#A70 INTEGERS 16 (2016)

HIGH RANK ELLIPTIC CURVES WITH TORSION $\mathbb{Z}/4\mathbb{Z}$ INDUCED BY KIHARA'S ELLIPTIC CURVES

Foad Khoshnam
Iran Insurance Applied Science Center, Tehran, Iran
khoshnam@ii-uast.ac.ir

Dustin Moody
Computer Security Division, National Institute of Standards & Technology, Gaithersburg, Maryland
dustin.moody@nist.gov

Received: 2/3/16, Accepted: 10/2/16, Published: 10/5/16

Abstract

Working over the field $\mathbb{Q}(t)$, Kihara constructed an elliptic curve with torsion group $\mathbb{Z}/4\mathbb{Z}$ and five independent rational points, showing the rank is at least five. Following his approach, we give a new infinite family of elliptic curves with torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank at least five. This matches the current record for such curves. In addition, we give specific examples of these curves with ranks 10 and 11.

1. Introduction

As is well-known, an elliptic curve E over a field $\mathbb{K}$ can be explicitly expressed by the generalized Weierstrass equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$. In this paper, we are interested in elliptic curves defined over the rationals, i.e., $\mathbb{K} = \mathbb{Q}$. The famous Mordell-Weil theorem says that every elliptic curve over $\mathbb{Q}$ has a commutative group $E(\mathbb{Q})$ which is finitely generated. That is, $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$, where r is a nonnegative integer and $E(\mathbb{Q})_{tors}$ is the subgroup of elements of finite order in $E(\mathbb{Q})$. This subgroup is called the torsion subgroup of $E(\mathbb{Q})$ and the integer r is known as the rank of E.

By Mazur's theorem [12], the torsion subgroup $E(\mathbb{Q})_{tors}$ can only be one of fifteen groups: $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$. While the possibilities for the torsion subgroup are finite, the situation is not as clear for the rank r. The folklore conjecture is that the rank can be arbitrarily large, but it seems to be very hard to find concrete examples of elliptic curves with large rank. The current record is an example of an elliptic curve over $\mathbb{Q}$ with rank at least 28, found by Elkies in May 2006 (see [5]). There is no known guaranteed algorithm to determine the rank and it is not known which integers can occur as ranks.

Let T be an admissible torsion group for an elliptic curve E over $\mathbb{Q}$. Define

$$B(T) = \sup\{\text{rank } E(\mathbb{Q}) : \text{torsion group of } E \text{ over } \mathbb{Q} \text{ is } T\},$$

$$G(T) = \sup\{\text{rank } E(\mathbb{Q}(t)) : \text{torsion group of } E \text{ over } \mathbb{Q}(t) \text{ is } T\},$$

$$C(T) = \limsup\{\text{rank } E(\mathbb{Q}) : \text{torsion group of } E \text{ over } \mathbb{Q} \text{ is } T\}.$$

There exists a conjecture in this setting that says $B(T)$ is unbounded for all T. Even though $B(T)$ is conjectured to be arbitrarily high, it appears difficult to find examples of curves with high rank. There has been much interest in finding high rank elliptic curves with specified torsion groups. See [2, 3] for tables with the best known lower bounds for $B(T), G(T)$, and $C(T)$, including references to the papers where each bound is found.

In this paper, we will consider elliptic curves with torsion group $\mathbb{Z}/4\mathbb{Z}$. The current record for the highest rank of an elliptic curve with this torsion group is 12, with a curve found by Elkies in 2006 [5], as well as another recently found by Dujella and Peral [2]. In 2004, Kihara [8] found an infinite one-parameter family of curves with torsion group $\mathbb{Z}/4\mathbb{Z}$ and having rank (at least) 4. He extended this to an infinite rank 5 family whose fifth point was parameterized by a positive rank curve. Later in [9], he improved his results to an unconditional family of rank (at least) 5. Dujella, et. al. [4], by using a suitable injective specialization, subsequently proved that the rank of Kihara's family over $\mathbb{Q}(t)$ is exactly equal to 5 and found explicit generators. In 2007, Elkies also found an infinite family with rank at least 5 and a rank 6 family dependent on a positive rank curve [6]. Thus, $B(\mathbb{Z}/4\mathbb{Z}) \geq 12$, $G(\mathbb{Z}/4\mathbb{Z}) \geq 12$, and $C(\mathbb{Z}/4\mathbb{Z}) \geq 6$.

