Points of Finite Order Exercises

1. Let C be a non-singular curve given by an equation

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

with integer coefficients. The duplication formula is

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

where ϕ is the indicated polynomial.

(a) Let $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ be the discriminant of $f(x)$. Find the polynomials $F(X)$ and $\Phi(X)$ so that

$$F(X)f(X) + \Phi(X)\phi(X) = D.$$

(*Hint.* $F(X)$ has degree 3 and $\Phi(X)$ has degree 2.)

(b) If $P = (x, y)$ is a rational point of finite order on C, prove that either $2P = \mathcal{O}$ or else $y^2|D$. (this is the strong form of the Nagell-Lutz theorem.)

Solution

(a) This is a rather tedious exercise. *Outline*: Using the hints, we can write

$$F(X) = \alpha_1 x^3 + \alpha_2 x^2 + \alpha_3 x + \alpha_4 \quad \text{and} \quad \Phi(X) = \beta_1 x^2 + \beta_2 x + \beta_3.$$

Insert these expression into $F(X)f(X) + \Phi(X)\phi(X) = D$ and equate the coefficients of successive positive powers of x to zero and the constant as D.

(b) If P has finite order, then $2P$ also has finite order and so they both have integer coordinates. The duplication formula

$$x(2P) = \frac{\phi(x)}{4f(x)} = \frac{\phi(x)}{4y^2}$$

show that y^2 divides $\phi(x)$ since $x(2P)$ is an integer. Furthermore, since $y^2 = f(x)$, y^2 divides $f(x)$. From part (a), it is now clear that the equation

$$F(X)f(X) + \Phi(X)\phi(X) = D$$

indicates y^2 divides D.

2. Let $p \geq 2$ be a prime and let C be the cubic curve

$$C \ : \ y^2 = x^3 + px.$$

Find all points of finite order in $C(\mathbb{Q})$.

Solution

Work out the discriminant first with $a = c = 0$ and $b = p$.

$$\begin{aligned} D &= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \\ &= -4p^3 \end{aligned}$$

By the strong form of Nagell-Lutz, either $y = 0$ or $y^2|D$. For $y = 0$, the equation becomes $0 = x^3 + px = x(x^2 + p)$ for which $x = 0$ is the only rational solution. So $(0, 0)$ is a rational point. For non-zero y, the possibilities are $\pm 1, \pm 2, \pm p, \pm 2p$. By symmetry of the curve, we can only consider the positive values of y. Since y^2 will be positive for all non-zero real y, $p > 0$ implies $x > 0$.

Suppose $y = 1$, then since $p \geq 2$, a positive integer for x means that $x^3 + xp \geq 2$ contradicting the equation of curve. So $y \neq \pm 1$. If $y = 2$ then $y^2 = 4$ which fixes $x < 2$ and the equation $4 = x^3 + px$ has solution $x = 1$ when $p = 3$. So there are two potential points of finite order, $(1, 2)$ and $(1, -2)$. Using the duplication formula for these points,

$$\begin{aligned} x(2P) &= \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)} \\ &= \frac{1 - 2p + p^2}{4 + 4p} \\ &= \frac{1 - 6 + 9}{4 + 12} \\ &= \frac{4}{16} = \frac{1}{4} \end{aligned}$$

we find that $2P$ does not have integer coordinates and so $(1, 2)$ and $(1, -2)$ cannot have finite order.

The remaining possible values of y are p and $2p$. If $y = p$, we have the equation $x^3 + px - p^2 = 0$. This is a monic polynomial so the root of the polynomial should divide the constant term. We are looking for integer solutions and so the possibilities for x are $1, p, p^2$. For $x = 1$,

$$1 + p - p^2 < 0$$

since $p > 2$. Similarly, inequalities for $x = p, p^2$ are respectively

$$p^3 + p^2 - p^2 = p^3 > 0 \quad \text{and} \quad p^6 + p^3 - p^2 > 0$$

Finally, for $y = 2p$, the equation of curve is $x^3 + px - 4p^2 = 0$. x must divide $4p^2$ so the possibilities are $1, 2, 4, p, 2p, 4p, p^2, 2p^2, 4p^2$. Consider $x = 2p$ first, we have the equation $8p^3 + 4p^2 - 4p^2 = 8p^3 > 0$. We can now eliminate the possibilities greater than or equal to $2p$ since the equation will end up with a 'greater than' inequality. Suppose $x = 4$, the equation $64 + 4p - 4p^2 = 0$ cannot be solved with a prime p. Also, if $x = 1$ or 2, We get a 'less than' inequality.

The last choice is where $x = p$. The equation $p^3 + p^2 - 4p^2 = p^3 - 3p^2 = 0$ can only be solved if $p = 3$. We have now another pair of potential points of finite order, namely, $(p, 2p)$ and $(p, -2p)$. Again, we use the duplication formula as a basic first step to check the finiteness of the order of a point.

$$\begin{aligned} x(2P) &= \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)} \\ &= \frac{p^4 - 2p^3 + p^2}{4(p^3 + p^2)} \\ &= \frac{81 - 54 + 9}{4(27 + 9)} \\ &= \frac{36}{4(36)} = \frac{1}{4} \end{aligned}$$

Again, $x(2P)$ not an integer implies $(p, 2p)$ and $(p, -2p)$ does not have finite order.

The points of finite order for the curve $y^2 = x^3 + px$ are $(0, 0)$ and, as always, the point at infinity, $\mathcal{O}$.