Nagell-Lutz, quickly.

Abstract.

In any first course in elliptic curves one proves the Nagell-Lutz theorem, which gives a way to determine the torsion subgroup of an elliptic curve over $\mathbb{Q}$. The "usual" proof, which is Lutz's from her thesis under Weil, has its pedagogical benefits, namely it leads one to face certain subgroups of the rational points determined by p-power congruences. Still, there is also a pedagogical benefit to a fast proof.

In this note we give such a fast proof.

1 Introduction.

The point of this note is to give a quick proof of the following theorem, which was proved by Nagell in [4] and Lutz in her thesis under Weil in [1].[1]

Theorem 1.1 (Nagell-Lutz). *Let $A, B \in \mathbb{Z}$ with $\Delta_{A,B} := -16 \cdot (4A^3 + 27B^2) \neq 0$. Let E be the elliptic curve over $\mathbb{Q}$ given by the affine Weierstrass equation $y^2 = x^3 + Ax + B$. Let (x, y) be a nonidentity $\mathbb{Q}$-point of finite order under the addition law on E. Then:*

- *$x, y \in \mathbb{Z}$, and*
- *either $y = 0$ or else $y^2 \mid \Delta_{A,B}$.*

This theorem allows one to find the points of finite order on such an elliptic curve $E/\mathbb{Q}$ "by hand" (— if the coefficients are small enough!) and consequently features in a standard introductory course on elliptic curves. A classic work tailored for exactly such introductory courses is Silverman-Tate's [6], in which a "bare-hands" proof of this theorem is given on pages $47 - 56$ (with the divisibility $y^2 \mid \Delta_{A,B}$ left as Exercise 2.11 of that chapter).

Unfortunately when I began learning the subject I simply could not get myself to understand that (or any other) proof! It involves a change of variables and some calculations which one can motivate a number of ways, and which were presumably inspired by the very natural, and arguably standard, argument using formal groups — but I wanted to avoid invoking such a structure, even behind the scenes, to prove such a concrete theorem! So the *true* purpose of this note is to give a very short "bare-hands" proof that might perhaps satisfy someone as confused as I was then!

The argument is essentially as follows. First off, a standard point: if $y^2 = x^3 +$ (lower degree and in $\mathbb{Z}[x]$) and x and y are rational, then the denominator

[1] Using the notion of canonical height it is "obvious" that the set of finite-order rational points on an elliptic curve over $\mathbb{Q}$ is computable in finite time, but this theorem gives another way. Without using the phrase "canonical height", said argument goes as follows: the x-coordinate of $2 \cdot (x, y)$ is $\frac{(3x^2+A)^2}{4\cdot(x^3+Ax+B)} - 2x = \frac{x^4-2A\cdot x^2-8B\cdot x+A^2}{4\cdot(x^3+Ax+B)}$, and the resultant of the numerator and denominator polynomials is $(-16\cdot(4A^3+27B^2))^2 = \Delta_{A,B}^2$. It follows that if $x, y \in \mathbb{Q}$ and either the numerator or denominator of $x \in \mathbb{Q}$ is very large, then the either the numerator or denominator of $2 \cdot (x, y)$ is much larger (since the resultant bounds cancellation), that of $4 \cdot (x, y)$ yet larger, etc. But if $P \in E(\mathbb{Q})_{\text{tors.}}$, then $\{2^n \cdot P\}_{n\in\mathbb{N}}$ is a finite set, and so the numerators and denominators of the points $2^n \cdot P$ remain bounded as $n \to \infty$.

of x is forced to be a square (and that of y is the corresponding cube). Now if $(x, y) \in E(\mathbb{Q})$ has order n, multiply so that without loss of generality[2] $n = p$ is prime. Since the identity point is at infinity, having order p means that when one plugs $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ into the formula for multiplication by p, the polynomial in the denominator of the formula must vanish. Looking at the formula for multiplication by p, it turns out the relevant polynomial is either $4y^2$ (when $p = 2$), so in that case $y = 0$ so $x^3 + Ax + B = 0$ and we are done, or $p > 2$ and it is of the form $\varphi_p(x)^2$ where φ_p has leading coefficient p. But that means $p \cdot \mathrm{num.}(x)^{\deg \varphi_p} \equiv 0 \pmod{\mathrm{denom.}(x)}$, so the denominator of x — a square! — divides p, and we are again done.

But first an interlude explaining why one might want to be able to find all finite-order rational points at all.

