Universitá degli Studi Roma Tre - Corso di Laurea in Matematica

Esercizi CR510

Dario Giannini

17 Marzo 2014

1. $C : u^2 + v^2 = c^2(1 + du^2v^2)$ é una curva ellittica parametrizzata tramite le coordinate di Edwards, in cui la somma é definita nella maniera seguente:
$$(u_1, v_1) + (u_2, v_2) = \left(\frac{u_1v_2 + u_2v_1}{c(1 + du_1u_2v_1v_2)}, \frac{v_1v_2 - u_1u_2}{c(1 + du_1u_2v_1v_2)}\right)$$
Si deve mostrare che il punto $P = (c, 0)$ ha ordine 4, ossia che $4P = (0, c)$, che é l'identitá del gruppo.
$P + P = (c, 0) + (c, 0) = (0, -c)$
$4P = 2P + 2P = (0, -c) + (0, -c) = (c, 0)$.

2. Come suggerito dal libro di testo si prova a dimostrare l'algoritmo dei quadrati successivi per induzione sulla lunghezza della rappresentazione binaria di k.
Sia $P \in E(\mathbb{F}_q)$ e $k \in \mathbb{N}$
(1) $a = k$; $B = \infty$; $C = P$.
(2) Se $2|a \;\Rightarrow a \leftarrow \frac{a}{2}$; $B \leftarrow B$; $C \leftarrow 2C$.
(3) Se a é dispari $\Rightarrow a \leftarrow a - 1$; $B \leftarrow B + C$; $C \leftarrow C$.
(4) If $(a \neq 0)$ GO TO **(2)**.
(5) OUTPUT $B = kP$.
Sia $k = a_0 + 2a_1 + 4a_2 + \ldots + 2^l a_l$.
BASE INDUZIONE: Sia $l = 0 \to k = a_0$ e ho due casi:
Se $a_0 = 0$ faccio una volta il passo **(2)** e come output ho $B = \infty$.
Se $a_0 = 1$ faccio una volta il passo **(3)** e come output ho $B = P$.
PASSO INDUTTIVO: Suppongo che l'algoritmo funzioni per $l-1$, ossia per tutti i numeri del tipo $k_0 = a_0 + 2a_1 + 4a_2 + \ldots + 2^{l-1}a_{l-1}$ e verifico che valga anche per l.
$k = a_0 + 2a_1 + 4a_2 + \ldots + 2^{l-1}a_{l-1} + 2^l a_l = k_0 + 2^l a_l$
Per ipotesi induttiva so che l'algoritmo vale per k_0, quindi:
$$kP = (k_0 + 2^l a_l)P = k_0P + 2^l a_l P$$
Mi basta quindi solamente verificare che funzioni per $2^l a_l$.
Applicando l'algoritmo devo effettuare l volte il passo **(2)** $a \leftarrow 1$; $B \leftarrow \infty$; $C \leftarrow 2^l P$
e una volta il passo **(3)** $a \leftarrow 0$; $B \leftarrow \infty + 2^l P$; $C \leftarrow C$.
Dunque l'algoritmo dei quadrati successivi funziona poiché B é proprio l'output finale.

3. $$E: \; x^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
Si vuole dimostrare la formula per calcolare il punto opposto nel caso dell'equazione di Weierstrass generale, ossia:
$$-(\alpha, \beta) = (\alpha, -a_1\alpha - a_3 - \beta)$$

Per farlo passo alle coordinate proiettive della curva; in particolare si é interessati a trovare l'altro punto d'intersezione tra la curva ellittica e la retta passante per il punto all'infinito $[0:1:0]$ e $[\alpha:\beta:1]$ (sarebbe (α,β) in coordinate affini). Tale punto sará proprio l'opposto di (α,β).

$$\begin{cases} x = \alpha z \\ y^2 z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3 \end{cases}$$

$$\begin{cases} x = \alpha z \\ y^2 z + a_1 \alpha yz^2 + a_3 yz^2 = \alpha^3 z^3 + a_2 \alpha^2 z^3 + a_4 \alpha z^3 + a_6 z^3 \end{cases}$$

Se $z = 0 \quad \Rightarrow \quad x = 0$ trovo il punto all'infinito che giá sapevo essere soluzione del sistema.
Pongo $z = 1$ in quanto il punto trovato deve essere in corrispondenza biunivoca con il piano affine e cerco le altre due soluzioni del sistema (ossia gli altri due punti di intersezione).

