2. Del

The Lutz-Nagell theorem and torsion points

Version 0.1— *Monday, September 1, 2014 2:36:34 PM*

This is a very preliminary version, and will change, (some more examples and exercises ??), but it covers basically what I'll do this week (and may be next). Both in Silverman and Milne this is done a little differently. Milne works over $\mathbb{Q}_p$-adic numbers, but the core of the arguments there are just the same as here (II.4 in Milne's book, and a little from II.3). Silverman uses something called formal groups which are nice things, but we have no time to dig into that.

Trygve Nagell was born in Kristiania in 1895. He studied mathematics at Det Kongelige Fredriks Universitet (as the university of Oslo was called at that time) i Kristiania (as Oslo was called at that time) with Axel Thue as a tutor, and he obtain his doktorgrad in Oslo (Kristiania changed the name to Oslo in 1925) in 1928 with a thesis about elliptic curves. In 1931 he was appointed professor in Uppsala. where he remain except for some extensive travels until his death in 1988. In this chapter we shall prove one of Nagell's theorems from 1935— it is may be, his most famous one. A few years later, in 1937, Elizabeth Lutz who was a student of André Weil, independently proved a p-adic version and now a days the theorem is named after the two.

The theme of this chapter is elliptic curves over $\mathbb{Q}$ and their torsion points. The group $E_{tor}(\mathbb{Q})$ of torsion points is relatively accessible. Given a specific elliptic curve over $\mathbb{Q}$ there is an algorithm to compute it which is based on the Lutz-Nagell theorem, the main result of this chapter.

During the later part of the 20th century people determined the torsion group of long series of elliptic curves. The list of torsion groups was strikingly restricted,

for example no curve with 11-torsion or n-torsion with $n > 12$ was found. In 1908 the italian mathematician Beppo Levi gave a conjectural[1] list of the possible torsion groups, and it was finally proved by Barry Mazur in 1976 that the list was exhaustive. The theorem is deep and we don't even touch a proof.

Theorem 2.1 (Barry Mazur) *Let E be an elliptic curve over $\mathbb{Q}$. Then the torsion group $E(\mathbb{Q})$ is one of the following:*

- *A cyclic group $\mathbb{Z}/n\mathbb{Z}$ with $2 \leq n \leq 10$ or $n = 12$.*
- *One of the groups $\mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2Z$ where $1 \leq n \leq 4$.*

The Lutz-Nagell theorem is more modest, but still forceful enough to make it possible to determine the torsion group of any specific elliptic curve, at least if one knows a Weierstrass equation for it. So the point of departure is an elliptic curve over $\mathbb{Q}$ with an integral Weierstrass equation:

$$y^2 = x^3 + ax + b \tag{2.1}$$

where a and b are in $\mathbb{Z}$. Any Weierstrass equation can be brought onto this form by an admissible change of coordinates. The discriminant $\Delta = 27b^2 + 4a^3$ plays prominent role in the theorem. A given curve has several equations of the form (2.1), *e.g.,* if one replaces y by c^3y and x by c^2x, the discriminant changes to $c^{-12}\Delta$, and in the applications of the Lutz-Nagell theorem, to get he most out of the theorem, one should work with equations whose discriminant is minimal, but it is not a premise for the theorem.

Theorem 2.2 (Lutz-Nagell) *If the elliptic curve E has the integral Weierstrass equation (2.1) above, and $P = (x, y)$ is a torsion point of E, then x and y are integers, and either $y = 0$ or y^2 is a divisor in the discriminant Δ, that is $y^2|\Delta$.*

The core of the theorem is the statement that torsion points ave integral coordinates. Since if P is torsion $2P$ will be torsion as well, the divisibility statement follows from the lemma below:

Lemma 2.1 *Let E be an elliptic curve over $\mathbb{Q}$ with the integral Weierstrass equation (2.1) above, and let $P = (x_1, y_1)$ be a rational point on E. If both P and $2P$ have integral coordinates, then $y_1 = 0$ or $y_1^2|\Delta$.*

PROOF: Let $2P = (x_2, y_2)$. By assumption the coordinates x_1, y_1, x_2, y_2 are are integers, and we may clearly assume that $y_1 \neq 0$. The equation of the curve reads

$$y^2 = g(x)$$

[1]The conjecture was later reformulated by Trygve Nagell in 1952, and by Andrew Ogg in 1968. In modern time it was known as "Ogg's conjecture", but today, of course, it is named Mazur's theorem.

