2)$$

$$= (x^4 - 2Ax^2 - 8Bx + A^2)/4(x^3 + Ax + B)$$

hence

$$x^4 - 4x_1x^3 - 2Ax^2 - 4(Ax_1 + 2B)x - 4Bx_1 + A^2 = 0.$$

Since $A, B \in \mathcal{O}_k$, and by inductive hypothesis, $2^nQ = 0$, so x_1, y_1 are algebraic integers. Thus x, and therefore, also y, are algebraic integers. (This argument shows us that if 2^nP is a point with algebraic integers as coordinates, then the same is true for P.)

Now let P be of order $n = 2^rm$, where m is odd. Setting $Q = 2^mP$, then Q is a torsion point of order m, hence it has algebraic integers as coordinates. Above remark finishes the proof. ∎

As a consequence of the proof we have

Corollary 4. *Let k be a number field such that $[k : \mathbf{Q}] \leq 3$, (resp. global function field of characteristic $p > 3$) with the ring of integers $\mathcal{O}_k$. Let E be an elliptic curve over k, defined by the equation* (1). *If $P = (x, y) \in E(k)$ is a torsion point of $E(k)$ of order ≥ 3, then $y^2|(4A^3 + 27B^2)$ in $\mathcal{O}_k$.*

Proof. Since $2P \neq 0$, we have $y \neq 0$. Set $Q = 2P = (x_1, y_1)$. By Theorem 3, x_1, y_1 are belong to $\mathcal{O}_k$. On the other hand,

$$x_1 = (x^4 - 2Ax^2 - 8Bx + A^2)/(4y^2) \in \mathcal{O}_k,$$

so

$$y^2|x^4 - 2Ax^2 - 8Bx + A^2. \tag{2}$$

Also, we have the following well-known identity for elliptic curves (see e.g. [Hu])

$$4A^3 + 27B^2 = (3x^2 + 4A)(x^4 - 2Ax^2 - 8Bx + A^2)$$

$$-(3x^3 - 5Ax - 27B)(x^3 + Ax + B).$$

From this and (2) the corollary follows. ∎

3. Application. We apply the results proved above to get a new and short proof of a theorem of Olson [O], and also an extension to the case of function field.

Theorem 5. ([O], Theorem 1, $k = \mathbf{Q}$) *Let E be an elliptic curve over $k = \mathbf{Q}$ (resp. a global function field k of characteristic $p > 3$), defined by the equation*

$$y^2 = x^3 + ADx + BD^3,\ A, B, D \in \mathcal{O}_k, D \text{ square free.} \tag{3}$$

If $E(k)$ has a torsion point of order ≥ 3, then $D|(4A^3 + 27B^2)$ in $\mathcal{O}_k$.

Proof. Let $k' = k(\sqrt{D})$. Via the transformation

$$\varphi : x \mapsto x_1 = x/D,\ y \mapsto y_1 = y/D^{3/2},$$

the elliptic curve E defined by (3) is mapped isomorphically over k' to the curve

$$E_1 : y_1^2 = x_1^3 + Ax_1 + B.$$

If $P = (x, y)$ is a torsion point of order $m \geq 3$ of $E(\mathbf{Q})$, then $P_1 = \varphi(P) = (x_1, y_1)$ is a torsion point of order m of $E_1(k)$. We consider two cases.

1) $k = \mathbf{Q}$. By Theorem 3, $x, y \in \mathbf{Z}$. Since $m \geq 3$, by Theorem 3 and Corollary 4, $x_1, y_1 \in \mathcal{O}_k$ and we have

$$y_1^2|(4A^3 + 27B^2)$$

in $\mathcal{O}_k$. In other words, for any discrete valuation v of k' we have

$$2v(y_1) \leq v(4A^3 + 27B^2). \tag{4}$$

Since $y_1 = y/D^{3/2} \in \mathcal{O}_k$, we have $v(y) \geq (3/2)v(D)$. We show that

