SOME DATA ON TORSION SUBGROUPS OF ELLIPTIC CURVES

JAVIER FERNANDEZ

A well known theorem of B. Mazur [1] states that the only possible groups that appear as torsion subgroups of elliptic curves over $\mathbb{Q}$ are of the form

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

where $\mathbb{Z}_d = \mathbb{Z}/(d\mathbb{Z})$ or

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \text{ for } d = 2, 4, 6, 8.$$

Table 1 shows, for each possible group, an elliptic curve that realizes the group, as well as a set of generators. All curves come from [2], Exercise 2.12.

Table 2 shows the frequency of each group over different regions of the space of elliptic curves. Two realizations of the elliptic curves are used. The usual Weierstrass form

$$y^2 = x^3 + ax^2 + bx + c, \tag{1}$$

and the reduced minimal model form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \text{ with } a_1, a_3 \in \{0, 1\},\ a_2 \in \{-1, 0, 1\}. \tag{2}$$

References

1. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).
2. Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

E-mail address: jfernand@math.utah.edu

Department of Mathematics, University of Utah, Salt Lake City, UT 84112

[1]Using the Weierstrass form (1) with $a, b, c \in [-100, 100]$.

[2]Using the Weierstrass form (1) with $a, b, c \in [-200, 200]$.

[3]Using the reduced minimal form (2) with $a_4 \in [-400, 400]$ and $a_6 \in [-2000, 2000]$.

[4]Based on the reduced minimal form (2) with $a_4 \in [-2000, 2000]$ and $a_6 \in [-10000, 10000]$, but only torsion groups of cardinality at least 9 are considered. The other groups are shown as *NC* (Not Computed) in the table.

group	curve	Weierstrass form[a]	generator(s)[b]	discriminant
$\mathbb{Z}_1$	$y^2 = x^3 - 2$	–	∞	$-2^2 3^3$
$\mathbb{Z}_2$	$y^2 = x^3 + 8$	–	$(-2, 0)$	$-2^6 3^3$
$\mathbb{Z}_3$	$y^2 = x^3 + 4$	–	$(0, 2)$	$-2^4 3^3$
$\mathbb{Z}_4$	$y^2 = x^3 + 4x$	–	$(2, 4)$	-2^8
$\mathbb{Z}_5$	$y^2 - y = x^3 - x^2$	$y^2 = x^3 - 4x^2 + 16$	$(4, 4)$	$-2^8 11^1$
$\mathbb{Z}_6$	$y^2 = x^3 + 1$	–	$(2, 3)$	-3^3
$\mathbb{Z}_7$	$y^2 = x^3 - 43x + 166$	–	$(3, 8)$	$-2^{15} 13^1$
$\mathbb{Z}_8$	$y^2 + 7xy = x^3 + 16x$	$y^2 = x^3 + 49x^2 + 256x$	$(-8, 24)$	$2^{16} 3^4 17^1$
$\mathbb{Z}_9$	$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$y^2 = x^3 - 3x^2 - 216x + 1872$	$(12, 24)$	$-2^{17} 3^5$
$\mathbb{Z}_{10}$	$y^2 + xy = x^3 - 45x + 81$	$y^2 = x^3 + x^2 - 720x + 5184$	$(0, 72)$	$-2^{18} 3^5 11^1$
$\mathbb{Z}_{12}$	$y^2 + 43xy - 210y = x^3 - 210x^2$	$y^2 = x^3 + 1009x^2 - 72240x + 705600$	$(0, 840)$	$2^{20} 3^6 5^3 7^4 13^1$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	$y^2 = x^3 - 4x$	–	$(2, 0), (-2, 0)$	2^8
$\mathbb{Z}_4 \times \mathbb{Z}_2$	$y^2 + xy - 5y = x^3 - 5x^2$	$y^2 = x^3 - 19x^2 - 40x + 400$	$(0, 20), (4, 0)$	$2^8 3^4 5^4$
$\mathbb{Z}_6 \times \mathbb{Z}_2$	$y^2 + 5xy - 6y = x^3 - 3x^2$	$y^2 = x^3 + 13x^2 - 240x + 576$	$(48, 360), (3, 0)$	$2^{10} 3^6 5^2$
$\mathbb{Z}_8 \times \mathbb{Z}_2$	$y^2 + 17xy - 120y = x^3 - 60x^2$	$y^2 = x^3 + 49x^2 - 16320x + 230400$	$(960, 30240), (15, 0)$	$2^{16} 3^8 5^4 7^2$

TABLE 1. Torsion Groups

[a] If the curve is already given in Weiertrass form we just put –

[b] These are points on the curve in Weierstrass form (1)

group	frequency			
	W I[1]	W II[2]	M I[3]	M II[4]
$\mathbb{Z}_1$	0.9817	0.9907113	0.9968541	NC
$\mathbb{Z}_2$	0.0177	0.0090987	0.0030424	NC
$\mathbb{Z}_3$	0.00018	$6.177\,10^{-5}$	$5.819\,10^{-5}$	NC
$\mathbb{Z}_4$	$8.8\,10^{-5}$	$2.551\,10^{-5}$	$1.248\,10^{-5}$	NC
$\mathbb{Z}_5$	$3.8\,10^{-6}$	$8.594\,10^{-7}$	$1.378\,10^{-6}$	NC
$\mathbb{Z}_6$	$5.0\,10^{-7}$	$5.625\,10^{-6}$	$2.730\,10^{-6}$	NC
$\mathbb{Z}_7$	$5.0\,10^{-7}$	$1.406\,10^{-7}$	$1.560\,10^{-7}$	NC
$\mathbb{Z}_8$	$6.2\,10^{-7}$	$2.188\,10^{-7}$	$1.820\,10^{-7}$	NC
$\mathbb{Z}_9$	0	0	$5.201\,10^{-8}$	$2.08\,10^{-9}$
$\mathbb{Z}_{10}$	0	0	$7.801\,10^{-8}$	$5.21\,10^{-9}$
$\mathbb{Z}_{12}$	0	0	$2.600\,10^{-8}$	$1.04\,10^{-9}$
$\mathbb{Z}_2 \times \mathbb{Z}_2$	0.00029	$9.363\,10^{-5}$	$2.741\,10^{-5}$	NC
$\mathbb{Z}_4 \times \mathbb{Z}_2$	$8.5\,10^{-6}$	$2.078\,10^{-6}$	$7.021\,10^{-7}$	NC
$\mathbb{Z}_6 \times \mathbb{Z}_2$	0	$1.094\,10^{-7}$	$5.201\,10^{-8}$	$4.17\,10^{-9}$
$\mathbb{Z}_8 \times \mathbb{Z}_2$	0	0	0	$1.04\,10^{-9}$

TABLE 2. Torsion group frequencies