Points of Finite Order

Alex Tao

23 June 2008

1 Points of Order Two and Three

If G is a group with respect to multiplication and g is an element of G then the *order of* g is the minimum positive integer α such that $g^\alpha = 1$ is satisfied. Similarly for a group with respect to addition, then the element P in the group has *order* m if m is the minimum positive integer satisfying $mP = \mathcal{O}$, where $\mathcal{O}$ is the identity element. If such m exists for P, then P is an element of *finite order*, if not then it has *infinite order*.

If we take the group of rational points on a non-singular elliptic curve

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

we could assign an order for each element P in the group where $\mathcal{O}$, the point at infinity is our identity element. If a point P has order 2, then we can write $2P = \mathcal{O}$ and the equivalent condition will be $P = -P$. From the previous set of notes we know that if $P = (x, y)$, then $-P = (x, -y)$. If we were to have $P = -P$, we must have the points lying on the x-axis where $y = 0$. Solving the cubic polynomial in x, we will find exactly 3 (complex) points of order 2 since non-singular ensures no repeated roots.

In the case of 3 real distinct roots, the complete set of points which satisfies $2P = \mathcal{O}$ consists of $\{\mathcal{O}, P_1, P_2, P_3\}$. This set forms the subgroup $C_2 \times C_2$, the *Four Group* in the group of points on the curve. Working with different fields may yield different groups. For complex numbers, we are guaranteed to have the Four Group; in real numbers, we either have the Four Group or the cyclic group of order two depending on whether there are 1 or 3 roots to the cubic; in the field of rational numbers, we can have either the Four Group, cyclic group of order 2, or trivial group in the respective cases of three, one, or no rational roots.

The points of order three satisfies $3P = \mathcal{O}$ and equivalently $2P = -P$. Looking at the x coordinate of points of order three then, $x(2P) = x(-P) = x(P)$. Conversely, if $x(2P) = x(P)$ is satisfied for some $P \neq \mathcal{O}$, it will be true that $2P = \pm P$. But $2P = P \Rightarrow P = \mathcal{O}$, so $2P = -P$ or $3P = \mathcal{O}$.

It is possible to modify the duplication formula to find the points of order three efficiently. Let $P = (x, y)$ then writing

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

then rearranging,

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

we have proved the (c) of the below proposition.

Before the proposition, let me first state an equivalent condition for singular points. If we write our equation of curve by $F(x, y) - y^2 - f(x) = 0$ and take partial derivatives,

$$\frac{\partial F}{\partial x} = -f'(x), \qquad \frac{\partial F}{\partial y} = 2y$$

then a singular point (x_0, y_0) implies $f'(x_0)$ and $y_0 = 0$. But by the equation of curve, $y = 0 \Rightarrow f(x_0) = 0$. x_0 is a root of $f(x)$ and $f'(x)$ and hence is a double root of $f(x)$. We now have the relation that if a there is a singular point on a curve, there there will exist some x_0 where $f(x_0) = f'(x_0) = 0$.

Points of Order Two and Three

Let C be the non-singular cubic curve

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

*Note that C is non-singular provided $f(x)$ and $f'(x)$ have no common complex roots.
(a) A point $P = (x, y) \neq \mathcal{O}$ on C has order two if and only if $y = 0$.
(b) C has exactly four points of order dividing 2. These four points form a group which is a product of two cyclic groups of order two.
(c) A point $P = (x, y) \neq \mathcal{O}$ on C 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) C has exactly nine points of order dividing 3. These nine points form a group which is a product of two cyclic groups of order three.