where $g(x)$ is a cubic polynomial in $\mathbb{Z}[x]$. Hence $y_1^2|g(x_1)$. The expression for the x-coordinate in the duplication formula (1.5) on page 13 in part one reads

$$2x_1 + x_2 = \big(\frac{g'(x_1)}{2y_1}\big)^2,$$

and therefore $y_1|g'(x_1)$. Now, the discriminant is the resultant of $g(x)$ and $g'(x)$, so one may write $\Delta = r(x)g(x) + s(x)g'(x)$, with $r, s \in \mathbb{Z}[x]$; in fact one has the explicit formula (see exercise 1.12 on page 25 in part one):

$$\Delta = -27(x^3 + ax - b)g(x) + (3x^2 + 4a)g'(x)^2.$$

Consequently $y_1^2|\Delta$. ❑

Example 2.1. Let E be the curve with equation $y^2 = x^3 + 1$. Then $E(\mathbb{Q})_{tors} = \mathbb{Z}/6\mathbb{Z}$. Indeed, $Q = (-1, 0)$ is the only two-torsion point. The curve has the two rational point $P = (0, 1)$ and $-P = (0, -1)$, and using the duplication formula one easily checks that $2P = -P$. Hence P and $-P$ are 3-torsion points. Computing $P + Q$ one finds $P + Q = (2, 3)$ and therefore $(2, 3)$ and $(2, -3)$ both are 6-torsion points. The discriminant is $\Delta = 27$, so by the Lutz-Nagell theorem, the only possible y-coordinates for torsion points are 0, ± 1 and ± 3, and from there one easily arrives at the above points being all torsion points. ❄

Example 2.2. Let a be an odd integer. Then $y^2 = x^3 - ax + 1$ has infinitely many rational points. There are rational points namely $(0, \pm 1)$, so if we can show that *e.g.*, $P = (0, 1)$ is not torsion, we are safe. But the duplication formula gives that the x-coordinate x_2 of $2P$ is

$$x_2 = \big(\frac{-a}{\pm 2}\big)^2 = \frac{a^2}{4}.$$

By Lutz-Nagell this is an integer contradicting the assumption that a be odd.

❄

One consequence of the Lutz-Nagell theorem is that the torsion group $E(\mathbb{Q})_{tors}$ is finite (there are only finitely many divisors in Δ and for each, $y^2 = g(x)$ has only three solutions). This is of course also a consequence of the group $E(\mathbb{Q})$ being finitely generated by the Mordell-theorem, but Mordell's theorem is considerably deeper (to put it mildly) than this lemma, so it is worth noting.

To establish the integrality statement in Lutz-Nagell, the strategy is to show that no prime number divides the denominators of x and y. In the process of implementing this—as in many other contexts with elliptic curves and diophantine equations in general—reduction modulo a prime p is the essential tool, so this is the place for us to discuss the reduction map in some detail.

2.1 Reduction modulo a prime

For any prime number p, there is a reduction mapping $\mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^n(\mathbb{F}_p)$. The image of P will be denoted by $\bar{P}$; a convention that extends the traditional notation $\bar{a}$ for the residue of an integer a mod p. For a point P in $\mathbb{P}^n(\mathbb{Q})$ with relatively prime integral homogenous coordinates, it is clear what $\bar{P}$ should be: We just reduce all the coordinates mod p, and at least one not being divisible by p, the reduced coordinates do not all vanish. The point is that the coordinates of any P may be brought on this form by scaling.

To have some more flexibility, we prefer a slightly more general and, in the end, more natural approach. Any rational number x not having p as a factor in denominator when written in reduced form, can be reduced mod p. Indeed, if $x = a/b$ with b not divisible by p, the residue $\bar{b}$ is non-zero in the field $\mathbb{F}_p$; hence $\bar{x} = \bar{a}/\bar{b}$ has a meaning.

Another way of stating this, is that there is a reduction map from the localisation $\mathbb{Z}_{(p)}$ to $\mathbb{F}_p$. Recall that the elements in $\mathbb{Z}_{(p)}$ are the rational numbers a/b with p not a factor in b. It is a local ring with maximal ideal generated by p and with residue field $\mathbb{F}_p$.

