Elliptic curves, number theory and cryptography

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

Aurore Guillevic

Aarhus University

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 $a', b', c' \in \mathbb{Z}$?

Solution 1. An isomorphism has the form $(x, y) \mapsto (u^2x, u^3y)$ for some non-zero u and the isomorphic curve is given by the equation $y'^2 = x'^3 + au^2x'^2 + bu^4x' + cu^6$. Let us start from the equation of E:

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

Multiplying the eq. by u^6 and then simplifying gives

$$\begin{array}{rcl} u^6y^2 & = & u^6x^3 + au^6x^2 + bu^6x + cu^6 \\ (u^3y)^2 & = & (u^2x)^3 + au^2(u^2x)^2 + bu^4(u^2x) + cu^6 \end{array}$$

Finally setting $x' = u^2x$ and $y' = u^3y$ one obtains the equation of E':

$$E'\colon y'^2 = x'^3 + au^2x'^2 + bu^4x' + cu^6\ .$$

Any choice of $u \neq 0$ such that $au^2, bu^4, cu^6 \in \mathbb{Z}$ is correct. For example $u = \mathrm{lcm}(\mathrm{denom}(a), \mathrm{denom}(b), \mathrm{denom}(c))$ where denom denotes the denominator.

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 the projection ρ_p

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

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 $E_{\text{tor}}(\mathbb{Q})$ of the elliptic curve

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

The discriminant of the curve is $\Delta = 11$.

(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 $E_{\text{tor}}(\mathbb{Q})$.

(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

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},\ x_{P+Q} = \lambda(a_1 + \lambda) - a_2 - x_1 - x_2,\ y_{P+Q} = \lambda(x_1 - x_{P+Q}) - a_1x_{P+Q} - y_1 - a_3 \ .$$

Negation is

$$-P(x_1, y_1) = (x_1, -a_1x_1 - y_1 - a_3) \ .$$

(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 $E_{\text{tor}}(\mathbb{Q})$.

Solution 2.

(1) Reducing the curve modulo 2, $E_2\colon y^2 + y = x^3 + x^2/\mathbb{F}_2 \iff y(y+1) = x^2(x+1)$ has points $\{(0,0), (0,1), (1,0), (1,1), \mathcal{O}\}$ that is, $\#E_2(\mathbb{F}_2) = 5 = 2 + 1 - (-2)$ and the trace of the curve is $t = -2$. The Hasse bound says $|t| \leq 2\sqrt{p}$, with $t = 2$ and $p = 2$, because $\sqrt{2} > 1$, yes it is satisfied.

(2) For $p = 3$, $E_3\colon y^2 - y = x^3 - x^2/\mathbb{F}_3 \iff y(y-1) = x^2(x-1)$ has points $\{(0,0), (0,1), (1,0), (1,1), \mathcal{O}\}$ that is, $\#E_3(\mathbb{F}_3) = 5 = 3 + 1 - (-1)$ and the trace of the curve is $t = -1$. The Hasse bound is satisfied.

(3) According to the reduction modulo p theorem, we should have

$$\#E_{\text{tor}}(\mathbb{Q}) \text{ divides } \#E_2(\mathbb{F}_2) = 5,\ \#E_{\text{tor}}(\mathbb{Q}) \text{ divides } \#E_3(\mathbb{F}_3) = 5$$

hence $\#E_{\text{tor}}(\mathbb{Q}) = 5$ or $\#E_{\text{tor}}(\mathbb{Q}) = 1$. In the first case, we need to find a point of order 5 to confirm the conjecture, in the second case, it would mean that $E_{\text{tor}}(\mathbb{Q}) = \{\mathcal{O}\}$ and to confirm that, we would need to find another prime $p \neq 2, 3$ such that the reduction mod p gives a curve $E_p(\mathbb{F}_p)$ that has no subgroup of order 5.

(4) The order of $P(0,0)$ is exactly 5. We obtain $2P = (1,1)$, $3P = (1,0)$, $4P = (0,1)$ and we recognize $-P$ hence $4P = -P \implies 5P = \mathcal{O}$ and because $P \neq \mathcal{O}$, we conclude that P has order 5. Indeed, $5P = 4P + P$ gives $\mathcal{O}$.

(5) We conclude that $\#E_{\text{tor}}(\mathbb{Q}) = 5$ and a generator is P.

Some SageMath code to check the answers:

```
E = EllipticCurve(QQ, [0,-1,-1,0,0])
E
E2 = E.change_ring(GF(2))
E2.order()
E3 = E.change_ring(GF(3))
E3.order()
P = E((0,0))
2*P
3*P
4*P
5*P
```

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 $E_{\mathrm{tor}}(\mathbb{Q})$.

Solution 3.

