1.13 26/07/06 - The Complex Picture and Introduction to the Nagell-Lutz Theorem

Last time, we mentioned (without proof) that if K is a field of characteristic $p \geq 0$, and $\overline{K}$ an algebraic closure of K, and E/K an elliptic curve, then for all $n \in \mathbb{Z}_{\geq 1}$ such that $p \nmid n$, we have that $E[n](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/n \oplus \mathbb{Z}/n$. We also saw proofs of this result when $n = 2, 3$. In particular, this holds for all $n \in \mathbb{Z}_{\geq 1}$ when $\operatorname{ch} K = 0$. Today I want to explain the *real reason* we might expect something like this to be true, over our favorite algebraically closed field of characteristic zero, namely $K = \mathbb{C}$.

1.13.A The Story over $K = \mathbb{C}$

The complex exponential $\exp : \mathbb{C} \to \mathbb{C}^\times$ is *singly periodic* with period $2\pi i$: it has the property that for all $z \in \mathbb{C}$ and $n \in \mathbb{Z}$ we have $\exp(z + n \cdot (2\pi i)) = \exp(z)$. (This is what makes the theory of Fourier series work!) But this is not the only kind of periodicity that a complex function can have. Since the complex numbers are "two-dimensional", we can ask if there are complex functions which have two "independent" periods. For various reasons related to those discussed in §1.12.A, mathematicians in the 19^{th} century (such as Weierstrass) got interested in studying these *doubly periodic* complex functions.

To set up the theory, suppose that $\Lambda \subset \mathbb{C}$ is a lattice, such as $\Lambda = \mathbb{Z}[i]$ or $\Lambda = \mathbb{Z}[\zeta_3]$ or $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$ for some $\tau \in \mathbb{C}$ with $\operatorname{Im} \tau > 0$. (I will not give a formal definition.) A function $f : \mathbb{C} \to \mathbb{C}$ is doubly periodic with periods in Λ iff for all $z \in \mathbb{C}$ and $\omega \in \Lambda$ we have $f(z + \omega) = f(z)$. For this to be true, it is sufficient to require this happens for two independent periods $\omega_1, \omega_2 \in \Lambda$ that form a $\mathbb{Z}$-basis of Λ. Specifying such a function is the same as specifying a function on the quotient group $\mathbb{C}/\Lambda$, which you should think of as being given by the fundamental parallelogram with opposite sides glued in Pac-Man style. The resulting object is topologically a torus. Now Liouville's Theorem from complex analysis implies that there cannot be any nonconstant holomorphic (i.e., complex-differentiable) doubly periodic functions with respect to Λ, but there can indeed be such functions if we allow some points where the function is not defined (i.e., has a pole); such functions are known as *meromorphic* functions.

One of the "simplest" such meromorphic functions, investigated by Weierstrass, is now called the *Weierstrass $\wp$-function*, defined by

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \smallsetminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{1.13.1}$$

This depends on Λ, so is probably more properly written as $\wp_\Lambda$. Note that this function is not defined at any points of Λ, but at least the terms of this series make sense when $z \notin \Lambda$.

Fact 1.13.2. The expression 1.13.1 converges to a holomorphic (i.e., complex differentiable) function on $\mathbb{C} \smallsetminus \Lambda$ that is Λ-periodic: for all $z \in \mathbb{C} \smallsetminus \Lambda$ and $\omega \in \Lambda$ we have $\wp(z + \omega) = \wp(z)$. When extended by $\wp(\omega) = \infty$ for all $\omega \in \Lambda$, the extended function $\wp$ is a Λ-periodic meromorphic function on $\mathbb{C}$, i.e., a meromorphic function on $\mathbb{C}/\Lambda$.

The above fact is not magical; it is just a matter of being careful about convergence and invoking the appropriate results from complex analysis. What is much more magical is

Fact 1.13.3. For any lattice $\Lambda \subset \mathbb{C}$, the infinite series defined by

$$g_2 := 60 \sum_{\omega \in \Lambda \smallsetminus \{0\}} \frac{1}{\omega^4} \text{ and } g_3 = 140 \sum_{\omega \in \Lambda \smallsetminus \{0\}} \frac{1}{\omega^6}$$

converge to complex numbers. Further, the function $\wp = \wp_\Lambda$ satisfies the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3. \tag{1.13.4}$$

This is very interesting, and looks suspiciously like what we have been doing. Specifically, consider the elliptic curve $E_\Lambda \subset \mathbb{P}^2_{\mathbb{C}}$ defined by the equation $y^2 = 4x^3 - g_2 x - g_3$. (This is not quite in