Proof

(a), (b) and (c) has been proved above.
Proof of (d):
Using the regular formula for additional of points,

$$x(2P) = \left[\frac{f'(x)}{2y}\right]^2 - a - x - x = \frac{(f'(x))^2}{4y^2} - a - 2x = \frac{f'^2(x)}{4f(x)} - a - 2x$$
$$= x$$

Rewriting the last equality

$$2f(x)(6x + 2a) - f'^2(x) = 0,$$

notice that we can write $f''(x) = 6x + a$, we can finally write $\psi_3(x)$ in the form

$$\psi_3(x) = 2f(x)f''(x) - f'^2(x).$$

Claim that $\psi_3(x)$ has four distinct (complex) roots.
It suffices to check that $\psi_3(x)$ and $\psi_3'(x)$ has no common roots.

$$\psi_3'(x) = 2f'(x)f''(x) + 2f(x)f'''(x) - 2f'(x)f''(x) = 2f(x)f'''(x) = 12f(x)$$

since $f'''(x) = 6$.
If there is a common root x_0 of $\psi_3(x)$ and $\psi_3'(x)$, then x_0 is a common root of

$$2f(x)f''(x) - f'^2(x) \quad (*) \qquad \text{and} \qquad 12f(x) \quad (**)$$

so $f(x_0) = 0 \Rightarrow f'(x_0) = 0$ contradicting that C is a non-singular curve and so $\psi_3(x)$ has four distinct roots.

For each x_i as a root of $\psi_3(x)$, there will be a pair $\pm f(x_i)$ satisfying the equation of curve totalling up with 8 distinct points. It should be noted that we are sure that $f(x_i) \neq 0$ for each point since it is a point of order two. So including $\mathcal{O}$, there are exactly nine points of order which divides 3. This group with nine elements must be $C_3 \times C_3$ since order of every element divides 3.

□

Geometrically, the points of order three are inflection points of the cubic. We have been working with complex numbers, but working with real and rational numbers will give different groups. These possibilities will be discussed later.

2 Real and Complex on Cubic Curves

Real points on the general cubic

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

either forms one connected component or 2 connected components depending on whether the cubic has one or three real roots. Apart from real coordinates, the curve also defines the set of complex coordinates which satisfy the cubic. Also, the set of rational coordinates lie inside the set of real coordinates. If we let the point at infinity be in the all of the discussed sets, which are subgroups of the complete set of points, we have the nested subgroups

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

The study of real and complex points will involve work in analysis.

Since the addition of real points on the curve is continuous, it forms a one-dimensional Lie group. This set is in fact compact although it contains *one* point at infinity. There is only one such connected group up to isomorphism, the group of rotations of a circle; the multiplicative group of complex numbers of absolute value one. From this isomorphism, we can immediately identify the set of real points of finite order as the roots of unity. For some integer m, the set of points of order dividing m will form the cyclic group of order m; explicitly

$$\left\{1, e^{2\pi i/m}, e^{4\pi i/m}, ..., e^{2(m-1)\pi i/m}\right\}.$$

This holds if we are considering the points in a single *connected* set $C(\mathbb{R})$.

If the curve consists of two components, then the group $C(\mathbb{R})$ is the direct product of the circle group with a group of order two. There will be two possibilities for the set of points with order dividing m. For odd m, we get a cyclic group of order m; for even m, we get a direct product of a cyclic group of order two and a cyclic group of order $\frac{1}{2}m$.

In the case for real points of order dividing three, we have the cyclic group of order three. But we have showed there exists eight points of order three hence not all points of order three are real and also not rational. This implies the quartic $\psi_3(x)$ in the previous section should have exactly one real root in x and two corresponding real y's to account for the two real points of order three.

Now consider working in the complex field $\mathbb{C}$ for the equation

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

Using the transformations $x \to x - \frac{1}{3}a$ then followed by $x \to 4x$ and $y \to 4y$, we change the form of the elliptic equation into the so called *classical* form

$$y^2 = 4x^3 - g_2 - g_3.$$

If this equation contains two distinct roots, it is possible to find two complex numbers ω_1, ω_2 we will call *periods*. The periods are $\mathbb{R}$-linear independent so that ω_1 is not a real multiple of ω_2. A subgroup of the complex points, L, could be formed by taking $\mathbb{Z}$-linear combinations of ω_1 and ω_2:

$$L = \{n_1\omega_1 + n_2\omega_2 \ ; \ n_1, n_2 \in \mathbb{Z}\}$$

L is called a *lattice*. The choice of ω_1 and ω_2 is not unique, but in fact g_2 and g_3 determines the L as a group uniquely. Conversely, it is possible to find g_2 and g_3 from L via the formulas:

$$g_2 = 60 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^4}, \qquad g_3 = 140 \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^6}$$