$$\begin{cases} x = \alpha \\ y^2 + a_1 \alpha y + a_3 y = \alpha^3 + a_2 \alpha^2 + a_4 \alpha + a_6 \end{cases}$$

$y = \beta$ é sicuramente una radice in quanto $(\alpha,\beta) \in E$ per ipotesi (é inoltre coerente con il fatto che (α,β) é soluzione per costruzione).
L'altro punto di soluzione, ossia il punto che stiamo cercando, sará determinato dall'altra radice del polinomio in y. Tale radice é $y = -\beta - \alpha a_1 - a_3$ come volevasi dimostrare. Infatti: $(-\beta - \alpha a_1 - a_3)^2 + (a_1\alpha + a_3)(-\beta - \alpha a_1 - a_3) = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6$
Da cui andando a svolgere tutti i calcoli e semplificando il piú possibile si arriva alla seguente:

$$\beta^2 + \alpha\beta a_1 + a_3\beta = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6$$

la quale é sempre verificata in quanto (α,β) é un punto di E.
Si é dunque dimostrato che il terzo punto di intersezione, nonché il punto opposto, é il punto $(\alpha, -a_1\alpha - a_3 - \beta)$.

4. Intuitivamente se si va dalla sfera al piano proiettivo tramite l'applicazione identitá la controimmagine di un punto del piano proiettivo sará costituita da due punti della sfera antipodali fra loro ($[x:y:z] = [-x:-y:z]$).
Infatti un punto del piano proiettivo puó essere identificato ad una retta passante per l'origine in $\mathbb{R}^3$ (insieme dei punti tra loro proporzionali) e ogni retta passante per l'origine interseca la sfera in due punti.

5. (a) Suppongo $a_1 \neq 0$ e che le due rette siano distinte tra loro, ossia che il rango della matrice $M = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}$ é uguale a 2. Detto in altri termini, almeno uno fra i determinanti delle sottomatrici quadrate di ordine due deve essere diverso da zero. Suppongo che $b_2 a_1 - a_2 b_1 \neq 0$ (sempre vero a meno di scambiare l'ordine delle variabili).

$$\begin{cases} a_1 x + b_1 y + c_1 z = 0 \\ a_2 x + b_2 y + c_2 z = 0 \end{cases} \quad \begin{cases} x = -\dfrac{b_1 y + c_1 z}{a_1} \\ y\left(b_2 - \dfrac{a_2 b_1}{a_1}\right) = z\left(\dfrac{a_2 c_1}{a_1} - c_2\right) \end{cases} \quad \begin{cases} x = -\dfrac{b_1 y + c_1 z}{a_1} \\ y = \dfrac{a_2 c_1 - a_1 c_2}{b_2 a_1 - a_2 b_1} z \end{cases}$$

Se pongo $\lambda = \dfrac{a_2c_1 - a_1c_2}{b_2a_1 - a_2b_1}$ le soluzioni del sistema saranno:

$$\left[-\frac{b_1\lambda + c_1}{a_1} z : \lambda z : z \right]$$

al variare di z in $\mathbb{R}$. Tuttavia ci si deve ricordare che si é sul piano proiettivo e che in realtá su di esso questo insieme di punti al variare di z in $\mathbb{R}$ corrisponde ad un solo punto di $\mathbb{P}_2$. Infatti le componenti di ogni punto dell'insieme dipendono linearmente dal parametro z e quindi individuano su $\mathbb{P}_2$ il solo punto $\left[-\dfrac{b_1\lambda + c_1}{a_1} : \lambda : 1 \right]$ ottenuto dividendo per z ogni componente.
Ricapitolando nel piano proiettivo si possono presentare due casi distinti:
Se $rank(M) = 2$, e quindi le due rette non coincidono, c'é un solo punto di intersezione fra le due.
Se $rank(M) = 1$, e quindi le rette coincidono, ce ne sono infiniti.

(b) Supponiamo che esistano due rette r_1, r_2 che passino entrambe per i punti $P_1, P_2 \in \mathbb{P}_2$ con $P_1 \neq P_2 \quad \Rightarrow \quad r_1 \cap r_2 \supset \{P_1, P_2\}$.
Tuttavia per il punto precedente tale configurazione puó essere possibile se e soltanto se $r_1 = r_2$.