The main contribution of this work is a new family of elliptic curves with torsion group $\mathbb{Z}/4\mathbb{Z}$, and rank (at least) 5. In fact, we show the family has rank exactly 5 over $\mathbb{Q}(t)$. This family matches the best known results for high rank for an infinite family of elliptic curves with torsion group $\mathbb{Z}/4\mathbb{Z}$. We also find two elliptic curves with rank 11, and many with rank 10, all of which have not been previously published. According to [2], there are only two other known curves with rank 11 (and torsion group $\mathbb{Z}/4\mathbb{Z}$).

Our starting point to find these families of curves is Kihara's original paper [8]. We review Kihara's method in Section 2, and in Section 3 find a new solution to some of Kihara's equations, leading to a different rank 4 family than Kihara found. In Section 4, we further specialize this family to create a fifth rational point. We show that the family has rank 5 over $\mathbb{Q}(t)$ in Section 5, and find the generators. We performed a computer search for specific curves in our families with high rank. The results are given in Section 6.

2. Kihara's Method

We briefly describe Kihara's construction [8]. Consider the projective curve

$$C : (x^2 - y^2)^2 + 2A(x^2 + y^2)z^2 + Bz^4 = 0.$$

C can be transformed into Weierstrass form by setting $X = (A^2 - B)y^2/x^2$ and $Y = (A^2 - B)y(Bz^2 + Ax^2 + Ay^2)/x^3$, resulting in the curve

$$E : Y^2 = X^3 + (2A^2 + 2B)X^2 + (A^2 - B)^2 X. \tag{1}$$

The point $P = (A^2 - B, 2A(A^2 - B))$ is on E and it can be easily checked that $2P = (0, 0)$ and $4P = \mathcal{O}$, the identity element of E. Now consider the affine model of C

$$H : (x^2 - y^2)^2 + 2A(x^2 + y^2) + B = 0.$$

If we assume that the points $P_1 = (r, s)$ and $P_2 = (r, u)$ are on H, then it is required that $A = (2r^2 - s^2 - u^2)/2$ and $B = s^2u^2 + s^2r^2 + u^2r^2 - 3r^4$. We further assume that the points $P_3 = (s, p)$ and $P_4 = (u, q)$ are also on H, and so we must have

$$p^2 = 3s^2 + u^2 - 3r^2, \tag{2}$$

$$q^2 = s^2 + 3u^2 - 3r^2. \tag{3}$$

Kihara gave the following parametric solution to the Diophantine equations (2),(3):

$$\begin{aligned} r &= t^2 - 33, \\ s &= t^2 - 2t - 27, \\ u &= t^2 - 6t + 33, \\ p &= t^2 - 12t + 3, \\ q &= t^2 - 20t + 27. \end{aligned}$$

Thus, there are four $\mathbb{Q}(t)$-rational points on the affine curve H, and consequently four $\mathbb{Q}(t)$-rational points on the corresponding elliptic curve E.

3. A Family of Elliptic Curves with Rank at Least 4

We solve the equations (2) and (3) in a different way. By subtracting (3) from (2), we have that

$$p^2 + 2u^2 = q^2 + 2s^2. \tag{4}$$

Recall the well-known Brahmagupta identity

$$\begin{aligned} (a^2 + Nb^2)(c + Nd^2) &= (ac - Nbd)^2 + N(ad + bc)^2 \\ &= (ac + Nbd)^2 + N(ad - bc)^2. \end{aligned}$$

By setting $N = 2$, and letting

$$\begin{aligned} p &= ac + 2bd, \\ q &= ac - 2bd, \\ u &= bc - ad, \\ s &= bc + ad, \end{aligned}$$

we see that we have a solution to (4).

