Elliptic curves, number theory and cryptography

6. handin – Elliptic curves over $\mathbb{Q}$, Nagell–Lutz theorem

Aurore Guillevic

Aarhus University

Mai 6, 2022

Due date: May 20, 4pm GMT+2 (16:00 Aarhus time)

Remember that 4 approved hand-ins out of 6 are required to take the final exam, according to the rule at https://www.kursuskatalog.au.dk/en/course/112277/Elliptic-Curves-Number-Theory-and-Cryptography.

Prerequisites for examination participation. *A participant may only take the final examination if he or she has handed in, and had approved, at least 4 out of 6 set exercises.*

1. Nagell–Lutz theorem

Question 1. Let E be an elliptic curve defined over $\mathbb{Q}$ by an equation

$$E\colon y^2 = x^3 + ax^2 + bx + c$$

where a, b, c are rational coefficients (in $\mathbb{Q}$). Which change of variables (this is an isomorphism) allows to obtain an isomorphic curve E' with an equation of integer coefficients $a', b', c' \in \mathbb{Z}$?

Theorem 1 (Reduction of a curve $E(\mathbb{Q})$ modulo a prime p (general version of Th. 8.9 in Washington's book))**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ by a generalized Weierstrass equation*

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

with integer coefficients ($a_i \in \mathbb{Z}$) and discriminant Δ. Let $E_{\mathrm{tor}}(\mathbb{Q})$ be the group of torsion points.

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

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

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

Remark 2. In Washington's book, Theorem 8.9, one requires $p \nmid 2\Delta$ because the square at the left for $y^2 + a_1xy + a_3y$ was completed as

$$y^2 + a_1xy + a_3y = \left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 - \frac{a_1^2}{4}x^2 - \frac{a_1a_3}{2}x - \frac{a_3^2}{4}$$

(from Washington's book page 10, §2.1) and to obtain this shorter equation (cancelling a_1 and a_3), a division by 2 is required. Therefore a reduction modulo 2 of a curve $Y^2 = X^3 + a_2X^2 + a_4X + a_6$ is not allowed as the curve would be singular.

Question 2. This question is about finding the torsion subgroup $E_{\mathrm{tor}}(\mathbb{Q})$ of the elliptic curve

$$E\colon y^2 - y = x^3 - x^2\ .$$

The discriminant of the curve is 11.

(1) Consider the curve modulo 2, and give the points on the curve with coordinates in $\mathbb{F}_2$. What is the order of the curve reduced modulo 2 (remember $\mathcal{O}$)? Is the Hasse bound satisfied?
(2) Do the same modulo $p = 3$.
(3) Conjecture a possibility for the order of $E_{\mathrm{tor}}(\mathbb{Q})$.
(4) What is the order of the point $P(0,0)$ on the curve?
Hint: for example you can compute multiples $2P, 4P, \ldots$ until you recognize something, or you get $\mathcal{O}$.
Hint: doubling formulas on a curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ are

$$\lambda = \frac{2a_2x_1 + 3x_1^2 - a_1y_1 + a_4}{a_1x_1 + a_3 + 2y_1},\ x_{2P} = \lambda(\lambda + a_1) - a_2 - 2x_1,\ y_{2P} = \lambda(x_1 - x_{2P}) - a_1x_{2P} - y_1 - a_3\ .$$

Addition formulas for $P(x_1, y_1), Q(x_2, y_2)$ are

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ x_{P+Q} = \lambda(a_1 + \lambda) - a_2 - x_1 - x_2,\ y_{P+Q} = \lambda(x_1 - x_{P+Q}) - a_1 x_{P+Q} - y_1 - a_3 \ .$$

Negation is

$$-P(x_1, y_1) = (x_1, -a_1 x_1 - y_1 - a_3) \ .$$

(5) Use the general version of the reduction theorem given in Th. 1 with $\Delta = 11$, $p = 2$, $p = 3$ and the answer about $P(0,0)$ to conclude about $E_{\mathrm{tor}}(\mathbb{Q})$.

Theorem 3 (Strong version of Nagell–Lutz theorem.)**.** *Let $E\colon y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x)$ an elliptic curve defined over $\mathbb{Q}$, with integer coefficients a_i, and let D be discriminant of the cubic polynomial $f(x)$,*

$$\Delta(f) = -4a_2^3a_6 + a_2^2a_4^2 + 18a_2a_4a_6 - 4a_4^3 - 27a_6^2 \ .$$

Let $P(x, y)$ be a rational point of finite order. Then x, y are integers, and either $y = 0$ (in this case P has order 2), or y^2 divides D (with y^2 instead of y, note that $y^2 \mid \Delta \implies y \mid \Delta$).