Recall the definition of p-adic valuation $v_p(x)$ of a rational number x. For an integer a the valuation $v_p(a)$ is the heighest power of p dividing a. For example $v_p(p^v) = v$ and $v_p(a) = 0$ if and only a and p are relatively prime. If $x = a/b$ is a rational number one has $v_p(x) = v_p(a/b) = v_p(a) - v_p(b)$. The valuation complies with the two rules

- $v_p(xy) = v_p(x) + v_p(y)$,
- $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Every rational number is on the form $x = x_0\, p^{v_p(x)}$ where neither the enumerator nor the denominator of x_0 is divisible by p.

The numbers of the local ring $\mathbb{Z}_{(p)}$ are the rational numbers x with $v_p(x) \geq 0$, that is, the rational numbers not having p as a factor in the denominator, and the units $\mathbb{Z}^*_{(p)}$ are those with $v_p(x) = 0$; that is the numbers such that p neither divides the enumerator nor the denominator.

Lemma 2.2 *Given a point $P \in \mathbb{P}^n(\mathbb{Q})$. One can find homogenous coordinates $(x_0; \ldots; x_n)$ for P with $v_p(x_i) \geq 0$ and with $v_p(x_i) = 0$ for at least one index. Two such representations are up to scaling by a unit in $\mathbb{Z}_{(p)}$ identical.*

Proof: Assume that $P = (x_0, \ldots, x_n)$ and let $v = \min\{\, v_p(x_i) \mid 0 \leq i \leq n \,\}$. Then obviously $P = (p^{-v}x_0, \ldots, p^{-v}x_n)$, and $v_p(p^{-v}x_i) = v_p(x_i) - v \geq 0$. This establishes the existence. For uniqueness, assume that $\alpha x_i = \beta x_i$,for $0 \leq i \leq n$, with α and β relatively prime integral numbers, and assume that $p|\alpha$. For at least one index p does not divide x_i the x_i's being relatively prime. It follows that $p|\beta$, contradicting the assumption that α and β be relatively prime. Hence $v_p(\alpha) = v_p(\beta) = 0$ and $\alpha\beta^{-1}$ is a unit in $\mathbb{Z}_{(p)}$. ❏

There is a "global" version of this:

Lemma 2.3 *Assume that $P \in \mathbb{P}^n(\mathbb{Q})$. Then up to sign, there is a unique way of representing $P = (x_0; \ldots; x_n)$ with the x_i's being relatively prime integers.*

The phrase "up to sign" means that $(x_0; \ldots; x_n) = (\epsilon x_0'; \ldots; \epsilon x_n')$ with $\epsilon = \pm 1$.

PROOF: If $(y_0; \ldots; y_n)$ and $(x_0; \ldots; x_n)$ are two representations of P by relatively prime integers, there are integers α and β such that $\alpha x_i = \beta y_i$ for all i. Assume a prime q divides α. Since the y_i's are relatively prime, q does not divide y_i for at least one index, and therefore q divides β. It follows that α and β have the same prime factors, and $\alpha = \pm\beta$.

Now, if $P = (x_0; \ldots; x_n)$ with $x_i \in \mathbb{Q}$, one scales the x_i's by the least common multiple of their denominators, thus obtaining a representation of P with integral coordinates, which after scaling by their greatest common divisor (or rather its inverse) become relatively prime. ❑

By this lemma any point $P \in \mathbb{P}^n(\mathbb{Q})$ may be represented as $P = (x_0; \ldots; x_n)$ with the x_i's integral and relatively prime, and we then define $\bar{P} = (\bar{x}_0; \ldots; \bar{x}_n)$. Since the x_i's are relatively prime, not all of them are congruent zero mod p, and since the representation is unique up to sign, $\bar{P}$ is well defined. In fact, one does not need the x_i's to be integers, by the first lemma, it sufficies that their denominators be without p as factor, that is one needs that $v_p(x_i) \geq 0$.

Now we turn to the specific situation of $\mathbb{P}^2$. The reduction map $\mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{F}_p)$ takes rational lines to lines. Indeed, if $ax + by + cz = 0$ is the equation of a rational line, one may, after a suitable scaling of the equation, assume that the coefficients are relatively prime integers. Thus $\bar{a}x + \bar{b}y + \bar{c}z = 0$ is the equation of a line in $\mathbb{P}^2(\mathbb{F}_p)$ into which the line $ax + by + cz = 0$ is mapped.

