Points of finite order and applications to the Nagell-Lutz Theorem

Daisy Gomez

May 2020

1 Introduction

The main topic of interest here is about points of finite order on elliptic curves. This field of study encompasses different areas of mathematics such as number theory, algebra, and geometry, which gives us an opportunity to see how these distinct fields are used together. In order to gain a good grasp of points of finite order, we should go over a few essential concepts.
In the most general terms, we define the equation for a cubic to be

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

However, for simplicity, we should familiarize ourselves with the Weierstrass Normal Form. After some manipulation, we find that a cubic in Weierstrass normal form is the following:

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

We will use this form for the cubic from this point forward. It is important to note that $f(x)$ can have either one or three real roots. We will let $C(\mathbb{Q})$ be the set of rational points on $f(x)$, $C(\mathbb{R})$ be the set of real points, and $C(\mathbb{C})$ the set of complex points. Then the following holds

$$\{O\} \subset C(\mathbb{Q}) \subset C(\mathbb{R}) \subset C(\mathbb{C}).$$

We should keep this in mind when we prove the theorem and deal with complex roots. Next we will go over the group law we will be working and some basic order principles.

2 Group Law and Order

We are interested in finding solutions of cubic curves. However, keep in mind that if we were only working towards the Nagell-Lutz theorem, the only points of interest would be rational points. Suppose we have two arbitrary points P and Q on the cubic curve. One can find a third point on the curve by connecting P and Q with a line. It is easy to tell that the line will intersect the cubic at a third point, which is known as a composition law with the following properties:

$$\text{connecting a point } P \text{ to a point } Q \text{ gives us } P * Q.$$

It should also be known that there is a more trivial case. If we only have one point P to start with, then we can use the same composition law as we draw a tangent line through P (we think of this as a line going through P and P) to get a third point, $P * P$. Another important thing to know is that the projective plane in which we are using this composition law on a cubic has a *point at infinity* O. Another rule, denoted with $+$, is made if we use O as the identity element to make this a group law:

$$\begin{gathered}\text{connecting } P * Q \text{ to } O \text{ gives us } O * (P * Q)\\ \Rightarrow P + Q = O * (P * Q).\end{gathered}$$

Also,

$$P + O = P$$

because if we join P to O, we get $P * O$ as the third point of intersection. Now if we join $P * O$ to O, the third intersection point is just P. In order for $+$ to be a group, it must satisfy associativity. We will not verify this now, but it turns out that $+$ is associative, and thus, it is a group so we call it the group law.

Next is the concept of order. We are only interested in elements of finite order for now. We say that an element P has order m if

$$mP = P_1 + P_2 + ... + P_m = O,$$

but $m'P \neq O$ for integers $1 \leq m' \leq m$. If such an m exists, then P is said to have finite order.

Now we move forward to take a look at the theorem of points of order 2 and 3.

Theorem 2.1 (Points of order 2 and 3)**.** *Let C be a non-singular cubic curve such that*

$$C\colon\ y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Then the following hold:

(a) A point P = (x, y) = O has order two if and only if y = 0.

(b) The curve C has exactly four points of order dividing two. These four points form a group that is a product of two cyclic groups of order two.

(c) A point P = (x, y) = O has order three if and only if x is a root of the polynomial

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$$

(d) The curve C has exactly 9 points of order dividing 3. These 9 points form a group that is the product of two cyclic groups of order 3.

Proof:

(a) For the forward direction, we will suppose that P = (x,y) $\neq O$ has order two. This means that

$$\begin{gathered}2P = O\\ P = -P\\ (x,\ y) = (x,\ -y) \Rightarrow y = 0.\end{gathered}$$

For the backward direction, we will suppose that P = (x,y) $\neq O$ such that y = 0. Then

$$P = (x,0) = P \Rightarrow 2P = O.$$

Hence, P has order two.