From (2), we require $r^2 = (3s^2 + u^2 - p^2)/3$. Substituting in, this translates to

$$r^2 = (4/3)b^2c^2 + (4/3)a^2d^2 - (1/3)a^2c^2 - (4/3)b^2d^2. \tag{5}$$

In order to find a parametric solution to (5) we fix c and d. Now we rewrite (5) in the form

$$4b^2(c^2 - d^2) + 4a^2(d^2 - c^2/4) = 3r^2. \tag{6}$$

If we consider $4(c^2 - d^2) = \alpha$ and $4(d^2 - c^2/4) = \beta$, then (6) can be written $\alpha b^2 + \beta a^2 = 3r^2$, with parametric solution given by

$$\begin{aligned} a &= (d^2 - c^2)m^2 + 3n^2, \\ b &= (d^2 - c^2)m^2 - 3cmn - 3n^2, \\ r &= c(d^2 - c^2)m^2 + (4(d^2 - c^2))mn - 3cn^2, \end{aligned}$$

for any c, d. Therefore

$$\begin{aligned} r &= 4c^2mn - cm^2d^2 + 3cn^2 - 4mnd^2 + c^3m^2, \\ s &= cm^2d^2 - c^3m^2 - 3c^2mn - 3cn^2 + m^2d^3 - dm^2c^2 + 3dn^2, \\ u &= cm^2d^2 - c^3m^2 - 3c^2mn - 3cn^2 - m^2d^3 + dm^2c^2 - 3dn^2, \\ p &= cm^2d^2 - c^3m^2 + 3cn^2 + 2m^2d^3 - 2dm^2c^2 - 6dcmn - 6dn^2, \\ q &= cm^2d^2 - c^3m^2 + 3cn^2 - 2m^2d^3 + 2dm^2c^2 + 6dcmn + 6dn^2. \end{aligned}$$

If we write the elliptic curve E from (1) in the form

$$Y^2 = X^3 + A_4X^2 + B_4X,$$

then a simple calculation yields

$$\begin{aligned}A_4 = &-240c^7m^7d^4n - 16c^{11}m^7n - 432c^5mn^7 - 16c^2m^8d^{10} + 48m^6d^{10}n^2\\ &+ 432m^2d^6n^6 - 1512c^6m^2n^6 - 808m^4d^8n^4 - 16c^6m^8d^6 - 736c^9m^5n^3\\ &+ 4c^8m^8d^4 - 1708c^8m^4n^4 + 24c^4m^8d^8 - 168c^{10}m^6n^2 - 2208c^7m^3n^5\\ &+ 4m^8d^{12} + 324d^4n^8 + 112c^9m^7d^2n - 2136c^6m^6d^4n^2 + 4528c^7m^5d^2n^3\\ &+ 1680c^4m^6d^6n^2 + 1104c^8m^6d^2n^2 + 9712c^6m^4d^2n^4 - 12840c^4m^4d^4n^4\\ &- 7440c^5m^5n^3d^4 + 208c^5m^7nd^6 + 11376c^5m^3n^5d^2 - 528c^2m^6d^8n^2\\ &+ 5968c^2m^4d^6n^4 - 10944c^3n^5d^4m^3 + 1728c^3n^7d^2m - 64c^3m^7d^8n\\ &+ 4672c^3m^5d^6n^3 + 6912c^4m^2d^2n^6 - 3888c^2m^2d^4n^6 + 3072m^3d^6n^5c\\ &- 1024m^5d^8n^3c,\end{aligned}$$

$$\begin{aligned}B_4 = &\,16m^2n^2(2n+mc)^2(-d+c)^2(2d+c)^2(-2d+c)^2(d+c)^2(n+dm+mc)^2\\ &\times(3n-dm+mc)^2(3n+dm+mc)^2(3cn+2c^2m-2d^2m)^2(n-dm+mc)^2.\end{aligned}$$

With the values given above, the curve $E(c,d,m,n)$ has a point of order 4, as well as four rational points. Using specialization, the four rational points can easily be shown to be independent. For instance, when $(c,d,m,n) = (3,2,1,1)$, the height pairing matrix has determinant 357.065396133752 as computed by SAGE [13]. Thus P_1, P_2, P_3, and P_4 are independent.