GOOD AND BAD REDUCTION OF AN ELLIPTIC CURVE Let E be an elliptic curve defined over $\mathbb{Q}$. We may put the equation E on Weierstrass normal form,

$$y^2 + a_1yx + a_3y = g(x) = x^3 + a_2x^2 + a_4x + a_6,$$

and we may assume that the a_i's all satisfy $v_p(a_i) \geq 0$. A replacement of x by c^2x and y by c^3y in any Weierstrass equation where c is an appropriate power of p will do. Often one will work with an equation with coefficients in $\mathbb{Z}$, and the same argument shows one can always admissibly change coordinates to arrive at an integral Weierstrass equation.

The curve defined over $\mathbb{F}_p$ by the equation

$$y^2 + \bar{a}_1yx + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

obtained by reducing the coefficients mod p is denoted $\bar{E}$. It is called *the reduction of E mod p*.

The discriminant of an elliptic curve being a polynomial in the Weierstrass coefficients a_i, it is clear that the discriminant of $\bar{E}$ is the reduction of the discriminant of E mod p. Hence if $p \not| \Delta$, the curve $\bar{E}$ is smooth, and we say that E has *good reduction*

at p. In case $p|\Delta$, the curve has *bad reduction at p*. It is singular, but in view of proposition 1.3 in part one, it has at most one singular point. This can either be a cusp or a node. In the former case, we say that E has *additive reduction at p*, and in the latter, E has *multiplicative reduction*. The multiplicative reduction is either *split* or *non-split* according to the node being split or non-split.

One says that Weierstrass equation is *minimal at p* if the valuation $v_p(\Delta)$ is minimal among the discriminants of all Weierstrass equations of E with coefficients in $\mathbb{Z}_{(p)}$. Such minimal equations always exist, and they are unique up to an admissible change coordinates of the type in proposition 1.10 in part one with c invertible in $\mathbb{Z}_{(p)}$:

Proposition 2.1 *Let E be an ellitiptic curve over $\mathbb{Q}$. For any prime p, E has a minimal Weierstrass equation over $\mathbb{Z}_{(p)}$, and it is unique up to an admissible change of coordinate as in 1.10 with c a unit in $\mathbb{Z}_{(p)}$.*

PROOF: Two Weierstrass equations are related by an admissible change of coordinates, and according to proposition 1.11 on page 16 in part one the two discriminants satisfy $\Delta = c^{12}\Delta'$. If both Δ and Δ' are of minimal p-adic valuation, one readily obtains $v_p(c) = 0$. Indeed, one has $v_p(\Delta') \leq v_p(\Delta) = 12v_p(c) + v_p(\Delta') \leq v_p(\Delta')$. This shows the uniqueness, existence is no deeper than the fact that any non-empty set of natural numbers has a least member. ❑

We saw in example 1.1 in part one that some properties of the reduced curve is sensitive to base change, like prime factors of the discriminant. As minimal equation is canonical, this confusion is eliminated. One of many reasons for using the general Weierstrass equation, is to be able to do reduction mod 2 and 3, so we stress the fact that the minimal model is chosen among the *general* Weierstrass equations.

REDUCTION MAP IS A GROUP HOMOMORPHISM For points $P \in E(\mathbb{Q})$ clearly $\bar{P} \in \bar{E}(\mathbb{F}_p)$, and the reduction map induces a map $E(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$. When E has good reduction at p, the set $\bar{E}(\mathbb{F}_p)$ is a group, and since the reduction map takes rational lines into lines, the reduction map is a group homomorphism:

Proposition 2.2 *Assume that the elliptic curve E has good reduction at p. Then the reduction map $E(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$ is a group homomorphism.*

THE KERNEL OF THE REDUCTION MAP The kernel of this map is clearly of high interest. Of course the neutral element $O = (0;1;0)$ is contained there, but there might certainly be other elements. So let P be a point in the kernel with $z \neq 0$, that is, $P = (x;y;1)$ is a point of $E(\mathbb{Q})$ that reduces to $(0;1;0)$ mod p. The coordinates x and y are rational numbers, and to find the reduced point one must clean the denominators of x and y for powers of p: One replaces $(x;y;1)$ by $(xp^{-v};yp^{-v};p^{-v})$ where $v = \min\{v_p(x), v_p(y), 0\}$. Since the y-coordinate of the reduced point is non-zero in $\mathbb{F}_p$, one sees that $v_p(y) = v$, and hence $v_p(x) > v$ since the x-coordinate is zero. The addional points in the kernel therefore are those with $v_p(x/y) > 0$. This subgroup is denoted by E^1 (it certainly depends on the prime p, but to keep the things simple, we do not include p in the notation). This establishes

