$\begin{array}{c} \text{Introduction}\\ \text{Torsion group } \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\\ \text{Torsion group } \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\\ \text{Torsion group } \mathbb{Z}/9\mathbb{Z}\end{array}$

Searching for elliptic curves with high rank in the PARI/GP software package

Vinko Petričević vinko.petricevic@ferit.hr (joint work with Andrej Dujella)

FERIT Osijek

June 23, 2023.

 $\begin{array}{c} \mbox{Introduction}\\ \mbox{Torsion group $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$}\\ \mbox{Torsion group $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$}\\ \mbox{Torsion group $\mathbb{Z}/9\mathbb{Z}$} \end{array}$

Motivation

Let *E* be an elliptic curve.

It is well known that the group $E(\mathbb{Q})$ is a finitely generated Abelian group (Mordell 1922).

 $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$

In 1928, Weil generalized it to Abelian varieties over number fields.

In 1978, Mazur proved that there are exactly 15 possible torsion groups for elliptic curves over $\mathbb{Q}:$

$$\mathbb{Z}/k\mathbb{Z}, \text{ for } k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12,$$

 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}, \text{ for } k = 2, 4, 6, 8.$

Kenku and Momose (1988) and Kamienny (1992) proved that in quadratic fields there can occur precisely the following 26 groups:

 $\mathbb{Z}/k\mathbb{Z}, \quad 1 \le k \le 18, k \ne 17,$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}, \quad 1 \le k \le 6,$ $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3k\mathbb{Z}, \quad k = 1, 2,$ $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$

2/15

 $\begin{array}{c} \mbox{Introduction}\\ \mbox{Torsion group $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$}\\ \mbox{Torsion group $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$}\\ \mbox{Torsion group $\mathbb{Z}/9\mathbb{Z}$} \end{array}$

Motivation

Motivation

The questions concerning the rank of elliptic curves are much more difficult than those which concern the torsion group, and satisfactory answers are still unknown. For a long time, it was believed that the rank can be arbitrarily large, i.e. that for any $M \in \mathbb{N}$, there is an elliptic curve E over \mathbb{Q} such that rank $(E) \geq M$. However, some recent papers provide different heuristic arguments on why the rank might actually be bounded.

Details on the record curves can be found on the web pages https://web.math.pmf.unizg.hr/~duje/tors/tors.html https://web.math.pmf.unizg.hr/~duje/tors/torsquad.html

In the last two years, we have found curves with the same rank as the record for $E(\mathbb{Q})$ and torsion group $\mathbb{Z}/9\mathbb{Z}$.

In $E(\mathbb{K})$ we broke the record for torsion groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Motivation

In the book *Number theory* of prof. Dujella, can be found formulas for elliptic curves with given torsion group.

The problem is that we need to calculate the rank for large number of curves. In various math packages there are commands that we can use to calculate the rank more or less well.

In the newer versions of PARI/GP software package, they added the command ellrank which in some situations calculate the rank of the elliptic curve very well. They also added support for multithreading, which allowed us to use supercomputers.

 $\begin{array}{c} \text{Introduction}\\ \textbf{Torsion group } \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\\ \text{Torsion group } \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\\ \text{Torsion group } \mathbb{Z}/9\mathbb{Z} \end{array}$

Torsion group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

In torsion group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ previous record was held by M. Jukić Bokun. In the paper On the rank of elliptic curves over $\mathbb{Q}(\sqrt{-3})$ with torsion groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ she have found rank 7 elliptic curve. We have improved her results and found elliptic curves over the field $\mathbb{Q}(\sqrt{-3})$ with ranks equal to 8 for torsion group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. We used some similar tools. Our main tool for calculating the rank over

 $\mathbb{Q}(\sqrt{-3})$ (the only field where $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ can appear) was also the fact that if *E* is an elliptic curve over \mathbb{Q} , then the rank of over $\mathbb{Q}(\sqrt{-3})$ is given by

$$rank(E(\mathbb{Q}(\sqrt{-3}))) = rank(E(\mathbb{Q})) + rank(E_{-3}(\mathbb{Q})),$$

where E_{-3} is the (-3)-twist of E over \mathbb{Q} .