4. An Infinite Family with Rank 5

Following the approach of Kihara's second paper [9], we seek to force a fifth point $P_5 = (p, M)$ on H. The point P_5 will only be rational if we have a rational solution to the equation

$$M^2 = 6s^2 + 3u^2 - 8r^2.$$

Substituting in the expresssions for r, s, and u in terms of c, d, m, and n, we note that the expression $6s^2 + 3u^2 - 8r^2$ is a quartic in m. In fact, this is expression is

$$((c+3d)(c^2-d^2))^2m^4 + \ldots + (3n^2(c-3d))^2.$$

If we set this equal to $(t_2m^2 + t_1m + t_0)^2$, where $t_2 = (c+3d)(c^2-d^2)$ and $t_0 = 3n^2(c-3d)$ then a little bit of algebra finds that setting

$$t_1 = -cn\frac{5c^2 - 9cd - 32d^2}{c+3d}$$

leads to $6s^2 + 3u^2 - 8r^2 = (t_2m^2 + t_1m + t_0)^2$, if

$$m = -12\frac{cdn(c+3d)}{(c^2-d^2)(3c^2+8cd+12d^2)}.$$

This leads to an infinite family with five rational points, in terms of c, d, and n. To simplify the coefficients, we perform an isomorphism $(x, y) \to (k^2x, k^3y)$ where

$$k = \frac{(c^2 - d^2)^2(3c^2 + 8dc + 12d^2)^4}{18n^4(c^2 - 4d^2)^2}.$$

The resulting family is the curve $E : y^2 = x^3 + A_5x^2 + B_5x$, where A_5 and B_5 are homogenous polynomials in c and d. We can thus set $d = 1$, obtaining

$$\begin{aligned}A_5 = {} & 34992\,c^{19} + 268272\,c^{18} + 563760\,c^{17} - 668655\,c^{16} - 3947184\,c^{15} + 1925820\,c^{14} \\ & + 44407056\,c^{13} + 137106486\,c^{12} + 233620224\,c^{11} + 231242652\,c^{10} + 51841920\,c^{9} \\ & - 219842399\,c^{8} - 358210752\,c^{7} - 238162320\,c^{6} - 9324288\,c^{5} + 125750880\,c^{4} \\ & + 110730240\,c^{3} + 39377664\,c^{2} + 8957952\,c + 1679616,\end{aligned}$$

$$\begin{aligned}B_5 = {} & 576(c-1)^2(c+1)^2c^4(c-2)^2(c+3)^2(c+2)^2(3c^2+c+6)^2(3c^2+7c+6)^2 \\ & (3c^2+8c+12)^2(3c^2-13c-6)^2(3c^2+5c-6)^2(3c^2+2c+3)^2.\end{aligned}$$

We denote this curve by E_c, since the parametrization is only dependent on c (and not n or d). Thus, we have an infinite number of curves in this family with rank at least 5, which can be proved by specialization at $c = -6/5$, where the height pairing matrix has determinant 5062.58320537396.

To verify that this family is different than Kihara's family, let $j(t)$ be the j-invariant of the elliptic curve E_t given in Kihara's paper [9]. Let $j(c)$ be the j-invariant of the curve E_c given above. We checked that there are no solutions to the equation $j(t) - j(c)$, for any value of $c = a/b$, with $0 < |a|, b \leq 100$. If the two families were isomorphic, then there would exist solutions.