6. Per dimostrare che le equazioni parametriche e cartesiane dell'esercizio individuano difatto la stessa retta si vuole mostrare che se una tripla $[x : y : z]$ soddisfa una delle due allora soddisfa anche l'altra (e viceversa).
Sia $[x : y : z]$ tale che $\begin{cases} x = a_1u + b_1v \\ y = a_2u + b_2v \\ z = a_3u + b_3v \end{cases}$ e andiamo a sostituire tali valori di x, y, z nell'equazione cartesiana per verificare se é soddifatta o meno.

$$a(a_1u+b_1v)+b(a_2u+b_2v)+c(a_3u+b_3v) = (aa_1+ba_2+ca_3)u+(ab_1+bb_2+cb_3)v = 0$$

Infatti i coefficienti di u e v sono entrambi nulli in quanto per ipotesi si ha che:

$$(a, b, c) \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix} = (aa_1 + ba_2 + ca_3, ab_1 + bb_2 + cb_3) = (0, 0)$$

Ora si vuole invece mostrare il viceversa, ossia che se $[x : y : z]$ soddisfa $ax + by + cz = 0$ allora soddisfa anche le equazioni parametriche.
L'insieme delle soluzioni di $ax + by + cz = 0$ é uno spazio vettoriale di dimensione 2 per Rouché-Capelli.
I vettori $[a_1 : a_2 : a_3]$ e $[b_1 : b_2 : b_3]$ soddisfano l'equazione e sono linearmente indipendenti per ipotesi, in quanto $rank(M) = 2$, quindi generano tale spazio e in particolare ne rappresentano una base. Ogni vettore dello spazio delle soluzioni, ossia ogni punto di $\mathbb{P}_2$ che soddisfa l'equazione cartesiana, potrá essere scritto come combinazione lineare di $[a_1 : a_2 : a_3]$ e

$[b_1 : b_2 : b_3]$, ossia:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} u + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} v$$

7. (a) É data la curva ellittica scritta in forma di Legendre:

$$E:\ y^2 = x(x-1(x-\lambda)) = x^3 - (1+\lambda)x^2 + \lambda x$$

Innanzitutto applico il cambiamento di variabile $\begin{cases} x \longmapsto x + \dfrac{1+\lambda}{3} \\ y \longmapsto y \end{cases}$ per riportare l'equazione nella forma canonica di Weierstrass.

$$y^2 = \left(x + \frac{1+\lambda}{3}\right)^3 - (1+\lambda)\left(x + \frac{1+\lambda}{3}\right)^2 + \lambda\left(x + \frac{1+\lambda}{3}\right)$$

Facendo tutti i calcoli si arriva alla seguente equazione:

$$y^2 = x^3 + \left(-\frac{\lambda^2-\lambda+1}{3}\right)x - \frac{2}{27}(\lambda+1)(\lambda-2)\left(\lambda - \frac{1}{2}\right)$$

Ora si deve solamente calcolare il j-invariante della forma di Weierstrass. Si tratteranno numeratore e denominatore separatamente per poter seguire al meglio i calcoli.

$$j(E) = 1728\frac{4A^3}{4A^3+27B^2}$$

NUMERATORE:

$N = 2^6 * 3^3 * 4\left(-\dfrac{\lambda^2-\lambda+1}{3}\right)^3 = -2^8(\lambda^2-\lambda+1)^3.$

DENOMINATORE:

$$\begin{aligned}
D &= 4\left(-\frac{\lambda^2-\lambda+1}{3}\right)^3 + 27\left[-\frac{2}{27}(\lambda+1)(\lambda-2)\left(\lambda-\frac{1}{2}\right)\right]^2 + \\
&+\frac{4}{27}\left[-(\lambda^2-\lambda+1)^3 + (\lambda-2)^2(\lambda+1)^2\left(\lambda-\frac{1}{2}\right)\right] = \\
&= \frac{4}{27}\left[-\lambda^6 + 3\lambda^4(\lambda-1) - 3\lambda^2(\lambda-1)^2 + (\lambda-1)^3 + \left(\lambda^3 - \frac{3}{2}\lambda^2 - \frac{3}{2}\lambda + 1\right)^2\right] = \\
&= \frac{4}{27}\left(-\lambda^6 + 3\lambda^5 - 3\lambda^4 - 3\lambda^4 + 6\lambda^3 - 3\lambda^2 + \lambda^3 - 3\lambda^2 + 3\lambda - 1\right) + \\
&+\frac{4}{27}\left(\lambda^6 + \frac{9}{4}\lambda^4 + \frac{9}{4}\lambda^2 + 1 - 3\lambda^5 - 3\lambda^4 + 2\lambda^3 + \frac{9}{2}\lambda^3 - 3\lambda^2 - 3\lambda\right) = \\
&= \frac{4}{27}\left[-\frac{27}{4}\lambda^4 + \frac{27}{2}\lambda^3 - \frac{27}{4}\lambda^2\right] = -\lambda^2(\lambda-1)^2
\end{aligned}$$