Equipped with the periods, we can define the regular function, *Weierstrass $\wp(u)$ function*

$$\wp(u) = \frac{1}{u^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right).$$

The $\wp$-function has poles at every point in L, so the lattice L actually forms a lattice of the poles of the $\wp$-function. $\wp$ is what we call a *doubly periodic function* because it satisfies

$$\wp(u + \omega_1) = \wp(u + \omega_2) = \wp(u) \text{ for all complex numbers } u.$$

It also follows that for any $\omega \in L$, $\wp(u + \omega) = \wp(u)$ is satisfied for all $u \in \mathbb{C}$. To conclude, this is very much like the periodic trigonometric functions $f(x) = \sin x$ and $f(x) = \cos x$ with period of 2π where 2π expresses the "interval distance" on the real line for the function $f(x)$ to repeat itself periodically. In the doubly periodic case on the complex plane, instead of "distances", we have "areas" defined by our complex periods ω_1 and ω_2. The "areas" are parallelograms with parallel sides consisting of ω_1 and ω_2 which will define how our doubly periodic function $\wp$ behaves throughout the complex plane.

This doubly periodic function $\wp$ satisfies the differential equation

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3, \qquad \text{where } \wp = \frac{d\wp}{du}.$$

In analogy to the elliptic curve equation, for every complex number u, we have a complex point P defined by

$$P(u) = (\wp(u), \wp'(u))$$

and we obtain a map from the complex u plane to $C(\mathbb{C})$. The obvious choice to send points lying in L is to $\mathcal{O}$ since they both lie at infinity.

To study the domain of the map, we only need to look at the points of one of the closed period parallelograms. The image of the map is the complete set of complex points satisfying $y^2 = 4x^3 - g_2x - g_2$. The complex plane is evidently not a one-to-one map onto the curve but the period parallelogram *does* map one-to-one onto the complex points of the curve. The map $u \mapsto P(u)$ is in fact a homomorphism, that is

$$P(u_1 + u_2) = P(u_1) + P(u_2)$$

where $u_1 + u_2$ is our usual addition of complex numbers and $P(u_1) + P(u_2)$ is the addition group law on cubic curves. The kernel of the map is the points which maps onto the identity element $\mathcal{O}$ and is exactly the points in the lattice L. To express exactly one of these parallelograms mathematically, we can write it as the factor group $\mathbb{C}/L$. So we have the relation that $\mathbb{C}/L$

is isomorphic to the group of complex points on the curve. If we observe the parallelogram closely, each pair of parallel sides is essentially the "same" side and this topologically forms a torus. This is because the intervals ω_1 and ω_2 each exhibit properties of a circle group so the points u defined by linear combinations of the pairs ω_1, ω_2

$$u = \lambda_1\omega_1 + \lambda_2\omega_2, \qquad \text{for } \lambda_1, \lambda_2 \in [0, 1]$$

are in fact elements of the direct product of two circle groups, a torus. Finally, we can say that the group of complex points on our curve is topologically a torus.

Now we return to the question of finding complex points of finite order lying on an elliptic curve. On the torus we could describe the order of a point as, "if h is a path from $\mathcal{O}$ to some point p on the torus, the order of p is the number of consecutive h-paths we need to take to return to $\mathcal{O}$". Conversely, to find an element of order of some given integer m, we are essentially trying to find a "straight" continuous for path h on the torus so that if the point $\mathcal{O}$ is reached if path is repeated n times for some n dividing m.

Take the example $m = 2$. There exist three such paths, taking the semicircular path around the small circle, the big circle, or the addition of both. Of course this can be interpreted with a more algebraic approach. We would like to find some $u \notin L$ such that $2u \in L$, these points are $\frac{w_1}{2}$, $\frac{w_2}{2}$ and $\frac{w_1+w_2}{2}$. Generally, to find the points u with ordering dividing m, we look for points in the period parallelogram so that $mu \in L$. The complex points of order dividing m generally forms a group of order m^2.