Weierstrass form, but it's close; also, we have to check that $\operatorname{disc}(4x^3-g_2x-g_3) = 16(g_2^3-27g_3^2) \neq 0$; I won't bother with this.) The magical fact 1.13.4 implies that if $z \in \mathbb{C} \smallsetminus \Lambda$, then the point $(x, y) = (\wp(z), \wp'(z))$ belongs to $E_\Lambda(\mathbb{C})$. We can then "complete" this map by defining $\omega \mapsto \mathscr{O} = [0:1:0]$ for all $\omega \in \Lambda$. The resulting map $\mathbb{C} \to E_\Lambda(\mathbb{C})$ is clearly Λ-periodic because $\wp$ is, and hence descends to a map of sets $\mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$. The third and craziest magical fact is

Fact 1.13.5. The map $\mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$ given by $[z] \mapsto [\wp_\Lambda(z) : \wp'_\Lambda(z) : 1]$ is an isomorphism of (complex Lie) groups.

In other words, the funny group law on the cubic curve $E_\Lambda(\mathbb{C})$ we defined using the chord and tangent process is just the "same" as the group law on the quotient group $\mathbb{C}/\Lambda$ of "addition modulo Λ". Ultimately, the key ingredient in the proof of 1.13.5 is another magical property of the $\wp = \wp_\Lambda$ function which says that if $u, v, w \in \mathbb{C} \smallsetminus \Lambda$ are such that $u + v + w \in \Lambda$ (i.e., $[u], [v], [w] \in \mathbb{C}/\Lambda$ classes that sum to zero in $\mathbb{C}/\Lambda$), then

$$\begin{vmatrix} \wp(u) & \wp'(u) & 1 \\ \wp(v) & \wp'(v) & 1 \\ \wp(w) & \wp'(w) & 1 \end{vmatrix} = 0.$$

In particular, we see immediately what n-torsion in $E_\Lambda(\mathbb{C})$ looks like: to find all points of order n in $\mathbb{C}/\Lambda$, we just divide the fundamental parallelogram into n^2 smaller ones by drawing n slits in each direction, and take the intersection points of these slits, which are the left-and-bottom vertices of the n^2 parallelograms. In particular, of course there are exactly n^2 of these, and they form a subgroup isomorphic to $\mathbb{Z}/n \oplus \mathbb{Z}/n$. (Some nice illustrations can be found in [2, §2.2].)

Because we're not going to prove these results, we are not going to use them. (The interested reader can find proofs in [8, Chapter VI] or in textbooks on complex analysis, such as [15, Chapter 7].) These results belong to a course on the *analytic* theory of elliptic curves; this course is one on the *algebraic* theory. I only wanted to mention them because they give context for a lot of things happening in this here. These ideas form the beginnings of many very beautiful stories in mathematics connecting elliptic curve theory to complex analysis and Riemann surfaces, and much more.

Unimportant Remark 1.13.6. This line of reasoning can be used to give a(n) (analytic) proof of 1.12.26 for $K = \mathbb{C}$, and then for any field K of characteristic zero by invoking the *Lefschetz principle* ([8, §V.6]).

1.13.B The Nagell-Lutz Theorem

Today, I want to start building towards two major theorems we will prove in this course: the Nagell-Lutz Theorem and the Mordell-Weil Theorem. We'll start with the first of these, with a discussion closely following [2, Chapter 2].

For the rest of this course (except perhaps at the very end), we're going to focus on the case of $K = \mathbb{Q}$, in which case we can work with short Weierstrass equations of the form

$$y^2 = x^3 + ax^2 + bx + c$$

with $a, b, c \in \mathbb{Z}$. Recall that if $f(x) := x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$, then the discriminant

$$D = \operatorname{disc}(f) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

is related to the discriminant Δ of E via

$$\Delta = 16D.$$

The Nagell-Lutz Theorem gives a complete algorithmic procedure (given factoring!) to find all torsion points on such an elliptic curve over $\mathbb{Q}$:

Theorem 1.13.7 (Nagell-Lutz)**.** In the above notation, let $a, b, c \in \mathbb{Z}$ be such that $D \neq 0$, and let $E/\mathbb{Q}$ be the corresponding elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$. If $P = (x_0, y_0) \in \operatorname{Tors} E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$, then in fact $x_0, y_0 \in \mathbb{Z}$ and either $y_0 = 0$ or $y_0^2 \mid D$.