We also started with a family of elliptic curves E(s, t):

$$y^{2} + s(ts^{2} - 12)xy + 4t(144s^{2} - 24ts^{4} + 432ts + 432t^{2} + t^{2}s^{6} - 36t^{2}s^{3})y = x^{3}.$$

 $\begin{array}{c} \quad \mbox{Introduction} \\ \hline \mbox{Torsion group } \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} \\ \hline \mbox{Torsion group } \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} \\ \hline \mbox{Torsion group } \mathbb{Z}/9\mathbb{Z} \end{array}$

Rank 8 curves

For $(s, t) \in \{(2/7, -45/134), (4/7, -630/923), (-6/7, 945/998)\}$ we get elliptic curve

 $y^2 + y = x^3 + x^2 + 8804205157156465x + 383138550586901919299306$, with 4 independent points of infinite order:

while (-3)-twist also have 4 independent points:

[364239808947/2209,278659347206075988/103823], [1338962052421/100,1549699239583785869/1000], [181213268371821/643204,3022985780907365891361/515849608], [63972838783,16180712076509801]. $\begin{array}{c} \quad \mbox{Introduction} \\ \hline \mbox{Torsion group } \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} \\ \hline \mbox{Torsion group } \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} \\ \hline \mbox{Torsion group } \mathbb{Z}/9\mathbb{Z} \end{array}$

Rank 8 curves

For (s, t) = (-17/7, 345/784) we get elliptic curve

 $y^2 + xy + y = x^3 - x^2 - 617578612649267520977x$

-1810438138102192424754169503871,

with 5 independent points:

[-2253623821475783/192721,165192115750406697024754/84604519], [6365701073973751/106929,459116006063876020943156/34965783], [82283478289207/81,746171021611085246684/729], [48974552317,9241713515007306], [11295664889614243/344569,734116315141191621603968/202262003],

while (-3)-twist have 3 independent points:

[69881507983, 1314126823438408],

[729852143293/9,309555491671516223/27],

[8427306357071/100, 13378211660467663051/1000].

 $\begin{array}{c} \quad \mbox{Introduction} \\ \mbox{Torsion group } \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} \\ \mbox{Torsion group } \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} \\ \mbox{Torsion group } \mathbb{Z}/9\mathbb{Z} \end{array}$

Torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

In torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ previous record was also held by Duje and M. Jukić Bokun (A. Dujella and M. Jukić Bokun, *On the rank of elliptic curves over* $\mathbb{Q}(i)$ with torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$. For $\mathbb{K} = \mathbb{Q}(i)$ (the only field where $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ can appear), we are also looking of curves and (-1)-twist and family with torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$:

$$y^{2} + 4xy + (-64t^{4} + 4)y = x^{3} + (-16t^{4} + 1)x^{2}.$$

We also used this family, and found elliptic curve with the record rank.

 $\begin{array}{c} \quad \mbox{Introduction} \\ \mbox{Torsion group $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$} \\ \mbox{Torsion group $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$} \\ \mbox{Torsion group $\mathbb{Z}/9\mathbb{Z}$} \end{array}$

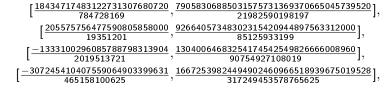
Rank 8 curve

For t = 180/6643 we get elliptic curve

 $y^2 = x^3 - x^2 - 1264285630784571919597349762400x$

 $-\ 546907189853176652858460972620151389392800000,$

with 4 independent points of infinite order:



while (-1)-twist have also 4 independent points:

 $[\frac{469572437338020,8659141260066207245250]}{17606416}, \frac{583152676543238826927776148008847}{73876521536}], \\ [177864765470100,343279086114405591450], \\ [\frac{447490645354678560274980}{2884441849}, \frac{22220310008210701689236734902375750}{1549147183842243}].$