Notes:
If we decide to work in any other subfield $\mathbb{F}$ of $\mathbb{C}$, then the $\mathbb{F}$-valued solutions in the $\mathbb{F}$-cubic forms a subgroup of the complex solutions $C(\mathbb{C})$. We may not be able to visualise it, but the group law still holds in fields such as $\mathbb{Z}/p$. In any case, $\mathcal{O} \in C(\mathbb{F})$ for all fields $\mathbb{F}$.

3 The Discriminant

If we have a rational curve in the normal form $y^2 = x^3 + ax^2 + bx + c$, using suitable transformations $X = d^2x$ and $Y = d^3y$ allows us to clear any denominators in the coefficients a, b and c. So from now we can assume the cubic equation to be an integer equation.

This chapter is set out to prove a theorem by Nagell and Lutz. The theorem states that a rational point (x, y) of finite order must have integer coordinates and $y = 0$ or $y|D$ where D is the discriminant of $f(x)$ defined by

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

It can be checked that if we factor f over the complex numbers as

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

then

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

so that if D is non-zero then the roots of $f(x)$ are distinct. Using these facts, there will only be a finite number of steps to find rational points of finite order. We start off by finding D using the coefficients from $f(x)$. Since y divides D, there are only a finite number of possibilities for the value of y. Once we have y, we can equate y^2 with $f(x)$, and since $f(x)$ is a monic integer polynomial, if an integer root exists, it must divide the constant term in $f(x)$. There is now again finitely many cases of possibilities for our first root. This process can be finitely repeated to extract all integer roots of the polynomial. It is worthy to note that this theorem does not imply that for a point (x, y) on the curve with integer coordinates and $y|D$ then the point has finite order.

To prove the second part of Nagell-Lutz theorem, we need the fact that

$$D = \{(18b-6a^2)x-(4a^3-15ab+27c)\}f(x)+\{2a^2-6b)x^2+(2a^3-7ab+9c)x+(a^2b+3ac-4b^2)\}f'(x).$$

The point is that D can be expressed as

$$D = r(x)f(x) + s(x)f'(x)$$

for some integer polynomials $r(x)$ and $s(x)$.

Lemma.
Let $P = (x, y)$ be a point on our cubic curve such that both P and $2P$ have integer coordinates, then either $y = 0$ or $y|D$.

Proof
Assume that $y \neq 0$ then we know that $2P \neq \mathcal{O}$ and we write $2P = (X, Y)$ where by assumption x, y, X, Y are all integers. Rewriting our duplication formulas, we have

$$2x + X = \lambda^2 - a, \qquad \lambda = \frac{f'(x)}{2y}.$$

With x, X and a all integers, it follows that λ must also be an integer and so $2y|f'(x)$; in particular, $y|f'(x)$. Also since $y^2 = f(x)$, we have $y|f(x)$. Now the relation

$$D = r(x)f(x) + s(x)f'(x)$$

implies that y also divides D since $r(x)$ and $s(x)$ will be integers.

□

4 Points of Finite Order Have Integer Coordinates

To show that a positive integer is 1, we could show that it is not divisible by any prime. So to show that a rational in it's lowest fractional term is an integer, we only need to show that it's denominator is not divisible by any prime. So a rational point (x, y) is an integer point if the denominator of x and y is not divisible by any prime p.

Each non-zero rational number can be expressed in the form $\frac{m}{n}p^\nu$ where m, n are integers coprime to p with $n > 0$. The order of such a rational numbers is definedrime to p with $n > 0$. The order of such a rational numbers is defined

$$\text{ord}\left(\frac{m}{n}p^\nu\right) = \nu.$$

If p divides the denominator of the rational number, then the order of the rational number will be negative. Similarly if p divides the numerator of the rational number, then the order of the rational number will be positive. The order of the rational number is zero if and only if p divides neither of the numerator or denominator.

