Week 13. Elliptic Curves over $\mathbb{Q}$, application to ECM

Aurore Guillevic

Aarhus University

May 3 & 5, 2022

This document at
`https://members.loria.fr/AGuillevic/files/Enseignements/AU/lectures/lecture13A.pdf`

1. Theorems on the structure of $E(\mathbb{Q})$

Theorem 1 (Mordell–Weil (Th. 8.17 in Washington's book and §8.4))**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. The group of rational points $E(\mathbb{Q})$ is isomorphic to*

$$E_{\mathrm{tor}}(\mathbb{Q}) \times E_\infty$$

where $E_{\mathrm{tor}}(\mathbb{Q})$ is the group of points of finite order (torsion points) and E_∞ is the group of points of infinite order.

The group E_∞ is isomorphic to $\mathbb{Z}^r$ where r is the rank *of the curve, the rank is a positive integer $r \geq 0$.*

On can find a list of records of elliptic curves with high rank at

- History of elliptic curves rank records:
  `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`
- High rank elliptic curves with prescribed torsion:
  `https://web.math.pmf.unizg.hr/~duje/tors/tors.html`

In practice, it is hard to compute r, and we don't even know if r is bounded. The maximum rank known today is $r = 28$ (Elkies).

Theorem 2 (B. Mazur (Th. 8.11 in Washington's book))**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. The possible torsion groups E_{tor} are*

$$\begin{cases} \mathbb{Z}/m\mathbb{Z},\ m \in \{1,2,\ldots,10\} \cup \{12\} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z},\ m \in \{1,2,3,4\} \end{cases} . \tag{1}$$

Example 1. We saw in Hand-in 1 that elliptic curves in Montgomery form $By^2 = x^3 + Ax^2 + x$ have a subgroup of order 4, isomorphic either to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It holds over $\mathbb{Q}$ and a finite field $\mathbb{F}_p$.

Theorem 3 (Lutz–Nagell (Th. 8.7 in Washington's book))**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ by an equation $y^2 = x^3 + ax + b$ with integer coefficients ($a, b \in \mathbb{Z}$). Let $P(x, y) \in E(\mathbb{Q})$. Suppose P has finite order. Then $x, y \in \mathbb{Z}$. If $y \neq 0$ then*

$$y \mid 4a^3 + 27b^2 \ .$$

Theorem 4 (Reduction of a curve $E(\mathbb{Q})$ modulo a prime p (Th. 8.9 in Washington's book))**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ by an equation $y^2 = x^3 + ax + b$ with integer coefficients ($a, b \in \mathbb{Z}$) and discriminant $\Delta = 4a^3 + 27b^2$. Let $E_{\mathrm{tor}}(\mathbb{Q})$ be the group of torsion points.*

Let p be a prime intger, denote E_p the curve obtained by reducing modulo p the coefficients a, b. Denote

$$\begin{array}{rcl} \rho_p \colon E_{\mathrm{tor}}(\mathbb{Q}) & \to & E_p(\mathbb{F}_p) \\ Q(x,y) & \mapsto & \begin{cases} (x \bmod p, y \bmod p) & \textit{if } Q = (x,y) \neq \infty \\ \mathcal{O} & \textit{if } Q = \infty \end{cases} \end{array}$$

If $p \nmid 2\Delta$, ρ_p induces an isomorphism of groups between $E_{\mathrm{tor}}(\mathbb{Q})$ and a subgroup of $E_p(\mathbb{F}_p)$.

2. Examples

Exercise 1. Let $E/\mathbb{Q}\colon y^2 = x^3 - 43x + 166$.

(1) Check that E is an elliptic curve and $P(3,8) \in E(\mathbb{Q})$.
(2) Calculate $2P, 4P, 8P$ (with SageMath if you prefer).
(3) Deduce the order of P.

Exercise 2. Let $E/\mathbb{Q}\colon y^2 = x^3 + 3$.

(1) Calculate Δ the curve discriminant
(2) Find $\#E_5(\mathbb{F}_5)$, $\#E_7(\mathbb{F}_7)$
(3) What is the order of $(1,2) \in E(\mathbb{Q})$?

Exercise 3. Let $E\colon y^2 = x^3 + x/\mathbb{Q}$. Determine the torsion points with Lutz–Nagell theorem. Which other theorem can we use and how?