A questo punto basta mettere insieme le due cose per trovare che:

$$j(E) = \frac{N}{D} = 2^8\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

(b) Nell'equazione di Legendre il valore di λ é definito come

$$\lambda := \frac{e_3 - e_1}{e_2 - e_1}$$

dove e_i sono le radici del polinomio in x. Tale valore di λ dipenderá quindi per costruzione dall'ordine che ho dato alle radici. In generale, se scambio l'ordine delle radici, a partire dalla curva originale faccio cambiamenti di variabile che generano valori di λ diversi. Questi ultimi dovranno peró descrivere la stessa curva ellittica quindi dall'espressione in **(a)** si dovrá ricavare lo stesso valore del j-invariante! $|S_3| = 6$, quindi esistono sei permutazioni delle radici da cui ricavo valori di λ differenti. Questi ultimi dipendono da λ e sono contenuti nell'insieme

$$\left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\right\}$$

É doveroso precisare che questo discorso puó essere fatto se e solo se gli elementi di questo insieme non coincidono fra loro. Ció accade se $\lambda \neq -1, \frac{1}{2}, 2$ o se $\lambda^2 - \lambda + 1 \neq 0$. Tali valori di λ determinano $j(E) = 0, 1728$ (come si vedrá nel punto successivo).
Riassumendo il tutto si ha che se $j(E) \neq 0, 1728$ ci sono 6 valori distinti di λ contenuti nell'insieme descritto sopra per cui la curva ha invariante $j(E)$.

(c) Se $j = 0$ segue subito dal punto **(a)** che $\lambda^2 - \lambda + 1 = 0$.
Se $j = 1728 \;\Rightarrow\; 2^8 \dfrac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$ da cui si ha che:
$4(\lambda^2 - \lambda + 1)^3 = 27\lambda^2(\lambda-1)^2$
$4\lambda^6 - 12\lambda^5 - 3\lambda^4 + 26\lambda^3 - 3\lambda^2 - 12\lambda + 4 = 0$
$(2\lambda-1)^2(\lambda-2)^2(\lambda+1)^2 = 0$, da cui si ricava subito che
se $j = 1728 \;\Rightarrow\; \lambda = -1, \frac{1}{2}, 2$.

8. Siano $C : u^2 - v^2 = 1$ e $P = (u_0, v_0) = (1, 0)$.

(a) Considero C come la curva nel piano uv e definisco L come la retta passante per P con coefficiente angolare m.

$$\begin{cases} u = u_0 + t \\ v = v_0 + mt \end{cases} \quad \Rightarrow \quad \begin{cases} u = 1 + t \\ v = mt \end{cases}$$

Si vuole trovare l'altro punto di intersezione tra L e C. Si ha che: $(1+t)^2 - m^2t^2 = 1 \;\Rightarrow\; t((1-m^2)t + 2)$ I due punti di intersezione saranno individuati da $t = 0$, da cui si ricava il punto di partenza P, e da $t = \dfrac{2}{m^2-1}$ da cui si ricava il secondo punto di intersezione, i.e. il punto che si voleva trovare:

$$u = \frac{m^2+1}{m^2-1} \quad v = \frac{2m}{m^2+1}$$

(b) $u^2 - v^2 = w^2 \;\Rightarrow$ per trovare i punti all'infinito della curva si pone $w = 0$ e si cercano le soluzioni rispetto le altre due variabili. In questo

caso si ha che:
$u^2 = v^2 \;\Rightarrow\; u = \pm v$ da cui si ricavano le soluzioni
$[v : v : 0]$ e $[-v : v : 0]$, al variare di $v \in \mathbb{R}$.
Tali soluzioni nel piano proiettivo corrispondono ai due punti
$[1 : 1 : 0]$ e $[1 : -1 : 0]$.