5. The Generators of the Rank 5 Family

Similarly as done in [4], we find the generators of the family E_c and prove the rank is 5 over $\mathbb{Q}(c)$. The key result needed is a theorem of Gusić and Tadić [7], for elliptic curves E given by $y^2 = x^3 + A(t)x^2 + B(t)x$, where $A, B \in \mathbb{Z}[t]$, with exactly one nontrivial 2-torsion point over $\mathbb{Q}(t)$. If $t \in \mathbb{Q}$ satisfies the condition that for every nonconstant square-free divisor h of $B(t)$ or $A(t)^2 - 4B(t)$ in $\mathbb{Z}[t]$ the rational number $h(t_0)$ is not a square in $\mathbb{Q}$, then the specialized curve E_{t_0} is elliptic and the specialization homomorphism at t_0 is injective.

If additionally there exist $P_1, \cdots, P_r \in E(\mathbb{Q}(t))$ such that $P_1(t_0), \cdots, P_r(t_0)$ are the free generators of $E(t_0)(\mathbb{Q})$, then $E(\mathbb{Q}(t))$and $E(t_0)(\mathbb{Q})$ have the same rank r, and $P_1, \cdots, P_r$ are the free generators of $E(\mathbb{Q}(t))$.

Just as in [4], the points P_i, for $i = 2, 3, 4, 5$, all satisfy $P_1 + P_i = 2Q_i$ for some point Q_i on $E(c)$. Concretely,

$$\begin{aligned}
Q_2 = {} & ((c-1)(c+1)(3c^2+c+6)(3c^2+7c+6)(3c^2-13c-6)(3c^2+5c-6) \\
& \times (9c^4+48c^3+115c^2+48c+36)^2, c(c-1)(9c^4+48c^3+115c^2+48c+36) \\
& \times (3c^2+c+6)(c+1)(3c^2+5c-6)(3c^2+7c+6)(9c^4-61c^2-96c-108) \\
& \times (3c^2-13c-6)(216c^9+1449c^8+3624c^7+4446c^6+1728c^5-1103c^4 \\
& -2784c^3+216c^2+3456c+1296)), \\
Q_3 = {} & (48c^3(c-1)(c+2)(c+1)(3c^2+c+6)(3c^2+8c+12)(3c^2-13c-6)(c+3)^2 \\
& \times (3c^2+5c-6)^2, -48c^3(c+1)(c-1)(c+3)^2(c+2)(3c^2+8c+12) \\
& \times (3c^2+5c-6)^2(3c^2+5c-6)^2(3c^2+c+6)(3c^2-13c-6)(162c^{10}+324c^9 \\
& -459c^8-3840c^7-8880c^6-9924c^5-4175c^4+11040c^3+18360c^2+8640c \\
& +1296)), \\
Q_4 = {} & (48c^3(c-2)(3c^2+c+6)(3c^2+8c+12)(3c^2-13c-6)(c+3)^2(c+1)^2 \\
& \times (6c^2-5c+6)^2(3c^2+7c+6)^2/(7c+6)^2, -48c^3(c+1)(c-1)(c+3)^2(c+2) \\
& \times (3c^2+8c+12)(3c^2+c+6)(3c^2-13c-6)(162c^{10}+324c^9-459c^8-3840c^7 \\
& -8880c^6-9924c^5-4175c^4+11040c^3+18360c^2+8640c+1296)), \\
Q_5 = {} & (64c^3(c-1)(c-2)(c+3)(3c^2+2c+3)(3c^2+8c+12)(3c^2-13c-6) \\
& \times (3c^2+5c-6)(3c^2+7c+6)^2, -48c^3(c-1)(c+1)(c+3)^2(c+2) \\
& \times (3c^2+8c+12)(3c^2+5c-6)^2(3c^2+c+6)(3c^2-13c-6)(162c^{10}+324c^9 \\
& -459c^8-3840c^7-8880c^6-9924c^5-4175c^4+11040c^3+18360c^2+8640c \\
& +1296)).
\end{aligned}$$