2 Motivation.

Let $A, B \in \mathbb{Z}$ with $\Delta_{A,B} := -16 \cdot (4A^3 + 27B^2) \neq 0$. Let $E_{A,B} : y^2 = x^3 + Ax + B$, an elliptic curve over $\mathbb{Q}$.[3] As such there is an addition law on $E_{A,B}(\mathbb{Q}) = \{\infty\} \cup \{(x, y) : x, y \in \mathbb{Q}, y^2 = x^3 + Ax + B\}$ making it into an abelian group. It was a "conjecture"[4] of Poincaré and is a theorem of Mordell [3] (arising from his study [2] of integer solutions of $y^2 = x^3 + k$, and generalized by Weil [7]) that $E_{A,B}(\mathbb{Q})$ is finitely generated.

This exactly says that there is a uniquely determined nonnegative integer $r \in \mathbb{N}$, the *rank*, and a uniquely determined finite subgroup $E_{A,B}(\mathbb{Q})_{\mathrm{tors.}} \subseteq E_{A,B}(\mathbb{Q})$, the *(rational) torsion subgroup*, such that $E_{A,B}(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{A,B}(\mathbb{Q})_{\mathrm{tors.}}$ as abelian groups.

The map $E \mapsto E(\mathbb{Q})$, thought of as $(A, B) \mapsto E_{A,B}(\mathbb{Q})$, taking an elliptic curve over $\mathbb{Q}$ to its group of rational points, is the fundamental object of study in the subject. The immediate question is: given (A, B), how can one compute $E_{A,B}(\mathbb{Q})$?

It is clear this is a fundamental question, and it is arguably *the* fundamental question in the subject. (Un)fortunately for modern mathematics, it is also wide open — indeed it is in our view one of the main "points" of the Birch and Swinnerton-Dyer conjecture.

The issue is that the function $(A, B) \mapsto r$, taking an elliptic curve to its rank

---

[2]This "without loss of generality" hides something, namely that if a multiple of a point is integral then it was, too, which we will quickly prove later as well (see Lemma 3.2).

[3]The pair (A, B) is uniquely determined given the elliptic curve $E_{A,B}/\mathbb{Q}$ so long as we impose that there is no prime p such that $p^4 | A$ and $p^6 | B$ (after all, we could introduce such powers by the scaling $(x, y) \mapsto (p^{-2} \cdot x, p^{-3} \cdot y)$).

[4]Poincaré asserted it without even indicating that there was something to be proved on page 171 of [5]:

> "On peut se proposer de choisir les arguments $\alpha_0, \ldots, \alpha_q$ de telle façon que $[\mathrm{span}_{\mathbb{Z}}(\{\alpha_0, \ldots, \alpha_q\})]$ comprenne tous les points rationnels de la cubique. …Il est clair que l'on peut choisir d'une infinité de manières le système des points rationnels fondamentaux."

over $\mathbb{Q}$, is not even known to be computable by a Turing machine (i.e. "by a computer program"). Notice that we are not worrying about efficiency at all![5] In fact one would solve the classic congruent number problem if one could just give a method to decide in finite time if a given curve in the special form $y^2 = x^3 - n^2 x$ has rank exactly 0.

Hopefully the above indication of our ignorance makes it clear that the fact that we are able to compute the other aforementioned invariant $(A, B) \mapsto E_{A,B}(\mathbb{Q})_{\mathrm{tors.}}$ of the abelian group $E_{A,B}(\mathbb{Q})$ is interesting. And so let us return to the point of this note.

3 Some preliminaries about division polynomials.

Before we give the proof let us define the division polynomials, which we think of as giving the denominators of the multiplication-by-n map on E — or alternatively as having roots exactly the n-torsion points of E.

First, the x-coordinate map $(x, y) \mapsto x$ is invariant under negating the starting point — after all, the negative (in the group law) of a point $(x, y) \in E$ is $(x, -y)$, which has the same x-coordinate. This means that the x-coordinate of $n \cdot (x, y) := \underbrace{(x, y) + \cdots + (x, y)}_{n \text{ times}}$ (the symbol "+" referring to the group law of E) is a rational function in x only — since it is unchanged when replacing y by $-y$ and x determines $y^2 = x^3 + Ax + B =: f(x)$. So this x-coordinate of $n \cdot (x, y)$ is a rational function in x, with some denominator. What is the denominator?

