# On the rank of elliptic curves over $\mathbf{Q}(i)$ with torsion group $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$

By Andrej Dujella[*)] and Mirela Jukić Bokun[**)]

(Communicated by Heisuke Hironaka, m.j.a., May 12, 2010)

**Abstract:** We construct an elliptic curve over $\mathbf{Q}(i)$ with torsion group $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ and rank equal to 7 and a family of elliptic curves with the same torsion group and rank $\geq 2$.

**Key words:** Elliptic curve; torsion group; rank.

**1. Introduction.** By the Mordell-Weil theorem, the group $E(\mathbf{K})$ of $\mathbf{K}$-rational points of an elliptic curve $E$ over a number field $\mathbf{K}$ is a finitely generated abelian group. Hence, $E(\mathbf{K})$ is isomorphic to the product of the torsion group and $r \geq 0$ copies of an infinite cyclic group:

$$E(\mathbf{K}) \simeq E(\mathbf{K})_{\text{tors}} \times \mathbf{Z}^r.$$

In the case $\mathbf{K} = \mathbf{Q}$, by Mazur's theorem [8], we know that $E(\mathbf{Q})_{\text{tors}}$ is one of the following 15 groups: $\mathbf{Z}/n\mathbf{Z}$ with $1 \leq n \leq 10$ or $n = 12$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2m\mathbf{Z}$ with $1 \leq m \leq 4$. If $\mathbf{K}$ is a quadratic field, by the results of Kamienny [4] and Kenku and Momose [5], there are 26 possible torsion groups: $\mathbf{Z}/n\mathbf{Z}$ with $1 \leq n \leq 16$ or $n = 18$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2m\mathbf{Z}$ with $1 \leq n \leq 6$, $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3m\mathbf{Z}$ with $n = 1, 2$ and $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. In the case of the Gaussian quadratic field $\mathbf{K} = \mathbf{Q}(i)$, by the recent results of Najman [10,11], there are exactly 16 possible torsion groups, namely, the 15 groups from Mazur's theorem and the group $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. On the other hand, it is not known which values of rank $r$ are possible. The folklore conjecture is that a rank can be arbitrarily large, maybe even if the torsion group is fixed, but it seems to be very hard to find elliptic curves with very large rank (especially if the curve also has a large torsion group). In the case $\mathbf{K} = \mathbf{Q}$, current records for each of the 15 possible torsion groups can be found at `http://web.math.hr/~duje/tors/tors.html`.

In this paper, we will consider elliptic curves over $\mathbf{Q}(i)$ with torsion group $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, the only torsion group which is possible over $\mathbf{Q}(i)$ but not possible over $\mathbf{Q}$. Recently, Rabarison [13] found an infinite family of such curves (parametrized by an elliptic curve with positive rank) with rank $\geq 2$ and a curve with rank equal to 3. We will improve these results by finding a parametric family of curves over $\mathbf{Q}(i)(T)$ with rank $\geq 2$ and a curve over $\mathbf{Q}(i)$ with rank equal to 7 (and several examples with rank equal to 6).

**2. The searching methods.** General form of elliptic curves over $\mathbf{Q}(i)$ with torsion group $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ is

$$y^2 + 4xy + (-64v^4 + 4)y = x^3 + (-16v^4 + 1)x^2. \quad (1)$$

Note that the points $T_1 = [0, 0]$ and

$$T_2 = \left[-2(2v+1)(4v^2+1), 2i(2v+1)^2(2v-i)^2(2v+i)\right]$$

are generators of the torsion group (see [13] for details).

It is well-known (see e.g. [14]) that if an elliptic curve $E$ is defined over $\mathbf{Q}$, then the rank of $E$ over $\mathbf{Q}(i)$ is given by

$$\text{rank}(E(\mathbf{Q}(i))) = \text{rank}(E(\mathbf{Q})) + \text{rank}(E_{-1}(\mathbf{Q})), \quad (2)$$

where $E_{-1}$ is the $(-1)$-twist of $E$ over $\mathbf{Q}$.