(b) We already know that C has four points of order dividing two from part (a) and because C is a quartic function. We will display these in the following set

$$\{O,\ P_1,\ P_2,\ P_3\}.$$

Note that O serves as the identity that always has order dividing two. From part (a), we observe that

$$P_1 = (x_1, 0),$$
$$P_2 = (x_2, 0),$$
$$P_3 = (x_3, 0),$$

These are complex roots of the Weierstrass cubic, $f(x)$. It is important to know here that if we allow complex coordinates, then there are exactly three points of order two. Now we check if it is a product of two cyclic groups of order two. Observe that the three points are colinear because they are on the x-axis. Hence, by the group law, we can add two of the three points and it will equal the third. This implies that the set is a Four Group, which is indeed a product of two cyclic groups of order 2.
Note that if we are talking about points with rational coordinates, there are three possibilities: it is either the Four Group, cyclic of order two, or trivial, depending on whether $f(x)$ has three, one, or zero rational roots. If we use real coordinates, it is either the Four Group or a cyclic group of order two, depending on whether $f(x)$ has three real roots or one real root.

(c) Note: there is a duplication formula used as an iterative method to find x-coordinate of $2P$ defined as

$$x = \tfrac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

Suppose that $P = (x,y) \neq O$ has order three. Then

$$3P = O \Rightarrow 2P = -P.$$

Thus, a point of order three will satisfy the above equality:

$$x(2P) = x(-P) = x(P).$$

Observe that if $P \neq O$ satisfies $x(2P) = x(P)$, then $2P = -P$ and $2P = P$. This leaves us with either $P = O$ or $3P = O$. Therefore, the points of order three are exactly the points that satisfy $x(2P) = x(P)$. Now in order to find the the points satisfying the duplication formula, we set x equal to the duplication formula:

$$x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

After cross multiplying, we get

$$4x^4 + 4ax^3 + 4bx^2 + 4cx = x^4 - 2bx^2 - 8cx + b^2 - 4ac$$
$$3x^4 + 4ax^3 + 6bx^2 + 12cx - b^2 + 4ac = 0$$

Hence, x must satisfy $\psi_3(x)$ for P to have order three.

(d) Note: C is non-singular if $f(x)$ and $f'(x)$ have no common complex roots. We will use this statement for proving (d).
From part (c), we know

$$\begin{aligned} x(2P) &= \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} \\ &= \frac{f'(x)^2}{4f(x)} - a - 2x. \end{aligned}$$

We also know that $\psi_3(x) = 2f(x)f''(x)$ - $f'(x)^2$. To check that the quartic $\psi_3(x)$ has four distinct roots, we need to show that $\psi_3(x)$ and $\psi_3'(x)$ have no common roots. However,

$$\psi_3'(x) = 2f(x)f'''(x) = 12f(x).$$

This means that if there were common roots between $\psi_3(x)$ and $\psi_3'(x)$, then they would satisfy both $2f(x)f''(x)$ - $f'(x)^2$ and $12f(x)$. This implies that they wold also be common roots of $f(x)$ and $f'(x)$, but this contradicts the fact that C is non-singular because we know that $f(x)$ and $f'(x)$ cannot share complex roots. Hence, $\psi_3(x)$ has four complex and distinct roots.

Now, we let P_1, P_2, and P_3 be these four complex roots of C. For each P_i, we let $r_i = \sqrt{f(P_i)}$. Then, from part (c), we can create the following set of points of order three

$$\{(P_1 \pm r_1), (P_1 \pm r_1), (P_1 \pm r_1), (P_1 \pm r_1)\}.$$

We observe that there are 8 total points, in addition to O, which gives us a total of 9 points. The only group with 9 elements such that every element has order dividing three is the product of two cyclic groups of order three. ■

After some further evaluation, it is found that if a point has finite order, then it has integer coordinates and is used in the Nagell-Lutz theorem.

Theorem 2.2 (Nagell-Lutz Theorem)**.** *Let*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, c, and let D be the discriminant of the cubic polynomial

$$D = 4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Let $P = (x, y)$ be a rational point of finite order. Then x and y are integers, and either y = 0, in which case P has order two, or else y divides D.

We will not prove this theorem, but now we have the basic tools necessary to begin.