Proposition 2.3 *Assume that the elliptic curve E over $\mathbb{Q}$ has good reduction at p. Let E^1 be the subset of $E(\mathbb{Q})$ given by $E^1 = \{\,(x;y;z) \in E(\mathbb{Q}) \mid v_p(x/y) \geq 1\,\}$. Then E^1 is the kernel of the reduction map $E(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$.*

2.2 The p-adic filtration

In view of the discution of the kernel of the reduction map above, it seems natural to introduce the following series of subsets of $E(\mathbb{Q})$. For each natural number n we define:

$$E^n = \{\,(x;y;1) \mid v_p(x/y) \geq n\,\} \cup \{O\}.$$

The sets $\{E^n\}$ clearly form a descending series of subsets (this is what mathematicians call a filtration), and the series is called the *p-adic filtration* of $E(\mathbb{Q})$. It certainly depends on the prime p, even if p is invisible in the notation. *A priori* the subsets E^n are, well, just subsets, but soon we shall see that they in fact are subgroups. Our main application of the p-filtration is the following proposition, from which the Lutz-Nagell theorem will bw deduced:

Proposition 2.4 *The subgroup $E^1 \subseteq E(\mathbb{Q})$ is torsion free.*

Another nice corollary, very useful when one wants to determine the torsion part of $E(\mathbb{Q})$, is the following, which by the way, also immediately shows that $E_{tors}(\mathbb{Q})$ is finite.

Corollary 2.1 *Assume that E has good reduction at the prime p. Then the reduction map $E_{tor}(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$ is injective.*

PROOF: On one hand E^1 is the kernel of the reduction map, ond the other hand it is torsion free, so $E^1 \cap E_{tors}(\mathbb{Q}) = 0$. ❑

This corollary impose severe restrictions on the torsion part $E^{tors}(\mathbb{Q})$. As an illustration, we study the curves $y^2 = x^3 - q^2x + 1$:

EXAMPLE 2.3. Let E be the curve $y^2 = x^3 - q^2x + 1$ where q is a prime different from 2 and 3. Then E has no non-trivial rational torsion points. The strategy to see this is to reduce E mod p for some small values of p, namely $p = 3$ and $p = 5$, and then use corollary 2.1.

The discriminant is $\Delta = 27 - 4q^6$. Now $\Delta \equiv -1 \mod 3$ (one is the only non-zero square in $\mathbb{F}_3$) and $\Delta \equiv 2 \pm 1 \mod 5$ if $q \neq 5$ (± 1 are the only non-zero squares in $\mathbb{F}_5$) and $\Delta \equiv 2 \mod 5$ if $q = 5$. Thus our curve E has good reduction both at 3 and 5.

We first reduce mod 3. The equation becomes $y^2 = x^3 - x + 1$, and counting the nuber of point in $\bar{E}(\mathbb{F}_3)$, one finds 7. Hence $\bar{E}(\mathbb{F}_3) = \mathbb{Z}/7\mathbb{Z}$ and $|E_{tors}(\mathbb{Q})|$ divides 7.

Next we reduce mod 5, and the equation becomes $y^2 = x^3 + x + 1$ or $y^2 = x^3 - x + 1$ acoording to $q^2 \equiv 1 \mod 5$ or $q^2 \equiv -1 \mod 5$. In the former case, E has 9 solutions

mod 5 and in the latter 8. Hence the order $|E_{tors}(\mathbb{Q})|$ divides 8 or 9, but we already showed that it divides 7. The only possibilty is that the order is one, and $\mathbb{E}_{tors}(\mathbb{Q})$ is trivial.