Exercise 4. Let $E\colon y^2 = x^3 - x/\mathbb{Q}$. Determine the torsion points with Lutz–Nagell theorem. Compute $\#E_3(\mathbb{F}_3)$ and $\#E_7(\mathbb{F}_7)$.

Solution 1.

```
E = EllipticCurve(QQ, [-43, 166])
P = E(3,8)
2*P
4*P
8*P
4*(-43)^3 + 27*166^2
(4*(-43)^3 + 27*166^2).factor()
[(x^3-x+5) % 7 for x in range(7)]
[y^2 % 7 for y in range(7)]
E.torsion_subgroup()
E3 = E.change_ring(GF(3)); E3.order() # this is 7
E5 = E.change_ring(GF(5)); E5.order() # this is 7 again
E11 = E.change_ring(GF(11)); E11.order() # this is 14=2*7
```

Solution 2.

(1) $\Delta = 4a^3 + 27b^2 = 27 \cdot 3^2 = 3^5 = 243$.

(2) $\#E_5(\mathbb{F}_5) = 6$, $\#E_7(\mathbb{F}_7) = 13$ hence $E(\mathbb{Q})$ has no torsion point except ∞.

ρ_p induces an isomorphism $E_{\mathrm{tor}}(\mathbb{Q}) \to^{\sim}$ a subgroup of $E_p(\mathbb{F}_p) \forall p,\ p \nmid 2\Delta$

$\implies \#E_{\mathrm{tor}}(\mathbb{Q}) \mid \#E(\mathbb{F}_p) \forall p,\ p \nmid 2\Delta$.
Applying this result to $p = 5, p = 7$:

$$\begin{cases} \#E_{\mathrm{tor}}(\mathbb{Q}) \mid \#E_5(\mathbb{F}_5) = 6 \\ \#E_{\mathrm{tor}}(\mathbb{Q}) \mid \#E_7(\mathbb{F}_7) = 13 \end{cases} \implies \#E_{\mathrm{tor}}(\mathbb{Q}) \mid \gcd(6, 13) = 1$$

$\implies \#E_{\mathrm{tor}}(\mathbb{Q}) = 1$ and $E_{\mathrm{tor}}(\mathbb{Q}) = \{\infty\}$.

(3) $(1, 2) \in E(\mathbb{Q})$ has infinite order. One can notice that $2(1, 2) = (-23/16, -11/64)$ has non-integer coefficients.

```
E = EllipticCurve(QQ, [0, 3])
[(x^3+3) % 5 for x in range(5)]
[y^2 % 5 for y in range(5)]
[(x^3+3) % 7 for x in range(7)]
[y^2 % 7 for y in range(7)]
E5 = E.change_ring(GF(5)); E5.order()
E7 = E.change_ring(GF(7)); E7.order()
E.torsion_points()
P = E(1,2)
2*P
```

Solution 3. Let $E\colon y^2 = x^3 + x/\mathbb{Q}$. Let $P(x, y)$ be a point of finite order of E (a torsion point). Then Lutz–Nagell ensures that P has integer coordinates $(x, y) \in \mathbb{Z}^2$, and moreover, either $y = 0$ (2-torsion point) or $y \mid \Delta = 4a^3 + 27b^2$.

(1) Is there a point with $y = 0$? Let's solve $y^2 = 0 = x^3 + x$. One obtains $x(x^2 + 1) = 0$ hence $x = 0$ because $x^2 + 1 = 0$ has no solution in $\mathbb{Q}$. The 2-torsion points of $E(\mathbb{Q})$ are $\{\infty, (0, 0)\}$.

(2) $\Delta = 4$, is there a point with $y \mid 4$? The possibilities are $y \in \{\pm 1, \pm 2, \pm 4\}$. In these cases, $y^2 \in \{1, 4, 16\}$. Is there a solution x in $\mathbb{Z}$ of $x^3 + x \in \{1, 4, 16\}$?

x	0	1	2	3	4	5	6	...
$x^3 + x$	0	2	10	30	68	130	222	...

The function $x \mapsto x^3 + x$ is strictly increasing for all $x \geq 1$, hence there is no solution to the equation.