(c) La parametrizzazione della curva in **(a)** puó essere scritta in coordinate proiettive come $[m^2+1, 2m, m^2-1]$. Se si pone $m = \pm 1$ e si sostituiscono tali valori di m nelle cordinate proiettive di C si ottengono i due punti all'infinito $[1 : 1 : 0]$ e $[1 : -1 : 0]$ ($m = \pm 1$ sono infatti gli unici due valori per cui la terza coordinata si annulla). A livello grafico tutto ció deriva dal fatto che la curva $u^2 - v^2 = 1$ nel piano uv é un iperbole i cui asintoti sono le rette $y = \pm x$. I valori del parametro m corrispondono dunque ai valori dei coefficienti angolari delle due rette che incontrano C all'infinito.

9. Siano $F:\; au^2 + bv^2 = e$ e $G:\; cu^2 + dw^2 = f$.
Si considera $P = (u_0, 0, 0) \in F \cap G$.

(a) Si é visto dall'esercizio precedente che una curva nel piano uv puó essere scritta in funzione del solo parametro m.
In particolare si ha che: $u = u_0 - \dfrac{2au_0}{a+bm^2}$
Sostituendo tale espressione di u in G si ha che:

$$dw^2 = f - c\left(u_0 - \frac{2au_0}{a+bm^2}\right)^2 \Rightarrow dw^2 = f - cu_0^2\left(\frac{bm^2-a}{a+bm^2}\right)^2$$

da cui sfruttando il fatto che $P \in G$, ossia che $cu_0^2 = f$:

$$dw^2 = f\left(1 - \left(\frac{bm^2-a}{bm^2+a}\right)^2\right) \;\Rightarrow\; w^2 = \frac{f}{d}\frac{4abm^2}{bm^2+a}$$

ossia un'espressione del tipo cercato.

(b)
$$J = \begin{pmatrix} F_u & F_v & F_w \\ G_u & G_v & G_w \end{pmatrix} = \begin{pmatrix} 2au & 2bv & 0 \\ 2cu & 0 & 2dw \end{pmatrix}$$

calcolata nel punto $(u_0, 0, 0)$ é uguale a:

$$J = \begin{pmatrix} 2au_0 & 0 & 0 \\ 2cu_0 & 0 & 0 \end{pmatrix}$$

Quindi $rank(J) = 1$ e in particolare non é massimo $\Rightarrow$
Il punto $(u_0, 0, 0)$ é un punto singolare!

10. Si vuole trasformare la cubica $x^3 + y^3 = d$ nella curva ellittica
$E:\; y^2 = x^3 - 432d^2$.
Per prima cosa faccio il seguente cambio di variabile:

$$\begin{cases} x = u + v \\ y = u - v \end{cases} \quad\Rightarrow\; (u+v)^3 + (u-v)^3 = d$$

Da cui si ricava l'equazione:$2u^3+6uv^2-d=0$. A questo punto moltiplico tutto per $\frac{d^2}{u^3}$ ottenendo l'equazione:

$$6\left(\frac{dv}{u}\right)^2=\left(\frac{d}{u}\right)^3-2d^2 \Rightarrow \frac{6}{36^2}\left(36\frac{dv}{u}\right)^2=\frac{1}{6^3}\left(6\frac{d}{u}\right)^3-2d^2$$

A questo punto per ottenere la curva ellittica di arrivo basterá moltiplicare tutto per 6^3 e applicare il cambio di variabili seguente per ottenere E.

$$\begin{cases} x_1 = 6\frac{d}{u} \\ y_1 = 36\frac{dv}{u} \end{cases}$$

11. Per tutti e tre i punti seguenti si dimostrano in maniera analoga i casi particolari.

    - Se $P_1+P_2=\infty$ si ha che: $f(P_1)+f(P_2)=\infty=f(\infty)=f(P_1+P_2)$ in quanto se P_1 e P_2 hanno la stessa ascissa, anche $f(P_1)$ e $f(P_2)$ avranno stessa ascissa (oppure se sono uguali con ordinata nulla anche le loro immagini tramite f saranno uguali con ordinata nulla).
    - Se $P_1=\infty$ allora $f(P_1)+f(P_2)=\infty+f(P_2)=f(P_2+\infty)=f(P_1+P_2)$.