Well, the x-coordinate of the sum of $P = (x, y)$ and $Q = (X, Y)$ is

$$x(P + Q) = \frac{(Y - y)^2}{(X - x)^2} - (X + x),$$

and so, limiting $Q \to P$, we find that

$$\begin{aligned} x(2P) &= \lim_{X \to x} \left(\frac{\left(\sqrt{f(X)} - \sqrt{f(x)}\right)^2}{(X - x)^2} - 2(X + x) \right) = \frac{f'(x)^2}{4f(x)} - 2x \\ &= \frac{x^4 - 2A \cdot x^2 + 8B \cdot x + A^2}{4 \cdot (x^3 + Ax + B)}. \end{aligned}$$

Continuing this procedure inductively gives the following theorem. Let $\varphi_n \in \mathbb{Z}[x, y, A, B]/(y^2 - f(x))$ be such that

$$\begin{aligned} &\varphi_0(x, y) := 0, \qquad \varphi_1(x, y) := 1, \qquad \varphi_2(x, y) := 2y, \\ &\varphi_3(x, y) := 3 \cdot x^4 + 6A \cdot x^2 + 12B \cdot x - A^2, \\ &\varphi_4(x, y) := 4y \cdot (x^6 + 5A \cdot x^4 + 20B \cdot x^3 - 5A^2 \cdot x^2 - 4AB \cdot x - 8B^2 - A^3), \end{aligned}$$

[5]— e.g. we are not demanding the computation end in time polynomial in the length of the input (A, B) in binary — we just want one program that returns a correct answer on each given curve after computing for however finitely long it needs!

and such that

$$\varphi_{2n+1}(x,y) = \varphi_{n+2}(x,y)\cdot\varphi_n(x,y)^3 - \varphi_{n-1}(x,y)\cdot\varphi_{n+1}(x,y),$$
$$\varphi_{2n}(x,y) = \frac{\varphi_n(x,y)}{2y}\cdot(\varphi_{n+2}(x,y)\cdot\varphi_{n-1}(x,y)^2 - \varphi_{n-2}(x,y)\cdot\varphi_{n+1}(x,y)^2).$$

Notice from the recurrence that when n is odd $\varphi_n(x,y)$ is a polynomial in x only, whereas when n is even $\varphi_n(x,y)$ is y times a polynomial in x. Also from the recurrence it follows that (using $y^2 = x^3 + Ax + B$) $\varphi_n(x,y)^2$, which is a polynomial in x only, is of degree $n^2 - 1$ in x — and if we further give x degree 1, y degree $\frac{3}{2}$, A degree 2, and B degree 3, then in fact $\varphi_n(x,y)$ is homogeneous of degree $\frac{n^2-1}{2}$ as an element of $\mathbb{Z}[x,y,A,B]/(y^2 - f(x))$. Now for the theorem.

Theorem 3.1. *The coordinates of $n\cdot(x,y)$ are (μ_n,ν_n) with*

$$\mu_n := \frac{x\cdot\varphi_n(x,y)^2 - \varphi_{n-1}(x,y)\cdot\varphi_{n+1}(x,y)}{\varphi_n(x,y)^2},$$
$$\nu_n := \frac{\varphi_{n+2}(x,y)\cdot\varphi_{n-1}(x,y)^2 - \varphi_{n-2}(x,y)\cdot\varphi_{n+1}(x,y)^2}{4y\cdot\varphi_n(x,y)^3}.$$

Notice that, writing $\mu_n =: \frac{\mathrm{num.}_n(x,y)}{\mathrm{den.}_n(x,y)}$ — thus $\mathrm{den.}_n(x,y) = \varphi_n(x,y)^2$ — $\mathrm{num.}_n(x,y), \mathrm{den.}_n(x,y) \in \mathbb{Z}[x,A,B]$, i.e. both the numerator and denominator polynomials in the formula for μ_n only depend on x (again using $y^2 = x^3 + Ax + B$). Moreover, $\mathrm{num.}_n(x,y)$ and $\mathrm{den.}_n(x,y)$ are respectively of degree n^2 and $n^2 - 1$ in x, and $\mathrm{num.}_n(x,y)$ is monic in x while $\mathrm{den.}_n(x,y)$ has leading coefficient in x equal to n^2.[6]

From these formulas we derive the principle that "if a multiple of a point is integral, then the point itself must have been integral to start with".

Lemma 3.2. *Let $A,B \in \mathbb{Z}$ with $\Delta_{A,B} \neq 0$. Let $n \in \mathbb{Z}^+$. Let $(x,y) \in E_{A,B}(\mathbb{Q})$ be such that $n\cdot(x,y)$ is integral, i.e. $n\cdot(x,y) = (X,Y)$ with $X,Y \in \mathbb{Z}$. Then: $x,y \in \mathbb{Z}$.*

Proof. Write $x =: \frac{s}{t}$ in lowest terms. By Theorem 3.1, $X = \frac{s^{n^2} + (\in t\cdot\mathbb{Z})}{(\in t\cdot\mathbb{Z})}$ since $\mathrm{num.}_n(x,y)$ is monic and of strictly larger degree than $\mathrm{den.}_n(x,y)$. Since $(s,t) = 1$, this cannot be an integer unless $t = 1$. Since $y^2 = x^3 + Ax + B$, it follows that $y \in \mathbb{Z}$ too. □

Actually we can be more precise about the denominators of rational points on E, as follows.