The torsion points are $E_{\mathrm{tor}} = \{(0, 0), \infty\}$.

```
[x^3+x for x in range(7)]
E = EllipticCurve(QQ, [1,0])
E.torsion_points()
E.torsion_subgroup()
E3 = E.change_ring(GF(3)); E3.order()
E5 = E.change_ring(GF(5)); E5.order()
E7 = E.change_ring(GF(7)); E7.order()
```

Solution 4. Let $E\colon y^2 = x^3 - x/\mathbb{Q}$. Let $P(x,y)$ be a point of finite order of E (a torsion point). Then Lutz–Nagell ensures that P has integer coordinates $(x,y) \in \mathbb{Z}^2$, and moreover, either $y = 0$ (2-torsion point) or $y \mid \Delta = 4a^3 + 27b^2$.

(1) Is there a point with $y = 0$? Let's solve $y^2 = 0 = x^3 - x$. One obtains $x(x^2-1) = 0$ hence $x \in \{0, 1, -1\}$ and the 2-torsion points of $E(\mathbb{Q})$ are $\{\infty, (0,0), (1,0), (-1,0)\}$.

(2) $\Delta = -4$, is there a point with $y \mid -4$? The possibilities are $y \in \{\pm 1, \pm 2, \pm 4\}$. In these cases, $y^2 \in \{1, 4, 16\}$. Is there a solution x in $\mathbb{Z}$ of $x^3 - x \in \{1, 4, 16\}$?

x	0	1	2	3	4	5	6	$\dots$
$x^3 - x$	0	0	6	24	60	120	210	$\dots$

The function $x \mapsto x^3 - x$ is strictly increasing for all $x \geq 1$, hence there is no solution to the equation.

The torsion points are $E_{\text{tor}} = \{(0,0), (-1,0), (1,0), \infty\}$.

```
[x^3-x for x in range(7)]
E = EllipticCurve(QQ, [-1,0])
E.torsion_points()
E.torsion_subgroup()
E3 = E.change_ring(GF(3)); E3.order()
E5 = E.change_ring(GF(5)); E5.order()
E7 = E.change_ring(GF(7)); E7.order()
```

3. Curves of prescribed torsion for ECM

3.1. **Montgomery and Brent–Suyama curves for ECM.** The following in Brent-Suyama parameterisation of curves is quoted from [4, §4.6.2].

Montgomery parameterisation of curves is

$$BY^2Z = X^3 + AX^2Z + XZ^2 \tag{2}$$

In a letter to Richard P. Brent on October 1985, Hiromi Suyama showed that curves in Montgomery form over $\mathbb{F}_p$ always have group order divisible by 4, and also showed a parametrization that ensures that the group order is divisible by 12, which Brent describes in [3]. This parametrization generates an infinite family of curves over $\mathbb{Q}$ which can be used to generate a large number of distinct curves modulo N. For a given integer parameter $\sigma \neq 0, 1, 3, 5$, let

$$u = \sigma^2 - 5,\ v = 4\sigma, \quad X_0 = u^3,\ Z_0 = v^3, \text{ and } A = \frac{(v-u)^3(3u+v)}{4u^3v} - 2\ . \tag{3}$$

Then the point $(X_0 : Z_0)$ is on the curve (2) with parameter A. The same parametrization is used by GMP-ECM [9, §1] and Prime95 [8].

Montgomery showed in his thesis [7] how to choose curves of the form (2) such that the curve over $\mathbb{Q}$ has a torsion subgroup of order 12 or 16, leading to group order divisible by 12 or 16, respectively, when the curve is mapped to $\mathbb{F}_p$ for almost all p. For curves with rational torsion group of order 12 he uses

$$t^2 = \frac{u^2 - 12}{4u},\ a = \frac{t^2 - 1}{t^2 + 3}, \quad X_0 = 3a^2{+}1,\ Z_0 = 4a \text{ and } A = \frac{-3a^4 - 6a^2 + 1}{4a^3}\ , \tag{4}$$

where $u^3 - 12u$ is a rational square. The solutions of $v^2 = u^3 - 12u$ form an elliptic curve of rank 1 and 2-torsion over $\mathbb{Q}$, with generator $(-2, 4)$ and 2-torsion point $(0, 0)$. However, adding the torsion point or not seems to produce isomorphic curves for ECM, so we ignore it. Hence for a given integer parameter $k > 1$ we can compute suitable values of u and v by computing $[k](-2, 4)$ on $v^2 = u^3 - 12u$. We can then let $t = v/(2u)$. This produces an infinite family of curves over $\mathbb{Q}$.