If we write some rational point (x, y) as

$$x = \frac{m}{np^\mu} \qquad \text{and} \qquad y = \frac{u}{wp^\sigma}$$

where $\mu > 0$ and p does not divide m, n, u, w. If we make use of the cubic curve equation and look at the orders of the rational numbers on both sides, we find the relation $2\sigma = 3\mu$ and for a positive integer ν, $\sigma = 3\nu$ and $\mu = 2\nu$. In particular, μ is positive so p also divides the denominator of y. These relations are also true if we start off by assuming that the denominator of y is divisible by p, so if p divides the denominator of either x or y, then p divides both denominators.

Define $C(p^\nu)$ as the set of rational points on the cubic curve such that $p^{2\nu}$ and $p^{3\nu}$ divides the denominators of x and y respectively and we can write

$$C(p^\nu) = \{(x, y) \in C(\mathbb{Q}) \ ; \ \text{ord}(x) \leq -2\nu, \text{ord}(y) \leq -3\nu\}.$$

This way, we can introduce a nested set of inclusions

$$C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset C(p^3) \ldots$$

since denominators that can be divided by p^i can also be divided by p^{i-1}. Again, we let $\mathcal{O}$ be inside each of these sets.

Our objective is to show that points of finite order has integer coordinates and so their coordinate denominator cannot be divided by any primes. This problem can be reformulated to showing that points of finite order does not lie in the set $C(p)$. The first thing we need to show is to prove that $C(p^\nu)$ is a subgroup of $C(\mathbb{Q})$. Here, I'll give a brief outline of the proof.

Firstly, we transform our xy-plane into ts-plane by

$$t = \frac{x}{y} \qquad \text{and} \qquad s = \frac{1}{y}$$

and the cubic equations transforms to

$$s = t^3 + at^2 s + bts^2 + cs^3.$$

There is a one-to-one correspondence with the points in both planes with the exception of $\mathcal{O}$ in the xy-plane and points of order two ($y = 0$) in the ts-plane. Lines in xy-plane also corresponds to lines in the ts-plane so we could check whether the group law holds even after the transformation.

We need to look at a special ring R_p. R_p consists of rational numbers which has order ≥ 0, that is, a number in R_p does not contain a factor of p in the denominator. The units in R_p will be rational numbers of order zero where no p's appear in the numerator or the denominator of the number. This is linked to the divisibilities of the points lying in $C(p)$. For a rational point (x, y) lying in $C(p^\nu)$, we can write the coordinates as

$$x = \frac{m}{np^{2(\nu+i)}} \qquad \text{and} \qquad y = \frac{u}{wp^{3(\nu+i}}$$

for some $i \geq 0$. In the ts-plane, these points are

$$t = \frac{x}{y} = \frac{mw}{nu}p^{\nu+i} \qquad \text{and} \qquad s = \frac{1}{y} = \frac{w}{u}p^{3(\nu+i)}.$$

Now we can see that a point (t, s) is in $C(p^\nu)$ if and only if $t \in p^\nu R_p$ and $s \in p^{3\nu}R_p$. As opposed to the (x, y) case, this means the numerators of t and s are divisible by p^ν and $p^{3\nu}$ respectively.

We need to check that each $C(p^\nu)$ is a subgroup. To verify this, we need to take two points in $C(p^\nu)$ so that p^ν divides the t coordinate of each point (remember we only need to check *one* of the coordinates), and check that p^ν also divides the sum of the two points using the group law. In the ts-plane, our zero point, the identity, is the origin $(0, 0)$.

To find the explicit formulas, we use the exact same method as we used for the xy-plane. Finding the line equation through the two given points P_1, P_2, and inseting it into the cubic equation. The exact formula for slope of the line is

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_1 + t_2)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)}.$$

Let $P_3 = (t_3, s_3)$ be the third intersection of the line $s = \alpha t + \beta$ and the cubic curve. (β can be found instantly using $\beta = s_1 - \alpha t_1 = s_2 - \alpha t_2$.) Comparing

coefficients in the equation combining the line and the cubic give the explicit formula for t_3 as

$$t_3 = -\frac{\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3} - t_2 - t_1$$

and s_3 found by the line equation $s_3 = \alpha t_3 - \beta$. To find $P_1 + P_2$, we take the line through P_3 and the zero element $(0, 0)$ and find the third intersection with the cubic curve. From the symmetry of the curve, if (t, s) is on the curve, so is $(-t, -s)$. This indicates that $P_1 + P_2 = (-t_3, -s_3)$.