It is easy to find some rational points on E, indeed the two points $(0, \pm 1)$ lies on E. As they are not torsion points, they generate a subgroup isomorphic to $\mathbb{Z}$, and E has infinitly many rational points. ❄

The group law in coordinates around $(0;1;0)$

For people used to Lie-groups it is very natural to study a group in a neigbourhood of the neutral element. This is fruitful for us and will give us the necessay insight to prove teh Lutz-Nagell theorem. In our case, as the neutral element lies at the point $(0;1;0)$ at infinity, the change of variable $t = x/y$ and $s = 1/y$ brings the neutral element to the origin. In those coordinates the equation (2.1) takes the form

$$s = t^3 + ats^2 + bs^3. \tag{2.2}$$

We need to express the group law in these coordinates. So let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ be two points on E and denote by $P_3 = (t_3, s_3)$ their sum $P_1 + P_2$.

Let $s = \alpha t + \beta$ be the equation of the line connecting the two points, or in case the two are equal, the tangent to E at that point. The slope α is of course given as $\alpha = (s_2 - s_1)/(t_1 - t_2)$ in case $t_1 \neq t_2$. And in case $P_1 = P_2$, one finds by implicit derivation that

$$\alpha = s'(t_1) = (3t_1^2 + as_1^2)(1 - 2at_1s_1 - 3bs_1^2)^{-1} \tag{2.3}$$

By the standard method (plug in the equation for the line in the Weierstrass equation and compute the coefficient of the second order term) this leads to

$$t_1 + t_2 + t_3 = -(3\alpha^2\beta b + 2\alpha\beta a)(1 + a\alpha^2 + \alpha^3 b)^{-1} \tag{2.4}$$

The p-adic valuations of x and y

Our task in proving the Lutz-Nagell theorem, is to show that both $v_p(x) \geq 0$ and $v_p(y) \geq 0$ if $(x;y;1)$ is a torsion point, or turned around, we must show that if either $v_p(x) < 0$ or $v_p(y) < 0$, then (x, y) is not a torsion point. Now x and y satisfy the integral Weierstrass equation (2.1) so $v_p(y) < 0$ implies that $v_p(x) < 0$. This leads us to study the situation with $v = v_p(x) < 0$.

Lemma 2.4 *With the notation above. Assume $v_p(x) < 0$. Then $v_p(x) = -2n$ and $v_p(y) = -3n$ for an integer $n \geq 1$.*

Hence $v_p(x/y) = n$ if and only if $v_p(x) = -2n$ and $v_p(y) = -3n$.

PROOF: The integral Weierstrass equation (2.1) reads

$$y^2 = x^3 + ax + b.$$

One finds $v_p(x^3 + ax + b) = \min\{3v_p(x), v_p(a) + v_p(x), v_p(b)\} = 3v_p(x)$, since $v_p(x) < 0$ and both a and b are integers. On the other hand $v_p(y^2) = 2v_p(y)$. Hence $2v_p(y) = 3v_p(y)$, and $n = -v_p(x)/2 = -v_p(y)/3$ is a positive integer. ❑

The p-adic filtration is a filtration of subgroups

This paragraph is devoted to the proof of the in this context fundamental result:

Proposition 2.5 *The p-adic filtration is a filtration of subgroups, that is the subsets E^n are subgroups. For each $n \geq 1$, the map $(x, y) \to t = x/y$ induces an injective group homomorphism $t\colon E^n/E^{5n} \to p^n Z/p^{5n}\mathbb{Z}$.*

Recall the definition of the filtration where $t(P) = x(P)/y(P)$:

$$E^n = \{\, P = (x; y; 1) \in E(\mathbb{Q}) \mid v_p(t(P)) \geq n \,\}.$$

Clearly t induces a map from E^n into $p^n\mathbb{Z}$, and by reduction a map to $p^n\mathbb{Z}/p^m\mathbb{Z}$ for any $m > n$, in particular for $m = 5n$ (this seemingly random choice will be clearer in a moment). Once we know it to be a group homomorphism, the kernel is by definition E^{5n}.