Curves with torsion 16 and positive rank over $\mathbb{Q}$ are more difficult to generate, see [67, 6.2] for details. We currently implement only one such curve with $X_0 = 8$, $Z_0 = 15$, and $A = 54721/14400$.

These parametrizations ensure that the group order is divisible by 12 or 16, respectively, but the resulting group order of the curve over $\mathbb{F}_p$ does not behave like an integer chosen uniformly at random from the integers that are multiple of 12 or 16, repsectively, in the Hasse interval around p. In particular, the average valuation of 2 in the group order for curves with rational torsion 12 is 11/3, slightly higher than 10/3 for curves in Brent–Suyama parametrization (which have rational torsion 6), making them somewhat more likely to find factors. The divisibility properties will be examined in more detail in [4, Chapter 5].

Very small σ-values for the Brent–Suyama parametrization lead to curves with simple rationals for the point coordinate and curve parameter, and very small k-values for Montgomery's parametrization for curves with rational torsion 12 lead to simple rationals for a, see Table 1. These rationals can be mapped to $\mathbb{Z}/N\mathbb{Z}$ easily, as the denominators are highly composite integers so that the required divisions modulo N can be done by the methods of [4, Section 4.3.4] and a few multiplications.

When factoring cofactors after the sieving step of NFS into large primes, only very few curves are required on average since the primes to be found are relatively small, and with an early-abort strategy, only the first few curves work on larger composites where arithmetic is more expensive. In spite of the small number of curves with such simple rationals as curve parameters, it is useful to implement them as special ases.

σ	X_0	Z_0	A
2	-1	512	$-3645/32$
4	1331	4096	$6125/85184$

k	a	$X0$	$Z0$	A
2	$-3/13$	$196/169$	$-12/13$	$-4798/351$
3	$28/37$	$3721/1369$	$112/37$	$-6409583/3248896$

Table 1. Some elliptic curves chosen by the Brent–Suyama parametrization with group order divisible by 12, and by Montgomery's parametrization with rational torsion group of order 12.

3.2. **More on Suyama curves.** [2, Chapter 3]

3.3. **Good curves for ECM in Edwards form.** An alternative to Montgomery form of elliptic curves: Edwards curves https://eecm.cr.yp.to/ https://eecm.cr.yp.to/goodcurves.html

References

[1] A. O. L. Atkin and F. Morain. Finding suitable curves for the elliptic curve method of factorization. *Mathematics of Computation*, 60(201):399–405, 1993.

[2] Razvan Barbulescu. *Algorithmes de logarithmes discrets dans les corps finis.* thèse de doctorat, Université de Lorraine, Nancy, France, 2013. https://tel.archives-ouvertes.fr/tel-00925228.

[3] R. P. Brent, R. E. Crandall, K. Dilcher, and C. Van Halewyn. Three new factors of fermat numbers. *Math. Comp.*, 69(231):1297–1304, 2000. https://doi.org/10.1090/S0025-5718-00-01207-2.

[4] Alexander Kruppa. *Speeding up Integer Multiplication and Factorization.* thèse de doctorat, Université Henri Poincaré - Nancy I, Nancy, France, January 2010. https://tel.archives-ouvertes.fr/tel-01748662v3.

[5] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. volume 33, pages 193–237, 1976.

[6] B. Mazur. Rational points on modular curves. In Jean-Pierre Serre and Don Bernard Zagier, editors, *Modular Functions of One Variable V*, volume 601 of *Lecture Notes in Math.*, pages 107–148, University of Bonn, 1977. Springer Berlin Heidelberg. https://link.springer.com/content/pdf/10.1007/BFb0063947.pdf.

[7] Peter L. Montgomery. *An FFT Extension to the Elliptic Curve Method of Factorization.* Phd thesis, UCLA, 1992.

[8] George Woltman and Scott Kurowski. The great internet mersenne prime search. https://www.mersenne.org/.

[9] Paul Zimmermann and Bruce Dodson. 20 years of ECM. In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, volume 4076 of *Lecture Notes in Computer Science*, pages 525–542. Springer, 2006. https://members.loria.fr/PZimmermann/papers/40760525.pdf.