We also have

$$\begin{aligned}
Q_1 = {} & (-24(c+2)(c-2)(c-1)(c+1)(3c^2-13c-6)(3c^2+5c-6)(3c^2+c+6) \\
& \times (3c^2+7c+6)(3c^2+2c+3)(c+3)(9c^5+3c^4-41c^3-67c^2-12c-36)^2 \\
& \times (3c^2+8c+12)/(9c^4-61c^2-96c-108)^2, 24(c-2)(c+2)(c+1)(c+3) \\
& \times (c-1)(3c^2-13c-6)(3c^2+5c-6)(3c^2+c+6)(3c^2+7c+6)(3c^2+2c+3) \\
& \times (3c^2+8c+12)(9c^5+3c^4-41c^3-67c^2-12c-36)(17496c^{18}+121743c^{17} \\
& +115425c^{16}-1292112c^{15}-5110992c^{14}-5428170c^{13}+14855802c^{12} \\
& +66008328c^{11}+120014112c^{10}+107134883c^9-34458947c^8-247766784c^7 \\
& -352545120c^6-246090528c^5-45834336c^4+75271680c^3+70170624c^2 \\
& +20715264c+1679616)/(9c^4-61c^2-96c-108)^3).
\end{aligned}$$

Checking the conditions of the Gusić and Tadić specialization theorem, a calculation shows $c = -21/20$ satisfies the squarefree requirements. Furthermore, $E_{-21/20}$

has rank 5, with generators

$$\begin{aligned}
W_1 = (&-20267924789539728753288856980600917277/3556814946304000000000\\
&0000000000, -44877945992984377975724906232511441789573574504730 2\\
&4651/33539911308059607040000000000000000000000000000),\\
W_2 = (&-13093678749940185033860723639114157/2441150464000000000000000\\
&0000, -69092878561298015416940736324954933546907667962989/603061\\
&810626560000000000000000000000000000),\\
W_3 = (&-15197282700176912764695930790260813/2917728256000000000000000\\
&0000, 81412088006787334224770902297938068184642194262723/78802004\\
&7380480000000000000000000000000000),\\
W_4 = (&32152011117817302350909977707/655360000000000000000000, 125934775\\
&37698657949624647957303231653667527/8388608000000000000000000000\\
&0000000),\\
W_5 = (&2601527024655173135032681319662136007508737243116036240559397896\\
&06971409/4549349522128061401278405671331450389401600000000000000\\
&0000000000, 29572656103560837694845166511685248784281246955726134\\
&929366720527095665119340576669429015697510994399436077 9/19406800\\
&99562020005390277748619119760466939598585539844027187200000000000\\
&00000000000000000000000000).
\end{aligned}$$

It can be checked that (disregarding torsion), $Q_1 = -2W_3 + W_5$, $Q_2 = -W_1 + W_2 - 3W_3 - W_4 + W_5$, $Q_3 = W_1 + 2W_3 + W_4 - W_5$, $Q_4 = W_1 + 2W_3 - W_5$, $Q_5 = W_2$. The matrix of conversion has determinant -1. Thus, the $Q_i(c)$ are the generators of E_c.

6. Examples of curves with high rank

The highest known rank of an elliptic curve over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/4\mathbb{Z}$ is rank 12 (see [2, 5]). From Dujella's table [2], there are also two known examples of curves with rank 11, and some elliptic curves with rank 10. Doing a computer search, we found two new curves with rank 11 and many curves with rank 10. We actually only list a few of the many rank 10 curves we found (over forty rank 10 curves). Note that the curves listed below are all new, meaning they have never appeared in the literature (to the best of our knowledge). We refer to [2] for the details of the other high rank curves with torsion group $\mathbb{Z}/4\mathbb{Z}$.

