Universitá degli Studi Roma Tre - Corso di Laurea in Matematica

Esercizi CR510

Dario Giannini

10 Marzo 2014

1. (a) Sia $x^3 + Ax^2 + Bx + C$ polinomio di terzo grado monico e siano x_1, x_2, x_3 le sue tre radici $\Rightarrow$
$x^3 + Ax^2 + Bx + C = (x - x_1)(x - x_2)(x - x_3) =$
$= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3$.
Affinché l'uguaglianza sia soddisfatta é necessario che $C = -x_1x_2x_3$.

(b) Siano $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ con $x_1 \neq 0$ e $x_2 \neq 0$.
Si vuole dimostrare che $P_3 = (x_3, y_3) = P_1 + P_2 =$
$= (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1)$ dove $m = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)$
sfruttando il punto precedente.
Suppongo $x_1 \neq x_2$ in quanto avrei il caso banale $P_1 + P_2 = \infty$.
Metto a sistema la retta passante per i due punti P_1 e P_2 e la curva ellittica per trovare il terzo punto d'intersezione fra queste.

$$\begin{cases} y = m(x - x_1) + y_1 \\ y^2 = x^3 + Ax + B \end{cases}$$

$(m(x - x_1) + y_1)^2 = x^3 + Ax + B \quad \Rightarrow$
$m^2x_1^2 + m^2x^2 - 2m^2xx_1 + y_1^2 + 2mxy_1 - 2mx_1y_1 = x^3 + Ax + B$
$x^3 - m^2x^2 + (A + 2m^2x_1 - 2my_1)x + B - m^2x_1^2 - y_1^2 + 2mx_1y_1 = 0$
Da cui sfruttando il punto precedente si ha che
$B - m^2x_1^2 - y_1^2 + 2mx_1y_1 = -x_1x_2x_3 \quad \Rightarrow \quad x_3 = \dfrac{m^2x_1^2 + y_1^2 - B - 2mx_1y_1}{x_1x_2}$
N.B.: Posso dividere senza problemi per x_1 e x_2 in quanto li ho supposti non nulli per ipotesi.
Sfruttando il fatto che $B = y_1^2 - x_1^3 - Ax_1$ poiché $(x_1, y_1) \in E$ si ha che:

$$x_3 = \frac{m^2x_1 + x_1^2 + A - 2my_1}{x_2}$$

A questo punto sostituisco A con la seguente espressione:

$$A = x_1x_2 + x_1x_3 + x_2x_3 - 2m^2x_1 + 2my_1$$

in quanto $A + 2m^2x_1 - 2my_1 = x_1x_2 + x_1x_3 + x_2x_3$.
Tale identitá é ottenuta dalla relazione tra le radici e il coefficiente del termine di primo grado trovata nel punto precedente.
Sostituendo si ha che:

$$x_3 = \frac{m^2x_1 + x_1^2 - 2my_1 + x_1x_2 + x_1x_3 + x_2x_3 - 2m^2x_1 + 2my_1}{x_2}$$

$$x_3 = \frac{-m^2x_1 + x_1^2 + x_1x_2 + x_1x_3 +}{x_2} + x_3$$

A questo punto semplificando gli x_3 posso anche semplificare il denominatore ottenendo:

$$-m^2x_1 + x_1^2 + x_1x_2 = -x_1x_3 \quad \Rightarrow$$
$$x_3 = m^2 - x_1 - x_2$$

Da ció si ricava subito che anche la formula per calcolare y_3 é corretta in quanto riflessione rispetto l'asse delle x del terzo punto di intersezione.

2. $(3,5) \in E : y^2 = x^3 - 2$ quindi per trovare un altro punto della curva ellittica sfrutto le formule di duplicazione del punto $(3,5)$.
   $2(3,5) = (m^2 - 6, m(m^2 - 9) - 5)$ dove $m = \frac{3x^2}{2y}|_{(3,5)} = \frac{27}{10}$.
   Basta sostituire m all'interno dell'espressione per ottenere il seguente punto che verifica l'equazione di E:

   $$P = \left(\frac{129}{100}, \frac{383}{1000}\right)$$

3. Siano $P = (2,9)$,$Q = (3,10)$ e $R = (-4,-3)$ e
   sia $E: \ y^2 = x^3 + 73$

   (a) $(P+Q) = (2,9)+(3,10) = (m^2-2-3, m(2-m^2+5)-9) = (-4,-3)$
   in quanto in questo caso $m = 1$.
   $(P+Q)+R = (-4,-3)+(-4,-3) = 2(-4,-3) =$
   $= (m^2+8, m(-4-m^2-8)-3)$
   dove $m = \frac{3x^2}{2y}|_{(-4,-3)} = -8$
   Sostituendo il valore di m ottenuto si ha che:

   $$(P+Q)+R = (72, 611)$$

   (b) $(Q+R) = (3,10)+(-4,-3) = (m^2-3+4, m(3-m^2-1)-10)$
   dove $m = \frac{13}{7} \quad \Rightarrow$

   $$(Q+R) = \left(\frac{218}{49}, -\frac{4353}{343}\right)$$

   .
   $P+(Q+R) = (2,9)+\left(\frac{218}{49}, -\frac{4353}{343}\right) = \left(m^2 - 2 - \frac{218}{49}, m\left(2 - \left(m^2 - 2 - \frac{218}{49}\right)\right) - 9\right)$
   dove $m = -\frac{62}{7} \quad \Rightarrow$
   Sostituendo il valore di m ottenuto si ha che:

   $$P+(Q+R) = (72, 611)$$

N.B.: Si noti come i risultati di questo esercizio siano coerenti con il fatto che la somma sia associativa.

4. Sia $E : y^2 = x^3 - 34x + 37$ e siano $P = (1,2), Q = (6,7) \in E$.

   - $P + Q = (m^2 - 7, m(1 - m^2 + 7) - 2) = (-6, -5)$ in quanto m=1.
   - $2P = 2(1,2) = (m^2 - 2, m(1 - m^2 + 2) - 2)$
     dove $m = \dfrac{3x^2 - 34}{2y}|_{(1,2)} = -\dfrac{31}{4}$
     Andando a sostituire il valore di m otteniamo:
     $$2P = \left(\frac{929}{16}, \frac{28175}{64}\right)$$
     A questo punto é semplice notare che:
     $$\left(\frac{929}{16}, \frac{28175}{64}\right) \equiv (-6, -5) \equiv (4, 0) \ \ (mod\, 5)$$

5. Sia $E: \ y^2 = x^3 + Ax + B$ e sia $(u, 0) \in E$.
   Supponiamo per assurdo che $3u^2 + A = 0 \ \Rightarrow$
   Poiché $(u, 0) \in E$ $u^3 + Au + B = 0$, quindi u sarebbe una radice multipla di $x^3 + Ax + B$.
   Infatti $(x^3 + Ax + B)' = 3x^2 + A$ e u é una radice con molteplicitá almeno 2 in quanto annulla anche la derivata oltre al polinomio stesso. Tuttavia il fatto che u sia una radice multipla costituisce un assurdo poiché per ipotesi E é una curva ellittica e per definizione $\Delta_E \neq 0$ (le radici del polinomio di terzo grado sono distinte, al massimo ce ne sono due complesse).

6. $P + Q + R = \infty \ \ \Leftrightarrow \ \ P + Q + R = \infty \ \ \Leftrightarrow \ \ (P + Q) = -R$
   ma per definizione di somma ció é possibile se e soltanto se la retta che passa per P e Q interseca la curva ellittica in R, quindi se e soltanto se P,Q e R sono collineari.