(1) The discriminant is $\Delta = 4a^3 + 27b^2 = 27 = 3^3$.
(2) The solutions for y according to the strong Nagell–Lutz theorem are $y = 0$ or $y^2 \mid 3^3$, that is, $y^2 \in \{1, 3^2\}$. For $y = 0$, the solution is $x = -1$, because $x^3+1 = (x-1)(x^2-x+1)$, and $x^2-x+1 = 0$ has no solution in $\mathbb{Q}$. For $y^2 = 3^2$, we solve $3^2 = x^3+1 \iff x^3 = 8$, and $x^3-8 = (x-2)(x^2+2x+4)$ has the only solution $x = 2$ in $\mathbb{Q}$. For $y^2 = 1$, we solve $x^3 + 1 = 1 \iff x = 0$. The points are $(0, 1), (0, -1)$. Finally the torsion points are $\{\mathcal{O}, (2, 3), (2, -3), (-1, 0), (0, 1), (0, -1)\}$.
(3) first we find the order of $(2, 3)$. It is not 2 as $y = 3 \neq 0$. We double the point: we obtain $\lambda = \frac{3x_1^2}{2y_1} = 12/6 = 2$, $x_2 = \lambda^2 - 2x_1 = 4 - 2 \cdot 2 = 0$, $y_2 = \lambda(x_1 - x_2) - y_1 = 2(2 - 0) - 3 = 1$. We double $(0, 1)$ and obtain $\lambda = 0, x_4 = 0, y_4 = -y_2 = -1$ and $2(0, 1) = (0, -1) = -(0, 1)$ hence $(0, 1)$ has order 3. We conclude that $(2, 3)$ has order 6, and $E_{\mathrm{tor}}(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$.

Question 4. Let $E\colon y^2 = x^3 + p^2$ be an elliptic curve over $\mathbb{Q}$, and p a prime.

(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 $y^2 \mid \Delta$).
Hint: the case $p = 2$ is Example 8.1 in Washington's book. Consider $p = 3$ and $p = 5$.

(3) Deduce the structure of $E_{\mathrm{tor}}(\mathbb{Q})$.

Solution 4.

(1) The discriminant of the curve is $\Delta = 4a^3 + 27b^2 = 27p^4 = 3^3p^4$. For $p = 3$ this is $\Delta = 3^7$, for $p = 5$ this is $\Delta = 3^35^4$.

(2) We solve the solutions of the equation $y = 0$ to obtain the 2-torsion points, and to $y^2 \mid \Delta = 3^3p^4$ to find the other torsion points. For the 2-torsion points, $y = 0 \iff (-x)^3 = p^2$ has no solutions in $\mathbb{Z}$ as p is a prime. For $y^2 \mid 3^3p^4$, the possibilities are $y^2 \in \{3^2, 3^2p^2, 3^2p^4, p^2, p^4, 1\}$. For each of these possibilities, we test if a solution to $y^2 = x^3 + p^2$ is possible.

- $p = 3$, $\Delta = 3^7$ and $y^2 \in \{1, 3^2, 3^4, 3^6\}$.
  - $y^2 = 1$, the eq. is $1 = x^3 + 9 \iff x^3 = -8$, the solutions are $(-2, 1)$ and $(-2, -1)$. These points have infinite order, indeed $[3](-2, 1) = (-629/441, 22870/9261)$ with rational coordinates.
  - $y^2 = 3^2$, the eq. is $9 = x^3 + 9 \iff x^3 = 0$, the solutions are $(0, 3)$ and $(0, -3)$. These points have order 3.
  - $y^2 = 3^4$, the eq. is $81 = x^3 + 9 \iff 72 = x^3$, but $72 = 2^3 \cdot 3^2$, there is no solution.
  - $y^2 = 3^6$, the eq. is $729 - 9 = x^3 \iff 720 = x^3$ but 720 is not a cube, there is no solution.

  Finally, the rational points of finite order for $p = 3$ are $\{(0, 3), (0, -3)\}$, with the point at infinity that makes 3 points, this forms a cyclic subgroup of order 3, and
  $$E_{\mathrm{tor}}(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}\ .$$
- $p = 5$, $\Delta = 3^35^4$ and $y^2 \in \{1, 3^2, 5^2, 3^25^2, 5^4, 3^25^4\}$.
  - $y^2 = 1$, the eq. is $1 = x^3 + 25 \iff x^3 = -24 = -3 \cdot 2^3$ there is no solution in $\mathbb{Z}$ for x.
  - $y^2 = 3^2$, the eq. is $9 = x^3 + 25 \iff -16 = x^3$ but $-16 = -2^4$ is not a cube, there is no solution.
  - $y^2 = 5^2$, the eq. is $5^2 = x^3 + 5^2$, the solutions are $x = 0$, $y = \pm 5$. These points $(0, 5), (0, -5)$ have order 3.
  - $y^2 = 3^25^2$, the eq. is $225 = x^3 + 25 \iff 200 = x^3$, there is no solution in $\mathbb{Z}$.
  - $y^2 = 5^4$, the eq. is $625 = x^3 + 25 \iff x^3 = 600$, there is no solution in $\mathbb{Z}$.
  - $y^2 = 3^25^4$, the eq. is $5625 = x^3 + 25 \iff x^3 = 5600$, there is no solution in $\mathbb{Z}$.