A common strategy for finding high rank elliptic curves over $\mathbb{Q}$ is the construction of families of elliptic curves with high generic rank, and then searching for adequate specialization with efficient sieving tools. One popular tool is the Mestre-Nagao sum, see for example [10, 11]. These sums are of the form

$$S(n,E) = \sum_{p \leq n,\ p \text{ prime}} \left(1 - \frac{p-1}{\#E(\mathbb{F}_p)}\right) \log p. \tag{7}$$

For our search, we used the family of elliptic curves with rank at least 4 given in Section 3. We attempted to search the rank 5 family, but the large coefficients proved too much of an impediment in the calculations. Since the curve in Section 3 with parameters $[c,d,m,n]$ is isomorphic to the curve with parameters $[cm/n, dm/n, 1, 1]$, we can take $m = n = 1$. Using the Mestre-Nagao sums (7), we looked for those curves E with $S(523,E) > 20$ and $S(1979,E) > 32$. We ranged over the values $c = p/q$ and $d = r/s$, with $-100 \leq p \leq 120, 1 \leq q \leq 100, -100 \leq r \leq 100$ and $1 \leq s \leq 100$.

After this initial sieving, we calculated the rank of the remaining curves with `mwrank` [1], though we note we were not always able to determine the rank exactly. Table 1 summarises the results.

c	d	rank
99/2	99/10	11
108/71	-74/71	11
1	3/34	10
41/22	71/66	10
67/13	24/13	10
74/83	61/83	10
82/3	45	10
88/75	47/30	10
82/63	11/9	10
115/79	23/79	10
139/16	97/16	10
-89/55	13/22	10
-96/7	81	10
-98/39	35/13	10
-99/32	51/8	10
-1/28	41/70	10
-9/7	66/91	10

Table 1: High rank elliptic curves with torsion subgroup $\mathbb{Z}/4\mathbb{Z}$

We give some details on the rank 11 curves. For the parameters $(c,d,m,n) = (99/2, 99/10, 1, 1)$ in the family from Section 3 we may write the first curve with rank equal to 11 in the form

$$\begin{aligned} y^2 + xy = {} & x^3 - 835989589245879094648543468307663017 70x \\ & + 2945584756350286890221962366255202390319646506418231 08900, \end{aligned}$$

with 11 independent rational points

$$\begin{aligned}
P_1 &= (-376658071791198860, 180552834744478233974878930 30),\\
P_2 &= (-10533246148223735060, 254379054304084801844464 9030),\\
P_3 &= (156463934499960842778983498260/33904961689, 1657040529599161192 7241\\
&\qquad 032829912617594508110/6243022310680637),\\
P_4 &= (-8857111031966280148983670369824404 60/418008125605759441, 5810099\\
&\qquad 56292043808342474664202960105645965798704050 8170/2702570837144118\\
&\qquad 45345707239),\\
P_5 &= (2310627833438618566207271440660/1518703775449, 244662015713267131 10\\
&\qquad 135052718307507812214184590/1871585228601003293),\\
P_6 &= (637984027011974650607003560/91718929, 618677927305924739906748 17890\\
&\qquad 00045078390/878392183033),\\
P_7 &= (-27871641836820690309740/2809, 1806199110727433199159170522308910/\\
&\qquad 148877),\\
P_8 &= (883414680732734546357429746 0/2255965009, 559250800133575059743294 15\\
&\qquad 0493626041731190/107151570032473),\\
P_9 &= (1358304570443828210036870576518625140/168942036456899281, 827898920\\
&\qquad 114464004948399788286383863554398242895941130/694395003794405730 00\\
&\qquad 500071),\\
P_{10} &= (1694354547857797725807403203760/7739952529, 22036032510063005220899\\
&\qquad 211362320831708782344 90/680937803643833),\\
P_{11} &= (15414353863073881481628313395478800508333445992849286812582722 7071\\
&\qquad 42713825223124/5430509537446180903039266616321573192062683481391 60\\
&\qquad 177767049, 5770301719524027190764073427701601361848088102472911 5224\\
&\qquad 151945894986238427125846869887651421936528580719895231543107906/400\\
&\qquad 18505995529089955912553495234850718945202096231776318645918988929 32\\
&\qquad 44718664501739178843).
\end{aligned}$$