In our case, the curve $E$ is given by (1) for $v \in \mathbf{Q}$, and $E_{-1}$ is given by

$$y^2 + 4xy + (-64v^4 + 4)y = x^3 + (16v^4 - 9)x^2 + (-2048v^8 + 256v^4 - 8).$$

There are several known techniques for finding elliptic curves over $\mathbf{Q}$ with relatively high rank within a given family of curves. The main idea is that a curve is more likely to have high rank if $\#E(\mathbf{F}_p)$ is relatively large for many primes $p$. Mestre [6] and Nagao [9] proposed several realizations of this idea involving the computation of various sums (see also [3]). It might be an interesting question to discover which variant (with suitable modifications) is the most appropriate for finding curves (defined over $\mathbf{Q}$) with high rank over $\mathbf{Q}(i)$. For a prime $p$, we put $a_p = a_p(E) = p + 1 -$

2000 Mathematics Subject Classification. Primary 11G05, 14H52, 11R11.

*) Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia.

**) Department of Mathematics, University of Osijek, Trg Ljudevita Gaja 6, 31000 Osijek, Croatia.

doi: 10.3792/pjaa.86.93

$\#E(\mathbf{F}_p)$ and $a'_p = a'_p(E) = p+1-\#E_{-1}(\mathbf{F}_p) = (-1)^{(p-1)/2}a_p$. Our experiments suggest that one reasonable possibility is to maximize the sum $S(N,E)+S(N,E_{-1})$, where

$$S(n,E) = \sum_{p\le n,\, p\,\text{prime}} \frac{-a_p+2}{p+1-a_p}\log(p),$$

$$S(n,E_{-1}) = \sum_{p\le n,\, p\,\text{prime}} \frac{-a'_p+2}{p+1-a'_p}\log(p),$$

and $n$ is a fixed positive integer of moderate size (say $n=1979$). We have implemented this algorithm in `PARI/GP` [12]. By testing the curves with parameters $v=r/s$ with $|r|,|s|\le 3000$, we find several curves with rank 6 and 7. The details on these curves will be given in the next section. To speed up the testing, it is useful to note that the parameters $\pm v$, $\pm\frac{1}{4v}$, $\pm\frac{2v-1}{4v+2}$, $\pm\frac{2v+1}{4v-2}$ give isomorphic curves over $\mathbf{Q}(i)$.

For curves with a large value of $S(n,E)+S(n,E_{-1})$, we try to compute the rank. Our main tool is Cremona's program `MWRANK` [2], which usually works well since our curves have rational 2-torsion points. However, in several cases we need to increase significantly the default height bound for quartic point search, e.g. we used the option `-b 15`. In several undecided cases where `MWRANK` gives only upper and lower bounds for the rank (usually of the form $r\le \text{rank}\le r+2$), we use the parity conjecture and Mestre's conditional upper bound [7] (see also the `APECS` documentation [1])

$$\text{rank} \le \frac{\pi^2}{8\lambda}\left(\log N - 2\sum_{p^m\le e^\lambda} b(p^m)F_\lambda(m\log p)\frac{\log p}{p^m} - M_\lambda\right),$$

where $N$ is the conductor, $b(p^m)=a_p^m$ if $p\mid N$ and $b(p^m)=\alpha_p^m+\alpha_p'^m$ if $p\nmid N$ where $\alpha_p$, $\alpha'_p$ are the roots of $x^2-a_px+p$,

$$M_\lambda = 2\left(\log 2\pi + \int_0^{+\infty}(F_\lambda(x)/(e^x-1)-e^{-x}/x)dx\right),$$

$F_\lambda(x)=F(x/\lambda)$ and the function $F$ can be taken as $F(x)=(1-|x|)\cos(\pi x)+\sin(\pi|x|)/\pi$ for $x\in[-1,1]$ and $F(x)=0$ elsewhere (which give upper bounds for the rank assuming the Birch and Swinnerton-Dyer conjecture and GRH) to determine the rank conditionally.