  Finally, the rational points of finite order for $p = 5$ are $\{(0, 5), (0, -5)\}$, with the point at infinity that makes 3 points, this forms a cyclic subgroup of order 3, and
  $$E_{\mathrm{tor}}(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}\ .$$

To generalize the result to any p, we can reduce the curve modulo a prime $q \neq 3, p$ and count the number of points. We already considered $p = 3$ and $p = 5$ above, now assume that p is different from 3 and 5. For example, let us consider $q = 5$ and $p \neq 5$. The possible values of $p^2 \bmod 5$ are $1, 4$. If $p^2 = 1 \bmod 5$ we mark $\circ$, otherwise $p^2 = 4 \bmod 5$ and we mark $\times$. In both cases, we obtain $\#E_5(\mathbb{F}_5) = 6$ (five points defined over $\mathbb{F}_5$, plus the point at infinity that makes 6 points).

$y \bmod 5$ $\downarrow$	$y^2 \bmod 5$ $\downarrow$	0 p^2	1 $1+p^2$	2 $2+p^2$	3 $3+p^2$	4 $4+p^2$	$\leftarrow x \bmod 5$ $\leftarrow x^3+p^2 \bmod 5$
0	0		$\times$			$\circ$	
1	1	$\circ$			$\times$		
2	4	$\times$		$\circ$			
3	4	$\times$		$\circ$			
4	1	$\circ$			$\times$		

From this result and the reduction theorem, $\#E_{\mathrm{tor}}(\mathbb{Q})$ divides 6 as long as $p \neq 5$. It means maybe there are points of order 3 and/or 2. We solve $y = 0$ to obtain the points of order two: $x^3 + p^2 = 0 \iff p^2 = (-x)^3$ has no solutions in $\mathbb{Q}$. Hence there is no point of order two over $\mathbb{Q}$. Finally, $P(0, p)$ has order 3, $\#E_{\mathrm{tor}}(\mathbb{Q}) = 3$ and $E_{\mathrm{tor}}(\mathbb{Q}) = \{\mathcal{O}, (0, p), (0, -p)\}$.

For $p = 2$, this is Example 8.1 in Washington's book. The points of finite order are $(0, \pm 2)$ of order 3.

Question 5 (**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).

Solution 5.

(1) The discriminant is $\Delta = -16(4a-1)a^4$. (Actually, the discriminant of $f_a = x^3 - (2a-1)x^2 + a^2x$ is $(4a-1)a^4$).
(2) The condition for E to be an elliptic curve is Δ non-zero, hence $a \neq 0$ and $a \neq 1/4$.
(3) We check that $P(a,a)$ satisfies the curve equation. The right-hand side is $a^3 - (2a-1)a^2 + a^2 \cdot a = 2a^3 - (2a^3 - a^2) = a^2$ and we obtain the right-hand side, we conclude that $P(a,a)$ is on the curve.
(4) First we do $2P$. We have $\lambda = \frac{3x_1^2 - 2(2a-1)x_1 + a^2}{2y_1}$, $\lambda = \frac{3a^2 - 2(2a-1)a + a^2}{2a} = (3a - 4a + 2 + a)/2 = 1 \neq 0$, $x_{2P} = \lambda^2 - 2a + (2a-1) = 1^2 - 1 = 0$, $y_{2P} = \lambda(a-0) - a = 0$ and $2P \neq \mathcal{O}$ but $2P$ has order 2. Because $P \neq \mathcal{O}, 2P \neq \mathcal{O}$, but $4P = \mathcal{O}$, we conclude that P has order 4.
(5) According to the strong Nagell–Lutz theorem, $y = 0$ or $y^2 \mid (4a-1)a^4$. We assume that $1-4a$ is not a square, hence $y^2 \in \{a^2, a^4, 1\}$.
(6) The possibilities for y are $y = 0$ and in this case, $x = 0$ or $x^2 - (2a-1)x + a^2 = 0$, the discriminant of the quadratic polynomial is $(2a-1)^2 - 4a^2 = 4a^2 - 4a + 1 - 4a^2 = 1 - 4a$, but we assumed that $1-4a$ is not a square, so there is only one point of order 2.
If $y^2 = a^2$, the solutions are $(a,a), (a,-a)$. Note that $f_a(x) - a^2 = x^3 - (2a-1)x^2 + a^2x - a^2 = (x-a)(x^2 - (a-1)x + a)$ and the quadratic polynomial has discriminant $a^2 - 6a + 1$ which has no reason to be a square.
If $y^2 = a^4$ or $y^2 = 1$, there is no obvious solution (SageMath).
In conclusion, the torsion points without any other assumption on a are $\{(0,0), (a,a), (a,-a), \mathcal{O}\}$.