Lemma 3.3. *Let $A,B \in \mathbb{Z}$. Let $x,y \in \mathbb{Q}$ be such that $y^2 = x^3 + Ax + B$. Then: there is a $d \in \mathbb{Z}^+$ such that the denominator of x is d^2, and that of y is d^3.*

Proof. Write $x =: \frac{s}{t}$ and $y =: \frac{u}{v}$ in lowest terms. Then on clearing denominators in $y^2 = x^3 + Ax + B$ we get that $t^3\cdot u^2 = v^2\cdot(s^3 + Ast^2 + Bt^3)$. Hence t^3 divides v^2, and v^2 divides t^3, so $t^3 = v^2$ and we are done. □

[6] The fact that $\deg_x \mathrm{den.}_n(x,y) = n^2 - 1$ is sensible because from the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/(\text{lattice})$ we know that there are exactly n^2 n-torsion points on E, and the nonidentity n-torsion points are the roots of $\mathrm{den.}_n(x,y)$ (since being n-torsion means that $n\cdot(x,y) = \infty$).

4 Proof of the Nagell-Lutz theorem.

It is finally time for the proof.

Proof of Theorem 1.1. If we can show the first claim for all torsion points, then the second follows too, because of the following. If (x, y) is torsion then so is $2 \cdot (x, y)$, and we already saw that the x-coordinate of $2 \cdot (x, y)$ is $\frac{f'(x)^2}{4f(x)} - 2x$. Hence it is either ∞, in which case $y^2 = f(x) = 0$, or else assuming the first claim we get that $f(x) \mid f'(x)^2$. But there is an explicit $\mathbb{Z}[x, A, B]$-linear combination[7] of $f(x)$ and $f'(x)^2$ which is equal to $\Delta_{A,B}$, so it follows that $y^2 = f(x) \mid \Delta_{A,B}$, too.

So let us show the first claim. Let m be the order of (x, y) and $p \mid m$ a prime. By Lemma 3.2 it suffices to show the first claim for $\frac{m}{p} \cdot (x, y)$, i.e. to assume without loss of generality that (x, y) has prime order p. Hence $\mathrm{den.}_p(x, y) = 0$, so $\varphi_p(x, y) = 0$. If $p = 2$ this means $y = 0$, i.e. $x^3 + Ax + B = 0$, so $x \in \mathbb{Z}$. Else p is odd, so write via Lemma 3.3 $x =: \frac{s}{d^2}$ in lowest terms and clear denominators to get the equation $p \cdot s^{\frac{p^2-1}{2}} + (\in d^2 \cdot \mathbb{Z}) = 0$. Thus $d^2 \mid p$, so $d = 1$. □

References.

[1] Élisabeth Lutz. Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques. *J. Reine Angew. Math.*, 177:238–247, 1937.

[2] L. J. Mordell. Indeterminate equations of the third and fourth degrees. *Quart. J.*, 45:170–186, 1914.

[3] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Philos. Soc.*, 21:179–192, 1922.

[4] Trygve Nagell. Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre. Skr. Norske Vid.-Akad., Oslo 1935, No. 1, 1-25, 1935.

[5] H. Poincaré. Sur les propriétés arithmétiques des courbes algébriques. *Journal de Mathématiques Pures et Appliquées. 5. Série*, 7:161–233, 1901.

[6] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[7] André Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52(1):281–315, 1929.

[7] The discriminant of a cubic $\sum_{i=0}^{3} c_i \cdot X^{3-i} Y^i$ is homogeneous of degree $4 = 2 \cdot 3 - 2$ in the c_i, invariant under $(X, Y) \mapsto (t^{-1} \cdot X, t \cdot Y)$, and vanishes when $c_3 = c_2 = 0$, so it is a $\mathbb{Z}[\{c_i\}_{i=0}^{3}]$-linear combination of c_3 and c_2^2. Explicitly, it is $c_1^2 c_2^2 - 4 \cdot c_0 c_2^2 - 4 \cdot c_1^2 c_3 - 27 \cdot c_0^2 c_3^2 + 18 \cdot c_0 c_1 c_2 c_3$.