**3. Examples of curves with the rank 6 and 7.** For $v=1460/357$ we have $\text{rank}(E(\mathbf{Q}))=3$ (indeed, `MWRANK` gives $3\le\text{rank}\le 5$, but Mestre bound (for $\lambda=15$) shows that $\text{rank}<3.897506$, so that, conditionally, rank is equal to 3), $\text{rank}(E_{-1}(\mathbf{Q}))=4$; while for $v=1480/2409$ we have $\text{rank}(E(\mathbf{Q}))=3$, $\text{rank}(E_{-1}(\mathbf{Q}))=4$ (unconditionally).

We give the details (minimal equations for $E$ and $E_{-1}$, torsion points and independent points of infinite order) only for the first curve:

$$E:\ y^2 = x^3 - x^2 - 1767249795031464614697898400x - 2825177437787255580814519386473473680000,$$

$$E_{-1}:\ y^2+xy = x^3 - 11045311218946653841861865 0x + 4414339746542586845022686541364802625 00.$$

Torsion points:

$\mathcal{O}$, $[48477160138401, 0]$,
$[-22065217762000, 0]$, $[-26411942376400, 0]$,
$[121160413850800, 1239452988906797667200]$,
$[121160413850800, -1239452988906797667200]$,
$[-24206093573998, 18526816004783080302]$,
$[-24206093573998, -18526816004783080302]$,
$[-8369705673280, 118518893593457483280\,i]$,
$[-8369705673280, -118518893593457483280\,i]$,
$[-44454179079520, 193750690508659134480\,i]$,
$[-44454179079520, -193750690508659134480\,i]$,
$[-22065217762000 + 17510804960880\,i,$
$14707239283698803688 0 - 36507927046839494400\,i]$,
$[-22065217762000 + 17510804960880\,i,$
$-14707239283698803688 0 + 36507927046839494400\,i]$,
$[-22065217762000 - 17510804960880\,i,$
$14707239283698803688 0 + 36507927046839494400\,i]$,
$[-22065217762000 - 17510804960880\,i,$
$-14707239283698803688 0 - 36507927046839494400\,i]$.

Independent points of infinite order:

$$P_1 = \left[\frac{76401467892191254548169 44}{45473430025}, \frac{20381190232493893534455417298148662272}{9696981585681125}\right],$$

$$P_2 = \left[-\frac{3039226723088080}{121}, \frac{22695919043355349868160}{1331}\right],$$

$$P_3 = \left[\frac{121705279763533930}{169}, \frac{42384437564661574388967130}{2197}\right],$$

$$P_4 = [-37767514808128, 124008728664726403344\, i],$$
$$P_5 = [25986466817360, 237965929380339246240\, i],$$
$$P_6 = [-130147271940280, 1415176379114426739720\, i],$$
$$P_7 = \left[-\frac{642568152906573040}{20449}, \frac{1789907061107961811453300 80}{2924207}\, i\right].$$

Furthermore, we obtain that the rank is equal to 6 for the following values of the parameter $v$: 1003/455, 72/535, 886/1073, 297/2503, 51/305, 175/1201, 924/613, 973/825 (unconditionally, by `MWRANK`), and 232/159, 380/831, 420/1073 (conditionally, using `MWRANK`, Mestre's bounds and the parity conjecture; unconditionally we have that $6 \le \text{rank} \le 8$).

**4. A family with the rank $\geq 2$.** We write the curve $E$ and its twist $E_{-1}$ in the form

$$y^2 = x^3 + Ax^2 + Bx, \quad y^2 = x^3 - Ax^2 + Bx$$

where $A = -(16v^4 + 24v^2 + 1)$, $B = 16(4v^2+1)^2v^2$.