Question 3. Let $E\colon y^2 = x^3 + 1$ be an elliptic curve over $\mathbb{Q}$.

(1) What is the discriminant Δ of the curve?
(2) Use the strong version of the Nagell–Lutz theorem (Th. 3) to deduce the torsion points of $E(\mathbb{Q})$ (consider the solutions to $y = 0$, and the solutions to $y^2 \mid \Delta$).
(3) Deduce the structure of $E_{\mathrm{tor}}(\mathbb{Q})$.

Question 4. Let $E\colon y^2 = x^3 + p^2$ be an elliptic curve over $\mathbb{Q}$, and p a prime. Note that this exercise is given in Wahsington's book for $p = 2$ (Exercise 8.1).

(1) What is the discriminant Δ of the curve?
(2) Use the strong version of the Nagell–Lutz theorem (Th. 3) to deduce the torsion points of $E(\mathbb{Q})$ (consider the solutions to $y = 0$, and the solutions to $y^2 \mid \Delta$).
(3) Deduce the structure of $E_{\mathrm{tor}}(\mathbb{Q})$.

Question 5 (Optional)**.** Let $E\colon y^2 = x^3 + p^2$ be an elliptic curve over $\mathbb{Q}$, and p a prime.

A generalization for p directly with the Strong Nagell-Lutz theorem might be technical. As hint on the expected answer, the order of the curve reduced modulo 5 is given, assuming that $p \neq 5$. The possible values of p^2 mod 5 are $1, 4$. If $p^2 = 1$ mod 5 we mark $\circ$, otherwise $p^2 = 4$ mod 5 and we mark $\times$. In both cases, we obtain $\#E_5(\mathbb{F}_5) = 6$.

		x	0	1	2	3	4
y	y^2	$x^3 + p^2$	p^2	$1 + p^2$	$3 + p^2$	$4 + p^2$	
0	0			$\times$			$\circ$
1	1		$\circ$			$\times$	
2	4		$\times$		$\circ$		
3	4		$\times$		$\circ$		
4	1		$\circ$			$\times$	

(1) Consider the curve over $\mathbb{Q}$. Does the curve has points of order 2 (with $y = 0$)?
(2) Combine $\#E_5(\mathbb{F}_5) = 6$ and your answer to the previous question to narrow the possible orders of $\#E_{\mathrm{tor}}(\mathbb{Q})$.
(3) Check that $P(0, p)$ is on the curve. What is the order of P?
(4) Deduce the structure of $E_{\mathrm{tor}}(\mathbb{Q})$.

Question 6 (**Optional**, this one is a bit long)**.** Let

$$E\colon y^2 = x^3 - (2a - 1)x^2 + a^2x$$

an elliptic curve defined over $\mathbb{Q}$, and $a \in \mathbb{Z}$. The aim is to show that this curve has always at least four torsion points. We do not assume anything about a except that is satisfies the required conditions so that E is non-singular.

(1) Compute the discriminant of the curve with the formula

$$E_{2,4}\colon y^2 = x^3 + a_2x^2 + a_4x, \quad \Delta = a_4^2(-a_2^2 + 4a_4) \ .$$

(2) What are the conditions on a so that Δ is non-zero and E is an elliptic curve?
(3) Check that $P(a, a)$ is a point on the curve.

(4) What is the order of the point $P(a, a)$?
Hint: the formulas for doubling a point $P(x_1, y_1)$ on a curve $y^2 = x^3 + a_2x^2 + a_4x$ are

$$\lambda = \frac{f'(x)}{2y}(x_1, y_1) = \frac{3x_1^2 + 2a_2x_1 + a_4}{2y_1}, x_{2P} = \lambda^2 - 2x_1 - a_2, y_{2P} = \lambda(x_1 - x_{2P}) - y_1 \ .$$

Feel free to do it directly with SageMath, or at least check your result with SageMath.

(5) Assume that $1 - 4a$ is not a square (and note that $4a - 1$ cannot be a square). Assume that any additional condition on a is **not** satisfied.
Let $P(x, y)$ a point on $E(\mathbb{Q})$ of finite order, according to the strong version of the Nagell–Lutz theorem, what are the possibilities for y?

(6) From your previous answer, deduce the torsion subgroup of $E(\mathbb{Q})$ in the general case of a (with only the assumption of 2). You can use SageMath to check that there is no solution in most of the cases (try to factor the cubic polynomial in x, a, if it has no root, consider that there is no solution).