$$v(y) \geq 2v(D). \tag{5}$$

Indeed, it is clear if $v(D) = 0$ or 1. If $v(D) = 2$ then from above we have $v(y) \geq 3$. Let $v_p = v|_{\mathbf{Q}}$ be the p-adic valuation obtained from v by restricting to $\mathbf{Q}$. Since $v(D) = 2$, it follows that $p|D$ and p is ramified in k, $p = \wp^2$, where $\wp$ is a prime in k. Since $v(y) \geq 3$, we have $p|y$, $y\mathcal{O}_k = py'\mathcal{O}_k = \wp^2.(y'\mathcal{O}_k)$, where $y' \in \mathbf{Z}$. Also, from $v(y) \geq 3$ it follows that $v(y') > 0$, $p|y'$, hence $v(y) \geq 4 = 2v(D)$. Therefore $v(y) \geq 2v(D)$ if $v(D) = 0, 1, 2$. On the other hand, since D is square free, $v(D) \leq 2$. Thus in all cases the inequality (5) holds. From this we derive

$$v(y_1 D^{3/2}) = v(y) \geq 2v(D),$$

i.e., for all valuations v of k' we have

$$v(D) \leq 2v(y_1) \leq v(4A^3 + 27B^2), \tag{6}$$

which means that D divides $(4A^3 + 27B^2)$ in $\mathbf{Z}$.

2) *char.k* $= p > 3$. Let $k' = k(\sqrt{D})$. For any non-trivial discrete valuation v on k', let $\pi \in k$ be a prime corresponding to the restriction $v_\pi := v|_k$. As above, by Theorem 3, we have x and y are belonging to $\mathcal{O}_k$, x_1 and y_1 are belonging to $\mathcal{O}_{k'}$, and (4) also holds. In a similar way, where we consider π instead of p, we arrive at (6), which shows $D|(4A^3 + 27B^2)$ in $\mathcal{O}_k$. ∎

Acknowledgements. We would like to thank the Abdus Salam I. C. T. P., S. I. D. A. and Max-Planck Institut für Mathematik, Bonn, for the hospitality and support, which help us to realize this work.

References

[Fu] Y. Fujita, Torsion of elliptic curves over number fields. Dissertation, Tohoku University, Sendai, 2003. Tohoku Mathematical Publications, 27. Tohoku University, Mathematical Institute, Sendai, 2003.

[Hu] D. Husemöller, Elliptic curves, Graduate Text in Math. v. 111, Second ed., Springer - Verlag, 2004.

[JKS] D. Jeon, C.H. Kim and A. Schweizer, On the torsion of elliptic curves over cubic number fields, Acta Arith. 113 (2004), 291-301.

[KT] S. Kotov und L. A. Trelina, S-Ganze Punkte auf elliptischen Kurven, J. für die reine und angew. Math., Bd. 306 (1979), 28 - 41.

[La] M. Laska, Punkte auf elliptischen Kurven über Q in quadratischen Zahlkörpern. Arch. Math. (Basel) 44 (1985), no. 2, 159–167.

[LL] M. Laska and M. Lorenz, Rational points on elliptic curves over Q in elementary abelian 2-extensions of Q. J. Reine Angew. Math. 355 (1985), 163–172.

[O] L. D. Olson, Torsion points on elliptic curves with given j-invariant, Manuscripta Math., Bd. 16 (1975), 145 - 150.

[P] P. Parent, Torsion des courbes elliptiques sur les corps cubiques. Ann. Inst. Fourier (Grenoble) 50 (2000), no. 3, 723–749.

[ScZi] S. Schmitt and H. G. Zimmer, Elliptic curves - a computational approach, Walter de Guyter, Berlin - New York, 2003.

[Si] J. Silverman, The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1992.

[Zi] H. G. Zimmer, Torsion groups of elliptic curves over cubic and certain biquadratic number fields. Arithmetic geometry (Tempe, AZ, 1993), 203–220, Contemp. Math., 174, Amer. Math. Soc., Providence, RI, 1994.