Let us consider the twist $y^2 = x^3 - Ax^2 + Bx$. We want to find a factor $B_1$ of $B$ such that $B_1 - A + B/B_1$ is a square (say $N^2$), which will produce a new point $[B_1, B_1N]$ on the twist. We take $B_1 = -(4v^2+1)$, which yields

$$N^2 = 4v^2(1 - 12v^2). \tag{3}$$

Forcing the right hand side of (3) to be a square, leads to the genus 0 curve $1 - 12v^2 = z^2$. Using a rational solution $v = 0$, $z = 1$, we obtain the parametric solution

$$v = -\frac{2t}{t^2+12}.$$

Moreover, we obtained a point of infinite order

$$P = [B_1, B_1N] = \left[-\frac{(t^2+4)(t^2+36)}{(t^2+12)^2}, \frac{4t(t^4+40t^2+144)(t^2-12)}{(t^2+12)^4}\right].$$

Hence, we have a family with rank $\geq 1$, $y^2 = x^3 - A'x^2 + B'x$, where $A' = -(t^8 + 144t^6 + 3424t^4 + 20736t^2 + 20736)$, $B' = 64t^2(t^2+4)^2(t^2+12)^2(t^2+36)^2$.

Now we consider the equation

$$N^2 = B_1'M^4 - A'M^2e^2 + B'/B_1'e^4.$$

By taking $M = 2$, $e = 1$, $B_1' = 32(t^2+36)^2$, we get

$$N^2 = 2(t^2+18)(t^2-4t+12)^2(t^2+4t+12)^2.$$

Thus, the condition again leads to a genus 0 curve $2(t^2+18) = z^2$. Using the rational solution $t = 0$, $z = 6$, we obtain the parametric solution:

$$t = \frac{12w}{2-w^2},$$

and the additional point of infinite order

$$Q = [4B_1', 2B_1'N] = \left[\frac{165888(w^4+4)^2}{(w^2-2)^4}, \frac{71663616(w^4+4)^2(w^2+2)\times(w^4+4w^3+8w^2-8w+4)\times(w^4-4w^3+8w^2+8w+4)}{(w^2-2)^9}\right].$$

It remains to check that the points $P$ and $Q$ are independent. It is sufficient to find a specialization for which the specialized points are independent, and we have checked that it is the case e.g. for $w = 2$. Hence, we obtained a family of curves with rank $\geq 2$.

**Acknowledgements.** The first author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 037-0372781-2821. The second author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 235-2352818-1042.

## References

[ 1 ] I. Connell, APECS. `ftp://ftp.math.mcgill.ca/pub/apecs/`

[ 2 ] J. E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge Univ. Press, Cambridge, 1997.

[ 3 ] A. Dujella, On Mordell-Weil groups of elliptic curves induced by Diophantine triples, Glas. Mat. Ser. III **42(62)** (2007), no. 1, 3–18.

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

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

[ 6 ] J.-F. Mestre, Construction de courbes elliptiques sur $\mathbf{Q}$ de rang $\geq 12$, C. R. Acad. Sci. Paris Ser. I **295** (1982), 643–644.

[ 7 ] J.-F. Mestre, Formules explicites et minorations de conducteurs de variétés algébriques, Compositio Math. **58** (1986), no. 2, 209–232.

[ 8 ] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent.

Math. **44** (1978), no. 2, 129–162.

[ 9 ] K. Nagao, An example of elliptic curve over $\mathbf{Q}$ with rank $\geq 20$, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), no. 8, 291–293.

[ 10 ] F. Najman, Torsion of elliptic curves over quadratic cyclotomic fields, Math. J. Okayama Univ. (to appear).

[ 11 ] F. Najman, Complete classification of torsion of elliptic curves over quadratic cyclotomic fields, J. Number Theory. (to appear).

[ 12 ] PARI/GP, version 2.3.3, Bordeaux, 2008. `http://pari.math.u-bordeaux.fr/`.

[ 13 ] F. P. Rabarison, Torsion et rang des courbes elliptiques definies sur les corps de nombres algébriques, Doctorat de Université de Caen, 2008.

[ 14 ] U. Schneiders and H. G. Zimmer, The rank of elliptic curves upon quadratic extension, in *Computational number theory* (*Debrecen,* 1989), 239–260, de Gruyter, Berlin.