 $\begin{array}{c} \text{Introduction}\\ \text{Torsion group } \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\\ \text{Torsion group } \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\\ \text{Torsion group } \mathbb{Z}/9\mathbb{Z}\end{array}$

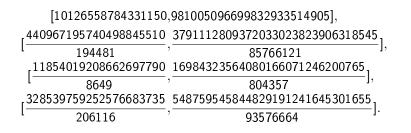
Torsion group $\mathbb{Z}/9\mathbb{Z}$ - rank 4 curves

In this torsion group, there were known 3 curves with rank 4, one from Fisher (2009), and two from van Beek (2015).

We have found 3 new curves.

 $y^{2} + xy = x^{3} - 8445699463299696674029285543155x$ + 9446705591085118541016112920676157302177853025.

Independent points of infinite order are:



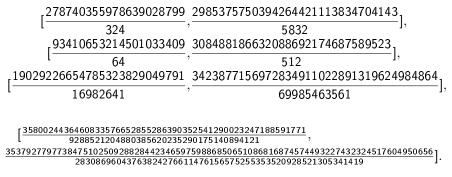
 $\begin{array}{c} \quad \mbox{Introduction} \\ \mbox{Torsion group } \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} \\ \mbox{Torsion group } \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} \\ \mbox{Torsion group } \mathbb{Z}/9\mathbb{Z} \end{array}$

Torsion group $\mathbb{Z}/9\mathbb{Z}$ - rank 4 curves

 $y^2 + xy + y = x^3 - x^2 - 3957522204786046962200201992567404677x$

+ 3029988614585142118644653464298252623281447852094930301.

Independent points of infinite order are:



Pari was unable to find the last point, but Dujella find it using Magma.

Introduction Torsion group Z/3Z × Z/3Z Torsion group Z/4Z × Z/4Z Torsion group Z/9Z

Torsion group $\mathbb{Z}/9\mathbb{Z}$ - rank 4 curves

 $y^2 + xy = x^3 - 23403453875708065582617252610904740290x$

+ 56740472134219104191564989530383862470828076555856412100. Independent points of infinite order are:

 $[-\frac{2124831061815491209344}{625},-\frac{153897336826049953226494844248254}{/15625}],$

 $[-\frac{25383574246817605139361514218789870}{11541875487800641},\\-\frac{12248431721078582644888104112139415756148879568434740}{1239979705847820288430561}],$

we were unable to find the fourth point, but R. Rathbun did it:

 $[\frac{11039168903707688516615907465345318179937903715079971086630}{254035585383892857719517730338266639041},$

4048944608766863824144593988025419443424110442121986160161

We have found many curves which could be a good candidate for huge rank. However, many of them had not big rank. To reduce them we used W. Stein's implementation of Bober's algorithm, which easily can be implement to work in multithreading (J. W. Bober: *Conditionally bounding analytic ranks of elliptic curves*).

I would like to acknowledge the usage of the supercomputing resources of University of Rijeka, BURA.

Funding

This work was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Program (Grant KK.01.1.1.01.0004).

Za više informacija posjetite: http://bela.phy.hr/quantixlie/hr/ https://strukturnifondovi.hr/

Sadržaj ove prezentacije isključiva je odgovornost Prirodoslovnomatematičkog fakulteta Sveučilišta u Zagrebu te ne predstavlja nužno stajalište Europske unije. For more information: http://bela.phy.hr/quantixlie/hr/ https://strukturnifondovi.hr/

The content of this presentation is exclusive responsibility of the Faculty of Science University of Zagreb and does not represent opinion of the European Union



EUROPSKA UNIJA Zajedno do fondova EU





Projekt sufinancira Europska unija iz Europskog fonda za regionalni razvoj Project co-financed by European Union through the European Regional Development Fund

Thank you for your attention