    (a) Sia $\varphi:(x,y)\longmapsto(x,-y)$. Affinché φ sia un omomorfismo deve accadere che:

    $$\varphi(P_1)+\varphi(P_2)=\varphi(P_1+P_2)$$

    Per quanto detto nell'introduzione supponiamo $P_1=(x_1,y_1)\neq(x_2,y_2)=P_2$, con $x_1\neq x_2$.
    $\varphi(P_1)+\varphi(P_2)=(x_1,-y_1)+(x_2,-y_2)=(m^2-x_1-x_2,m(x_1-x_3)+y_1)$ dove $m=-\frac{y_2-y_1}{x_2-x_1}$.
    $\varphi(P_1+P_2)=\varphi[(m'^2-x_1-x_2,m'(x_1-x_3)-y_1)]=$
    $=(m'^2-x_1-x_2,-m'(x_1-x_3)+y_1)$ dove $m'=\frac{y_2-y_1}{x_2-x_1}$.
    Quindi dal fatto che $m=-m'$ segue subito l'uguaglianza.
    In maniera del tutto analoga si tratta il caso in cui $P_1=P_2$, con $y\neq 0$
    Infatti cambia solo il valore di m e m', che sono comunque uno l'opposto dell'altro.
    Stessa cosa si potrá dire per i casi seguenti in cui non verrá neanche menzionato.

    (b) Sia $\psi:(x,y)\longmapsto(\zeta x,-y)$, dove ζ é una radice cubica dell'unitá non banale. Innanzitutto si vuole dimostrare che ψ é una biezione da E in sé, se la curva é della forma $y^2=x^3+B$.
    $Ker(\psi)$ é banale, quindi ψ é iniettiva. Inoltre preso un elemento $(x,y)\in E\ \exists\ (x_1,y_1)\in E$ t.c. $\psi((x_1,y_1))=(x,y)$. Infatti basta prendere $(x_1,y_1)=(\zeta^2x,-y)$.

É da notare il fatto che $(\zeta^2 x, -y) \in E$ solo se E é della forma particolare che si sta trattando.
Ora rimane da mostrare che ψ é un omomorfismo.
$\psi(P_1)+\psi(P_2) = (\zeta x_1, -y_1)+(\zeta x_2, -y_2) = = (m^2-\zeta x_1-\zeta x_2, m(\zeta x_1 - x_3) + y_1)$
dove $m = -\dfrac{y_2 - y_1}{\zeta(x_2 - x_1)} = -\zeta^2 \dfrac{y_2 - y_1}{x_2 - x_1}$.
$\psi(P_1 + P_2) = \psi[(m'^2 - x_1 - x_2, m'(x_1 - x_3) - y_1)] =$
$= (\zeta m'^2 - \zeta x_1 - \zeta x_2, -m'(x_1 - x_3) + y_1)$ dove $m' = \dfrac{y_2 - y_1}{x_2 - x_1}$.
Quindi dal fatto che $m = -\zeta^2 m'$ e $\zeta^3 = 1$ segue subito l'uguaglianza.

(c) Sia $\chi : (x, y) \longmapsto (-x, iy)$ dove i é l'unitá immaginaria, quindi una radice quarta dell'unitá non banale. Innanzitutto si vuole dimostrare che χ é una biezione da E in sé, se la curva é della forma $y^2 = x^3+Ax$. $Ker(\chi)$ é banale, quindi χ é iniettiva. Inoltre preso un elemento $(x, y) \in E \; \exists \; (x_1, y_1) \in E$ t.c. $\chi((x_1, y_1)) = (x, y)$. Infatti basta prendere $(x_1, y_1) = (-x, -iy)$.
É da notare il fatto che $(-x, -iy) \in E$ solo se E é della forma particolare che si sta trattando.
Ora rimane da mostrare che χ é un omomorfismo.
$\chi(P_1) + \chi(P_2) = (-x_1, iy_1) + (-x_2, iy_2) = = (m^2 + x_1 + x_2, m(-x_1 - x_3) - iy_1)$
dove $m = -i\dfrac{y_2 - y_1}{x_2 - x_1}$.
$\chi(P_1 + P_2) = \chi[(m'^2 - x_1 - x_2, m'(x_1 - x_3) - y_1)] =$
$= (-m'^2 + x_1 + x_2, im'(x_1 - x_3) + iy_1)$ dove $m' = \dfrac{y_2 - y_1}{x_2 - x_1}$.
Quindi dal fatto che $m = -im'$ e $i^2 = -1$ segue subito l'uguaglianza.