Now we inspect every part of the formula for t_3 to check which group of points it lies in. In the numerator of the formula for α, each term lies inside of $p^{3\nu}R_p$ since all of t_1, t_2, s_1, s_2 lies inside $p^{\nu}R_p$, so the numerator is in $p^{2\nu}$. All the terms apart from 1 in the denominator is divisible by p so the denominator is not divisible by p and so has order zero. These two facts together implies that $\alpha \in p^{2\nu}R_p$. Also, terms on the right hand side of the formula $\beta = s - \alpha t$ are in $p^{3\nu}R_p$ means that $\beta \in p^{3\nu}R_p$. The last step is to observe the fraction expression for $t_1 + t_2 + t_3$. The denominator is a unit in R_p since no p divides it. The numerator is evidently in $p^{3\nu}$ so we have

$$t_1 + t_2 + t_3 \in p^{3\nu}R_p.$$

Since t_1 and t_2 are divisible by p, it follows that t_3 is also divisible by p. $t(P_1 + P_2) = -t_3$ so the t coordinate of $(P_1 + P_2)$ lies in $p^{\nu}R$. Hence $C(p^{\nu})$ is closed under addition and is a subgroup of $C(\mathbb{Q})$.

We have shown that

$$t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{3\nu}R_p,$$

or rewritten in a slightly different way,

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3\nu}R_p}.$$

The map $p \mapsto t(p)$ looks like a homomorphism maps elements that follow the cubic curve group law addition to additional group of rational numbers. The fact that $t(P_1 + P_2) \neq t(P_1) + t(P_2)$ doesn't quite make it a homomorphism. However, the kernel of this map is the subgroup $C(p^{3\nu})$, and if we take the quotient group $C(p^{\nu})/C(p^{3\nu})$ to map from instead, we will find a one-to-one homomorphism

$$\frac{C(p^{\nu})}{C(p^{3\nu})} \longrightarrow \frac{p^{\nu}R_p}{p^{3\nu R_p}},$$
$$P = (x, y) \longmapsto t(P) = \frac{x}{y}.$$

Notes:

The quotient group $p^{\nu}R_p/p^{3\nu}R_p$ is a cyclic group of order $p^{2\nu}$.
The quotient group $C(p^{\nu})/C(p^{3\nu})$ is a cyclic group of order p^{σ} for some $0 \leq \sigma 2\nu$.

We can summarise the results by the following proposition:

Proposition

Let p be a prime, R_p be the ring of integers with denominators prime to p, and $C(p^\nu)$ be the set of rational points (x, y) on the cubic of x which has denominators that are divisible by $p^{2\nu}$ plus the point $\mathcal{O}$.
(a) $C(P)$ consists of all rational points (x, y) for which the denominator of either x or y is divisible by p.
(b) For every $\nu \geq 1$, the set $C(p^\nu)$ is a subgroup of the group of rational points $C(\mathbb{Q})$.
(c) the map

$$\frac{C(p^\nu)}{C(p^{3\nu})} \longrightarrow \frac{p^\nu R_p}{p^{3\nu R_p}}, \qquad P = (x, y) \longmapsto t(P) = \frac{x}{y}$$

is a one-to-one homomorphism. (By convention, $\mathcal{O} \mapsto 0$.)

Corollary

(a) For every prime p, the subgroup $C(p)$ does not contain any points of finite order except from $\mathcal{O}$.
(b) If $P = (x, y) \neq \mathcal{O}$ is a rational point of finite order, then x and y are integers.