The second curve with rank 11 has the parameters $(c, d, m, n) = (108/71, -74/71, 1, 1)$, and can be put in the form

$$\begin{aligned} y^2+xy+y={}&x^3-x^2-6733405851080577415475454221932585499304047x\\ &+4800325455798548390824144090920449266363788590480449836501600119, \end{aligned}$$

with 11 independent rational points

$$\begin{aligned}
P_1 &= (-859040480466684135399409946637/357701569, -570851739448307375446\\
&\qquad 298525772903969793199258/6765209774497),\\
P_2 &= (-86666288433783782765420030182168946493/403989240106987441, -2027\\
&\qquad 5473440123939103498192448687826487891735533319052199446/2567761585\\
&\qquad 12087335734025239),\\
P_3 &= (-7409440973597749452172160724317853/20224187231161, -772709352834\\
&\qquad 8812288313690883962192020793939126647174/90950819347058299091),\\
P_4 &= (-3573159919562444687416081900533/2363029321, -1233150435614496041\\
&\qquad 9570336229779531484558668734/114869218323131),\\
P_5 &= (50457757689930470323988196055818601/239245222129, 113333723486760862\\
&\qquad 45255625501336274920485602295184476/117021297764291383),\\
P_6 &= (753320280758446140552599814044467/192925628289, 16528039595145598724\\
&\qquad 636047412511736643691300872486/84739302490262337),\\
P_7 &= (11399590407313172614495459849827/3813186001, 25128614496449358884398\\
&\qquad 093023284000254237912586/235468048747751),\\
P_8 &= (480337863259420232838048924818817/751461863161, -1792845917173405724\\
&\qquad 5864188117030228724320095652326/651418993856512909),\\
P_9 &= (5955153195237282506441093676187/220789881, -14466844741047487243113\\
&\qquad 690100138781156335681006/3280716841779),\\
P_{10} &= (1375362162769333581779723763/543169, -2527191573457340016030881768\\
&\qquad 3399948364442/400315553),\\
P_{11} &= (21920079230111700414086050318699/4818025, 102627348546574245945365\\
&\qquad 125069231207443139803042/10575564875).
\end{aligned}$$

References

[1] J. Cremona, mwrank program, http://maths.nottingham.ac.uk/personal/jec/ftp/progs/.

[2] A. Dujella, High rank elliptic curves with prescribed torsion http://web.math.pmf.unizg.hr/~duje/tors/tors.html.

[3] A. Dujella, Infinite families of elliptic curves with high rank and prescribed torsion `http://web.math.pmf.unizg.hr/~duje/tors/generic.html`.

[4] A. Dujella, I. Gusić and P. Tadić, The rank and generators of Kihara's elliptic curve with torsion $\mathbb{Z}/4\mathbb{Z}$ over $\mathbb{Q}(t)$, *Proc. Japan Acad. Ser. A Math. Sci.* **91** (2015), 105-109.

[5] N. D. Elkies, $\mathbb{Z}^{28}$ in $E(\mathbb{Q})$, etc., Number Theory Listserver, May 2006.

[6] N. D. Elkies, Three lectures on elliptic surfaces and curves of high rank, Lecture notes, Oberwolfach, 2007, arXiv:0709.2908 `http://arxiv.org/abs/0709.2908`.

[7] I. Gusić and P. Tadić, Injectivity of the specialization homomorphism of elliptic curves, *J. Number Theory*, **148** (2015) 137-152.

[8] S. Kihara, On the rank of elliptic curves with a rational point of order 4, *Proc. Japan Acad. Ser A Math. Sci.* **80** (2004), 26-27.

[9] S. Kihara, On the rank of elliptic curves with a rational point of order 4, II, *Proc. Japan Acad. Ser A Math. Sci.* **80** (2004), 158-159.

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

[11] K. Nagao, An example of elliptic curv over $\mathbb{Q}$ with rank ≥ 20, *Proc. Japan Acad. Ser. A Math. Sci.*, **69** (1993), 291-293.

[12] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

[13] Sage software, *Version 4.5.3*, `http://www.sagemath.org`.