That E^n is a subgroup and t a group homomorphism, is contained in the following result:

Lemma 2.5 *If $n \geq 1$ and $P_1, P_2 \in E^n$, then $t(P_1) + t(P_2) \equiv t(P_1 + P_2) \mod p^{5n}$*

PROOF: Recall the formula (2.4) relating the t-coordinate of a sum to the t-coordinates of the two addends:

$$t_1 + t_2 + t_3 = -(3\alpha^2\beta b + 2\alpha\beta a)(1 + a\alpha^2 + \alpha^3 b)^{-1}. \qquad (\star)$$

We shall estimate the p-adic valuation of the right side of this equation, and for that we need a good estimate of $v_p(\alpha)$. If $P_1 \neq P_2$, one finds from the equation (2.2) on page 8, that

$$\begin{aligned} s_2 - s_1 =& t_2^3 - t_1^3 + at_2s_2^2 - at_1s_1^2 + b(s_2^3 - s_1^3) = \\ =& t_2^3 - t_1^3 + at_2(s_2^2 - s_1^2) - as_1^2(t_1 - t_2) + b(s_2^3 - s_1^3) \end{aligned}$$

this gives

$$(s_2 - s_1)A = (t_2 - t_1)B$$

where $A = 1 + a(s_1 + s_2) - b(s_1^2 + 2s_1s_2 + s_2^2)$ and $B = t_2^2 + t_1t_2 + t_2^2 - as_1^2$. Since $v_p(s_i) \geq 3n$ and $v_p(t_i) \geq n$, one has $v_p(A) = 0$ and $v_p(B) \geq 2n$, hence $v_p(\alpha) = v_p(B) \geq 2n$. In case $P_1 = P_2$, this follows directly from (2.3) on page 8.

In turn we arrive at an estimate of $v_p(\beta)$; we have $\beta = s_1 - \alpha t_1$, so $v_p(\beta) \geq \min\{v_p(s_1), v_p(\alpha) + v_p(t_1))\} \geq 3n$, and the formula ($\star$) above proves the lemma, since $v_p(2\alpha\beta a) = v_p(2) + v_p(\alpha) + v_p(\beta) + v_p(a) \geq 5n$. ❑

Proof of Lutz-Nagell

Finally things come together, and we shall prove

Proposition 2.6 *The subgroup E^1 is torsion free.*

PROOF: By proposition 2.5 the group E^1 does not have torsion relatively prime to p. Indeed, assume that $mP = 0$ with $(m, p) = 1$ and $P \neq 0$. Let $n \geq 1$ be such that $P \in E^n$, but $P \notin E^{n+1}$. Then $mt(P) = 0$, but because the group $p^n Z/p^{5n}\mathbb{Z}$ has no m-torsion, it follows hat $t(P) = 0$. Hence $P = 0$, which is a contradiction.

If P is of finite order $m \geq 1$, the prime p therefore is a factor of m, and we may write $m = pl$ for an integer l. The point $P' = lP$ is of order p and $P' \neq 0$. Let now $n \geq 1$ be such that $P' \in E^n$, but $P' \notin E^{n+1}$. We have $pt(P') = 0$, so $pt(P') \equiv 0 \mod p^{5n}$, and therefore $t(P') \equiv 0 \mod p^{5n-1}$. Since $5n - 1 > n + 1$ this contradicts the fact that $P' \notin E^{n+1}$. ❑

This immediately finihes off the proof of the Lutz-Nagell theorem:

Corollary 2.2 *If $(x; y; 1)$ is a torsion points of $E(\mathbb{Q})$, then x and y are both integers.*

PROOF: We may assume $P \neq O$. If either x or y is not an integer, there is at least one prime p with $v_p(x) < 0$. Hence for that p, one has $P \in E^1$. But P is torsion and E^1 is torsion free, so $P = 0$. Contradiction. ❑

Corollary 2.3 *Assume that E has good reduction at p. Then the reduction homomorphism $\rho\colon E_{tor}(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$ is injective.*

PROOF: The kernel of ρ is equal to E^1. Indeed, if the point $(x; y; z)$ with integral coordinates maps to the point $(0; 1; 0)$, one has $v_p(x) \geq 1$ and $v_{p(y)} = 0$. Hence $v_p(x/y) \geq 1$ and $P \in E^1$.