Proof

(a) Suppose a rational point P has order m. If P is in some subgroup of $C(p)$, the denominator of the point P will be divisible by some finite positive power of p, ν say, and not by $\nu + 1$. This way, we can write $P \in C(p^\nu)$ and $P \notin C(p^{\nu+1})$.

Consider the first case where $p \nmid m$. Use the congruence relation

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3\nu} R_p}$$

with the same point P, m times

$$t(mP) \equiv mt(P) \pmod{p^{3\nu} R_p}.$$

But $mP = \mathcal{O}$ so $t(mP) = t(\mathcal{O}) = 0$ and we have

$$0 \equiv mt(P) \pmod{p^{3\nu} R_p}.$$

Since m is coprime to p, it follows that $t(P) \equiv 0$. This means $P \in C(p^{3\nu})$ and since $\nu > 0$, $P \in C(p^{\nu+1})$ yielding a contradiction.

Now suppose $p|m$. Write $m = pn$ and look at the point $P' = nP$. P has order m so P' has order p; also, $P' \in C(p)$ because as a subgroup, $C(P)$ has closure property. Just as the previous case, there exist some $\nu > 0$ such that $P' \in C(p^\nu)$ but $p \notin C(p^{\nu+1})$. Using the congruence relation again

$$0 = t(\mathcal{O}) = t(pP') \equiv pt(P') \pmod{p^{3\nu} R_p}.$$

So $t(P') \equiv 0 \pmod{p^{3\nu-1}R_p}$, but $3\nu - 1 \geq \nu + 1$ yields the contradiction $P' \in C(p^{\nu+1})$.
This completes the proof of part (a).
(b) Since no points of finite order lies in $C(p)$ for any prime p, all points of finite order does not have a denominator that can be divided by any prime and so must have integer coordinates.

□

5 The Nagell-Lutz Theorem and Further Developments

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 $f(x)$,

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

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.

To close the final step of the proof of the theorem, we go back to the lemma we used. The lemma required that the finite order element P and $2P$ have integer coordinates. We have proved that points of finite order has integer coordinates, since P has finite order, $2P$ must also have finite order.

It is important to remember that the theorem is not an "if and only if" statement, that is, there could be integer points that satisfies $y = 0$ or $y|D$ that does not have finite order. To identify a point of finite order, one must be able to find some integer n such that $nP = \mathcal{O}$. We could though, however, identify points of *infinite* order easily with this theorem. For an arbitrary point P, we can compute the coordinates of αP for some integer α. Now if αP does not have integer coordinates, then it has infinite order and P also must have infinite order.

The points of order two and three has been discuss earlier in this section. The natural question is what other orders could occur. Take the example

$$y^2 = x^3 - x^2 + x.$$

The point $P = (1, 1)$ has order four. It can be easily verified that $2P = (0, 0)$ and we know $(0, 0)$ has order two. $3P = (1, -1)$ also has order four. It is possible to show that there are no other points of finite order on this curve

using Nagell-Lutz theorem. The discriminant $D = -3$ for this curve so y could take the values $\pm 1, \pm 3$. To find possible x, we have the equation

$$x^3 - x^2 + x - 9 = 0.$$

The possible rational roots of x here must divide 9 but we can check quickly that $\pm 1, \pm 3, \pm 9$ are all not roots of the equation. So the curve does not contain any other points finite order.

It is in fact possible to write infinitely many curves with a point of order four. Similarly, it is also possible to write curves with orders 5, 6, 7, 8, 9, 10 or 12. This section will end with the following theorem that will not be proved:

Mazur's Theorem

Let C be a non-singular rational cubic curve, and suppose that $C(\mathbb{Q})$ contains a point of finite order m. Then either

$$1 \leq m \leq 10 \qquad \text{or} \qquad m = 12.$$

More precisely, the set of all points of finite order in $C(\mathbb{Q})$ forms a subgroup which has one of the following two forms:
(i) A cyclic group of order N with $1 \leq N \leq 10$ or $N = 12$.
(ii) The product of a cyclic group of order two and a cyclic group of order $2N$ with $1 \leq N \leq 4$.