Proofs of this result were published by the Norwegian mathematician Trygve Nagell (1895-1988) and the French mathematician Élisabeth Lutz (1914-2008) in the 1930s. Lutz's paper came out when she was just 23 years old. Nagell was a student of Alex Thue, famous, among many things, for his work on integer points on elliptic curves, and Lutz was a student of André Weil, famous, among many things, for being one of the founders of modern algebraic geometry in the early 20$^{\text{th}}$ century, which he studied extensively in jail after refusing to fight for France in World War II. The Nagell-Lutz Theorem (1.13.7) can in some ways be thought of as being similar to the Rational Root Theorem (1.1.2). Before we give a proof, let's look at a few examples (more to be found on Exercise Sheet 4).

Example 1.13.8. Consider the curve $E : y^2 = x^3 + 4$. Then $D = -2^4 3^3$. A nontrivial rational torsion point (x, y) must have either $y = 0$ (not possible, by 1.1.2) or have $y^2 \mid D$. This forces $y \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$. A simple check shows that the only possibility that allows rational x is $y = \pm 2$ with $x = 0$. This tells us that $\operatorname{Tors} E(\mathbb{Q}) = \{\mathscr{O}, (0, \pm 2)\}$, and this forces $\operatorname{Tors} E(\mathbb{Q}) \cong_{\mathsf{Ab}} \mathbb{Z}/3$. Note that this is really a result about the field $K = \mathbb{Q}$; indeed, we have

$$E[2](\overline{\mathbb{Q}}) = \{\mathscr{O}, (2^{2/3}\omega^i, 0)\}_{i=0,1,2} \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

Example 1.13.9. Consider the curve $E : y^2 = x^3 - 16x + 16$, and the point $P = (0, 4) \in E(\mathbb{Q})$ a point of finite order? Well, we have that

$$2P = (4, 4), \quad 3P = (-4, -4), \quad 4P = (8, -20), \quad 5P = (1, -1), \quad \text{and } 6P = (24, 116).$$

However, we see that

$$7P = \left(-\frac{20}{9}, \frac{172}{27}\right).$$

At this point, we can use 1.13.7 to tell us that $7P \notin \operatorname{Tors} E(\mathbb{Q})$ and hence $P \notin \operatorname{Tors} E(\mathbb{Q})$. In other words, the "tangent" process iterated with the seed $P = P_0$ will necessarily give us infinitely many distinct points on E; in particular, E *has* infinitely many rational points! Note that this example also illustrates the important point that the converse to 1.13.7 is false: we have $D = 2^8 \cdot 37$ and $P = (0, 4)$ has integer coordinates $(x_0, y_0) = (0, 4)$ with $y_0^2 \mid D$, but $P \notin \operatorname{Tors} E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$.

Example 1.13.10. Let's revisit the example of 1.2.B. We are interested in studying the curves $E : y^2 = x^3 - 432\alpha^2$ for various α. Let's study two cases:

(a) When $\alpha = 1$, we're looking at the curve $y^2 = x^3 - 432$ corresponding to Fermat's Last Theorem for $n = 3$. This has discriminant $D = -2^8 3^9$. Let's apply 1.13.7. Clearly, there are no solutions with $y = 0$. The condition $y^2 \mid D$ gives us lots of possibilities, but only finitely many. It's easy to check them on a computer, and from doing this we get easily that the only values that work are $y = \pm 36$, which correspond to $x = 12$. Therefore, $\operatorname{Tors} E(\mathbb{Q}) = \{\mathscr{O}, (12, \pm 36)\} \cong_{\mathsf{Ab}} \mathbb{Z}/3$. In particular, to prove Fermat's Last Theorem for $n = 3$, it only remains to show that E has no points of infinite order, which as we shall see below is equivalent to $\operatorname{rank} E = 0$. This is what we'll prove later.

(b) When $\alpha = 2$, we're looking at the curve $y^2 = x^3 - 2^6 3^3$. (You might be interested in studying this curve if you care about cubes of integers in arithmetic progression; this is going to be an exercise on the last sheet.) We know from the theory of admissible changes of coordinates that we may change the coefficient c in the equation by a sixth power without affecting the isomorphism class of the curve, so we might as well work with the curve $E : y^2 = x^3 - 27$ instead. The advantage of working with this curve is that it still has integer Weierstrass coefficients, although much smaller, and so 1.13.7 still applies. There *is* a solution $(3, 0)$ with $y = 0$. For solutions with $y \neq 0$, we have $y^2 \mid D = -3^9$, giving us the possibilities $y = \pm 3^i$ for $i = 0, 1, 2, 3, 4$. Checking these options by hand (or by using a computer), we see that none of these options work, and hence $\operatorname{Tors} E(\mathbb{Q}) = \{\mathscr{O}, (3, 0)\} \cong_{\mathsf{Ab}} \mathbb{Z}/2$. Again, it remains to investigate the rank of E, which we will do later.

We'll prove 1.13.7 next time.