On the other hand, if $P = (x; y; 1) \in E^1$, then $(x; y; 1) = (x_0 p^{-2n}; y_0 p^{-3n}; 1) = (x_0 p^n, y_0, p^{3n})$ which gives $(0; 1; 0)$ upon reduction mod p. ❑

Application and examples

We shall as

Proposition 2.7 *Assume that E is the elliptic curve $y^2 = x^3 + Ax = g(x)$ with A an integer free from fourth powers. Then*

$$E_{tor}(\mathbb{Q}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{if } -A \text{ is a square}, \\ \mathbb{Z}/4\mathbb{Z} & \text{if } A = 4, \\ \mathbb{Z}/2\mathbb{Z} & \text{otherwise}. \end{cases}$$

The assumptiom that A be without factors being forth powers is not restrictive as any such factor can be removed by an appropriate scaling as in 1.4. The proof of the proposition depends on $E_{tors}(\mathbb{Q})$ being isomorphic to a subgroup of $\bar{E}(\mathbb{F}_p)$. The following lemma about the number of points E has modulo certain primes is essential.

Lemma 2.6 *Is $p \equiv 3 \mod 4$, the curve E has exactly $p+1$ points in $\mathbb{F}_p$.*

PROOF: Since $p \equiv 3 \mod 4$, we know that -1 is not a square mod p. Since $g(-x) = -g(x)$, not both elements x and $-x$ in $\mathbb{F}^p$ are squares (if they were, -1 would be a square), and hence one of them is not the x-coordinate of a point in $\bar{E}(\mathbb{F}_p)$. On the other hand, if $a \in \mathbb{F}_p$, either a or $-a$ is a square. This gives p points in $\bar{E}(\mathbb{F}_p)$, and in addition, there is the point $(0;1;0)$ at infinity. ❑

PROOF OF PROPOSITION 2.7: First of all, the point $(0,0)$, is a 2-torsion point since the y-coordinate is 0. If $-A$ is a square, say $-A = a^2$, then the equation takes the form $y^2 = x(x-a)(x+a)$, and there are three 2-torsion points. Hence, if the index of $E(\mathbb{Q})$ is two, *i.e.,* it consists solely of 2-torsion points, it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if $-A$ is a square, and to $\mathbb{Z}/2\mathbb{Z}$ otherwise.

The point $(0,0)$ is 2-divisible only if $A = 4$. Indeed, assume that $2(x,y) = (0,0)$. The duplication formulas 1.5 on page 13 then reads

$$0 = (\frac{3x^2 + A}{2y})^2 - 2x \qquad 0 = \frac{3x^2 + A}{2y}x - y,$$

and by simple manipulations one finds $A = x^2$. But as A is free of quadratic factors, x is free of squares, which contradicts the Weierstrass equation that reads $y^2 = x^3 + Ax = 2x^3$, unless $x = 2$.

The rest of the proof is two show that the order of $E(\mathbb{Q})$ divides 4, and that is where corollary 2.1 on page 7 comes into play.

First of all, no odd prime $q > 3$ is a factor in $|E_{tors}(\mathbb{Q})|$. Indeed, by Dirichlet's theorem about primes in arithmetical progressions, there are infinity many primes p with $p \equiv 3 \mod 4q$. Then $p \equiv 3 \mod 4$ and $p + 1 \equiv 4 \mod q$. This shows that q is not a factor in $p+1$, hence not in $\#\bar{E}(\mathbb{F}_p)$ by the lemma, and therefore neither in $|E_{tors}(\mathbb{Q})|$.

Now choose p sufficiently large,*i.e.,* not dividing Δ, such that $p \equiv 3 \mod 12$. then $p \equiv 3 \mod 4$ and $p + 1 \equiv 4 \mod 3$. Hence 3 is not a factor in $\mathbb{E}_{tor}(\mathbb{Q})$.

Choosing large p with $p \equiv 3 \mod 8$ an analogous argument shows that 8 is not a factor in $|E_{tors}(\mathbb{Q})|$, and the remaining possibilities are 1, 2 and 4 This closes the case when the index of $E(\mathbb{Q})$ is two, it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if $g(x)$ has three roots, that is , if and only if $-A$ is a square. ❑

PROBLEM 2.1. Let p be an odd prime. Show that there is an exact sequence

$$0 \longrightarrow \mu_2 \longrightarrow \mathbb{F}_p^* \xrightarrow{\phi} \mathbb{F}_p^* \xrightarrow{\psi} \mu_2 \longrightarrow 0$$

where $\psi(x) = x^{(p-1)/2}$ and $\phi(x) = x^2$ and where $\mu_2 = \{\pm 1\}$. Show that if $p \equiv 3 \mod 4$ then $\psi(-1) = -1$ and hence -1 is not a square and if $a \in \mathbb{F}_p$, then either a or $-a$ is a square. ✸